UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/508,887	10/22/2021	Kevin Alan Tussy	FACETC.0082P	9577

32856 7590 01/18/2024

WEIDE & MILLER, LTD.
10655 PARK RUN DRIVE
SUITE 100
LAS VEGAS, NV 89144

EXAMINER	
ABEDIN, SHANTO	

ART UNIT	PAPER NUMBER
2494	

MAIL DATE	DELIVERY MODE
01/18/2024	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.
17/508,887	16-Jan-2024	11874910

WEIDE & MILLER, LTD.
10655 PARK RUN DRIVE
LAS VEGAS, NV 89144

EGRANT NOTIFICATION

Your electronic patent grant (eGrant) is now available, which can be accessed via Patent Center at https://patentcenter.uspto.gov

The electronic patent grant is the official patent grant under 35 U.S.C. 153. For more information, please visit https://www.uspto.gov/electronicgrants

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/508,887	01/16/2024	11874910	FACETC.0082P	9577

32856 7590 12/27/2023

WEIDE & MILLER, LTD.
10655 PARK RUN DRIVE
SUITE 100
LAS VEGAS, NV 89144

ISSUE NOTIFICATION

The projected patent number and issue date are specified above. The patent will issue electronically. The electronically issued patent is the official patent grant pursuant to 35 U.S.C. § 153. The patent may be accessed on or after the issue date through Patent Center at https://patentcenter.uspto.gov/. The patent will be available in both the public and the private sides of Patent Center. Further assistance in electronically accessing the patent, or about Patent Center, is available by calling the Patent Electronic Business Center at 1-888-217-9197.

The USPTO is implementing electronic patent issuance with a transition period, during which period the USPTO will mail a ceremonial paper copy of the electronic patent grant to the correspondence address of record. Additional copies of the patent (i.e., certified and presentation copies) may be ordered for a fee from the USPTO's Certified Copy Center at https://certifiedcopycenter.uspto.gov/index.html. The Certified Copy Center may be reached at (800)972-6382.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)

(application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Center (https://patentcenter.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Patents Stakeholder Experience (OPSE), Stakeholder Support Division (SSD) at (571)-272-4200.

IR103 (Rev. 10/09)

INVENTOR(s) (Please see PATENT CENTER site https://patentcenter.uspto.gov for additional inventors):

Kevin Alan Tussy, Las Vegas, NV;

APPLICANT(s) (Please see PATENT CENTER site https://patentcenter.uspto.gov for additional applicants):

FaceTec, Inc., Las Vegas, NV;

IR103 (Rev. 10/09)

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/508,887	**12/05/2023 01:56:24 PM Z ET**	**FACETC.0082P**

Title of Invention

FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	9577	FILED BY	Elizabeth Escoffie
PATENT CENTER #	63491850	FILING DATE	10/22/2021
CUSTOMER #	32856	FIRST NAMED INVENTOR	Kevin Alan Tussy
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Chad Miller

Documents

TOTAL DOCUMENTS: 2

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
CWMW18744TRANS.pdf	1	Transmittal Letter	21 KB
FACETC0082PISSEFEE.pdf	1	Issue Fee Payment (PTO-85B)	198 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
CWMW18744TRANS.pdf	3CD91356387EE9C1F44307EB7DC52EA4BB9EFFA51379C896BE6BE655FA8BAB8FE7016BF659D19D2FCDBB9BABA7EE6CC37F107C423D87C596E83C31DF1FC9AF8B

FACETC0082PISSEFEE.pdf	5BFB5FF84D21153C2A5689E17982EC2ABDBFC22033881938E D5C2BB3A45B7ECBE1E328007B98D756280AA5AD8FFD7CE4E 0C9D34F1B1CB77BFDFCC7F326B26391

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/508,887	12/05/2023 01:56:24 PM Z ET	FACETC.0082P

Title of Invention

FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	9577	FILED BY	Elizabeth Escoffie
PATENT CENTER #	63491850	AUTHORIZED BY	Chad Miller
CUSTOMER #	32856	FILING DATE	10/22/2021
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	Kevin Alan Tussy

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
CARD / 8764	E2023B5D57209600	Chad Miller

PRE-AUTHORIZED ACCOUNT	PRE-AUTHORIZED CATEGORY
502200	37 CFR 1.16 (National application filing, search, and examination fees); 37 CFR 1.17 (Patent application and reexamination processing fees); 37 CFR 1.19 (Document supply fees); 37 CFR 1.20 (Post Issuance fees); 37 CFR 1.21 (Miscellaneous fees and charges)

FEE CODE	DESCRIPTION	ITEM PRICE($)	QUANTITY	ITEM TOTAL($)
2501	UTILITY ISSUE FEE	480.00	1	480.00
			TOTAL AMOUNT:	$480.00

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement

Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications. **Because electronic patent issuance may occur shortly after issue fee payment, any desired continuing application should preferably be filed prior to payment of this issue fee in order not to jeopardize copendency.**

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

32856 7590 09/05/2023

WEIDE & MILLER, LTD.
10655 PARK RUN DRIVE
SUITE 100
LAS VEGAS, NV 89144

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

Chad W. Miller	(Typed or printed name)
/Chad W. Miller/	(Signature)
December 5, 2023	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/508,887	10/22/2021	Kevin Alan Tussy	FACETC.0082P	9577

TITLE OF INVENTION: FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0.00	$0.00	$480	12/05/2023

EXAMINER	ART UNIT	CLASS-SUBCLASS
ABEDIN, SHANTO	2494	713-186000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/AIA/122 or PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Weide & Miller, Ltd.
2
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: FaceTec, Inc.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Las Vegas, NV

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☑ Corporation or other private group entity ☐ Government

4a. Fees submitted: ☑ Issue Fee ☑ Publication Fee (if required)

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

☑ Electronic Payment via Patent Center or EFS-Web ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. 502200

5. **Change in Entity Status** (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

☐ Applicant asserting small entity status. See 37 CFR 1.27

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

☐ Applicant changing to regular undiscounted fee status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Chad W. Miller/ Date December 5, 2023

Typed or printed name Chad W. Miller Registration No. 44,943

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor	:	Kevin Alan Tussy
Appl. No.	:	17/508,887
Filed	:	October 22, 2021
For	:	FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS
Examiner	:	Shanto Abedin

Group Art Unit: 2494

I hereby certify that this correspondence and all marked attachments are being deposited with the United States Patent Office via EFSWeb filing, on:

December 5, 2023
(Date)

/Chad W. Miller/
Chad W. Miller Reg. No. 44,943

TRANSMITTAL

Mail Stop Issue Fee
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In response to the Notice of Allowance mailed September 5, 2023 with respect to the above-referenced application please find enclosed the following:

(X) Part B of the Issue Fee Transmittal.

(X) The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Account No.: 502200.

Respectfully submitted,

Dated: December 5, 2023

By: /Chad W. Miller/
Chad W. Miller
Attorney of Record
Registration No. 44,943
Weide & Miller, Ltd.
10655 Park Run Drive, Suite 100
Las Vegas, NV 89144
(702) 382-4804 (Pacific Time)
cmiller@weidemiller.com

CWM-W-18744

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

32856 7590 09/05/2023

WEIDE & MILLER, LTD.
10655 PARK RUN DRIVE
SUITE 100
LAS VEGAS, NV 89144

EXAMINER	
ABEDIN, SHANTO	
ART UNIT	**PAPER NUMBER**
2494	

DATE MAILED: 09/05/2023

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/508,887	10/22/2021	Kevin Alan Tussy	FACETC.0082P	9577

TITLE OF INVENTION: FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0.00	$0.00	$480	12/05/2023

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 40% the amount of undiscounted fees, and micro entity fees are 20% the amount of undiscounted fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications. **Because electronic patent issuance may occur shortly after issue fee payment, any desired continuing application should preferably be filed prior to payment of this issue fee in order not to jeopardize copendency.**

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

32856 7590 09/05/2023
WEIDE & MILLER, LTD.
10655 PARK RUN DRIVE
SUITE 100
LAS VEGAS, NV 89144

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)

(Signature)

(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/508,887	10/22/2021	Kevin Alan Tussy	FACETC.0082P	9577

TITLE OF INVENTION: FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0.00	$0.00	$480	12/05/2023

EXAMINER	ART UNIT	CLASS-SUBCLASS
ABEDIN, SHANTO	2494	713-186000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/AIA/122 or PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1________________

2________________

3________________

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. Fees submitted: ❑Issue Fee ❑Publication Fee (if required)

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

❑ Electronic Payment via Patent Center or EFS-Web ❑ Enclosed check ❑ Non-electronic payment by credit card (Attach form PTO-2038)

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. __________

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

❑ Applicant asserting small entity status. See 37 CFR 1.27

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

❑ Applicant changing to regular undiscounted fee status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature ________________ Date ________________

Typed or printed name ________________ Registration No. ________________

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/508,887	10/22/2021	Kevin Alan Tussy	FACETC.0082P	9577

32856 7590 09/05/2023

WEIDE & MILLER, LTD.
10655 PARK RUN DRIVE
SUITE 100
LAS VEGAS, NV 89144

EXAMINER	
ABEDIN, SHANTO	
ART UNIT	**PAPER NUMBER**
2494	

DATE MAILED: 09/05/2023

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)

(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	**Application No.** 17/508,887	**Applicant(s)** Tussy, Kevin Alan	
	Examiner SHANTO ABEDIN	**Art Unit** 2494	**AIA (FITF) Status** Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1.☑ This communication is responsive to filing of 06/21/2023.
 ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on ______.

2.☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on ______; the restriction requirement and election have been incorporated into this action.

3.☑ The allowed claim(s) is/are 1-24 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4.☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a) ☐All b) ☐ Some* c) ☐ None of the:

1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ______ .
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: ______ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5.☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date ______ .

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6.☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1.☐ Notice of References Cited (PTO-892)
2.☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date ______.
3.☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material ______.
4.☐ Interview Summary (PTO-413), Paper No./Mail Date. ______.
5. ☐ Examiner's Amendment/Comment
6. ☑ Examiner's Statement of Reasons for Allowance
7. ☐ Other ______.

/SHANTO ABEDIN/
Primary Examiner, Art Unit 2494

Notice of Pre-AIA or AIA Status

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

DETAILED ACTION

1. This is in response to the communication filed on 06/21/2023. Claims 1-24 were pending in the application. Claims 1-24 have been allowed.

Terminal Disclaimer

2. The terminal disclaimer filed on 06/21/2023 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of patent No (s). 10,614,204, 10,776,471 and 11,157,606 has been reviewed and is accepted. The terminal disclaimer has been recorded.

Response to Arguments

3. Applicant's arguments, see remarks filed on 6/21/2023, with respect to obviousness type double patenting rejections of claims 1-24 have been fully considered and are persuasive. Previous obviousness type double patenting rejections have been withdrawn as terminal disclaimer filed on 6/21/2023 has been approved.

Examiner's Reasons for Allowance

4. The following is an examiner's statement of reasons for allowances:

No reason for allowance is necessary as the record is clear in light of further search conducted and terminal disclaimer filed on 06/21/2023, and prosecution history of the parent applications. See MPEP 1302.14(1).

Independent claim 1 is patentable over the cited prior arts because they do not anticipate nor fairly and reasonably teach independently or in combination a device comprising besides other limitations: capturing at least one first image of the user taken with the camera of the computing device at a first location which is a first distance from the user; processing the at least one first image or a portion thereof to create first data; capturing at least one second image of the user taken with the camera of the computing device is at a second distance from the user, the second distance being different than the first distance, the capturing at least one second image of the user occurring after movement of the camera or the user to establish the camera at the second distance from the user; comparing the first data to the second data to determine whether expected differences exist between the first data and the second data which indicates three- dimensionality of the user; verifying the images of the user exhibit three dimensional traits when the expected differences exist between the first data and the second data as a result of capturing the at least one first image and the at least one second image at different distances from the user.

Independent claim 10 is patentable over the cited prior arts because they do not anticipate nor fairly and reasonably teach independently or in combination a method comprising besides other limitations: moving the camera from the first location to a second location, the second location being a second distance from the user, or the user moving to change the distance between the user and the camera from the first distance to the second distance; capturing at least one second image of the user taken with the camera when the camera is the second distance from the user, the second distance being different than the first distance; comparing the first data to the second data to determine whether expected differences exist between the first data and the second data which <u>indicate</u> three-dimensionality of the user; and verifying the images of the user exhibit three-dimensional traits when the first data and the second data have expected differences resulting from the at least one first image being captured <u>with</u> <u>the</u> <u>camera</u> at a different distance from the user than when the at least one second image is captured.

Independent claim 22 is patentable over the cited prior arts because they do not anticipate nor fairly and reasonably teach independently or in combination a method comprising besides other limitations: changing a distance between the user and the camera to a second distance by the user moving the camera, or the user moving relative to the camera, or both; comparing one or more aspects of the user's head from the first image to one or more aspects of the user's head from the second image to determine whether expected differences, between the first image and the second image, exist which indicates three-dimensionality of the user, such that the expected differences between the first image and the second image result from the first image being captured when the camera is at a different distance from the user than when the second image is captured; and responsive to the comparing determining that expected differences between the first image and the second image exist, providing notice to the user, a third party, or both that the three- dimensionality of the user is verified.

Conclusion

5. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SHANTO ABEDIN whose telephone number is 571-272-3551. The examiner can normally be reached on M-F from 10:00 AM to 6:30 PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jay Kim, can be reached on 571-272-3804. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through

Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/SHANTO ABEDIN/

Primary Examiner, Art Unit 2494

Search Notes	**Application/Control No.** 17/508,887	**Applicant(s)/Patent Under Reexamination** Tussy, Kevin Alan
	Examiner SHANTO ABEDIN	**Art Unit** 2494

CPC - Searched*		
Symbol	**Date**	**Examiner**
CPC Search: G06F21/32, G06V40/168, G06V40/172, G06V40/18, G06V40/20	01/24/2023	SA
CPC Search: G06F21/32, G06V40/168, G06V40/172, G06V40/18, G06V40/20	08/26/2023	SA

CPC Combination Sets - Searched*		
Symbol	**Date**	**Examiner**

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	**Date**	**Examiner**
Inventor Assignee/ Double Patenting search	01/24/2023	SA
CPC classification search (with limited keyword search)	01/24/2023	SA
PE2E databases keyword search (see search history)	01/24/2023	SA
NPL: Google Scholar, IEEE Xplore search (see search history)	01/24/2023	SA
Consulted search notes from related application No. 16/817,428 and 15/900,681	01/24/2023	SA
PE2E databases keyword search (see search history)	08/26/2023	SA
NPL: Google Scholar, IEEE Xplore search (see search history)	08/26/2023	SA

/SHANTO ABEDIN/ Primary Examiner, Art Unit 2494	

Search Notes	Application/Control No. 17/508,887	Applicant(s)/Patent Under Reexamination Tussy, Kevin Alan
	Examiner SHANTO ABEDIN	Art Unit 2494

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**
Claim Interference Search	G06F21/32, G06V40/168, G06V40/172, G06V40/18, G06V40/20	01/24/2023	SA
Claim Interference Search	G06F21/32, G06V40/168, G06V40/172, G06V40/18, G06V40/20	08/26/2023	SA

/SHANTO ABEDIN/ Primary Examiner, Art Unit 2494	

Issue Classification	Application/Control No. 17/508,887	Applicant(s)/Patent Under Reexamination Tussy, Kevin Alan
	Examiner SHANTO ABEDIN	Art Unit 2494

CPC						
Symbol					Type	Version
G06F	/	21	/	32	F	2013-01-01
G06V	/	40	/	18	I	2022-01-01
G06V	/	40	/	20	I	2022-01-01
G06V	/	40	/	168	I	2022-01-01
G06V	/	40	/	172	I	2022-01-01
G06F	/	2221	/	2111	A	2013-01-01
H04W	/	12	/	65	A	2021-01-01
H04W	/	12	/	68	A	2021-01-01

CPC Combination Sets								
Symbol					Type	Set	Ranking	Version
	/		/					

NONE (Assistant Examiner) (Date)	Total Claims Allowed: 24	
/SHANTO ABEDIN/ 26 August 2023 Primary Examiner, Art Unit 2494 (Primary Examiner) (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 9

Issue Classification	Application/Control No. 17/508,887	Applicant(s)/Patent Under Reexamination Tussy, Kevin Alan
	Examiner SHANTO ABEDIN	Art Unit 2494

INTERNATIONAL CLASSIFICATION				
CLAIMED				
G06F21/32	/	21	/	32
G06V40/18	/	40	/	18
G06V40/20	/	40	/	20
G06V40/16	/	40	/	16
H04W12/65	/	12	/	65
H04W12/68	/	12	/	68

NON-CLAIMED				
	/		/	

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**

CROSS REFERENCES(S)						
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**					

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 24	
/SHANTO ABEDIN/ Primary Examiner, Art Unit 2494 (Primary Examiner)	26 August 2023 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 9

Issue Classification	Application/Control No. 17/508,887	Applicant(s)/Patent Under Reexamination Tussy, Kevin Alan
	Examiner SHANTO ABEDIN	**Art Unit** 2494

☑ Claims renumbered in the same order as presented by applicant ☐ CPA ☑ T.D. ☐ R.1.47

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
	1		10		19										
	2		11		20										
	3		12		21										
	4		13		22										
	5		14		23										
	6		15		24										
	7		16												
	8		17												
	9		18												

NONE (Assistant Examiner) (Date)	**Total Claims Allowed:** 24	
/SHANTO ABEDIN/ 26 August 2023 Primary Examiner, Art Unit 2494 (Primary Examiner) (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 9

Bibliographic Data

Application No: 17/508,887

Foreign Priority claimed: ○ Yes ◉ No

35 USC 119 (a-d) conditions met: ☐ Yes ☐ No ☐ Met After Allowance

Verified and Acknowledged: /SHANTO ABEDIN/

Examiner's Signature Initials

Title: FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
10/22/2021	713	2494	FACETC.0082P
RULE			

APPLICANTS

FaceTec, Inc., Las Vegas, NV,

INVENTORS

Kevin Alan Tussy, Las Vegas, NV, UNITED STATES

CONTINUING DATA

This application is a CON of 16817428 03/12/2020 PAT 11157606

16817428 is a CON of 15900681 02/20/2018 PAT 10614204

15900681 has PRO of 62460670 02/17/2017

15900681 is a CIP of 14839505 08/28/2015 PAT 9953149

14839505 has PRO of 62188584 07/03/2015

14839505 has PRO of 62139558 03/27/2015

14839505 has PRO of 62101317 01/08/2015

14839505 has PRO of 62085963 12/01/2014

14839505 has PRO of 62064415 10/15/2014

14839505 has PRO of 62054847 09/24/2014

14839505 has PRO of 62043224 08/28/2014

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

11/01/2021

**** SMALL ENTITY ****

STATE OR COUNTRY

UNITED STATES

ADDRESS

WEIDE & MILLER, LTD.
10655 PARK RUN DRIVE
SUITE 100
LAS VEGAS, NV 89144
UNITED STATES

FILING FEE RECEIVED

$880

Pcca: A new approach for **distance** learning from sparse pairwise constraints
A Mignon, F Jurie - 2012 IEEE conference on computer vision ..., 2012 - ieeexplore.ieee.org
... the **distance** means computing L such that, for a given **threshold** t... **face verification**, we use the popular Labeled Faces in the Wild (LFW) dataset [16]. It contains more than 13,000 **images** ...
Save Cite Cited by 739 Related articles All 18 versions

Discriminative deep metric learning for **face verification** in the wild
J Hu, J Lu, YP Tan - Proceedings of the IEEE conference on ..., 2014 - openaccess.thecvf.com
... In this paper, we consider the second one where **face images** ... **distance** of the positive pair is less than a smaller **threshold** ... We follow the standard evaluation protocol on the "**View** 2" ...
Save Cite Cited by 785 Related articles All 15 versions

Deep learning **face** representation by joint identification-**verification**
Y Sun, Y Chen, X Wang, X Tang - Advances in neural ..., 2014 - proceedings.neurips.cc
... the entire LFW **face image** including the **face** region and large ... (2) requires the **distance** larger than a margin m. θve = {m} is ... a **threshold** optimized on the training data for **face verification**...
Save Cite Cited by 2533 Related articles All 15 versions

Neural network-based **face** detection
HA Rowley, S Baluja, T Kanade - IEEE Transactions on pattern ..., 1998 - ieeexplore.ieee.org
... equal number of pixels in the **dimensions** of scale and position, ... To examine the effect of this **threshold** value during testing, ... **distance** metrics measure the **distance** of an input **image** to ...
Save Cite Cited by 6139 Related articles All 59 versions

Tour the world: building a web-scale landmark recognition engine
YT Zheng, M Zhao, Y Song, H Adam... - ... IEEE Conference on ..., 2009 - ieeexplore.ieee.org
... Moreover, we also adopt a multi-**view face** detector [15] to filter out ... **image** matching. The clustering process is then equivalent to erasing graph edges above a certain **distance threshold** ...
Save Cite Cited by 483 Related articles All 22 versions

Gabor wavelets and general discriminant analysis for **face** identification and **verification**
LL Shen, L Bai, M Fairhurst - Image and Vision Computing, 2007 - Elsevier
... However, due to the high **dimensionality** of the feature vector, especially in **face** recognition, S ... **distance** of the test **face** with the training **images** of the identity is below a global **threshold**, ...
Save Cite Cited by 368 Related articles All 9 versions

Combining RGB and ToF cameras for real-time 3D hand gesture interaction
M Van den Bergh, L Van Gool - 2011 IEEE workshop on ..., 2011 - ieeexplore.ieee.org
... **face** is detected and the **distance** from the **face** to the **camera** is measured. Based on this **distance**, a **threshold** is applied to the depth **image** to ... , and half for **validation**. The 350 sample ...
Save Cite Cited by 418 Related articles All 10 versions

Face recognition using the nearest feature line method
SZ Li, J Lu - IEEE transactions on neural networks, 1999 - ieeexplore.ieee.org
... In the following, we define a new **distance** measure that will be used in the NFL and ... **images** taken **live** and hence the feature points cannot be ordered in terms of a single **parameter** as ...
Save Cite Cited by 722 Related articles All 14 versions

Learning locally-adaptive decision functions for person **verification**
Z Li, S Chang, F Liang, TS Huang... - Proceedings of the ..., 2013 - openaccess.thecvf.com
... decisions based on a fixed **threshold**. We show that this is ... for **verification** that can be viewed as a joint model of a **distance** ... both human body **verification** and **face verification** problems. ...
Save Cite Cited by 610 Related articles All 14 versions

On the use of SIFT features for **face authentication**

M Bicego, A Lagorio, E Grosso... - 2006 Conference on ..., 2006 - ieeexplore.ieee.org

... of 2D **images**, it was never applied to **face** recognition/... In this paper the simple Euclidean **Distance** has been investigated, even ... The **parameter** R indicates the cost ratio between false ac...

Moving **face** spoofing detection via 3D projective invariants
M De Marsico, M Nappi, D Riccio… - 2012 5th IAPR …, 2012 - ieeexplore.ieee.org
… to **face recognition**, we can distinguish a real **face** in front of a … a global **distance** between candidate **image** points and their … We rather exploit it to check **three-dimensionality** of the **face**. …
☆ Save 99 Cite Cited by 147 Related articles All 7 versions

Why the mobile biometrics surge demands true **liveness**
J Wojewidka - Biometric Technology Today, 2017 - Elsevier
… This is a 3D **face recognition** system that uses expensive … **three-dimensionality**, but not necessarily for proving **liveness**. … **liveness** – including eye blink, on-screen prompt **movement**, …
☆ Save 99 Cite Cited by 4 Related articles

Liveness detection based on 3D **face** shape analysis
A Lagorio, M Tistarelli, M Cadoni… - … on Biometrics and …, 2013 - ieeexplore.ieee.org
… be able to detect the **movement** of the **face**. This can be … can verify the **three-dimensionality** of the **face** captured by the … sensor spoofmg attacks for **face recognition**. The considered …
☆ Save 99 Cite Cited by 121 Related articles All 6 versions

Three-dimensional human **face identification** card
Y Yan, C Zhou, C Li, JJ Yu - Holography, Diffractive Optics …, 2018 - spiedigitallibrary.org
… **three-dimensionality** and beauty, but also enhances the security of identity cards, and can be widely applied to various situations requiring **authentication**. … **distance**, so that the **image** …
☆ Save 99 Cite Related articles All 3 versions

A Low-cost Life Sign Detection Method based on Time Series Analysis of **Facial** Feature Points
T Bloecher, LG Iriarte, J Schneider… - … Conference on Bio …, 2017 - scitepress.org
… on the **verification** of the actual **three-dimensionality** of the **face**, … located **facial** feature points, the **movement** information of this set … Automatic **face recognition** and tracking systems are …
☆ Save 99 Cite Cited by 1 Related articles All 4 versions

Face anti-spoofing: Visual approach
A Anjos, J Komulainen, S Marcel, A Hadid… - Handbook of Biometric …, 2014 - Springer
… of attacks to visual spectrum **face recognition** systems. We introduce … **Images** can also be easily captured at **distance** without prior … for measuring **three-dimensionality** of the **face** without …
☆ Save 99 Cite Cited by 34 Related articles All 6 versions

FAMC: **Face Authentication** for Mobile Concurrence
VV Salunkhe, MMP Deshmukh, PA Pimplekar… - International Journal on … - academia.edu
… involves the estimation of the **three dimensionality** of faces. An … The **movement** detection of the **face** or other parts like smile, … used LBP for **face detection** and LBPH for **face recognition**. …
☆ Save 99 Cite Related articles

A study of **liveness** detection in **face** biometric systems
S Hemalatha, A Wahi - International Journal of Computer Applications, 2014 - Citeseer
… on spoof attack against **face recognition** system, ie in this … on the estimation of the **threedimensionality** of faces, which … the Euclidean **distance** is measured from the captured **face images**. …
☆ Save 99 Cite Cited by 5 Related articles All 4 versions

Real-time **face detection** and motion analysis with application in "**liveness**" assessment
K Kollreider, H Fronthaler, MI Faraj… - IEEE Transactions on …, 2007 - ieeexplore.ieee.org
… Also, the commercial **face recognition** systems suffer from … for the **three-dimensionality** of the (somehow) detected **face**(s) by … **movement** classification and lip-reading for the purpose of "…
☆ Save 99 Cite Cited by 339 Related articles All 12 versions

Human **Recognition** using **Face**, Fingerprint and Voice

P Melin, O Castillo, P Melin, O Castillo - … Systems for Pattern Recognition …, 2005 - Springer

… The task of identifying people by **face recognition** can be … and that a degree of **three-dimensionality** can be observed. Other … biometric **verification** process involves computing a **distance** …

☆ Save 99 Cite Cited by 12 Related articles All 3 versions

Access provided by: United States Patent and Trademark Office
Sign Out

All

ADVANCED SEARCH

Search within results
Download PDFs Items Per Page Export Alert Set Search Alerts Search History

Showing 1-10 of 10 results for
("Abstract":liveness) AND ("All Metadata":three-dimensional) AND ("All Metadata":image) AND ("Full Text & Metadata":face) ✕
recognition ✕

Filters Applied: 1990 - 2018 ✕

Conferences (8) Journals (2)

Filter
Alert Set Search Alerts | Sort Relevance Sort

Show

All Results
Subscribed Content
Open Access Only

Year

Single Year Range
2009 2018
From 2009 To 2018

Author

Affiliation

Publication Title

Publisher

A liveness detection method for face recognition based on optical flow field
Wei Bao; Hong Li; Nan Li; Wei Jiang
2009 International Conference on Image Analysis and Signal Processing
Year: 2009 | Conference Paper | Publisher: IEEE
Cited by: Papers (78) | Patents (15)

Abstract HTML

A liveness detection method for face recognition based on optical flow field

Wei Bao; Hong Li; Nan Li; Wei Jiang
2009 International Conference on Image Analysis and Signal Processing
Year: 2009 | Conference Paper | Publisher: IEEE

Liveness detection based on 3D face shape analysis
Andrea Lagorio; Massimo Tistarelli; Marinella Cadoni; Clinton Fookes; Sridha Sridharan
2013 International Workshop on Biometrics and Forensics (IWBF)
Year: 2013 | Conference Paper | Publisher: IEEE
Cited by: Papers (53) | Patents (1)

Abstract HTML

In recent years face recognition systems have been applied in various useful applications, such as surveillance, access control, criminal investigations, law enforcement, and others. However face biometric systems can be highly vulnerable to spoofing attacks where an impostor tries to bypass the face recognition system using a photo or video sequence. In this paper a ... Show More

Conference Location

Publication Topics

Liveness detection based on 3D face shape analysis

Andrea Lagorio; Massimo Tistarelli; Marinella Cadoni; Clinton Fookes; Sridha Sridharan
2013 International Workshop on Biometrics and Forensics (IWBF)
Year: 2013 | Conference Paper | Publisher: IEEE

Face liveness detection using 3D structure recovered from a single camera
Tao Wang; Jianwei Yang; Zhen Lei; Shengcai Liao; Stan Z. Li
2013 International Conference on Biometrics (ICB)
Year: 2013 | Conference Paper | Publisher: IEEE
Cited by: Papers (74) | Patents (8)

Abstract HTML

Face liveness detection using 3D structure recovered from a single camera

Tao Wang; Jianwei Yang; Zhen Lei; Shengcai Liao; Stan Z. Li
2013 International Conference on Biometrics (ICB)
Year: 2013 | Conference Paper | Publisher: IEEE

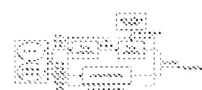
A Binocular Framework for Face Liveness Verification under Unconstrained Localization
Qi Li; Zhonghang Xia; Guangming Xing
2010 Ninth International Conference on Machine Learning and Applications
Year: 2010 | Conference Paper | Publisher: IEEE
Cited by: Papers (3) | Patents (1)

Abstract HTML

A Binocular Framework for Face Liveness Verification under Unconstrained Localization

Qi Li; Zhonghang Xia; Guangming Xing
2010 Ninth International Conference on Machine Learning and Applications
Year: 2010 | Conference Paper | Publisher: IEEE

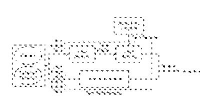
Empirical Study of Face Authentication Systems Under OSNFD Attacks
Yan Li; Yingjiu Li; Ke Xu; Qiang Yan; Robert H. Deng
IEEE Transactions on Dependable and Secure Computing
Year: 2018 | Volume: 15, Issue: 2 | Journal Article | Publisher: IEEE
Cited by: Papers (20)



Abstract HTML

Empirical Study of Face Authentication Systems Under OSNFD Attacks

Yan Li; Yingjiu Li; Ke Xu; Qiang Yan; Robert H. Deng
IEEE Transactions on Dependable and Secure Computing
Year: 2018 | Volume: 15, Issue: 2 | Journal Article | Publisher: IEEE



Face spoofing detection based on 3D lighting environment analysis of image pair
Xu Zhang; Xiyuan Hu; Mingyang Ma; Chen Chen; Silong Peng
2016 23rd International Conference on Pattern Recognition (ICPR)
Year: 2016 | Conference Paper | Publisher: IEEE
Cited by: Papers (3) | Patents (1)

Abstract HTML

Face spoofing detection based on 3D lighting environment analysis of image pair

Xu Zhang; Xiyuan Hu; Mingyang Ma; Chen Chen; Silong Peng
2016 23rd International Conference on Pattern Recognition (ICPR)
Year: 2016 | Conference Paper | Publisher: IEEE

Improving facial recognition accuracy by applying liveness monitoring technique
A. Asaduzzaman; A. Mummidi; Muhammad F. Mridha; Fadi N. Sibai
2015 International Conference on Advances in Electrical Engineering (ICAEE)
Year: 2015 | Conference Paper | Publisher: IEEE
Cited by: Papers (3)

Abstract HTML ©

Improving facial recognition accuracy by applying liveness monitoring technique

A. Asaduzzaman; A. Mummidi; Muhammad F. Mridha; Fadi N. Sibai
2015 International Conference on Advances in Electrical Engineering (ICAEE)
Year: 2015 | Conference Paper | Publisher: IEEE

Generalized face anti-spoofing by detecting pulse from face videos
Xiaobai Li; Jukka Komulainen; Guoying Zhao; Pong-Chi Yuen; Matti Pietikäinen
2016 23rd International Conference on Pattern Recognition (ICPR)
Year: 2016 | Conference Paper | Publisher: IEEE
Cited by: Papers (20)

Abstract HTML ©

Generalized face anti-spoofing by detecting pulse from face videos

Xiaobai Li; Jukka Komulainen; Guoying Zhao; Pong-Chi Yuen; Matti Pietikäinen
2016 23rd International Conference on Pattern Recognition (ICPR)
Year: 2016 | Conference Paper | Publisher: IEEE

A Robust and Secure Palm Vessel Biometric Sensing System Based on Photoacoustics
Yuehang Wang; Zhengxiong Li; Tri Vu; Nikhila Nyayapathi; Kwang W. Oh; Wenyao Xu; Jun Xia
IEEE Sensors Journal
Year: 2018 | Volume: 18, Issue: 14 | Journal Article | Publisher: IEEE
Cited by: Papers (27)

Abstract HTML ©

A Robust and Secure Palm Vessel Biometric Sensing System Based on Photoacoustics

Yuehang Wang; Zhengxiong Li; Tri Vu; Nikhila Nyayapathi; Kwang W. Oh; Wenyao Xu; Jun Xia
IEEE Sensors Journal
Year: 2018 | Volume: 18, Issue: 14 | Journal Article | Publisher: IEEE

A discriminative spatio-temporal mapping of face for liveness detection
Nagashri N Lakshminarayana; Neeti Narayan; Nils Napp; Srirangaraj Setlur; Venu Govindaraju
2017 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA)
Year: 2017 | Conference Paper | Publisher: IEEE
Cited by: Papers (20)

Abstract HTML ©

A discriminative spatio-temporal mapping of face for liveness detection

Nagashri N Lakshminarayana; Neeti Narayan; Nils Napp; Srirangaraj Setlur; Venu Govindaraju
2017 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA)
Year: 2017 | Conference Paper | Publisher: IEEE

IEEE Account

» Change Username/Password

» Update Address

Purchase Details

» Payment Options

» Order History

» View Purchased Documents

Profile Information

» Communications Preferences

» Profession and Education

» Technical Interests

Need Help?

» **US & Canada:** +1 800 678 4333

» **Worldwide:** +1 732 981 0060

» Contact & Support

About IEEE *Xplore* | Contact Us | Help | Accessibility | Terms of Use | Nondiscrimination Policy | Sitemap | Privacy & Opting Out of Cookies

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L1	22564	(three) near3 (dimensional OR dimensionality) SAME (determin$3 OR based OR compar$3 OR verify$3)(compar$3 OR match$3 OR verifying) SAME (image) SAME (distance) SAME (face OR facial OR portion OR side)(illumination OR brightness)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/08/26 05:54 PM
L2	8614	((image)(distance)(liveness OR three-dimensional$4) (face OR facial OR head)).clm. (second) SAME (image OR picture) SAME (distance OR movement)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/08/26 07:43 PM
L3	8198	(biometric)(authentication) (liveness OR dimensionality OR live)(authentication OR identity) near3 (server)(predetermined OR expected OR thresold) SAME (match$3 OR image OR compar$3)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/08/26 08:22 PM
L4	221043	(G06F21/32 OR G06V40/168 OR G06V40/172 OR G06V40/18 OR	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU,	AND	ON	ON	2023/08/26 08:24 PM

		G06V40/20).cpc.	CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L5	1207	L1 L4	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/08/26 08:24 PM
L6	17734	L2 OR L3 OR L5	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/08/26 08:24 PM
L7	40	(US-0066758-$ | US-0105551-$ | US-0111493-$ | US-0196753-$ | US-0276484-$ | US-10032066-$ | US-10917431-$ | US-10963669-$ | US-1693801-$ | US-20110196753-$ | US-20110276484-$ | US-20120066758-$ | US-20170111493-$ | US-	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA,	OR	ON	ON	2023/08/26 08:25 PM

		20190105551-$ | US-3075573-$ | US-8200980-$ | US-8355528-$ | US-8787627-$ | US-9286507-$ | US-9621548-$).DID.	VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L8	200	(US-7333963-$ | US-7415152-$ | US-7428320-$ | US-7519200-$ | US-7636450-$ | US-7646909-$ | US-7660444-$ | US-7710693-$ | US-7783118-$ | US-7788247-$ | US-7804982-$ | US-7809722-$ | US-7945653-$ | US-7960470-$ | US-8121408-$ | US-8165352-$ | US-8210247-$ | US-8244211-$ | US-8280120-$ | US-8316237-$ | US-8326000-$ | US-8392268-$ | US-8396246-$ | US-8411909-$ | US-8416312-$ | US-8457367-$ | US-8460024-$ | US-8649604-$ | US-8709801-$ | US-8722977-$ | US-8743051-$ | US-8750574-$ | US-8856541-$ | US-8867849-$ | US-8922480-$ | US-8959578-$ | US-9037354-$ | US-9069447-$ | US-9076008-$ | US-9076028-$ | US-9137246-$ | US-9152849-$ | US-9202105-$ | US-9209355-$ | US-9424491-$ | US-9430695-$ | US-9448687-$ | US-9459132-$ | US-9600649-$ | US-9607138-$ | US-9708909-$ | US-	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/08/26 08:26 PM

		9740848-$ | US- 9798420-$ | US- 9911036-$ | US- 9958687-$ | US- D485279-$ | US- D596192-$ | US- D601582-$ | US- D606082-$ | US- D625325-$ | US- D637604-$ | US- D640277-$ | US- D650793-$ | US- D663743-$ | US- D663744-$ | US- D667423-$ | US- D692018-$ | US- D692915-$ | US- D702714-$ | US- D712909-$ | US- D713410-$ | US- D715317-$ | US- D717339-$ | US- D717829-$ | US- D725151-$ | US- D725668-$ | US- D726221-$ | US- D728623-$ | US- D730389-$ | US- D730941-$ | US- D731552-$ | US- D733755-$ | US- D736812-$ | US- D737325-$ | US- D738921-$ | US- D740833-$ | US- D742417-$ | US- D745567-$ | US- D747354-$ | US- D752078-$ | US- D753132-$ | US- D756401-$ | US- D757084-$ | US- D759723-$ | US- D761268-$ | US- D761277-$ | US- D762655-$ | US- D762673-$ | US- D762715-$ | US- D763271-$ | US- D763306-$ | US- D764526-$ | US- D764534-$ | US- D765117-$ | US- D765133-$ | US- D765674-$ | US- D766298-$ | US- D766314-$ | US- D766926-$ | US-					

<table>
<tr><td></td><td></td><td>D769933-$ | US-D772288-$ | US-D772929-$ | US-D776680-$ | US-D777755-$ | US-D778923-$ | US-D778940-$ | US-D780781-$ | US-D783633-$ | US-D783652-$ | US-D784363-$ | US-D787527-$ | US-D788122-$ | US-D788810-$ | US-D790567-$ | US-D791158-$ | US-D794663-$ | US-D798321-$ | US-D798902-$ | US-D799544-$ | US-D800743-$ | US-D801990-$ | US-D803870-$ | US-D805546-$ | US-D805548-$ | US-D806113-$ | US-D807378-$ | US-D807381-$ | US-D817994-$ | US-D819075-$ | US-D820305-$ | US-D821439-$ | US-D821443-$ | US-D822054-$ | US-D823335-$ | US-D823867-$ | US-D823891-$ | US-D825587-$ | US-D825588-$).DID.</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>L9</td><td>17963</td><td>L6 OR L7 OR L8</td><td>(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)</td><td>OR</td><td>ON</td><td>ON</td><td>2023/08/26 08:26 PM</td></tr>
<tr><td>L11</td><td>953</td><td>L9 (authentication OR identity OR verificatoin)</td><td>(US-PGPUB; USPAT; USOCR; FIT (AU, AP,</td><td>AND</td><td>ON</td><td>ON</td><td>2023/08/26 08:29 PM</td></tr>
</table>

		near5 (server) (liveness OR three-dimensionality OR real)(movement OR motion OR distance)(biometric OR face OR facial OR head).clm. (image OR picture).clm.	AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L12	38	L2 L3	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/08/26 08:29 PM
L13	78	L7 OR L12	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/08/26 08:29 PM
L14	2056	L5 OR L11	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO,	AND	ON	ON	2023/08/26 08:39 PM

			RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L15	1231	L3 (captur$3 OR camera) SAME (distance) SAME (image)(live OR liveness OR three-dimensional$3)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/08/26 08:40 PM
L16	2832	L14 OR L15	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/08/26 08:40 PM
L17	1530	L16 (recognition)(face OR facial)(motion OR movement)(authentication)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/08/26 08:41 PM
L18	1400	L16 (recognition)(face OR facial)(motion OR movement)(authentication)(distance)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU,	AND	ON	ON	2023/08/26 08:41 PM

			CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L19	431	L16 ((image)(distance)(dimensional$3 OR liveness)).clm.	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/08/26 08:42 PM
L20	802	L18 (G06F21/32 OR G06V40/168 OR G06V40/172 OR G06V40/18 OR G06V40/20).cpc.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/08/26 08:42 PM
L21	1119	L19 OR L20	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN,	AND	ON	ON	2023/08/26 08:42 PM

			WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L22	159	L21 (recognition)(face OR facial)(motion OR movement) ((authentication)(distance)).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/08/26 08:47 PM
L23	80	L21 ((authentication)(distance) (image)(captur$3 OR camera)(server)).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/08/26 08:48 PM
L24	114	L19 L20	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/08/26 08:48 PM
L25	227	L22 OR L23 OR L24	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB,	AND	ON	ON	2023/08/26 08:49 PM

			HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L26	104	L25 @ad<"20180220"	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/08/26 08:51 PM
L27	77	L26 (recognition)(authentication)(second) SAME (image) SAME (distance)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/08/26 09:03 PM
L28	56	L26 (recognition)(authentication)(second) SAME (image) SAME (distance) (live OR liveness OR three-dimensionality)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT;	AND	ON	ON	2023/08/26 09:04 PM

			IBM_TDB)				
L29	58	L26 (authenticat$3 OR identity).ab. (server)(image)(face OR facial)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/08/26 09:04 PM
L30	7	L28 ((image) SAME (distance) (live OR liveness OR three-dimensionality)).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/08/26 09:05 PM
L31	12	L29 ((image OR camera)(threshold OR match$3) (distance) (live OR liveness OR three-dimensionality)).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/08/26 09:11 PM
L32	16	L30 OR L31	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV,	AND	ON	ON	2023/08/26 09:12 PM

			MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L33	1	L32 Kevin near3 Tussy.in.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/08/26 09:12 PM
L34	12	L32 NOT FaceTec.as.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/08/26 09:13 PM
L35	7	L34 ((live OR liveness OR three-dimensionality OR real) (identity OR verification OR authentication)(biometric OR facial OR recognition)).ab.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/08/26 09:14 PM

L36	7	L34 ((live OR liveness OR three-dimensionality OR real) (identity OR verification OR authentication)(biometric OR facial OR recognition)).ab. (distance OR movement).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/08/26 09:15 PM

PE2E SEARCH - Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
N1	1519	((image)(distance)(liveness OR three-dimensional$4) (face OR facial OR head)).clm. (second) SAME (image OR picture) SAME (distance OR movement)	(US-PGPUB; USPAT)	AND	ON	ON	2023/08/26 09:17 PM
N2	3985	(biometric)(authentication) (liveness OR dimensionality OR live)(authentication OR identity) near3 (server)(predetermined OR expected OR thresold) SAME (match$3 OR image OR compar$3)	(US-PGPUB; USPAT)	AND	ON	ON	2023/08/26 09:17 PM
N3	8050	(biometric)(authenticat$3)(server)(recognition)(image)(G06F21/32 OR G06V40/168 OR G06V40/172 OR G06V40/18 OR G06V40/20).cpc.	(US-PGPUB; USPAT)	AND	ON	ON	2023/08/26 09:17 PM
N4	28	((image OR camera)(threshold OR match$3) (distance) (live OR liveness OR three-dimensionality)).clm. (recognition)(authentication).clm. (second) SAME (image) SAME	(US-PGPUB; USPAT)	AND	ON	ON	2023/08/26 09:18 PM

		(distance)					
N5	20	(US-0066758-$ | US-0105551-$ | US-0111493-$ | US-0196753-$ | US-0276484-$ | US-10032066-$ | US-10917431-$ | US-10963669-$ | US-1693801-$ | US-20110196753-$ | US-20110276484-$ | US-20120066758-$ | US-20170111493-$ | US-20190105551-$ | US-3075573-$ | US-8200980-$ | US-8355528-$ | US-8787627-$ | US-9286507-$ | US-9621548-$).DID.	(US-PGPUB; USPAT)	OR	ON	ON	2023/08/26 09:22 PM
N6	148	(US-7333963-$ | US-7415152-$ | US-7428320-$ | US-7519200-$ | US-7636450-$ | US-7646909-$ | US-7660444-$ | US-7710693-$ | US-7783118-$ | US-7788247-$ | US-7804982-$ | US-7809722-$ | US-7945653-$ | US-7960470-$ | US-8121408-$ | US-8165352-$ | US-8210247-$ | US-8244211-$ | US-8280120-$ | US-8316237-$ | US-8326000-$ | US-8392268-$ | US-8396246-$ | US-8411909-$ | US-8416312-$ | US-8457367-$ | US-8460024-$ | US-8649604-$ | US-8709801-$ | US-8722977-$ | US-8743051-$ | US-8750574-$ | US-8856541-$ | US-8867849-$ | US-8922480-$ | US-8959578-$ | US-	(US-PGPUB; USPAT)	OR	ON	ON	2023/08/26 09:22 PM

		9037354-$ | US- 9069447-$ | US- 9076008-$ | US- 9076028-$ | US- 9137246-$ | US- 9152849-$ | US- 9202105-$ | US- 9209355-$ | US- 9424491-$ | US- 9430695-$ | US- 9448687-$ | US- 9459132-$ | US- 9600649-$ | US- 9607138-$ | US- 9708909-$ | US- 9740848-$ | US- 9798420-$ | US- 9911036-$ | US- 9958687-$ | US- D485279-$ | US- D596192-$ | US- D601582-$ | US- D606082-$ | US- D625325-$ | US- D637604-$ | US- D640277-$ | US- D650793-$ | US- D663743-$ | US- D663744-$ | US- D667423-$ | US- D692018-$ | US- D692915-$ | US- D702714-$ | US- D712909-$ | US- D713410-$ | US- D715317-$ | US- D717339-$ | US- D717829-$ | US- D725151-$ | US- D725668-$ | US- D726221-$ | US- D728623-$ | US- D730389-$ | US- D730941-$ | US- D731552-$ | US- D733755-$ | US- D736812-$ | US- D737325-$ | US- D738921-$ | US- D740833-$ | US- D742417-$ | US- D745567-$ | US- D747354-$ | US- D752078-$ | US- D753132-$ | US- D756401-$ | US- D757084-$ | US- D759723-$ | US-					

		D761268-$ | US-D761277-$ | US-D762655-$ | US-D762673-$ | US-D762715-$ | US-D763271-$ | US-D763306-$ | US-D764526-$ | US-D764534-$ | US-D765117-$ | US-D765133-$ | US-D765674-$ | US-D766298-$ | US-D766314-$ | US-D766926-$ | US-D769933-$ | US-D772288-$ | US-D772929-$ | US-D776680-$ | US-D777755-$ | US-D778923-$ | US-D778940-$ | US-D780781-$ | US-D783633-$ | US-D783652-$ | US-D784363-$ | US-D787527-$ | US-D788122-$ | US-D788810-$ | US-D790567-$ | US-D791158-$ | US-D794663-$ | US-D798321-$ | US-D798902-$ | US-D799544-$ | US-D800743-$ | US-D801990-$ | US-D803870-$ | US-D805546-$ | US-D805548-$ | US-D806113-$ | US-D807378-$ | US-D807381-$ | US-D817994-$ | US-D819075-$ | US-D820305-$ | US-D821439-$ | US-D821443-$ | US-D822054-$ | US-D823335-$ | US-D823867-$ | US-D823891-$ | US-D825587-$ | US-D825588-$).DID.					
N7	23	N1 N2	(US-PGPUB; USPAT)	AND	ON	ON	2023/08/26 09:22 PM
N8	274	N3 (distance) SAME	(US-PGPUB; USPAT)	AND	ON	ON	2023/08/26

		(face OR camera).clm. (match$3 OR threshold)					09:23 PM
N9	454	N4 OR N5 OR N6 OR N7 OR N8	(US-PGPUB; USPAT)	AND	ON	ON	2023/08/26 09:23 PM
N10	22	N9 ((live OR liveness OR three-dimensionality OR real) (identity OR verification OR authentication)(biometric OR facial OR recognition)).ab. (distance OR movement).clm.	(US-PGPUB; USPAT)	AND	ON	ON	2023/08/26 09:24 PM
N11	63	N9 ((image OR camera)(threshold OR match$3) (distance) (live OR liveness OR three-dimensionality)).clm.	(US-PGPUB; USPAT)	AND	ON	ON	2023/08/26 09:24 PM
N12	84	N5 OR N10 OR N11	(US-PGPUB; USPAT)	AND	ON	ON	2023/08/26 09:25 PM
N13	30	N12 @ad<"20180220"	(US-PGPUB; USPAT)	AND	ON	ON	2023/08/26 09:34 PM
N14	0	N13 Kevin near3 Tussy.in.	(US-PGPUB; USPAT)	AND	ON	ON	2023/08/26 09:35 PM
N15	21	N13 ((dimensional$3 OR liveness OR live OR real)(image)(distance OR path OR movement)).clm.	(US-PGPUB; USPAT)	AND	ON	ON	2023/08/26 09:37 PM
N16	8	N15 ((live OR liveness OR three-dimensionality OR real) (identity OR verification OR authentication)(biometric OR facial OR recognition)).ab.	(US-PGPUB; USPAT)	AND	ON	ON	2023/08/26 09:37 PM
N17	3	N16 (face OR facial OR head).clm. (distance) SAME (face OR camera).clm. (match$3 OR threshold)	(US-PGPUB; USPAT)	AND	ON	ON	2023/08/26 09:38 PM

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L1	116	Kevin near3 Tussy.in.	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 07:32 PM
L2	26	FaceTec.as.	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 07:33 PM
L3	131	L1 OR L2	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 07:39 PM
L4	197937	(G06F21/32 OR G06V40/168 OR G06V40/172 OR G06V40/18 OR	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU,	AND	ON	ON	2023/01/23 07:42 PM

		G06V40/20).cpc.	CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L5	25	L3 ((image)(distance)(liveness OR three-dimensionality)).clm.	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 07:43 PM
L6	6	L3 ((image)(distance)(liveness OR three-dimensionality)(illumination OR visibility OR suitable)(face OR facial OR head)).clm.	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 07:46 PM
L7	2	"10614204".pn.	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA,	AND	ON	ON	2023/01/23 07:47 PM

			VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L8	4	"11157606".pn.	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 07:49 PM
L9	8	"11157606".pn. "10614204".pn. "10776471".pn.	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/01/23 08:01 PM
L10	3	L9 ((image)(distance)(liveness OR three-dimensional$4)(face OR facial OR head)).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:01 PM
L11	22045	((image)(distance)(liveness OR three-dimensional$4)(face OR facial OR head)).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB,	AND	ON	ON	2023/01/23 08:07 PM

			HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L12	14595	((image) SAME (distance)(liveness OR three-dimensional$4)(face OR facial OR head)).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:07 PM
L13	19006	((image) SAME (distance)(liveness OR three-dimensional$4 OR live OR physical)(face OR facial OR head)).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:08 PM
L14	14256	((image) SAME (distance)(liveness OR three-dimensional$4 OR live OR physical) SAME (distance OR expected OR determin$3)(face OR facial OR head)).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT;	AND	ON	ON	2023/01/23 08:09 PM

			IBM_TDB)				
L15	4444	((second) SAME (image) SAME (distance)(liveness OR three-dimensional$4 OR live OR physical) SAME (distance OR expected OR determin$3)(face OR facial OR head)).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:09 PM
L16	118	((second) SAME (image) SAME (distance)(liveness OR three-dimensional$4 OR live OR physical) SAME (distance OR expected OR determin$3)(face OR facial OR head)).clm. (biometric)(authentication)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:09 PM
L17	175	((second) SAME (image) SAME (distance)(liveness OR three-dimensional$4 OR live OR physical) SAME (distance OR expected OR determin$3)(face OR facial OR head)).clm. (biometric)(authentication OR identity)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:10 PM
L18	107	((second) SAME (image) SAME (distance)(liveness OR three-dimensional$4 OR live OR physical) SAME (distance OR expected OR determin$3)(face OR	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV,	AND	ON	ON	2023/01/23 08:10 PM

		facial OR head)).clm. (biometric)(authentication OR identity)(predetermined OR expected OR threshold).clm.	MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L19	99	((second) SAME (image) SAME (distance)(liveness OR three-dimensional$4 OR live OR physical) SAME (distance OR expected OR determin$3)(face OR facial OR head)).clm. (biometric)(authentication OR identity)(predetermined OR expected OR threshold).clm. (face OR facial)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:11 PM
L20	63	((second) SAME (image) SAME (distance)(liveness OR three-dimensional$4 OR live OR physical) SAME (distance OR expected OR determin$3)(face OR facial OR head)).clm. (biometric)(authentication OR identity)(predetermined OR expected OR threshold).clm. (face OR facial)(camera).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:11 PM
L21	25	L20 @ad<"20180220"	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:12 PM
L22	10	L21 NOT FaceTec.as.	(US-PGPUB; USPAT;	AND	ON	ON	2023/01/23

			USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				08:12 PM
L23	272	((liveness OR three-dimensional$4 OR live OR physical) (face OR facial OR head) SAME (side OR portion OR captur$3)(illuminat$4 OR brightness)).clm.(authentication)(biometric)(distance)(image)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:16 PM
L24	377	L16 OR L23	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:16 PM
L25	144	L24 (authentication OR live OR liveness OR dimensional$4).ab. (image) SAME (distance)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL,	AND	ON	ON	2023/01/23 08:17 PM

			PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L26	61	L25 @ad<"20180220"	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:17 PM
L27	24	L26 NOT FaceTec.as.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:18 PM
L28	7	L27 (second) SAME (image) SAME (captur$3 OR camera) SAME (distance)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:19 PM
L29	33	L22 OR L27	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY,	AND	ON	ON	2023/01/23 08:20 PM

			CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L30	12	L29 (second OR compar$3 OR match$3) SAME (image) SAME (captur$3 OR camera) SAME (distance OR movement OR moving OR path).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:20 PM
L31	14	L29 (illumination OR brightness).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:22 PM
L32	23	L30 OR L31	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH,	AND	ON	ON	2023/01/23 08:22 PM

			TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L33	12	L32 (distance).clm. (liveness OR dimensional$4)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:23 PM
L34	40	(US-0066758-$ | US-0105551-$ | US-0111493-$ | US-0196753-$ | US-0276484-$ | US-10032066-$ | US-10917431-$ | US-10963669-$ | US-1693801-$ | US-20110196753-$ | US-20110276484-$ | US-20120066758-$ | US-20170111493-$ | US-20190105551-$ | US-3075573-$ | US-8200980-$ | US-8355528-$ | US-8787627-$ | US-9286507-$ | US-9621548-$).DID.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/01/23 08:37 PM
L35	88	(US-0031173-$ | US-0065855-$ | US-0065885-$ | US-0070678-$ | US-0081338-$ | US-0091136-$ | US-0094849-$ | US-0103652-$ | US-0109584-$ | US-0125991-$ | US-0133599-$ | US-0143598-$ | US-0190758-$ | US-0198368-$ | US-0201709-$ | US-0218792-$ | US-0236832-$ | US-	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/01/23 08:38 PM

		0264780-$ | US-20030103652-$ | US-20030133599-$ | US-20030198368-$ | US-20030236832-$ | US-20040070678-$ | US-20040081338-$ | US-20040091136-$ | US-20040109584-$ | US-20040125991-$ | US-20040143598-$ | US-20040190758-$ | US-20040201709-$ | US-20040218792-$ | US-20040264780-$ | US-20050031173-$ | US-20050065855-$ | US-20050065885-$ | US-20050094849-$ | US-6678664-$ | US-6687390-$ | US-6697502-$ | US-6711584-$ | US-6728401-$ | US-6775397-$ | US-6840149-$ | US-D485279-$).DID.					
L36	128	L34 OR L35	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/01/23 08:38 PM
L37	8	L36 (second OR compar$3 OR match$3) SAME (image) SAME (captur$3 OR camera) SAME (distance OR movement OR moving OR path)(authentication OR identity OR recognition)(live OR liveness OR physical)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO;	AND	ON	ON	2023/01/23 08:39 PM

			JPO; DERWENT; IBM_TDB)				
L38	24	L36 (G06F21/32 OR G06V40/168 OR G06V40/172 OR G06V40/18 OR G06V40/20).cpc.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:39 PM
L39	26	L37 OR L38	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:40 PM
L40	1	L38 (image).clm. (illumination OR distance).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:40 PM
L41	49	L32 OR L39	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS,	AND	ON	ON	2023/01/23 08:41 PM

			IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L43	23	L41 (three near3 dimension$3)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:42 PM
L44	21	L41 (three near3 dimension$3)(image).clm.(face OR facial)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:42 PM
L45	17	L41 (three near3 dimension$3)(image).clm.(face OR facial)(liveness OR authentication)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:42 PM

L46	7	L41 (three near3 dimension$3)(image).clm.(face OR facial)(liveness OR authentication)(distance).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:44 PM
L47	2	16/405,906	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/01/24 01:51 PM
L48	6	"11157606".pn. "10614204".pn. "11157606".pn.	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/01/24 07:55 PM
L49	8	"11157606".pn. "10614204".pn. "10776471".pn.	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO,	OR	ON	ON	2023/01/24 08:01 PM

			MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L50	44264	(captur$3 OR camera) SAME (image) SAME (distance OR movement OR path)(liveness OR three-dimensionality OR dimensional$4)(face OR facial)(authenticat$3)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:15 PM
L51	15082	L50 (second OR compar$3 OR match$3) SAME (image) SAME (captur$3 OR camera) SAME (distance OR movement OR moving OR path)(authentication OR identity OR recognition)(live OR liveness OR physical)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:16 PM
L52	4016	L50 (illumination OR brightness).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:16 PM
L53	6978	L51 (illumination OR brightness) (image).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT,	AND	ON	ON	2023/01/24 08:16 PM

			AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L54	9472	L52 OR L53	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:17 PM
L55	2217	L54 (biometric OR authenticat$3 OR customer OR liveness OR three-dimensionality OR dimensional$3).ab.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:18 PM
L56	965	L54 (biometric OR authenticat$3 OR customer OR liveness OR three-dimensionality OR dimensional$3).ab. (image).clm.(face OR facial).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE,	AND	ON	ON	2023/01/24 08:18 PM

			SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L57	1067	L54 (illumination OR brightness)(distance).clm. (image).clm.(face OR facial).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:19 PM
L58	1868	L24 OR L56 OR L57	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:19 PM
L59	530	L58 (compar$3 OR match$3) SAME (image).clm. (distance).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:20 PM
L60	359	L56 L57	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU,	AND	ON	ON	2023/01/24 08:21 PM

			CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L61	222	L59 L60	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:21 PM
L62	667	L59 OR L60	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:21 PM
L63	398	L62 (second) SAME (image).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN,	AND	ON	ON	2023/01/24 08:21 PM

			WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L64	218	L62 (second) SAME (image) SAME (distance).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:22 PM
L65	373	L62 (portion OR second) SAME (image) SAME (distance OR face).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:22 PM
L66	218	L64 L65	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:23 PM
L67	373	L64 OR L65	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB,	AND	ON	ON	2023/01/24 08:23 PM

			HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L68	157	L67 (compar$3 OR match$3 OR verifying) SAME (image) SAME (distance).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:23 PM
L69	228	L67 (compar$3 OR match$3 OR verifying) SAME (image) SAME (distance) SAME (face OR facial OR portion OR side)(illumination OR brightness)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:24 PM
L70	90	L67 (compar$3 OR match$3 OR verifying) SAME (image) SAME (distance) SAME (face OR facial OR portion OR side)(illumination OR brightness).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT;	AND	ON	ON	2023/01/24 08:26 PM

			IBM_TDB)				
L71	203	L68 OR L70	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:30 PM
L72	27	FaceTec.as.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/01/24 08:31 PM
L73	117	Kevin near2 Tussy.in.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/01/24 08:31 PM
L74	132	L72 OR L73	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV,	OR	ON	ON	2023/01/24 08:31 PM

			MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L75	44	L74 (three-dimensionality OR dimensional)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:32 PM
L76	20	L74 (three near3 dimensionality)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:32 PM
L77	43	L74 (three) near3 (dimensional OR dimensionality)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:33 PM
L78	42	L74 (three) near3	(US-PGPUB; USPAT;	AND	ON	ON	2023/01/24

		(dimensional OR dimensionality) SAME (determin$3 OR based OR compar$3 OR verify$3)	USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				08:33 PM
L79	40	L74 @ad<"20140828"	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:35 PM
L80	1	L79 (authenticat$3 OR customer OR liveness OR three-dimensionality OR dimensional$3).ab. (biometric OR user OR customer OR verify$3 OR movement OR motion OR face OR facial).ab. (image).clm.(face OR facial).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:36 PM
L81	0	L80 NOT Tussy.in.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL,	AND	ON	ON	2023/01/24 08:37 PM

			PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				

PE2E SEARCH - Search History (Interference)

There are no Interference searches to show.

Application Number * 17/508,887 *	Application/Control No. 17/508,887	Applicant(s)/Patent under Reexamination Tussy, Kevin Alan	
	Examiner ABEDIN, SHANTO	**Art Unit** 2494	

Document Code - DISQ	**Internal Document - DO NOT MAIL**

TERMINAL DISCLAIMER	☑ APPROVED	☐ DISAPPROVED
Date Filed: **21 June 2023**	**This patent is subject to a Terminal Disclaimer**	

Approved/Disapproved by:
/JEAN PROCTOR/ **Technology Center:** **OPLC** **Telephone:** **(571)272-1040** 3 td's

U.S. Patent and Trademark Office
TSS-IFW

Terminal Disclaimer

Part of Paper No. 20230622

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT	Docket Number (Optional) FACETC.0082P

In re Application of: Kevin Alan Tussy

Application No.: 17/508,887

Filed: October 22, 2021

For: FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS

The applicant, FaceTec, Inc., owner of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of **prior patent** No. 10,614,204 as the term of said **prior patent** is presently shortened by any terminal disclaimer. The applicant hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the **prior patent** are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the applicant does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the **prior patent**, "as the term of said **prior patent** is presently shortened by any terminal disclaimer," in the event that said **prior patent** later:

- expires for failure to pay a maintenance fee;
- is held unenforceable;
- is found invalid by a court of competent jurisdiction;
- is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
- has all claims canceled by a reexamination certificate;
- is reissued; or
- is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2 below, if appropriate.

1. ☐ The undersigned is the applicant. If the applicant is an assignee, the undersigned is authorized to act on behalf of the assignee.

I hereby acknowledge that any willful false statements made are punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. 44,943

/Chad W. Miller/ — Signature
June 21, 2023 — Date

Chad W. Miller — Typed or printed name

Attorney of Record — Title
(702) 382-4804 — Telephone Number

☑ Terminal disclaimer fee under 37 CFR 1.20(d) included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

PTO/AIA/26 (04-14)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT

Docket Number (Optional): FACETC.0082P

In re Application of: Kevin Alan Tussy

Application No.: 17/508,887

Filed: October 22, 2021

For: FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS

The applicant, FaceTec, Inc., owner of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of **prior patent** No. 10,776,471 as the term of said **prior patent** is presently shortened by any terminal disclaimer. The applicant hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the **prior patent** are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the applicant does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the **prior patent**, "as the term of said **prior patent** is presently shortened by any terminal disclaimer," in the event that said **prior patent** later:

- expires for failure to pay a maintenance fee;
- is held unenforceable;
- is found invalid by a court of competent jurisdiction;
- is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
- has all claims canceled by a reexamination certificate;
- is reissued; or
- is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2 below, if appropriate.

1. ☐ The undersigned is the applicant. If the applicant is an assignee, the undersigned is authorized to act on behalf of the assignee.

I hereby acknowledge that any willful false statements made are punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. 44,943

/Chad W. Miller/	June 21, 2023
Signature	Date

Chad W. Miller
Typed or printed name

Attorney of Record	(702) 382-4804
Title	Telephone Number

☑ Terminal disclaimer fee under 37 CFR 1.20(d) included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

PTO/AIA/26 (04-14)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT	Docket Number (Optional) FACETC.0082P

In re Application of: Kevin Alan Tussy

Application No.: 17/508,887

Filed: October 22, 2021

For: FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS

The applicant, FaceTec, Inc., owner of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of **prior patent** No. 11,157,606 as the term of said **prior patent** is presently shortened by any terminal disclaimer. The applicant hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the **prior patent** are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the applicant does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the **prior patent**, "as the term of said **prior patent** is presently shortened by any terminal disclaimer," in the event that said **prior patent** later:

- expires for failure to pay a maintenance fee;
- is held unenforceable;
- is found invalid by a court of competent jurisdiction;
- is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
- has all claims canceled by a reexamination certificate;
- is reissued; or
- is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2 below, if appropriate.

1. ☐ The undersigned is the applicant. If the applicant is an assignee, the undersigned is authorized to act on behalf of the assignee.

I hereby acknowledge that any willful false statements made are punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. 44,943

/Chad W. Miller/ — Signature

June 21, 2023 — Date

Chad W. Miller — Typed or printed name

Attorney of Record — Title

(702) 382-4804 — Telephone Number

☑ Terminal disclaimer fee under 37 CFR 1.20(d) included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

PTO/AIA/26 (04-14)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT	Docket Number (Optional) FACETC.0082P

In re Application of: Kevin Alan Tussy

Application No.: 17/508,887

Filed: October 22, 2021

For: FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS

The applicant, FaceTec, Inc., owner of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of **prior patent** No. 10,776,471 as the term of said **prior patent** is presently shortened by any terminal disclaimer. The applicant hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the **prior patent** are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the applicant does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the **prior patent**, "as the term of said **prior patent** is presently shortened by any terminal disclaimer," in the event that said **prior patent** later:

- expires for failure to pay a maintenance fee;
- is held unenforceable;
- is found invalid by a court of competent jurisdiction;
- is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
- has all claims canceled by a reexamination certificate;
- is reissued; or
- is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2 below, if appropriate.

1. ☐ The undersigned is the applicant. If the applicant is an assignee, the undersigned is authorized to act on behalf of the assignee.

I hereby acknowledge that any willful false statements made are punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. 44,943

/Chad W. Miller/ — Signature

June 21, 2023 — Date

Chad W. Miller — Typed or printed name

Attorney of Record — Title

(702) 382-4804 — Telephone Number

☑ Terminal disclaimer fee under 37 CFR 1.20(d) included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT	Docket Number (Optional) FACETC.0082P

In re Application of: Kevin Alan Tussy

Application No.: 17/508,887

Filed: October 22, 2021

For: FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS

The applicant, FaceTec, Inc., owner of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of **prior patent** No. 11,157,606 as the term of said **prior patent** is presently shortened by any terminal disclaimer. The applicant hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the **prior patent** are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the applicant does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the **prior patent**, "as the term of said **prior patent** is presently shortened by any terminal disclaimer," in the event that said **prior patent** later:

- expires for failure to pay a maintenance fee;
- is held unenforceable;
- is found invalid by a court of competent jurisdiction;
- is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
- has all claims canceled by a reexamination certificate;
- is reissued; or
- is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2 below, if appropriate.

1. ☐ The undersigned is the applicant. If the applicant is an assignee, the undersigned is authorized to act on behalf of the assignee.

I hereby acknowledge that any willful false statements made are punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. 44,943

/Chad W. Miller/ — Signature

June 21, 2023 — Date

Chad W. Miller — Typed or printed name

Attorney of Record — Title

(702) 382-4804 — Telephone Number

☑ Terminal disclaimer fee under 37 CFR 1.20(d) included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Electronic Patent Application Fee Transmittal

Application Number:	17508887
Filing Date:	22-Oct-2021
Title of Invention:	FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS
First Named Inventor/Applicant Name:	Kevin Alan Tussy
Filer:	Chad W. Miller
Attorney Docket Number:	FACETC.0082P

Filed as Small Entity

Filing Fees for **Utility under 35 USC 111(a)**

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 2 months with $0 paid	2252	1	256	256
Miscellaneous:				
STATUTORY OR TERMINAL DISCLAIMER	2814	3	170	510
	Total in USD ($)			**766**

Electronic Acknowledgement Receipt

EFS ID:	48188647
Application Number:	17508887
International Application Number:	
Confirmation Number:	9577
Title of Invention:	FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS
First Named Inventor/Applicant Name:	Kevin Alan Tussy
Customer Number:	32856
Filer:	Chad W. Miller
Filer Authorized By:	
Attorney Docket Number:	FACETC.0082P
Receipt Date:	21-JUN-2023
Filing Date:	22-OCT-2021
Time Stamp:	20:10:54
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$766
RAM confirmation Number	E20236KK15579419
Deposit Account	502200
Authorized User	Chad Miller

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.21 (Miscellaneous fees and charges)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.16 (National application filing, search, and examination fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		CWMW18048OAR.pdf	48978 9e9d4dcdafba1b6aef58b454ce970536269ba7b2	yes	8

Multipart Description/PDF files in .zip description

Document Description	Start	End
Amendment/Request for Reconsideration-After Non-Final Rejection	1	1
Claims	2	7
Applicant Arguments/Remarks Made in an Amendment	8	8

Warnings:

Information:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
2	Terminal Disclaimer Filed	FACETC0082PTD10614204.pdf	196196 ca36fccc80ca048b25dacfc419802e5b09947c4e	no	3

Warnings:

Information:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
3	Terminal Disclaimer Filed	FACETC0082PTD10776471.pdf	126663 c64f075af0a51aa873348b92025d38e5a89336f6	no	1

Warnings:

Information:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
4	Terminal Disclaimer Filed	FACETC0082PTD11157606.pdf	126660 94b16ba6e4163737cb2cf90fc238bf273218247f	no	1

Warnings:

Information:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
5	Fee Worksheet (SB06)	fee-info.pdf	40463 adfdbf92ee4df183e26be433055ce8d92a73acda	no	2

Warnings:	
Information:	
Total Files Size (in bytes):	538960

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor	:	Kevin Alan Tussy	Group Art Unit: 2494
Appl. No.	:	17/508,887	I hereby certify that this correspondence and all marked attachments are being deposited with the United States Patent Office via EFSWeb filing, on:
Filed	:	October 22, 2021	June 21, 2023 (Date)
For	:	FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS	/Chad W. Miller/ Chad W. Miller Reg. No. 44,943
Examiner	:	Shanto Abedin	

RESPONSE TO OFFICE ACTION

Mail Stop Amendment
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In response to the Office Action dated January 31, 2023, please amend the above-identified patent application as follows. **The associated fees for Terminal Disclaimers (3) and a two-month extension of time request are submitted herewith.**

<u>IN THE CLAIMS</u>:

1. (original) A computing device for verifying three-dimensionality of a user via a user's camera equipped computing device, the computing device comprising:

a processor configured to execute machine executable code;

a screen configured to provide a user interface to the user;

a camera configured to capture images;

one or more memories configured to store machine readable instructions that are stored on the memory of the authentication server which when executed by the processor, cause the computing device to:

capturing at least one first image of the user taken with the camera of the computing device at a first location which is a first distance from the user;

processing the at least one first image or a portion thereof to create first data;

capturing at least one second image of the user taken with the camera of the computing device is at a second distance from the user, the second distance being different than the first distance, the capturing at least one second image of the user occurring after movement of the camera or the user to establish the camera at the second distance from the user;

processing the at least one second image or a portion thereof to create second data;

comparing the first data to the second data to determine whether expected differences exist between the first data and the second data which indicates three-dimensionality of the user;

verifying the images of the user exhibit three dimensional traits when the expected differences exist between the first data and the second data as a result of capturing the at least one first image and the at least one second image at different distances from the user.

2. (original) The system according to claim 1, further comprising:

interpolating the first data and the second data to obtain estimated intermediate data;

capturing at least one third image of the user taken with the camera of the computing device at a third distance from the user, the third distance being between the first distance and the second distances;

processing the at least one third image or a portion thereof to obtain third data; and

comparing the estimated intermediate data with the third data to determine whether the third data matches the estimated intermediate data.

3. (original) The system according to claim 1, further comprising verifying the presence of one or more features on a side of a user's head in the at least one first image, and verifying the absence or reduced visibility of the one or more features on the side of the user's head in the at least one second image due to image capture at different distances from the user's head, wherein the first distance is larger than the second distance.

4. (original) The system according to claim 1, wherein the machine readable instructions is configured to display one or more prompts on the screen of the computing device to guide the user to capture the at least one first image at the first distance and the at least on second image at the second distance.

5. (original) The system according to claim 1, further comprising comparing the first data, second data, or both to enrollment data derived from an enrollment image, the enrollment image captured and stored prior to an authenticating; and

only authenticating the user when the first data, the second data, or both match the enrollment data within a predetermined threshold.

6. (original) The system according to claim 1, wherein the computing device is a hand-held device, and the user holds the device at the first and second distance to capture the at least one first image and the at least one second image.

7. (original) The system according to claim 1, wherein the first data and the second data comprise biometric data.

8. (original) The system according to claim 1, wherein the first data and the second data comprise a mapping of facial features.

9. (original) The method according to claim 1, wherein the first image and the second image is of the user's face and the user's head and facial features are held steady and without movement during capture of the first image and the second image.

10. (currently amended) A method for evaluating ~~authenticating~~ three-dimensionality of a user ~~with a computing device during an authentication session~~, the method comprising:

capturing at least one first image of the user taken with a camera at a first location which is a first distance from the user~~, the camera associated with the computing device~~;

processing the at least one first image or a portion thereof to create first data;

moving the camera from the first location to a second location, the second location being a second distance from the user, or the user moving to change the distance between the user and the camera from the first distance to the second distance;

capturing at least one second image of the user taken with the camera ~~associated with the computing device~~ when the camera is the second distance from the user, the second distance being different than the first distance;

processing the at least one second image or a portion thereof to create second data;

comparing the first data to the second data to determine whether expected differences exist between the first data and the second data which indicate ~~indicated~~ three-dimensionality of the user;

verifying the images of the user exhibit three-dimensional traits when the first data and the second data have expected differences resulting from the at least one first image being captured with the camera at a different distance from the user than when the at least one second image is captured.

11. (currently amended) The method according to claim 10, further comprising:

interpolating the first data and the second data to obtain estimated intermediate data;

capturing at least one third image of the user taken with the camera ~~of the computing device~~ at a third distance from the user, the third distance being between the first distance and the second distances;

processing the at least one third image or a portion thereof to obtain third data; and

comparing the estimated intermediate data with the third data to determine whether the third data matches the estimated intermediate data.

12. (original) The method according to claim 10, further comprising verifying the presence of ears of the user in the at least one first image, and verifying the absence or reduced visibility of the ears in the at least one second image, wherein the first distance is larger than the second distance.

13. (currently amended) The method according to claim 10, <u>further comprising</u> ~~wherein the computing device is configured to display~~ one or more prompts on a screen ~~associated with the computing device~~ to guide the user to capture the at least one first image at the first distance and the at least on second image at the second distance.

14. (original) The method according to claim 13, wherein the one or more prompts are an oval shape guide on the screen within which an image of a face of the user is aligned to capture the at least one first image and the at least one second image.

15. (currently amended) The method according to claim 10, wherein <u>the camera is part of a</u> ~~the~~ computing device is a hand-held device, and the user holds the computing device at the first distance when capturing at least one first image and at the second distances when capturing the at least one second image.

16. (original) The method according to claim 10, wherein the first data and the second data comprise biometric data.

17. (currently amended) The method according to claim 10, wherein the first data and the second data comprise a map~~ping~~ of facial features.

18. (currently amended) The method according to claim 10, further comprising illuminate a screen of a ~~the~~ computing device while capturing the at least one first image and/or the at least one second image, and processing the at least one first image and/or the at least one second image to detect a reflection of the illumination from a face of the user.

19. (original) The method according to claim 10, wherein a face of the user is held steady when capturing the at least one first image and the at least one second image and the camera moves from the first location to the second location.

20. (currently amended) The method according to claim 10, wherein the first data and the second data are maintained on a ~~the~~ computing device.

21. (currently amended) The method of claim 10 wherein the camera is part of ~~computing device is~~ one of a smartphone, tablet, laptop, or desktop computer.

22. (previously presented) A method, performed by a user using a user's computer device, for verifying three-dimensionality of the user, the method comprising:

capturing a first image of the user's head with a camera at a first distance from the user, the camera associated with the user's computing device;

changing a distance between the user and the camera to a second distance by the user moving the camera, or the user moving relative to the camera, or both;

capturing a second image of the user's head with the camera when the camera is at the second distance from the user, the second distance being different than the first distance;

comparing one or more aspects of the user's head from the first image to one or more aspects of the user's head from the second image to determine whether expected differences, between the first image and the second image, exist which indicates three-dimensionality of the user, such that the expected differences between the first image and the second image result from the first image being captured when the camera is at a different distance from the user than when the second image is captured; and

responsive to the comparing determining that expected differences between the first image and the second image exist, providing notice to the user, a third party, or both that the three-dimensionality of the user is verified.

23. (previously presented) The method of claim 22 wherein the one or more aspects of the user's head from the first image is first data resulting from processing the first image and the one or more aspects of the user's head from the second image is second data resulting from processing the second image.

24. (previously presented) The method of claim 22 wherein the user's head is the user's face.

REMARKS

The Office Action dated January 31, 2023 has been carefully reviewed and considered. Claims 1-24 are pending and rejected in the Office Action. In the Office Action, the Examiner rejected claims 1-24 on the grounds of double patenting based on the Tussy references, U.S. Patent No. 11,157,606, U.S. Patent No. 10,776,471, and U.S. Patent No. 10,614,204.

Claim Amendments

The Applicant requests entry of the clarifying amendments set forth above.

Statutory Double Patenting Rejection

Claims 1-24 are rejected on the grounds of double patenting based on the commonly owned Tussy references. The Examiner requested Terminal Disclaimers based on U.S. Patent No. 11,157,606, U.S. Patent No. 10,776,471, and U.S. Patent No. 10,614,204.

In response, the Applicant submits herewith Terminal Disclaimer documents (3) including the associated fees, as set forth by the Examiner in the immediate Office Action. As such, it is respectfully submitted that the double patenting rejections have been obviated.

SUMMARY

In view of the foregoing, all the claims now pending in this application are believed to be in condition for allowance and request issuance of a Notice of Allowance. If any issues remain outstanding, the Examiner is invited to contact the undersigned by telephone.

Respectfully submitted,

Dated: June 21, 2023

By: /Chad W. Miller/
Chad W. Miller
Attorney of Record, Registration No. 44,943
Weide & Miller, Ltd.
10655 Park Run Drive, Suite 100
Las Vegas, NV 89144
(702) 382-4804 (Pacific Time)
cmiller@weidemiller.com

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 17/508,887	Filing Date 10/22/2021	☐ To be Mailed

ENTITY: ☐ LARGE ☑ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

	(Column 1)	(Column 2)			
FOR	NUMBER FILED	NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $50 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $240 =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT	06/21/2023	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0		x $40 =	0
	Independent (37 CFR 1.16(h))	* 6	Minus	*** 6	= 0		x $192 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	0

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=		x $0 =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=		x $0 =	
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.	SLIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/DIANIECE M JACOBS/
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".	
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.	

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/508,887	10/22/2021	Kevin Alan Tussy	FACETC.0082P	9577

32856 7590 01/31/2023

WEIDE & MILLER, LTD.
10655 PARK RUN DRIVE
SUITE 100
LAS VEGAS, NV 89144

EXAMINER	
ABEDIN, SHANTO	

ART UNIT	PAPER NUMBER
2494	

MAIL DATE	DELIVERY MODE
01/31/2023	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

Office Action Summary	**Application No.** 17/508,887	**Applicant(s)** Tussy, Kevin Alan	
	Examiner SHANTO ABEDIN	**Art Unit** 2494	**AIA (FITF) Status** Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 11/12/2021.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL.** 2b) ☑ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-24 is/are pending in the application.
5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-24 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☑ The drawing(s) filed on 10/22/2021 is/are: a)☑ accepted or b)☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
Certified copies:
a)☐ All b)☐ Some** c)☐ None of the:
1.☐ Certified copies of the priority documents have been received.
2.☐ Certified copies of the priority documents have been received in Application No. _____.
3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☑ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b)
Paper No(s)/Mail Date 01/24/2022; 05/05/2022 and 06/30/2022.

3) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date ______.

4) ☐ Other: ______.

Notice of Pre-AIA or AIA Status

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

DETAILED ACTION

1. This is in response to the communication filed on 11/12/2021. Claims 1-24 are pending in the application. Claims 1-24 are rejected.

Priority

2. Applicant's claim for the benefit of a prior-filed application under 35 U.S.C. 119(e) or under 35 U.S.C. 120, 121, 365(c), or 386(c) is acknowledged.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); and *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985).

The USPTO Internet website contains terminal disclaimer forms which may be used. Please visit www. uspto.gov/patent/patents-forms. The filing date of the application in which the form is filed determines what form (e.g., PTO/SB/25, PTO/SB/26, PTO/AIA/25, or PTO/AIA/26) should be used. A web-based eTerminal Disclaimer may be filled out completely online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and approved immediately upon submission. For more information about eTerminal Disclaimers, refer to www.uspto.gov/patents/process/file/efs/ guidance /eTD-info-I.jsp.

3. Claims 1-24 of the instant application are rejected under the judicially created doctrine of obviousness type double patenting as being unpatentable over claims 1-20 of the commonly owned US Patent No. 11,157,606 B2.

In particular, claims 1-2, 10-11 and 22 of the instant application are being unpatentable over claims 1, 10 and 19 of the commonly owned US Patent No. 11,157,606 B2; claims 3-6 and 12-15 of the instant application are being unpatentable over claims 3-6, 11-15 and 20 of the commonly owned US Patent No. 11,157,606 B2; claims 7-9, 16-21 and 23-24 of the instant application are being unpatentable over claims 6-9, 15-18 and 20 of the commonly owned US Patent No. 11,157,606 B2.

Although the conflicting claims are not identical, they are not patentably distinct from each other because claims 1-20 of patent No. 11,157,606 B2 contains every element of claims 1-24 of the instant application and thus anticipate the claim(s) of the instant application. Claims 1-24 of the instant application therefore is not patently distinct from the conflicting claim set of the earlier patent and as such is unpatentable over obvious-type double patenting. A later patent/application claim is not patentably distinct from an earlier claim if the later claim is anticipated by the earlier claim.

This is a non-statutory obviousness type double patenting rejection.

4. Claims 1-24 of the instant application are rejected under the judicially created doctrine of obviousness type double patenting as being unpatentable over claims 1-20 of the commonly owned US Patent No. 10,776,471 B2.

In particular, claims 1, 10 and 22 of the instant application are being unpatentable over claims 1 and 10 of the commonly owned US Patent No. 10,776,471 B2; claims 2 and 11 of the instant application are being unpatentable over claims 2 and 11 of the commonly owned US Patent No. 10,776,471 B2; claims 3-6 and 12-15 of the instant application are being unpatentable over claims 3-6 and 12-17 of the commonly owned US Patent No. 10,776,471 B2; and claims 7-9, 16-21 and 23-24 of the instant application are being unpatentable over claims 6-9 and 15-20 of the commonly owned US Patent No. 10,776,471 B2.

Although the conflicting claims are not identical, they are not patentably distinct from each other because claims 1-20 of patent No. No. 10,776,471 B2 contains every element of claims 1-24 of the instant application and thus anticipate the claim(s) of the instant application. Claims 1-24 of the instant application therefore is not patently distinct from the conflicting claim set of the earlier patent and as such is unpatentable over obvious-type double patenting. A later patent/application claim is not patentably distinct from an earlier claim if the later claim is anticipated by the earlier claim.

This is a non-statutory obviousness type double patenting rejection.

5. Claims 1-24 of the instant application are rejected under the judicially created doctrine of obviousness type double patenting as being unpatentable over claims 1-20 of the commonly owned US Patent No. 10,614,204 B2.

In particular, claims 1-2, 10-11 and 22 of the instant application are being unpatentable over claims 1-2 and 13 of the commonly owned US Patent No. 10,614,204 B2; claims 3-6 and 12-15 of the instant application are being unpatentable over claims 3-8 of the commonly owned US Patent No. 10,614,204 B2; claims 7-9, 16-21 and 23-24 of the instant application are being unpatentable over claims 5-12 of the commonly owned US Patent No. 10,614,204 B2.

Although the conflicting claims are not identical, they are not patentably distinct from each other because claims 1-20 of patent No. No. 10,614,204 B2 contains every element of claims 1-24 of the instant application and thus anticipate the claim(s) of the instant application. Claims 1-24 of the instant application therefore is not patently distinct from the conflicting claim set of the earlier patent and as such is unpatentable over obvious-type double patenting. A later patent/application claim is not patentably distinct from an earlier claim if the later claim is anticipated by the earlier claim.

This is a non-statutory obviousness type double patenting rejection.

Allowable Subject Matter

6. Claims 1-24 would be allowable if rewritten or amended (or if a terminal disclaimer is filed) to overcome the obviousness type double patenting rejections, set forth in this Office action.

Conclusion

7. A shortened statutory period for response to this action is set to expire in 3 (Three) months and 0 (Zero) days from the mailing date of this letter. Failure to respond within the period for response will result in ABANDOMENT of the application (see 35 U.S.C 133, M.P.E.P 710.02(b)). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SHANTO ABEDIN whose telephone number is 571-272-3551. The examiner can normally be reached on M-F from 8:30 AM to 6:30 PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jung (Jay) Kim, can be reached on 571-272-3804. The RightFax number for faxing directly to the examiner is 571-273-3551.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/SHANTO ABEDIN/
Primary Examiner, Art Unit 2494

Notice of References Cited

Application/Control No. 17/508,887	Applicant(s)/Patent Under Reexamination Tussy, Kevin Alan	
Examiner SHANTO ABEDIN	Art Unit 2494	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-8396265-B1	03-2013	Ross; Steven James	G06V40/172	382/103
*	B	US-9607138-B1	03-2017	Baldwin; Leo Benedict	H04W12/06	1/1
*	C	US-20140337948-A1	11-2014	Hoyos; Hector	G06Q20/40145	726/7
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No. 17/508,887	Applicant(s)/Patent Under Reexamination Tussy, Kevin Alan
	Examiner SHANTO ABEDIN	Art Unit 2494

CPC - Searched*		
Symbol	**Date**	**Examiner**
CPC Search: G06F21/32, G06V40/168, G06V40/172, G06V40/18, G06V40/20	01/24/2023	SA

CPC Combination Sets - Searched*		
Symbol	**Date**	**Examiner**

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	**Date**	**Examiner**
Inventor Assignee/ Double Patenting search	01/24/2023	SA
CPC classification search (with limited keyword search)	01/24/2023	SA
PE2E databases keyword search (see search history)	01/24/2023	SA
NPL: Google Scholar, IEEE Xplore search (see search history)	01/24/2023	SA
Consulted search notes from related application No. 16/817,428 and 15/900,681	01/24/2023	SA

/SHANTO ABEDIN/ Primary Examiner, Art Unit 2494	

Search Notes	Application/Control No. 17/508,887	Applicant(s)/Patent Under Reexamination Tussy, Kevin Alan
	Examiner SHANTO ABEDIN	Art Unit 2494

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**
Claim Interference Search	G06F21/32, G06V40/168, G06V40/172, G06V40/18, G06V40/20	01/24/2023	SA

/SHANTO ABEDIN/
Primary Examiner, Art Unit 2494

Index of Claims	Application/Control No. 17/508,887	Applicant(s)/Patent Under Reexamination Tussy, Kevin Alan
	Examiner SHANTO ABEDIN	Art Unit 2494

✓	**Rejected**		-	**Cancelled**	N	**Non-Elected**		A	**Appeal**
=	**Allowed**		÷	**Restricted**	I	**Interference**		O	**Objected**

CLAIMS

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	01/26/2023								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								
	22	✓								
	23	✓								
	24	✓								

Pcca: A new approach for **distance** learning from sparse pairwise constraints
A Mignon, F Jurie - 2012 IEEE conference on computer vision …, 2012 - ieeexplore.ieee.org
… the **distance** means computing L such that, for a given **threshold** t… **face verification**, we use the popular Labeled Faces in the Wild (LFW) dataset [16]. It contains more than 13,000 **images** …
Save Cite Cited by 739 Related articles All 18 versions

Discriminative deep metric learning for **face verification** in the wild
J Hu, J Lu, YP Tan - Proceedings of the IEEE conference on …, 2014 - openaccess.thecvf.com
… In this paper, we consider the second one where **face images** … **distance** of the positive pair is less than a smaller **threshold** … We follow the standard evaluation protocol on the "**View** 2" …
Save Cite Cited by 785 Related articles All 15 versions

Deep learning **face** representation by joint identification-**verification**
Y Sun, Y Chen, X Wang, X Tang - Advances in neural …, 2014 - proceedings.neurips.cc
… the entire LFW **face image** including the **face** region and large … (2) requires the **distance** larger than a margin m. θve = {m} is … a **threshold** optimized on the training data for **face verification**…
Save Cite Cited by 2533 Related articles All 15 versions

Neural network-based **face** detection
HA Rowley, S Baluja, T Kanade - IEEE Transactions on pattern …, 1998 - ieeexplore.ieee.org
… equal number of pixels in the **dimensions** of scale and position, … To examine the effect of this **threshold** value during testing, … **distance** metrics measure the **distance** of an input **image** to …
Save Cite Cited by 6139 Related articles All 59 versions

Tour the world: building a web-scale landmark recognition engine
YT Zheng, M Zhao, Y Song, H Adam… - … IEEE Conference on …, 2009 - ieeexplore.ieee.org
… Moreover, we also adopt a multi-**view face** detector [15] to filter out … **image** matching. The clustering process is then equivalent to erasing graph edges above a certain **distance threshold** …
Save Cite Cited by 483 Related articles All 22 versions

Gabor wavelets and general discriminant analysis for **face** identification and **verification**
LL Shen, L Bai, M Fairhurst - Image and Vision Computing, 2007 - Elsevier
… However, due to the high **dimensionality** of the feature vector, especially in **face** recognition, S … **distance** of the test **face** with the training **images** of the identity is below a global **threshold**, …
Save Cite Cited by 368 Related articles All 9 versions

Combining RGB and ToF cameras for real-time 3D hand gesture interaction
M Van den Bergh, L Van Gool - 2011 IEEE workshop on …, 2011 - ieeexplore.ieee.org
… **face** is detected and the **distance** from the **face** to the **camera** is measured. Based on this **distance**, a **threshold** is applied to the depth **image** to … , and half for **validation**. The 350 sample …
Save Cite Cited by 418 Related articles All 10 versions

Face recognition using the nearest feature line method
SZ Li, J Lu - IEEE transactions on neural networks, 1999 - ieeexplore.ieee.org
… In the following, we define a new **distance** measure that will be used in the NFL and … **images** taken **live** and hence the feature points cannot be ordered in terms of a single **parameter** as …
Save Cite Cited by 722 Related articles All 14 versions

Learning locally-adaptive decision functions for person **verification**
Z Li, S Chang, F Liang, TS Huang… - Proceedings of the …, 2013 - openaccess.thecvf.com
… decisions based on a fixed **threshold**. We show that this is … for **verification** that can be viewed as a joint model of a **distance** … both human body **verification** and **face verification** problems. …
Save Cite Cited by 610 Related articles All 14 versions

On the use of SIFT features for **face authentication**

M Bicego, A Lagorio, E Grosso... - 2006 Conference on ..., 2006 - ieeexplore.ieee.org

... of 2D **images**, it was never applied to **face** recognition/... In this paper the simple Euclidean **Distance** has been investigated, even ... The **parameter** R indicates the cost ratio between false ac...

☆ Save 99 Cite Cited by 522 Related articles All 20 versions

Robust **face detection** using the hausdorff **distance**
O Jesorsky, KJ Kirchberg, RW Frischholz - … Biometric Person Authentication …, 2001 - Springer
… **Face recognition** is a major area of research within biometric signal processing. Since most techniques (eg Eigenfaces) assume the **face images** … The **parameter** set ˆp that minimizes h(…
Save Cite Cited by 1345 Related articles All 16 versions

Gabor wavelets and general discriminant analysis for **face identification** and **verification**
LL Shen, L Bai, M Fairhurst - Image and Vision Computing, 2007 - Elsevier
… However, due to the high **dimensionality** of the feature vector, especially in **face** … if the mean **distance** of the test **face** with the training **images** of the identity is below a global **threshold**, …
Save Cite Cited by 368 Related articles All 9 versions

Face recognition using the nearest feature line method
SZ Li, J Lu - IEEE transactions on neural networks, 1999 - ieeexplore.ieee.org
… In the following, we define a new **distance** measure that will be used in the NFL and … **images** taken **live** and hence the feature points cannot be ordered in terms of a single **parameter** as …
Save Cite Cited by 722 Related articles All 14 versions

Deep learning **face** representation by joint **identification-verification**
Y Sun, Y Chen, X Wang, X Tang - Advances in neural …, 2014 - proceedings.neurips.cc
… and using both **face identification** and **verification** signals as … (2) requires the **distance** larger than a margin m. θve = {m} is … a **threshold** optimized on the training data for **face verification**. …
Save Cite Cited by 2533 Related articles All 15 versions

Kernel machine-based one-**parameter** regularized fisher discriminant method for **face recognition**
WS Chen, PC Yuen, J Huang… - IEEE Transactions on …, 2005 - ieeexplore.ieee.org
… samples is smaller than the **dimensionality** of feature vector. In … using **face images** with pose, illumination **facial expressions** … class **distance** and simultaneously maximizes between-class …
Save Cite Cited by 142 Related articles All 5 versions

Enhanced local texture feature sets for **face recognition** under difficult lighting conditions
X Tan, B Triggs - IEEE transactions on image processing, 2010 - ieeexplore.ieee.org
… metric based on local **distance** transforms further improves the … **face** alignment is within a few pixels, our default **parameter** … on **dimensionality** increasing techniques for improving **face** …
Save Cite Cited by 2973 Related articles All 32 versions

Counter-measures to photo attacks in **face recognition**: a public database and a baseline
A Anjos, S Marcel - 2011 international joint conference on …, 2011 - ieeexplore.ieee.org
… **Images** can also be easily cap tured at **distance** without … : motion, texture anal ysis and **liveness** detection. In motion analysis one … ing the **threshold** T on the EER at the development set. …
Save Cite Cited by 385 Related articles All 19 versions

Enhanced local texture feature sets for **face recognition** under difficult lighting conditions
X Tan, B Triggs - Analysis and Modeling of Faces and Gestures: Third …, 2007 - Springer
… with a local **distance** transform based similarity metric further … The default **parameter** values (for 120×120 **face images** in … on **dimensionality** increasing techniques for improving **face** …
Save Cite Cited by 984 Related articles All 39 versions

Distance measures for PCA-based **face recognition**
V Perlibakas - Pattern recognition letters, 2004 - Elsevier
… SSE-based **distance** we need to extract less **images** in order to … Because the **dimensionality** (N 2) of the matrix C is large … faces a **threshold** τ is chosen and it is said that the **face** with …
Save Cite Cited by 409 Related articles All 8 versions

Discriminative deep metric learning for **face verification** in the wild

J Hu, J Lu, YP Tan - … computer vision and pattern recognition, 2014 - openaccess.thecvf.com

… In this paper, we consider the second one where **face images** … **distance** of the positive pair is less than a smaller **threshold** … and existing videobased **face recognition** methods on the YTF …

IEEE.org IEEE *Xplore* IEEE SA IEEE Spectrum More Sites Cart Create Account Personal Sign In

Browse My Settings Help Access provided by: **United States Patent and Trademark Office** Sign Out

Access provided by: **United States Patent and Trademark Office** Sign Out

All

ADVANCED SEARCH

Search within results

Download PDFs | Export | Alert Set Search Alerts | Search History

Showing **1-2** of **2** results for
("Abstract":authentication) OR ("Abstract":recognition) AND ("All Metadata":image) AND ("Full Text & Metadata":distance) AND ("Full Text & Metadata":camera) AND ("Full Text & Metadata":liveness) ✕
facial ✕ verification ✕ live ✕

Filters Applied: 1991 - 2014 ✕

Conferences (2)

Filter

Alert Set Search Alerts | sort: Sort Relevance

Show

All Results

Subscribed Content

Open Access Only

Year

Single Year | Range

2012 2014

From 2012 To 2014

Author

Affiliation

Publication Title

Publisher

Face verification using temporal affective cues
Ee-Sin Ng; Alex Yong-Sang Chia
Proceedings of the 21st International Conference on Pattern Recognition (ICPR2012)
Year: 2012 | Conference Paper | Publisher: IEEE
Cited by: Patents (1)

Abstract HTML

It is widely accepted that biometric authentication systems based on human faces are vulnerable to spoofing attacks, in which attackers exploit recaptured photos of legitimate users to gain unauthorized access. To address this vulnerability, numerous approaches which employ complex physics-based models to verify the live-ness of presented images have been proposed. While capable of dis... Show More

Face verification using temporal affective cues
Ee-Sin Ng; Alex Yong-Sang Chia
Proceedings of the 21st International Conference on Pattern Recognition (ICPR2012)
Year: 2012 | Conference Paper | Publisher: IEEE

Conference Location

Publication Topics

Biometric authentication for older adults
Marc Alexander Kowtko
IEEE Long Island Systems, Applications and Technology (LISAT) Conference 2014
Year: 2014 | Conference Paper | Publisher: IEEE
Cited by: Papers (12)

Abstract HTML

In recent times, cyber-attacks and cyber warfare have threatened network infrastructures from across the globe. The world has reacted by increasing security measures through the use of stronger passwords, strict access control lists, and new authentication means; however, while these measures are designed to improve security and Information Assurance (IA), they may create accessibility chall... Show More

Biometric authentication for older adults
Marc Alexander Kowtko
IEEE Long Island Systems, Applications and Technology (LISAT) Conference 2014
Year: 2014 | Conference Paper | Publisher: IEEE

Access provided by:
United States Patent and Trademark Office

Sign Out

All

ADVANCED SEARCH

Search within results

Download PDFs | Export | Alert Set Search Alerts | Search History

Showing **1-5** of **5** results for
("Abstract":authentication) OR ("Abstract":recognition) AND ("All Metadata":image) AND ("Full Text & Metadata":distance) AND ("Full Text & Metadata":camera) AND ("Full Text & Metadata":liveness) ✕
three-dimensional ✕ face ✕ authentication ✕ camera ✕

Filters Applied: 1991 - 2014 ✕

Conferences (4) Journals (1)

Filter

Alert Set Search Alerts | sort: Sort Relevance

Show

All Results

Subscribed Content

Open Access Only

Year

Single Year Range

2010 2014

From 2010 To 2014

Author

Affiliation

Publication Title

Publisher

Continuous 3D Face Authentication Using RGB-D Cameras
Mauricio Pamplona Segundo; Sudeep Sarkar; Dmitry Goldgof; Luciano Silva; Olga Bellon
2013 IEEE Conference on Computer Vision and Pattern Recognition Workshops
Year: 2013 | Conference Paper | Publisher: IEEE
Cited by: Papers (18) | Patents (1)

Abstract HTML

Continuous 3D Face Authentication Using RGB-D Cameras
Mauricio Pamplona Segundo; Sudeep Sarkar; Dmitry Goldgof; Luciano Silva; Olga Bellon
2013 IEEE Conference on Computer Vision and Pattern Recognition Workshops
Year: 2013 | Conference Paper | Publisher: IEEE

Robust 3D face recognition from low resolution images
A. Drosou; P. Moschonas; D. Tzovaras
2013 International Conference of the BIOSIG Special Interest Group (BIOSIG)
Year: 2013 | Conference Paper | Publisher: IEEE

Conference Location

Publication Topics

▾ Abstract HTML

This paper proposes a combined approach for robust face recognition from low resolution images captured by a low-budget commercial depth camera. The low resolution of the facial region of interest is compensated via oversampling techniques and efficient trimming algorithms for the generation of an accurate 3D facial model. Two state of the art algorithms for geometric feature extractio... Show More

Robust 3D face recognition from low resolution images

A. Drosou; P. Moschonas; D. Tzovaras
2013 International Conference of the BIOSIG Special Interest Group (BIOSIG)
Year: 2013 | Conference Paper | Publisher: IEEE

A new approach of stereoscopic imaging analysis for biometric recognition using traditional eigenface technique
Narasimhan Renga Raajan; Mohan Vishnu Priya; Subramanian Suganya; D. Parthiban; A. Jenifer Philomina; Balakrishnan Monisha; Mohan Ram Kumar
2012 International Conference on Computing, Communication and Applications
Year: 2012 | Conference Paper | Publisher: IEEE
Cited by: Papers (1)

▸ Abstract HTML

A new approach of stereoscopic imaging analysis for biometric recognition using traditional eigenface technique

Narasimhan Renga Raajan; Mohan Vishnu Priya; Subramanian Suganya; D. Parthiban; A. Jenifer Philomina; Balakrishnan Monisha; Mohan Ram Kumar
2012 International Conference on Computing, Communication and Applications
Year: 2012 | Conference Paper | Publisher: IEEE

An Evaluation of Video-to-Video Face Verification
Norman Poh; Chi Ho Chan; Josef Kittler; Sébastien Marcel; Christopher Mc Cool; Enrique Argones Rúa; José Luis Alba Alba Castro; Mauricio Villegas; Roberto Paredes; Vitomir Štruc; Nikola Pavešić; Albert Ali Salah; Hui Fang; Nicholas Costen
IEEE Transactions on Information Forensics and Security

Year: 2010 | Volume: 5, Issue: 4 | Journal Article | Publisher: IEEE
Cited by: Papers (29)

Abstract HTML

Person recognition using facial features, e.g., mug-shot images, has long been used in identity documents. However, due to the widespread use of web-cams and mobile devices embedded with a camera, it is now possible to realize facial video recognition, rather than resorting to just still images. In fact, facial video recognition offers many advantages over still image recognition; these incl... Show More

An Evaluation of Video-to-Video Face Verification

Norman Poh; Chi Ho Chan; Josef Kittler; Sébastien Marcel; Christopher Mc Cool; Enrique Argones Rúa; José Luis Alba Alba Castro; Mauricio Villegas; Roberto Paredes; Vitomir Štruc; Nikola Pavešić; Albert Ali Salah; Hui Fang; Nicholas Costen
IEEE Transactions on Information Forensics and Security
Year: 2010 | Volume: 5, Issue: 4 | Journal Article | Publisher: IEEE

3D head model fitting evaluation protocol on synthetic databases for acquisition system comparison
Catherine Herold; Vincent Despiegel; Stéphane Gentric; Séverine Dubuisson; Isabelle Bloch
2014 International Conference on Computer Vision Theory and Applications (VISAPP)
Year: 2014 | Volume: 3 | Conference Paper | Publisher: IEEE

Abstract HTML

3D head model fitting evaluation protocol on synthetic databases for acquisition system comparison

Catherine Herold; Vincent Despiegel; Stéphane Gentric; Séverine Dubuisson; Isabelle Bloch
2014 International Conference on Computer Vision Theory and Applications (VISAPP)
Year: 2014 | Volume: 3 | Conference Paper | Publisher: IEEE

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

SHEET 1 OF 1

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2003/217294	11/03	Kyle			
		2011/0196753	08/11	Hodgdon, et al.			
		2011/0276484	11/11	Pearson, et al.			
		2012/0066758	03/12	Kasturi			
		8,200,980	06/12	Robinson, et al.			
		8,355,528	01/13	Bladel, et al.			
		8,787,627	07/14	Freedman			
		9,286,507	03/16	Shuster			
		9,621,548	04/17	Bud			
		2017/0111493	04/17	Stone			
		10,032,066	07/18	Gongaware, et al.			
		2019/0105551	04/19	Ray			
		10,917,431	02/21	Turgeman			
		10,963,669	03/21	Berini, et al.			

FOREIGN PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION YES	TRANSLATION NO
		3075573	01/13	Canada			X	
		1693801	08/06	Europe			X	

EXAMINER INITIAL		**OTHER DOCUMENTS** (INCLUDING AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.)

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 01/26/2023

***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

CWM-W-16753

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		5,031,228	07/91	Lu			
		5,699,449	12/97	Javidi			
		5,784,056	07/98	Nielsen			
		5,781,650	07/98	Lobo, et al.			
		5,835,616	11/98	Lobo, et al.			
		5,842,194	11/98	Arbuckle			
		5,850,470	12/98	Kung, et al.			
		5,956,122	09/99	Doster			
		5,982,912	11/99	Fukui, et al.			
		6,134,339	10/00	Luo			
		6,173,068	01/01	Prokoski			
		6,212,030	04/01	Koriyama, et al.			
		6,246,779	06/01	Fukui, et al.			
		6,301,370	10/01	Steffens, et al.			
		6,310,601	10/01	Moore, et al.			
		2002/0103813	05/02	Frigon			
		2002/0054059	05/02	Scheiderman			
		2002/0055955	05/02	Lloyd-Jones, et al.			
		6,389,176	05/02	Hsu, et al.			
		2002/0087622	07/02	Anderson			
		6,461,807	10/02	Friend, et al.			
		2002/0191818	12/02	Matsuo, et al.			
		2003/0039380	02/03	Sukegawa, et al.			
		2003/0053663	03/03	Chen, et al.			
		2003/0063669	04/03	Lee, et al.			
		2003/0095053	05/03	Kandogan			

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 01/26/2023
***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.	

CWM-W-16209

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2003/0103652	06/03	Lee, et al.			
		2003/0133599	07/03	Tian, et al.			
		2003/0198368	10/03	Kee			
		2003/0236832	12/03	McIntyre, et al.			
		6,678,664	01/04	Ganesan			
		D485,279	01/04	DeCombe			
		6,697,502	02/04	Luo			
		6,687,390	02/04	Avni, et al.			
		6,711,584	03/04	Wajda, et. al.			
		6,728,401	04/04	Hardeberg			
		2004/0070678	04/04	Toyama, et al.			
		2004/0081338	04/04	Takenaka			
		2004/0091136	05/04	Dombrowski			
		2004/0109584	06/04	Lestideau			
		2004/0125991	07/04	Yokoi			
		2004/0143598	07/04	Drucker, et al.			
		6,775,397	08/04	Hamalainen			
		2004/0190758	09/04	Doi, et al.			
		2004/0201709	10/04	McIntyre, et al.			
		2004/0218792	11/04	Spoonhower, et al.			
		2004/0264780	12/04	Zhang, et al.			
		6,840,149	01/05	Beal			
		2005/0031173	02/05	Hwang			
		2005/0065885	03/05	Gordon			
		2005/0065855	03/05	Geller			
		2005/0094849	05/05	Sung, et al.			

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 01/26/2023
***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.	

CWM-W-16209

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2005/0100195	05/05	Li			
		2005/0117802	06/05	Yonaha et al.			
		2005/0141766	06/05	Nagahashi, et al.			
		2005/0180627	08/05	Yan, et al.			
		2005/0190273	09/05	Toyama, et al.			
		2005/0220347	10/05	Enomoto			
		6,961,361	11/05	Tanaka			
		2005/0251015	11/05	Takikawa, et al.			
		2005/0265603	12/05	Porter			
		7,003,135	02/06	Hsieh, et al.			
		2006/0050933	03/06	Adam, et al.			
		2006/0110014	05/06	Philomin			
		2006/0133672	06/06	Li			
		2006/0156029	07/06	Algazi			
		2006/0173560	08/06	Widrow			
		2006/0218225	09/06	Hee Voon, et al.			
		2006/0224523	10/06	Elvitigala			
		2006/0222215	10/06	Jung, et al.			
		2006/0239515	10/06	Zhang, et al.			
		2006/0251292	11/06	Gokturk, et al.			
		2006/0251339	11/06	Gokturk, et al.			
		2006/0251338	11/06	Gokturk, et al.			
		2006/0253491	11/06	Gokturk, et al.			
		2006/0274978	12/06	Fukuda, et al.			
		2007/0074114	03/07	Adjali, et al.			
		2007/0081744	04/07	Gokturk, et al.			

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 01/26/2023
***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.	

CWM-W-16209

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

SHEET 4 OF 16

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		7,211,138	05/07	Yamamoto, et al.			
		7,218,774	05/07	Liu			
		2007/0098230	05/07	Norita			
		2007/0098303	05/07	Gallagher, et al.			
		7,231,657	06/07	Honarvar, et al.			
		2007/0177805	08/07	Gallagher			
		2007/0206834	09/07	Shinkai, et al.			
		2007/0211925	09/07	Aoki, et al.			
		7,289,648	10/07	Liu			
		7,308,581	12/07	Geosimonian			
		2007/0290499	12/07	Tame			
		2008/0046458	02/08	Tseng, et al.			
		2008/0037869	02/08	Zhou			
		7,333,963	02/08	Widrow, et al.			
		2008/0077595	03/08	Leebow			
		2008/0080743	04/08	Schneiderman, et al.			
		2008/0080745	04/08	Vanhoucke, et al.			
		2008/0091723	04/08	Zuckerberg, et al.			
		2008/0100195	05/08	Kim, et al.			
		2008/0130960	06/08	Yagnik			
		7,415,152	08/08	Jiang, et al.			
		7,428,320	09/08	Northcott, et al.			
		2008/0212849	09/08	Gao			
		2008/0317379	12/08	Steinberg, et al.			
		7,519,200	04/09	Gokturk, et al.			
		D596,192	07/09	Shotel			

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 01/26/2023
***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.	

CWM-W-16209

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
INFORMATION DISCLOSURE CITATION BY APPLICANT (USE SEVERAL SHEETS IF NECESSARY)	INVENTOR(S) Kevin Alan Tussy	
	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2009/0185784	09/09	Hiroike, et al.			
		2009/0226052	09/09	Fedel			
		2009/0232367	09/09	Shinzaki			
		D601,582	10/09	Chaudhri			
		2009/0252383	10/09	Adam, et al.			
		2009/0324022	12/09	Sangberg, et al.			
		D606,082	12/09	Parker			
		7,636,450	12/09	Bourdev			
		2009/0324018	12/09	Tell			
		2009/0324137	12/09	Stallings, et al.			
		7,646,909	01/10	Jiang, et al.			
		2010/0050134	02/10	Clarkson			
		7,660,444	02/10	Hamalainen			
		2010/0054601	03/10	Anbalagan, et al.			
		2010/0067750	03/10	Matsuo			
		2010/0054600	03/10	Anbalagan, et al.			
		2010/0061631	03/10	Omori			
		7,710,693	05/10	Guzman-Casillas, et al.			
		2010/0158327	06/10	Kangas, et al.			
		7,783,118	08/10	Zhou			
		7,788,247	08/10	Wang, et al.			
		2010/0232656	09/10	Ryu			
		7,804,982	09/10	Howard, et al.			
		2010/0245614	09/10	Matsunaga			
		7,809,722	10/10	Gokturk, et al.			
		D625,325	10/10	Vu			

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 01/26/2023
***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.	

CWM-W-16209

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2010/0272363	10/10	Steinberg, et al.			
		2010/0287053	11/10	Ganong, et al.			
		2010/0310133	12/10	Mason, et al.			
		2010/0318366	12/10	Sullivan			
		2010/0317420	12/10	Hoffberg			
		2011/0063108	03/11	Aonuma, et al.			
		D637,604	05/11	Brinda			
		7,945,653	05/11	Zuckerberg, et al.			
		7,960,470	06/11	Okahira			
		D640,277	06/11	Woo			
		2011/0169853	07/11	Oiwa			
		2011/0202531	08/11	Zuckerberg, et al.			
		2011/0225481	09/11	Zuckerberg, et al.			
		2011/0282906	11/11	Wong			
		D650,793	12/11	Impas			
		8,121,408	02/12	Omori			
		8,165,352	04/12	Mohanty, et al.			
		2012/0140993	06/12	Bruso, et al.			
		D663,743	07/12	Tanghe			
		D663,744	07/12	Tanghe			
		8,210,247	07/12	Blomgren			
		8,244,211	08/12	Clark			
		D667,423	09/12	Nagamine			
		2012/0235790	09/12	Zhao, et al.			
		8,280,120	10/12	Hoyos, et al.			
		8,316,237	11/12	Felsher, et al.			

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 01/26/2023
***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.	

CWM-W-16209

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2012/0323704	12/12	Steelberg			
		8,326,000	12/12	Jung, et al.			
		2013/0007032	01/13	Klappert			
		2013/0015946	01/13	Lau			
		8,392,268	03/13	Smith, et al.			
		2013/0066526	03/13	Mondragon			
		2013/0057693	03/13	Baranek			
		8,396,246	03/13	Anbalagan, et al.			
		2013/0077835	03/13	Kritt, et al.			
		8,411,909	04/13	Zhao, et al.			
		2013/0086674	04/13	Horvitz, et al.			
		8,416,312	04/13	Matsunaga			
		8,457,367	06/13	Sipe			
		8,460,024	06/13	Damodharan, et al.			
		2013/0179298	07/13	Segman			
		2013/0226740	08/13	Biliosa			
		2013/0236066	09/13	Shubinsky			
		2013/0246158	09/13	Cannon			
		D692,018	10/13	Wenz			
		2013/0267204	10/13	Schultz, et al.			
		D692,915	11/13	Brinda			
		2013/0342672	12/13	Gray, et al.			
		2014/0012756	01/14	Beraja			
		2014/0022179	01/14	Yoon			
		2014/0059673	02/14	Azar			
		8,709,801	04/14	Pan, et al.			

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 01/26/2023
***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.	

CWM-W-16209

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

SHEET 8 OF 16

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2014/0098174	04/14	Summers			
		D702,714	04/14	Abratowski			
		8,722,977	05/14	Wooten, Jr.			
		2014/0118257	05/14	Baldwin			
		2014/0123275	05/14	Azar			
		8,743,051	06/14	Moy, et al.			
		2014/0165187	06/14	Daesung			
		2014/0169643	06/14	Todoroki			
		2014/0173443	06/14	Hawkins, III			
		8,750,574	06/14	Ganong, et al.			
		2014/0197922	07/14	Stanwood			
		2014/0198959	07/14	Derakhshani			
		D712,909	09/14	Francisco			
		D713,410	09/14	Francisco			
		8,856,541	10/14	Chaudhury			
		8,867,849	10/14	Kirkham			
		D715,317	10/14	Perace			
		2014/0337791	11/14	Agnetta			
		2014/0337948	11/14	Hoyos			
		2014/0351761	11/14	Bae			
		D717,339	11/14	Wen			
		D717,829	11/14	Lee			
		8,922,480	12/14	Freed, et al.			
		2015/0052462	02/15	Kulkarni			
		2015/0055821	02/15	Fotland			
		8,959,578	02/15	Simpson, et al.			

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 01/26/2023
***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.	

CWM-W-16209

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/ SHEET 9 OF 16

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2015/0074615	03/15	Han			
		2015/0077323	03/15	Ramaswamy			
		D725,151	03/15	Bray			
		D725,668	03/15	Clare			
		D726,221	04/15	Gomez			
		9,037,354	05/15	Mondragon			
		2015/0148106	05/15	Choi			
		D728,623	05/15	Lim			
		D730,389	05/15	Izotov			
		2015/0131872	05/15	Ganong, et al.			
		9,069,447	06/15	Kim			
		2015/0153571	06/15	Ballard			
		D730,941	06/15	Marianek			
		D731,552	06/15	Seo			
		9,076,008	07/15	Moy			
		9,076,028	07/15	Summers			
		2015/0205399	07/15	Kim			
		2015/0205454	07/15	Ainslie			
		2015/0212684	07/15	Sabia			
		D733,755	07/15	Kadosh			
		2015/0227286	08/15	Kangas, et al.			
		D736,812	08/15	Yoo			
		D737,325	08/15	Kim			
		9,137,246	09/15	Parry, et al.			
		D738,921	09/15	Lim			
		2015/0310260	10/15	Summers			

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 01/26/2023
***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.	

CWM-W-16209

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/ SHEET 10 OF 16

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		D740,833	10/15	Bae			
		9,152,849	10/15	Ganong, et al.			
		D742,417	11/15	Brunner			
		9,202,105	12/15	Wang, et al.			
		9,209,355	12/15	Senda, et al.			
		2015/0378433	12/15	Savastinuk			
		D745,567	12/15	Park			
		2016/0026425	01/16	Lee			
		D747,354	01/16	Park			
		2016/0063235	03/16	Tussy			
		D752,078	03/16	Guesnon, Jr.			
		2016/0071111	03/16	Wang, et al.			
		2016/0087991	03/16	Matsuoka			
		D753,132	04/16	Cuthbert			
		2016/0117544	04/16	Hoyos, et al.			
		D756,401	05/16	Soldner			
		D757,084	05/16	Chaudhri			
		D759,723	06/16	Butcher			
		2016/0209939	07/16	Zambetti			
		D761,268	07/16	Oh			
		D761,277	07/16	Harvell			
		9,424,491	08/16	Kirkham			
		9,430,695	08/16	Summers			
		D762,655	08/16	Kai			
		D762,673	08/16	Seo			
		D762,715	08/16	Williamson			

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 01/26/2023

***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

CWM-W-16209

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		D763,271	08/16	Everette			
		D763,306	08/16	Lee			
		D764,526	08/16	Gomez			
		D764,534	08/16	Seo			
		D765,117	08/16	Joo			
		D765,133	08/16	Joo			
		9,448,687	09/16	McKenzie			
		2016/0259528	09/16	Foss			
		2016/0261675	09/16	Block			
		2016/0284123	09/16	Hare			
		D765,674	09/16	Kim			
		D766,926	09/16	Fleischmann			
		D766,314	09/16	Bauer			
		D766,298	09/16	Bae			
		9,459,132	10/16	Fehrenbach, et al.			
		D769,933	10/16	Sabia			
		2016/0342826	11/16	Apostolos, et al.			
		D772,288	11/16	Montes			
		D772,929	11/16	Montes			
		2016/0335483	11/16	Pfursich, et al.			
		2016/0364561	12/16	Lee			
		D776,680	01/17	Bae			
		D777,755	01/17	Beaty			
		8,649,604	02/17	Steinberg, et al.			
		D778,923	02/17	Zhou			
		D778,940	02/17	Williamson			

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 01/26/2023

***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

CWM-W-16209

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

SHEET 12 OF 16

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2017/0053406	02/17	Hirvonen			
		9,607,138	03/17	Baldwin			
		2017/0083086	03/17	Mazur			
		D780,781	03/17	Ding			
		9,600,649	03/17	Parry, et al.			
		D783,633	04/17	Oh			
		D783,652	04/17	Guan			
		D784,363	04/17	Fleming, et al.			
		D787,527	05/17	Wilberding			
		D788,122	05/17	Tada			
		D788,810	06/17	Kim			
		D790,567	06/17	Su			
		D791,158	07/17	Shiino			
		9,708,909	07/17	Atkinson, et al.			
		9,740,848	08/17	Parry, et al.			
		2017/0220843	08/17	Apostolos, et al.			
		D794,663	08/17	Sakuma			
		D798,321	09/17	Lieb			
		9,798,420	10/17	Ichikawa			
		D798,902	10/17	Choi			
		D799,544	10/17	Kim			
		D800,743	10/17	Rhodes			
		D801,990	11/17	Reissner			
		D803,870	11/17	Landry			
		D805,546	12/17	Wu			
		D805,548	12/17	King			

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 01/26/2023

***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

CWM-W-16209

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		D806,113	12/17	Beckman			
		D807,378	01/18	Imamura			
		D807,381	01/18	Hersh			
		9,911,036	03/18	Hartman			
		9,958,687	05/18	Chern, et al.			
		2018/0139157	05/18	Decculus			
		D817,994	05/18	Jou			
		D819,075	05/18	Tsuji			
		2018/0165508	06/18	Othman, et al.			
		D820,305	06/18	Clediere			
		D821,439	06/18	Sowden			
		D821,443	06/18	Jang			
		D822,054	07/18	Persson			
		D823,335	07/18	Alonso			
		D823,867	07/18	Berlow			
		D823,891	07/18	Lupe			
		D825,587	08/18	O'Rourke			
		D825,588	08/18	Hashimoto			
		2018/0342018	11/18	Pancholi			
		2019/0080189	03/19	VAN OS			
		10,360,464	07/19	McKay, et al.			
		2019/0213311	07/19	Tussy			
		2020/0042685	02/20	Tussy, et al.			
		2021/0011986	01/21	Tussy			

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 01/26/2023

***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

CWM-W-16209

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

SHEET 14 OF 16

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

FOREIGN PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION YES	TRANSLATION NO
		1388802	02/04	EP				
		1455297	09/04	EP				
		2005-287878	10/05	JP				
		2006-259923	09/06	JP				
		2006/130542	12/06	WIPO				
		2007-148968	06/07	JP				
		2007-304801	11/07	JP				
		2008/107002	09/08	WIPO				
		2007/119818	08/09	WIPO				
		20130097581	09/13	KR				
		2014-010686	01/14	JP				
		103593594	02/14	CN				
		2015/070320	05/15	WIPO				
		2017/100929	06/17	WIPO				
		10-1755995	07/17	KR				
		10-2019-0038923	04/19	KR				

EXAMINER INITIAL		**OTHER DOCUMENTS** (INCLUDING AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.)
		Hagai Aronowitz, et al., Multi-Modal Biometrics for Mobile Authentication, IJCB, 2014
		Silvio Barra, et al., FAME: Face Authentication for Mobile Encounter, IEEE, 2013
		Girija Chetty and Michael Wagner, “Automated lip feature extraction for liveness verification in audio-video authentication”, Human Computer Communication laboratory School of Information Sciences and Engineering, University of Canberra, Australia, Proc. Image and Vision Computer (2004), 1 January, 2004, 6 pages.
		Rogssignol, Joe. "How to customise the Lock screen in iOS 7." iDownloadBlog, posted January 11, 2014 (Retrieved from the internet 3/30/2016). Internet URL: <http: //www.idownloadblog.com/2014/01/11/how-to-theme-the-lock-screen-on-oos-7/>
		android_locked-out-PDF, screenshot, date unknown, author unknown.
		android-lock-screen1-PDF, screenshot, date unknown, author unknown.

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 01/26/2023

***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

CWM-W-16209

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

SHEET 15 OF 16

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

EXAMINER INITIAL		**OTHER DOCUMENTS** (INCLUDING AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.)
		facetime-PDF, screenshot, date unknown, author unknown.
		BLETSKO et al., "Using Skin-Color Motion for 3D Face Modelling and Synthesis", September 6, 2003, WISP 2003, pages 295-299_
		image 9-PDF, screenshot, date unknown, author unknown.
		iphone-Facetime-PDF, screen shot, date unknown, author unknown.
		keyboard-PDF, screen shot, date unknown, author unknown.
		passcode-lock-PDF, screen shot, date unknown, author unknown.
		passcode-PDF, screen shot, date unknown, author unknown.
		screen Shot-PDF, screen shot, date unknown, author unknown.
		screenshot_2012-06-20-16-06-32-PDF, screen shot, date unknown, author unknown.
		topic_facetime_ios-PDF, screen shot, date unknown, author unknown.
		Shutterstock [online], 4 August 2014 [retried 24 July 2016]. Retrieved from the internet URL:http://www.tineye.com/search/543afefb8836762927558call587ce7f99a706ad/.,pic-199246373 stock phot male silhouette image.
		wp_ss_20130124_00071-PDF, screen shot, January 24, 2013, author unknown.
		After Effects Tutorial - 17 - Introduction to Masking, by thenewboston, uploaded 12/07/2008, youtube.com [online], [retrieved 06/15/2017]. Available from <URL:https://www.youtube.com/watch?v=kWd51xDqzlc>
		Optical Illusions - Animated GIF & JPG, dated 10/28/2013, plus.google.com [online], [retrieved 06/19/2017]. Available from internet <URL:https://plus.google.com/+Whak-Off/posts/CX4YhzXSQy2>
		The Universal Face Login for 5 Billion Smartphones, zoomlogin.com [online], [retrieved 06/19/2017]. Available from internet <URL:https://zoomlogin.com/>
		Wong, Yongkang, et al. "Patch-based probabilistic image quality assessment for face selection and improved video-based face recognition." CVPR 2011 WORKSHOPS. IEEE, 2011
		RAFALOVITCH, "Viewfinder Friends-idea for Facebook application", November 14, 2007, http://blog.outerthoughts.com/2007/11/viewfinder-friends-idea-for-facebook-application/, 5pages.
		KISHORE, "How to Add, Upload, and Tag Your Pictures and Photos in FaceBook", http://www.online-tech-tips.com/fun-stuff/how-to-add-upload-and-tag-your-pictures-and-photos-in-facebook/, August 11, 2007, 13 pages.
		BECKER et al., "Evaluation of Face Recognition Techniques for Application to Facebook", IEEE International conference on Automatic Face and Gesture Recognition, 2008, 6 pages.
		BAKER, "Google & Riya Face Recognition Photo Search", November 22, 2005, http://www.searchenginejournal.com/google-riya-face-recognition-photo-search/25501, 1 page_
		PONCE, "Riya, Photo Sharing with Face Recognition", October 28, 2005, http://www.ohgizmo.com/2005/10/28/riya-photo-sharing-with-face-recognition/, 2 pages_
		FACEBOOK, "Making Photo Tagging Easier", https://m.facebook.com/notes/facebook/making-photo-tagging-easier/467145887130/?_tn_=C&_rdr, 2 pages
		MICHELSON et al., "Auto-tagging the Facebook", 2006, http://cs229.stanford.edu/proj2006/MichelsonOrtizAutoTaggingTheFacebook.pdf, 5 pages.
		ARRINGTON, "First Screen Shots of Riya", October 26, 2005, http://techcrunch.com/2005/10/26/riya-prepares-tolaunch-alpha/, 10 pages
		ARRINGTON, "Ojos - Auto Name & Tag Your Photos", August 15, 2005, http://techcrunch.com/2005/08/31/ojos-auto-name-tag-your-photos/, 8 pages.

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 01/26/2023

***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

CWM-W-16209

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

EXAMINER INITIAL		**OTHER DOCUMENTS** (INCLUDING AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.)
		STONE, et al. "Autotagging Facebook: Social network context improves photo annotation," In Workshop on Internet Vision, 2008, 2 pages_
		SCHUON et al., "CS229 Project Report: Automated photo tagging in Facebook", December 2007, http://cs229. Stanford.edu/proj2007/SchuonRobertsonZou-AutomatedPhotoTaggingInFacebook.pdf, 5 pages.
		YADAV, "Facebook - The Complete Biography", August 25, 2006, http://mashable.com12006/08/25/facebook-protile/, 7 pages_
		UNKNOWN, "What does it mean to "tag" someones picture on facebook, whats the point of doing it?", November 28, 2007, https://answers.yahoo.com/question/index?qid=20071128123629AAY0DLP, 2 pages.
		Yang, et al., "Detecting Faces in Images: A Survey", January 2002, IEEE Trans. Pattern Analysis Machine Intelligence, 24(1), 2 pages
		Japan Patent Office ("JPO") Preliminary Report issued for Application No. JP2020-023503 on February 9, 2021

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 01/26/2023
***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.	

CWM-W-16209

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/ SHEET 1 OF 1

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)

FOREIGN PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION	
							YES	NO

EXAMINER INITIAL		**OTHER DOCUMENTS** (INCLUDING AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.)
		"An Overview of Face Liveness Detection", Chakraborty, et al., Dept. of Computer Science and Engineering, National Institute of Technology, Silchar India, International Journal on Information Theory (IJIT), Vol. 3, No. 2, DOI: 10.512/ijit.2014.3202, 15 pages, April 2014.
		"SVO Fast Semi-Direct Monocular Visual Odometry", Christian Forster, et al., ResearchGate, Conference Paper in Proceedings - IEEE International Conference on Robotics and Automation, DOI: 10.1109/ICRA.2014.6906584, https://www.researchgate.net/publication/262378002, 9 pages, May 18, 2014.
		"Evaluating Liveness by Face Images and the Structure Tensor", Kollreider, et al., Halmstad University, SE-30118, Sweden, Halmstad University Post-Print, ©IEEE 2005, Fourth IEEE Workshop on Automatic Identification Advanced Technologies, 2005, IEEE: 2005. PGS. 75-80, DOI: http://dx.doi.org/10.1109/AUTOID.2005.20, 7 pages, date unknown.
		"An Iterative Image registration Technique with an Application to Stereo Vision", Lucas, et al., Computer Science Department, Carnegie-Mellon University, Pittsburgh, Pennsylvania 15213, From Proceedings of Imaging Understanding Workshop, PP. 121-130 (1981)., pgs. 121-130, 10 pgs., date unknown.
		"Head Gesture Recognition Using Optical Flow Based Classification with Reinforcement of GMM Based Background Subtraction", Saikia, et al., Department of Electronics and Communication Engineering, DBCET, Assam Don Bosco University, International Journal of Computer Application (0975-8887), Volume 65- No. 25, March 2013, 7 pgs.
		"A Liveness Detection Method for Face Recognition Base on Optical Flow Field", Bao, et al., College of Computer Science, Zhejiang University, 978-1-4244-3986-7/09/$25.00 ©2009 IEEE,IEEE Xplore (03/15/22 download), 4 pages.

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 01/26/2023
***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.	

CWM-W-16566

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L1	116	Kevin near3 Tussy.in.	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 07:32 PM
L2	26	FaceTec.as.	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 07:33 PM
L3	131	L1 OR L2	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 07:39 PM
L4	197937	(G06F21/32 OR G06V40/168 OR G06V40/172 OR G06V40/18 OR	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU,	AND	ON	ON	2023/01/23 07:42 PM

		G06V40/20).cpc.	CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L5	25	L3 ((image)(distance)(liveness OR three-dimensionality)).clm.	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 07:43 PM
L6	6	L3 ((image)(distance)(liveness OR three-dimensionality)(illumination OR visibility OR suitable)(face OR facial OR head)).clm.	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 07:46 PM
L7	2	"10614204".pn.	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA,	AND	ON	ON	2023/01/23 07:47 PM

			VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L8	4	"11157606".pn.	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 07:49 PM
L9	8	"11157606".pn. "10614204".pn. "10776471".pn.	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/01/23 08:01 PM
L10	3	L9 ((image)(distance)(liveness OR three-dimensional$4)(face OR facial OR head)).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:01 PM
L11	22045	((image)(distance)(liveness OR three-dimensional$4)(face OR facial OR head)).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB,	AND	ON	ON	2023/01/23 08:07 PM

			HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L12	14595	((image) SAME (distance)(liveness OR three-dimensional$4)(face OR facial OR head)).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:07 PM
L13	19006	((image) SAME (distance)(liveness OR three-dimensional$4 OR live OR physical)(face OR facial OR head)).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:08 PM
L14	14256	((image) SAME (distance)(liveness OR three-dimensional$4 OR live OR physical) SAME (distance OR expected OR determin$3)(face OR facial OR head)).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT;	AND	ON	ON	2023/01/23 08:09 PM

			IBM_TDB)				
L15	4444	((second) SAME (image) SAME (distance)(liveness OR three-dimensional$4 OR live OR physical) SAME (distance OR expected OR determin$3)(face OR facial OR head)).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:09 PM
L16	118	((second) SAME (image) SAME (distance)(liveness OR three-dimensional$4 OR live OR physical) SAME (distance OR expected OR determin$3)(face OR facial OR head)).clm. (biometric)(authentication)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:09 PM
L17	175	((second) SAME (image) SAME (distance)(liveness OR three-dimensional$4 OR live OR physical) SAME (distance OR expected OR determin$3)(face OR facial OR head)).clm. (biometric)(authentication OR identity)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:10 PM
L18	107	((second) SAME (image) SAME (distance)(liveness OR three-dimensional$4 OR live OR physical) SAME (distance OR expected OR determin$3)(face OR	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV,	AND	ON	ON	2023/01/23 08:10 PM

		facial OR head)).clm. (biometric)(authentication OR identity)(predetermined OR expected OR threshold).clm.	MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L19	99	((second) SAME (image) SAME (distance)(liveness OR three-dimensional$4 OR live OR physical) SAME (distance OR expected OR determin$3)(face OR facial OR head)).clm. (biometric)(authentication OR identity)(predetermined OR expected OR threshold).clm. (face OR facial)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:11 PM
L20	63	((second) SAME (image) SAME (distance)(liveness OR three-dimensional$4 OR live OR physical) SAME (distance OR expected OR determin$3)(face OR facial OR head)).clm. (biometric)(authentication OR identity)(predetermined OR expected OR threshold).clm. (face OR facial)(camera).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:11 PM
L21	25	L20 @ad<"20180220"	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:12 PM
L22	10	L21 NOT FaceTec.as.	(US-PGPUB; USPAT;	AND	ON	ON	2023/01/23

			USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				08:12 PM
L23	272	((liveness OR three-dimensional$4 OR live OR physical) (face OR facial OR head) SAME (side OR portion OR captur$3)(illuminat$4 OR brightness)).clm.(authentication)(biometric)(distance)(image)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:16 PM
L24	377	L16 OR L23	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:16 PM
L25	144	L24 (authentication OR live OR liveness OR dimensional$4).ab. (image) SAME (distance)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL,	AND	ON	ON	2023/01/23 08:17 PM

			PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L26	61	L25 @ad<"20180220"	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:17 PM
L27	24	L26 NOT FaceTec.as.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:18 PM
L28	7	L27 (second) SAME (image) SAME (captur$3 OR camera) SAME (distance)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:19 PM
L29	33	L22 OR L27	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY,	AND	ON	ON	2023/01/23 08:20 PM

			CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L30	12	L29 (second OR compar$3 OR match$3) SAME (image) SAME (captur$3 OR camera) SAME (distance OR movement OR moving OR path).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:20 PM
L31	14	L29 (illumination OR brightness).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:22 PM
L32	23	L30 OR L31	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH,	AND	ON	ON	2023/01/23 08:22 PM

			TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L33	12	L32 (distance).clm. (liveness OR dimensional$4)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:23 PM
L34	40	(US-0066758-$ | US-0105551-$ | US-0111493-$ | US-0196753-$ | US-0276484-$ | US-10032066-$ | US-10917431-$ | US-10963669-$ | US-1693801-$ | US-20110196753-$ | US-20110276484-$ | US-20120066758-$ | US-20170111493-$ | US-20190105551-$ | US-3075573-$ | US-8200980-$ | US-8355528-$ | US-8787627-$ | US-9286507-$ | US-9621548-$).DID.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/01/23 08:37 PM
L35	88	(US-0031173-$ | US-0065855-$ | US-0065885-$ | US-0070678-$ | US-0081338-$ | US-0091136-$ | US-0094849-$ | US-0103652-$ | US-0109584-$ | US-0125991-$ | US-0133599-$ | US-0143598-$ | US-0190758-$ | US-0198368-$ | US-0201709-$ | US-0218792-$ | US-0236832-$ | US-	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/01/23 08:38 PM

		0264780-$ | US-20030103652-$ | US-20030133599-$ | US-20030198368-$ | US-20030236832-$ | US-20040070678-$ | US-20040081338-$ | US-20040091136-$ | US-20040109584-$ | US-20040125991-$ | US-20040143598-$ | US-20040190758-$ | US-20040201709-$ | US-20040218792-$ | US-20040264780-$ | US-20050031173-$ | US-20050065855-$ | US-20050065885-$ | US-20050094849-$ | US-6678664-$ | US-6687390-$ | US-6697502-$ | US-6711584-$ | US-6728401-$ | US-6775397-$ | US-6840149-$ | US-D485279-$).DID.					
L36	128	L34 OR L35	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/01/23 08:38 PM
L37	8	L36 (second OR compar$3 OR match$3) SAME (image) SAME (captur$3 OR camera) SAME (distance OR movement OR moving OR path)(authentication OR identity OR recognition)(live OR liveness OR physical)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO;	AND	ON	ON	2023/01/23 08:39 PM

			JPO; DERWENT; IBM_TDB)				
L38	24	L36 (G06F21/32 OR G06V40/168 OR G06V40/172 OR G06V40/18 OR G06V40/20).cpc.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:39 PM
L39	26	L37 OR L38	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:40 PM
L40	1	L38 (image).clm. (illumination OR distance).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:40 PM
L41	49	L32 OR L39	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS,	AND	ON	ON	2023/01/23 08:41 PM

			IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L43	23	L41 (three near3 dimension$3)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:42 PM
L44	21	L41 (three near3 dimension$3)(image).clm.(face OR facial)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:42 PM
L45	17	L41 (three near3 dimension$3)(image).clm.(face OR facial)(liveness OR authentication)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:42 PM

L46	7	L41 (three near3 dimension$3)(image).clm.(face OR facial)(liveness OR authentication)(distance).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/23 08:44 PM
L47	2	16/405,906	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/01/24 01:51 PM
L48	6	"11157606".pn. "10614204".pn. "11157606".pn.	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/01/24 07:55 PM
L49	8	"11157606".pn. "10614204".pn. "10776471".pn.	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO,	OR	ON	ON	2023/01/24 08:01 PM

			MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L50	44264	(captur$3 OR camera) SAME (image) SAME (distance OR movement OR path)(liveness OR three-dimensionality OR dimensional$4)(face OR facial)(authenticat$3)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:15 PM
L51	15082	L50 (second OR compar$3 OR match$3) SAME (image) SAME (captur$3 OR camera) SAME (distance OR movement OR moving OR path)(authentication OR identity OR recognition)(live OR liveness OR physical)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:16 PM
L52	4016	L50 (illumination OR brightness).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:16 PM
L53	6978	L51 (illumination OR brightness) (image).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT,	AND	ON	ON	2023/01/24 08:16 PM

			AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L54	9472	L52 OR L53	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:17 PM
L55	2217	L54 (biometric OR authenticat$3 OR customer OR liveness OR three-dimensionality OR dimensional$3).ab.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:18 PM
L56	965	L54 (biometric OR authenticat$3 OR customer OR liveness OR three-dimensionality OR dimensional$3).ab. (image).clm.(face OR facial).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE,	AND	ON	ON	2023/01/24 08:18 PM

			SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L57	1067	L54 (illumination OR brightness)(distance).clm. (image).clm.(face OR facial).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:19 PM
L58	1868	L24 OR L56 OR L57	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:19 PM
L59	530	L58 (compar$3 OR match$3) SAME (image).clm. (distance).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:20 PM
L60	359	L56 L57	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU,	AND	ON	ON	2023/01/24 08:21 PM

			CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L61	222	L59 L60	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:21 PM
L62	667	L59 OR L60	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:21 PM
L63	398	L62 (second) SAME (image).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN,	AND	ON	ON	2023/01/24 08:21 PM

			WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L64	218	L62 (second) SAME (image) SAME (distance).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:22 PM
L65	373	L62 (portion OR second) SAME (image) SAME (distance OR face).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:22 PM
L66	218	L64 L65	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:23 PM
L67	373	L64 OR L65	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB,	AND	ON	ON	2023/01/24 08:23 PM

			HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L68	157	L67 (compar$3 OR match$3 OR verifying) SAME (image) SAME (distance).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:23 PM
L69	228	L67 (compar$3 OR match$3 OR verifying) SAME (image) SAME (distance) SAME (face OR facial OR portion OR side)(illumination OR brightness)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:24 PM
L70	90	L67 (compar$3 OR match$3 OR verifying) SAME (image) SAME (distance) SAME (face OR facial OR portion OR side)(illumination OR brightness).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT;	AND	ON	ON	2023/01/24 08:26 PM

			IBM_TDB)				
L71	203	L68 OR L70	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:30 PM
L72	27	FaceTec.as.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/01/24 08:31 PM
L73	117	Kevin near2 Tussy.in.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/01/24 08:31 PM
L74	132	L72 OR L73	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV,	OR	ON	ON	2023/01/24 08:31 PM

			MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L75	44	L74 (three-dimensionality OR dimensional)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:32 PM
L76	20	L74 (three near3 dimensionality)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:32 PM
L77	43	L74 (three) near3 (dimensional OR dimensionality)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:33 PM
L78	42	L74 (three) near3	(US-PGPUB; USPAT;	AND	ON	ON	2023/01/24

		(dimensional OR dimensionality) SAME (determin$3 OR based OR compar$3 OR verify$3)	USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				08:33 PM
L79	40	L74 @ad<"20140828"	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:35 PM
L80	1	L79 (authenticat$3 OR customer OR liveness OR three-dimensionality OR dimensional$3).ab. (biometric OR user OR customer OR verify$3 OR movement OR motion OR face OR facial).ab. (image).clm.(face OR facial).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2023/01/24 08:36 PM
L81	0	L80 NOT Tussy.in.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL,	AND	ON	ON	2023/01/24 08:37 PM

			PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				

PE2E SEARCH - Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
N1	1809	((image) SAME (distance)(liveness OR three-dimensional$4 OR live OR physical) SAME (distance OR expected OR determin$3)(face OR facial OR head)).clm.	(US-PGPUB; USPAT)	AND	ON	ON	2023/01/24 08:38 PM
N2	51	((second) SAME (image) SAME (distance)(liveness OR three-dimensional$4 OR live OR physical) SAME (distance OR expected OR determin$3)(face OR facial OR head)).clm. (biometric)(authentication)	(US-PGPUB; USPAT)	AND	ON	ON	2023/01/24 08:39 PM
N3	1809	N1 (illumination OR brightness OR distance OR movement).clm.	(US-PGPUB; USPAT)	AND	ON	ON	2023/01/24 08:40 PM
N4	1809	N1 (illumination OR brightness OR distance OR movement) SAME (image OR face).clm.	(US-PGPUB; USPAT)	AND	ON	ON	2023/01/24 08:40 PM
N5	4435	(three) near3 (dimensional OR dimensionality) SAME (determin$3 OR based OR compar$3 OR verify$3) (compar$3 OR match$3 OR verifying) SAME (image) SAME (distance) SAME (face OR facial OR portion OR side)(illumination OR brightness)	(US-PGPUB; USPAT)	AND	ON	ON	2023/01/24 08:41 PM
N6	38264	(G06F21/32 OR G06V40/168 OR G06V40/172 OR G06V40/18 OR G06V40/20).cpc.	(US-PGPUB; USPAT)	AND	ON	ON	2023/01/24 08:41 PM
N7	155	N4 N5	(US-PGPUB; USPAT)	AND	ON	ON	2023/01/24

							08:42 PM
N8	563	(N6)(N4 OR N5)(image).clm.	(US-PGPUB; USPAT)	AND	ON	ON	2023/01/24 08:42 PM
N9	20	(US-0066758-$ | US-0105551-$ | US-0111493-$ | US-0196753-$ | US-0276484-$ | US-10032066-$ | US-10917431-$ | US-10963669-$ | US-1693801-$ | US-20110196753-$ | US-20110276484-$ | US-20120066758-$ | US-20170111493-$ | US-20190105551-$ | US-3075573-$ | US-8200980-$ | US-8355528-$ | US-8787627-$ | US-9286507-$ | US-9621548-$).DID.	(US-PGPUB; USPAT)	OR	ON	ON	2023/01/24 08:43 PM
N10	35	(US-0039380-$ | US-0053663-$ | US-0054059-$ | US-0055955-$ | US-0063669-$ | US-0087622-$ | US-0095053-$ | US-0103813-$ | US-0191818-$ | US-20020054059-$ | US-20020055955-$ | US-20020087622-$ | US-20020103813-$ | US-20020191818-$ | US-20030039380-$ | US-20030053663-$ | US-20030063669-$ | US-20030095053-$ | US-5031228-$ | US-5699449-$ | US-5781650-$ | US-5784056-$ | US-5835616-$ | US-5842194-$ | US-5850470-$ | US-5956122-$ | US-5982912-$ | US-6134339-$ | US-6173068-$ | US-6212030-$ | US-6246779-$ | US-6301370-$ | US-6310601-$ | US-6389176-$ | US-	(US-PGPUB; USPAT)	OR	ON	ON	2023/01/24 08:43 PM

		6461807-$).DID.					
N11	712	N7 OR N8 OR N9 OR N10	(US-PGPUB; USPAT)	OR	ON	ON	2023/01/24 08:44 PM
N13	176	N11 ((camera OR captur$3) SAME (image) SAME (distance OR movement OR moving) SAME (face OR facial OR head OR side)).clm.	(US-PGPUB; USPAT)	AND	ON	ON	2023/01/24 08:49 PM
N14	345	N11 ((three near3 dimensional$3) OR (liveness)).clm.	(US-PGPUB; USPAT)	AND	ON	ON	2023/01/24 08:50 PM
N15	345	N11 ((three near3 dimensional$3) OR (liveness)).clm. (image).clm.	(US-PGPUB; USPAT)	AND	ON	ON	2023/01/24 08:50 PM
N16	293	N11 ((three near3 dimensional$3) OR (liveness)).clm. (image).clm. (distance).clm.	(US-PGPUB; USPAT)	AND	ON	ON	2023/01/24 08:50 PM
N17	362	N13 OR N16	(US-PGPUB; USPAT)	AND	ON	ON	2023/01/24 08:50 PM
N18	104	N17 @ad<"20140828"	(US-PGPUB; USPAT)	AND	ON	ON	2023/01/24 08:51 PM
N19	40	N18 (authenticat$3 OR verifying)(image).clm. (distance).clm.	(US-PGPUB; USPAT)	AND	ON	ON	2023/01/24 08:52 PM
N20	23	N18 (authenticat$3 OR verifying)(image).clm. (illumination OR brightness) (face OR facial).clm.	(US-PGPUB; USPAT)	AND	ON	ON	2023/01/24 08:52 PM
N21	41	N19 OR N20	(US-PGPUB; USPAT)	AND	ON	ON	2023/01/24 08:53 PM
N22	41	N21 NOT FaceTec.as.	(US-PGPUB; USPAT)	AND	ON	ON	2023/01/24 08:53 PM
N23	29	N22 (camera) SAME (distance) SAME (image)	(US-PGPUB; USPAT)	AND	ON	ON	2023/01/24 08:54 PM
N24	20	N23 (distance) SAME (image) SAME (three-dimensionality OR liveness OR live OR physical) SAME (determin$3 OR compar$3 OR threshold OR range)	(US-PGPUB; USPAT)	AND	ON	ON	2023/01/24 08:55 PM
N25	14	N24 (captur$3) SAME (distance) SAME (image) SAME (face OR facial)(image)	(US-PGPUB; USPAT)	AND	ON	ON	2023/01/24 08:57 PM

		SAME (three-dimensionality OR liveness OR live OR physical) SAME (determin$3 OR compar$3 OR threshold OR range)					
N26	10	"8396265".pn. "9607138".pn. "10268911".pn. "20040190758" "20130219480" "20150262024"	(US-PGPUB; USPAT)	OR	ON	ON	2023/01/24 08:59 PM
N27	1	N26 (captur$3 OR camera) SAME (distance) SAME (image) SAME (face OR facial OR head).clm. (image) SAME (three-dimensionality OR liveness OR live OR physical) SAME (determin$3 OR compar$3 OR threshold OR range).clm.	(US-PGPUB; USPAT)	AND	ON	ON	2023/01/24 09:00 PM
N28	2	N26 (captur$3 OR camera) SAME (distance) SAME (image) SAME (face OR facial OR head).clm. (image) SAME (three-dimensionality OR liveness OR live OR physical) SAME (determin$3 OR compar$3 OR threshold OR range) (compar$3 OR match$3 OR verifying OR threshold) SAME (second OR distance) SAME (image).clm.	(US-PGPUB; USPAT)	AND	ON	ON	2023/01/24 09:01 PM
N29	2	N27 OR N28	(US-PGPUB; USPAT)	AND	ON	ON	2023/01/24 09:01 PM
N30	69	N9 OR N10 OR N25	(US-PGPUB; USPAT)	AND	ON	ON	2023/01/24 09:02 PM
N31	5	N30 (captur$3 OR camera) SAME (distance) SAME (image) SAME (face OR facial OR head).clm. (image) SAME (three-dimensionality OR	(US-PGPUB; USPAT)	AND	ON	ON	2023/01/24 09:02 PM

		liveness OR live OR physical) SAME (determin$3 OR compar$3 OR threshold OR range) .clm. (compar$3 OR match$3 OR verifying OR threshold) SAME (second OR distance) SAME (image).clm.					
N32	5	N31 @ad<"20140828"	(US-PGPUB; USPAT)	AND	ON	ON	2023/01/24 09:03 PM
N33	3	N32 (three) near3 (dimensional$4)	(US-PGPUB; USPAT)	AND	ON	ON	2023/01/24 09:04 PM
N34	3	N32 (three) near3 (dimensional$4).clm. (distance).clm.	(US-PGPUB; USPAT)	AND	ON	ON	2023/01/24 09:05 PM
N35	3	N32 (three) near3 (dimensional$4).clm. (face OR camera) SAME (image) SAME (distance).clm.	(US-PGPUB; USPAT)	AND	ON	ON	2023/01/24 09:05 PM
N36	3	N32 (three) near3 (dimensional$4) SAME (verifying OR determin$3 OR based).clm. (face OR camera) SAME (image) SAME (distance).clm. (captur$3 OR movement).clm.	(US-PGPUB; USPAT)	AND	ON	ON	2023/01/24 09:06 PM
N37	1	N32 (three) near3 (dimensional$4) SAME (verifying OR determin$3 OR based).clm. (face OR camera) SAME (image) SAME (distance) SAME (second).clm. (captur$3 OR movement).clm.	(US-PGPUB; USPAT)	AND	ON	ON	2023/01/24 09:07 PM
N38	1	N26 (captur$3 OR camera) SAME (distance) SAME (image) SAME (face OR facial OR head).clm. (image) SAME (three-dimensionality OR liveness OR live OR physical) SAME (determin$3 OR compar$3 OR threshold OR range OR predetermined).clm.	(US-PGPUB; USPAT)	AND	ON	ON	2023/01/24 09:07 PM

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE **INFORMATION DISCLOSURE CITATION BY APPLICANT** (USE SEVERAL SHEETS IF NECESSARY)	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
	INVENTOR(S) Kevin Alan Tussy	
	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2003/217294	11/03	Kyle			
		2011/0196753	08/11	Hodgdon, et al.			
		2011/0276484	11/11	Pearson, et al.			
		2012/0066758	03/12	Kasturi			
		8,200,980	06/12	Robinson, et al.			
		8,355,528	01/13	Bladel, et al.			
		8,787,627	07/14	Freedman			
		9,286,507	03/16	Shuster			
		9,621,548	04/17	Bud			
		2017/0111493	04/17	Stone			
		10,032,066	07/18	Gongaware, et al.			
		2019/0105551	04/19	Ray			
		10,917,431	02/21	Turgeman			
		10,963,669	03/21	Berini, et al.			

FOREIGN PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION	
							YES	NO
		3075573	01/13	Canada			X	
		1693801	08/06	Europe			X	

EXAMINER INITIAL		**OTHER DOCUMENTS** (INCLUDING AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.)

EXAMINER	DATE CONSIDERED

***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

CWM-W-16753

Innovation, Sciences et Développement économique Canada
Office de la Propriété Intellectuelle du Canada

Innovation, Science and Economic Development Canada
Canadian Intellectual Property Office

CA 3075573 A1 2013/01/03

(21) **3 075 573**

(12) **DEMANDE DE BREVET CANADIEN**
CANADIAN PATENT APPLICATION

(13) **A1**

(22) Date de dépôt/Filing Date: 2012/05/15
(41) Mise à la disp. pub./Open to Public Insp.: 2013/01/03
(62) Demande originale/Original Application: 2 840 171
(30) Priorité/Priority: 2011/06/29 (US61/502,453)

(51) Cl.Int./Int.Cl. *G07C 11/00* (2006.01), *G06F 21/32* (2013.01)

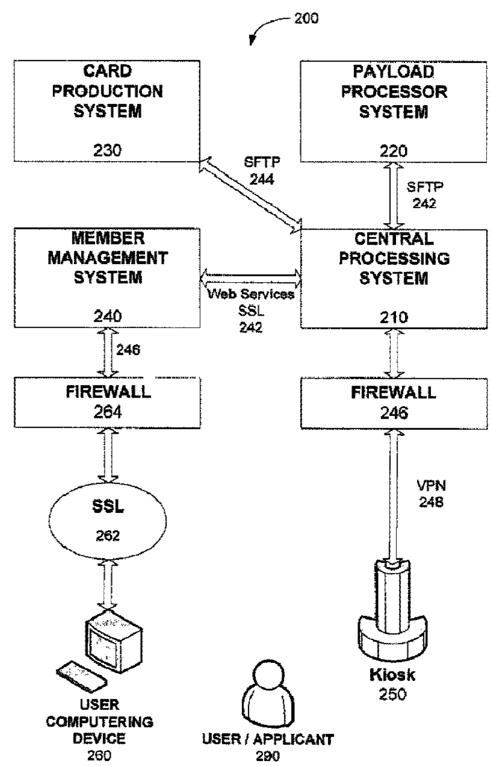
(71) Demandeur/Applicant:
ALCLEAR, LLC, US

(72) Inventeurs/Inventors:
CORNICK, KENNETH, US;
SEIDMAN BECKER, CARYN, US

(74) Agent: GOWLING WLG (CANADA) LLP

(54) Titre : SYSTEME ET PROCEDE POUR SOUMETTRE UN UTILISATEUR A UN SYSTEME SECURISE DE VERIFICATION BIOMETRIQUE

(54) Title: SYSTEM AND METHOD FOR USER ENROLLMENT IN A SECURE BIOMETRIC VERIFICATION SYSTEM



(57) Abrégé/Abstract:
A computer-implemented method and system for verifying the identity of a user in an identity authentication and biometric verification system which includes collecting information from the user regarding the user's identity, which is then electronically

(57) **Abrégé(suite)/Abstract(continued):**
authenticated. Upon authentication, personal information regarding the verified identity of the user is retrieved from a source database which is used to verify the identity of the user, via user interaction. Upon successful verification and authentication, biometric data regarding the user is electronically collected.

Abstract

A computer-implemented method and system for verifying the identity of a user in an identity authentication and biometric verification system which includes collecting information from the user regarding the user's identity, which is then electronically authenticated. Upon authentication, personal information regarding the verified identity of the user is retrieved from a source database which is used to verify the identity of the user, via user interaction. Upon successful verification and authentication, biometric data regarding the user is electronically collected.

SYSTEM AND METHOD FOR USER ENROLLMENT IN A SECURE BIOMETRIC VERIFICATION SYSTEM

CROSS REFERENCE TO RELATED APPLICATIONS

This application claims priority to U.S. Patent Application Serial No. 61/502,453 filed June 29, 2011, which is incorporated herein by reference in its entirety.

FIELD OF THE INVENTION

The invention relates generally to a biometric verification system, and more specifically to a method and system for authenticating a user's identity.

BACKGROUND OF THE INVENTION

The present invention generally pertains to identity verification systems. More specifically, the present invention pertains to biometric security systems that provide an enhanced defense against fraudulent use of an individual's identity to complete a transaction.

Within a typical biometric security system, there are at least two operations, enrollment and verification. The operation of enrollment encompasses the original sampling of a person's biographic and biometric information, confirmation of the identity and its owner, and the creation and storage of a biometric template associated with the identity (a.k.a., an enrollment template) that is a data representation of the original sampling. The operation of verification includes an invocation of a biometric sample for the identification of a system user through comparison of a data representation of the biometric sample with one or more stored enrollment templates.

Biometric information is, by nature, reasonably public knowledge. A person's biometric data is often casually left behind or is easily seen and captured. This is true for all forms of biometric data including, but not limited to, fingerprints, iris features, facial features, and voice information. As an example, consider two friends meeting. The one friend recognizes the other by their face and other visible key characteristics. That information is public knowledge. However, a photo of that same person 'is' not that person. This issue similarly applies, electronically, to computer-based biometric authentication wherein a copy of authorized biometric information is susceptible to being submitted as a representation of the corresponding original information. In the context of biometric security applications, what is important, what enables a secure verification, is a unique and trusted invocation of an authorized biometric.

SUMMARY OF THE INVENTION

The purpose and advantages of the invention will be set forth in and apparent from the description that follows. Additional advantages of the invention will be realized and attained by the devices, systems and methods particularly pointed out in the written description and claims hereof, as well as from the appended drawings.

To achieve these and other advantages and in accordance with the purpose of the invention, as embodied, the invention includes in one aspect a computer-implemented method for verifying the identity of a user in an identity authentication and biometric verification system. The method includes collecting information from the user regarding the user's identity (such as a passport), which is then electronically authenticated. Upon authentication, personal information regarding the verified identity of the user is retrieved from a source database, which is used to verify the user, via user interaction. Upon successful verification and authentication, biometric data regarding the user is electronically collected and matched to the personal information retrieved from the source database. Another aspect of the invention may include the functionality to perform scoring or qualification screening as well as providing a user with a token on a smart card device or via a cardless system.

In a further illustrated aspect of the invention, provided is an authentication and biometric verification system adapted to electronically couple to at least one electronic source database for authenticating the identity of a user. The system preferably includes a central processing system configured to receive information regarding the identity of a user and verifying the identity of the user based upon the received information. Upon successful verification, the central processing system is further configured to retrieve from at least one electronic source database information relating to the user verified identity to authenticate a user's identity via interaction with the user applicant. Further provided is a biometric collection device electronically coupled to the central processing system adapted and configured to collect biometric data from a user applicant upon successful authentication of the user applicant. A payload processor component is further preferably provided and electronically coupled to the central processing system adapted and configured to convert the collected user applicant biometric information into an electronic payload.

BRIEF DESCRIPTION OF THE DRAWINGS

The objects and features of the invention can be understood with reference to the following detailed description of an illustrative embodiment of the present invention taken together in conjunction with the accompanying drawings in which:

FIG. 1 is a system level diagram of a computering environment used by the present invention;

FIG. 2 is a system level diagram of components of the present invention in accordance with an illustrated embodiment; and

FIGS. 3 and 4 are flow charts depicting operation of the present invention in accordance with the illustrated embodiment of FIG. 2.

WRITTEN DESCRIPTION OF CERTAIN EMBODIMENTS OF THE INVENTION

The present invention is now described more fully with reference to the accompanying drawings, in which an illustrated embodiment of the present invention is shown. The present invention is not limited in any way to the illustrated embodiment as the illustrated embodiment described below is merely exemplary of the invention, which can be embodied in various forms, as appreciated by one skilled in the art. Therefore, it is to be understood that any structural and functional details disclosed herein are not to be interpreted as limiting, but merely as a basis for the claims and as a representative for teaching one skilled in the art to variously employ the present invention. Furthermore, the terms and phrases used herein are not intended to be limiting but rather to provide an understandable description of the invention.

It is to be appreciated that the embodiments of this invention as discussed below preferably include software algorithms, programs, and/or code residing on computer useable medium having control logic for enabling execution on a machine having a computer processor. The machine typically includes memory storage configured to provide output from execution of the computer algorithm or program. Where a range of values is provided, it is understood that each intervening value, to the tenth of the unit of the lower limit unless the context clearly dictates otherwise, between the upper and lower limit of that range and any other stated or intervening value in that stated range is encompassed within the invention. The upper and lower limits of these smaller ranges is also encompassed within the invention, subject to any specifically excluded limit in the stated range. Where the stated range includes one or both of the limits, ranges excluding either or both of those included limits are also included in the invention.

Unless defined otherwise, all technical and scientific terms used herein have the same meaning as commonly understood by one of ordinary skill in the art to which this invention belongs. Although any methods and materials similar or equivalent to those described herein can also be used in the practice or testing of the present invention, exemplary methods and materials are now described. All publications mentioned herein are incorporated herein by reference to disclose and describe the methods and/or materials in connection with which the publications are cited.

It must be noted that as used herein and in the appended claims, the singular forms "a", "an," and "the" include plural referents unless the context clearly dictates otherwise. Thus, for example, reference to "a stimulus" includes a plurality of such stimuli and reference to "the signal" includes reference to one or more signals and equivalents thereof known to those skilled in the art, and so forth.

Turning now descriptively to the drawings, in which similar reference characters denote similar elements throughout the several views, Fig. 1 depicts an exemplary general-purpose computing system in which illustrated embodiments of the present invention may be implemented.

A generalized computering embodiment in which the present invention can be realized is depicted in FIG. 1 illustrating a processing system 100 which generally comprises at least one processor 102, or processing unit or plurality of processors, memory 104, at least one input device 106 and at least one output device 108, coupled together via a bus or group of buses 110. In certain embodiments, input device 106 and output device 108 could be the same device. An interface 112 can also be provided for coupling the processing system 100 to one or more peripheral devices, for example interface 112 could be a PCI card or PC card. At least one storage device 114, which houses at least one database 116 can also be provided. The memory

104 can be any form of memory device, for example, volatile or non-volatile memory, solid state storage devices, magnetic devices, etc. The processor 102 could comprise more than one distinct processing device, for example to handle different functions within the processing system 100. Input device 106 receives input data 118 and can comprise, for example, a keyboard, a pointer device such as a pen-like device or a mouse, audio receiving device for voice controlled activation such as a microphone, data receiver or antenna such as a modem or wireless data adaptor, data acquisition card, etc. Input data 118 could come from different sources, for example keyboard instructions in conjunction with data received via a network. Output device 108 produces or generates output data 120 and can comprise, for example, a display device or monitor in which case output data 120 is visual, a printer in which case output data 120 is printed, a port for example a USB port, a peripheral component adaptor, a data transmitter or antenna such as a modem or wireless network adaptor, etc. Output data 120 could be distinct and derived from different output devices, for example a visual display on a monitor in conjunction with data transmitted to a network. A user could view data output, or an interpretation of the data output, on, for example, a monitor or using a printer. The storage device 114 can be any form of data or information storage means, for example, volatile or non-volatile memory, solid state storage devices, magnetic devices, etc.

In use, the processing system 100 is adapted to allow data or information to be stored in and/or retrieved from, via wired or wireless communication means, at least one database 116. The interface 112 may allow wired and/or wireless communication between the processing unit 102 and peripheral components that may serve a specialized purpose. Preferably, the processor 102 receives instructions as input data 118 via input device 106 and can display processed results or other output to a user by utilizing output device 108. More than one input device 106 and/or output device 108 can be provided. It should be appreciated that the processing system 100 may be any form of terminal, server, specialized hardware, or the like.

It is to be appreciated that the processing system 100 may be a part of a networked communications system. Processing system 100 could connect to a network, for example the Internet or a WAN. Input data 118 and output data 120 could be communicated to other devices via the network. The transfer of information and/or data over the network can be achieved using wired communications means or wireless communications means. A server can facilitate the transfer of data between the network and one or more databases. A server and one or more databases provide an example of an information source.

Thus, the processing computing system environment 100 illustrated in FTG. 1 may operate in a networked environment using logical connections to one or more remote computers. The remote computer may be a personal computer, a server, a router, a network PC, a peer device, or other common network node, and typically includes many or all of the elements described above.

It is to be further appreciated that the logical connections depicted in FTG. 1 include a local area network (LAN) and a wide area network (WAN), but may also include other networks such as a personal area network (PAN). Such networking environments are commonplace in offices, enterprise-wide computer networks, intranets, and the Internet. For instance, when used in a LAN networking environment, the computing system environment 100 is connected to the LAN through a network interface or adapter. When used in a WAN networking environment, the computing system environment typically includes a modem or other means for establishing communications over the WAN, such as the Internet. The modem, which may be internal or external, may be connected to a system bus via a user input interface, or via another appropriate mechanism. In a networked environment, program modules depicted relative to the computing system environment 100, or portions thereof, may be stored in a remote memory storage device. It is to be appreciated that the illustrated network connections of FIG. 1 are exemplary and other means of establishing a communications link between multiple computers may be used.

FIG. 1 is intended to provide a brief, general description of an illustrative and/or suitable exemplary environment in which embodiments of the below described present invention may be implemented. FIG. 1 is an example of a suitable environment and is not intended to suggest any limitation as to the structure, scope of use, or functionality of an embodiment of the present invention. A particular environment should not be interpreted as having any dependency or requirement relating to any one or combination of components illustrated in an exemplary operating environment. For example, in certain instances, one or more elements of an environment may be deemed not necessary and omitted. In other instances, one or more other elements may be deemed necessary and added.

In the description that follows, certain embodiments may be described with reference to acts and symbolic representations of operations that are performed by one or more computing devices, such as the computing system environment 100 of FIG. 1. As such, it will be understood that such acts and operations, which are at times referred to as being computer-executed, include the manipulation by the processor of the computer of electrical signals representing data in a structured form. This manipulation transforms the data or maintains them at locations in the memory system of the computer, which reconfigures or otherwise alters the operation of the computer in a manner understood by those skilled in the art. The data structures in which data is maintained are physical locations of the memory that have particular properties defined by the format of the data. However, while an embodiment is being described in the foregoing context, it is not meant to be limiting as those of skill in the art will appreciate that the acts and operations described hereinafter may also be implemented in hardware.

Embodiments may be implemented with numerous other general-purpose or special-purpose computing devices and computing system environments or configurations. Examples of well-known computing systems, environments, and configurations that may be suitable for use with an embodiment include, but are not limited to, personal computers, handheld or laptop devices, tablet devices, personal digital assistants, multiprocessor systems, microprocessor-based systems, set top boxes, programmable consumer electronics, network, minicomputers, server computers, game server computers, web server computers, mainframe computers, and distributed computing environments that include any of the above systems or devices.

Embodiments may be described in a general context of computer-executable instructions, such as program modules, being executed by a computer. Generally, program modules include routines, programs, objects, components, data structures, etc., that perform particular tasks or implement particular abstract data types. An embodiment may also be practiced in a distributed computing environment where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote computer storage media including memory storage devices.

With the exemplary computing system environment 100 of FIG. 1 being generally shown and discussed above, reference is now made to FIG. 2 which depicts an illustrated embodiment of the system of the present invention, designated generally by reference numeral 200. With regards to system architecture 200, system 200 is to be understood to consist of two primary data processing environments: (i) a backend environment, which is generally a processing system and a database of records, and (ii) a customer service environment, which preferably contains only a subset of data required to service users 290 and applicant users on a day-to-day basis. As depicted in the illustrated embodiment of FIG. 2, all connections and interactions between the systems are understood to be handled through encrypted methods such as secure internet connections ("SSL"), virtual private networks ("VPN") and any other similar known, or unknown methods. Additionally firewalls may be used for added security protection. It is to be understood, in accordance with the illustrated embodiments, data in transit is preferably encrypted at all times.

In accordance with the illustrated embodiment of FIG. 2, system 200 preferably includes a central processing system 210 (preferably encompassing components of computering system 100) operative and configured to manage and protect the biographic and biometric information used to provision the services of the system 200 to Users 290 and "Benefit Providers". It is to be understood and appreciated the term "Benefit Providers", for purposes of the present invention, is to be understood to mean organizations that leverage the verification process described herein to confirm user identity in order to provide a product or service to a User 290. For example, CLEAR® is a service provider approved by the Transportation Security Administration (TSA) that performs biometric verification in order to provide the benefit of bypassing the traditional TSA Travel Document Checker (TDC). As discussed further below, central processing system 210 is preferably adapted and configured to communicate with third party data sources having information relevant, and preferably personal, to a user 290 so as to authenticate the user. An example of such a third party data source includes, but is not limited to, LexisNexis, and other similar data sources.

Central processing system 210 is electronically coupled to a pay load processor system 220, a card production system 230 and member management system 240, each preferably encompassing components of computering system 100. Briefly, payload processor system 220 is operative and configured to convert User 290 biographic and biometric information into an electronic payload that can be loaded onto a smart card or other identity confirmation token for use in verification processes. Card production system 230 is operative and configured to create smart cards or other tokens containing the User 290 payload. And member management system 240 is operative and configured to manage User 290 information and transactions such as biographic data updates (change of address, phone number, email, etc...) as well as billing information and transactions. The member management system 240 may also provide information regarding usage and benefits.

It is to be appreciated and understood by one skilled in the art, the central processing system 210 is configured and operative to transmit data with each of the payload processor system 220, the card production system 230 and member management system 240 through any known suitable means. In the illustrated embodiment of FIG. 2, an encrypted transmission method such as Secure File Transfer Protocol (SFTP) or Secure Socket Layer (SSL) (242, 244, 246) is employed to transmit data between the central processing system 210, the payload processing system 220, the card production system 230, and the member management system 240. While the illustrated embodiment of the invention depicts a cryptographic Secure Sockets Layer (SSL) 246 to transmit data between the central processing system and the member management system 240 (the SSL 246 is to be understood to be only an exemplary method for transmitting data as any suitable method may be utilized).

In accordance with the illustrated embodiment of FIG. 2, system 200 further includes a plurality of kiosk devices 250 disposed in differing geographic locations (such as airports, but not limited thereto) for enabling enrollment and identity verification, as discussed further below. For the purposes of the present invention, each kiosk device 250 is to be understood to be an electronic kiosk (or computer kiosk or interactive kiosk) housing a computer terminal preferably employing software configured to enable the required user 290 enrollment and verification functionality while preventing users 290 from accessing system functions. It is to be appreciated and understood each computerized kiosk 250 communicates with the central processing system 210. Each kiosk 250 may be configured and operational to include biometric capture devices (such as fingerprint and/or iris capture devices, camera(s), card readers(s), trackballs, computer keyboards, pushbuttons and other typical input devices associated with interactive computer kiosks).

It is to be appreciated and understood by one skilled in the art, each kiosk 250 electronically communicates with the central processing system 210 using any known and suitable secure electronic method. In the illustrated embodiment of FIG. 2, a Virtual Private Network (VPN) link 248 is established between each kiosk 250 and the central processing system 210, preferably through a firewall 246. Input devices that communicate with the kiosk 250 can be physically attached to the kiosk 250 or remotely communicating with the kiosk 250 to provide the information needed to perform enrollment or verification functions.

To aid the enrollment process, system 200 is further configured and operative to couple to third party computering devices 260 accessible by a user 290 for enrollment purposes, as further explained below. It is to be appreciated and understood by one skilled in the art, each third party computering device 260 (e.g., a desktop or laptop computer, tablet device, smart phone, etc.) electronically communicates with the member management system 240 using any known and suitable secure electronic method. In the illustrated embodiment of FIG. 2, each third party computering device 260 electronically communicates with the member management system 240 via an internet Secure Sockets Layer (SSL) connection 262, preferably through a firewall 264.

It is to be appreciated and understood system 200 is preferably operative and configured to maintain remote monitoring capability of its field located kiosks 250 whereby monitoring and measuring of system performance and metrics will provide the information necessary for system 200 to continually evaluate the performance and effectiveness of all components of system 200. It is to be further appreciated and understood, data relating to an applicant, member, and/or potential member 290 is not to be stored locally at a kiosk 250. That is, no personally identifiable information is stored in kiosks 250 or any other field storage devices associated with system 200 (e.g., laptops). Additionally, it is to be understood and appreciated, system 200 utilizes the aforesaid encryption such as SFTP, SSL, and VPN connections, along with protection by Firewalls, to ensure the security of data in system 200.

With the system 200 in accordance with the illustrated embodiments of FIGS. 1 and 2 being described above, its method and process of operation will now be described in accordance with the illustrated diagrams of FIGS. 3 and 4 (with continuing reference to FIGS. 1 and 2). First, with reference to FIG. 3 an exemplary enrollment process for an applicant user 290 with system 200 will be described.

Starting at step 310, a user first preferably provides the appropriate enrollment payment information and user background/demographic information to system 200. This information is preferably input to the member management system 240. It is to be appreciated this information may be input to the member management system 240 from a user, via a user computering device 260 or a system kiosk 250 as illustrated in FIG. 2. In particular, the user computering device 260 preferably couples to the member management system 240 using an internet address coupling (e.g., www.clearme.com), which coupling is preferably an SSL internet 262 coupled connection, through firewall(s) 264, providing a secure and encrypted coupling.

Next, at step 320 the member management system 240 is configured and operative to store the aforesaid user payment and billing information along with the user's background and demographic information necessary for membership information and verification purposes. The remaining portion of the user 290 input information from step 310 is preferably transmitted to the central processing system 210. It is also to be appreciated that if a kiosk 250 is used for user enrollment purposes, the user's 290 input enrollment information is preferably transmitted to the central processing system 210, which in turns sends user billing/payment information and other appropriate membership information to the member management system 240 for storage therein.

Next, to complete the enrollment process, a user 290 is preferably present at a kiosk 250 (or user computering device 260) whereby the central processing system 210 is configured and operative to send user demographic information to the kiosk 250 the user is present at, preferably in real-time, so as to be authenticated by a user 290 preferably in the presence of a system attendant for user authentication (step 330). That is, this is the process whereby the user's identity is authenticated via data collected from external sources such as a passport, drivers license (and the like) and the successful completion of answers to questions which are specific to the user, as set forth above. Upon such user authentication, the kiosk 250 is preferably configured and operative to scan and authorize certain user documentation to authenticate the user 290 (step 340). For instance, each kiosk 250 may be configured and operative to only accept those forms of identification that Benefit Providers such as the TSA has deemed acceptable and that can be authenticated.

As an additional measure of security for verifying the identity of an enrolling user 290, system 200 is configured and operative to perform an authentication user test (step 330). As mentioned above, once the identity of the user applicant is authenticated (step 320), the central processing system 210 is preferably adapted and configured to communicate with a remote third party data source (e.g., Lexis Nexis) to retrieve data relevant and personal to the verified identity of the user applicant 290. This data (e.g., the amount of a mortgage or automobile payment), is used by central processing system 210 to authenticate the user applicant 290 so as to mitigate any instance of identity theft, as now discussed below.

In a preferred embodiment, the aforesaid retrieved authenticating data is utilized by system 200 to formulate a quiz/test using the aforesaid retrieved authenticating data (e.g., the amount of a mortgage payment). It is to be appreciated and understood the functionality of the aforesaid authentication user test (step 330) is to strengthen the individual authentication and enrollment requirements and further decrease an imposter's ability to enroll under an alias. For instance, a question presented may be the amount of the user' s monthly mortgage payment and/or identify the most recent user employers. Thus, with regards to the aforementioned authentication user test (step 330), system 200 has incorporated an additional step in the secure member enrollment process. That is, system 200 has made the successful "in-person" completion of an identity authentication test, (i.e. a personalized questionnaire populated by commercially available data) as an additional eligibility requirement. In one embodiment, the identity authentication test consists of posing applicants randomized questions plus an auxiliary question. To successfully complete the quiz, an applicant user 290 preferably answers a predetermined number of questions correctly during a limited time period while being observed by an enrollment specialist. If an applicant/user 290 does not properly respond to the randomized questions and successfully complete the quiz, the applicant/user 290 is preferably not permitted to complete the enrollment process.

Upon the successful authentication of the applicant user's 290 identity documents and the passing of the aforesaid identity authentication test (step 330), each kiosk 250 is additionally preferably configured and operative to collect user biometric information (e.g., fingerprints, retain/iris scan, facial image, voice and the like) (step 340).

The collected applicant/user 290 biometric information (step 340) is provided to the payload processor system 220 (step 360). Which payload processor system 220 formats a user 290 biometric template based upon the user' s collected biometric information (step 340) which is then sent to the central processing system 210 (step 350). The user 290 biometric template is then preferably sent from the central processing system 210 to the card production system 230 which produces a user identification token such as a smartcard having embedded or links to user biometric and biographic information using any known means (smart chip, magnetically or optically encoded information and the like) (step 360). The user identification token may then be issued to a user 290 for use thereof (step 370). It is to be understood and appreciated the invention is not to be understood to be limited to the use of such a user issued token residing on a smart card or like device but rather may encompass matching a user' s retrieved biometric information with that previously stored in system 200.

With reference now to FIG. 4, the process for user 290 use of the aforesaid user identification token will now be briefly discussed. Starting at step 410, an enrolled user 290 presents the user identification token to a kiosk 250 associated with a third party requiring identity verification of the user 290 (e.g., airport security, admittance to an event requiring heightened security, or to a merchant desiring to verify a client remitting payment using a credit card or other ACH type of payment). Next, the kiosk 250 is configured and operative to confirm a biometric match between biometric data stored for the user 290 on the user identification token or in the central processing system 210 and the matching biometric features of the user 290 collected at the time of verification (step 420). If there is a match, the user's identity is verified and authenticated (step 430).

As used herein, the term "software" is meant to be synonymous with any code or program that can be in a processor of a host computer, regardless of whether the implementation is in hardware, firmware or as a software computer product available on a disc, a memory storage device, or for download from a remote machine. The embodiments described herein include such software to implement the equations, relationships and algorithms described above. One skilled in the art will appreciate further features and advantages of the invention based on the above-described embodiments. Accordingly, the invention is not to be limited by what has been particularly shown and described, except as indicated by the appended claims. All publications and references cited herein are expressly incorporated herein by reference in their entirety.

Optional embodiments of the present invention may also be said to broadly consist in the parts, elements and features referred to or indicated herein, individually or collectively, in any or all combinations of two or more of the parts, elements or features, and wherein specific integers are mentioned herein which have known equivalents in the art to which the invention relates, such known equivalents are deemed to be incorporated herein as if individually set forth. For instance, while the above illustrated embodiments make reference to a user token dedicated for use of a user' s identification in an airport environment, other embodiments encompass using a token dedicated for another purpose such as a credit or debit card which incorporates the biometric authentication features mentioned above, along with the aforesaid secure enrollment process (FIG. 3).

The above presents a description of a best mode contemplated for carrying out the present invention identity authentication and biometric verification system and method, and of the manner and process of making and using the identity authentication and biometric verification system and method, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains to make and use these devices and methods. The present invention identity authentication and biometric verification system and method is, however, susceptible to modifications and alternative method steps from those discussed above that are fully equivalent. Consequently, the present invention identity authentication and biometric verification system and method is not limited to the particular embodiments disclosed. On the contrary, the present invention identity authentication and biometric verification system and method encompasses all modifications and alternative constructions and methods coming within the spirit and scope of the present invention.

The descriptions above and the accompanying drawings should be interpreted in the illustrative and not the limited sense. While the invention has been disclosed in connection with the preferred embodiment or embodiments thereof, it should be understood that there may be other embodiments which fall within the scope of the invention as defined by the following claims. Where a claim, if any, is expressed as a means or step for performing a specified function, it is intended that such claim be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof, including both structural equivalents and equivalent structures, material-based equivalents and equivalent materials, and act based equivalents and equivalent acts.

What is claimed is:

1. A biometric identification system, comprising:

at least one non-transitory storage medium that stores instructions; and

at least one processor that executes the instructions to:

receive input information regarding an identity of a person from an input component of an electronic device;

receive first document information from at least one second input component of the electronic device that scanned a first document associated with the identity of the person, the first document comprising at least one of a passport, a driver's license, a state identification, or a military identification;

receive second document information from the at least one second input component of the electronic device that scanned a second document associated with the identity of the person, the second document comprising a boarding pass;

electronically retrieve data source information relating to the identity of the person from at least one data source;

authenticate the identity of the person based on the input information, the first document information, the second document information, and the data source information;

upon authenticating the identity of the person, receive biometric data for the person electronically collected using a biometric capture device of the electronic device; and

upon confirming a biometric match between the biometric data and received biometric data from an airport security device, transmit an indication to the airport security device to admit the person.

2. The biometric identification system of claim 1, wherein the airport security device comprises an airport security checkpoint.

3. The biometric identification system of claim 1, wherein the airport security device comprises an airport boarding gate.

4. The biometric identification system of claim 1, wherein the biometric data comprises a facial image.

5. The biometric identification system of claim 1, wherein:

the biometric match is a first biometric match;

the received biometric data is first received biometric data;

the airport security device is a first airport security device;

the indication is a first indication; and

upon confirming a second biometric match between the biometric data and second received biometric data from a second airport security device after transmitting the first indication, the at least one processor transmits a second indication to the second airport security device to admit the person.

6. The biometric identification system of claim 5, wherein the first airport security device and the second airport security device are located at a same airport.

7. The biometric identification system of claim 1, wherein the electronic device and the airport security device are located at a same airport.

8. A biometric identification system, comprising:

at least one non-transitory storage medium that stores instructions; and

at least one processor that executes the instructions to:

receive input information regarding an identity of a person from at least one input component of an electronic device;

receive first document information from a first document associated with the identity of the person via the at least one input component of the electronic device, the first document comprising at least one of a passport, a driver's license, a state identification, or a military identification;

receive second document information from a second document associated with the identity of the person via the at least one input component of the electronic device, the second document comprising a boarding pass;

electronically retrieve data source information relating to the identity of the person from at least one data source;

authenticate the identity of the person based on the input information, the first document information, the second document information, and the data source information;

upon authenticating the identity of the person, receive biometric data for the person electronically collected using a biometric capture device of the electronic device; and

upon confirming a biometric match between the biometric data and received biometric data from an airport security device, transmit an indication to the airport security device to admit the person.

9. The biometric identification system of claim 8, wherein the biometric data comprises at least one of a fingerprint, a retina scan, an iris scan, a facial image, or a voice.

10. The biometric identification system of claim 8, wherein:

the biometric match is a first biometric match;

the received biometric data is first received biometric data;

the indication is a first indication; and

upon confirming a second biometric match between the biometric data and second received biometric data from a third party device, the at least one processor transmits a second indication to the third party device verifying the identity of the person.

11. The biometric identification system of claim 8, wherein the at least one processor verifies the first document information using the data source information.

12. The biometric identification system of claim 8, wherein the at least one processor verifies the first document information using the data source information.

13. The biometric identification system of claim 8, wherein the biometric capture device comprises a camera.

14. The biometric identification system of claim 8, wherein the biometric data comprises a biometric template formatted based upon biometric information collected by the biometric capture device.

15. A biometric identification system, comprising:

at least one non-transitory storage medium that stores instructions; and

at least one processor that executes the instructions to:

receive input information regarding an identity of a person from at least one input component of at least one electronic device;

receive first document information from a first document associated with the identity of the person via the at least one input component of the at least one electronic device, the first document comprising at least one of a passport, a driver's license, a state identification, or a military identification;

receive second document information from a second document associated with the identity of the person via the at least one input component of the at least one electronic device, the second document comprising a boarding pass;

electronically retrieve data source information relating to the identity of the person from at least one data source;

authenticate the identity of the person based on the input information, the first document information, the second document information, and the data source information;

upon authenticating the identity of the person, receive biometric data for the person electronically collected using a biometric capture device of the at least one electronic device; and

upon confirming a biometric match between the biometric data and received biometric data from an airport security device, transmit an indication to the airport security device to admit the person.

16. The biometric identification system of claim 15, wherein the at least one electronic device deletes the biometric data after the biometric data is received by the at least one processor.

17. The biometric identification system of claim 15, wherein the at least one electronic device comprises a third party computing device.

18. The biometric identification system of claim 15, wherein the at least one electronic device comprises a kiosk.

19. The biometric identification system of claim 15, wherein the biometric capture device comprises at least one of a fingerprint capture device, an iris capture device, or a camera.

20. The biometric identification system of claim 15, wherein the at least one electronic device does not store personally identifiable information for the person.

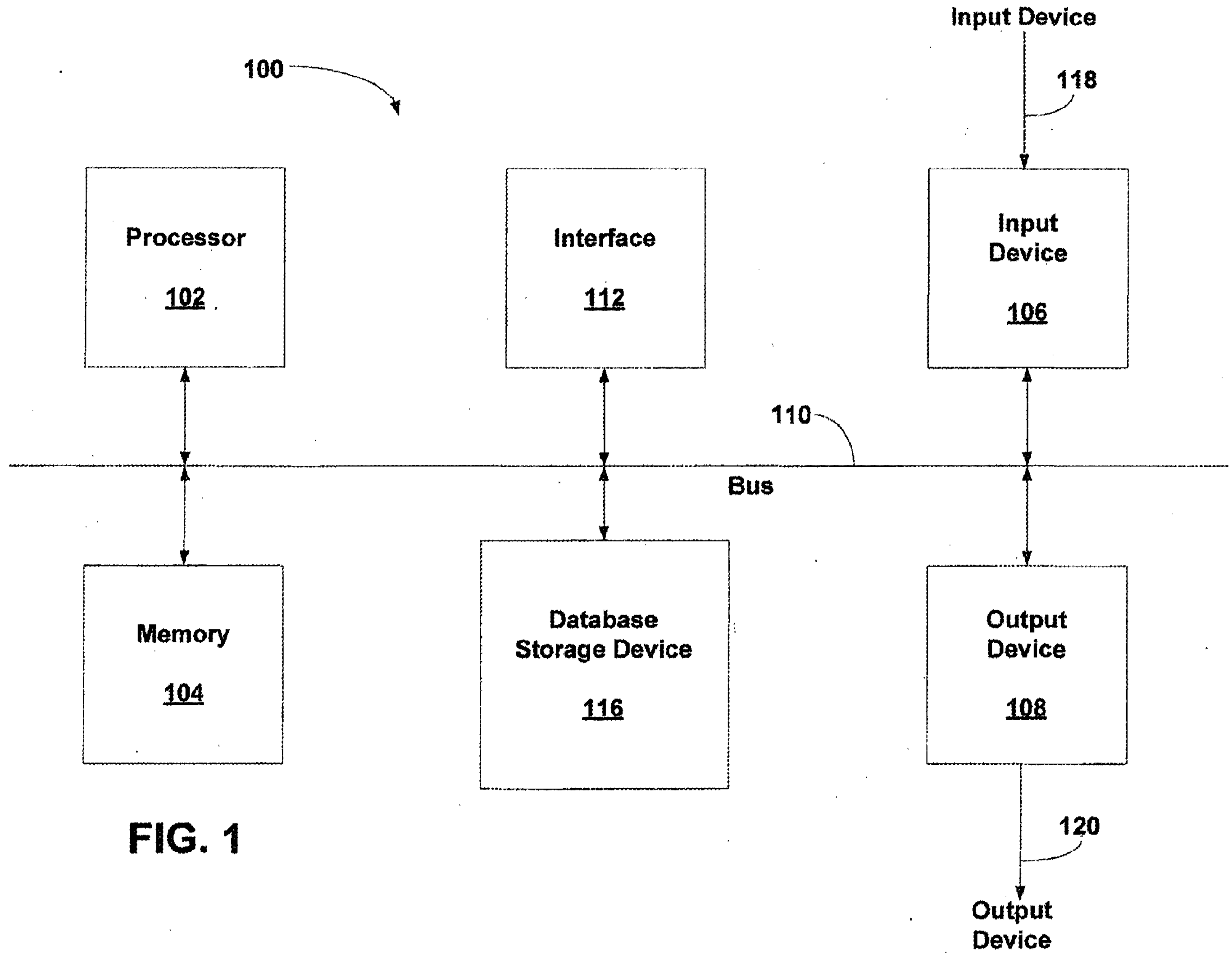

100
Input Device
118
Processor
102
Interface
112
Input
Device
106
110
Bus
Memory
104
Database
Storage Device
116
Output
Device
108
120
Output
Device

FIG. 1

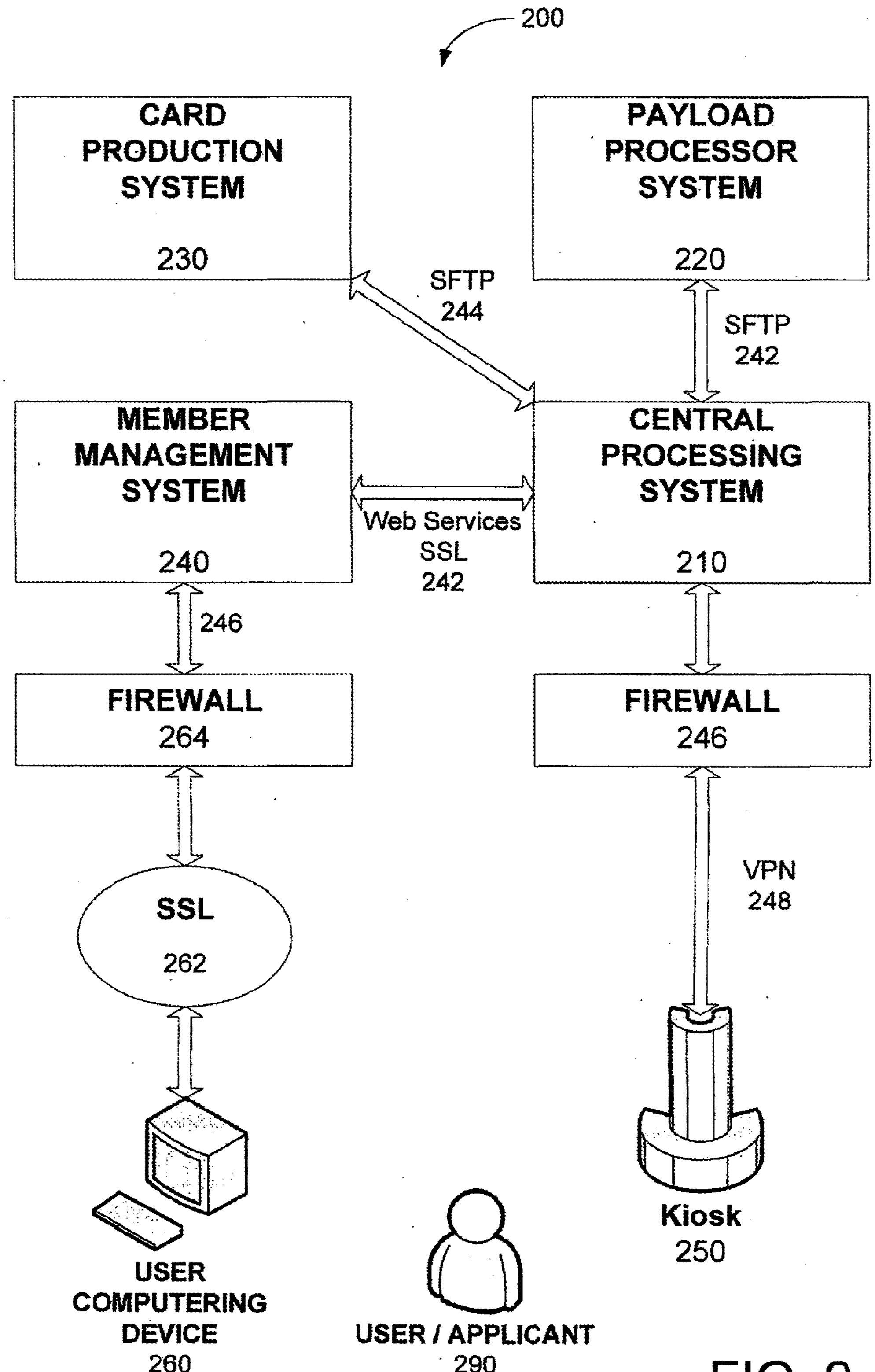

200
CARD PRODUCTION SYSTEM
230
PAYLOAD PROCESSOR SYSTEM
220
SFTP
244
SFTP
242
MEMBER MANAGEMENT SYSTEM
240
CENTRAL PROCESSING SYSTEM
210
Web Services
SSL
242
246
FIREWALL
264
FIREWALL
246
VPN
248
SSL
262
Kiosk
250
USER COMPUTERING DEVICE
260
USER / APPLICANT
290

FIG. 2

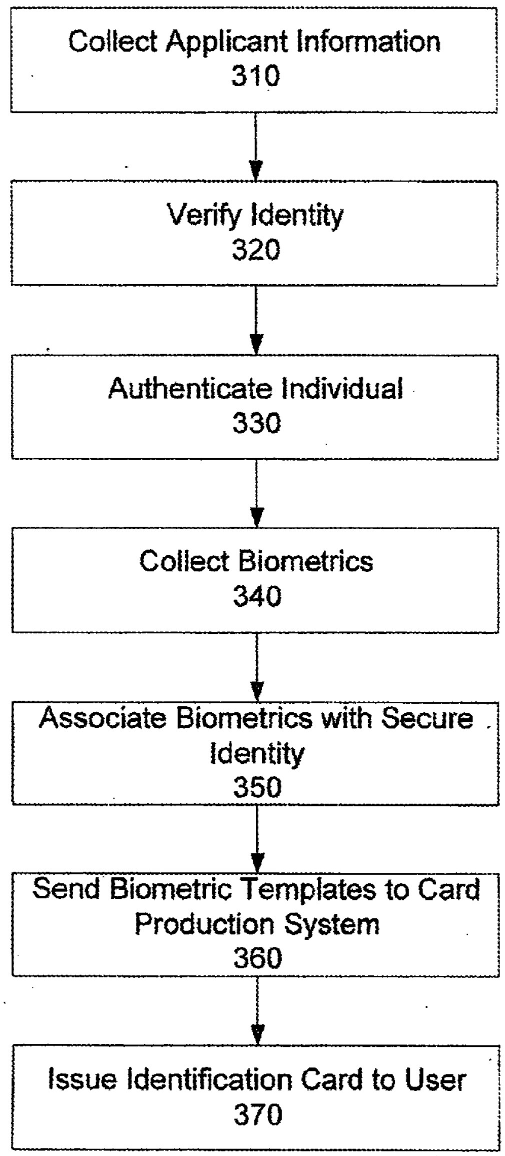

Collect Applicant Information
310
Verify Identity
320
Authenticate Individual
330
Collect Biometrics
340
Associate Biometrics with Secure Identity
350
Send Biometric Templates to Card Production System
360
Issue Identification Card to User
370

FIG. 3

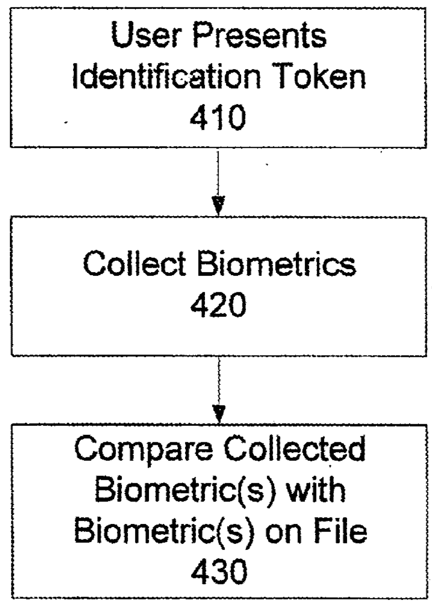

User Presents Identification Token
410
Collect Biometrics
420
Compare Collected Biometric(s) with Biometric(s) on File
430

FIG. 4

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 693 801 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
23.08.2006 Bulletin 2006/34

(51) Int Cl.:
G07C 9/00 $^{(2006.01)}$

(21) Application number: **06003192.9**

(22) Date of filing: **16.02.2006**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL BA HR MK YU

(30) Priority: **16.02.2005 US 653678 P**

(71) Applicants:
- **Schaufele, David**
  Parksville BC V9P A1A (CA)
- **Cihi, Guy**
  Saipan MP 96950 (US)

(72) Inventors:
- **Schaufele, David**
  Parksville BC V9P A1A (CA)
- **Cihi, Guy**
  Saipan MP 96950 (US)

(74) Representative: **Grünecker, Kinkeldey, Stockmair & Schwanhäusser Anwaltssozietät**
Maximilianstrasse 58
80538 München (DE)

(54) Biometric-based systems and methods for identity verification

(57) Biometric-based systems and corresponding methods for identity verification are disclosed herein. A security system in accordance with one embodiment of the invention can include an audio input module configured to receive and digitize a spoken utterance from a person and a video input module configured to receive multiple digital images of at least a portion of the person at least approximately contemporaneously with receiving the spoken utterance from the person. The security system can also include a first data processing module configured to receive the digitized spoken utterance and digital images of the person and correlate them together to form a biometric template for the person. The security system further includes a memory storing prerecorded audio and video data as individual templates of individual people and a second data processing module configured to receive the biometric template and compare it for a match with one of the stored templates of audio and video data.

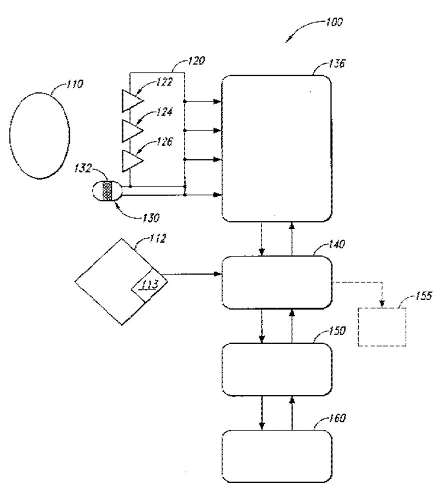


Fig. 1

EP 1 693 801 A2

Description

CROSS-REFERENCE TO RELATED APPLICATION(S)

[0001] This application claims the benefit of U.S. Provisional Application No. 60/653,678, filed February 16, 2005 (Attorney Docket No. 57295-8001 US).

TECHNICAL FIELD

[0002] The following disclosure relates generally to biometric-based systems and methods for identity verification and, more specifically, to biometric systems and corresponding methods for verifying an individual's identity, authenticating documents, and/or monitoring public health.

BACKGROUND

[0003] Biometrics is the science of using measurable biological properties to identify individuals. The use of biometric-based identification systems is becoming increasingly popular because such systems can provide substantially more security than many traditional security systems (e.g., usernames, passwords or personal identification numbers (PINs)). Biometric markers or templates used for personal identification can include, for example, measurements of unique visible features, such as fingerprints, hand and face geometry, and retinal and iris patterns, as well as the measurement of unique behavioral responses, such as the recognition of vocal patterns and the analysis of hand movements.

[0004] . Biometric-based systems generally require a device for measuring and recording the biological measurements in electronic form and comparing the measurements to a known value. Many conventional systems, for example, rely on digital imaging technologies. The raw biometric data of an individual's presumably unique features is obtained by a system including optics, a camera, and other electronic equipment configured to capture and digitize images. The digital representation of the images (i.e., the raw or unprocessed image data) is then processed by an algorithm that converts the image data into a particular representation (i.e., a biometric marker or template). The biometric marker or template is then compared with one or more previously stored values. If the values match within a desired level of accuracy, the person is identified and/or authorized.

[0005] Several types of technologies can be used for biometric identification of superficial anatomical traits. Biometric fingerprint identification systems, for example, generally require an individual under test to place his or her finger on a visual scanner. The scanner reflects light off of the person's finger and records the way the light is reflected off of the ridges that make up the fingerprint. Other systems can employ differing pressures or other means to "read" a person's fingerprint. Another example includes hand and face identification systems that use scanners and/or cameras to detect the relative anatomical structure, spacing, and/or geometry of a person's face or hand. Still another example is biometric authentication of an individual's eye. Retinal scans generally require a person to place his or her eye close to or upon a retinal scanning device. The scanning device then scans the retina to form an electronic version of the highly detailed, unique blood vessel pattern of the person's retina.

[0006] Other types of technologies can be used for biometric identification of behavioral traits. Voice recognition systems, for example, generally use a microphone or other suitable recording device to capture and record the voice pattern of an individual. The individual typically repeats a standard word or phrase and the biometric device compares the measured voice pattern to one or more voice patterns stored in the system. Still another example includes biometric signature authentication in which the verification process includes not only making a record of the contact pattern between the writing utensil and the recording device, but also measuring and recording the speed and/or pressure applied during the writing process.

[0007] There are a number of drawbacks with conventional biometric-based systems. For example, some hand recognition systems can require large, expensive scanners and expose individuals to health risks. Signature recognition systems can be susceptible to errors based on variations in an individual's behavior. Voice recognition systems have difficulty when a user has a cold and can be fooled by digital recordings. Retinal scans generally require expensive high-resolution, proprietary camera equipment and ideal lighting conditions. Moreover, many users may not be comfortable allowing a bright light to shine into their eyes. Retinal devices also generally require users to place their eyes close to or in contact with a scanning device, thus exposing the users to potential infections or other health risks. Furthermore, iris-recognition cameras generally require a significant amount of coordination for users to position their eyes properly for scanning and even small deviations can negatively affect the test results. Heavy make-up, facial hair, and poor lighting conditions can present difficulties for two-dimensional facial recognition systems, while cosmetic surgery can present difficulties for three-dimensional face recognition systems.

[0008] Still another drawback with many conventional systems is that searching large databases of biometric images can require substantial amounts of processing power, as well as causing a number of so-called "one to many" searches.

More specifically, some types of biometrics technologies can produce high numbers of false positives when the database size is very large. Large numbers of false positives, for example, can occur with large databases of facial images that are used with facial recognition systems because the systems are configured to simply match pixels between a photo and a digital photo taken on-site to verify an individual's identity.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] Figure 1 is a schematic illustration of a biometric-based identity verification system configured in accordance an embodiment of the invention.
[0010] Figure 2 is a partially schematic display diagram of a method for generating an audio recording portion of an individual's MBDS template in accordance with an embodiment of the invention.
[0011] Figures 3-5 are partially schematic isometric views of grids illustrating the three-dimensional nature of a MBDS template having an audio input and multiple video inputs captured synchronously over a selected time period.
[0012] Figures 6-8 are flow diagrams illustrating methods for using the biometric-based system of Figure 1 to control access to secure areas and/or secure systems in accordance with various embodiments of the invention.
[0013] Figure 9 is a display diagram of a voice spectrograph configured in accordance with another embodiment of the invention.

DETAILED DESCRIPTION

A. General Overview

[0014] The following disclosure relates generally to biometric-based systems and corresponding methods for identity verification. Embodiments of the invention, for example, include systems and methods for creating a unique biometric template (e.g., a multi-biometric data series (MBDS) template) having a particular combination of biometric data that can be widely utilized for personal identification and security verification. As used herein, an MBDS template or biometric template includes an individual's voice audio input captured synchronously and correlated with multiple video inputs over a selected time period (e.g., the time it takes an individual to state his or her name into a microphone and video camera). Voice recognition biometric data markers, when correlated with corresponding face recognition data markers, create a three-dimensional biometric template that has unique linear relationships between visual and vocal performance and, accordingly, can assist in positively identifying a particular individual.
[0015] The large number of unique biometric markers in each MBDS template can significantly improve the accuracy of personal identity verification as compared with conventional biometric systems that rely on a single or small number of unique markers. Additionally, the disclosed systems including MBDS templates can provide a significant decrease in statistical probability error as compared with many conventional systems. The number of data markers is inversely related to the verification error-as the number of markers increases, the potential error decreases. The low statistical probability of error associated with the disclosed systems is accordingly suitable for high security applications, as well as medium and low-security environments. Furthermore, verification errors can be reduced to the levels of other significantly more intrusive biometric-based security screening methods, such as iris or retinal scanning and time-consuming DNA analysis. Moreover, the disclosed systems require little or no physical contact and, therefore, present minimal health risk to the user.
[0016] Compared with conventional biometric-based systems that require expensive equipment and ideal testing conditions, embodiments of the invention can provide accurate results with less than ideal conditions and relatively inexpensive equipment. For example, low-resolution image recognition (unacceptable for iris or retina verification) can be combined with voice recognition to provide identification systems having a high degree of accuracy. Biometric features like eye-blinking, mouth position (i.e., open mouth, closed mouth, etc.), breathing patterns, and the timing associated with such behavioral habits provide unique data markers that can be tracked even with low-resolution video (e.g., bank machine kiosks or Web cams in which lighting may be less than ideal).
[0017] The biometric-based systems and methods described below can be used to control access to secure areas and various types of secure electronic devices and systems. For example, the disclosed systems and methods can prevent unauthorized access into secure areas such as airports, train stations, bus and ship terminals, public and private buildings, shopping complexes, and other desired areas. The biometric systems can also be used to prevent unauthorized access to a wide variety of electronic systems including, but not limited to, computer network systems, Web-based systems, automated transaction mechanisms, cellular phones, personal digital assistants, banking systems, and the like. The various biometric-based systems and methods can also be used to validate a number of different types of self-authenticating documents (e.g., passports, visas, etc.) that include machine-readable components for storing an individual's biometric data, electronic transmission systems (e.g., Internet, wireless, satellite, etc.), and other related systems. Furthermore, aspects of the invention can be used to help quickly identify potential public health risks and assist law

enforcement and health officials in implementing necessary procedures (e.g., quarantines, etc.).

[0018] Aspects of the invention can be characterized in a number of different ways. For example, one aspect can include a synchronous measurement of both audio and video input where an individual takes one or more of the following actions to facilitate the authentication process-

(a) states his or her full legal name (or a portion thereof) in any order and using any initial or word combination to create a digital signature or template containing a unique combination of personal biometric data;

(b) states his or her legal name several times (and in generally the same way) to create baseline template data with acceptable standard deviation tolerance, thus permitting natural human behavior variation and reliable identity verification;

(c) states a secret password following his or her legal name to provide variable security requirements suitable for corporate or military applications;

(d) states the name of one or more small children accompanying the individual to accommodate family members traveling with young children and help prevent child trafficking and kidnapping;

(e) speaks out loud in a unique way to create a MBDS template represented by a three dimensional vector reference containing coordinates (x, y, z) for each data marker, with z representing time as measured by seconds or frame numbers;

(f) follows instructions (either verbal or written) to provide a verifiable recording of biometric markers that can be used to authenticate machine-readable personal identification and verify on-site personal identity; and/or

(g) follows instructions (either verbal or written) to provide a verifiable recording of biometric markers that can be used to verify on-site personal identity and permit access to, or maintain access to, on-line services provided by Internet, intranet, LAN, and/or other suitable electronic networking systems.

[0019] Another aspect of the invention can include a synchronous measurement of both audio and video input in which an individual-

(a) who experiences difficulty using a worn out machine readable device (e.g., a security pass, national ID card, driver's license, passport, RFID tag, or the like) can still provide biometric input for comparison with a database reference file to receive identity verification and receive low-level clearance to a secure area;

(b) who forgot, lost, or had his or her personal identification stolen can still provide biometric input for comparison with a database reference file to receive identity verification and limited access to an automated ticket kiosk or bank machine; and/or

(c) who failed an initial background check can resubmit biometric input with both eyes closed while near-field infrared illumination is used to create a three-dimensional wire-frame projection grid animation, blood-vessel face-map image, and/or voice spectrograph image that can be compared individually or in combination with corporate, government, and/or law enforcement databases to provide identity verification for the individual.

[0020] Still another aspect of invention can include using an individual's biometric data (including both audio and video data measured synchronously) to-

(a) combine face recognition markers (captured during the period of time that it takes a person to clearly state his or her legal name) with corresponding voice recognition markers (recorded simultaneously during the same event) to create a three-dimensional data map or template/vector that is unique to each individual and store the biometric template on a database, machine-readable device (e.g., passport, driver's license, staff ID, national ID card, credit or bank card, PDA, CD, DVD, RFID, microchip implant, etc.), or another suitable storage medium;

(b) verify personal identity and/or authenticate a machine-readable device containing the individual's biometric data by matching the individual's baseline three-dimensional data map or template/vector with on-site biometric data measurements;

(c) verify an individual's identity through analysis using face recognition and voice recognition technology;

(d) provide baseline template and standard deviation records that are stored on at least one private security, corporate, government, military, or public law enforcement database;

(e) verify an individual's identity against at least one law enforcement or private security database; and/or

(f) verify a machine-readable device's authenticity against at least one law enforcement or private security database.

[0021] Yet another aspect of invention can include-

(a) updating an individual's reference file of previous biometric template/vector recordings (e.g., using old driver's license photos) to create a stronger baseline template and provide acceptable standard deviation tolerance parameters that can accommodate natural variations in human behavior and appearance;

(b) updating an individuals reference file of previous biometric template/vector recordings to create acceptable standard deviation parameters so that the symptoms of a common cold (e.g., sore throat, itchy eyes, runny nose, etc.) will not negatively affect identity verification; and/or

(c) updating an individual's reference file of previous biometric template/vector recordings to create acceptable standard deviation tolerance parameters so that alterations in visual appearance (e.g., a beard or mustache) will not significantly interfere with identity verification and other systems (e.g., infrared video face recognition and voice recognition) can take priority over color video face recognition during the verification analysis.

[0022] Still another aspect of invention can include using an individual's biometric data (including both audio and video data measured synchronously) to-

(a) verify data stored on an individual's machine-readable device (e.g., passport, driver's license, staff ID, national ID card, credit or bank card, PDA, CD, DVD, RFID, microchip implant, etc.) by matching (1) the device's stored biometric data with (2) on-site biometric data and, optionally, matching one or both of (1) and (2) with biometric data stored on a corporate, government, law enforcement, or military database;

(b) authenticate a physical key or portable communication device (e.g., cellular phone, PDA, etc.) and, upon positive identification, provide secure access to a computer network, Internet, database, Web site, or other types of electronic systems;

(c) purchase, issue, and/or validate an electronic ticket, voucher, debit card, or other type of financial instrument;

(d) permit secure financial, e-money, or other types of commercial transactions from a remote terminal; and/or

(e) permit low-level security clearance (e.g., limited access, entrance, or cash withdrawal in the event that the individual's machine-readable device is forgotten, lost, stolen or unavailable due to some unforeseen circumstance or unexpected emergency.

[0023] Still yet another aspect of the invention can include using an individual's biometric data (including both audio and video data measured synchronously) to control access to secure areas such as-

(a) schools or public gathering areas such as sports arenas, bus, train, or subway station/terminals, shopping complexes, domestic or international airports, military or civilian government areas, international borders, and transit facilities in between any of the above mentioned locations;

(b) automated banking machines, e-ticket kiosks, network terminals to educational, corporate, or military networks, and/or secure financial networks; and/or

(c) existing law enforcement infrastructure and associated facilities containing databases of personal identification, such as photographs, fingerprints, health records, or the like.

[0024] Further aspects of the invention be directed to the advantages associated with using multiple biometric data (such as the MBDS template) to positively identify an individual. Such advantages can include-

(a) the color video data benefits from face recognition technology to improve verification accuracy;

(b) the black & white video data benefits from face recognition technology to improve verification accuracy;

(c) passive infrared data benefits from technology to determine that a live person is presenting the secure biometric data to prevent fraud;

(d) passive infrared data benefits from technology to determine a possible health risk like SARS or Asian Bird Flu;

(e) near-field infrared illumination revealing surface blood vessel pattern data benefits from technology to determine a possible health risk and provides a significantly greater number of biometric markers for high security applications;

(f) near-field infrared illumination revealing three-dimensional facial characteristics that can be mapped over time to create a computer graphic simulation provide a significantly greater number of biometric markers for high security applications;

(g) the audio data benefits from speech recognition technology to improve verification accuracy;

(h) the audio data benefits from audio analysis technology to create a voice spectrograph to improve verification accuracy; and/or

(i) the audio data benefits from noise reduction or noise cancellation technology to facilitate applications in public areas where background noise is present to improve verification accuracy.

[0025] As described in detail below, embodiments of the invention can be used in a number of different environments and can include a number of different advantages. In several embodiments, for example, the system can be used at security checkpoints to compare an individual's baseline biometric data stored on a suitable machine-readable device (e.g., driver's license) with on-site measurements and law enforcement databases. Mobile checkpoints can also make use of some or all of the elements available to provide on-site identity verification. State-of-the-art audiovisual technology now facilitates wide application of high-speed data transmission for timely identity verification and document authentication. For example, wide-field scanning technology (e.g., Bluetooth, RFID, etc.) could recognize the order of machine-readable identification reference file numbers for users queuing in front of a security checkpoint, automated kiosk, or bank machine, and request each user's reference files in advance to speed up on-site verification of the MBDS templates.

[0026] Any standardized security system should not only meet the high standards expected of it, but also offer significant advantages to the public. By way of example, when a drink spills on a machine-readable student ID card during lunch break, a student is still able to attend classes and gain temporary on-line computer access in order to complete assignments. Application for and receipt of a new student ID card in exchange for the damaged one could be easily accomplished without delay. When an old security pass expires, staff can still gain limited entrance to facilities, fill out a request form, and be quickly issued a new security pass. When a security ID card begins to wear out and can no longer be verified, an employee could still gain access to his or her office and Intranet by entering a MBDS template at security checkpoints. Important work could continue in a timely manner while a request for a replacement security ID card is processed.

[0027] In another embodiment, the system can provide the day-to-day convenience of bank machine transactions even when one's bank card is forgotten at home, left in another wallet or purse, or otherwise misplaced. By entering a MBDS template and receiving low-level security clearance, for example, a mother shopping at a mall would still be able to withdraw a limited amount of money from the nearest bank machine without the inconvenience of having to return home to retrieve her bankcard or credit card. Another advantage of the system is that it may facilitate widespread acceptance of its use in an international security system suitable for the USVisit program.

[0028] In the event of an emergency (e.g., valuables and/or identification are lost or stolen) cash withdrawal, car rental reservation, and/or transportation ticket purchases could still be accomplished following successful identity verification by entering a MBDS template and receiving low-level security clearance. Business travelers would not become stranded as the result of a misfortune. Additionally, credit card company notification to cancel a lost or stolen card, and 911 emergency assistance (either medical or law enforcement in nature) could become programmed options available at automated ticket kiosks and bank machines that form an integral part of a national security system.

[0029] The MBDS template system can also be an important feature in an e-cash system. For example, many mobile devices (e.g., cellular phones, PDAs, etc.) can be interoperable with IC credit/debit cards, ATMs, and the like. One such feature can allow a user to "charge up" the phone with credit and then use the phone as a credit/debit instrument in financial transactions. In several applications, a credit/debit phone can be combined with the above-described MBDS template system and the resulting device could be configured to accept a user's MBDS input for verification before e-commerce features are activated or transactions take place. In the event the device was lost or stolen, it could not be used by anyone other than the owner. In other applications, the device could be used in a high volume transit system to allow passengers to pay fares without requiring the passengers to carry tokens or passes. Newer technologies like Bluetooth and WiFi allow a wider field of activation and could provide significant monitoring advantages in identity verification. In still further applications, credit/debit phones can be combined with the MBDS template system to perform a variety of other functions.

[0030] In one embodiment, automated kiosks can provide automated responses to assist the user. Another embodiment may include face-to-face communication with service personnel using the audio and video capabilities of the system. A company representative can review an unverifiable biometric input and explain directly to the user what the problem seems to be and suggest ways to improve the MBDS template recording (e.g., speaking louder, standing closer to the machine, not turning one's head to the side, etc.)

[0031] Another advantage of the features described herein is flexibility. In times of peace, for example, low-security requirements would facilitate normal movement of trade and industry. Citizens would go about their daily business knowing that a secure environment had been created through the use of a safe, reliable system for personal identification. When necessary, however, the security level of the system could be quickly increased in a prioritized, systematic way, without undue inconvenience to the public to provide an effective and efficient system of personal identification and infectious disease monitoring. Furthermore, if a possible health risk is detected, an automated Notification of Poor Health Condition (NPHC) could be issued to the user and directions to the nearest hospital or medical clinic open at that particular time of day or night could be provided.

[0032] Yet another advantage of the systems described herein is the ability of a user (even without a machine-readable device) to verify his or her personal identity and gain low-level security clearance by comparing a MBDS template recorded on-site with a MBDS template stored on file with a corporate, government, and/or law enforcement database. Although fast verification speed with a machine-readable device is generally desirable (due to the assistance provided by reference number or alphabetical search methods), the disclosed security systems can still provide identity verification without such a device. In some instances, the verification processes may take longer because the process requires more time for searching through various databases.

[0033] Still another advantage of the system is that secure Internet access can be accomplished without an ID card and can generally only require transmission of an individual's MBDS template data. An electronic authorization key or USB dongle is optional for users of secure financial systems.

[0034] Currently, many automated bank machines offer only a service telephone. In another embodiment of the system, an automated kiosk employing the MBDS template technology could provide face-to-face video conferencing with financial administrators at bank machines, sales representatives at ticket kiosks, emergency 911 operators, police, medical personnel, or the like.

[0035] In still another embodiment of the system, car rental might be refused after infrared video data and comparisons with healthy baseline data reveals significant physical changes to one's health (e.g., slurred speech or other symptoms of intoxication).

[0036] The MBDS template also provides an effective method of monitoring public health risks when incorporated into automated cash machines and entrances to public facilities. For example, the system could be configured to screen users for possible health risks like SARS or Asian Bird Flu through the use of passive and/or active infrared technology that measures body temperature. Elevated body temperature can be apparent in a person's face regardless of the ambient air temperature. This feature could help screen individuals for infectious disease like SARS, Asian Bird Flu, and the like, and prevent screened individuals from purchasing a passenger ticket for mass transit or entering pubic areas, thus helping control the spread of a contagion.

[0037] Low-level security applications might focus primarily on personal identification authentication and therefore not require the additional time required for verification with databases. Normal entrance to secure areas could be accomplished quickly by instantly verifying on-site MBDS template data and the template stored on a machine-readable device designed for identification, such as a company security pass or key card. For example, an employee who forgets his security ID pass would still be able to enter low-security areas by simply waiting a bit longer at the security checkpoint, while his MBDS template is verified against company databases.

[0038] Another advantage of the MBDS template system is flexible integration into everyday activities. For example, a mother could hold her child in her arms so that the child is visible in the wide angle camera view and then simply state the child's name following her own (e.g., "Jane Smith and John Jr."). This would make up an additional file stored on her machine-readable identification at the time it was issued. For example, a national ID card might contain such an additional file for the mother and all of her children individually. This would allow her to identify herself and one or more young children traveling with her.

[0039] Programs are now in place in the United States to encourage implanting microchips in children, to facilitate quickly locating them in case they become lost in a large shopping mall or suddenly go missing. While this may initially cause concern among some, others may choose to try and protect their children by increasing the surveillance tracking capability afforded by this new technology, especially in high crime areas. One of the first things a young child learns to say is his or her name and, accordingly, the disclosed systems may be suitable for use with student ID cards, RFID devices, and/or implantable microchip devices.

[0040] By way of example, each child participating in a school field trip to the zoo may be issued some form of machine-readable device (e.g., a student RFID in the form of a reusable wristband and including watch to facilitate prearranged meeting times). The device could also contain a microchip with the student's personal MBDS template file. The zoo could employ a low-level security system with high-speed verification to permit high volume visitor traffic. In this way, a teacher could monitor movement of students on a wireless handheld device similar to a PDA and be notified if one or more children attempt to leave the secure area.

[0041] The following description provides specific details for a thorough understanding of various embodiments of the invention. One skilled in the art will understand, however, that the invention may be practiced without many of these details. Additionally, some well-known structures or functions may not be shown or described in detail, so as to avoid unnecessarily obscuring the relevant description of the various embodiments.

[0042] The terminology used in the description presented below is intended to be interpreted in its broadest reasonable manner, even though it is being used in conjunction with a detailed description of certain specific embodiments of the invention. Certain terms may even be emphasized below; however, any terminology intended to be interpreted in any restricted manner will be overtly and specifically defined as such in this Detailed Description section.

[0043] Although not required, aspects and embodiments of the invention will be described in the general context of computer-executable instructions, such as routines executed by a general-purpose computer, e.g., a server or personal computer. Those skilled in the relevant art will appreciate that the invention can be practiced with other computer system configurations, including Internet appliances, hand-held devices, wearable computers, cellular or mobile phones, multi-processor systems, microprocessor-based or programmable consumer electronics, set-top boxes, network PCs, mini-computers, mainframe computers and the like. The invention can be embodied in a special purpose computer or data processor that is specifically programmed, configured or constructed to perform one or more of the computer-executable instructions explained in detail below. Indeed, the term "computer," as used generally herein, refers to any of the above devices, as well as any data processor.

[0044] The invention can also be practiced in distributed computing environments, where tasks or modules are performed by remote processing devices, which are linked through a communications network, such as a Local Area Network ("LAN"), Wide Area Network ("WAN") or the Internet. In a distributed computing environment, program modules or sub-routines may be located in both local and remote memory storage devices. Aspects of the invention described below may be stored or distributed on computer-readable media, including magnetic and optically readable and removable computer discs, stored as firmware in chips (e.g., EEPROM chips), as well as distributed electronically over the Internet or over other networks (including wireless networks). Those skilled in the relevant art will recognize that portions of the invention may reside on a server computer, while corresponding portions reside on a client computer. Data structures and transmission of data particular to aspects of the invention are also encompassed within the scope of the invention.

[0045] As used in this application, the terms "module" or "component" are intended to refer to a computer-related entity, either hardware, a combination of hardware and software, software, or software in execution, data processing or data storage and retrieval. For example, a module or component may be, but are not limited to being, a process running on a processor, a processor, an object, an executable, a thread of execution, a program, raw or processed digital data, a data template and a computer. By way of illustration, both an application running on a server, the data within the application and the server can be considered a module or component.

B. <u>Embodiments of Biometric-Based Identity Verification Systems and Methods for Using Such Systems</u>

[0046] Figure 1 is a schematic illustration of a biometric-based identity verification system 100 configured in accordance an embodiment of the invention. The system 100 can be used, for example, to control access to secure facilities or areas (e.g., transportation terminals, office buildings, government buildings, financial institutions, international borders, schools, sports arenas, etc.) or control activation of electronic systems (e.g., computer systems, ATMs, e-ticket kiosks, cellular systems, financial networks, communication systems, transportation systems, etc.). In still other embodiments, the system 100 can be configured to control access to different types of secure areas and/or secure systems. Although the below-described systems generally include only biometric-based characteristics as inputs, in other embodiments non-biometric based data can be used in conjunction with the biometric-based inputs to control access.

[0047] To begin the verification process, an individual 110 approaches the system 100 and presents a personal identification card 112 ("ID card 112"). The ID card 112 can include a driver's license, passport, national ID card, security pass, passbook, bank book, credit or bank card, PDA, CD, DVD, RFID, microchip implant, electronic ticket, or the like that includes machine-readable data 113 (e.g., the individuals biometric data). The data 113 from the ID card 112 can be input into a local security component 140 for verification using a number of different known input methods (e.g., card reader, barcode scanner, RFID, Bluetooth, etc). In embodiments where the individual's ID card 112 does not include machine-readable data 113, the desired information from the ID card 112 can be manually input into the local security component 140. In still other embodiments, the system 100 can be used to verify the individual's identity without the use of the ID card 112.

[0048] Either before or after presenting the ID card 112, the individual 110 can provide biometric input to a video input module 120 and an audio input module 130. The video input module 120 can include one or more sensors (three are shown) configured to capture image and video data from the individual 110. In the illustrated embodiment, for example, a first sensor 122 captures color video data, a second sensor 124 captures black & white video data, and a third sensor 126 captures infrared video data of the individual. The video data can include a number of different formats (e.g., NTSC, PAL, MPEG(2, 3, 4), SECAM, M-PAL, N-PAL, MESECAM, etc.). The sensors 122/124/126 can be part of the same digital camera or each sensor may be part of a different camera. In still other embodiments, the digital imaging unit 120 can include a different number of sensors to capture video data from the individual 110.

[0049] The audio input module 130 can include a microphone 132 or other suitable recording device configured to capture and process audio input from the individual 110. The audio data can include a number of different formats (e.g., WAV, AIFF, AU, WMA, Apple Lossless, MP3, AAC, etc.) As explained in greater detail below, the data from the three video sensors 122/124/126 and the data from the audio input module 130 is captured synchronously and combined to create a MBDS template 136 that includes at least four unique biometric data markers to verify and authenticate the individual's identity. Further details of the MBDS template 136 are described in greater detail below with respect to Figures 2-5.

[0050] The generated MBDS template 136 can be sent to the local security component 140 for processing and comparison with the data 113 from the individual's ID card 112. The MBDS template 136 can also be sent to one or more additional on-site and/or off-site systems for processing and verification. In the illustrated embodiment, for example, the MBDS template 136 can be sent to an off-site security component 150 and one or more corporate, government, and/or law enforcement databases 160 (e.g., FBI, Homeland Security, INS, local police, etc.) for additional verification. In this way, the individual's MBDS template 136 can be checked against a number of different known sources to further authenticate the individual's identity and confirm that the individual should be given access to the secure area or system. In embodiments where the system 100 is installed at an airport, the MBDS template 136 may optionally be sent to an airport security system 155 (shown in broken lines) for additional clearances (e.g., security checkpoint clearance, boarding gate clearance, no-fly lists, etc.) In other embodiments, the system 100 can include a different number of security components to verify the individual's MBDS template 136 and/or the MBDS template 136 can be compared with different types of databases.

[0051] If the individual's identity verification is successful and no security alerts appear after the MBDS template 136 is checked against the various databases, then local security component 140 provides an authorization message or alert to the individual 110 and the individual can gain entry to the secure area and/or access to the secure system.

[0052] By way of an example, if the system 100 is installed at an automated banking kiosk, a person desiring access to the kiosk approaches the kiosk and presents a personal identification card including machine-readable data (e.g., a credit card, bank debit card, or bank book). The person is then scanned by the digital video input 120 while he or she speaks into the digital audio input 130. The digital video and audio data are combined to create the person's MBDS template 136. The newly-created MBDS template 136 is compared against the person's MBDS template previously on record and, if the templates match, the person is authenticated. After authentication, the person can perform various banking functions, such as making a deposit, transferring money between accounts, withdrawing cash, etc. Figures 6-8 provide further details of methods for using the system 100 to control access to secure areas and/or secure systems.

[0053] Figure 2 is a partially schematic display diagram of a method 200 for generating an audio recording portion of an individual's MBDS template in accordance with an embodiment of the invention. The method 200 can be used, for example, with the audio input module 130 of the system 100 described above to record and process audio input from the individual 110. In other embodiments, however, the method 200 can be used with other suitable systems.

[0054] The method 200 begins during an initial period 202 with a voice prompt instructing a person wishing to gain access to a secure area or secure system to begin the process. The voice prompt, for example, can instruct the person to repeat a desired word or phrase into a microphone or other suitable recording device. The voice prompt can be activated automatically when the person moves into a specific area (i.e., motion activated), scans his or her ID card 112 (Figure 1), or takes another type of suitable action to activate the audio input process. In other embodiments, the audio input process can be activated by other suitable methods such as textual prompts or instructions to guide the person rather than voice prompts.

[0055] During a next period 204, the person provides a voice sample to calibrate the recording device. In the illustrated embodiment, for example, the person provides a first voice input 206 (e.g., "Hello" or another short phrase) into the microphone and a status signal 210 (e.g., a red light or other suitable visual or audio signal) indicates that the calibration process is in progress. The first voice input 206 provides a baseline voice signal level 212 for the audio recording process.

If the calibration process is unsuccessful (i.e., the signal level 212 is outside of desired ranges), a voice (or text) prompt instructs the person to adjust his or her positioning (e.g., move closer to the camera/microphone unit, adjust face positioning, speak with a louder voice, etc.) and the calibration process described above starts again. If the calibration process fails several times (e.g., three attempts), the method 200 can proceed based on the average signal level 212 calculated from the two closest first voice input results. In other embodiments, however, the calibration process may be aborted altogether after two or more failures.

[0056] During period 214, the status signal 210 indicates (e.g., with a yellow light) that a sound floor calibration is in process. The sound floor calibration measures and averages background signal levels 216 to create a sound floor level 218. The sound floor level 218 can be subtracted from the person's recorded audio input to help isolate the person's natural voice. One advantage of the sound floor calibration process is that creating the sound floor level can improve the rate at which the verification process is completed because the resulting recorded audio will not have to undergo extensive post-processing to remove background noise. Another advantage of the sound floor calibration process is that on-site background noise samples can improve security by providing a fail-safe that rejects the use of pre-recorded audio input (without such background noise) that may be presented to gain false access. In other embodiments, a number of different noise cancellation processes could be used in addition to, or in lieu of, the above-described sound floor calibration process. Suitable noise reduction or noise cancellation technology is commercially available from BOSE®, Dolby®, DBX®, and/or THX®.

[0057] The method 200 continues at period 220 where the status signal 210 indicates (e.g., with a green light) the start or "head" of the MBDS template recording. At the "head," an inhalation breath 222 typically occurs prior to the beginning of speech. The inhalation breath 222 (combined with corresponding face recognition and voice recognition markers) can form a unique biometric characteristic for the person under test. This particular characteristic, for example, can be used to index the person's resulting MBDS template within a database and help facilitate rapid searching of the database for the stored information.

[0058] The recording process continues at period 224 with the person providing a second voice input 226 (e.g., his or her given name) and a third voice input 228 (e.g., his or her family name) into the microphone. In the illustrated embodiment, for example, the person states "John" (i.e., the second voice input 226) and "Smith" (i.e., the third voice input 228) and each input is recorded. In other embodiments, the second and third voice inputs 226 and 228 can include different words/phrases and/or the recording process can include a different number of voice inputs. At period 230, the end or "tail" of the recording process (much like the "head") can be used to index the person's resulting MBDS template within a particular database. For example, the person may exhale, blink, or exhibit some other unique biometric characteristic after stating his or her name. These visual characteristics (in conjunction with the recorded audio input) can be used to index the person's MBDS template.

[0059] A frequent difficulty encountered with large database searches is distinguishing between individuals with the same or similar names. As such, the method 200 can include a number of features to help distinguish individual audio inputs. In one embodiment, for example, the process includes a five second recording window for the person to provide the second and third voice inputs 226 and 228 (along with video input recording about 150 frames at approximately 30 frames per second with standard digital video, or about 50-75 frames at about 10-15 frames per second via a Web cam). The five-second recording window allows the person enough time to state his or her full legal name and then, optionally, add a secret code word or another key word. Furthermore, systems incorporating the MBDS template could examine the head and tail section separately (when necessary) to help distinguish between individuals with the same or similar names, and rank them in order from most to least statistically probable before a direct comparison of the principal MBDS template is undertaken. Such features can improve searching efficiency and reduce false-positive and false-negative errors.

[0060] As discussed previously, the beginning or "head" of the recording generally includes an open mouth and silent breath before speech begins, and the end or "tail" generally includes a closed mouth, silent pause, and/or a blink of the eyes to relieve stress upon completion of the recording. Accordingly, in several embodiments the person's MBDS template can also include frame numbers corresponding with significant changes in biometric data markers that can be used to improve verification accuracy. For example, an individual's MBDS template could include the following notations: (frame 10, mouth open), (frame 30, speech begins), (frame 120, speech ends), (frame 130, mouth closed), (frame 140, eyes closed) (blink), (frame 145, eyes open). In other embodiments, however, the MBDS template can include different notations or the template may not include any notations.

[0061] The recorded audio input obtained during periods 220, 224, and 230 can then be processed and become part of the person's unique MBDS template 136 (Figure 1). At periods 232 and 234, the personal identity verification process and the document authentication process, respectively, can proceed with the person's recorded audio input (along with other visual and/or audio biometric markers) being compared against one or more previously-recorded biometric inputs. If verification is successful, at period 236 the person will be allowed access to the secure area and/or secure system. If the verification process is unsuccessful, however, the method 200 can be repeated one or more additional times before the process is aborted. In several embodiments, technical support can be provided (either via a live person or prerecorded instructions) to the person to help determine why the verification process failed (e.g., voice too quiet, bad positioning with respect to the microphone, physical damage to the person's ID card, etc.). Additionally, in some cases low security access can be possible following identity verification even in situations where the person does not have an ID card or the ID card is damaged.

[0062] Figures 3-5 are partially schematic isometric views of grids illustrating the three-dimensional nature of a MBDS template having an audio input and multiple video inputs captured synchronously over a selected time period. The illustrated grids include audio data (as described above with respect to Figure 2) combined with video data from the video input module 120 (Figure 1). Figure 3, for example, is a display diagram illustrating three consecutive frames (Frames 1-3) including data from four different biometric data markers (e.g., audio, color video, black & white video, and infrared video inputs) that can be used to create an individual's MBDS template.

[0063] The first data marker 300, for example, can include audio input that has been recorded and processed (e.g., using voice recognition software that examines and measures tonal changes in speech audio) to measure the various frequencies that make up the recorded audio. The resulting data can be represented as data elements 302 recorded at peaks and troughs in sound level and frequency. In the illustrated embodiment, for example, the recorded audio input can be processed to form a graphical representation of sound frequency and volume. This audio measurement technique is familiar and widely used for graphic equalizer displays on consumer audio equipment with narrow frequency bands lined up side by side and illuminated to indicate their respective levels.

[0064] The most common vocal frequencies in human speech are generally between 100 Hz and 2,500 Hz. Accordingly, frequency measurements would generally focus in the range of the human voice to exclude as much background noise as possible. Low-security applications (such as the embodiment illustrated in Figure 3) can employ twelve divisions of 200 Hz each, with frequency and volume recorded for each frame of corresponding video data. These inflection points plotted against time can reveal unique speech patterns that can be recognized even when audio quality is low. In medium or high security applications (such as the embodiments illustrated in Figures 4 and 5), further processing may be required to divide the audio spectrum into a greater number of divisions for greater accuracy. In other embodiments, a different number of divisions could be used. In still further embodiments, noise cancellation technology and other suitable audio processing applications can be included to improve accuracy and/or processing speed.

[0065] The second data marker 310 can include the digital color video input (e.g., from the first sensor 122 of the video input module 120 of Figure 1), the third data marker 320 can include the black & white video input (e.g., from the second sensor 124 of the video input module 120), and the fourth data marker 330 can include the infrared video input (e.g., from the third sensor 126 of the video input module 120). The resulting video data can be represented as multiple video data elements 340 arranged in a pattern generally corresponding to the captured images. The second data marker 310 (i.e., color video data) can be used primarily for face recognition, focusing in particular on the eyes, nose, and mouth spatial relationship. The third data marker 320 (i.e., black & white video data) can be used to increase resolution and improve face recognition verification speed. The fourth data marker 330 (i.e., infrared video data) can be used to improve verification accuracy in low light or nighttime environments, as well as evaluating the color temperature of cheeks and forehead to confirm that a living person is present and screen for possible health related diseases such as SARS. In several embodiments, face recognition technology may be used to further process the video data.

[0066] The MBDS templates combine measurements of frequency(x), volume(y), and frame number(z), to create the three-dimensional data matrix that plots all data markers using (x, y, z) coordinates. By way of example, a high-speed wireless or Internet Web cam generally records video at about 15 frames per second. If 12 audio data markers are captured per frame of video over a period of 5 seconds, the resulting MBDS template includes about 900 data markers. Furthermore, if low-resolution face recognition software tracks a minimum of 16 data markers locating eyes, nose, and mouth in each frame of digital video, the resulting MBDS template would include approximately 2100 unique biometric data markers. As discussed previously, such MBDS templates accordingly include an exponential increase in data markers over conventional biometric systems and, therefore, provide extremely accurate identity verification along with a corresponding exponential decrease in verification error. Furthermore, by using (x, y, z) coordinates to represent all data markers, this resulting MBDS templates are relatively small electronic files (e.g., a compressed RTF file can be about 4 kilobytes), which allows the MBDS templates to be stored on a number of different storage devices and/or transmitted quickly via the Internet, wireless devices, cellular phones, PDAs, etc. An advantage of this feature is that it can significantly improve verification speeds because the MBDS templates are small files that can be transferred quickly between on-site security components and off-site databases.

[0067] Figure 4 is a display diagram illustrating three consecutive frames (Frames 4-6) including data from the four biometric data markers (e.g., audio, color video, black & white video, and infrared video) that can be used to create an individual's MBDS template in accordance with another embodiment of the invention. The data markers in Figure 4 can be generally similar to the data markers described above with respect to Figure 3. The data markers in Figure 4 differ from those described above, however, in that the markers in Figure 4 include a larger number of data elements and, accordingly, can be used for applications requiring greater security. Frame 4, for example, illustrates a first data marker 400 (e.g., a full volume speech pattern) including multiple audio data elements 402 illustrating sound level and frequency (e.g., a full-volume speech pattern), and a second data marker 410, a third data marker 420, and a fourth data marker 430 including multiple video data elements 440 illustrating the person under test with his or her mouth and eyes open.

[0068] Frame 5 of Figure 4 illustrates a pause in speech (as demonstrated by the low sound level shown by the first data marker 400 and the person's blinking eyes shown in the second, third, and fourth data markers 410-430). This type of individual characteristic (i.e., the blinking) might occur naturally or could be incorporated intentionally by the person to create a unique template feature. In several embodiments, starting the MBDS template with one's mouth and eyes closed (as shown in Frame 5) can be a trigger (similar to a film's "timing slate") to activate face recognition software and thus improve verification speed.

[0069] Frame 6 of Figure 4 illustrates the beginning of speech with the person's mouth partially open (as shown in the second, third, and fourth data markers 410-430) and as indicated by the medium sound level of the first data marker 400. In several embodiments, this type of pattern may also be found randomly throughout each MBDS template and can provide a unique reference characteristic for the individual templates.

[0070] Figure 5 is a display diagram illustrating three consecutive frames (Frames 7-9) including the four biometric data markers (e.g., audio, color video, black & white video, and infrared video) that can be used to create an individual's MBDS template in accordance with still another embodiment of the invention. The data markers in Figure 5 differ from those described above with respect to Figures 3 and 4 in that the data markers include a significantly larger number of data elements and, accordingly, can be used for high-security applications. By increasing the number of data elements, the accuracy of the verification process can be improved while maintaining acceptable processing rates.

[0071] In one embodiment, for example, medium and/or high-level security verification processes can include 24 divisions of 100 Hz each, with frequency and volume recorded at 30 frames per second. Standard digital video (30 frames/second) x (24 audio data markers/frame) x (5 seconds) = 3,600 data markers. If standard resolution face recognition software tracks a minimum of 32 data markers locating eyes, nose and mouth in each frame of color digital video, approximately 4,800 markers would be recorded in an MBDS template, for a total of about 8,400 markers. If the black & white and infrared video inputs are combined as well, over 18,000 data markers would be contained in a single MBDS template with about 7,000 markers forming the head and tail sections of the recording and over 10,000 markers representing the main body of the MBDS template.

[0072] Frame 7, for example, illustrates an initial stage of the process showing a first data marker 500 (e.g., a full-volume speech pattern) including multiple audio data elements 502 and a second data marker 510, a third data marker 520, and a fourth data marker 530 including multiple video data elements 540 illustrating the person under test with his or her mouth and eyes open.

[0073] Frame 8 of Figure 5 illustrates a pause in the person's speech with a low sound level shown by the first data marker 500 and the person's single blinking eye shown in the second, third, and fourth data markers 510-530. This type of individual characteristic (i.e., blinking one eye) might occur naturally or could be incorporated intentionally by the person to create a unique template. For example, a person could start the recording process with his or her mouth and one (or both) eyes closed. In several embodiments, starting the MBDS template with one's mouth and one eye closed (as shown in Frame 8) can be a trigger (similar to a film's "timing slate") to activate face recognition software. Furthermore, an initial pause before beginning the recording process and the interval between blinking one's eyes and beginning to speak can provide a useful baseline measurement to reduce false positives. Moreover, the initial breath that is required before beginning to speak is also a unique biometric characteristic that can form the first "chapter" in the "table of contents" that make up an individual's MBDS template and may help speed up database comparison searches.

[0074] Figures 6-8 are flow diagrams illustrating methods for using the biometric-based systems described above with reference to Figures 1-5 control access to secure areas and/or secure systems in accordance with various embodiments of the invention. Figure 6, for example, is a flow diagram illustrating a method 600 for controlling access to secure areas in accordance with one embodiment of the invention. The method 600 can be used with the system 100 (Figure 1) to restrict access to a number of different types of secure areas (e.g., airports and other transportation terminals, public and private buildings, international borders, sports arenas, etc.) A typical security checkpoint, for example, can include a number of automated stations or kiosks that each include the system 100 to avoid congestion and allow greater movement of visitors, passengers, and/or or personnel. A number of partitions or other suitable dividers can be arranged between the individual stations to form a number of individual controlled areas, thus providing a degree of privacy and security between adjoining stations. In other embodiments, the stations can have a number of other arrangements relative to each other. In still other embodiments, the method 600 can be used to restrict access to a number of other types of secure areas. Furthermore, the method 600 can be used with other suitable systems in addition to, or in lieu of, the system 100.

[0075] In blocks 602, 604, and 606, the method begins with activation of the security system using any number of suitable activation methods (e.g., motion activation, RFID scanning activation by near-field scanning or wide-field scanning, voice activation, etc.). Upon activation, in block 608 a voice prompt instructs the person being identified (also referred to herein as the "user") to "Please begin now." In embodiments where the checkpoint is located at a transportation terminal, the voice prompts can also include instructions to the user regarding specific travel procedures, documents that need to be provided, etc. In block 610, a voice level calibration window (e.g., along with a corresponding visual signal, such as a red light) indicates that calibration is beginning and prompts the user to provide one or more spoken words (e.g., "Hello") so that the system can properly adjust the audio recording levels before the user begins the main audio input process.

[0076] In block 612, another visual signal (e.g., a yellow light) followed by an audio command (e.g., a recorded countdown, such as "3...2...1..." instructs the user that a sound floor calibration process is underway to create a sound floor level for the audio input. When the security checkpoint is used in medium and high-level security environments, the method 600 can include proceeding to block 614 and using this brief period of time where the user is facing the camera (generally with his or her mouth closed) to create a color and black & white "mug shot" photo or digital images. The captured images could then be forwarded to various law enforcement databases in block 616 for screening while the remaining steps of the identity verification process are completed. If any positive matches are found for the user during the database search, in block 618 a security alert can be issued for the user. One advantage of this feature is that it provides additional screening time for searching the databases because the other verification processes can proceed simultaneous with the searches. This can significantly reduce the amount of time required for verification of an individual user, while still providing an extensive and thorough search of relevant databases.

[0077] The method continues in block 620 with another visual signal (e.g., a green light) notifying the user that the recording process is beginning. The user can then state his or her name (e.g., "John Smith") or another phrase into a microphone or suitable recording device. In decision block 622, the method continues with verification of the user's identity and (if applicable) authentication of the user's documents based on the user's audio and visual inputs. As discussed in detail above with respect to Figures 3-5, for example, the user's audio input is correlated with a number of captured video images of the user to create a unique MBDS template for the user. The on-site MBDS template can be compared against one or more of the user's stored MBDS templates from the user's ID card and/or one or more external databases in block 624. If the information matches, the user's identity is verified.

[0078] In situations requiring only low-level security, on-site identity verification (where the user has an ID card including stored biometric information) could occur almost instantaneously and the method can proceed to block 626 where the system signals the user that verification was successful (e.g., provides the user with a verbal "Welcome" signal or another suitable signal) and the user is granted access to the secure area in block 628. In situations requiring medium or high-level security, however, a typical "Please wait a moment ..." verbal or written instruction can be provided to the user while the database search is conducted with corporate, government, and/or law enforcement databases. If the user's machine-readable ID card or device was successfully scanned at the initial stages of the method and the user's stored MBDS template was successfully retrieved from the card or device, then verification can proceed while the user is performing the other steps of the method and, accordingly, the verification process can be completed in a relatively short time.

[0079] If identity verification or device authentication failure occurs at decision block 622, the method continues in block 630 and reviews the failure to determine what went wrong. If the failure was due to problems with the audio or video inputs, for example, the method continues in block 632 with instructions to the user regarding adjustments to help correct the errors. The method then goes back to block 612 to begin the recording process again. In many cases, for example, speaking with a staff member can reassure users who are experiencing difficulties and/or adjusting to the new system and thereby help eliminate any such errors. Furthermore, in cases where the user's ID card or other machine-readable device is malfunctioning, the user can still be granted limited access to the secure area if the area is a low-security environment. If the process fails one or more additional times, the process can proceed to block 634 and a security alert can be issued and/or the user can be detained while security staff is summoned in block 636.

[0080] Figure 7 is a flow diagram illustrating a method 700 for controlling access to high-security areas in accordance with another embodiment of the invention. The method 700 can be generally similar to the method 600 described above. Accordingly, like reference numbers refer to similar features and/or processes in Figures 6 and 7. The method 700 differs from the method 600 in that a number of additional processes can be included (e.g., near-field infrared scanning of the user) to improve verification accuracy and screen users for potential public health risks.

[0081] For example, in block 714 the method 700 includes capturing not only the color and black & white images as described above with respect to method 600, but also including one or more additional biometric characteristics, such as a blood vessel face map (BVFM) created via infrared scanning, voice spectrograph data, and/or a three-dimensional mask image. In one embodiment, for example, a user's MBDS template could also include the user's voice spectrograph data, a BVFM, and a three-dimensional mask of the user. These additional biometric inputs could further improve the accuracy of the verification process and provide additional checks to help prevent fraud. For example, by increasing the number of audio and video data markers captured during the selected period of time (e.g., the five second window in which a user states his or her name), the verification accuracy of the MBDS template system can approach that of DNA testing without requiring intrusive tests and/or unreasonable delays. In other embodiments, a number of other biometric inputs can be used with the audio and video inputs.

[0082] In blocks 722 and 724, the method can include (in addition to the standard identity verification processes) checking the user's BVSM and/or three-dimensional mask against the user's previously-stored healthy baseline data to determine if the user poses a public health risk. In the event that a user is flagged for a possible health risk due to elevated facial temperature detected by passive infrared data, then one or more additional scans can be performed using the infrared sensor to confirm the health risk and provide the necessary information to facilitate rapid quarantine procedures. If analysis confirms that elevated facial skin temperature is symptomatic of a health-related concern (e.g., SARS), a security health alert can be issued in block 734 and the user can be denied access to the secure area while health guidance information is provided.

[0083] By way of example, a user who exhibits high body temperature when viewed by a passive infrared camera can be flagged as a possible health risk. Elevated skin temperature in the user's cheeks and forehead areas are generally a sign of illness because the body's defensive response generally includes elevated body temperature. On-site measurements (when compared with healthy baseline data) could provide early detection and confirmation of infectious disease like SARS or Asian Bird Flu. If a possible health risk is flagged or confirmed, a Notification of Poor Health Condition (NPHC) could be issued to the user and directions to the nearest hospital or medical clinic open at that particular time of day or night could be provided.

[0084] One advantage of the method 700 is that using such non-obtrusive methods to detect public health risks can isolate the risks at the earliest possible stage and provide the user with immediate communication with a health professional to dispense further. Furthermore, by recognizing that serious health risks are relatively rare occurrences, the invention can be configured to detect common health problems without causing undue inconvenience to the user. For example, a common cold or slight fever would not prevent the user from accessing the desired secure area, but an automated NPHC may still be issued to the user and the user could be given directions to the nearest hospital or medical clinic. A user suffering from flu symptoms or a high fever, however, may activate a health warning and, in some cases, be prevented from entering the secure area. Accordingly, monitoring user's health using the above-described systems and methods can represent the first line of defense in containment of many infectious diseases and help prevent an epidemic.

[0085] One feature of the above-described systems and corresponding methods is that verification accuracy can vary between different areas of a single installation, with different security requirements designed to minimize delay and inconvenience for users. By way of example, when the domestic terror alert is low, an airport security checkpoint can be configured to accept low-level security screening, with perhaps 95% verification (5% error) and requiring between about 2-5 seconds per person. At the airport entrance, a medium-level security checkpoint might accept 99% verification (1% error) with national law enforcement databases, requiring about 10-15 seconds per person while baggage is scanned. At the check-in counter, high-security might require 99.9% verification (0.1% error) and international background checks could take about 1-2 minutes while boarding passes and baggage tagging procedures are completed. Furthermore, extremely high-security environments including active infrared illumination biometric input could be employed to further increase verification accuracy (99.99% or 0.01% error) for air-traffic controllers and/or security staff.

[0086] Figure 8 is a flow diagram illustrating a method 800 for controlling access to a secure electronic system (e.g., a computer network system, a cellular system, a Web-based system, a personal digital assistant, a credit/debit ATM mobile phone, a financial network, etc.) in accordance with still another embodiment of the invention. The method 800 can be generally similar to the method 600 described above with reference to Figure 6. Accordingly, like reference numbers refer to similar features and/or processes in Figures 6 and 8. In block 802, a user activates the system (e.g., logs on to the Internet) and at block 804 a display prompt instructs the user to begin the verification process (e.g., audio instructions such as "Please begin now" or suitable textual instructions). The next steps of the method 800 are generally similar to the methods described above with respect to the method 600 except that a user generally does not need to provide an ID card or other device including machine-readable data to gain access to the electronic system. When access is granted (at block 626), the user is authorized to use the system.

[0087] Figure 9 is a display diagram of a voice spectrograph 900 configured in accordance with another embodiment of the invention. In the illustrated embodiment, for example, a person under test alternated breathing deeply with his or her chest 905 before exhaling, then breathed in again with his or her nose and chest 906 mixed before exhaling, then finally breathed deeply again using only the chest 907. The spectrograph 900 can include up to four different elements of measurement (e.g., elements 901, 902, 903 and 904), with each element representing a distinct characteristic helpful in identification. Voice analysis technology can create a sound spectrograph image for the MBDS template, thus graphically representing the audio portion of the template by measuring frequency and intensity (volume) over time. In this way, voice spectrograph data may help replace fingerprints as a less intrusive and generally more accurate biometric identification system.

Conclusion

[0088] Unless the context clearly requires otherwise, throughout the description and the claims, the words "comprise," "comprising," and the like are to be construed in an inclusive sense, as opposed to an exclusive or exhaustive sense;

that is to say, in the sense of "including, but not limited to." As used herein, the terms "connected," "coupled," or any variant thereof, means any connection or coupling, either direct or indirect, between two or more elements; the coupling of connection between the elements can be physical, logical, or a combination thereof. Additionally, the words "herein," "above," "below," and words of similar import, when used in this application, shall refer to this application as a whole and not to any particular portions of this application. Where the context permits, words in the above Detailed Description using the singular or plural number may also include the plural or singular number respectively. The word "or," in reference to a list of two or more items, covers all of the following interpretations of the word: any of the items in the list, all of the items in the list, and any combination of the items in the list.

[0089] The above detailed description of embodiments of the invention is not intended to be exhaustive or to limit the invention to the precise form disclosed above. While specific embodiments of, and examples for, the invention are described above for illustrative purposes, various equivalent modifications are possible within the scope of the invention, as those skilled in the relevant art will recognize. For example, while processes or blocks are presented in a given order, alternative embodiments may perform routines having steps, or employ systems having blocks, in a different order, and some processes or blocks may be deleted, moved, added, subdivided, combined, and/or modified to provide alternative or subcombinations. Each of these processes or blocks may be implemented in a variety of different ways. Also, while processes or blocks are at times shown as being performed in series, these processes or blocks may instead be performed in parallel, or may be performed at different times.

[0090] The teachings of the invention provided herein can be applied to other systems, not necessarily the system described above. The elements and acts of the various embodiments described above can be combined to provide further embodiments.

[0091] Any patents and applications and other references noted above, including any that may be listed in accompanying filing papers, are incorporated herein by reference. Aspects of the invention can be modified, if necessary, to employ the systems, functions, and concepts of the various references described above to provide yet further embodiments of the invention.

[0092] These and other changes can be made to the invention in light of the above Detailed Description. While the above description describes certain embodiments of the invention, and describes the best mode contemplated, no matter how detailed the above appears in text, the invention can be practiced in many ways. Details of the data collection and processing system may vary considerably in its implementation details, while still being encompassed by the invention disclosed herein. As noted above, particular terminology used when describing certain features or aspects of the invention should not be taken to imply that the terminology is being redefined herein to be restricted to any specific characteristics, features, or aspects of the invention with which that terminology is associated. In general, the terms used in the following claims should not be construed to limit the invention to the specific embodiments disclosed in the specification, unless the above Detailed Description section explicitly defines such terms. Accordingly, the actual scope of the invention encompasses not only the disclosed embodiments, but also all equivalent ways of practicing or implementing the invention under the claims.

[0093] While certain aspects of the invention are presented below in certain claim forms, the inventors contemplate the various aspects of the invention in any number of claim forms. For example, a number of aspects of the invention may be embodied in a computer-readable medium. Accordingly, the inventors reserve the right to add additional claims after filing the application to pursue such additional claim forms for other aspects of the invention.

Claims

1. A biometric-based security system, comprising:

an audio input module configured to receive and digitize a spoken utterance from a person;
a video input module configured to receive multiple digital images of at least a portion of the person at least approximately contemporaneously with receiving the spoken utterance from the person;
a first data processing module configured to receive the digitized spoken utterance and digital images of the person and correlate them together to form a biometric template for the person;
a memory storing prerecorded audio and video data as individual templates of individual people; and
a second data processing module configured to receive the biometric template and compare it for a match with one of the stored templates of audio and video data.

2. The security system of claim 1, further comprising a personal identification document having a memory for storing prerecorded audio and video data of the owner of the document as a personal document template, and wherein the second data processing module receives the personal document template from the personal identification document and compares it for a match with the person's biometric template and/or one of the stored templates of audio and video data to authenticate the personal identification document.

3. The security system of claim 2 wherein the personal identification document includes a driver's license, passport, national ID card, security pass, passbook, bank book, credit or bank card, PDA, CD, DVD, RFID, and/or microchip implant.

4. The security system of claim 1 wherein the video input module includes a color video sensor, a black & white video sensor, and an infrared video sensor.

5. The security system of claim 4 wherein:

   the color video sensor is configured to capture one or more digital images of the person's face;
   the black & white video sensor is configured to capture one or more digital image of the person's face; and
   the infrared video sensor is configured to capture one or more digital images of the person's skin surface blood vessels and/or skin temperature.

6. The security system of claim 4 wherein the infrared video sensor is configured to capture one or more digital images of the person's face to create a blood vessel face map and/or a three-dimensional mask image of the person's face.

7. The security system of claim 1 wherein:

   the multiple digital images of a person include a digital image of skin surface blood vessels and/or skin temperature;
   at least some of the individual templates of prerecorded audio and video data stored on the memory include a baseline digital image of skin surface blood vessels and/or skin temperature; and
   the second data processing module is further configured to compare the baseline digital images of skin surface blood vessels and/or skin temperature with the person's skin surface blood vessels and/or skin temperature.

8. The security system of claim 1 wherein the biometric template includes a three-dimensional vector with the digitized spoken utterance and multiple digital images.

9. The security system of claim 1 wherein:

   the audio input module receives multiple audio data markers during a security session;
   the video input module receives multiple frames of video during the security session; and
   the first processing module accumulates the multiple audio data markers and multiple frames of video and correlates them together to form the biometric template.

10. The security system of claim 1 wherein the system is a self-contained unit installed on a portable electronic device, and wherein the system is configured to control access to the portable device.

11. The security system of claim 1 wherein the system is a self-contained unit installed at a security checkpoint and configured to control access to a secure area.

12. A biometric-based security system, comprising:

   audio input means for receiving and digitizing a spoken utterance from a person;
   video input means for receiving multiple digital images of the person at least approximately contemporaneously with receiving the spoken utterance from the person;
   first data processing means for receiving the digitized spoken utterance and digital images of the person and correlating them together to form a biometric template for the person;
   memory means for storing prerecorded audio and video data as individual templates of individual people; and
   second data processing means for receiving the biometric template and comparing it for a match with one of the stored templates of audio and video data.

13. The security system of claim 12 wherein the biometric template includes a three-dimensional vector with the digitized spoken utterance and multiple digital images.

14. The security system of claim 12 wherein:

the audio input means receives multiple audio data markers during a security session;
the video input means receives multiple frames of video during the security session; and
the first processing means accumulates the multiple audio data markers and multiple frames of video and correlates them together to form the biometric template.

15. The security system of claim 12 wherein the video input means includes a color video sensor, a black & white video sensor, and an infrared video sensor.

16. The security system of claim 15 wherein:

the color video sensor is configured to capture one or more digital images of the person's face;
the black & white video sensor is configured to capture one or more digital image of the person's face; and
the infrared video sensor is configured to capture one or more digital images of the person's skin surface blood vessels and/or skin temperature.

17. The security system of claim 12 wherein the video input means is configured to capture one or more digital images of the person's face to create a blood vessel face map and/or a three-dimensional mask image of the person's face.

18. The security system of claim 12 wherein the audio input means includes a voice spectrograph.

19. A monitoring method for use with a person, the method comprising:

receiving voice data representing an predetermined utterance of the person, wherein the voice data representing the predetermined utterance forms an audio biometric feedback component for the person;
receiving multiple digital images of the person, wherein the digital images form a video biometric feedback component for the person;
correlating the received voice data and the received digital images to form a biometric record for the person;
storing prerecorded audio and video data records for each of multiple individual people;
comparing the biometric record for the person to the stored audio and video data records; and
making a decision based on the comparing of the biometric record for the person to the stored audio and video data records.

20. A method of claim 19, further comprising:

receiving digital images that include at least one image of skin surface blood vessels and/or skin temperature; and
storing with at least some of the records at least one baseline digital image of skin surface blood vessels and/or skin temperature for individual people.

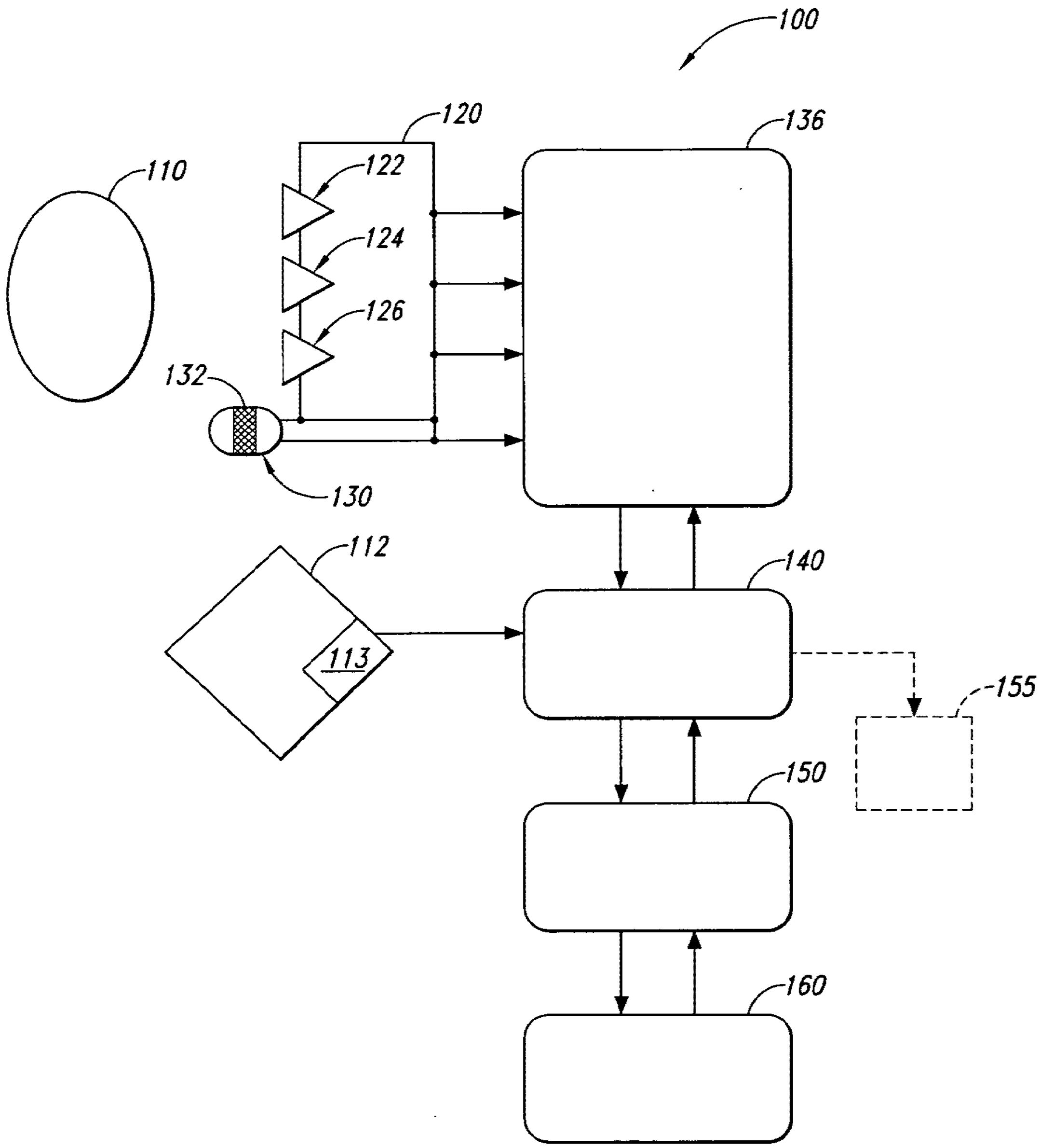


Fig. 1

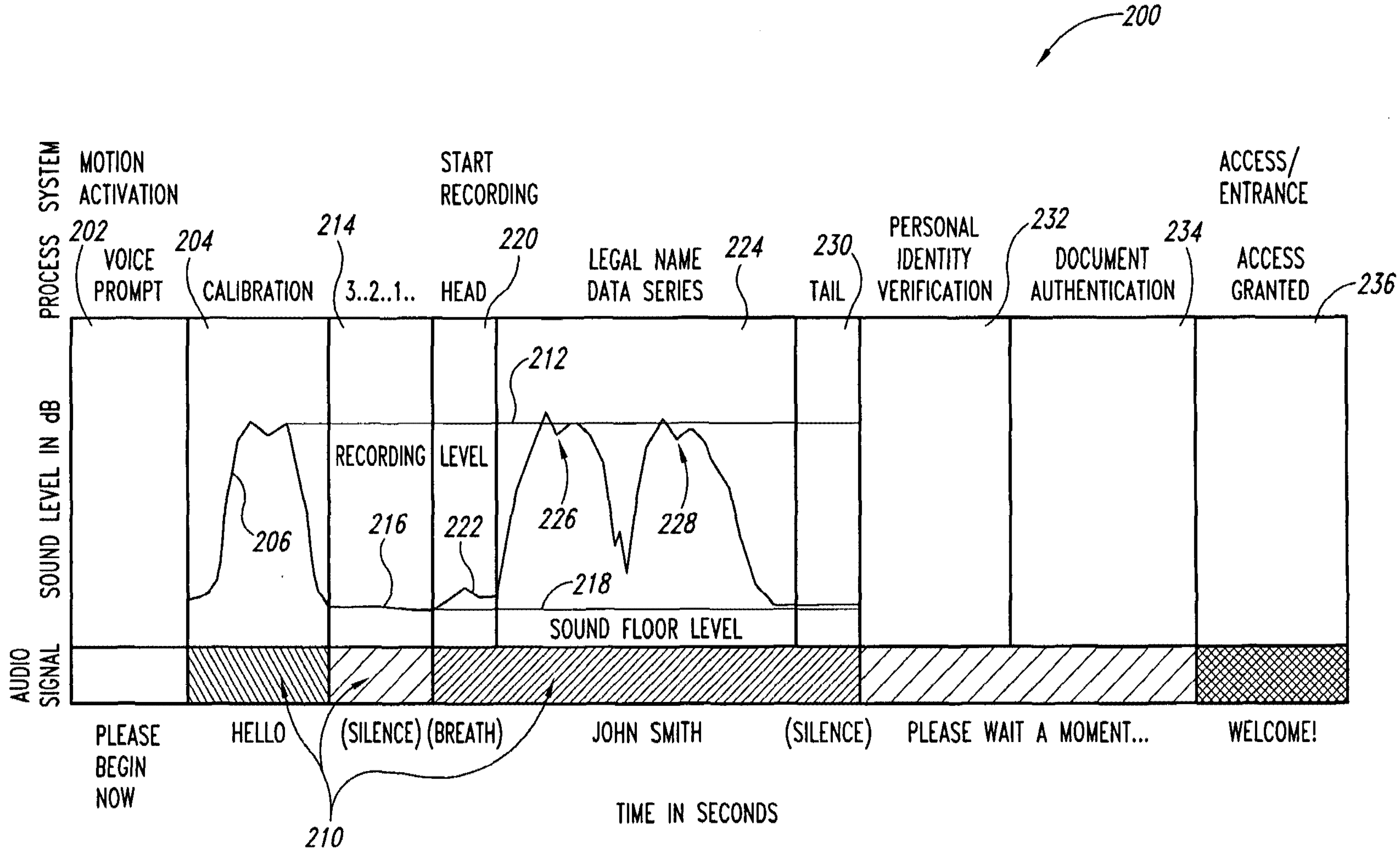

200
SYSTEM
PROCESS
MOTION ACTIVATION
START RECORDING
ACCESS/ ENTRANCE
202
VOICE PROMPT
204
CALIBRATION
214
3..2..1..
220
HEAD
LEGAL NAME DATA SERIES
224
230
TAIL
PERSONAL IDENTITY VERIFICATION
232
DOCUMENT AUTHENTICATION
234
ACCESS GRANTED
236
SOUND LEVEL IN dB
212
RECORDING
LEVEL
206
216
222
226
228
218
SOUND FLOOR LEVEL
AUDIO SIGNAL
PLEASE BEGIN NOW
HELLO
(SILENCE)
(BREATH)
JOHN SMITH
(SILENCE)
PLEASE WAIT A MOMENT...
WELCOME!
TIME IN SECONDS
210

Fig. 2

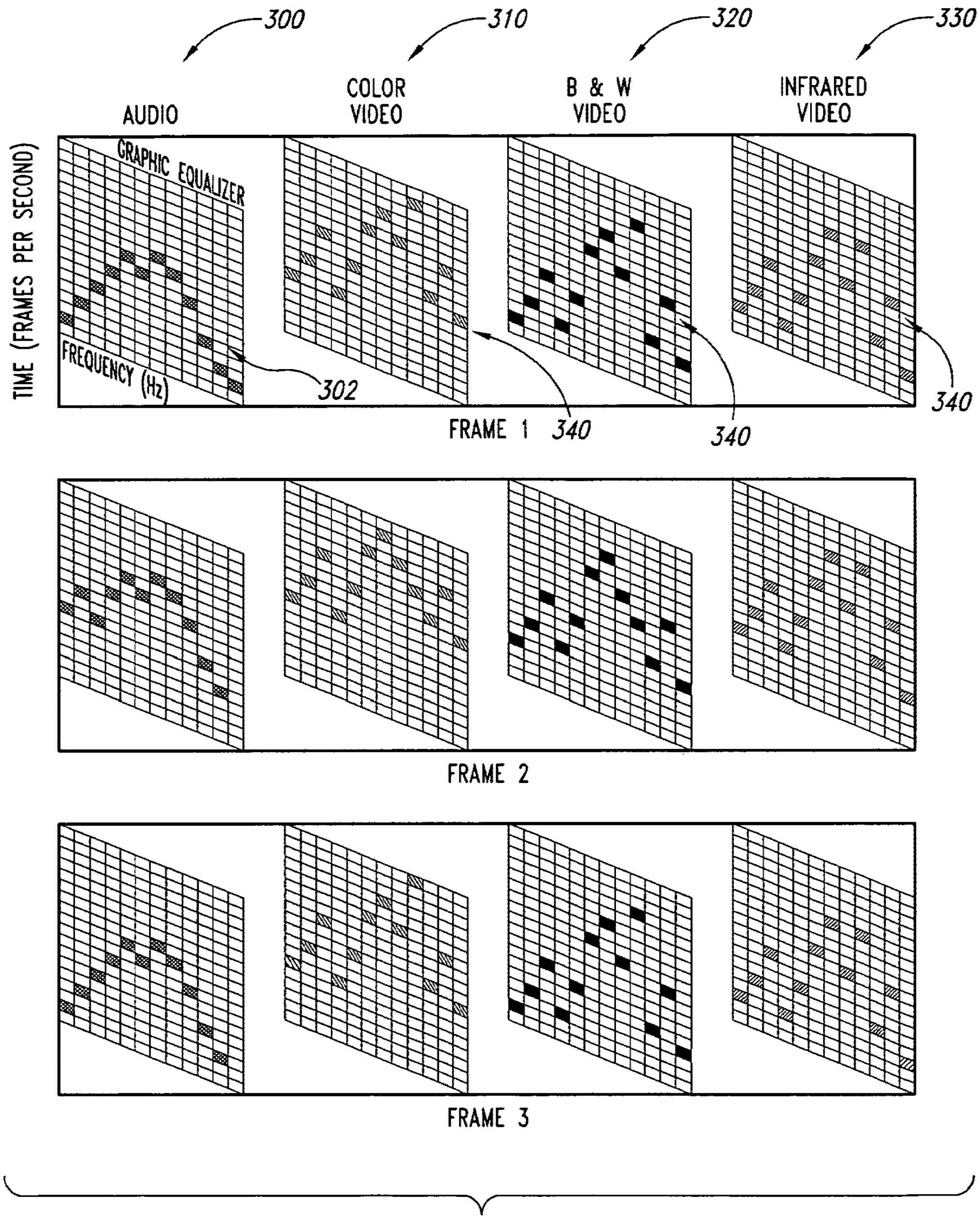

300
310
320
330
AUDIO
COLOR VIDEO
B & W VIDEO
INFRARED VIDEO
TIME (FRAMES PER SECOND)
GRAPHIC EQUALIZER
FREQUENCY (Hz)
302
340
340
340
FRAME 1
FRAME 2
FRAME 3

Fig. 3

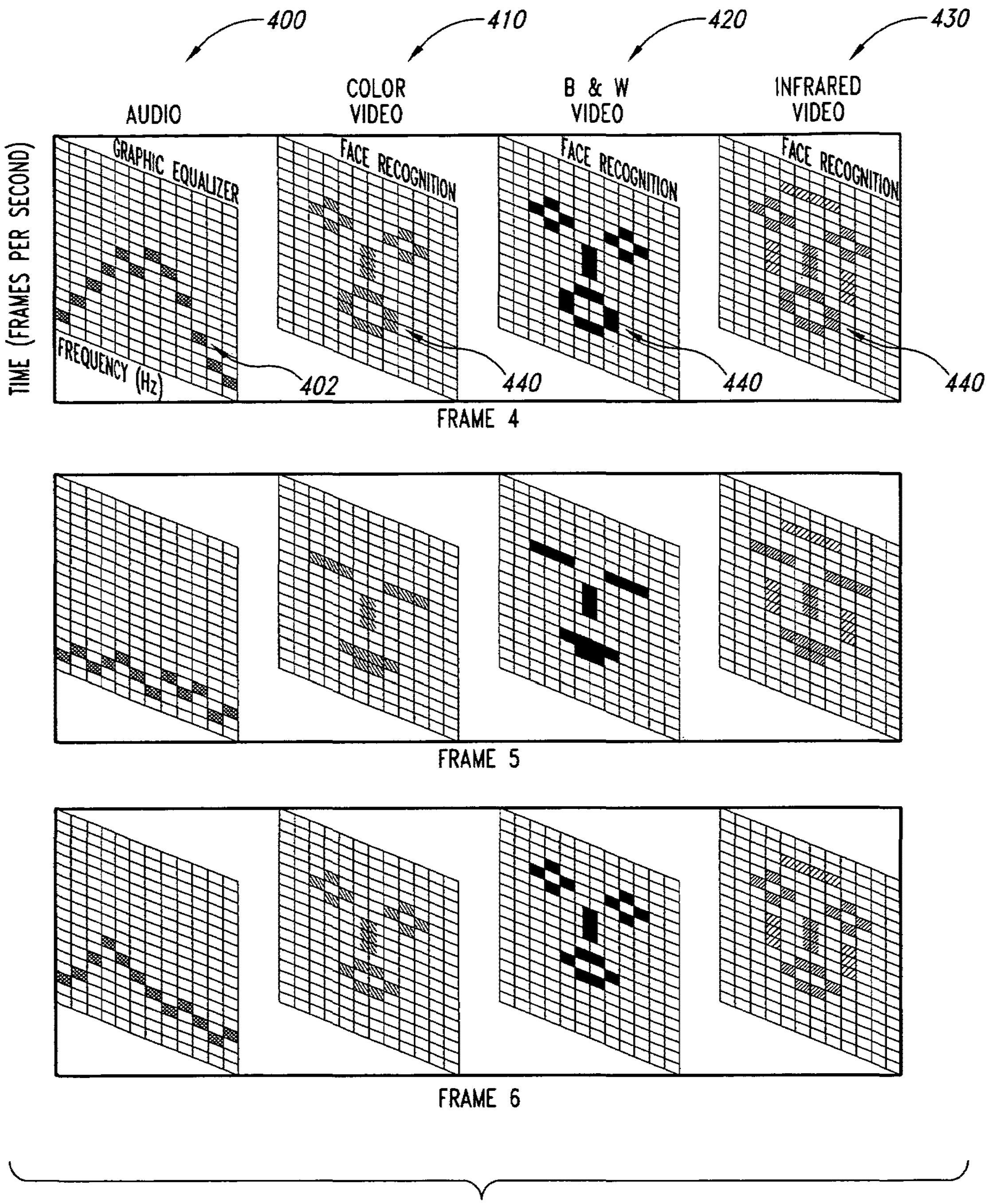

400
410
420
430
AUDIO
COLOR VIDEO
B & W VIDEO
INFRARED VIDEO
TIME (FRAMES PER SECOND)
GRAPHIC EQUALIZER
FACE RECOGNITION
FACE RECOGNITION
FACE RECOGNITION
FREQUENCY (Hz)
402
440
440
440
FRAME 4
FRAME 5
FRAME 6

Fig. 4

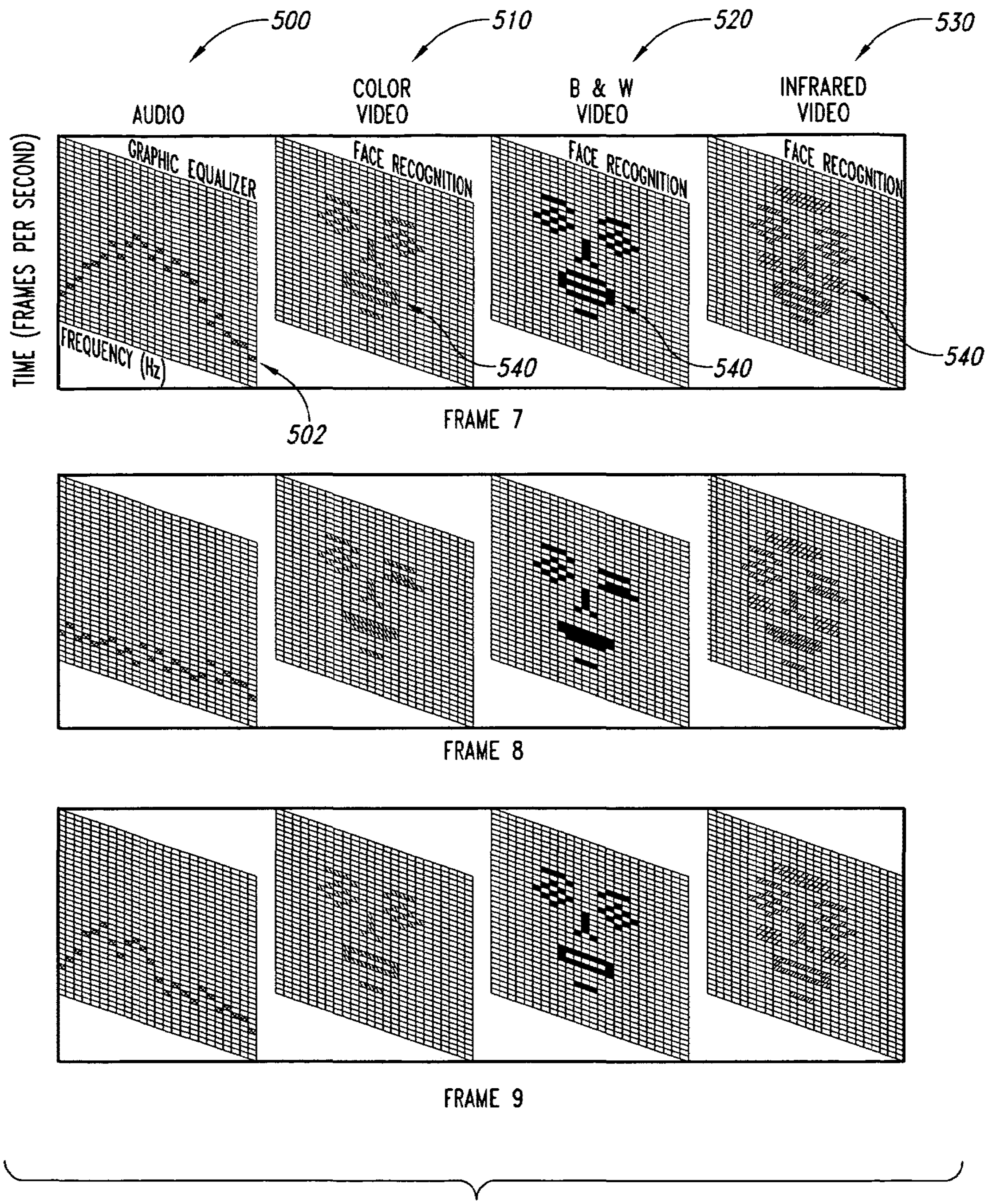

500
510
520
530
AUDIO
COLOR VIDEO
B & W VIDEO
INFRARED VIDEO
TIME (FRAMES PER SECOND)
GRAPHIC EQUALIZER
FACE RECOGNITION
FACE RECOGNITION
FACE RECOGNITION
FREQUENCY (Hz)
540
540
540
502
FRAME 7
FRAME 8
FRAME 9

Fig. 5

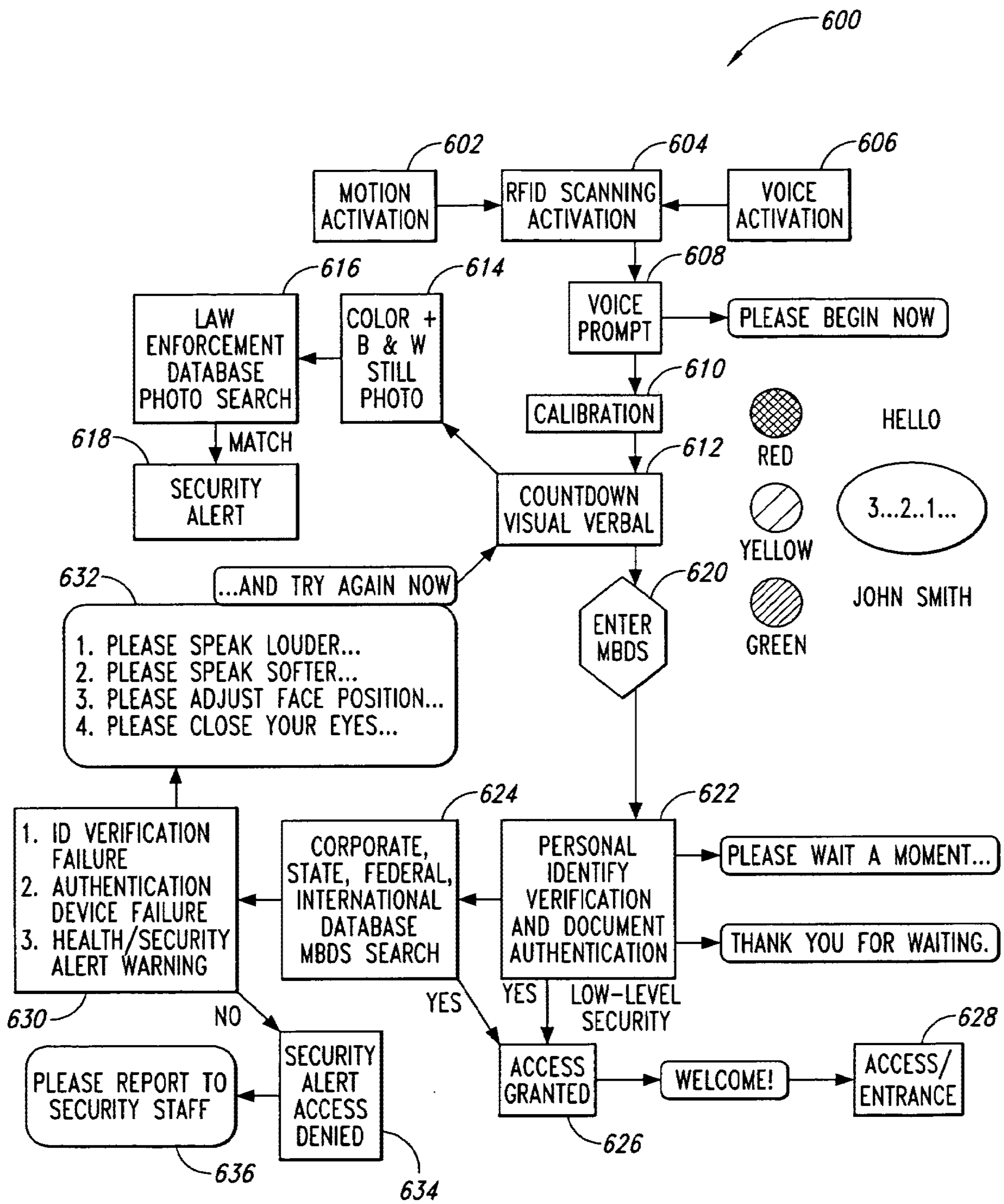

600
602
MOTION ACTIVATION
604
RFID SCANNING ACTIVATION
606
VOICE ACTIVATION
608
VOICE PROMPT
PLEASE BEGIN NOW
610
CALIBRATION
612
COUNTDOWN VISUAL VERBAL
614
COLOR + B & W STILL PHOTO
616
LAW ENFORCEMENT DATABASE PHOTO SEARCH
MATCH
618
SECURITY ALERT
RED
YELLOW
GREEN
HELLO
3...2..1...
JOHN SMITH
620
ENTER MBDS
632
...AND TRY AGAIN NOW
1. PLEASE SPEAK LOUDER...
2. PLEASE SPEAK SOFTER...
3. PLEASE ADJUST FACE POSITION...
4. PLEASE CLOSE YOUR EYES...
622
PERSONAL IDENTIFY VERIFICATION AND DOCUMENT AUTHENTICATION
PLEASE WAIT A MOMENT...
THANK YOU FOR WAITING.
624
CORPORATE, STATE, FEDERAL, INTERNATIONAL DATABASE MBDS SEARCH
630
1. ID VERIFICATION FAILURE
2. AUTHENTICATION DEVICE FAILURE
3. HEALTH/SECURITY ALERT WARNING
NO
YES
YES
LOW-LEVEL SECURITY
626
ACCESS GRANTED
WELCOME!
628
ACCESS/ ENTRANCE
634
SECURITY ALERT ACCESS DENIED
636
PLEASE REPORT TO SECURITY STAFF

Fig. 6

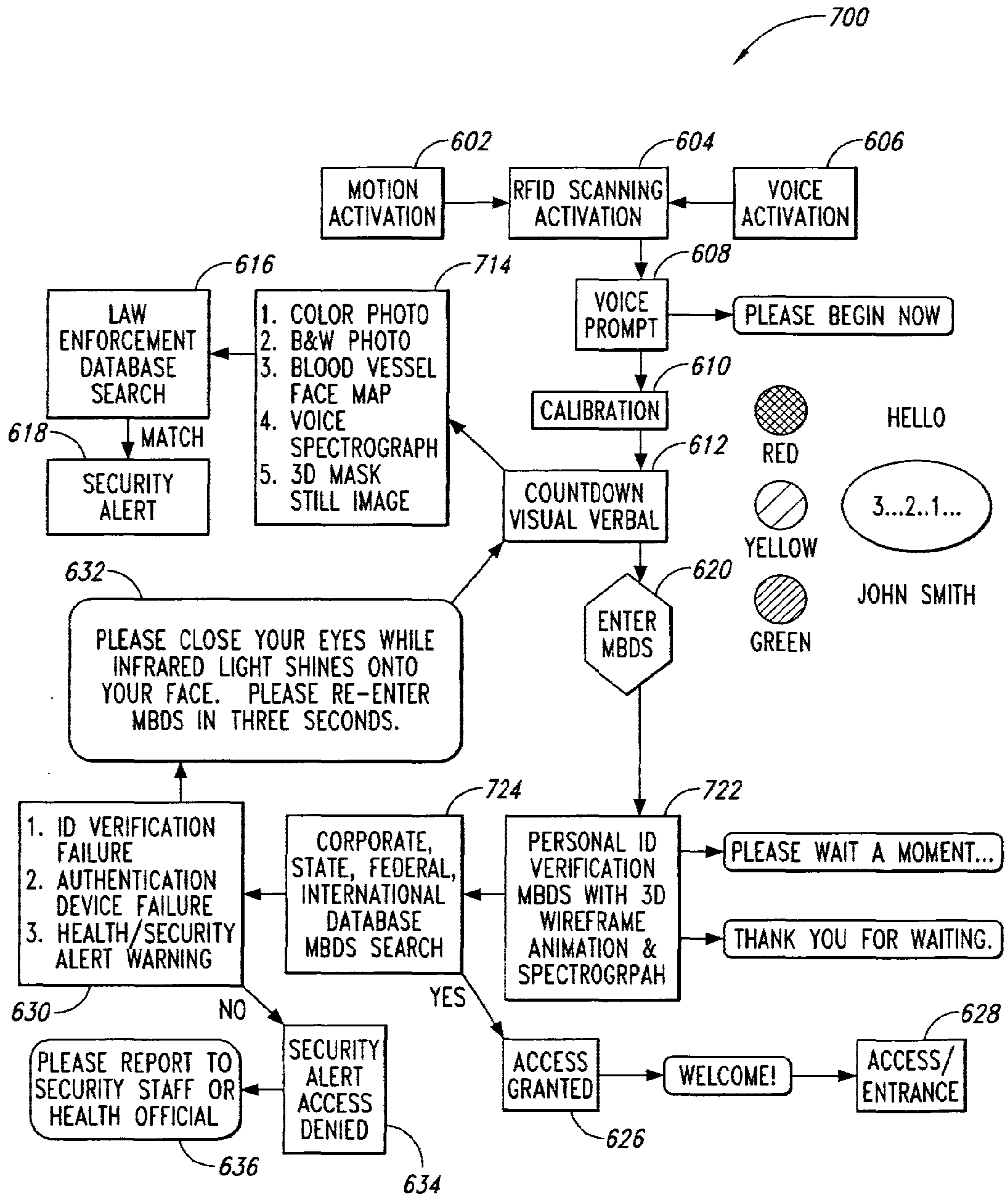

700
602
MOTION ACTIVATION
604
RFID SCANNING ACTIVATION
606
VOICE ACTIVATION
608
VOICE PROMPT
PLEASE BEGIN NOW
610
CALIBRATION
612
COUNTDOWN VISUAL VERBAL
RED
YELLOW
GREEN
HELLO
3...2..1...
JOHN SMITH
620
ENTER MBDS
616
LAW ENFORCEMENT DATABASE SEARCH
MATCH
618
SECURITY ALERT
714
1. COLOR PHOTO
2. B&W PHOTO
3. BLOOD VESSEL FACE MAP
4. VOICE SPECTROGRAPH
5. 3D MASK STILL IMAGE
632
PLEASE CLOSE YOUR EYES WHILE INFRARED LIGHT SHINES ONTO YOUR FACE. PLEASE RE-ENTER MBDS IN THREE SECONDS.
722
PERSONAL ID VERIFICATION MBDS WITH 3D WIREFRAME ANIMATION & SPECTROGRPAH
PLEASE WAIT A MOMENT...
THANK YOU FOR WAITING.
724
CORPORATE, STATE, FEDERAL, INTERNATIONAL DATABASE MBDS SEARCH
1. ID VERIFICATION FAILURE
2. AUTHENTICATION DEVICE FAILURE
3. HEALTH/SECURITY ALERT WARNING
630
NO
YES
SECURITY ALERT ACCESS DENIED
634
PLEASE REPORT TO SECURITY STAFF OR HEALTH OFFICIAL
636
ACCESS GRANTED
626
WELCOME!
ACCESS/ ENTRANCE
628

Fig. 7

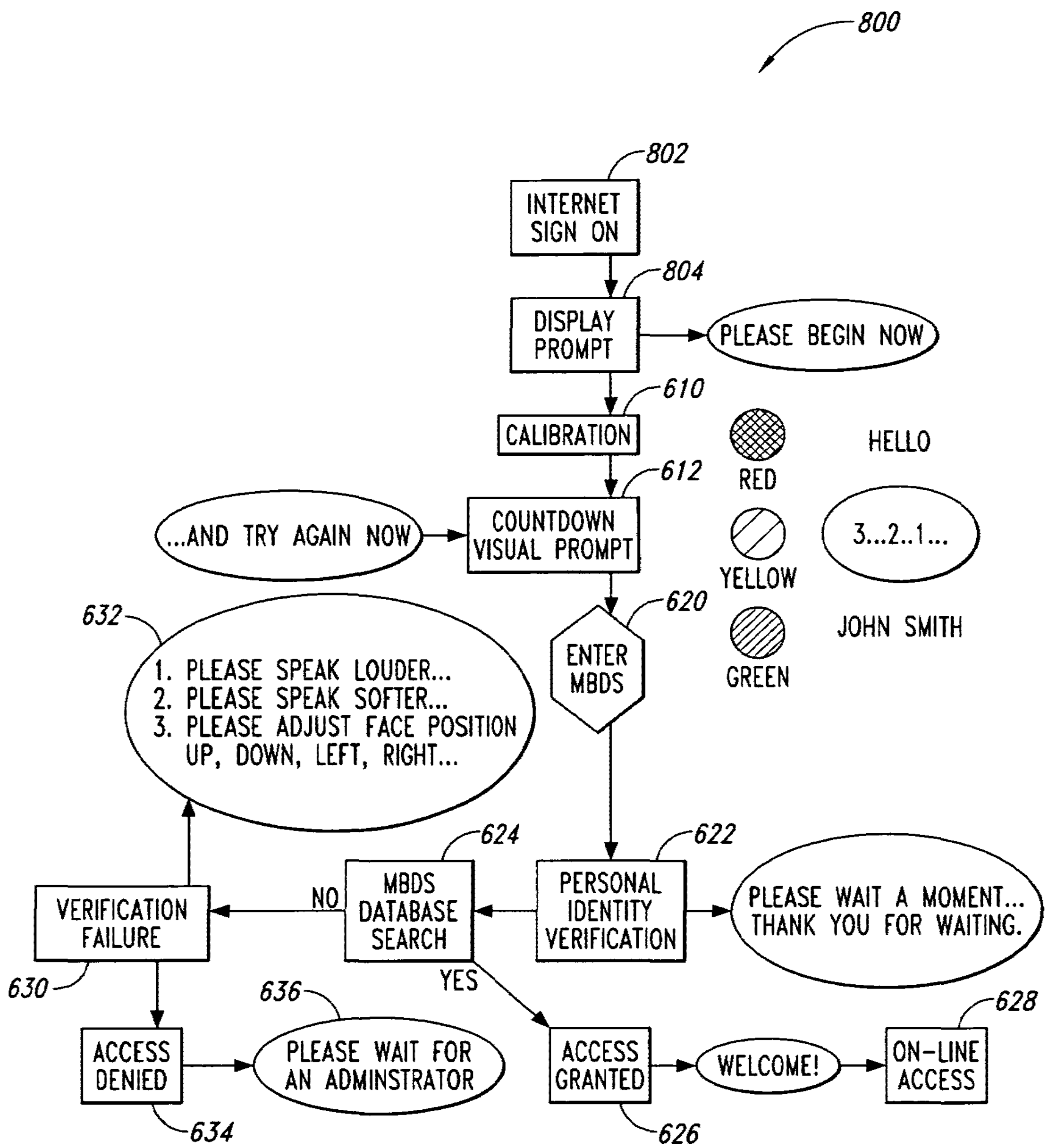
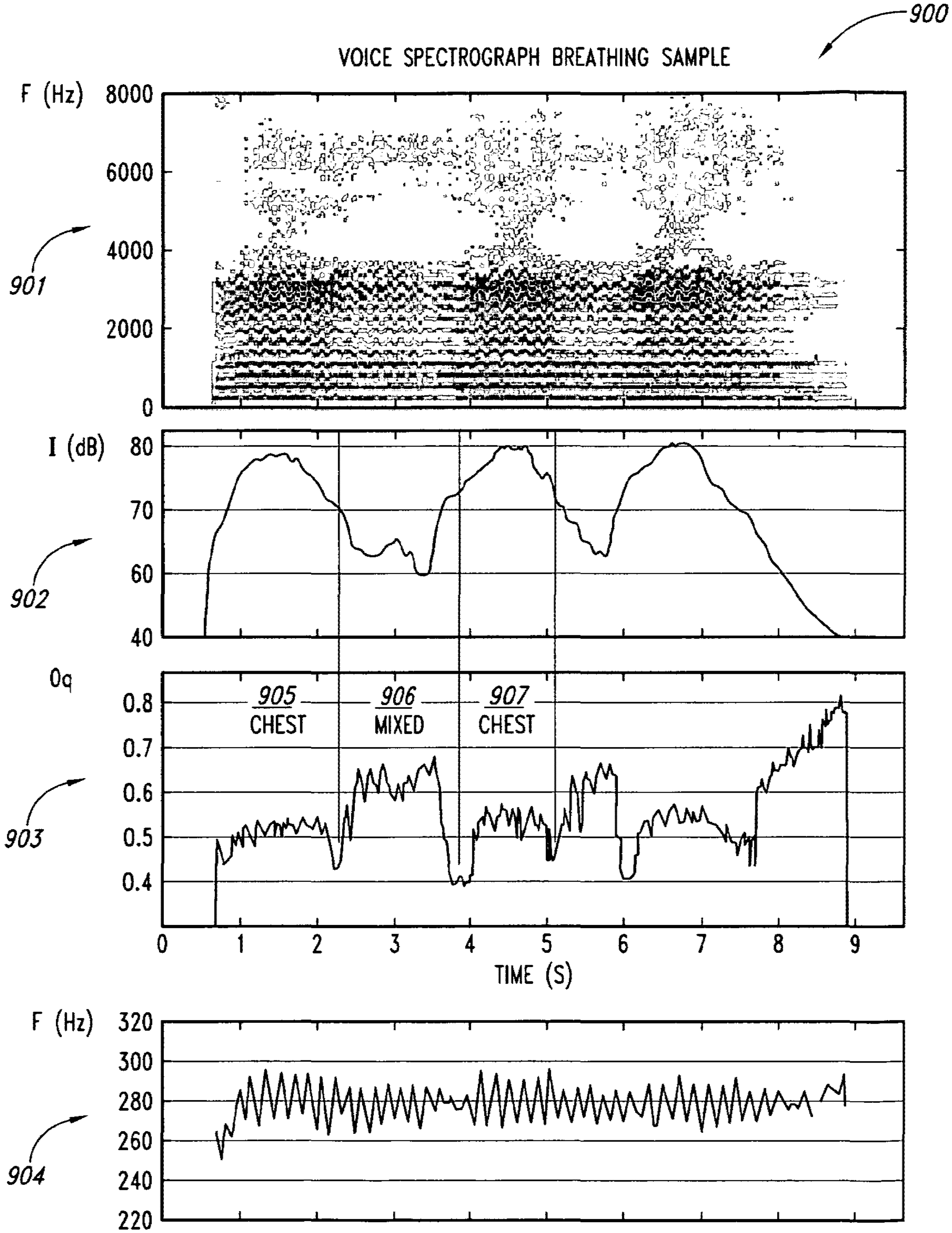

800
802
INTERNET SIGN ON
804
DISPLAY PROMPT
PLEASE BEGIN NOW
610
CALIBRATION
RED
HELLO
612
...AND TRY AGAIN NOW
COUNTDOWN VISUAL PROMPT
YELLOW
3...2..1...
632
620
ENTER MBDS
JOHN SMITH
GREEN
1. PLEASE SPEAK LOUDER...
2. PLEASE SPEAK SOFTER...
3. PLEASE ADJUST FACE POSITION UP, DOWN, LEFT, RIGHT...
624
622
VERIFICATION FAILURE
NO
MBDS DATABASE SEARCH
PERSONAL IDENTITY VERIFICATION
PLEASE WAIT A MOMENT... THANK YOU FOR WAITING.
630
636
YES
628
ACCESS DENIED
PLEASE WAIT FOR AN ADMINSTRATOR
ACCESS GRANTED
WELCOME!
ON-LINE ACCESS
634
626

Fig. 8



900
VOICE SPECTROGRAPH BREATHING SAMPLE
F (Hz)
8000
6000
4000
2000
0
901
I (dB)
80
70
60
40
902
Oq
0.8
0.7
0.6
0.5
0.4
903
905
CHEST
906
MIXED
907
CHEST
0
1
2
3
4
5
6
7
8
9
TIME (S)
F (Hz)
320
300
280
260
240
220
904

Fig. 9

Electronic Acknowledgement Receipt

EFS ID:	46076711
Application Number:	17508887
International Application Number:	
Confirmation Number:	9577
Title of Invention:	FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS
First Named Inventor/Applicant Name:	Kevin Alan Tussy
Customer Number:	32856
Filer:	Chad W. Miller
Filer Authorized By:	
Attorney Docket Number:	FACETC.0082P
Receipt Date:	30-JUN-2022
Filing Date:	22-OCT-2021
Time Stamp:	18:29:43
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	CWMW16752TRANSM.pdf	17034 226b98c218311a91eee08029bdbf77c884ef2e5e	no	1

Warnings:

Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	CWMW16753PTO1449.pdf	23170 30055bd430fa512de8cf548c8d655238d791f799	no	1
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Foreign Reference	REF1CA3075573.pdf	1837677 b03bdd52890de5b81af7dc393c0c86c9dd8787a0	no	26
Warnings:					
Information:					
4	Foreign Reference	REF2EP1693801.pdf	2510720 3e31a7e201e8cd384f83d32ffee20190648052ed	no	26
Warnings:					
Information:					
			Total Files Size (in bytes):	4388601	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor	:	Kevin Alan Tussy	Group Art Unit: OPAP
App. No.	:	17/508,887	
Filed	:	October 22, 2021	
For	:	FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS	
Examiner	:	Central Docket	

I hereby certify that this correspondence and all marked attachments are being deposited with the United States Patent and Trademark Office via EFSWeb, on:

June 29, 2022
(Date)

/Chad W. Miller/
Chad W. Miller, Reg. No. 44,943

SECOND SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Enclosed is form PTO-1449 listing 14 references, copies of which are not required to be provided in accordance with 37 C.F.R. §1.98(e), and 2 foreign references, copies of which are enclosed herewith. This Information Disclosure Statement is being filed before the mailing of the first Office Action on the merits, and as such, no fee is required in accordance with 37 C.F.R. §1.97(b)(3).

Respectfully submitted,

Dated: June 29, 2022

By: /Chad W. Miller/
Chad W. Miller
Attorney for Applicant
Weide & Miller, Ltd.
Registration No. 44,943
10655 Park Run Drive, Suite 100
Las Vegas, NV 89144
Tel. (702) 382-4804 (Pacific Time)
cmiller@weidemiller.com

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)

FOREIGN PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION	
							YES	NO

EXAMINER INITIAL		**OTHER DOCUMENTS** (INCLUDING AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.)
		"An Overview of Face Liveness Detection", Chakraborty, et al., Dept. of Computer Science and Engineering, National Institute of Technology, Silchar India, International Journal on Information Theory (IJIT), Vol. 3, No. 2, DOI: 10.512/ijit.2014.3202, 15 pages, April 2014.
		"SVO Fast Semi-Direct Monocular Visual Odometry", Christian Forster, et al., ResearchGate, Conference Paper in Proceedings - IEEE International Conference on Robotics and Automation, DOI: 10.1109/ICRA.2014.6906584, https://www.researchgate.net/publication/262378002, 9 pages, May 18, 2014.
		"Evaluating Liveness by Face Images and the Structure Tensor", Kollreider, et al., Halmstad University, SE-30118, Sweden, Halmstad University Post-Print, ©IEEE 2005, Fourth IEEE Workshop on Automatic Identification Advanced Technologies, 2005, IEEE: 2005. PGS. 75-80, DOI: http://dx.doi.org/10.1109/AUTOID.2005.20, 7 pages, date unknown.
		"An Iterative Image registration Technique with an Application to Stereo Vision", Lucas, et al., Computer Science Department, Carnegie-Mellon University, Pittsburgh, Pennsylvania 15213, From Proceedings of Imaging Understanding Workshop, PP. 121-130 (1981)., pgs. 121-130, 10 pgs., date unknown.
		"Head Gesture Recognition Using Optical Flow Based Classification with Reinforcement of GMM Based Background Subtraction", Saikia, et al., Department of Electronics and Communication Engineering, DBCET, Assam Don Bosco University, International Journal of Computer Application (0975-8887), Volume 65- No. 25, March 2013, 7 pgs.
		"A Liveness Detection Method for Face Recognition Base on Optical Flow Field", Bao, et al., College of Computer Science, Zhejiang University, 978-1-4244-3986-7/09/$25.00 ©2009 IEEE,IEEE Xplore (03/15/22 download), 4 pages.

EXAMINER	DATE CONSIDERED

***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

CWM-W-16566

Electronic Acknowledgement Receipt

EFS ID:	45637466
Application Number:	17508887
International Application Number:	
Confirmation Number:	9577
Title of Invention:	FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS
First Named Inventor/Applicant Name:	Kevin Alan Tussy
Customer Number:	32856
Filer:	Chad W. Miller
Filer Authorized By:	
Attorney Docket Number:	FACETC.0082P
Receipt Date:	05-MAY-2022
Filing Date:	22-OCT-2021
Time Stamp:	20:19:22
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	CWMW16565TRANS.pdf	16695 81650c525d29a9fa99d02297dc576cc952323287	no	1

Warnings:

Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	CWMW16566PTO1449.pdf	24126 21ffb28165c3023ad425d2f72ed96b34038cb195	no	1
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Non Patent Literature	REF1ChakrobortyAnOverviewofFaceLivenessDetection.pdf	1573007 421955f33207dac7eae91005e79a9510234dec14	no	15
Warnings:					
Information:					
4	Non Patent Literature	REF2ForsterSVOFastSemiDirectMonocularVisualOdometry.pdf	2541298 3bc30ac825f32de54d8b2b055fdf98d0bc0d3aff	no	9
Warnings:					
Information:					
5	Non Patent Literature	REF3KollreiderEvaluatingLivenessByFaceImagesAndThe.pdf	500017 6aea849250f2d5af379a12aba089f578bb498632	no	7
Warnings:					
Information:					
6	Non Patent Literature	REF4LucasAnIterativeImage.pdf	1045554 a28530c60ddb0cd46a8bb88423e8e479af9495ca	no	10
Warnings:					
Information:					
7	Non Patent Literature	REF5SaikiHeadGestureRecognition.pdf	466240 bd0240eb0e4493cc3c5cf5d0cca3c27ede9e4eab	no	7
Warnings:					
Information:					
8	Non Patent Literature	REF6BaoALivenessDetectionMethodForFaceRecognitionBasedOnOpticalFlowField.pdf	1212565 2dc2ff02d3111d83b0da4d8c13206663dcb09638	no	4
Warnings:					
Information:					

Total Files Size (in bytes):	7379502

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor	:	Kevin Alan Tussy	)
App. No.	:	17/508,887	)
Filed	:	October 22, 2021	)
For	:	FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS	)
Examiner	:	Central Docket	)

Group Art Unit: OPAP

I hereby certify that this correspondence and all marked attachments are being deposited with the United States Patent and Trademark Office via EFSWeb, on:

May 4, 2022
(Date)

/Chad W. Miller/
Chad W. Miller, Reg. No. 44,943

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Enclosed is form PTO-1449 listing 6 publications, copies of which are enclosed herewith. This Information Disclosure Statement is being filed before the mailing of the first Office Action on the merits, and as such, no fee is required in accordance with 37 C.F.R. §1.97(b)(3).

Respectfully submitted,

Dated: May 4, 2022

By: /Chad W. Miller/
Chad W. Miller
Attorney for Applicant
Weide & Miller, Ltd.
Registration No. 44,943
10655 Park Run Drive, Suite 100
Las Vegas, NV 89144
Tel. (702) 382-4804 (Pacific Time)
cmiller@weidemiller.com

CWM-W-16565

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
17/508,887	10/22/2021	Kevin Alan Tussy	FACETC.0082P

CONFIRMATION NO. 9577

PUBLICATION NOTICE

OC000000131774285

32856
WEIDE & MILLER, LTD.
10655 PARK RUN DRIVE
SUITE 100
LAS VEGAS, NV 89144

Title: FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS

Publication No. US-2022-0043896-A1
Publication Date: 02/10/2022

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Public Records Division. The Public Records Division can be reached by telephone at (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, by mail addressed to the United States Patent and Trademark Office, Public Records Division, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently https://portal.uspto.gov/pair/PublicPair. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		5,031,228	07/91	Lu			
		5,699,449	12/97	Javidi			
		5,784,056	07/98	Nielsen			
		5,781,650	07/98	Lobo, et al.			
		5,835,616	11/98	Lobo, et al.			
		5,842,194	11/98	Arbuckle			
		5,850,470	12/98	Kung, et al.			
		5,956,122	09/99	Doster			
		5,982,912	11/99	Fukui, et al.			
		6,134,339	10/00	Luo			
		6,173,068	01/01	Prokoski			
		6,212,030	04/01	Koriyama, et al.			
		6,246,779	06/01	Fukui, et al.			
		6,301,370	10/01	Steffens, et al.			
		6,310,601	10/01	Moore, et al.			
		2002/0103813	05/02	Frigon			
		2002/0054059	05/02	Scheiderman			
		2002/0055955	05/02	Lloyd-Jones, et al.			
		6,389,176	05/02	Hsu, et al.			
		2002/0087622	07/02	Anderson			
		6,461,807	10/02	Friend, et al.			
		2002/0191818	12/02	Matsuo, et al.			
		2003/0039380	02/03	Sukegawa, et al.			
		2003/0053663	03/03	Chen, et al.			
		2003/0063669	04/03	Lee, et al.			
		2003/0095053	05/03	Kandogan			

EXAMINER	DATE CONSIDERED

***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

CWM-W-16209

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE **INFORMATION DISCLOSURE CITATION BY APPLICANT** (USE SEVERAL SHEETS IF NECESSARY)	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
	INVENTOR(S) Kevin Alan Tussy	
	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

U.S. PATENT DOCUMENTS							
EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2003/0103652	06/03	Lee, et al.			
		2003/0133599	07/03	Tian, et al.			
		2003/0198368	10/03	Kee			
		2003/0236832	12/03	McIntyre, et al.			
		6,678,664	01/04	Ganesan			
		D485,279	01/04	DeCombe			
		6,697,502	02/04	Luo			
		6,687,390	02/04	Avni, et al.			
		6,711,584	03/04	Wajda, et. al.			
		6,728,401	04/04	Hardeberg			
		2004/0070678	04/04	Toyama, et al.			
		2004/0081338	04/04	Takenaka			
		2004/0091136	05/04	Dombrowski			
		2004/0109584	06/04	Lestideau			
		2004/0125991	07/04	Yokoi			
		2004/0143598	07/04	Drucker, et al.			
		6,775,397	08/04	Hamalainen			
		2004/0190758	09/04	Doi, et al.			
		2004/0201709	10/04	McIntyre, et al.			
		2004/0218792	11/04	Spoonhower, et al.			
		2004/0264780	12/04	Zhang, et al.			
		6,840,149	01/05	Beal			
		2005/0031173	02/05	Hwang			
		2005/0065885	03/05	Gordon			
		2005/0065855	03/05	Geller			
		2005/0094849	05/05	Sung, et al.			

EXAMINER	DATE CONSIDERED
***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.	

CWM-W-16209

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE **INFORMATION DISCLOSURE CITATION BY APPLICANT** (USE SEVERAL SHEETS IF NECESSARY)	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
	INVENTOR(S) Kevin Alan Tussy	
	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2005/0100195	05/05	Li			
		2005/0117802	06/05	Yonaha et al.			
		2005/0141766	06/05	Nagahashi, et al.			
		2005/0180627	08/05	Yan, et al.			
		2005/0190273	09/05	Toyama, et al.			
		2005/0220347	10/05	Enomoto			
		6,961,361	11/05	Tanaka			
		2005/0251015	11/05	Takikawa, et al.			
		2005/0265603	12/05	Porter			
		7,003,135	02/06	Hsieh, et al.			
		2006/0050933	03/06	Adam, et al.			
		2006/0110014	05/06	Philomin			
		2006/0133672	06/06	Li			
		2006/0156029	07/06	Algazi			
		2006/0173560	08/06	Widrow			
		2006/0218225	09/06	Hee Voon, et al.			
		2006/0224523	10/06	Elvitigala			
		2006/0222215	10/06	Jung, et al.			
		2006/0239515	10/06	Zhang, et al.			
		2006/0251292	11/06	Gokturk, et al.			
		2006/0251339	11/06	Gokturk, et al.			
		2006/0251338	11/06	Gokturk, et al.			
		2006/0253491	11/06	Gokturk, et al.			
		2006/0274978	12/06	Fukuda, et al.			
		2007/0074114	03/07	Adjali, et al.			
		2007/0081744	04/07	Gokturk, et al.			

EXAMINER	DATE CONSIDERED
***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.	

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		7,211,138	05/07	Yamamoto, et al.			
		7,218,774	05/07	Liu			
		2007/0098230	05/07	Norita			
		2007/0098303	05/07	Gallagher, et al.			
		7,231,657	06/07	Honarvar, et al.			
		2007/0177805	08/07	Gallagher			
		2007/0206834	09/07	Shinkai, et al.			
		2007/0211925	09/07	Aoki, et al.			
		7,289,648	10/07	Liu			
		7,308,581	12/07	Geosimonian			
		2007/0290499	12/07	Tame			
		2008/0046458	02/08	Tseng, et al.			
		2008/0037869	02/08	Zhou			
		7,333,963	02/08	Widrow, et al.			
		2008/0077595	03/08	Leebow			
		2008/0080743	04/08	Schneiderman, et al.			
		2008/0080745	04/08	Vanhoucke, et al.			
		2008/0091723	04/08	Zuckerberg, et al.			
		2008/0100195	05/08	Kim, et al.			
		2008/0130960	06/08	Yagnik			
		7,415,152	08/08	Jiang, et al.			
		7,428,320	09/08	Northcott, et al.			
		2008/0212849	09/08	Gao			
		2008/0317379	12/08	Steinberg, et al.			
		7,519,200	04/09	Gokturk, et al.			
		D596,192	07/09	Shotel			

EXAMINER	DATE CONSIDERED
***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.	

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2009/0185784	09/09	Hiroike, et al.			
		2009/0226052	09/09	Fedel			
		2009/0232367	09/09	Shinzaki			
		D601,582	10/09	Chaudhri			
		2009/0252383	10/09	Adam, et al.			
		2009/0324022	12/09	Sangberg, et al.			
		D606,082	12/09	Parker			
		7,636,450	12/09	Bourdev			
		2009/0324018	12/09	Tell			
		2009/0324137	12/09	Stallings, et al.			
		7,646,909	01/10	Jiang, et al.			
		2010/0050134	02/10	Clarkson			
		7,660,444	02/10	Hamalainen			
		2010/0054601	03/10	Anbalagan, et al.			
		2010/0067750	03/10	Matsuo			
		2010/0054600	03/10	Anbalagan, et al.			
		2010/0061631	03/10	Omori			
		7,710,693	05/10	Guzman-Casillas, et al.			
		2010/0158327	06/10	Kangas, et al.			
		7,783,118	08/10	Zhou			
		7,788,247	08/10	Wang, et al.			
		2010/0232656	09/10	Ryu			
		7,804,982	09/10	Howard, et al.			
		2010/0245614	09/10	Matsunaga			
		7,809,722	10/10	Gokturk, et al.			
		D625,325	10/10	Vu			

EXAMINER	DATE CONSIDERED
***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.	

CWM-W-16209

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE **INFORMATION DISCLOSURE CITATION BY APPLICANT** (USE SEVERAL SHEETS IF NECESSARY)	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
	INVENTOR(S) Kevin Alan Tussy	
	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2010/0272363	10/10	Steinberg, et al.			
		2010/0287053	11/10	Ganong, et al.			
		2010/0310133	12/10	Mason, et al.			
		2010/0318366	12/10	Sullivan			
		2010/0317420	12/10	Hoffberg			
		2011/0063108	03/11	Aonuma, et al.			
		D637,604	05/11	Brinda			
		7,945,653	05/11	Zuckerberg, et al.			
		7,960,470	06/11	Okahira			
		D640,277	06/11	Woo			
		2011/0169853	07/11	Oiwa			
		2011/0202531	08/11	Zuckerberg, et al.			
		2011/0225481	09/11	Zuckerberg, et al.			
		2011/0282906	11/11	Wong			
		D650,793	12/11	Impas			
		8,121,408	02/12	Omori			
		8,165,352	04/12	Mohanty, et al.			
		2012/0140993	06/12	Bruso, et al.			
		D663,743	07/12	Tanghe			
		D663,744	07/12	Tanghe			
		8,210,247	07/12	Blomgren			
		8,244,211	08/12	Clark			
		D667,423	09/12	Nagamine			
		2012/0235790	09/12	Zhao, et al.			
		8,280,120	10/12	Hoyos, et al.			
		8,316,237	11/12	Felsher, et al.			

EXAMINER	DATE CONSIDERED
***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.	

CWM-W-16209

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE **INFORMATION DISCLOSURE CITATION BY APPLICANT** (USE SEVERAL SHEETS IF NECESSARY)	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
	INVENTOR(S) Kevin Alan Tussy	
	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2012/0323704	12/12	Steelberg			
		8,326,000	12/12	Jung, et al.			
		2013/0007032	01/13	Klappert			
		2013/0015946	01/13	Lau			
		8,392,268	03/13	Smith, et al.			
		2013/0066526	03/13	Mondragon			
		2013/0057693	03/13	Baranek			
		8,396,246	03/13	Anbalagan, et al.			
		2013/0077835	03/13	Kritt, et al.			
		8,411,909	04/13	Zhao, et al.			
		2013/0086674	04/13	Horvitz, et al.			
		8,416,312	04/13	Matsunaga			
		8,457,367	06/13	Sipe			
		8,460,024	06/13	Damodharan, et al.			
		2013/0179298	07/13	Segman			
		2013/0226740	08/13	Biliosa			
		2013/0236066	09/13	Shubinsky			
		2013/0246158	09/13	Cannon			
		D692,018	10/13	Wenz			
		2013/0267204	10/13	Schultz, et al.			
		D692,915	11/13	Brinda			
		2013/0342672	12/13	Gray, et al.			
		2014/0012756	01/14	Beraja			
		2014/0022179	01/14	Yoon			
		2014/0059673	02/14	Azar			
		8,709,801	04/14	Pan, et al.			

EXAMINER	DATE CONSIDERED
***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.	

CWM-W-16209

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE **INFORMATION DISCLOSURE CITATION BY APPLICANT** (USE SEVERAL SHEETS IF NECESSARY)	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
	INVENTOR(S) Kevin Alan Tussy	
	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2014/0098174	04/14	Summers			
		D702,714	04/14	Abratowski			
		8,722,977	05/14	Wooten, Jr.			
		2014/0118257	05/14	Baldwin			
		2014/0123275	05/14	Azar			
		8,743,051	06/14	Moy, et al.			
		2014/0165187	06/14	Daesung			
		2014/0169643	06/14	Todoroki			
		2014/0173443	06/14	Hawkins, III			
		8,750,574	06/14	Ganong, et al.			
		2014/0197922	07/14	Stanwood			
		2014/0198959	07/14	Derakhshani			
		D712,909	09/14	Francisco			
		D713,410	09/14	Francisco			
		8,856,541	10/14	Chaudhury			
		8,867,849	10/14	Kirkham			
		D715,317	10/14	Perace			
		2014/0337791	11/14	Agnetta			
		2014/0337948	11/14	Hoyos			
		2014/0351761	11/14	Bae			
		D717,339	11/14	Wen			
		D717,829	11/14	Lee			
		8,922,480	12/14	Freed, et al.			
		2015/0052462	02/15	Kulkarni			
		2015/0055821	02/15	Fotland			
		8,959,578	02/15	Simpson, et al.			

EXAMINER	DATE CONSIDERED
***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.	

CWM-W-16209

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE **INFORMATION DISCLOSURE CITATION BY APPLICANT** (USE SEVERAL SHEETS IF NECESSARY)	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
	INVENTOR(S) Kevin Alan Tussy	
	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2015/0074615	03/15	Han			
		2015/0077323	03/15	Ramaswamy			
		D725,151	03/15	Bray			
		D725,668	03/15	Clare			
		D726,221	04/15	Gomez			
		9,037,354	05/15	Mondragon			
		2015/0148106	05/15	Choi			
		D728,623	05/15	Lim			
		D730,389	05/15	Izotov			
		2015/0131872	05/15	Ganong, et al.			
		9,069,447	06/15	Kim			
		2015/0153571	06/15	Ballard			
		D730,941	06/15	Marianek			
		D731,552	06/15	Seo			
		9,076,008	07/15	Moy			
		9,076,028	07/15	Summers			
		2015/0205399	07/15	Kim			
		2015/0205454	07/15	Ainslie			
		2015/0212684	07/15	Sabia			
		D733,755	07/15	Kadosh			
		2015/0227286	08/15	Kangas, et al.			
		D736,812	08/15	Yoo			
		D737,325	08/15	Kim			
		9,137,246	09/15	Parry, et al.			
		D738,921	09/15	Lim			
		2015/0310260	10/15	Summers			

EXAMINER	DATE CONSIDERED
***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.	

CWM-W-16209

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		D740,833	10/15	Bae			
		9,152,849	10/15	Ganong, et al.			
		D742,417	11/15	Brunner			
		9,202,105	12/15	Wang, et al.			
		9,209,355	12/15	Senda, et al.			
		2015/0378433	12/15	Savastinuk			
		D745,567	12/15	Park			
		2016/0026425	01/16	Lee			
		D747,354	01/16	Park			
		2016/0063235	03/16	Tussy			
		D752,078	03/16	Guesnon, Jr.			
		2016/0071111	03/16	Wang, et al.			
		2016/0087991	03/16	Matsuoka			
		D753,132	04/16	Cuthbert			
		2016/0117544	04/16	Hoyos, et al.			
		D756,401	05/16	Soldner			
		D757,084	05/16	Chaudhri			
		D759,723	06/16	Butcher			
		2016/0209939	07/16	Zambetti			
		D761,268	07/16	Oh			
		D761,277	07/16	Harvell			
		9,424,491	08/16	Kirkham			
		9,430,695	08/16	Summers			
		D762,655	08/16	Kai			
		D762,673	08/16	Seo			
		D762,715	08/16	Williamson			

EXAMINER	DATE CONSIDERED

***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

CWM-W-16209

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE **INFORMATION DISCLOSURE CITATION BY APPLICANT** (USE SEVERAL SHEETS IF NECESSARY)	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
	INVENTOR(S) Kevin Alan Tussy	
	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

U.S. PATENT DOCUMENTS							
EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		D763,271	08/16	Everette			
		D763,306	08/16	Lee			
		D764,526	08/16	Gomez			
		D764,534	08/16	Seo			
		D765,117	08/16	Joo			
		D765,133	08/16	Joo			
		9,448,687	09/16	McKenzie			
		2016/0259528	09/16	Foss			
		2016/0261675	09/16	Block			
		2016/0284123	09/16	Hare			
		D765,674	09/16	Kim			
		D766,926	09/16	Fleischmann			
		D766,314	09/16	Bauer			
		D766,298	09/16	Bae			
		9,459,132	10/16	Fehrenbach, et al.			
		D769,933	10/16	Sabia			
		2016/0342826	11/16	Apostolos, et al.			
		D772,288	11/16	Montes			
		D772,929	11/16	Montes			
		2016/0335483	11/16	Pfursich, et al.			
		2016/0364561	12/16	Lee			
		D776,680	01/17	Bae			
		D777,755	01/17	Beaty			
		8,649,604	02/17	Steinberg, et al.			
		D778,923	02/17	Zhou			
		D778,940	02/17	Williamson			

EXAMINER	DATE CONSIDERED
***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.	

CWM-W-16209

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE **INFORMATION DISCLOSURE CITATION BY APPLICANT** (USE SEVERAL SHEETS IF NECESSARY)	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
	INVENTOR(S) Kevin Alan Tussy	
	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

U.S. PATENT DOCUMENTS							
EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2017/0053406	02/17	Hirvonen			
		9,607,138	03/17	Baldwin			
		2017/0083086	03/17	Mazur			
		D780,781	03/17	Ding			
		9,600,649	03/17	Parry, et al.			
		D783,633	04/17	Oh			
		D783,652	04/17	Guan			
		D784,363	04/17	Fleming, et al.			
		D787,527	05/17	Wilberding			
		D788,122	05/17	Tada			
		D788,810	06/17	Kim			
		D790,567	06/17	Su			
		D791,158	07/17	Shiino			
		9,708,909	07/17	Atkinson, et al.			
		9,740,848	08/17	Parry, et al.			
		2017/0220843	08/17	Apostolos, et al.			
		D794,663	08/17	Sakuma			
		D798,321	09/17	Lieb			
		9,798,420	10/17	Ichikawa			
		D798,902	10/17	Choi			
		D799,544	10/17	Kim			
		D800,743	10/17	Rhodes			
		D801,990	11/17	Reissner			
		D803,870	11/17	Landry			
		D805,546	12/17	Wu			
		D805,548	12/17	King			

EXAMINER	DATE CONSIDERED
***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.	

CWM-W-16209

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE **INFORMATION DISCLOSURE CITATION BY APPLICANT** (USE SEVERAL SHEETS IF NECESSARY)	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
	INVENTOR(S) Kevin Alan Tussy	
	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		D806,113	12/17	Beckman			
		D807,378	01/18	Imamura			
		D807,381	01/18	Hersh			
		9,911,036	03/18	Hartman			
		9,958,687	05/18	Chern, et al.			
		2018/0139157	05/18	Decculus			
		D817,994	05/18	Jou			
		D819,075	05/18	Tsuji			
		2018/0165508	06/18	Othman, et al.			
		D820,305	06/18	Clediere			
		D821,439	06/18	Sowden			
		D821,443	06/18	Jang			
		D822,054	07/18	Persson			
		D823,335	07/18	Alonso			
		D823,867	07/18	Berlow			
		D823,891	07/18	Lupe			
		D825,587	08/18	O'Rourke			
		D825,588	08/18	Hashimoto			
		2018/0342018	11/18	Pancholi			
		2019/0080189	03/19	VAN OS			
		10,360,464	07/19	McKay, et al.			
		2019/0213311	07/19	Tussy			
		2020/0042685	02/20	Tussy, et al.			
		2021/0011986	01/21	Tussy			

EXAMINER	DATE CONSIDERED

***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

FOREIGN PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION	
							YES	NO
		1388802	02/04	EP				
		1455297	09/04	EP				
		2005-287878	10/05	JP				
		2006-259923	09/06	JP				
		2006/130542	12/06	WIPO				
		2007-148968	06/07	JP				
		2007-304801	11/07	JP				
		2008/107002	09/08	WIPO				
		2007/119818	08/09	WIPO				
		20130097581	09/13	KR				
		2014-010686	01/14	JP				
		103593594	02/14	CN				
		2015/070320	05/15	WIPO				
		2017/100929	06/17	WIPO				
		10-1755995	07/17	KR				
		10-2019-0038923	04/19	KR				

EXAMINER INITIAL		**OTHER DOCUMENTS** (INCLUDING AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.)
		Hagai Aronowitz, et al., Multi-Modal Biometrics for Mobile Authentication, IJCB, 2014
		Silvio Barra, et al., FAME: Face Authentication for Mobile Encounter, IEEE, 2013
		Girija Chetty and Michael Wagner, “Automated lip feature extraction for liveness verification in audio-video authentication”, Human Computer Communication laboratory School of Information Sciences and Engineering, University of Canberra, Australia, Proc. Image and Vision Computer (2004), 1 January, 2004, 6 pages.
		Rogssignol, Joe. "How to customise the Lock screen in iOS 7." iDownloadBlog, posted January 11, 2014 (Retrieved from the internet 3/30/2016). Internet URL: <http: //www.idownloadblog.com/2014/01/11/how-to-theme-the-lock-screen-on-oos-7/>
		android_locked-out-PDF, screenshot, date unknown, author unknown.
		android-lock-screen1-PDF, screenshot, date unknown, author unknown.

EXAMINER	DATE CONSIDERED

***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

CWM-W-16209

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

EXAMINER INITIAL		**OTHER DOCUMENTS** (INCLUDING AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.)
		facetime-PDF, screenshot, date unknown, author unknown.
		BLETSKO et al., "Using Skin-Color Motion for 3D Face Modelling and Synthesis", September 6, 2003, WISP 2003, pages 295-299_
		image 9-PDF, screenshot, date unknown, author unknown.
		iphone-Facetime-PDF, screen shot, date unknown, author unknown.
		keyboard-PDF, screen shot, date unknown, author unknown.
		passcode-lock-PDF, screen shot, date unknown, author unknown.
		passcode-PDF, screen shot, date unknown, author unknown.
		screen Shot-PDF, screen shot, date unknown, author unknown.
		screenshot_2012-06-20-16-06-32-PDF, screen shot, date unknown, author unknown.
		topic_facetime_ios-PDF, screen shot, date unknown, author unknown.
		Shutterstock [online], 4 August 2014 [retried 24 July 2016]. Retrieved from the internet URL:http://www.tineye.com/search/543afefb8836762927558call587ce7f99a706ad/.,pic-199246373 stock phot male silhouette image.
		wp_ss_20130124_00071-PDF, screen shot, January 24, 2013, author unknown.
		After Effects Tutorial - 17 - Introduction to Masking, by thenewboston, uploaded 12/07/2008, youtube.com [online], [retrieved 06/15/2017]. Available from <URL:https://www.youtube.com/watch?v=kWd51xDqzlc>
		Optical Illusions - Animated GIF & JPG, dated 10/28/2013, plus.google.com [online], [retrieved 06/19/2017]. Available from internet <URL:https://plus.google.com/+Whak-Off/posts/CX4YhzXSQy2>
		The Universal Face Login for 5 Billion Smartphones, zoomlogin.com [online], [retrieved 06/19/2017]. Available from internet <URL:https://zoomlogin.com/>
		Wong, Yongkang, et al. "Patch-based probabilistic image quality assessment for face selection and improved video-based face recognition." CVPR 2011 WORKSHOPS. IEEE, 2011
		RAFALOVITCH, "Viewfinder Friends-idea for Facebook application", November 14, 2007, http://blog.outerthoughts.com/2007/11/viewfinder-friends-idea-for-facebook-application/, 5pages.
		KISHORE, "How to Add, Upload, and Tag Your Pictures and Photos in FaceBook", http://www.online-tech-tips.com/fun-stuff/how-to-add-upload-and-tag-your-pictures-and-photos-in-facebook/, August 11, 2007, 13 pages.
		BECKER et al., "Evaluation of Face Recognition Techniques for Application to Facebook", IEEE International conference on Automatic Face and Gesture Recognition, 2008, 6 pages.
		BAKER, "Google & Riya Face Recognition Photo Search", November 22, 2005, http://www.searchenginejournal.com/google-riya-face-recognition-photo-search/25501, 1 page_
		PONCE, "Riya, Photo Sharing with Face Recognition", October 28, 2005, http://www.ohgizmo.com/2005/10/28/riya-photo-sharing-with-face-recognition/, 2 pages_
		FACEBOOK, "Making Photo Tagging Easier", https://m.facebook.com/notes/facebook/making-photo-tagging-easier/467145887130/?_tn_=C&_rdr, 2 pages
		MICHELSON et al., "Auto-tagging the Facebook", 2006, http://cs229.stanford.edu/proj2006/MichelsonOrtizAutoTaggingTheFacebook.pdf, 5 pages.
		ARRINGTON, "First Screen Shots of Riya", October 26, 2005, http://techcrunch.com/2005/10/26/riya-prepares-tolaunch-alpha/, 10 pages
		ARRINGTON, "Ojos - Auto Name & Tag Your Photos", August 15, 2005, http://techcrunch.com/2005/08/31/ojos-auto-name-tag-your-photos/, 8 pages.

EXAMINER	DATE CONSIDERED

***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

CWM-W-16209

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE **INFORMATION DISCLOSURE CITATION BY APPLICANT** (USE SEVERAL SHEETS IF NECESSARY)	ATTY. DOCKET NO. FACETC.0082P	APPLICATION NO. 17/508,887
	INVENTOR(S) Kevin Alan Tussy	
	FILING DATE October 22, 2021	GROUP ART UNIT OPAP

EXAMINER INITIAL		**OTHER DOCUMENTS** (INCLUDING AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.)
		STONE, et al. "Autotagging Facebook: Social network context improves photo annotation," In Workshop on Internet Vision, 2008, 2 pages_
		SCHUON et al., "CS229 Project Report: Automated photo tagging in Facebook", December 2007, http://cs229. Stanford.edu/proj2007/SchuonRobertsonZou-AutomatedPhotoTaggingInFacebook.pdf, 5 pages.
		YADAV, "Facebook - The Complete Biography", August 25, 2006, http://mashable.com12006/08/25/facebook-protile/, 7 pages_
		UNKNOWN, "What does it mean to "tag" someones picture on facebook, whats the point of doing it?", November 28, 2007, https://answers.yahoo.com/question/index?qid=20071128123629AAY0DLP, 2 pages.
		Yang, et al., "Detecting Faces in Images: A Survey", January 2002, IEEE Trans. Pattern Analysis Machine Intelligence, 24(1), 2 pages
		Japan Patent Office ("JPO") Preliminary Report issued for Application No. JP2020-023503 on February 9, 2021

EXAMINER	DATE CONSIDERED
***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.	

CWM-W-16209

Electronic Acknowledgement Receipt

EFS ID:	44818708
Application Number:	17508887
International Application Number:	
Confirmation Number:	9577
Title of Invention:	FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS
First Named Inventor/Applicant Name:	Kevin Alan Tussy
Customer Number:	32856
Filer:	Chad W. Miller
Filer Authorized By:	
Attorney Docket Number:	FACETC.0082P
Receipt Date:	24-JAN-2022
Filing Date:	22-OCT-2021
Time Stamp:	22:51:46
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	CWMW16210TRANS.pdf	16941 0b8a21a956eed9f280ed14355a14d2d1b17b7287	no	1

Warnings:

Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	CWMW16209PTO1449.pdf	214786 b08626cce9d76898af23ab62adacb6d0ed39c14b	no	16
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Foreign Reference	REF1EP1388802.pdf	750815 082210c933a7c09edb2e4676f7ab8d2f1a937d64	no	18
Warnings:					
Information:					
4	Foreign Reference	REF2EP1455297.pdf	984816 f8930c419eecb70adceed0eac2352e22eecdf00b	no	19
Warnings:					
Information:					
5	Foreign Reference	REF3JP2005287878V2.pdf	4493073 f32d48c55e4411e04c1e5483be753396a8010d57	no	42
Warnings:					
Information:					
6	Foreign Reference	REF4JP2006259923V3.pdf	1541678 1a15d5c695ad926fd50e5b55ad3787fe621117f8	no	35
Warnings:					
Information:					
7	Foreign Reference	REF5WO2006130542.pdf	1470800 6bd67801adfaa3c3f142d2002278b0fe0b73e3b4	no	35
Warnings:					
Information:					
8	Foreign Reference	REF6JP2007148968V2.pdf	1240659 7c33a05e5288223da6fbd072e6d7f48c145fdfec	no	31
Warnings:					
Information:					

9	Foreign Reference	REF7JP2007304801V2.pdf	1487692 b8fd6a8e12256e7ded3255b0f6b55895652e2d16	no	42
Warnings:					
Information:					
10	Foreign Reference	REF8WO2008107002.pdf	1183596 a30508c994ff76b9f97eadb0a8c655d1ecb199d9	no	29
Warnings:					
Information:					
11	Foreign Reference	REF9WO2007119818.pdf	4204229 a2dc1e56db9ed93dcce2a1e1157397a1309e5530	no	46
Warnings:					
Information:					
12	Foreign Reference	REF10KR20130097581EngTrans.pdf	3067544 6c3f6c96388e39ab0fb4a6a253e0024751c22832	no	50
Warnings:					
Information:					
13	Foreign Reference	REF11JP2014010686V2.pdf	2852185 9b06026f0dfe2bf1b2d2b9461e5d1df1fb9896c5	no	60
Warnings:					
Information:					
14	Foreign Reference	REF12CN103593594EngTrans.pdf	3475260 2f23a005183a2b46f9d7de2b4f3156b9e8ce8969	no	40
Warnings:					
Information:					
15	Foreign Reference	REF13WO2015070320.pdf	7525397 45fd66d1ff90c6e72103d88ab8223474c7e7b02a	no	124
Warnings:					
Information:					

16	Foreign Reference	REF14WO2017100929.pdf	4215994 b085a75cfe9a52c6724ec54cf76424f84518d6aa	no	70
Warnings:					
Information:					
17	Foreign Reference	REF15KR2101755995.pdf	1484133 c36e813f7f37bbe1736dd3286df0509ea5a77a6a	no	46
Warnings:					
Information:					
18	Foreign Reference	REF16KR1020190038923v5.pdf	3115950 1b098fbca7b39b60867a3bb976f0d4947190cbcc	no	37
Warnings:					
Information:					
19	Non Patent Literature	REF1HagaiAronowitzMultimodal.pdf	708683 efc10a29a932cc47c80d1a4fa8ee4c2ab704dca3	no	8
Warnings:					
Information:					
20	Non Patent Literature	REF2SilvioBarraFAME.pdf	708495 d43c11d6861fe81dc6ea1767a496c506c89a15a7	no	7
Warnings:					
Information:					
21	Non Patent Literature	REF3GirijaChettyAutoLipFeatExtract.pdf	1054434 c7dab8ab2c006809c9eb693cf737ab02bf7bf25e	no	6
Warnings:					
Information:					
22	Non Patent Literature	REF4ROGSSIGNOL.pdf	1346214 2d639d084f34a906d7c2b6406a089b06adba2ff4	no	4
Warnings:					
Information:					

23	Non Patent Literature	REF5androidlockedoutPDF.pdf	126682 86fd39237e369a43bafb497681a55738579d94e6	no	1
Warnings:					
Information:					
24	Non Patent Literature	REF6androidlockscreen1PDF.pdf	357822 db4565b0e811eea91a712cc92ecbdc57775fec3d	no	1
Warnings:					
Information:					
25	Non Patent Literature	REF7facetimePDF2.pdf	704788 afc0819071dfb0d02ca1948e59dff78fd5a29b58	no	1
Warnings:					
Information:					
26	Non Patent Literature	REF8BletskoUsingSkinColor.pdf	455637 748ed4bf381e4cfdbecad78638bea7bceccab1a	no	2
Warnings:					
Information:					
27	Non Patent Literature	REF9image9PDF.pdf	44982 86dac3d9822823d6a62571b861342a1e92b0f137	no	1
Warnings:					
Information:					
28	Non Patent Literature	REF10iphoneFacetimePDF2.pdf	636230 95a856cda0b83c1527f4b3889f33b83a67645b8e	no	1
Warnings:					
Information:					
29	Non Patent Literature	REF11keyboardPDF2.pdf	867687 6f67af52de8bf8106d4cc1045f49ae623811ea37	no	1
Warnings:					
Information:					

30	Non Patent Literature	REF12passcodelockPDF.pdf	92641 f280e90eeae916478a361c9d3ffccba0fe73242b	no	1
Warnings:					
Information:					
31	Non Patent Literature	REF13passcodePDF.pdf	105836 095652321a53cdd6cf662cf8d2eb6e8ed8529490	no	1
Warnings:					
Information:					
32	Non Patent Literature	REF14screenshotPDF.pdf	271950 5b2f052c76883ed521abaf623e9f754ce097e7f5	no	1
Warnings:					
Information:					
33	Non Patent Literature	REF15screenshot20120620160632PDF.pdf	259196 337df3ef48b8eac82e57256c627c29edc5e9b599	no	1
Warnings:					
Information:					
34	Non Patent Literature	REF16topicfacetimeiosPDF2.pdf	645151 89670bd0eb0ded68a0b3a00f30aabfec704eef5b	no	1
Warnings:					
Information:					
35	Non Patent Literature	REF17ShutterstcokOnlinetTineye.pdf	396893 a09c3b6843aa1cde750c282f3fe1dff35fdfe01e	no	2
Warnings:					
Information:					
36	Non Patent Literature	REF18wpss2013012400071PDF.pdf	49869 5971474a1eb9f58ca1ab5dc690f84525118b4146	no	1
Warnings:					
Information:					

37	Non Patent Literature	REF19fterEffectsTutorial173.pdf	867537 139c2aee576ab2e0eeb0fe5b10e47e49318956ff	no	3
Warnings:					
Information:					
38	Non Patent Literature	REF20OpticalIllusionsAnimatedGIF.pdf	501054 434ee9dd06f65be2bee9c29eb62b626abe873d5c	no	3
Warnings:					
Information:					
39	Non Patent Literature	REF21TheUniversalFaceLoginFor5Billion.pdf	574465 cba681bd8d8c2112a23fb4989031208be636d96e	no	3
Warnings:					
Information:					
40	Non Patent Literature	REF22PatchBasedProbabilisticImageQuality.pdf	803052 48355fa9437cb1dd3f9baadcb395d55ad115d0bd	no	8
Warnings:					
Information:					
41	Non Patent Literature	REF23RafalovitchViewfinderFriendsIdeaForFacebook.pdf	144131 dce696578d4f656430d186eb5b7d0c0a8faf5eb1	no	5
Warnings:					
Information:					
42	Non Patent Literature	REF24KishoreHowToAddUploadAndTagYourPictures.pdf	877701 b47b5f70f2de40c9031286480bd523d3af2d866b	no	12
Warnings:					
Information:					
43	Non Patent Literature	REF25BeckerEvaluationofFaceRecognitionTechniques.pdf	78052 1b376ee5c3cd44c10f1ceca9502eb74dc16e94cc	no	2
Warnings:					
Information:					

44	Non Patent Literature	REF26BakerGoogleAndRiyaRecognition.pdf	631186 dc7c806db310a4d5cd17ca875ec6b07dc0f20ce8	no	10
Warnings:					
Information:					
45	Non Patent Literature	REF27PonceRiyaPhotoSharingWithFaceRecognition.pdf	498321 d56e63089b2c52a1940be9d2644d0e50e86ab976	no	3
Warnings:					
Information:					
46	Non Patent Literature	REF28FacebookMakingPhotoTaggingEasier.pdf	180994 e836ccace1cae545baabd362c243b057a85b7f99	no	2
Warnings:					
Information:					
47	Non Patent Literature	REF29MichelsonAutoTagging.pdf	317201 0716c0ffda73fc49eaade96c0ca8eeec9612738a	no	5
Warnings:					
Information:					
48	Non Patent Literature	REF30ArringtonFirstScreenShotsOfRiya.pdf	905717 3dca18d41d3134e27e841f47b735428142472130	no	10
Warnings:					
Information:					
49	Non Patent Literature	REF31ArringtonOjosAutoNameAndTagYourPhotos.pdf	744168 a5fca50a4015948ea0ae168f6a7bd97a7f4810c7	no	9
Warnings:					
Information:					
50	Non Patent Literature	REF32StoneAutotaggingFacebook.pdf	844249 6d95990d3ca9add1db6e61935e7cbf423d110115	no	8
Warnings:					
Information:					

51	Non Patent Literature	REF33SchuonCS229ProjectReport.pdf	284691 034fd7a9d9ffe242b08ef25814ea7fc5ecc1256e	no	5
Warnings:					
Information:					
52	Non Patent Literature	REF34YadavFacebookTheCompleteAutobiography.pdf	2257507 3f250f052214759dd0bc8830c0e350950c90dc31	no	12
Warnings:					
Information:					
53	Non Patent Literature	REF35UnknownWhatDoesItMeanToTag.pdf	264516 a994e1db2447a0fdaa93954b36a8ba4fbb1a5c86	no	2
Warnings:					
Information:					
54	Non Patent Literature	REF36YangDetectingFacesInImagesASurvey.pdf	2077629 d182b80eb548161f0e323cd94a6843d45fda3703	no	25
Warnings:					
Information:					
55	Non Patent Literature	REF37JPOPrelimRprtJP2020023503V2.pdf	161248 7f0218602c03c528a0ea64063f696aebd39a8ebe	no	7
Warnings:					
Information:					
			Total Files Size (in bytes):	65172157	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor	:	Kevin Alan Tussy	Group Art Unit: OPAP
App. No.	:	17/508,887	
Filed	:	October 22, 2021	
For	:	FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS	
Examiner	:	Central Docket	

I hereby certify that this correspondence and all marked attachments are being deposited with the United States Patent and Trademark Office via EFSWeb, on:

January 24, 2022
(Date)

/Chad W. Miller/
Chad W. Miller, Reg. No. 44,943

INFORMATION DISCLOSURE STATEMENT

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Enclosed is form PTO-1449 listing 336 U.S. references, copies of which are not required to be provided in accordance with 37 C.F.R. §1.98(e), 16 foreign references and 37 publications. This Information Disclosure Statement is being filed before the mailing of the first Office Action on the merits, and as such, no fee is required in accordance with 37 C.F.R. §1.97(b)(3).

Respectfully submitted,

Dated: January 24, 2022

By: /Chad W. Miller/

Chad W. Miller
Attorney for Applicant
Weide & Miller, Ltd.
Registration No. 44,943
10655 Park Run Drive, Suite 100
Las Vegas, NV 89144
Tel. (702) 382-4804 (Pacific Time)
cmiller@weidemiller.com

CWM-W-16210

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor	:	Kevin Alan Tussy	Group Art Unit: OPAP
Appl. No.	:	17/508,887	
Filed	:	October 22, 2021	
For	:	FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETER	
Examiner	:	Central Docket	

I hereby certify that this correspondence and all marked attachments are being deposited with the United States Patent Office via EFSWeb filing, on:

November 12, 2021
(Date)

/Chad W. Miller/
Chad W. Miller Reg. No. 44,943

PRELIMINARY AMENDMENT

Mail Stop Amendment
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This Preliminary Amendment is for entry into the above-referenced application. Please amend the above-referenced application as follows:

IN THE CLAIMS:

1. (original) A computing device for verifying three-dimensionality of a user via a user's camera equipped computing device, the computing device comprising:

a processor configured to execute machine executable code;

a screen configured to provide a user interface to the user;

a camera configured to capture images;

one or more memories configured to store machine readable instructions that are stored on the memory of the authentication server which when executed by the processor, cause the computing device to:

capturing at least one first image of the user taken with the camera of the computing device at a first location which is a first distance from the user;

processing the at least one first image or a portion thereof to create first data;

capturing at least one second image of the user taken with the camera of the computing device is at a second distance from the user, the second distance being different than the first distance, the capturing at least one second image of the user occurring after movement of the camera or the user to establish the camera at the second distance from the user;

processing the at least one second image or a portion thereof to create second data;

comparing the first data to the second data to determine whether expected differences exist between the first data and the second data which indicates three-dimensionality of the user;

verifying the images of the user exhibit three dimensional traits when the expected differences exist between the first data and the second data as a result of capturing the at least one first image and the at least one second image at different distances from the user.

2. (original) The system according to claim 1, further comprising:

interpolating the first data and the second data to obtain estimated intermediate data;

capturing at least one third image of the user taken with the camera of the computing device at a third distance from the user, the third distance being between the first distance and the second distances;

processing the at least one third image or a portion thereof to obtain third data; and

comparing the estimated intermediate data with the third data to determine whether the third data matches the estimated intermediate data.

3. (original) The system according to claim 1, further comprising verifying the presence of one or more features on a side of a user's head in the at least one first image, and verifying the absence or reduced visibility of the one or more features on the side of the user's head in the at least one second image due to image capture at different distances from the user's head, wherein the first distance is larger than the second distance.

4. (original) The system according to claim 1, wherein the machine readable instructions is configured to display one or more prompts on the screen of the computing device to guide the user to capture the at least one first image at the first distance and the at least on second image at the second distance.

5. (original) The system according to claim 1, further comprising comparing the first data, second data, or both to enrollment data derived from an enrollment image, the enrollment image captured and stored prior to an authenticating; and

only authenticating the user when the first data, the second data, or both match the enrollment data within a predetermined threshold.

6. (original) The system according to claim 1, wherein the computing device is a hand-held device, and the user holds the device at the first and second distance to capture the at least one first image and the at least one second image.

7. (original) The system according to claim 1, wherein the first data and the second data comprise biometric data.

8. (original) The system according to claim 1, wherein the first data and the second data comprise a mapping of facial features.

9. (original) The method according to claim 1, wherein the first image and the second image is of the user's face and the user's head and facial features are held steady and without movement during capture of the first image and the second image.

10. (original) A method for authenticating three-dimensionality of a user with a computing device during an authentication session, the method comprising:

capturing at least one first image of the user taken with a camera at a first location which is a first distance from the user, the camera associated with the computing device;

processing the at least one first image or a portion thereof to create first data;

moving the camera from the first location to a second location, the second location being a second distance from the user, or the user moving to change the distance between the user and the camera from the first distance to the second distance;

capturing at least one second image of the user taken with the camera associated with the computing device when the camera is the second distance from the user, the second distance being different than the first distance;

processing the at least one second image or a portion thereof to create second data;

comparing the first data to the second data to determine whether expected differences exist between the first data and the second data which indicated three-dimensionality of the user;

verifying the images of the user exhibit three-dimensional traits when the first data and the second data have expected differences resulting from the at least one first image being captured at a different distance from the user than when the at least one second image is captured.

11. (original) The method according to claim 10, further comprising:

interpolating the first data and the second data to obtain estimated intermediate data;

capturing at least one third image of the user taken with the camera of the computing device at a third distance from the user, the third distance being between the first distance and the second distances;

processing the at least one third image or a portion thereof to obtain third data; and

comparing the estimated intermediate data with the third data to determine whether the third data matches the estimated intermediate data.

12. (original) The method according to claim 10, further comprising verifying the presence of ears of the user in the at least one first image, and verifying the absence or reduced visibility of the ears in the at least one second image, wherein the first distance is larger than the second distance.

13. (original) The method according to claim 10, wherein the computing device is configured to display one or more prompts on a screen associated with the computing device to guide the user to capture the at least one first image at the first distance and the at least on second image at the second distance.

14. (original) The method according to claim 13, wherein the one or more prompts are an oval shape guide on the screen within which an image of a face of the user is aligned to capture the at least one first image and the at least one second image.

15. (original) The method according to claim 10, wherein the computing device is a hand-held device, and the user holds the computing device at the first distance when capturing at least one first image and at the second distances when capturing the at least one second image.

16. (original) The method according to claim 10, wherein the first data and the second data comprise biometric data.

17. (original) The method according to claim 10, wherein the first data and the second data comprise a mapping of facial features.

18. (original) The method according to claim 10, further comprising illuminate a screen of the computing device while capturing the at least one first image and/or the at least one second image, and processing the at least one first image and/or the at least one second image to detect a reflection of the illumination from a face of the user.

19. (original) The method according to claim 10, wherein a face of the user is held steady when capturing the at least one first image and the at least one second image and the camera moves from the first location to the second location.

20. (original) The method according to claim 10, wherein the first data and the second data are maintained on the computing device.

21. (original) The method of claim 10 wherein the computing device is one of a smartphone, tablet, laptop, or desktop computer.

22. (new) A method, performed by a user using a user's computer device, for verifying three-dimensionality of the user, the method comprising:

capturing a first image of the user's head with a camera at a first distance from the user, the camera associated with the user's computing device;

changing a distance between the user and the camera to a second distance by the user moving the camera, or the user moving relative to the camera, or both;

capturing a second image of the user's head with the camera when the camera is at the second distance from the user, the second distance being different than the first distance;

comparing one or more aspects of the user's head from the first image to one or more aspects of the user's head from the second image to determine whether expected differences, between the first image and the second image, exist which indicates three-dimensionality of the user, such that the expected differences between the first image and the second image result from the first image being captured when the camera is at a different distance from the user than when the second image is captured; and

responsive to the comparing determining that expected differences between the first image and the second image exist, providing notice to the user, a third party, or both that the three-dimensionality of the user is verified.

23. (new) The method of claim 22 wherein the one or more aspects of the user's head from the first image is first data resulting from processing the first image and the one or more aspects of the user's head from the second image is second data resulting from processing the second image.

24. (new) The method of claim 22 wherein the user's head is the user's face.

REMARKS

In this Preliminary Amendment, Applicant requests entry of the additional claims set forth above. No new matter is added.

CONCLUSION

Given the foregoing, the Applicant asserts that the claims are in a condition for allowance and respectfully requests a notice as to the same. If any matters remain outstanding, the Examiner is invited to contact the undersigned by telephone and is hereby authorized to contact the undersigned by email.

Respectfully submitted,

Dated: November 12, 2021

By: /Chad W. Miller/
Chad W. Miller
Attorney of Record
Registration No. 44,943
Weide & Miller, Ltd.
10655 Park Run Drive, Suite 100
Las Vegas, NV 89144
(702) 382-4804 (Pacific Time)
cmiller@weidemiller.com

Electronic Patent Application Fee Transmittal

Application Number:	17508887
Filing Date:	22-Oct-2021
Title of Invention:	FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS
First Named Inventor/Applicant Name:	Kevin Alan Tussy
Filer:	Chad W. Miller
Attorney Docket Number:	FACETC.0082P

Filed as Small Entity

Filing Fees for **Utility under 35 USC 111(a)**

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
CLAIMS IN EXCESS OF 20	2202	3	50	150
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**150**

Electronic Acknowledgement Receipt

EFS ID:	44274701
Application Number:	17508887
International Application Number:	
Confirmation Number:	9577
Title of Invention:	FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS
First Named Inventor/Applicant Name:	Kevin Alan Tussy
Customer Number:	32856
Filer:	Chad W. Miller
Filer Authorized By:	
Attorney Docket Number:	FACETC.0082P
Receipt Date:	12-NOV-2021
Filing Date:	22-OCT-2021
Time Stamp:	19:24:06
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$150
RAM confirmation Number	E2021ABJ25171310
Deposit Account	502200
Authorized User	Chad Miller

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.21 (Miscellaneous fees and charges)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.16 (National application filing, search, and examination fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		CWMW16061PRELIMAMEND.pdf	43993 fca9637489803d194602ba7ef04d33df99994fb5	yes	8

Multipart Description/PDF files in .zip description

Document Description	Start	End
Preliminary Amendment	1	1
Claims	2	7
Applicant Arguments/Remarks Made in an Amendment	8	8

Warnings:

Information:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
2	Fee Worksheet (SB06)	fee-info.pdf	37597 bfd8f36907f1a6c0e22470d41f75bc49c0a5e039	no	2

Warnings:

Information:

Total Files Size (in bytes): 81590

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 17/508,887	Filing Date 10/22/2021	☐ To be Mailed

ENTITY: ☐ LARGE ☑ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

	(Column 1)	(Column 2)			
FOR	NUMBER FILED	NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $50 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $240 =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT	11/12/2021	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 24	Minus	** 21	= 3		x $50 =	150
	Independent (37 CFR 1.16(h))	* 3	Minus	*** 3	= 0		x $240 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	150

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=		x $0 =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=		x $0 =	
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.	LDRC
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/EVA V GILLIS/
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".	
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.	

PATENT APPLICATION FEE DETERMINATION RECORD
Substitute for Form PTO-875

Application or Docket Number
17/508,887

APPLICATION AS FILED - PART I

FOR	NUMBER FILED (Column 1)	NUMBER EXTRA (Column 2)	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	80		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	350		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	400		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	21 minus 20 =	* 1	x 50 =	50	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	2 minus 3 =	*	x 240 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
			TOTAL	880		TOTAL	

* If the difference in column 1 is less than zero, enter "0" in column 2.

APPLICATION AS AMENDED - PART II

AMENDMENT A

	CLAIMS REMAINING AFTER AMENDMENT (Column 1)		HIGHEST NUMBER PREVIOUSLY PAID FOR (Column 2)	PRESENT EXTRA (Column 3)	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
Application Size Fee (37 CFR 1.16(s))									
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

AMENDMENT B

	CLAIMS REMAINING AFTER AMENDMENT (Column 1)		HIGHEST NUMBER PREVIOUSLY PAID FOR (Column 2)	PRESENT EXTRA (Column 3)	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
Application Size Fee (37 CFR 1.16(s))									
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
17/508,887	10/22/2021	2144	880	FACETC.0082P	21	2

CONFIRMATION NO. 9577

FILING RECEIPT

OC000000129301535

32856
WEIDE & MILLER, LTD.
10655 PARK RUN DRIVE
SUITE 100
LAS VEGAS, NV 89144

Date Mailed: 11/02/2021

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

Kevin Alan Tussy, Las Vegas, NV;

Applicant(s)

FaceTec, Inc., Las Vegas, NV;

Power of Attorney: The patent practitioners associated with Customer Number 000032856

Domestic Priority data as claimed by applicant

This application is a CON of 16/817,428 03/12/2020 PAT 11157606
which is a CON of 15/900,681 02/20/2018 PAT 10614204
which claims benefit of 62/460,670 02/17/2017
and is a CIP of 14/839,505 08/28/2015 PAT 9953149
which claims benefit of 62/043,224 08/28/2014
and claims benefit of 62/054,847 09/24/2014
and claims benefit of 62/064,415 10/15/2014
and claims benefit of 62/085,963 12/01/2014
and claims benefit of 62/101,317 01/08/2015
and claims benefit of 62/139,558 03/27/2015
and claims benefit of 62/188,584 07/03/2015

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 11/01/2021
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 17/508,887**
Projected Publication Date: 02/10/2022
Non-Publication Request: No
Early Publication Request: No
**** SMALL ENTITY ****
Title

FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS

Preliminary Class

715

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

PTO/AIA/82A (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	
Filing Date	October 22, 2021
First Named Inventor	Kevin Alan Tussy
Title	FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS
Art Unit	Unknown
Examiner Name	Unknown
Attorney Docket Number	FACETC.0082P

SIGNATURE of Applicant or Patent Practitioner

Signature	/Chad W. Miller/	Date (Optional)	
Name	Chad W. Miller	Registration Number	44,943
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)			

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ *Total of ____________ forms are submitted.

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)

☑ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above: 000032856

OR

☐ I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter or the boxes above to:

☑ The address associated with the above-mentioned Customer Number

OR

☐ The address associated with Customer Number:

OR

Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

FACETEC, INC.

☐ Inventor or Joint Inventor (title not required below)

☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)

☑ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)

☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature		Date (Optional)	
Name	Kevin Alan Tussy		
Title	President for FaceTec, Inc.		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ Total of forms are submitted.

FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS

INVENTOR

KEVIN ALAN TUSSY

BACKGROUND

1. Field

[0001] The disclosed embodiments relate to biometric security. More specifically, the disclosed embodiments relate to facial recognition authentication systems.

2. Related Art

[0002] With the growth of personal electronic devices that may be used to access several user accounts, and the increasing threat of identity theft and other security issues, there is a growing need for ways to securely access user accounts via electronic devices. Account holders are thus often required to have longer passwords that meet various criteria such as using a mixture of capital and lowercase letters, numbers, and other symbols. With smaller electronic devices, such as smart phones, smart watches, “Internet of Things” (“IoT’) devices and the like, it may become cumbersome to attempt to type such long passwords into the device each time access to the account is desired. In some instances, users may even decide to deactivate such cumbersome security measures due to their inconvenience on their devices. Thus, users of such devices may prefer other methods of secure access to their user accounts.

[0003] One other such method may be using biometrics. For example, an electronic device may have an optical reader that may scan a user’s fingerprint to determine that the person requesting access to a device or an account is authorized. However, such fingerprint systems are often prohibitively large and expensive for use on an inexpensive electronic device and are often considered unreliable and unsecure.

[0004] In addition, facial recognition is generally known and may be used in a variety of contexts. Two-dimensional facial recognition is commonly used to tag people in images on social networks or in photo editing software. Facial recognition software, however, has not been widely implemented on its own to securely authenticate users attempting to gain access to an account because it not considered secure enough. For example, two-dimensional facial recognition is considered unsecure because faces may be photographed or recorded, and then the resulting prints or video displays showing images of the user may be used to spoof the system. Accordingly, there is a need for reliable, cost-effective, and convenient method to authenticate users attempting to log in to, for example, a user account.

SUMMARY

[0005] The disclosed embodiments have been developed in light of the above and aspects of the invention may include a method for enrolling and authenticating a user in an authentication system via a user's computing device. The user's device includes a camera and, in some instances, includes at least one movement detecting sensor, such as an accelerometer, magnetometer, and gyroscope, or the camera is used for this function.

[0006] In one embodiment, the user may enroll in the system by providing enrollment images of the user's face. The enrollment images are taken by the camera of the mobile device as the user moves the mobile device to different positions relative to the user's head. The user may thus obtain enrollment images showing the user's face from different angles and distances. The system may also utilize one or more movement sensors of a mobile device to determine an enrollment movement path that the phone takes during the imaging. At least one image is processed to detect the user's face within the image, and to obtain biometric information from the user's face in the image. The image processing may be done on the user's mobile device or at a remote device, such as an authentication server or a user account server. The enrollment information (the enrollment biometrics, movement, and other information) may be stored on the mobile device or remote device.

[0007] The system may then authenticate a user by the user providing at least one authentication image via the camera of the mobile device while the user moves the mobile device to different positions relative to the user's head. In other embodiments, multiple authentication images may be required. In some examples, the user may move his or her face to different positions relative to the camera of the computing device or move the camera to a different position relative to their face. The authentication images are processed for face detection and facial biometric information. Path parameters are also obtained during the imaging of the authentication images (authentication movement). The authentication information (authentication biometric, movement, and other information) is then compared with the enrollment information to determine whether the user should be authenticated or denied. Image processing and comparison may be conducted on the user's mobile device, or may be conducted remotely.

[0008] In some embodiments, multiple enrollment profiles may be created by a user to provide further security. For example, a user may create an enrollment wearing accessories such as a hat or glasses, or while making a funny face. In further embodiments, the user's enrollment information may be linked to a user email address, phone number, or other identifier.

[0009] The authentication system may include feedback displayed on the mobile device to aid a user in learning and authentication with the system. For instance, an accuracy meter may provide feedback on a match rate of the authentication biometrics or movement. A movement meter may provide feedback on the movement detected by the mobile device.

[0010] In some embodiments, the system may reward users who successfully utilize the authentication system or who otherwise take fraud preventing measures. Such rewards may include leaderboards, status levels, reward points, coupons or other offers, and the like. In some embodiments, the authentication system may be used to login to multiple accounts.

[0011] In addition to biometric and movement matching, some embodiments may also utilize banding detection, glare detection, and screen edge detection to further secure the system. In other embodiments, other user attributes may be detected and matched including users' gender, age, ethnicity, and the like.

[0012] The system may also provide gradual access to user account(s) when the user first sets up the authentication system. As the user successfully implements the system, authorization may be expanded. For example, during a time period as the user gets accustomed to the authentication system, lower transaction limits may be applied.

[0013] In some embodiments, the mobile device may show video feedback of what the user is imaging to aid the user to image his or her face during enrollment or authentication. The video feedback may be displayed on only a portion of the display screen of the mobile device. For example, the video feedback may be displayed in an upper portion of the display screen. The video feedback display may be position on a portion of the display screen that corresponds with a location of a front-facing camera of the mobile device.

[0014] To facilitate imaging in low-light, portions of the screen other than the video feedback may be displayed in a bright color, such as white. In some embodiments, and LED or infrared light may be used, and near infrared thermal imaging may be done with an infrared camera. The mobile device used for imaging may thus have multiple cameras for capture visible light and infrared images. The mobile device may also have multiple cameras (two or more) imaging in a single spectrum or multiple spectrum to provide stereoscopic, three-dimensional images. In such an embodiment, the close-up frames (zoomed) may create the most differentiation as compared to images captured from a distance. In such an embodiment, the frames captured at a distance may be unnecessary.

[0015] In some embodiments, to provide added security, the mobile device may output objects, colors, or patterns on the display screen to be detected during the imaging. The predetermined object or pattern may be a unique one-dimensional or two-dimensional barcode. For example, a QR code (two-dimensional barcode) may be displayed on the screen and reflected off the user's eye. If the QR code is detected in the image, then the person may be authenticated. In other embodiments, an object may move on the screen and the system may detect whether a user's eyes follow the movement.

[0016] In some embodiments, the system may provide prompts on a video feedback display to aid the user in moving the device relative to the user's head during enrollment and/or authentication. The prompts may include ovals or frames displayed on the display screen in which the user must place his or her face by moving the mobile device until his or her face is within the oval or frame. The prompts may preferably be of differing sizes and may also be centered on different positions of the screen. When an actual, three-dimensional person images himself or herself close up and far away, it has been found that the biometric results are different due to perspective distortion as compared to when a spoof attempt is made using two-dimensional pictures that include imaged pictures of the person both close up and far away. Thus, a three-dimensional person may be validated when biometric results show differences in perspective distortion in the close-up and far away images. This also allows the user to have multiple biometric profiles for each of the distances.

[0017] In other embodiments, biometrics from images obtained between the close-up and far away images may be analyzed for incrementally different biometric results. In this manner, the morphing of the face from the far face to the warped close up face is captured and tracked. The incremental frames during an authentication may then be matched to frames captured at similar locations during enrollment along the motion path and compared to ensure that the expected similarities and difference are found. This results in a motion path and captured image and biometric data that can prove a three-dimensional face is presently being imaged. Thus, not only are the close-up and far away biometrics compared, but also biometric data obtained in between. The biometric data obtained in between must also correspond to a correct morphing speed along the motion path, greatly enhancing the security of the system.

[0018] The touch screen may be utilized in some embodiments. For example, the user may need to enter a swipe a particular code or pattern in addition to the authentication system described herein. The touchscreen may also detect a size and orientation of a user's finger, and whether a right hand or a left hand is used on the touch screen. Voice parameters may also be used as an added layer of security. The system may detect edge sharpness or other indicators to ensure that the obtained images are of sufficient quality for the authentication system.

[0019] When a camera has an autofocus, the autofocus may be controlled by the system to validate the presence of the actual, three-dimensional person. The autofocus may check that different features of the user or environment focus at different focus points, which also may be referred to as focal lengths. This disclosure covers both focus points and focal length. In other embodiments, authentication images may be saved to review the person who attempted to authenticate with the system.

[0020] In some embodiments, the match thresholds required may be adapted over time. The system may thus account for changing biometrics due to age, weight gain/loss, environment, user experience, security level, or other factors. In further embodiments, the system may utilize image distortion prior to obtaining biometric information to further protect against fraudulent access.

[0021] The system may utilize any number or combination of the security features as security layers, as described herein. When authentication fails, the system may be configured so that it is unclear which security layer triggered the failure to preserve the integrity of the security system.

[0022] Other systems, methods, features and advantages of the invention will be or will become apparent to one with skill in the art upon examination of the following figures and detailed description. It is intended that all such additional systems, methods, features and advantages be included within this description, be within the scope of the invention, and be protected by the accompanying claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0023] The components in the figures are not necessarily to scale, emphasis instead being placed upon illustrating the principles of the invention. In the figures, like reference numerals designate corresponding parts throughout the different views.

[0024] Figure 1 illustrates an example environment of use of the facial recognition authentication system, according to one exemplary embodiment.

[0025] Figure 2 illustrates an example embodiment of a mobile device.

[0026] Figure 3 illustrates exemplary software modules that are part of the mobile device and server.

[0027] Figure 4 shows a method for performing facial recognition authentication according to one embodiment.

[0028] Figure 5 shows a method for enrolling a user in a facial recognition authentication system, according to one exemplary embodiment.

[0029] Figures 6A and 6B show an example of movement of a mobile device about a user's face according to one exemplary embodiment.

[0030] Figures 7A and 7B show an example of movement of a mobile device about a user's face according to one exemplary embodiment.

[0031] Figure 8 shows a method of providing authentication information in a facial recognition authentication system, according to one exemplary embodiment.

[0032] Figure 9 shows a method of verifying authentication credentials in a facial recognition authentication system, according to one exemplary embodiment.

[0033] Figure 10 illustrates an exemplary display showing a graphical and numeric feedback in a facial recognition authentication system.

[0034] Figures 11A, 11B, and 11C illustrate exemplary video feedback displays corresponding to front-facing camera positions in a facial recognition authentication system.

[0035] Figure 12 shows an exemplary video display feedback of a facial recognition authentication system where edge pixels on the sides of the display are stretched horizontally.

[0036] Figures 13A and 13B illustrates exemplary screen displays with face alignment indicators shown as an oval to serve as a guide as the user moves the mobile device closer to or away from their face.

[0037] Figure 14 shows a method of verifying liveness or three-dimensionality of a user utilizing pixel velocity analysis detection.

[0038] Figure 15 illustrates an exemplary mobile device display showing a graphical code entry interface with an imaging area.

[0039] Figure 16 illustrates an example mobile device display showing a numeric and graphical code entry interface with an imaging area.

DETAILED DESCRIPTION OF EMBODIMENTS

[0040] A system and method for providing secure and convenient facial recognition authentication will be described below. The system and method may be achieved without the need for additional expensive biometric readers or systems while offering enhanced security over conventional facial recognition systems.

Facial Recognition Authentication Environment

[0041] Figure 1 illustrates an example environment of use of the facial recognition authentication system described herein. This is but one possible environment of use and system. It is contemplated that, after reading the specification provided below in connection with the figures, one of ordinary skill in the art may arrive at different environments of use and configurations.

[0042] In this environment, a user 108 may have a mobile device 112 which may be used to access one or more of the user's accounts via authentication systems. A user 108 may have a mobile device 112 that can capture a picture of the user 108, such as an image of the user's face. The user may use a camera 114 on or connected to the mobile device 112 to capture an image or multiple images or video of himself or herself. The mobile device 112 may comprise any type of mobile device capable of capturing an image, either still or video, and performing processing of the image or communication over a network.

[0043] In this embodiment, the user 108 may carry and hold the mobile device 112 to capture the image. The user may also wear or hold any number of other devices. For, example, the user may wear a watch 130 containing one or more cameras 134 or biosensors disposed on the watch. The camera 134 may be configured to create an image from visible light as well as infrared light. The camera 134 may additionally or alternatively employ image intensification, active illumination, or thermal vision to obtain images in dark environments.

[0044] When pointed towards a user 108, the camera 134 may capture an image of the user's face. The camera 134 may be part of a module that may either include communication capability that communicates with either a mobile device 112, such as via Bluetooth®, NFC, or other format, or communication directly with a network 116 over a wired or wireless link 154. The watch 130 may include a screen on its face to allow the user to view information. If the camera module 134 communicates with the mobile device 112, the mobile device 134 may relay communications to the network 116. The mobile device 134 may be configured with more than one front facing camera 114 to provide for a 3D or stereoscopic view, or to obtain images across different spectral ranges, such as near infrared and visible light.

[0045] The mobile device 112 is configured to wirelessly communicate over a network 116 with a remote server 120. The server 120 may communicate with one or more databases 124. The network 116 may be any type of network capable of communicating to and from the mobile device including but not limited to a LAN, WAN, PAN, or the Internet. The mobile device 112 may communicate with the network via a wired or wireless connection, such as via Ethernet, Wi-Fi, NFC, and the like. The server 120 may include any type of computing device capable of communicating with the mobile device 112. The server 120 and mobile device 112 are configured with a processor and memory and are configured to execute machine readable code or machine instructions stored in the memory.

[0046] The database 124, stored on mobile device or remote location as shown, may contain facial biometric information and authentication information of users 108 to identify the users 108 to allow access to associated user data based on one or more images or biometric information received from the mobile device 112 or watch 134. The data may be, for example, information relating to a user account or instruction to allow access to a separate account information server 120B. The term biometric data may include among other information biometric information concerning facial features (distorted or undistorted) and path parameters. Examples of path parameters may include an acceleration and speed of the mobile device, angle of the mobile device during image capture, distance of the mobile device to the user, path direction in relation to the user's face position in relation to the user, or any other type parameter associated with movement of the mobile device or the user face in relation to a camera. Other data may also be included such as GPS data, device identification information, and the like.

[0047] In this embodiment, the server 120 processes requests for identification from the mobile device 112 or user 108. In one configuration, the image captured by the mobile device 112, using facial detection, comprises one or more images of the user's face 108 during movement of the mobile device relative to the user's face, such as in a side to side or horizontal arc or line, vertical arc or line, forward and backwards from the user's face, or any other direction of motion. In another configuration, the mobile device 112 calculates biometric information from the obtained images and sends the biometric information to the server 120. In yet another embodiment, the mobile device 112 compares biometric information with stored biometric information on the mobile device 112 and sends an authentication result from the comparison to the server 120.

[0048] The data including either the image(s), biometric information, or both are sent over the network 116 to the server 120. Using image processing and image recognition algorithms, the server 120 processes the person's biometric information, such as facial data, and compares the biometric information with biometric data stored in the database 124 to determine the likelihood of a match. In other embodiments, the image processing and comparison is done on the mobile device 112, and data sent to the server indicates a result of the comparison. In further embodiments, the image processing and comparison is done on the mobile device 112 without accessing the server, for example, to obtain access to the mobile device 112 itself.

[0049] By using facial recognition processing, an accurate identity match may be established. Based on this and optionally one or more other factors, access may be granted, or an unauthorized user may be rejected. Facial recognition processing is known in the art (or is an established process) and as a result, it is not described in detail herein.

[0050] Also shown is a second server 120B with associated second database 124B, and third server 120C with associated third database 124C. The second and third database may be provided to contain additional information that is not available on the server 120 and database 124. For example, one of the additional servers may only be accessed based on the authentication of the user 108 performed by the server 120.

[0051] Executing on the mobile device 112 is one or more software applications. This software is defined herein as an identification application (ID App). The ID App may be configured with either or both of facial detection and facial recognition and one or more software modules which monitor the path parameters and/or biometric data. Facial detection as used herein refers to a process which detects a face in an image. Facial recognition as used herein refers to a process that can analyze a face using an algorithm, mapping its facial features, and converting them to biometric data, such as numeric data. The biometric data can be compared to that derived from one or more different images for similarities or dis-similarities. If a high percentage of similarity is found in the biometric data, the individual shown in the images may be considered to be a match.

[0052] With the ultimate goal of matching a face of a user to an identity or image stored in a database 124, to authenticate the user, the ID App may first process the image captured by the camera 114, 134 to identify and locate the face that is in the image. As shown in Figure 1, there may be the face 108. The authentication may be used for logging into an online account or for numerous other access control functions.

[0053] The portion of the photo that contains the detected face may then be cropped, cut, and stored for processing by one or more facial recognition algorithms. By first detecting the face in the image and cropping only that portion of the face, the facial recognition algorithm need not process the entire image. Further, in embodiments where the facial recognition processing occurs remotely from the mobile device 112, such as at a server 120, much less image data is required to be sent over the network to the remote location. It is contemplated that the entire image, a cropped face, or only biometric data may be sent to the remote server 120 for processing.

[0054] Facial detection software can detect a face from a variety of angles. However, facial recognition algorithms are most accurate in straight on images in well-lit situations. In one embodiment, the highest quality face image for facial recognition that is captured is processed first, then images of the face that are lower quality or at different angles other than straight toward the face are then processed. The processing may occur on the mobile device or at a remote server which has access to large databases of image data or facial identification data.

[0055] The facial detection is preferred to occur on the mobile device and is performed by the mobile device software, such as the ID App. This reduces the number or size of images (data) that are sent to the server for processing where faces are not found and minimizes the overall amount of data that must be sent over the network. This reduces bandwidth needs and network speed requirements are reduced.

[0056] In another preferred embodiment, the facial detection, facial recognition, and biometric comparison all occur on the mobile device. However, it is contemplated that the facial recognition processing may occur on the mobile device, the remote server, or both.

[0057] Figure 2 illustrates an example embodiment of a mobile device. This is but one possible mobile device configuration and as such it is contemplated that one of ordinary skill in the art may differently configure the mobile device. The mobile device 200 may comprise any type of mobile communication device capable of performing as described below. The mobile device may comprise a PDA, cellular telephone, smart phone, tablet PC, wireless electronic pad, an IoT device, a "wearable" electronic device or any other computing device.

[0058] In this example embodiment, the mobile device 200 is configured with an outer housing 204 configured to protect and contain the components described below. Within the housing 204 is a processor 208 and a first and second bus 212A, 212B (collectively 212). The processor 208 communicates over the buses 212 with the other components of the mobile device 200. The processor 208 may comprise any type processor or controller capable of performing as described herein. The processor 208 may comprise a general-purpose processor, ASIC, ARM, DSP, controller, or any other type processing device. The processor 208 and other elements of the mobile device 200 receive power from a battery 220 or other power source. An electrical interface 224 provides one or more electrical ports to electrically interface with the mobile device, such as with a second electronic device, computer, a medical device, or a power supply/charging device. The interface 224 may comprise any type electrical interface or connector format.

[0059] One or more memories 210 are part of the mobile device 200 for storage of machine readable code for execution on the processor 208 and for storage of data, such as image data, audio data, user data, medical data, location data, accelerometer data, or any other type of data. The memory 210 may comprise RAM, ROM, flash memory, optical memory, or micro-drive memory. The machine-readable code as described herein is non-transitory.

[0060] As part of this embodiment, the processor 208 connects to a user interface 216. The user interface 216 may comprise any system or device configured to accept user input to control the mobile device. The user interface 216 may comprise one or more of the following: keyboard, roller ball, buttons, wheels, pointer key, touch pad, and touch screen. A touch screen controller 230 is also provided which interfaces through the bus 212 and connects to a display 228.

[0061] The display comprises any type display screen configured to display visual information to the user. The screen may comprise a LED, LCD, thin film transistor screen, OEL CSTN (color super twisted nematic), TFT (thin film transistor), TFD (thin film diode), OLED (organic light-emitting diode), AMOLED display (active-matrix organic light-emitting diode), capacitive touch screen, resistive touch screen or any combination of these technologies. The display 228 receives signals from the processor 208 and these signals are translated by the display into text and images as is understood in the art. The display 228 may further comprise a display processor (not shown) or controller that interfaces with the processor 208. The touch screen controller 230 may comprise a module configured to receive signals from a touch screen which is overlaid on the display 228.

[0062] Also part of this exemplary mobile device is a speaker 234 and microphone 238. The speaker 234 and microphone 238 may be controlled by the processor 208. The microphone 238 is configured to receive and convert audio signals to electrical signals based on processor 208 control. Likewise, the processor 208 may activate the speaker 234 to generate audio signals. These devices operate as is understood in the art and as such are not described in detail herein.

[0063] Also connected to one or more of the buses 212 is a first wireless transceiver 240 and a second wireless transceiver 244, each of which connect to respective antennas 248, 252. The first and second transceiver 240, 244 are configured to receive incoming signals from a remote transmitter and perform analog front-end processing on the signals to generate analog baseband signals. The incoming signal maybe further processed by conversion to a digital format, such as by an analog to digital converter, for subsequent processing by the processor 208. Likewise, the first and second transceiver 240, 244 are configured to receive outgoing signals from the processor 208, or another component of the mobile device 208, and up convert these signal from baseband to RF frequency for transmission over the respective antenna 248, 252. Although shown with a first wireless transceiver 240 and a second wireless transceiver 244, it is contemplated that the mobile device 200 may have only one such system or two or more transceivers. For example, some devices are tri-band or quad-band capable, or have Bluetooth®, NFC, or other communication capability.

[0064] It is contemplated that the mobile device, and hence the first wireless transceiver 240 and a second wireless transceiver 244 may be configured to operate according to any presently existing or future developed wireless standard including, but not limited to, Bluetooth, WI-FI such as IEEE 802.11 a, b, g, n, wireless LAN, WMAN, broadband fixed access, WiMAX, any cellular technology including CDMA, GSM, EDGE, 3G, 4G, 5G, TDMA, AMPS, FRS, GMRS, citizen band radio, VHF, AM, FM, and wireless USB.

[0065] Also part of the mobile device is one or more systems connected to the second bus 212B which also interface with the processor 208. These devices include a global positioning system (GPS) module 260 with associated antenna 262. The GPS module 260 can receive and process signals from satellites or other transponders to generate location data regarding the location, direction of travel, and speed of the GPS module 260. GPS is generally understood in the art and hence not described in detail herein. A gyroscope 264 connects to the bus 212B to generate and provide orientation data regarding the orientation of the mobile device 204. A magnetometer 268 is provided to provide directional information to the mobile device 204. An accelerometer 272 connects to the bus 212B to provide information or data regarding shocks or forces experienced by the mobile device. In one configuration, the accelerometer 272 and gyroscope 264 generate and provide data to the processor 208 to indicate a movement path and orientation of the mobile device.

[0066] One or more cameras (still, video, or both) 276 are provided to capture image data for storage in the memory 210 and/or for possible transmission over a wireless or wired link or for viewing later. The one or more cameras 276 may be configured to detect an image using visible light and/or near-infrared light. The cameras 276 may also be configured to utilize image intensification, active illumination, or thermal vision to obtain images in dark environments. The processor 208 may process image data to perform image recognition, such as in the case of, facial detection, item detection, facial recognition, item recognition, or bar / box code reading.

[0067] A flasher and/or flashlight 280, such as an LED light, are provided and are processor controllable. The flasher or flashlight 280 may serve as a strobe or traditional flashlight. The flasher or flashlight 280 may also be configured to emit near-infrared light. A power management module 284 interfaces with or monitors the battery 220 to manage power consumption, control battery charging, and provide supply voltages to the various devices which may require different power requirements.

[0068] Figure 3 illustrates exemplary software modules that are part of the mobile device and server. Other software modules may be provided to provide the functionality described below. It is provided that for the functionality described herein there is matching software (non-transitory machine-readable code, machine executable instructions or code) configured to execute the functionality. The software would be stored on a memory and executable by a processor.

[0069] In this example confirmation, the mobile device 304 includes a receive module 320 and a transmit module 322. These software modules are configured to receive and transmit data to remote device, such as cameras, glasses, servers, cellular towers, or WIFI system, such as router or access points.

[0070] Also part of the mobile device 304 is a location detection module 324 configured to determine the location of the mobile device, such as with triangulation or GPS. An account setting module 326 is provided to establish, store, and allow a user to adjust account settings. A log in module 328 is also provided to allow a user to log in, such as with password protection, to the mobile device 304. A facial detection module 308 is provided to execute facial detection algorithms while a facial recognition module 321 includes software code that recognizes the face or facial features of a user, such as to create numeric values which represent one or more facial features (facial biometric information) that are unique to the user.

[0071] An information display module 314 controls the display of information to the user of the mobile device. The display may occur on the screen of the mobile device or watch. A user input/output module 316 is configured to accept data from and display data to the user. A local interface 318 is configured to interface with other local devices, such as using Bluetooth® or other shorter-range communication, or wired links using connectors to connected cameras, batteries, data storage elements. All of the software (with associated hardware) shown in the mobile device 304 operate to provide the functionality described herein.

[0072] Also shown in Figure 3 is the server software module 350. These modules are located remotely from the mobile device and can be located on any server or remote processing element. As is understood in the art, networks and network data use a distributed processing approach with multiple servers and databases operating together to provide a unified server. As a result, it is contemplated that the module shown in the server block 350 may not all be located at the same server or at the same physical location.

[0073] As shown in Figure 3, the server 350 includes a receive module 352 and a transmit module 354. These software modules are configured to receive and transmit data to remote devices, such as cameras, watches, glasses, servers, cellular towers, or WIFI systems, such as router or access points.

[0074] An information display module 356 controls a display of information at the server 350. A user input/output module 358 controls a user interface in connection with the local interface module 360. Also located on the server side of the system is a facial recognition module 366 that is configured to process the image data from the mobile device. The facial recognition module 366 may process the image data to generate facial data (biometric information) and perform a compare function in relation to other facial data to determine a facial match as part of an identify determination.

[0075] A database interface 368 enables communication with one or more databases that contain information used by the server modules. A location detection module 370 may utilize the location data from the mobile device 304 for processing and to increase accuracy. Likewise, an account settings module 372 controls user accounts and may interface with the account settings module 326 of the mobile device 304. A secondary server interface 374 is provided to interface and communicate with one or more other servers.

[0076] One or more databases or database interfaces are provided to facilitate communication with and searching of databases. In this example embodiment the system includes an image database that contains images or image data for one or more people. This database interface 362 may be used to access image data users as part of the identity match process. Also part of this embodiment is a personal data database interface 376 and privacy settings data module 364. These two modules 376, 364 operate to establish privacy setting for individuals and to access a database that may contain privacy settings.

Authentication System

[0077] An authentication system with path parameters that is operable in the above described environment and system will now be described in connection with Figure 4. Figure 4 shows a method for performing facial recognition authentication with path parameters according to one embodiment of the invention. As will be described in more detail below, the system utilizes the features of the mobile device 112 and server 120 defined above to generate a secure and convenient login system as one example of an authentication system. This reduces the burden of the user having to type in complex passwords onto a small screen of a mobile device, prevents fraud through means such as key logging or screen shot captures, and increases security by combining several path parameters and/or device parameters which must be met before user is authenticated.

[0078] In step 410, the system enrolls a user in the facial recognition authentication system. In one embodiment, an authentication server, such as the server 120 (Figure 1), may be configured to authenticate a user to allow access to a user's account, such as a bank or other account, via the mobile device 112. The authentication server 120 may be included as a part of a server of the institution or entity providing user accounts (hereinafter "account server"), or the authentication server may be provided separately. For example, in the environment shown in Figure 1, Servers 120B and 120C may represent account servers. In other embodiments, the account server and the authentication server are one in the same. In one embodiment, the authentication server 120 may provide an authentication application to the user for installation on the mobile device 112.

[0079] An enrollment process according to one embodiment will be described with reference to Figure 5. In this embodiment, a user via a mobile device 112 establishes a connection between the mobile device 112 and the account server 120B in step 510. As just one example, the user may establish a connection with a server of a financial institution such as a bank, or this connection may occur later in the process after authentication. The user then provides typical login information to authenticate the user, such as a user name and password for a financial account in step 512. In step 514, the user may next receive a prompt at the mobile device 112 to enroll in the facial recognition authentication system. The user then, via the user interface, indicates that he or she would like to set up the authentication system in response to the prompt.

[0080] Next, in step 516, the mobile device 112 may send device information to the authentication server 120. The device information may include among other information a device identifier that uniquely identifies the mobile device of the user. Such information may include device manufacturer, model number, serial number, and mobile network information. In step 518, when the authentication server 120 is incorporated with the account server 120B, the authentication server 120 associates and stores the device information with the user's account information. When the authentication server 120 is separate from the account server 120B, the account server 120B may generate a unique identifier related to the account information and send the unique identifier to the authentication server 120. The authentication server 120 may associate the device information and the unique identifier with each other and may store the information in a database 124.

[0081] The user is next prompted to provide a plurality of images of his or her face using a camera 114 on the mobile device 112 (hereinafter, "enrollment images") in step 510. The enrollment images of the user's face are taken as the user holds the mobile device and moves the mobile device to different positions relative to his or her head and face. Thus, the enrollment images of the user's face are taken from many different angles or positions. Furthermore, the path parameters of the mobile device are monitored and recorded for future comparison in step 522. Some non-limiting examples of how a user might hold a mobile device and take a plurality of images of her face is shown in FIGS 6A-7B.

[0082] In Figure 6A and 6B, the user holds the mobile device 112 on one side of his or her face and moves the mobile device 112 in an arc like path horizontally about his or her face until the mobile device 112 is on the other side of her or her face. In FIGS. 7A and 7B, the user holds the mobile device 112 far away from his or her face, and then brings the mobile device 112 forward closer to his or her face. Of course, any number of other paths may be used in addition to those shown in FIGS. 6A-7B. Additionally, the user may move his or her head while the camera is held fixed. The user could also hold the camera steady and move their head in relation to the camera. This method thus can be implemented with a webcam on a laptop or desktop, or on any other device, such as an IoT device where a camera is mounted on a similarly stationary location or object.

[0083] The enrollment images may be obtained as follows. The user holds and orients a mobile device 112 with a camera 114 so that the camera 114 is positioned to image the user's face. For example, the user may use a front facing camera 114 on a mobile device 112 with a display screen and may confirm on the display screen that his or her face is in position to be imaged by the camera 114.

[0084] Once the user has oriented the device, the device may begin obtaining the enrollment images of the user. In one embodiment, the user may press a button on the device 112 such as on a touchscreen or other button on the device to initiate the obtaining of the enrollment images. The user then moves the mobile device to different positions relative to his or her head as the device images the user's face from a plurality of angles or positions as described above. When the above-mentioned front-facing camera is used, the user may continually confirm that his or her face is being imaged by viewing the imaging on the display screen. The user may again press the button to indicate that the imaging is completed. Alternatively, the user may hold the button during imaging, and then release the button to indicate that imaging is complete.

[0085] As described above, the mobile device 112 may include face detection. In this embodiment in step 524, the mobile device may detect the user's face in each of the enrollment images, crop the images to include only the user's face, and send, via a network, the images to the authentication server 120. In step 526, upon receipt of the enrollment images, the authentication server 120 performs facial recognition on the images to determine biometric information ("enrollment biometrics") for the user. The authentication server 120 may then associate the enrollment biometrics with the device information and the unique identifier (or account information) and stores the biometric information in the database 124 in step 528. For added security, in step 530, the mobile device 112 and the authentication server 120 may be configured to delete the enrollment images after the enrollment biometrics of the user are obtained.

[0086] In another embodiment, the mobile device 112 may send the images to the authentication server 120 without performing face detection. The authentication server 120 may then perform the face detection, facial recognition, and biometric information processing. In another embodiment, the mobile device 112 may be configured to perform the facial detection, facial recognition, and biometric processing, and then send the results or data resulting from the processing to the authentication server 120 to be associated with the unique identifier or user account. This prevents sensitive personal data (images) from leaving the user's device. In yet another embodiment, the mobile device 112 may perform each of the above-mentioned steps, and the mobile device 112 may store the enrollment information without sending any of the enrollment biometrics or images to the server.

[0087] In one embodiment, the mobile device's gyroscope, magnetometer, and accelerometer are configured to generate and store data while the user moves the mobile device about his or her head to obtain the enrollment images (path parameters). The mobile device may process this data in step 532 to determine a path or arc in which the mobile device moved while the user imaged his or her face ("enrollment movement"). By using data from the accelerometer, magnetometer, and gyroscope, the system may check when a user is ready to begin scanning himself/herself, as well as determining the scan path. The data is thus used to determine when to start and stop the scan interval. The data may additionally include the time elapsed during scanning. This time may be measured from the user pressing the button to start and stop the imaging or may be measured from the duration the button is held down while imaging, or during more movement or to complete sweep.

[0088] The enrollment movement of the mobile device 112 (which is data that defined the movement of the mobile device during image capture) may be sent to the authentication server 120. The authentication server 120 associates and stores the enrollment movement, the enrollment biometrics, the device information, and the unique identifier or account information. Alternatively, the data generated by the gyroscope, magnetometer, and accelerometer may be sent to the server 120, and the server 120 may process the data to determine the enrollment movement. In another embodiment, the enrollment movement may be stored on the mobile device 112, such that all enrollment information is maintained on the mobile device 112.

[0089] Thus, in the above described embodiment, the enrollment information may thus comprise the device information, the enrollment biometrics, and the enrollment movement (based on movement of the mobile device 112).

[0090] Returning to Figure 4, once enrollment is complete, the authentication server 120 may later receive credentials from a user attempting to authenticate with the system as shown in step 420. For example, a user may attempt to log in to a user account. When a user attempts to log in, instead of or in addition to providing typical account credentials such as user name and password, the user may again take a plurality of images or video of his or her face as the mobile device 112 is held in the hand and moved to different positions relative to the head ("authentication images") in the same manner as was done during enrollment (such as shown in FIGS. 6A-7B). In this manner, the user may provide the necessary images (the term images includes video as video is a succession of images) from many different angles and/or positions, and may provide path parameters of the device while obtaining the images ("authentication movement") to both confirm the identity of the user as well as the liveness and realness of that individual to ensure it is not a video, screen shot, or other representation of the person.

[0091] In one embodiment outlined in Figure 8, the user via the mobile device 112 obtains several authentication images in step 810 while moving the mobile device 112 to different positions relative to the user's head. Using facial detection in step 812, the mobile device 112 detects the user's face in each of the authentication images, crops the images, and sends the images to the authentication server 120. In another embodiment, the mobile device 112 sends the images to the server 124, and the server 124 performs facial detection. In step 814, the authentication routing 120 may perform facial recognition on the authentication images to obtain biometric information ("authentication biometrics"). In another embodiment, the mobile device 112 performs facial recognition to obtain the authentication biometrics and sends the authentication biometrics to the server 120.

[0092] In step 816, the mobile device 112 sends the device information identifying the device and sends path parameters such as gyroscope, magnetometer, and accelerometer information defining the path of the mobile device taken during imaging, as well as the elapsed time during imaging ("authentication movement") to the server 120. The credentials received by the authentication server 120 for a login in the facial recognition system may thus comprise the device information, the authentication images or the authentication biometrics, and the authentication movement (path parameters).

[0093] Returning to Figure 4, in step 430, the authentication server 120 verifies that the credentials received from the mobile device 112 sufficiently correspond with the information obtained during enrollment. For example, as shown in step 910 in Figure 9, by using algorithms to process the characteristics of the face and light striking the face between the different images, the authentication server 120 can determine that the face in the authentication images is three-dimensional, i.e. not a representation on a printed picture or video screen. Where the mobile device 120 sends only the authentication biometrics 120 to the server, the server 120 may validate the realness or three-dimensional aspects of the user imaged by comparing the biometric results of the different images.

[0094] In step 920, the authentication server 120 may then compare the login credentials with the information stored from the enrollment process. In step 920, the server 120 compares the identification of the device obtained during the login process to that stored during enrollment. In step 930, the authentication biometrics may be compared with the enrollment biometrics to determine whether they sufficiently correspond with the enrollment biometrics. In step 940, the authentication movement may be compared with the enrollment movement to determine whether it sufficiently corresponds with the enrollment movement.

[0095] In some embodiments, a copy of the enrollment information may be stored on the mobile device 112, and the mobile device 112 may verify that the credentials received on the mobile device 112 sufficiently correspond with the enrollment information. This would allow a user to secure documents, files, or applications on the mobile device 112 itself in addition to securing a user's account hosted on a remote device, such as the authentication server 120, even when a connection to the authentication server 120 may be temporarily unavailable, such as when a user does not have access to the Internet. Further, this would allow the user to secure access to the mobile device 112 itself. Or enrollment info may be stored on server.

[0096] Accordingly, in step 950, if the authentication server 120 or mobile device 112 determines that the enrollment information sufficiently corresponds with the credentials received, then the server or mobile device may verify that the identification of the user attempting login corresponds the account holder. This avoids the cumbersome process of the user having to manually type in a complex password using the small screen of the mobile device. Many passwords now require capital, non-text letter, lower case, and numbers.

[0097] The level of correspondence required to determine that the enrollment information sufficiently corresponds with the authentication information in the login attempt may be set in advance. For example, the level of correspondence may be a 99.9% match rate between the enrollment biometrics and the authentication biometrics and a 90% match rate between the enrollment movement and the authentication movement. The required level of correspondence may be static or elastic based on the established thresholds.

[0098] For example, the required level of correspondence may be based on GPS information from the mobile device 112. In one embodiment, the authentication server 120 may require a 99.9% match rate as the level of correspondence when the GPS information of the mobile device corresponds with the location of the user's home or other authorized location(s). In contrast, if the GPS information shows the device is in a foreign country far from the user's home, the authentication server may require a 99.99% match rate as the level of correspondence or may be denied entirely. Hence, the required match between pre-stored authentication data (enrollment information) and presently received authentication data (authentication information) is elastic in that the required percentage match between path parameters or images my change depending on various factors, such as time of day, location, frequency of login attempt, date, or any other factor.

[0099] The required level of correspondence may additionally depend on time. For instance, if a second authentication attempt is made shortly after a first authentication attempt in a location far from the first authentication location based on GPS information from the mobile device 112, the level of correspondence threshold may be set higher. For example, a user can not travel from Seattle to New York in 1 hour. Likewise, login attempts at midnight to three in the morning may be a sign of fraud for some users based on patterns of the users' usage.

[0100] The level of correspondence between the enrollment information and the authentication information may be the result of compounding the various parameters of the enrollment information and the authentication information. For example, when the button hold time in the authentication information is within 5% of the button hold time of the enrollment information, the correspondence of the button hold time may constitute 20% of the overall match. Similarly, when the motion path trajectory of the authentication information is within 10% of the enrollment information, the motion path trajectory may constitute 20% of the overall match. Further parameter match rates such as the face size and facial recognition match in the authentication information as compared to the enrollment information may constitute the remaining 10% and 50% of the overall level of correspondence. In this manner, the total overall level of correspondence may be adjusted (total of all parameters being more than 75%, for example), or the match rate of individual parameters may be adjusted. For example, on a second attempted login, the threshold match rate of one parameter may be increased, or the overall level of correspondence for all parameters may be increased. The threshold match rates may also be adjusted based on the account being authenticated or other different desired levels of security.

[0101] Returning to Figure 4, in step 440, the authentication server 120 may grant or deny access based on the verification in step 430. For example, if the authentication server 120 verifies that the credentials match the enrollment information, then the server 120 may authenticate the user to allow access to the user's account. In the instance where the authentication server 120 is separate from the account server 120B (such as a bank's server), the authentication server 120 may transmit the unique identifier to the account server along with an indication that the identity of the user associated with the unique identifier has been verified. The account server 120B may then authorize the user's mobile device 112 to transmit and receive data from the account server 120B. Of course, all this may occur at only the account server 120B or on the mobile device 112 itself.

[0102] Alternatively, if the credentials provided by the user are not verified, the authentication server may transmit a message to display on the screen of the mobile device 112 indicating that the login attempt failed. The authentication server 120 may then allow the user to try again to log in via the facial recognition login system, or the authentication server 120 may require the user to enter typical account credentials, such as a user name and password.

[0103] In one embodiment, the server 120 may allow three consecutive failed login attempts before requiring a user name and password. If in one of the attempts, the required level of correspondence is met, then the user may be verified, and access may be granted. According to one embodiment, the authentication server 120 may retain the information from each successive authentication attempt and combine the data from the multiple authentication attempts to achieve more accurate facial biometric information of the person attempting to authenticate. In addition, the level of correspondence may be increased at each successive attempt to authenticate. In addition, by averaging the path data (authentication movement) and/or image data (authentication images/biometrics) from several login attempts, the login data (enrollment information) is perfected and improved.

[0104] Accordingly, the above described authentication system allows for authentication to a remote server 120 or on the mobile device 112 itself. This may be accomplished as described above by the mobile device 112 capturing the authentication credentials, and the authentication server 120 processing and analyzing the credentials compared to the enrollment information (cloud processing and analysis); the mobile device 112 capturing the authentication credentials and processing the credentials, and the authentication server 120 analyzing the credentials compared to the enrollment information (mobile device processing, cloud analysis); or the mobile device 112 capturing the authentication credentials, and processing and analyzing the credentials compared to the enrollment information (mobile device processing and analysis).

Advantages and Features of the Embodiments

[0105] The above described system provides several advantages. As one advantage, the facial recognition authentication system provides a secure login. For example, if during a login attempt the camera of the mobile device imaged a digital screen displaying a person rotating their head while the phone was not moving, the accelerometer, magnetometer, and gyroscope data would not detect any motion. Thus, the enrollment movement and the authentication movement would not correspond, and the login attempt would be denied.

[0106] In addition, because a plurality of images are used as enrollment images and authentication images, histograms or other photo manipulation techniques may be used to determine if a digital screen is present in place of a human face in the images. For example, the system may check for light frequency, changes in the captured images, or banding in an image which would indicate an electronic display generated the image, backlighting, suspicious changes in lighting, or conduct other analyses on the images by comparing the images to determine that the actual live user is indeed alive, present, and requesting authorization to login.

[0107] As yet another advantage, as explained above, not only must the enrollment biometrics sufficiently correspond to the authentication biometrics, but also the enrollment movement must match the authentication movement, and the device information must match the enrollment device information. For example, an application may be downloaded to a mobile device that has a digital camera. The application may be a login application or may be an application from a financial institution or other entity with which the user has an account. The user may then login to the application using typical login credential such as a website user name and password. Further, the user may have a device code from logging in on another device or may use the camera to scan QR code or other such code to pair the device to their user account.

[0108] The user then holds the mobile device to move the mobile phone to different positions relative to his or her head while keeping his or her face visible to the camera as it is moved. As the mobile device is moved, the camera takes the enrollment images of the face. During imaging, the speed and angle of the current user's mobile device movement is measured using the accelerometer, magnetometer, and gyroscope to generate the enrollment movement. Further continuous imaging and detection of the face throughout the process has been shown to prevent fraud. This is because a fraud attempt cannot be made by rotating images in and out of the front of the camera.

[0109] For example, a user may start the movement from right to left or from left to right as shown in FIGS. 6A and 6B. The movement may also be in a front and back direction as shown in FIGS. 7A and 7B. Any other movement may be utilized such as starting in the center, then going right, and then going back to center. Vertical and diagonal movements may also be used to further compound the complexity of the enrollment movement. When the user then later attempts login, the user must repeat the motion pattern in the authentication movement to match the enrollment movement in addition to the biometric data and device information matching. Thus, the security of the system is greatly enhanced.

[0110] The system therefore provides enhanced security for authenticating a user who has a mobile device. As explained above, the system may use at least any one or more of the following in any number of combinations to securely authenticate the user: physical device verification, mobile network verification, facial recognition including the size of the face in the image, a face detected in every frame during the movement, accelerometer information, gyroscope information, magnetometer information, pixels per square inch, color bits per pixel, type of image, user entered code or pattern, and GPS information.

[0111] As another advantage, the facial recognition login system provides a convenient manner for a user to login to an account with a mobile device. For example, once enrolled, a user does not need to enter a user name and password on the small mobile device each time the user wishes to access the account. Instead, the user simply needs to image himself or herself while mimicking the enrollment movement with the mobile device. This is especially advantageous with smaller mobile devices such as mobile phones, smart watches, and the like. It also saves time, eliminates lost or forgotten passwords, prevents others from spying on passwords as they are entered, and reduces error caused by typing.

[0112] The system may be further configured to allow a user to securely log on to multiple devices, or to allow users to securely share devices. In one embodiment, the enrollment information may be stored on an authentication server (or on "the cloud") and thus is not associated only with the user's original device. This allows the user to use any number of suitable devices to authenticate with the authentication server. In this manner, a user may use a friend's phone (third party device) or other device to access his or her information, such as account information, address book information, email or other messaging, etc. by performing the authentication operation on any device.

[0113] For example, the user may provide an email address, user name code, or similar identifier on the friend's phone such that the authentication server compares the login information with enrollment information for the user's account. This would indicate to the authentication server which authentication profile to use, but does not by itself allow access to the user's data, accounts, or tasks. Upon logging out of a friend's phone, access to the user's information on the friend's phone is terminated. The provides the benefit of allowing a user to securely access account or other authentication accessible information or tasks using any device without having to type the user's password into the third-party device, where it could be logged or copied. In a sense, the user is the password such that the user's facial features and stored facial data is the stored password and by providing the user's face to the camera, the user is providing the password.

[0114] Such a system may also be implemented without storing the user's enrollment information on the remote server, but instead maintaining enrollment information on the user's device. For example, when the user requests to log in to third-party device, the authentication server may send an authentication request to the user's device. The user may then authenticate the action using the above described system by providing authentication images and authentication movement to the user's device. The user's device then authenticates the user based on the enrollment information stored on the user's device. This data could be stored in the application or other secure location and highly encrypted. The user's device provides verification of whether the authentication was successful to the authentication server, whereupon the authentication server authenticates the user on the third-party device.

[0115] Through cloud-based authentication, a single user may also securely transfer data between authenticated devices. In one embodiment, a user may own a first device, such as a mobile phone, and is authenticated on the first device via the authentication system. The user may then acquire a new device, such as a new phone, tablet computer, or other device. Using the cloud-based authentication system, the user may authenticate on the new device and transfer data from the first device to the new device. The transfer of data may be completed via the Internet, a local network connection, a Bluetooth connection, a wired connection, or a near field communication. The authentication process may also be part of a security check to resent or restore a system after the phone is lost or stolen. Thus, the authentication system may be used to activate or authenticate a new device, with the authentication used to verify the user of the new device.

[0116] Similarly, the system may facilitate secure access to a single shared device by multiple people to control content or other features on the device. In many cases, passwords can be viewed, copied, guessed, or otherwise detected, particularly when a device is shared by several users. The users may be, for example, family members including parents and children, coworkers, or other relationships, such as students. The authentication system may allow each of the family members to log in based on his or her own unique enrollment information associated with a user account.

[0117] The device may restrict access to certain content or features for one or more of the certain user's accounts, such as children's user accounts, while allowing access to content and features for others, such as the parents' accounts. By using the authentication system for the shared device, the users such as children are unable to utilize a password to try and gain access to the restricted content because the authentication system requires the presence of the parent for authentication, as explained above. Thus, device sharing among users with different privileges is further secured and enhanced. Likewise, in a classroom setting, a single device may be securely shared between multiple people for testing, research, and grade reporting.

Adaptations and Modifications

[0118] Numerous modifications may be made to the above system and method without departing from the scope of the invention. For example, the images may be processed by a facial recognition algorithm on the device and may also be converted to biometric data on the device which is then compared to previously created biometric data for an authorized user. Alternatively, the images from a device may be sent through a wired or wireless network where the facial recognition algorithms running on a separate server can process the images, create biometric data and compare that data against previously stored data that assigned to that device.

Multiple Profiles for a Single User

[0119] Further, the photo enrollment process may be done multiple times for a user to create multiple user profiles. For example, the user may enroll with profiles with and without glasses on, with and without other wearable devices, in different lighting conditions, wearing hats, with different hair styles, with or without facial or ear jewelry, or making different and unique faces, such as eyes closed, winking or tongue out to establish another level of uniqueness to each user profile. Such 'faces' made by the user would not be available on the user's Social Media Pages and hence not available for copying, manipulation, and use during a fraud attempt. Each set of enrollment images, enrollment biometrics, or both may be saved along with separate enrollment movement. In one embodiment at least three images are captured as the mobile device completes the path. It is contemplated that any number of images may be captured.

Linking Enrollment Information

[0120] It is also contemplated that the enrollment process may be linked to an email address, phone number, or other identifier. For example, a user may sign up with an email address, complete one or more enrollments as described above, and confirm the enrollments via the same email address. The email address may then further enhance the security of the system. For example, if a user unsuccessfully attempts to login via the authentication system a predetermined number of times, such as three times for example, then the authentication system locks the account and sends an email to the email address informing the user of the unsuccessful login attempts. The email might also include one or more pictures of the person who failed to login and GPS or other data from the login attempt. The user may then confirm whether this was a valid login attempt and reset the system, or the user may report the login attempt as fraudulent. If there is a reported fraudulent login, or if there are too many lockouts, the system may delete the account associated with the email address to protect the user's security. Thus, future fraudulent attempts could not be possible.

Feedback Meters

[0121] To further facilitate imaging, the mobile device may include various feedback meters such as a movement meter or accuracy meter as shown in Figure 10. In one embodiment, the mobile device 1012 may display a movement meter 1024 that indicates the amount of movement the mobile device 1012 makes as the user moves the mobile device 1012 to different positions relative to his/her head. For example, the movement meter 1024 may be represented as a line that slides from one side of the screen. In this manner, the enrollment process may require a certain threshold of device movement to register a user with the multi-dimensional authentication system. For example, the system could require that the mobile device 1012 is moved in an arc or straight line and rotate at least 45 degrees to create the enrollment information. In another example, the system could require an acceleration experienced by the device exceeding a threshold amount. The movement meter may also aid the user in learning how to image himself/herself using the authentication system.

[0122] The mobile device 1012 may also display an accuracy meter 1026 or any other visual representation of authenticated frames to aid the user in authenticating himself/herself using the authentication system and learning to improve authentication. The accuracy meter 1026 may show a user a match rate (graphical, alpha, or numerical) of a predetermined number of images obtained during the authentication process. The accuracy meter can be represented on the display in a variety of ways including numeric percentages, color representation, graphical, and the like. A combination of representations may also be utilized.

[0123] For example, as shown in Figure 10, match rates for a predetermined number of images taken during authentication are represented on the accuracy meter. In the embodiment shown in Figure 10, each of the images may be represented by a column in a graph, and the accuracy can be shown for each image in each column. For example, the column with a longer bar represent higher accuracy, and a column with a lower bar represents lower accuracy. In addition to match rates for images, the match rates for the path parameter may also be displayed. Over time the user can improve.

[0124] In another embodiment, each of the images may be represented on a table as a color that corresponds to the match rate. The color dark green may represent a very high match rate, light green may represent a good match rate, yellow may represent a satisfactory match rate, red may represent a mediocre match rate, and grey may represent a poor match rate. Other colors schemes may also be used.

[0125] The height of the bars or the colors used may correspond to predetermined match rates. For example, a full bar or dark green may be a match rate greater than 99.9%, a three-quarter bar or light green may be a match rate between 90% and 99.9%, a half bar or yellow may be a match rate of 50-90%, red may be a match rate of 20%-50%, and a single line to a quarter bar or grey may be a match rate of 0-20%. A pie chart, line graph, or any other type of representation could also be used or any other numerical or graphical display. An overall score may be presented or a score per image.

[0126] The accuracy meter may also include a message 1028 indicating an overall match score. For example, the accuracy meter may indicate an average overall match score or the number of images which achieved a 99.9% match rate and display the message to a user. With the movement meter 1024 and the accuracy meter 1026 as described above, the user may quickly learn to use the authentication system due to the feedback presented by the meters 1024, 1026.

Gamification and Rewards

[0127] The movement and accuracy meters 1024, 1026 may also be configured to incorporates game features, aspects, or techniques into the authentication system to encourage a user to try and get the best match possible (such as a high number score or a high percentage of frames), increasing the user's skill in utilizing the authentication system. This also builds user adoption rates for the technology.

[0128] For example, the user may compete with themselves to mimic or improve past authentication scores to encourage or train the user to achieve a high score. Further modifications of the authentication meter may also be incorporated such as the ability to share accuracy match results with others to demonstrate one's skill in using the system or to compete against others. In other instances, the user may receive a reward, such as a gift or coupon, for high accuracy scores. While this may slightly increase costs, the reduction in fraud loss would far outweigh the additional cost.

[0129] Further game techniques may be incorporated into the authentication system to encourage users to take actions which will prevent unauthorized or fraudulent authentication. In one embodiment, the authentication system may award users that engage in fraud preventing activities. One such activity is utilizing the facial recognition authentication system described herein. For example, based on the above described accuracy meter, the system may reward a user that successfully authenticates with the system above a certain match rate. The system may award reward points, cash, or other prizes based on the successful authentication or on a predetermined number of successful authentications. Where reward points are utilized, the points may be cashed in for predetermined prizes.

[0130] Other game features may involve award levels for users who gain a predetermined amount of experience using the authentication feature. For example, different reward levels may be based on users successfully authenticating 100 times, 500 times, 1000 times, etc. Because each instance of fraud loss can be significant and can damage the goodwill of the business or organization, the benefits to fraud prevention are significant.

[0131] In one embodiment, the user may be notified that he or she has achieved various competency levels, such as a “silver level” upon achieving 100 successful authentications, a “gold level” for achieving 500 successful authentications, or a “platinum level” for achieving 1000 successful authentications. A set number of points awarded for each authentication above a given match rate may increase based on the user’s experience level. Of course, the names of the levels and the number of authentications for each level as described above are only exemplary and may vary as desired.

[0132] In one embodiment, an authentication only counts toward reward levels when business is transacted at the web site while in other embodiments, repeated attempts may be made, all of which count toward rewards. Another feature may incorporate a leaderboard where a user may be notified of a user ranking comparing his or her proficiency or willingness in using the authentication system as compared with other users.

[0133] Successful use of the authentication system benefits companies and organizations that utilize the system by reducing costs for fraudulent activities and the costs of preventing fraudulent activities. Those cost savings may be utilized to fund the above described game features of the authentication system.

[0134] Further activities that correspond to the authentication system and contribute to the reduction of fraud may also be incorporated to allow a user to earn points or receive prizes. Such activities may include a user creating a sufficiently long and strong password that uses a certain number and combination of characters. This encourages and rewards users to set passwords that are not easily compromised. Other examples may include rewarding users to take time to perform verification steps in addition to an initial authentication such as a mobile phone or email verification of the authentication, answering one or more personal questions, or other secondary verifications as currently known or later developed. This rewards users for taking on added time and inconvenience to lower the risk of fraud to a company or organization.

[0135] As another example, if the authentication service is used to login to websites or apps that provide affiliate programs, then the reward or gift can be subsidized from the affiliate commissions on purchases made on those sites. For example, if a commerce (product or service) web site utilizes the method and apparatus disclosed herein to avoid fraud, and thus increase profits, then a percentage of each purchase made by a user using the authentication service will be provided to the authentication service. By reducing fraud, consumer purchases are more likely and additional users will be willing to enter financial and personal information. An affiliate link, code, or referral source or identifier may be used to credit the authentication system with directing the consumer to the commerce (product or service) web site.

Multiple Account Login

[0136] It is also contemplated that the authentication system may be configured to allow a user to access many different web sites with a single authentication. Because the authentication process and result are unique to the user, the user may first designate which participating web sites the user elects to log into and then after selecting which one or more web sites to log into, the user performs the authentication described herein. If the secure authentication is successful, then the user is logged into the selected web sites. In this way, the authentication process is a universal access control for multiple different web sites and prevents the user from having to remember multiple different user names and passwords while also reducing fraud and password overhead for each user.

Automatic Start/Stop of Imaging

[0137] It is also contemplated that the system may be configured to have the video camera running on the phone. The mobile device would capture image frames and path parameter data when the phone moves (using the camera, gyroscope, magnetometer, and accelerometer) but only process into biometric data on the device or send the frames up to the server if a face is detected in them. In other embodiment, no image data or frames is sent to the server and instead the analysis is performed on the user's mobile device, such as a phone. In this embodiment, the application executing on the mobile device could trigger the software application to start saving frames once the phone is moving and then if the phone continues to move in the correct path (a semi-circle, for example) and the system detects a face in the frame the mobile device would start to send images, a portion of the image, or biometric data to the server for processing. When the system senses motion it may trigger the capture of images at certain intervals. The application may then process the frames to determine if the images contain a face. If the images do include a face, then the application crops it out and then verifies if the motion path of the mobile device is similar to the one use used during enrollment. If the motion path is sufficiently similar, then the application can send the frames one at a time to the server to be scanned or processed as described above.

Banding and Edge Detection

[0138] When a fraudulent attempt is made using a display screen, such as an LED, LCD, or other screen, the system may detect the fraudulent login attempt based on expected attributes of the screen. In one embodiment, the authentication system will run checks for banding produced by digital screens. When banding is detected, the system may recognize a fraudulent attempt at a login. In another embodiment, the system will run checks for edge detection of digital screens. As the mobile device is moved to obtain the authentication movement during a login attempt, the system checks the captured images to for edges of a screen to recognize a fraudulent login attempt. The system may also check for other image artifacts resulting from a screen such as glare detection. Any now know or later developed algorithms for banding and screen edge detection may be utilized. Upon detection of fraud will prevent authentication and access to the website or prevent the transaction or account access.

Other Attributes Estimation

[0139] The authentication system may further conduct an analysis on the enrollment images to estimate at least one of a gender, an approximate age, and an ethnicity. In an alternative embodiment, the user may manually enter one or more of their gender, an approximate age, and an ethnicity, or this information may be taken or obtained from existing records which are known to be accurate. The authentication system may then further store a user's estimated gender, age, and ethnicity as enrollment credentials or user data. Thus, when the user later attempts to authenticate with the system, the system will compare derived gender, age, and ethnicity obtained from authentication images (using biometric analysis to determine such data or estimates thereof based on processing) with the stored gender, age, and ethnicity to determine whether to authenticate the user. For example, if the derived data for gender, age and ethnicity matches the stored enrollment credentials, then the authentication is successful, or this aspect of the authentication is successful.

[0140] The authentication system may make the gender, age, and ethnicity estimations based on a single image during the authentication process or based on multiple images. For example, the authentication system may use an image from the plurality of images that has an optimal viewing angle of the user's face for the analysis. In other embodiments, a different image may be used for each analysis of age, gender, and ethnicity when different images reveal the best data for the analysis. The authentication may also estimate the gender, age, and ethnicity in a plurality of the images and average the results to obtain overall scores for a gender, age, and ethnicity.

[0141] As an alternative to obtaining the gender, age, and ethnicity as enrollment information, the estimated gender, age, and ethnicity estimations as authentication credentials may be set over a course of repeated use of the authentication system. For example, if in previous successful authentications using biometrics and movement information, the authentication system always estimates a user's age being between 40 and 50, then the authentication may set credentials for that user requiring later login information to include images of a face estimated to be between 40 and 50. Alternatively, gender, age, and ethnicity estimations may be implemented as one of many factors contributing to an overall authentication score to determine whether or not to authenticate a user.

[0142] For example, if the authentication process has a gender estimation of + or - 0.2 of 1.9 male rating, then if the actual results do not fall within that range the system may deny access for the user. Likewise, if the user's age range always falls between 40-50 years of age during prior authentication attempts or enrollment, and an authentication attempt falls outside that range, the system may deny access or use the result as a compounding factor to deny access.

[0143] In a further embodiment, when a bracelet or watch capable of obtaining an EKG signature is used, a certain EKG signature may be required at login. The EKG signature could also be paired with the facial recognition rotation to provide multiple stage sign-on for critical security and identification applications. Further, the credentials could also include GPS information where login is only allowed within certain geographic locations as defined during enrollment. In one configuration the GPS coordinates of the mobile device are recorded and logged for a login attempt or actual login. This is additional information regarding the location of the user. For example, if the GPS coordinates are in a foreign country known for fraud, then the attempt was likely fraudulent, but if the GPS coordinate indicate the attempt or login was made in the user's house, then fraud is less likely. In addition, some applications may only allow a user to login when at specified location such as a secure government facility or at a hospital.

[0144] The enrollment information may further include distance information. Because the motion arc (speed, angle, duration…) is unique to each user, face detection software on the device can process the images and determine if the device is too close or too far from the subject. Or in other words, the enrollment information may consider the size of the face in the images. Thus, the potential enrollment information may also vary based on the length of a user's arm, head, and face size, and on the optics of the camera in the user's particular mobile device. The user may also be positioned at a fixed computer or camera, such as laptop, desktop, or atm. The user may then move the face either forwards and back, side to side, or up and down (or a combination) to create the images. Hence, this method of operation is not limited to a mobile device. In one embodiment, the camera is located in an automobile, such as in a mirror, and the person moves their head or face to authenticate.

Gradual Authentication Access

[0145] In one embodiment, the system is set to limit what the user can do when first enrolled and authenticated. Then, after further authentications or after a predetermined time period and number of authentications, additional capabilities may be granted. For example, during the first 20 authentications during the first 3 months, a maximum transaction of $100 may be allowed. This builds a database of known authentication data in connection with non-objected to transactions by the user. Then, during the next 20 authentications a transaction limit of $3000 may be established. This limits the total loss in the event of fraud when the authentication data is limited, and the user is new to the system. For example, if an unauthorized user is able to fraudulently enroll in the authentication system.

Video Display for Imaging

[0146] When the user images himself/herself using a front-facing camera, the user may confirm that his/her face is being imaged by viewing the image on the display, as described above. The image shown on the display may be configured to be smaller in area than the entire display and may be positioned in an upper portion of the display towards the top of the device. When the user's image is shown only in the top portion of the user's display screen, the user's eyes tend to look more closely at the front camera. When the user's eyes are tracking up, the accuracy of the facial recognition may be improved. Further, tracking the movement of the eyes from frame to frame may allow the system to validate that the images are of a live person, and are not from a photograph or video recording of the person.

[0147] The image shown on the display may also be positioned to correspond with a camera location on the user's device, as shown in FIGS 11A-11C. Mobile devices that are available today may include front-facing cameras disposed at many different positions. For example, one mobile device 1112a, 1112b may have a front-facing camera 1114a, 1114b that is disposed above the display and off center towards one side or the other, as shown in FIGS 11A and 11B. Accordingly, the feedback image 1116a, 1116b of the user shown on the display may be positioned to correspond with the location of the camera 1114a, 1114b as shown. In FIG 11A, where a camera 1114a is above the display and is off-center at a position left of the center, then the image 1116a may be shown in an upper left corner of the display. In FIG 11B, where a camera 1114b is above the display and is off-center at a position right of the center, then the image 1116b may be shown in an upper right corner of the display. As shown in Figure 11C, a mobile device 1112c may have a camera 1114c that is disposed centered directly above the display. There, the image 1116c may be displayed centered in an upper portion of the display. In this manner, a user's eyes are directed close to and/or track as close to the camera as possible, aiding eye tracking and movement verification. The user is also able to better see the feedback image, and other feedback or information on the screen, as they move the mobile device.

[0148] The image viewed on the display by the user may further be modified such that the edge pixels on the sides display are stretched horizontally as shown in Figure 12. That is, a predetermined area 1206, 1208 on both the right and the left sides are warped to stretch towards right and left edges, respectively, of the screen. This allows a larger vertical portion of the displayed image to be shown on the display. Simultaneously, this trains a user to use the system correctly by keeping his or her face in the center of the screen, as his or her face would become warped on the screen if it becomes off center and part of the face enters the one of the warped areas.

Authentication in Low-light Environments

[0149] To facilitate imaging, the screen on the mobile device may additionally be displayed with a white background, and the brightness of the screen may be increased to light up the user's face in dark environment. For example, a portion of the display could provide video feedback for the user to ensure he or she is imaging himself or herself, while the remaining portion of the display is configured to display a bright white color. Referring to the example shown in Figure 11C, this may be done by showing the video feedback 1116c on a center of the display, with the surrounding areas being displayed as bright white bars around the video feedback 1116c. In very dark situation, an LED flash on the back side of the mobile device and the back facing camera may be used. Alternatively, the camera may be configured to create an image using infrared light or other night vision techniques.

[0150] When infrared imaging is used as thermal imaging, further security enhancements are possible. Particularly, the thermal imaging may be analyzed to indicate whether the obtained images are from an actual user or are fraudulent images from a screen or other device. When a person is in front of an infrared thermal imaging camera, the heat radiation detected should be fairly oval shaped designating the person's head. In contrast, the heat radiating from a screen is typically rectangular. Further, the heat patterns detected in the actual person's face as well as the movement of the heat patterns in the images can be compared with expected heat patterns of a human face to distinguish the images from fraudulent authorization attempts using a screen.

Detecting Output from the Mobile Device

[0151] The display or other light source on the mobile device may further be utilized to provide additional security measures. During the authentication process described above, light from the display or other light source is projected onto the user's face and eyes. This projected light may then be detected by the camera of the mobile device during imaging. For example, the color tone detected on the skin, or a reflection of the light off the cornea of a user's eye may be imaged by the camera on the mobile phone. Because of this, random light patterns, colors, and designs may be utilized to offer further security and ensure there is a live person attempting authentication and not merely an image or video of a person being imaged by a fraudster.

[0152] As one example, when a user begins authentication, the authentication server may generate and send instructions to the user's device to display a random sequence of colors at random intervals. The authentication server stores the randomly generated sequence for later comparison with the authentication information received from the mobile device. During authentication imaging, the colors displayed by the device are projected onto the user's face and are reflected off the user's eyes (the cornea of the eyes) or any other surface that receives and reflects the light from the screen. The camera on the user's mobile device detects the colors that are reflected off the user's skin or eyes (or other surface) and generates color data indicating the colors detected based on the screen projection. This data may be returned to the authentication server to determine if the color sequence or pattern sent to the mobile device matches that known sequence or pattern projected by the screen of the user device. Based on this comparison at the authentication server the authentication is a success or denied. The comparison with the random sequence of colors in the instructions may alternatively occur exclusively at the user device to determine that a live user is being authenticated.

[0153] As another example, when a user begins authentication, the authentication server may send instructions the user's device to display a randomly generated pattern which is then stored on the authentication server. This pattern may include graphics, text, lines or bars, flashing light patters, colors, a QR code, or the like. The randomly generated pattern is displayed during authentication imaging, and the pattern is reflected off the user's eyes (cornea). The camera of the user's device detects the reflected pattern off the eye of the user and processes the reflected, mirrored image of the displayed pattern. The processed pattern (such as being converted to a numeric value) is transmitted to the authentication server and compared to the pattern that was randomly generated and stored on the authentication server to verify if the pattern displayed by the screen and imaged after reflection off the user's face establishes a pattern match.

[0154] If a match occurs, this establishes or increases the likelihood that a live person is being imaged by the device. If the pattern is not a match, or does not meet a match threshold level, then the authentication process may fail (access denied) or the account access or transaction amount may be limited. It is noted that this example could also be incorporated on desktop computer with a webcam that does not incorporate the enrollment movement and authentication movement described above. Further, this example may not only be incorporated with facial recognition, but could also serve as an added layer of security for iris recognition or any other type of eye blood vessel recognition, or any facial feature that is unique to a user.

[0155] When the above example is implemented on a desktop computer, eye tracking may also be utilized to further demonstrate the presence of a live user. For example, the screen could show a ball or other random object or symbol moving in a random pattern that the user watches with his or her eyes. The camera can detect this real time movement to verify the user is live, and not a picture or display, and verify that the eye or head movements correspond to and match the expected movement of the object or words on the screen, which are known by the authentication system. Eye tracking can also be done by establishing an anchor point, such as via a mouse click at a location on the screen (assuming that the user is looking at the location where the mouse click takes place), and then estimating where the user is looking at the screen relative to the anchor position.

[0156] The use of a moving object on the screen may also be beneficial during enrollment on either a mobile or stationary device. For example, while capturing the enrollment images, the device may display a moving digital object (such as a circle or words(s)) that moves around the screen so that the user is encouraged to follow it with his or her head and eyes. This movement may be involuntary from the user, or the device may be configured to instruct the user to follow the object. This results in movement of the head and/or eyes creating small changes in the orientation of the user's head and face with the device camera, providing more complete enrollment information. With more complete enrollment information, the system may better ensure that the user will later be authenticated at a high rate even at slightly different angles during future authentication attempts.

Intuitive User Training and Enhanced Security by "Zooming"

[0157] In one embodiment, the system is configured to aid the user to easily learn to authenticate with the system. As shown in Figure 13A, once enrollment or authentication is begun as described previously, the system causes the user's mobile device 1310 to display a small oval 1320 on the screen 1315 while the mobile device 1310 is imaging the user. Instructions 1325 displayed on the screen 1315 instruct the user to hold the mobile device 1310 so that his or her face or head appears within in the oval 1320. Because the oval 1320 is small, the user is required to hold the mobile device 1310 away from his or her body, such as by straightening his or her arm while holding the mobile device 1310. The maximum arm length and face size is unique to the user. In other embodiment, the arm may not be fully straightened such as to accommodate operation when space is not available, such as in a car or in a crowded location. It is noted that while the small oval 1320 is shown centered in the display, it may be positioned anywhere on the screen 1315.

[0158] Next, as shown in Figure 13B, the system causes the user's mobile device 1310 to display a larger oval 1330 on the display 1315. The display 1315 may also show corresponding instructions 1335 directing the user to "zoom in" on his or her face to fill the oval 1330 with his or her face. The user does this by bringing the mobile device 1310 closer to his or her face in a generally straight line to the user's face (such as shown in FIGS. 7A and 7B) until the user's face fills the oval 1330 or exceeds the oval. In other embodiments, the large oval 1330 may simply be a prompt for the user to bring the mobile device 1310 closer to the user's face.

[0159] Thus, the system provides and teaches the user a simple method to provide enrollment and authentication images along with enrollment and authentication movement as explained above. The system may also teach varying enrollment and authentication movement by varying the location of the small oval 1320 on the screen 1315, and by changing the order and the size of the ovals displayed. For example, the user may zoom in half way, then out, then in all the way, by moving the mobile device. The system may be configured to monitor that the camera's zoom function (when equipped) is not in use, which typically requires the user to touch the screen.

[0160] In one embodiment, the enrollment movement may be omitted, and the authentication movement may be compared to expected movement based on the prompts on the screen. For example, the device or authentication server generates a series of differently sized ovals within which the user must place his or her face by moving the mobile device held in the user's hand. In this manner, the authentication movement may be different during each login depending on the order, size, and placement of the ovals shown on the screen.

[0161] The system may also incorporate other security features when the "zoom in" movement is used as shown in Figures. 13A and 13B. The zoom in feature is typically from moving the device closer or further from the user, but a camera zoom function is also contemplated. When images are taken at relatively close distances between the subject and the camera, the images are distorted through what is known as perspective distortion. Some texts may refer to this distortion as fish-eye type distortion, but perspective distortion is a more accurate technical terminology. Further, lenses configured as wide-angle lenses may contribute barrel distortion (a type of lens distortion) in an image. Other types of lens distortions are also present. These distortions may be tracked for different types of lenses for different devices. The degree of distortion experienced by a user performing the "zoom in" movement to fit their face within the screen displayed prompts may vary and is dependent on the type of optics used in the camera's lens, the type of distortion, and other factors.

[0162] The distortion becomes more obvious on an image of a person's face when the person images his or her face close to the lens. The effect results in the relative dimensions of the person's face appearing different than when the imaging is done with the person's face farther away from the lens. For example, a person's nose may appear as much wider and taller relative to a person's face when the image is taken at a close proximity as compared to when the image is taken at a distance. The differences in the relative dimensions are caused by the relatively larger differences in distances between the various facial features and the camera when the person is imaged close to the lens as compared to the relatively equal distances between the facial features and the camera when the person is imaged at a distance farther from the lens.

[0163] Such differences have been found to be significant in many facial recognition algorithms. That is, a facial recognition algorithm may not result in a high likelihood of a match between images of a live person imaged at a close proximity and the same person imaged at a far proximity. In contrast, if a two-dimensional photograph of a person is imaged by the camera at both a close proximity and a farther proximity, the relative distances (length) between the lens and the facial features of the two-dimensional image do not change so significantly. Thus, a facial recognition algorithm would recognize the two-dimensional photograph as a high likelihood of a match when imaged at both a close proximity and a distance farther from the lens.

[0164] This effect also changes what parts of the user may be viewed by the camera of the user's mobile device based on the angle between the camera and facial features of the user. For example, when imaged farther away, the camera may image the user's face with the user's ears visible in the image. However, when the user device is moved close to the user's face, the image captured by the camera no longer includes the user's ears. This is because other facial features of the user's face, such as the user's cheeks/cheekbones now block the line of sight from the camera to the user's ears. In contrast, when a two-dimensional picture is imaged by the camera, the same facial features of the two-dimensional picture will always be visible to the camera whether the camera is close to the two-dimensional picture or far away. Thus, the three-dimensions or liveness of the user's face may further be verified by detecting changes in what part of the user face or other features are present in the image.

[0165] This effect as described above may be used to increase the security of the authentication system. For example, during enrollment, enrollment images may be provided by the user at both close and far proximities from the lens, in addition to other positions through the movement. Later, during authentication, authentication images may be obtained at both the close and far distances from the lens to determine if they match with the enrollment information obtained from the enrollment images. Further, because perspective distortion is expected when an actual, three-dimensional person is present, an absence of the relative change in the dimensions of the facial features alerts the system to a fraudulent attempt at authentication. This effect could not easily be re-created with a two-dimensional picture (printed photograph or screen) and thus, this step can serve as a secure test to prevent a two-dimensional picture (in place of a 3D face) from being used for authentication.

[0166] In other words, using this movement of "zooming" in and out on the user's face, two or more biometric profiles could be created for the same person. One of the multiple profiles for the person may be imaged farther from the camera, and one of the multiple profiles may be for the person imaged closer to the camera. For the system to authenticate the person, the authentication images and biometrics must match the two or more profiles in the enrollment images and biometrics.

[0167] In addition, the system may detect the presence of a real person as compared with a fraudulent photograph of a person by comparing the background of the images obtained at a close and a far proximity. When the mobile device 1310 is held such that the person's face fits within the oval 1320, objects in the background that are almost directly behind the person may be visible. However, when the mobile device 1310 is held such that the person's face fits within the larger oval 1330, the person's face blocks the cameras ability to see the same objects that are almost directly behind the person. Thus, the system may compare the backgrounds of the images obtained at the close and the far proximity to determine whether the real person is attempting authentication with the system.

[0168] Of course, in Figures. 13A and 13B, shapes or guides other than ovals 1320 and 1330 may be used to guide the user to hold the mobile device 1310 at the appropriate distance from his or her face. For example, the mobile device 1310 may show a full or partial square or rectangle frame. Further, the system may vary the size and location of the frame, such as the ovals 1320, 1330 to add further security. For example, the system may require a medium sized frame, a small frame, and then a large frame. As another example, the system may require a small frame at a first location and a second location, and then a large frame. This may be done randomly to teach different users different enrollment and authentication movements, or to increase the security of the authentication system.

[0169] The number of frame sizes presented to the user may also vary for a single user based on the results of other security features described herein. For example, if the GPS coordinates of the mobile device show that the device is in an unexpected location, more frames at different distances may be required for authentication. One or more indicators, such as lights, words, or symbols may be presented on the screen to be visible to the user to direct the user to the desired distance that the mobile device should be from the user.

[0170] In Figures 13A and 13B, the system may predict the expected perspective distortion of the images based on the mobile device used for enrollment and authentication, and based on known and trusted enrollment data. In addition, or as an alternative, the known specifications of a mobile phone camera for a given model may be utilized to predict the expected distortion of the person's facial features at different distances from the lens. Thus, the authentication may be device dependent. Further, enrollment information from the user is not required at every possible distance from the camera.

[0171] For example, as described above, enrollment images and biometrics may be obtained at at least two distances from the user. During authentication, multiple intermediary images are captured in addition to images corresponding the close and far distances of the enrollment images and biometrics. Based on the expected pattern of distortion of these intermediary images according to the distanced traveled by the device, the system may validate that the change in distortion of the images is happening at the correct rate, even though only two enrollment profiles are obtained.

[0172] The capturing of these images may be still images or video, such that frames or images are extracted from the video that is taken during the movement from the first position distant from the user and the second position proximate the user. Thus, it is contemplated the operation may capture numerous frames during the zoom motion and ensure that the distortion is happening at the correct rate for the head size and the movement of the mobile device distance based on data from the accelerometers, magnetometers, and so forth.

[0173] Over time based on accumulated data, or calculated data during design phase, the system will have data indicating that if a phone is moved a certain distance toward a user's face, then the distortion effect should fall within a known percentage of the final distortion level or initial distortion level. Thus, to fool or deceive the authentication system disclosed herein, the fraud attempt would not only need to distort the fraudulent two-dimensional picture image, but would also need to cut the background, and then make a video of the face, distortion, and background that does all of this incrementally and at the correct speed, all while not having any banding from the video screen or having any screen edges visible, which is very unlikely.

[0174] Many currently known facial detection and facial recognition algorithms are configured to only look for a face within an image where the depicted head is smaller than the image's dimensions. If a user's the forehead, ears or chin were not visible in the frame the remainder of the face would not be detected. Thus, to ensure that the facial detection and recognition algorithms detect and recognize the user's face in the zoomed in image (Figure 13B), the system may add a large buffer zone around the image taken at a close proximity. This creates a larger overall image and allows current facial detection and recognition algorithms to detect and recognize the face, even where the face of the user is large in the original image. In one embodiment, the face detection may be configured to detect portions of the face such as eyes, nose and mouth and extrapolate that the entire face is present based on one of more of those features being present.

[0175] When the enrollment and authentication movements resulting from the process described with Figures 13A and 13B is used, the eye tracking security features described above may also be enhanced. For example, when the user is instructed to bring the mobile device 1310 closer to his or her face to fill the oval 1330, the QR code, a random shape, a bar code, color, text, numbers or any other visual indictor may be displayed on the screen. At this close distance, the reflection of the displayed indicator off the user's eye or face may be more easily imaged by the camera. Furthermore, eye movement, blinking, and the like to determine the "liveness" of the person being imaged may also be more easily obtained at the close proximity.

[0176] In one embodiment, at least one blink is required to prove liveness for authentication. In another embodiment, blinks may be counted, and the number of blinks may be averaged over time during authentications. This allows for an additional factor in authentication to be the number of blinks observed during the motion. If a pattern of when the user blinks during the motion is observed, the system may verify that the user blinks at the expected time and device location during the motion during future authentication attempts. In some instances, the system may prompt the user to blink, wink, smile, etc. and monitor the captured images to verify that the user has performed the prompted action within a predetermined time. A series of prompted actions may be given to the user to perform (for example, blink, wink right eye, then smile). In one example, the system may prevent authentication (lock out a user) if the prompted actions are performed out of order or are not performed within the time period because this may be indicative of a fraudulent recording being used in place of a live user.

[0177] In other embodiments, the size or location of the oval or frame may change to sizes or locations other than that shown in Figures 13A, 13B such that the user must position and/or angle the phone to place his or her face within the oval. This establishes yet another method of insuring liveness of the user. The oval may start small and become larger or start large and become smaller. The shape may be shapes other than oval, such as square, triangular, rectangular, or any other shape. Instead of or in additional to a shape, text may be shown instructing the user to move the phone closer or farther from the user's face.

[0178] In one exemplary method, the mobile device is positioned at a first distance from the user and a first image captured for processing. This distance may be linearly away from the user and in this embodiment not in an arc or orbit. This may occur by the user moving the mobile device, either by hand, or by the mobile device being on a movable device or rail system. Or, the lens system may be adjusted if in a fixed system to change the size of the user's face in relation to the frame size. Alternatively, the user may stay stationary, the multiple cameras may be used, or camera may move without the user moving. Once some form of movement (from a device, camera, lens, or user) has occurred to establish the camera at a second distance, a second image is captured for processing. Movement from the first position to the second position may be straight toward the user. Processing occurs on both images.

[0179] The processing may include calculations to verify a difference between the two images, or a difference in biometrics obtained from the two images, that indicates that a real person is being imaged. Processing may occur to compare the first authentication image to a first enrollment image (corresponding to the first distance) to determine if a match is present and then compare the second authentication image to a second enrollment image (corresponding to the second distance) to determine if a match is present. If a match occurs, then authentication may proceed.

[0180] Variations on these methods are also possible with the system requiring a match at the first distance, but a failure to match at the second distance, thereby indicating that the second image is not of a two-dimensional picture. The processing resulting in a match or failure to match may be any type image or facial recognition processing algorithm. As with other processing described herein, the processing may occur on the mobile device, one or more remote servers, or any combination of such devices.

[0181] All the processing described herein may occur on only the mobile device, only a remote server, or a combination there. The biometric data may be stored on the mobile device or the server or may be split between the two for security purposes. For example, the images could be processed on the mobile device, but compared to enrollment data in the cloud or at a remote server. Or, the images could be sent to the cloud (remote server) for processing and comparison.

Pixel Relative Velocities for Depth Detection

[0182] The system may further incorporate the use of an operation referred to generally herein as pixel velocity analysis to determine whether the authentication information obtained by the device includes images and/or biometric information of a live, three-dimensional person. Pixel velocity analysis tracks the pattern of apparent motion of objects, surfaces, and edges in a visual scene. For instance, pixel velocity analysis tracks the apparent motion of features in successive images caused by the relative motion between a camera and the scene in at least two frames.

[0183] In one example, when there is relative movement between the camera and scene, an object closer to the camera within the scene will appear to move at a different rate than an object farther from the camera. This movement or pixel velocity is reflected in changes in pixel values that represent the objects in the picture as the objects change their location in the picture as the camera is moved.

[0184] For example, a background element may be represented in the array of pixels in the images, such as a clock on a wall or a distant tree in the landscape. A foreground element may also be represented in the array of pixels as a face or facial feature of a person being imaged. As the relative distance between the camera and the foreground element and the background element change, the pixels representing the foreground and the background elements will change their position within the array of pixels. Different pixels will represent or capture the particular elements as the camera is moved. Importantly, the differences in distances between the camera and the foreground element and the camera and the background element cause the rate of change of the pixels (pixel velocity) of the foreground element and the background element to be different.

[0185] In some instances, different features of a foreground object may be compared for relative changes in pixel velocities. In this instance, the pixel velocities of different facial features may be compared, such as the nose or cheek. The pixel velocities for the different facial features of a real, three-dimensional person will be different based on their location on the frame of images and on the relative distances from the camera. For example, the pixels that represent the user's nose may move very little as the camera is moved closer to or further from the user face while pixels that represent a feature on the outside of the face will move to a greater degree.

[0186] In some instances, as the camera is moved closer to the use, some background elements will be obscured by the user's face and thus certain elements will be obscured. This would not occur if a two-dimensional image of the user was being imaged, such as in a fraud or spoofing attempt, instead of a live three-dimensional user.

[0187] The different rates of movement can be captured and compared in frames taken at incremental times. By detecting the different rates of movement or velocities of objects (rate of change over time or based on camera position) in the foreground and the background of the image, it can be determined that the image is a live, three-dimensional image as compared to a two-dimensional picture being used in a fraudulent authorization attempt.

[0188] For example, an item in the background (distant from the camera) may move at a different rate (number of pixel locations in the array per unit of time or per frame) as compared to an item in foreground (close to the camera). By detecting the differing rates of change in the pixel array that are represented in the successive images, it can be determined that the objects within the images are three-dimensional. In contrast, if a two-dimensional printed picture is used in an attempt to spoof the system, all the pixels in the images of the printed picture move at the same rate. This is because all the features shown on a two-dimensional printed picture are located at essentially the same distance from the camera.

[0189] In particular, items in the foreground move at a higher rate of speed (movement in the pixel array) as compared items in the background. If the device's camera is imaging the user's face, then the foreground will be the user's face and the background will be the scene behind the user, such as a wall, building, trees, or other items behind the user's face. By detecting the rate of change of pixel locations of items in the foreground as compared to the pixel locations in the pixel array that forms the image of items in the background, a determination is made that the scene is a three-dimensional scene.

[0190] Further, pixel velocity analysis also includes edge detection. That, certain identified features in a three-dimensional image may be visible in some frames, but may not be visible in other frames. This typically happens around the edges of an object in the foreground of an image. For example, when a user images his or her face while moving the camera from a distance far away from his or her face to a distance closer to his or her face, objects in the background of an image will disappear as the face of the user takes up more and more space in the frame. Pixel velocity analysis is configured to identify objects in the background around the edges of the face and checks that the objects move to disappear behind the face as the face become enlarged, or that the detected face displaces or covers the features as the face enlarges in the image as the camera moves closer. This will not occur with a two-dimensional picture.

[0191] Further comparisons can be made by observing the rate of pixel locations within the face itself. For example, if pixels on the foreground change at a different rate as compared to pixels on the background, or displace background pixels, then the person can be identified or characterized as three-dimensional. For example, if pixels showing the nose displace pixels on the upper lip and inner cheeks, and the pixels showing cheeks displace pixels representing the ears, and the pixels showing the chin displace pixels representing the neck in the images as the camera is moved closer to the face, then the person being imaged can be identified as a real three-dimensional person. Further, movement or velocity of the identified features themselves change based on their location in the frame and their distance from the camera. Thus, features on the outside of the face exhibit different pixel velocities than features toward the center of the face. Similar, features such as the eyes and cheeks exhibit different pixel velocities as compared to the nose due to the different relative distances from the camera.

[0192] To perform this comparison, two or more images must be captured. For example, a first image is taken at a first distance from the user and then a second image is taken at a second distance from the user, and so on. The comparison is made between the pixel locations of one or more elements (items) in the first image and the second image and can be correlated with the motion of the device as determined by the accelerometer and gyro.

[0193] The pixel velocities detected for various identified features in the images may be mapped to form a "heat" map or other type mapping of the pixel velocities. In this example where a face is being imaged, detected pixel velocities are mapped to each of the detected facial features. For features with high pixel velocities, the map may show "hot" areas, such as for features on the edge of the face such as a chin or cheekbone. For areas with low pixel velocities, such as features at the center of the image like the nose, the map may show "cool" areas. By analyzing this heat or rate of change map, a determination may be made whether the image is that of a two-dimensional picture or a live human in a three-dimensional environment.

[0194] Pixel velocity analysis may advantageously be used in the above described authentication system when the device and camera are moved from one position to another. For example, the system may conduct pixel velocity analysis in two or more images as the person authenticating moves the device to fit his or her face within the small and large ovals as shown in Figures 13A and 13B.

[0195] An example of this process is described with reference to Figure 14. When a first image is received by the device or server, feature recognition is performed on the image to detect predetermined objects within the image in step 1402. In this instance, facial or feature detection is used to confirm the presence of a user's face and/or facial features on the user's face, such as the user's nose, eyes, cheekbones, chin, etc.

[0196] Next, the system analyses the pixel placement in one or more subsequent frames to determine whether the pixels representing the detected features correspond with features located in the foreground or the background of the scene in step 1404.

[0197] In one embodiment, when the user moves the device to fit his or her face within the ovals, such as those shown in FIGS. 13A and 13B, the face of the user is identified as the foreground of the image, or the features within the ovals 1320, 1330. The area around the face showing the room or environment of the person is identified as the background of the image, or the features within area 1315. Additionally, the facial features can be verified to behave with characteristics of relatively different distances and locations in the frame. For example, the nose, mouth, and chin may be considered foreground features while the cheeks, ears and jawline may be considered background features.

[0198] In step 1406, the various features are tracked through successive images to obtain two-dimensional vectors characterizing the flow or movement of the features. The movement of the features in this example is caused as the user moves the device to fit his/her face within the oval shown in the exemplary screen displays of FIGS. 13A and 13B. Such movement may include the nose displacing pixels on the upper lip and inner cheeks and then the cheeks displacing pixels representing the ears and the chin displacing pixels representing the neck.

[0199] The device (processor executing machine readable code stored in memory) then compares image frames (formed by an array of pixels) as the device moves closer to the face of the user. The pixels representing objects in the image are tracked to determine the velocity characteristics of the objects represented by the pixels in the foreground and the background. The system detects these changes in position of items based on pixel data, or two-dimensional pixel velocity vectors, by comparing the successive images taken by the device. When the live, three-dimensional user is authenticating, velocity characteristics of the foreground features (face) and the background features differ significantly as compared to velocity characteristics of a two-dimensional spoof being imaged. That is, the velocity characteristics of facial features are different for a live, three-dimensional person are different as compared to a two-dimensional spoof as the user moves the device to fill his/her face in the oval shown in FIGS. 13A and 13B.

[0200] Thus, in step 1408, the system checks if the two-dimensional vectors of foreground features match expected values of a live, three-dimensional person. The expected values or expected rate of change of an item in an image, defined by pixel location or values, may be based on testing over time such as expected location, expected displacement, expected rate of change of the item, or even expected differences in the rate to change which would indicate three-dimensionality (as opposed to a 2D photograph or video screen of a person). In this example, testing may set an expected value of movement or velocities of the ears, cheekbone, nose, etc. When two-dimensional vectors match expected values, the method proceeds to step 1410 to increase a likelihood that the images are of a live, three-dimensional person. If the two-dimensional vectors do not match expected values, (or match values that are expected when a two-dimensional spoof is used) then the method decreases the likelihood that the images are of a live, three-dimensional person as shown in step 1412.

[0201] When a live, three-dimensional person is being imaged, the two-dimensional vectors, or displacement of pixels between successive images are different in the foreground and background of the image. Thus, in step 1414, the system also analyzes the two dimensional vectors of background objects to determine whether these match expected values. The likelihood of the images being of a live, three-dimensional person is again updated in either steps 1410 or 1412.

[0202] As explained above, some pixels representing certain background objects may appear or disappear completely. For example, as the user moves the device from arm's length to closer in towards his or her face, pixels, edges, and/or features of the user's face will have a higher rate of movement than features in the background, such as a picture frame on a wall, a clock, etc. Additionally, some pixels that are visible on or around the user's face when the device is furthest out from the user will no longer be visible when the user moves the device closer to his or her face. The pixels around a person's face may be defined as the facial halo and the items in these pixels (facial halo) will no longer be captured by the camera in the image due to the person's face taking up more of the image and 'expanding' due to the movement of the camera closer to the person's face. As mentioned above, this check may be referred to as edge detection. In step 1416, the system verifies whether background images around the edges of foreground images match expected values. The system also ensures that pixels representing the edge of the foreground object (such as the face) replace pixels of background objects near the edges of the foreground object. The likelihood of the images being of a live, three-dimensional user is adjusted in step 1410 and 1412 based on the outcome of the edge detection in step 1416. Thus, by tracking these pixels and the displacement, the system can verify whether the pixel velocity analysis is consistent with three dimensional objects having a foreground and background.

[0203] In step 1418, the liveness or three-dimensionality of the user being imaged and authenticated is validated based on the various checks described above. A determination that the user attempting authenticate is a live person is one element that must be met as part of the authentication. Thus, attempts at fraudulent access to an account or device using screens or photos of the person can be more reliably prevented. This prevents attempts at fooling the authentication system with a two-dimensional image such as a printed picture, a digital a projection or a digital screen image of a person.

[0204] Further enhancements may also be achieved using pixel velocity analysis for liveness or three-dimensionality. When the user brings the device (camera) closer to the user's face, the facial features will distort differently due to the large relative distances between the various features and the camera and the placement of the features in the field of view of the camera as the camera comes closer to the face. This effect may be referred to as perspective distortion. When this distortion begins to occur, pixels in the center of the frame that represent the features in the center of the face such as the nose will have the least amount of distortion in the frame, whereas the pixels that represent the outer portions of the face such as the cheeks, the chin, and the forehead will show the most relative pixel movement (more than pixels at the center of the frame) and the highest acceleration. Thus, the three-dimensionality can also be shown by comparing the features on the face itself. This is because at close proximity to the device, facial features closer to the device can be considered foreground features, and facial features farther from the device are background features. For example, pixels representing the nose will show less movement between frames than pixels representing the cheekbone because of the nose's shorter relative distance from the camera when the device is held at eye level.

[0205] Pixel velocity analysis may also be used to track liveness characteristics that are very difficult to recreate during a fraudulent authentication event. For example, the human eyes are never completely still even when focusing on an object. There is always, quick involuntary movement of the eyes as the eyes scan an object, moving around to locate interesting parts of the object, and developing a mental, three-dimensional "map" corresponding to the scene. These movements are called saccades and are involuntary. Saccades last from 20ms-200ms and serve as the mechanism of eye fixation. Two-dimensional velocity vectors, based on movement of the eyes based on pixel values, may thus be generated by the saccadic motion of the eyes across frames. The presence of these vectors, the hertz of the eye jitter and the acceleration of the pixel movement between frames can be compared to measurements of verified sessions and can be used to increase confidence that the user in front of the camera is not an inanimate spoof such as a photo, a wax sculpture, or doll.

[0206] In another example, when a bright light is presented to the human eyes, the pupil will constrict to mitigate the light's path to the retina. Cameras on typical mobile devices such as smart phones generally operate at high enough resolutions that two-dimensional velocity vectors will track the pupils constricting when compared over a series of frames where the amount of light entering the eyes increases, such as when the user moves the device and screen closer to his or her face, or when a front-facing flash of a mobile device is activated.

[0207] Another feature that may be detected by pixel velocity analysis is reflection off the eye of the user. The surface of the eye reflects a larger amount of the light hitting it when the pupil contracts, providing a brighter reflection of the light emitting object. In the case of the device with an illuminated screen being moved closer to the face of the user, the size and brightness of the reflection of the device's screen will increase while the size of the pupil contracts. It is possible to observe and document these two-dimensional vectors in a consistent motion path and then provide a liveness evaluation on video frame sessions based on the expected two-dimensional vectors being observed or absent.

[0208] Facial recognition algorithms use landmarked points on the face to measure the distance and angles between the facial features. This creates the unique look of individuals and the corresponding unique biometric data. In some embodiments, pixel velocity analysis may be used not only to verify the three-dimensionality of the person, but may also be used as an additional or alternative facial recognition algorithm.

[0209] In this instance, the device may recognize two-dimensional vectors of the features throughout the user's face as the user provides enrollment images while moving the camera in and out to fit the ovals as shown in Figures 13A and 13B. These two-dimensional vectors formed are caused by the distortion and movement of the facial features that occurs when the camera is brought close to the user's face due to the three-dimensional characteristics of the user's face. Tracking the two-dimensional vectors and mapping the two-dimensional vectors to each of the features of the user's face results in the creation of a unique "heat" map of the user's face using a two-dimensional camera. The "heat" map indicates "hot spots" where larger two-dimensional vectors show increased pixel velocities of certain facial features as opposed to "cool" areas where smaller two-dimensional vectors show small pixel velocities of other facial features.

[0210] Such maps have been found to be unique to each user as the user moves the device with the camera in and out to fit the ovals as shown in FIGS. 13A and 13B. Thus, the map of the two-dimensional vectors of pixel movement corresponding to facial features resulting from the device movement or the head movement can be used itself as biometric data in addition to verifying three-dimensionality of the person being imaged. That is, the two-dimensional vectors of the various facial features may not only be compared to expected values to determine the three-dimensionality of the user's face, but the two-dimensional vectors of the various facial features created as the user moves the device and camera relative to the user's face are themselves unique to each user based on the unique face of the user. Thus, unique heat maps are captured based on the three-dimensional facial features of the user registering with the authentication system, which can be associated with the user as biometric information for authentication.

[0211] Using previously authenticated and stored heat maps of the users face, the system may thus analyze new authentication images with pixel velocity analysis not only to determine the liveness or three-dimensionality of the person, but also to authenticate the identity of the person. These checks may occur simultaneously. That is, the system compares the heat map obtained from the authentication images to determine whether it matches the heat map obtained during enrollment based on person's unique, three-dimensional facial features. The two-dimensional vectors generated by the pixel velocity analysis are also examined to ensure they correspond with a three-dimensional person as opposed to a two-dimensional spoof. If the images captured by the device camera are determined to not represent a live user or do not match the authentication information, then it is contemplated that authentication will fail and access will be denied.

[0212] Pixel velocity analysis may allow for use of the authentication system with a stationary two-dimensional camera, such as on a laptop, an ATM, a car dashboard, or a desktop. That is, with the liveness detection provided by the pixel velocity analysis, it may be possible to omit the movement information provided by the accelerometer, magnetometer, and gyroscope of the device, which are lacking in such stationary devices as an ATM machine. This may be done by the user moving his or her head in relation to a stationary camera. The user's movement may be from normal, observable human movements, or may be a user action that is deliberately requested such as instructing a user to fit his/her face into an oval changing size on a screen so that the user leans in to fill the larger oval. Alternatively, the instruction could be a voice instruction. This provides the ability to verify the three-dimensionality of the user from the stationary two-dimensional camera. The individual's identity may be verified using facial recognition algorithms while additional identity confirmation, liveness and three-dimensionality detection can be provided by the pixel velocity analysis when compared to previously captured data from a similar motion scenario.

Touch Screen Enhancements

[0213] Additional added security modifications may include information about a user's finger. Many mobile devices with touch screens can detect the location and approximate size of a user's touch on the screen. Accordingly, an approximate size of a user's finger or thumb may be measured by the system. In addition to the size of a finger, an orientation angle of the finger or whether the fingers or thumbs of the right or left hand are used can be detected.

[0214] In one embodiment, a user selects an account to open, begins enrollment imaging, or begins authentication imaging by touching the touchscreen of the user device. The authentication system may thus detect whether the touch by a user during authentication corresponds with previously stored enrollment information including the size of the user's finger or thumb, amount of pressure applied to the screen and whether the user is right or left handed. This adds an additional security layer for the authentication system.

[0215] Furthermore, the authentication system may require that the user initiates an authentication by touching a fingerprint reader or the touchscreen in one or more predetermined manners. In one embodiment, as shown in Figure 15, a touchscreen 1410 may be divided up into predetermined regions 1420. For example, there may be nine equal, circular, square, or other shaped regions 1420 on the touchscreen 1410 of the mobile device. During enrollment, the user selects one of the regions 1420 of the screen 1410 to touch to initiate authentication. During authentication, if the preselected region 1420 is not touched to begin authentication or during the entire authentication process, then authentication is denied. This is but one possible design possibility and other design options are contemplated.

[0216] The regions 1420 on the touchscreen may be visually represented by a grid, or may not be displayed at all on the touchscreen 1410. As shown in Figure 16, in addition to or in place of the regions 1420, buttons 1520 may be displayed on a touchscreen 1510. Here, the user may initiate the authentication by pressing one or more of the buttons 1520 in a predetermined pattern. The user may also initiate authentication via a predetermined swiped pattern. The position to be touched by the user may change with each authentication attempt and may be conveyed to the user through any instructions from the authentication server, such as a code, number, letter, color, captcha or other indicator.

Voice Parameters

[0217] It is also contemplated that the user could record their voice by speaking a phrase while recording their images during the enrollment process when first using the system. Then, to authenticate, the user would also have to also speak the phrase when also moving the mobile device to capture the image of their face. Thus, one additional path parameter may be the user's spoken voice and use of voice recognition as another layer or element of the authentication process.

Image Quality Assurance

[0218] The authentication system may also process the images received from the mobile device to determine if the images are of sufficient quality. For example, the system may check the images for blurriness caused by the images being out of focus or by the camera lens being obscured by fingerprints, oils, etc. The system may alert that user that the quality of the images is insufficient (or too bright or too dark) and direct the user to adjust a focus, exposure, or other parameter, or to clean the lens of the camera.

Autofocus

[0219] The authentication system may also utilize an autofocus feature when the mobile device camera is equipped with such. For example, when an actual, three-dimensional person is being imaged, the system checks to ensure that the sharpness of the image changes throughout as the camera perform auto-focusing. In another embodiment, the system may control the autofocus so that the camera focuses on a first location or distance to check for sharpness (in focus) of a portion of the image containing a face. The system then controls the camera to focus at a second location or distance where the presence of a face is not detected and check for sharpness (in focus) of a portion of the image. If a three-dimensional person in a real environment is being imaged, it is expected that the focus settings should be different at the first and second locations, which suggests a real person is presently being imaged. However, if the face appears to become large but the focus points of both locations are the same, this indicates that a two-dimensional video screen is being imaged, indicating a fraudulent login attempt.

[0220] The system may also control the auto-focus of the device to check for different focus points of different particular features in the image. For example, when a person's face is imaged from the front, a person's ear is expected to have a different focus point (more distant) than the tip of a person's nose.

Images of Login Attempt

[0221] The authentication server may also be configured to store the authentication images for a predetermined length of time. The images may provide additional security benefits as evidence of a person attempting to log in to a user's account. For example, the system may store a predetermined number of prior log in attempts, such as twenty login attempts, or store images from login attempts for a predetermined time period, such as during the past seven days or weeks. Any fraud or attempted fraud will result in pictures of the person attempting the login being stored or sent to the authentication server of the account server.

[0222] The mere knowledge that photos will be taken and sent is a significant deterrent to any potentially dishonest person because they know their picture will be taken and stored, and it is an assurance of security to the user. Likewise, any attempted and failed attempt can have the photo stored and indicator of who is attempting to access the account. It is also contemplated that an email or text message along with the picture of the person attempting the failed log in may be sent to the authorized user so they know who is attempting to access their account. This establishes the first line of security for the account as the user with the photo or image also being possessed by the authentication server.

Adaptive Match Thresholds

[0223] Further, the level or percentage of correspondence between the enrollment information and the authentication information to authenticate the user may change over time. In other words, the system may comprise an adaptive threshold.

[0224] After a user regularly uses the authentication system described above, the user will have logged in with the system by moving the mobile device in the predetermined path relative to his or her head many times. Accordingly, it may be expected that as the user will gain experience using the authentication system, and that the user will gradually settle into a comfortable and standardized motion path. In contrast, the initial enrollment movement of a user will likely be the most awkward and clumsy movement as the user has little experience with the authentication system.

[0225] To make the authentication system more convenient for the user without losing security, the adaptive threshold system allows the enrollment movement to adapt so that the user is not locked into the awkward and clumsy initial movement as the enrollment movement. To facilitate this, upon each successfully authorization, the successful authorization movement is stored, and the motion path is added to a list of acceptable motion paths. The list of acceptable motion paths may be limited to a predetermined number of paths. When a new successfully authorization is completed and the list of acceptable motion paths is full, the older enrollment motion path is deleted and the newest is stored in its place. Alternatively, the motion path that is least like the other motion paths stored on the list may be deleted. Thus, by storing the most alike or newest motion paths, the enrollment movement may slowly adapt over time as the user because familiar with the system and settles into a comfortable motion path for authentication.

[0226] In addition, other enrollment information may adaptively change in a similar manner as the user information. For example, successful authentication photos or biometric information can be stored as part of the enrollment information and old enrollment information may be discarded over time. In this manner, the authentication system can be convenient for a user even over a long period of time as the user experiences aging, facial hair growth, different styles of makeup, new glasses, or other subtle face alterations.

[0227] Determining how much variance is allowed over time in the motion path, the biometric information, or both may be set by the entity requiring authentication to meet that entity's security requirements. Time or number of scans after the initial enrollment can be used to modify the adaptive threshold. For example, during a first few days after enrollment, the threshold may be lower while a security threat is low and the differences in paths are likely to be higher. After several authentications or several days, the threshold may increase. The threshold further may be set based on trending data of either the motion path or biometric information. For example, the threshold may be more lenient in a direction the data is trending, while having a tighter tolerance for data against the trend.

[0228] A temporal aspect may also be added along with the location information. For example, if the user conducts and authenticates a transaction near his home, and then one hour later another transaction is attempted in a foreign country, the transaction may be denied. Or it may be denied if the distance between the prior authentication location and the next authentication location cannot be traveled or is unlikely to have been traveled in the amount of time between login or authentication attempts. For example, if the user authenticates in Denver, but an hour later an attempt is made in New York, Russia or Africa, then either first or second attempt is fraudulent because the user likely cannot travel between these locations in 1 hour.

[0229] Further, if the next transaction is attempted at a more reasonable time and distance away from the first transaction, the level of correspondence threshold may be raised to provide added security, without automatically denying the transaction. Likewise, an altimeter may be used such that if the altitude determined by the mobile device is different than the altitude of the city in which the user is reported to be located, then this may indicate a fraud attempt. Thus, altitude or barometric readings from the mobile device may be used to verify location and can be cross referenced against GPS data, IP address or router location data, or user identified location.

Upgrading Facial Recognition Algorithms

[0230] Often, new facial recognition algorithms or other features of an application may need to be updated to ensure the security of the authentication system. When new algorithms are implemented, it is necessary to obtain new enrollment information corresponding to the new algorithm. However, it is undesirable to require users who have already authenticated with the system enroll again every time the application is updated. This would inconvenience and frustrate the user if, for example, the user is logging into a payment system to make a purchase at a store, and the application prompts the user to enter a password and/or re-enroll rather than allowing the user to quickly complete the transaction as planned.

[0231] Accordingly, in one embodiment the system performs a biometrics "handoff" to update the enrollment information with a new facial recognition algorithm based on an application or software update. For example, when the software or application is updated with a new facial recognition algorithm, the application retains the prior facial recognition algorithm. During the next login attempt the images captured are used to authenticate the user along with any and all liveness checks using the older facial recognition algorithm. If the person is authenticated, the images are then authorized to be used by the new facial recognition algorithm to generate new enrollment information with the new biometrics algorithm. The new enrollment biometric information is considered trustworthy because it is based on a successful login attempt using the prior biometrics algorithm. This process may be done a certain number of times (login with old algorithm creating enrollment information with new algorithm) until a sufficient biometric profile on the new facial recognition algorithm is created. Once the new profile is created, the prior biometric profile based on the old facial recognition algorithm is deleted. In this manner, it is not necessary for a user to re-enroll when the application is updated with new facial recognition algorithms or other features.

Random Image Distortion

[0232] To provide an additional layer of security to the facial recognition authentication system, the system may utilize random image distortion. For example, a user may be assigned a random distortion algorithm upon enrollment into the system. The distortion algorithm may include such distortions to the image as widening or narrowing the person's face by a predetermined amount, adding or superimposing a predetermined shape at a predetermined position on the user's face. As one example of this, the distortion may be a circle superimposed at 100 pixels above the user's left eye.

[0233] With the uniquely assigned distortion on the images from the user, the biometric data for that user will be unique to the account or device used by the user. That is, the enrollment biometrics stored on the authentication server or on the mobile device will reflect not only the facial features of the user, but also will reflect the uniquely assigned image distortion. Thus, even if an accurate, fraudulent representation of a person were used on a different device or via a different account, the proffered authentication biometrics would not sufficiently correspond due to a different or an absence of the unique distortion. Thus, the overall security may be enhanced.

Security Layers

[0234] It is noted that each of the above embodiments, modifications, and enhancements may be combined in any combination as necessary to create multiple layers of security for authentication. For example, the facial recognition may be combined with motion detection or path detection, or may operate independently of these features for authentication. Further, when more than one of the above described enhancements or modifications are combined, the authentication system may be configured so as not to provide any feedback or indication on which layer failed authentication.

[0235] For example, when a predetermined touch pattern to initiate authentication is combined with the authentication movement and facial authentication, the system does not indicate whether a touch pattern was incorrect, or the authentication movement or authentication images failed to correspond to the enrollment information. Instead, the system provides an identical denial of authentication no matter what failure occurs. This is the case when any number of the security features described above are combined. In this manner, it is difficult for a fraudster to detect what aspect of the fraudulent credentials must be corrected, further enhancing the security of the system.

[0236] All of the above features may be incorporated together, or only some features may be used and others omitted. For example, when the device prompts the user to move the device so that the user places his or her head within a first small frame (such as an oval) then to a second large frame (such as in FIGS. 7A, 7B, 13A, and 13B), the system may be configured such that facial recognition need not be performed on the image(s) in the first frame (distantly captured frames). The security of the system is maintained by performing facial recognition throughout the imaging at some point between the first and second frames, and at the second frame. This may especially be true when also integrated with another layer of security, such as checking eye tracking following a moving object on the screen or reading a reflection of a QR code or random shape off the user's eye. In another embodiment, when two or more cameras are used creating three dimensional, stereoscopic images, the facial recognition may not be performed at the first, far away frame, but instead the liveness of the person may be validated at the closer in frame only after the movement of the device. In still other embodiments, other security layers may be used, and the motion parameters may be omitted. Such combinations may be beneficial for larger or stationary devices, such as gaming laptop computers, personal desktop computers, a stationary kiosk, or the like.

Example Applications

[0237] Likewise, although described herein as financial account authentication, the authentication using path parameters and image data may be implemented in any environment requiring verification of the user's identity before allowing access, such as auto access, room access, computer access, web site or data access, phone use, computer use, package receipt, event access, ticketing, courtroom access, airport security, retail sales transaction, IoT access, or any other type of situation.

[0238] For example, an embodiment will be described where the above authentication system is used to securely conduct a retail sales transaction. In this embodiment, a user is enrolled with the authentication server or an authentication application on the mobile device as described above and has generated enrollment information including enrollment images and/or biometrics, and enrollment movement. In this example, the user initiates or attempts to complete a transaction at a retail establishment with a credit card, smart card, or using a smart phone with NFC capabilities.

[0239] The user begins the transaction by swiping a credit card, smart card, or using an application on a smartphone with NFC capabilities to pay for goods or services. The retail establishment would then authorize the card or account with the relevant network of the financial institution ("Gateway"). For example, the retail establishment, through a Gateway such as one operated by VISA or AMERICAN EXPRESS would determine whether the account is available and has sufficient available funds.

[0240] The Gateway would then communicate with the authorization server to authorize the transaction by verifying the identity of the user. For example, the Gateway may send an authorization request to the authentication server, and the authentication server then sends a notification, such as a push notification, to the user's mobile device to request that the user authenticate the transaction.

[0241] Upon receipt of the notification from the authentication server, such as through a vibration, beep, or other sound on the mobile device, the user may then authenticate his or her identify with the mobile device. The authentication server may also send information concerning the transaction to the user for verification by the user. For example, the authentication server may send information that causes the mobile device to display the merchant, merchant location, and the purchase total for the transaction.

[0242] Next, as before, the user may hold the mobile device and obtain a plurality of authentication images as the user moves the mobile device to different positions relative to the user's head. While moving the mobile device to obtain the authentication images, the mobile phone further tracks the path parameters (authentication movement) of the mobile device via the gyroscope, magnetometer, and the accelerometer to obtain the authentication movement of the device. The mobile device may then send the device information, the authentication images, and the authentication movement to the authentication server. In other embodiments, the mobile device may process the images to obtain biometric data and send the biometric data to the server. In still other embodiments, the mobile device may process the images, obtain the authentication information, compare the authentication information to enrollment information stored on the mobile device, and send pass/fail results of the comparison to the authentication server.

[0243] The authentication server may then authenticate the identity of the user and confirm that the user wishes to authorize the transaction on his or her account if the device information, authentication images and/or biometrics, and authentication movement correspond with the enrollment device information, the enrollment images and/or biometrics, and the enrollment movement. The authentication server then transmits an authorization message to the Gateway. Once the gateway has received confirmation of the authorization, the Gateway then communicates with the retail establishment to allow the retail transaction.

[0244] Several advantages may be obtained when a retail transaction is authorized utilizing the above system and method. Because the identity verification of the user and the confirmation of the transaction is completed via the authentication system and mobile device, there is no longer a requirement for a user to provide his or her credit card or signature, or to enter a pin number into the retailer's point of sale system. Further, the retail establishment does not need to check a photo identification of the user. The above method and system also has the advantage that it provides secure transactions that can work with mobile and online transactions that do not have cameras, such as security cameras, on the premises.

[0245] In the secure retail transaction described above, the user obtains the total amount due on his or her mobile device from the retail establishment via the Gateway and authentication server. However, in one embodiment, the mobile phone may use the camera as a bar code, QR code, or similar scanner to identify the items and the prices of the items being purchased. The mobile device may then total the amount due and act as the checkout to complete the transaction with the retail establishment.

[0246] In another embodiment, a user of the application may want to anonymously pay an individual or a merchant. In this instance, the user would designate an amount to be paid into an application, and the application would create a unique identifying transaction number. This number may then be shown to the second user, so the second user can type the identifying transaction number on an application on a separate device. The unique identifying transaction number may also be sent from the user to the second user via NFC, Bluetooth, a QR code, or other suitable methods. The second user may also type the amount and request payment.

[0247] Upon receiving the payment request and unique identifying transaction number, the authentication server may send a notification to the first user's mobile device to authenticate the transaction. The user would then verify his or her identity using the facial recognition authentication system described above. The user may alternatively or additionally verify his or her identity using other biometric data such as a fingerprint or retina scan, path-based motion and imaging, or the user may enter a password. Upon authentication, the user's device would send a request to the user's payment provider to request and authorize payment to the second user. In this manner, the payment may be done securely while the users in the transaction are anonymous.

[0248] According to one embodiment, as an additional measure of security, the GPS information from the mobile device may also be sent to the authentication server to authenticate and allow the retail transaction. For example, the GPS coordinates from the mobile device may be compared with the coordinates of the retail establishment to confirm that the user is actually present in the retail establishment. In this manner, a criminal that has stolen a credit card and attempts to use the card from a distant location (as compared to the retail location) is unable to complete a transaction because the user's phone is not at the location of the retail establishment. IP addresses may also be used to determine location.

[0249] As explained above, the level or percentage of correspondence between the enrollment information and the authentication information to authenticate the user may also be adjusted based on the coordinates of the GPS of the mobile device. For example, if the retail establishment and GPS coordinates of the mobile device are near a user's home, then the level of correspondence may be set at a lower threshold, such as at a 99% match rate. Alternatively, if the location is very far from the user's home, and is in a foreign country, for example, then the level of correspondence may be set at a higher threshold, such as at a 99.999% match rate.

[0250] While various embodiments of the invention have been described, it will be apparent to those of ordinary skill in the art that many more embodiments and implementations are possible that are within the scope of this invention. In addition, the various features, elements, and embodiments described herein may be claimed or combined in any combination or arrangement.

CLAIMS

What is claimed is:

1. A computing device for verifying three-dimensionality of a user via a user's camera equipped computing device, the computing device comprising:

a processor configured to execute machine executable code;

a screen configured to provide a user interface to the user;

a camera configured to capture images;

one or more memories configured to store machine readable instructions that are stored on the memory of the authentication server which when executed by the processor, cause the computing device to:

capturing at least one first image of the user taken with the camera of the computing device at a first location which is a first distance from the user;

processing the at least one first image or a portion thereof to create first data;

capturing at least one second image of the user taken with the camera of the computing device is at a second distance from the user, the second distance being different than the first distance, the capturing at least one second image of the user occurring after movement of the camera or the user to establish the camera at the second distance from the user;

processing the at least one second image or a portion thereof to create second data;

comparing the first data to the second data to determine whether expected differences exist between the first data and the second data which indicates three-dimensionality of the user;

verifying the images of the user exhibit three dimensional traits when the expected differences exist between the first data and the second data as a result of capturing the at least one first image and the at least one second image at different distances from the user.

2. The system according to claim 1, further comprising:

interpolating the first data and the second data to obtain estimated intermediate data;

capturing at least one third image of the user taken with the camera of the computing device at a third distance from the user, the third distance being between the first distance and the second distances;

processing the at least one third image or a portion thereof to obtain third data; and

comparing the estimated intermediate data with the third data to determine whether the third data matches the estimated intermediate data.

3. The system according to claim 1, further comprising verifying the presence of one or more features on a side of a user's head in the at least one first image, and verifying the absence or reduced visibility of the one or more features on the side of the user's head in the at least one second image due to image capture at different distances from the user's head, wherein the first distance is larger than the second distance.

4. The system according to claim 1, wherein the machine readable instructions is configured to display one or more prompts on the screen of the computing device to guide the user to capture the at least one first image at the first distance and the at least on second image at the second distance.

5. The system according to claim 1, further comprising comparing the first data, second data, or both to enrollment data derived from an enrollment image, the enrollment image captured and stored prior to an authenticating; and

only authenticating the user when the first data, the second data, or both match the enrollment data within a predetermined threshold.

6. The system according to claim 1, wherein the computing device is a hand-held device, and the user holds the device at the first and second distance to capture the at least one first image and the at least one second image.

7. The system according to claim 1, wherein the first data and the second data comprise biometric data.

8. The system according to claim 1, wherein the first data and the second data comprise a mapping of facial features.

9. The method according to claim 1, wherein the first image and the second image is of the user's face and the user's head and facial features are held steady and without movement during capture of the first image and the second image.

10. A method for authenticating three-dimensionality of a user with a computing device during an authentication session, the method comprising:

capturing at least one first image of the user taken with a camera at a first location which is a first distance from the user, the camera associated with the computing device;

processing the at least one first image or a portion thereof to create first data;

moving the camera from the first location to a second location, the second location being a second distance from the user, or the user moving to change the distance between the user and the camera from the first distance to the second distance;

capturing at least one second image of the user taken with the camera associated with the computing device when the camera is the second distance from the user, the second distance being different than the first distance;

processing the at least one second image or a portion thereof to create second data;

comparing the first data to the second data to determine whether expected differences exist between the first data and the second data which indicated three-dimensionality of the user;

verifying the images of the user exhibit three-dimensional traits when the first data and the second data have expected differences resulting from the at least one first image being captured at a different distance from the user than when the at least one second image is captured.

11. The method according to claim 10, further comprising:

interpolating the first data and the second data to obtain estimated intermediate data;

capturing at least one third image of the user taken with the camera of the computing device at a third distance from the user, the third distance being between the first distance and the second distances;

processing the at least one third image or a portion thereof to obtain third data; and

comparing the estimated intermediate data with the third data to determine whether the third data matches the estimated intermediate data.

12. The method according to claim 10, further comprising verifying the presence of ears of the user in the at least one first image, and verifying the absence or reduced visibility of the ears in the at least one second image, wherein the first distance is larger than the second distance.

13. The method according to claim 10, wherein the computing device is configured to display one or more prompts on a screen associated with the computing device to guide the user to capture the at least one first image at the first distance and the at least on second image at the second distance.

14. The method according to claim 13, wherein the one or more prompts are an oval shape guide on the screen within which an image of a face of the user is aligned to capture the at least one first image and the at least one second image.

15. The method according to claim 10, wherein the computing device is a hand-held device, and the user holds the computing device at the first distance when capturing at least one first image and at the second distances when capturing the at least one second image.

16. The method according to claim 10, wherein the first data and the second data comprise biometric data.

17. The method according to claim 10, wherein the first data and the second data comprise a mapping of facial features.

18. The method according to claim 10, further comprising illuminate a screen of the computing device while capturing the at least one first image and/or the at least one second image, and processing the at least one first image and/or the at least one second image to detect a reflection of the illumination from a face of the user.

19. The method according to claim 10, wherein a face of the user is held steady when capturing the at least one first image and the at least one second image and the camera moves from the first location to the second location.

20. The method according to claim 10, wherein the first data and the second data are maintained on the computing device.

21. The method of claim 10 wherein the computing device is one of a smartphone, tablet, laptop, or desktop computer.

ABSTRACT

Systems and methods for enrolling and authenticating a user in an authentication system via a user's camera of camera equipped mobile device include capturing and storing enrollment biometric information from at least one first image of the user taken via the camera of the mobile device, capturing authentication biometric information from at least one second image of the user, capturing, during imaging of the at least one second image, path parameters via at least one movement detecting sensor indicating an authentication movement of the mobile device, comparing the authentication biometric information to the stored enrollment biometric information, and comparing the authentication movement of the mobile device to an expected movement of the mobile device to determine whether the authentication movement sufficiently corresponds to the expected movement.

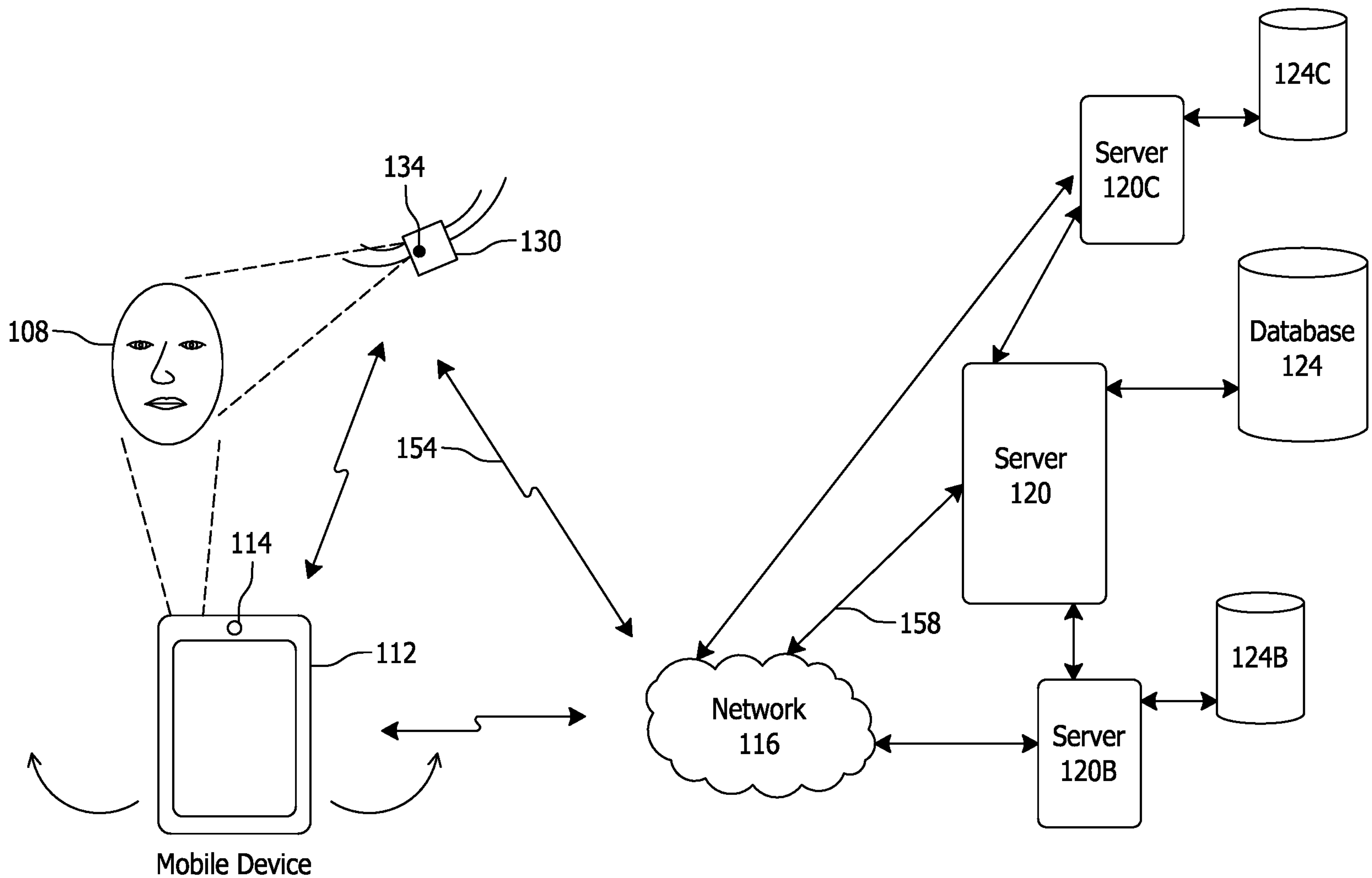

134
130
108
154
114
112
Mobile Device
Network
116
158
Server
120C
124C
Database
124
Server
120
124B
Server
120B

FIG. 1

1/15

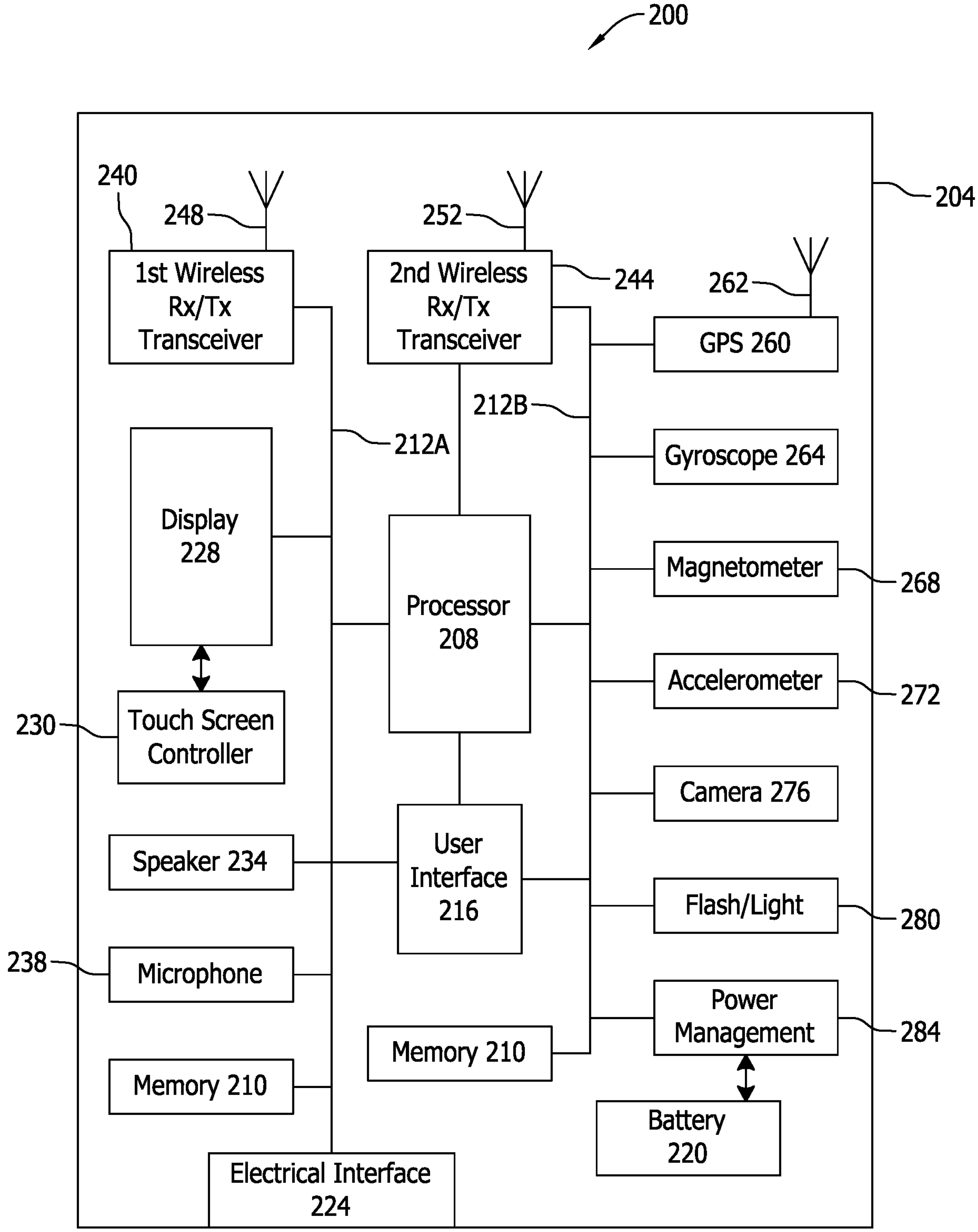

200
204
240
248
252
1st Wireless Rx/Tx Transceiver
2nd Wireless Rx/Tx Transceiver
244
262
GPS 260
212B
212A
Gyroscope 264
Display 228
Processor 208
Magnetometer
268
Accelerometer
272
230
Touch Screen Controller
Camera 276
Speaker 234
User Interface 216
Flash/Light
280
238
Microphone
Power Management
284
Memory 210
Memory 210
Battery 220
Electrical Interface 224

FIG. 2

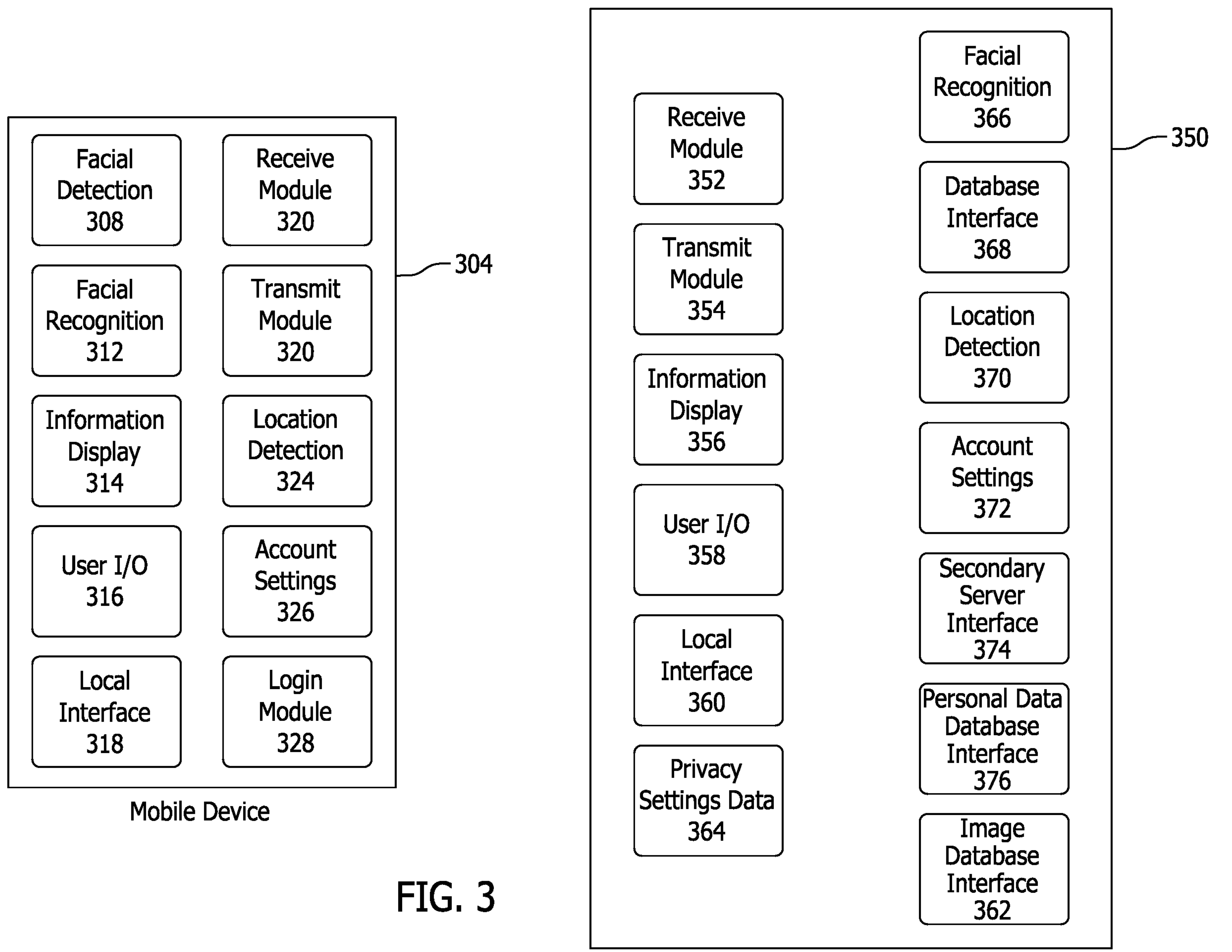

Facial Detection 308
Receive Module 320
Facial Recognition 312
Transmit Module 320
Information Display 314
Location Detection 324
User I/O 316
Account Settings 326
Local Interface 318
Login Module 328
304
Mobile Device
Receive Module 352
Transmit Module 354
Information Display 356
User I/O 358
Local Interface 360
Privacy Settings Data 364
Facial Recognition 366
Database Interface 368
Location Detection 370
Account Settings 372
Secondary Server Interface 374
Personal Data Database Interface 376
Image Database Interface 362
350

FIG. 3

3/15

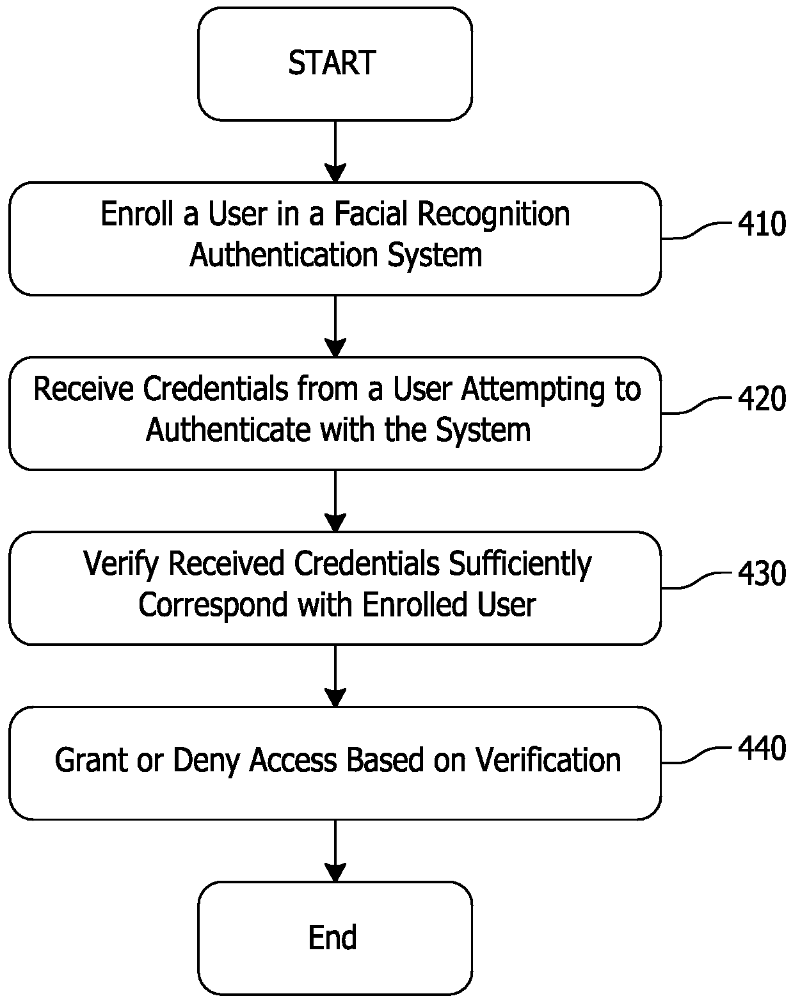

START
Enroll a User in a Facial Recognition Authentication System
410
Receive Credentials from a User Attempting to Authenticate with the System
420
Verify Received Credentials Sufficiently Correspond with Enrolled User
430
Grant or Deny Access Based on Verification
440
End

FIG. 4

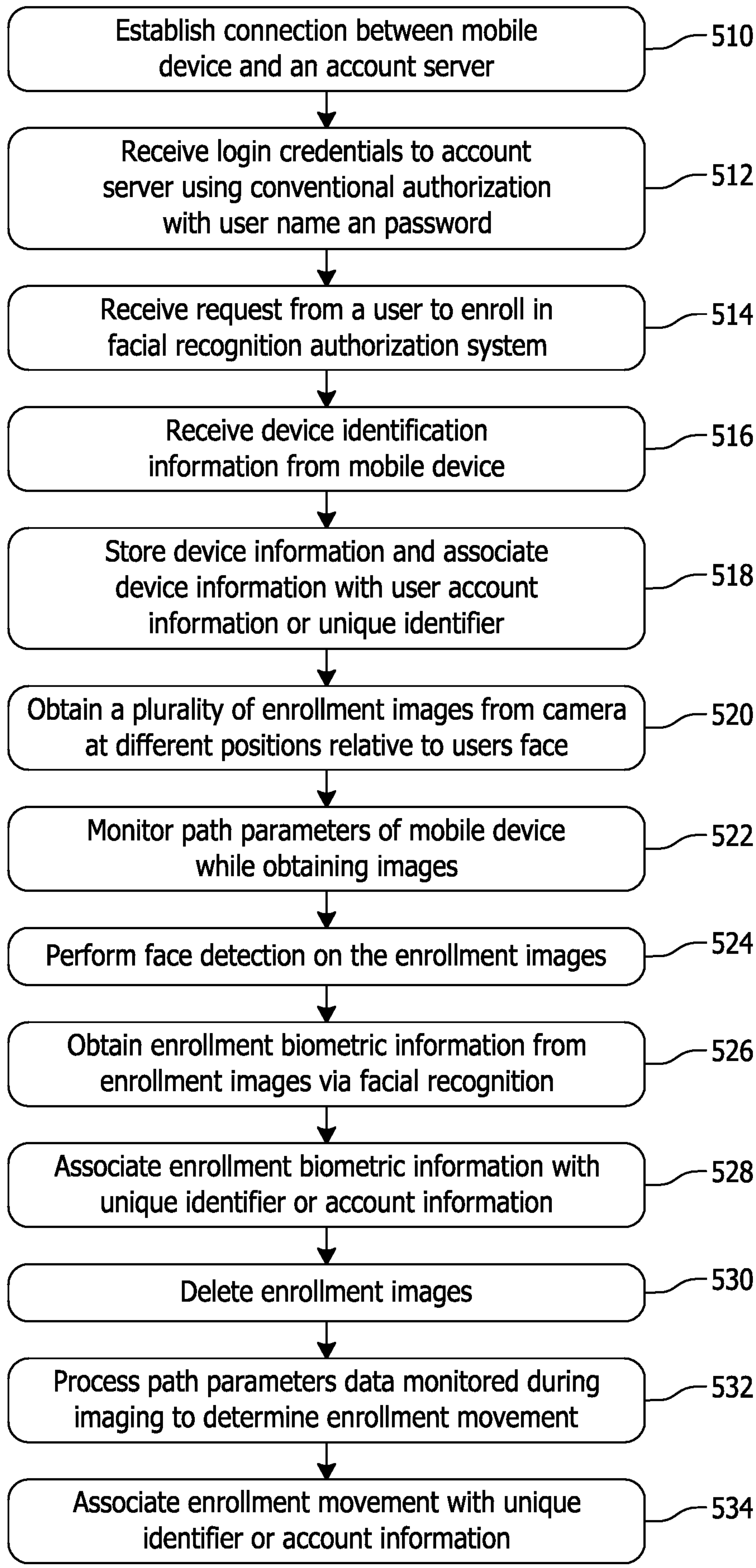

Establish connection between mobile device and an account server
510
Receive login credentials to account server using conventional authorization with user name an password
512
Receive request from a user to enroll in facial recognition authorization system
514
Receive device identification information from mobile device
516
Store device information and associate device information with user account information or unique identifier
518
Obtain a plurality of enrollment images from camera at different positions relative to users face
520
Monitor path parameters of mobile device while obtaining images
522
Perform face detection on the enrollment images
524
Obtain enrollment biometric information from enrollment images via facial recognition
526
Associate enrollment biometric information with unique identifier or account information
528
Delete enrollment images
530
Process path parameters data monitored during imaging to determine enrollment movement
532
Associate enrollment movement with unique identifier or account information
534

FIG. 5

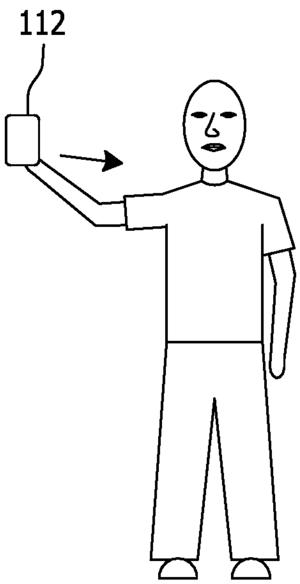


FIG. 6A

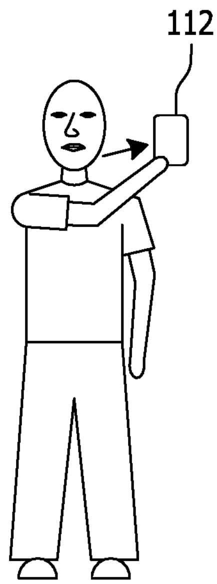


FIG. 6B

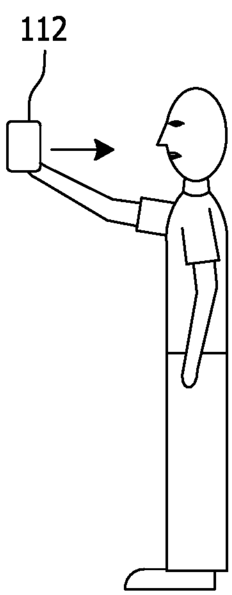


FIG. 7A

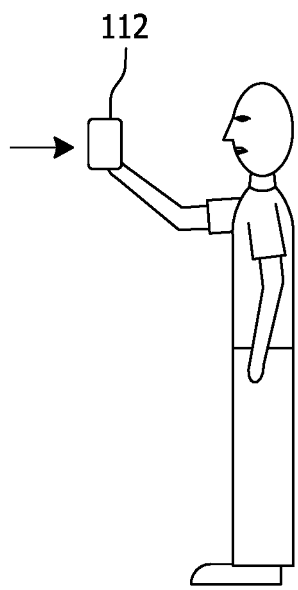


FIG. 7B

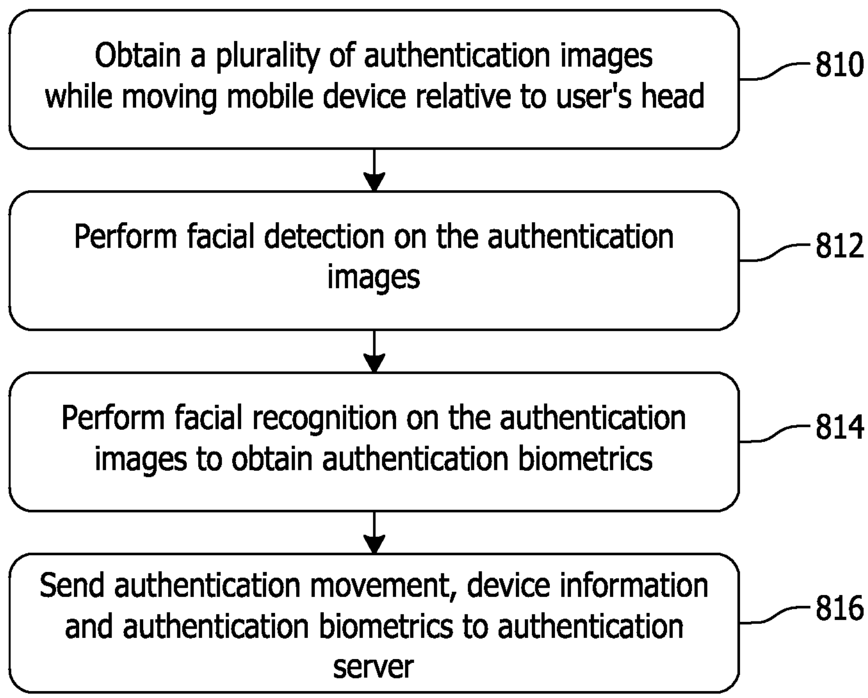

Obtain a plurality of authentication images while moving mobile device relative to user's head
810
Perform facial detection on the authentication images
812
Perform facial recognition on the authentication images to obtain authentication biometrics
814
Send authentication movement, device information and authentication biometrics to authentication server
816

FIG. 8

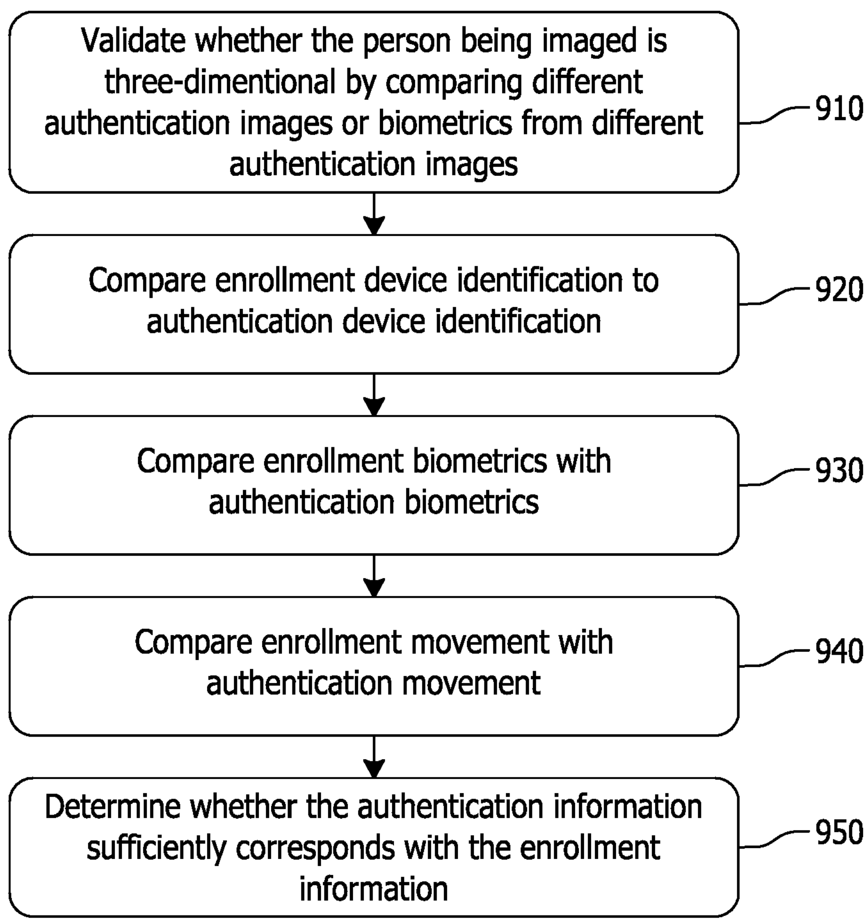

Validate whether the person being imaged is three-dimentional by comparing different authentication images or biometrics from different authentication images
910
Compare enrollment device identification to authentication device identification
920
Compare enrollment biometrics with authentication biometrics
930
Compare enrollment movement with authentication movement
940
Determine whether the authentication information sufficiently corresponds with the enrollment information
950

FIG. 9

FIG. 10

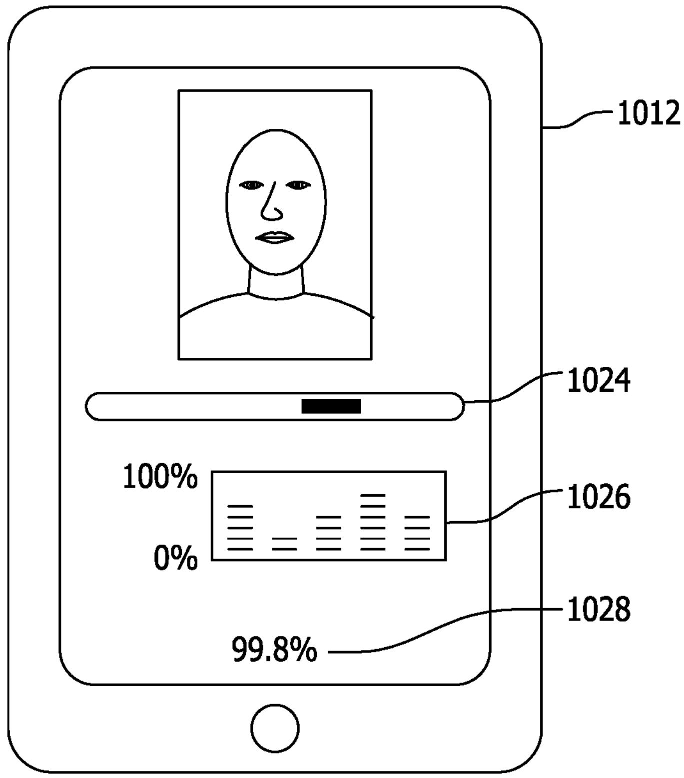
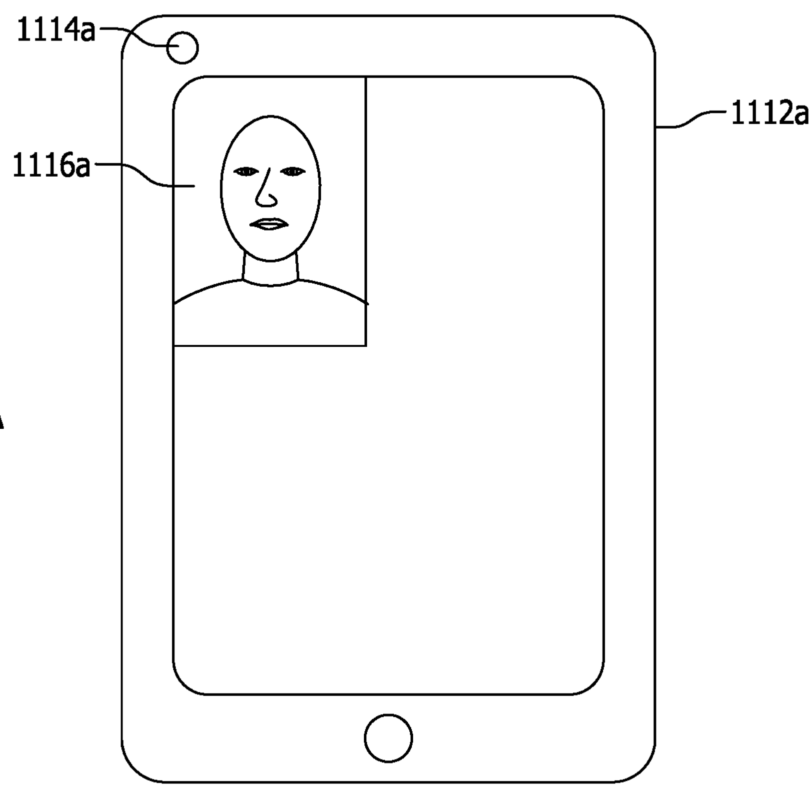


FIG. 11A



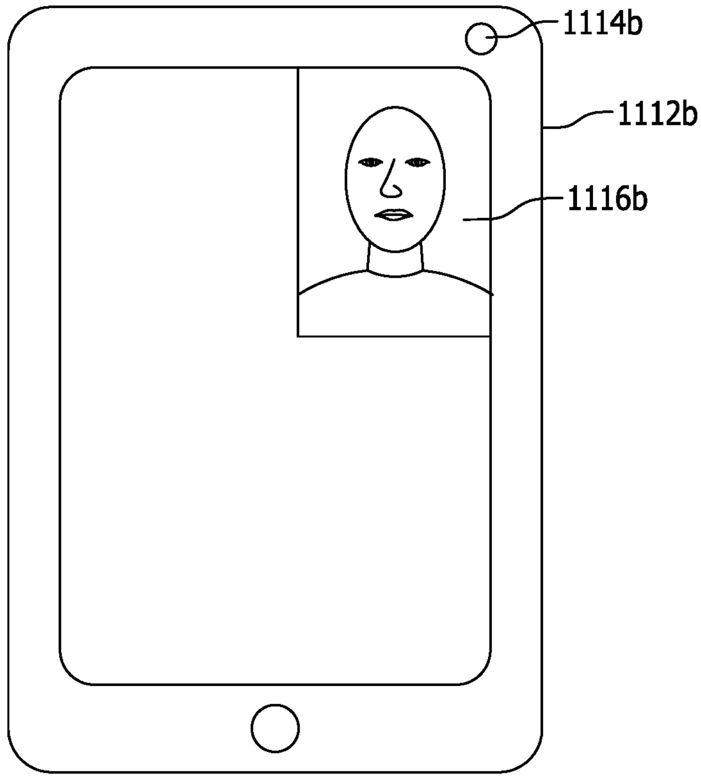


FIG. 11B

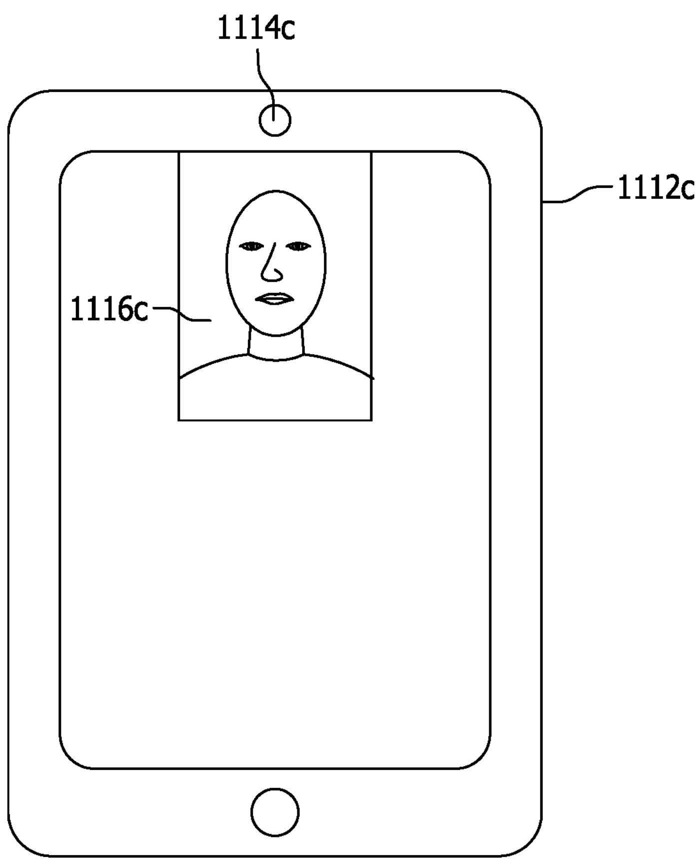


FIG. 11C

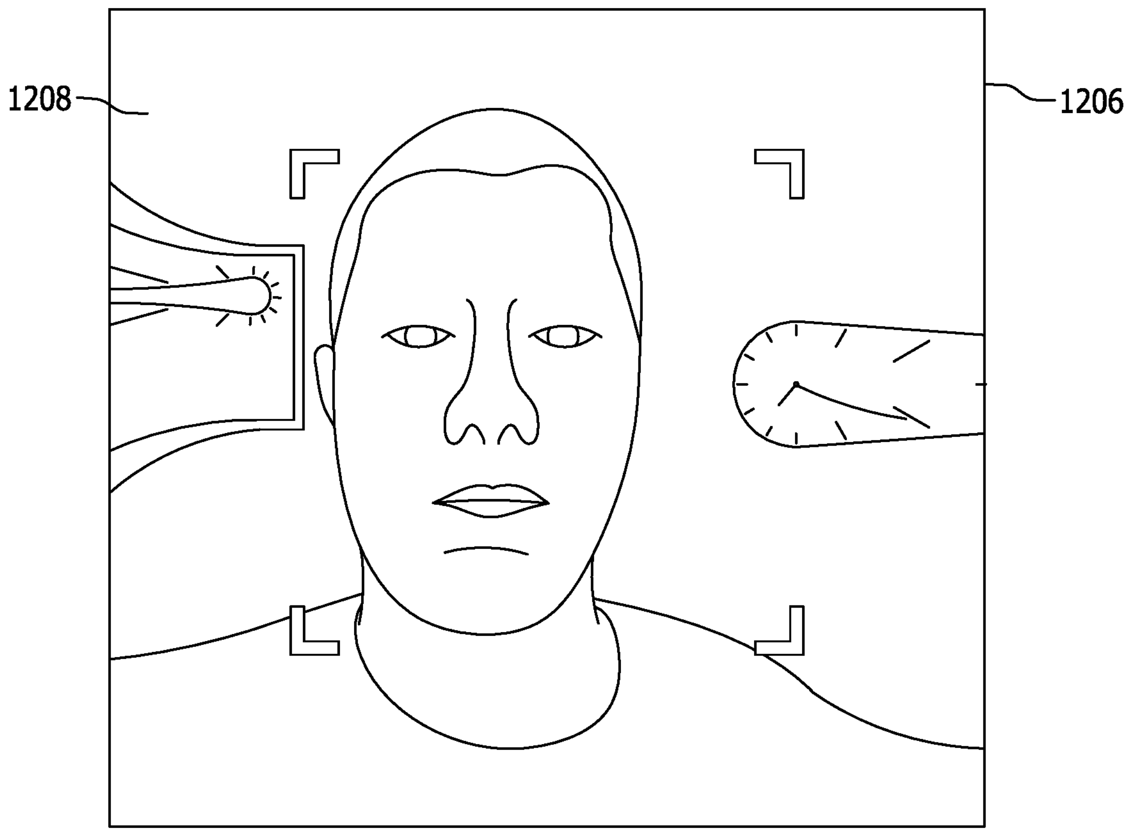


FIG. 12

FIG. 13A

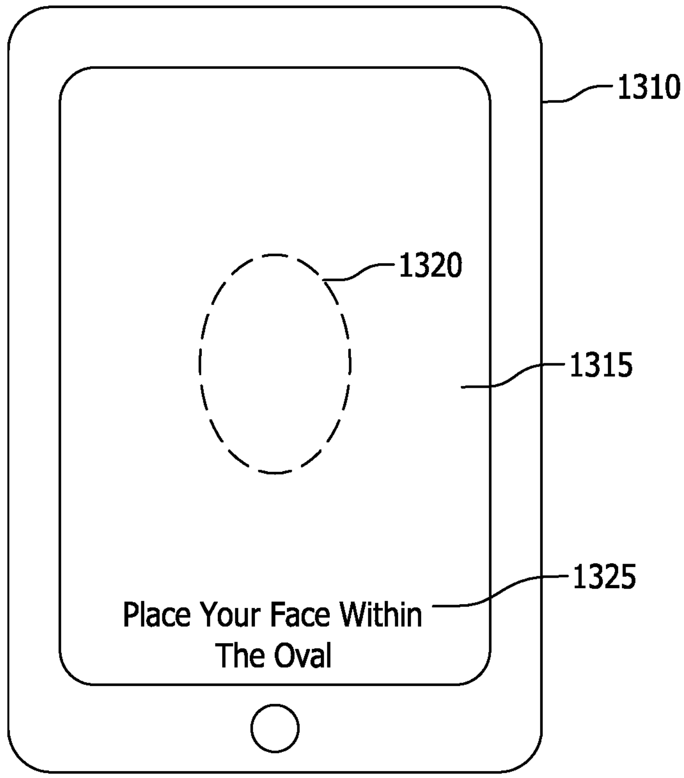
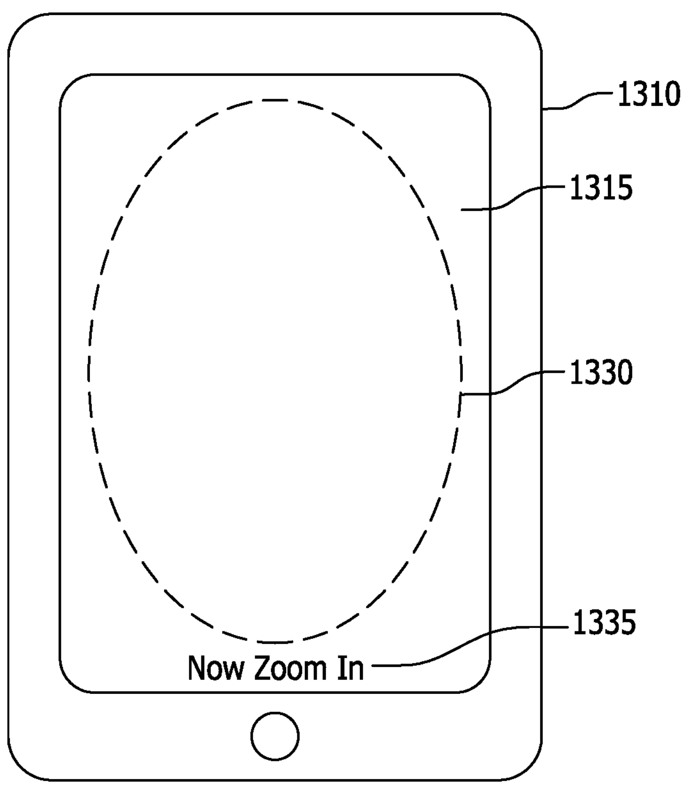


FIG. 13B



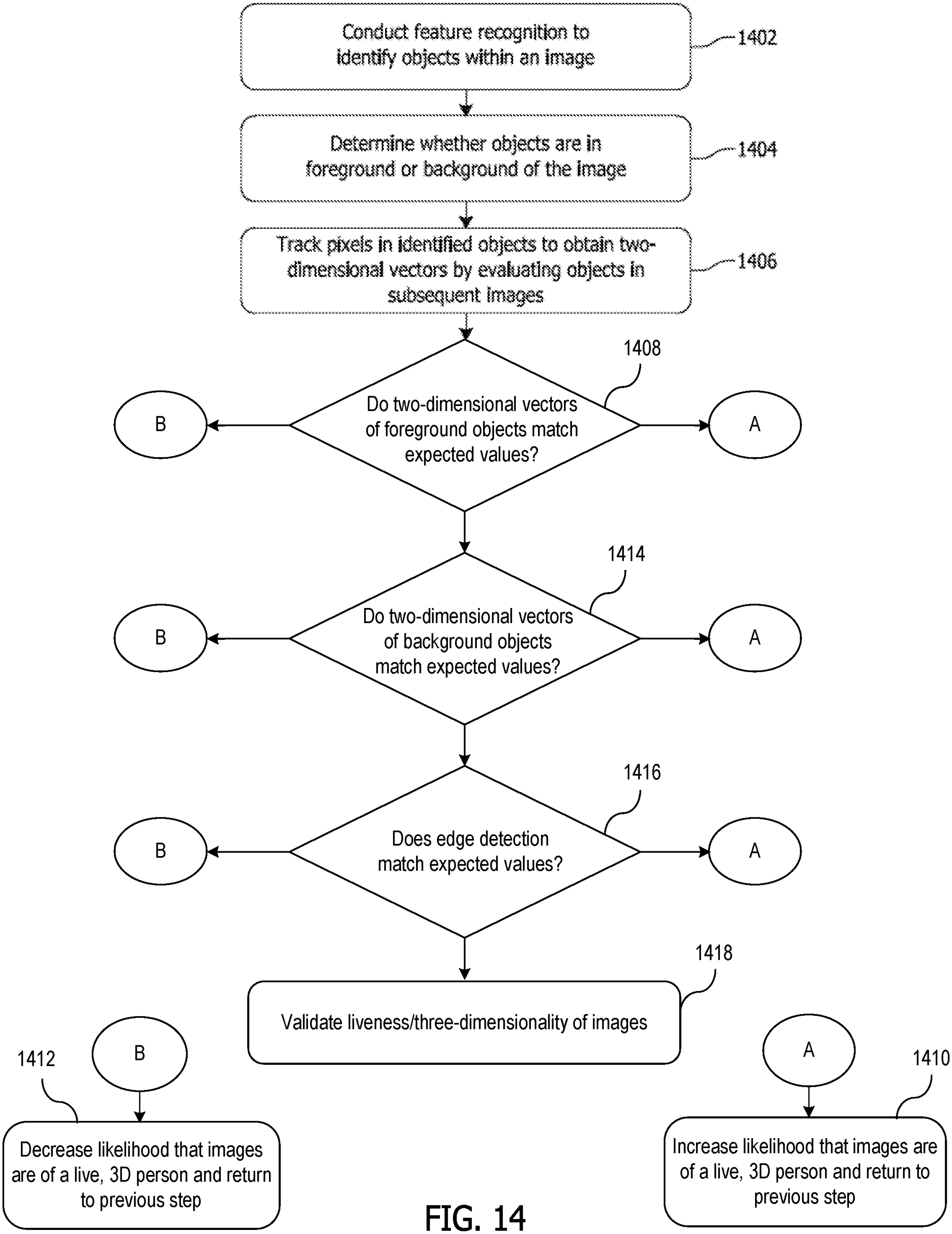

Conduct feature recognition to identify objects within an image
1402
Determine whether objects are in foreground or background of the image
1404
Track pixels in identified objects to obtain two-dimensional vectors by evaluating objects in subsequent images
1406
1408
Do two-dimensional vectors of foreground objects match expected values?
B
A
1414
Do two-dimensional vectors of background objects match expected values?
B
A
1416
Does edge detection match expected values?
B
A
1418
Validate liveness/three-dimensionality of images
1412
B
Decrease likelihood that images are of a live, 3D person and return to previous step
A
1410
Increase likelihood that images are of a live, 3D person and return to previous step

FIG. 14

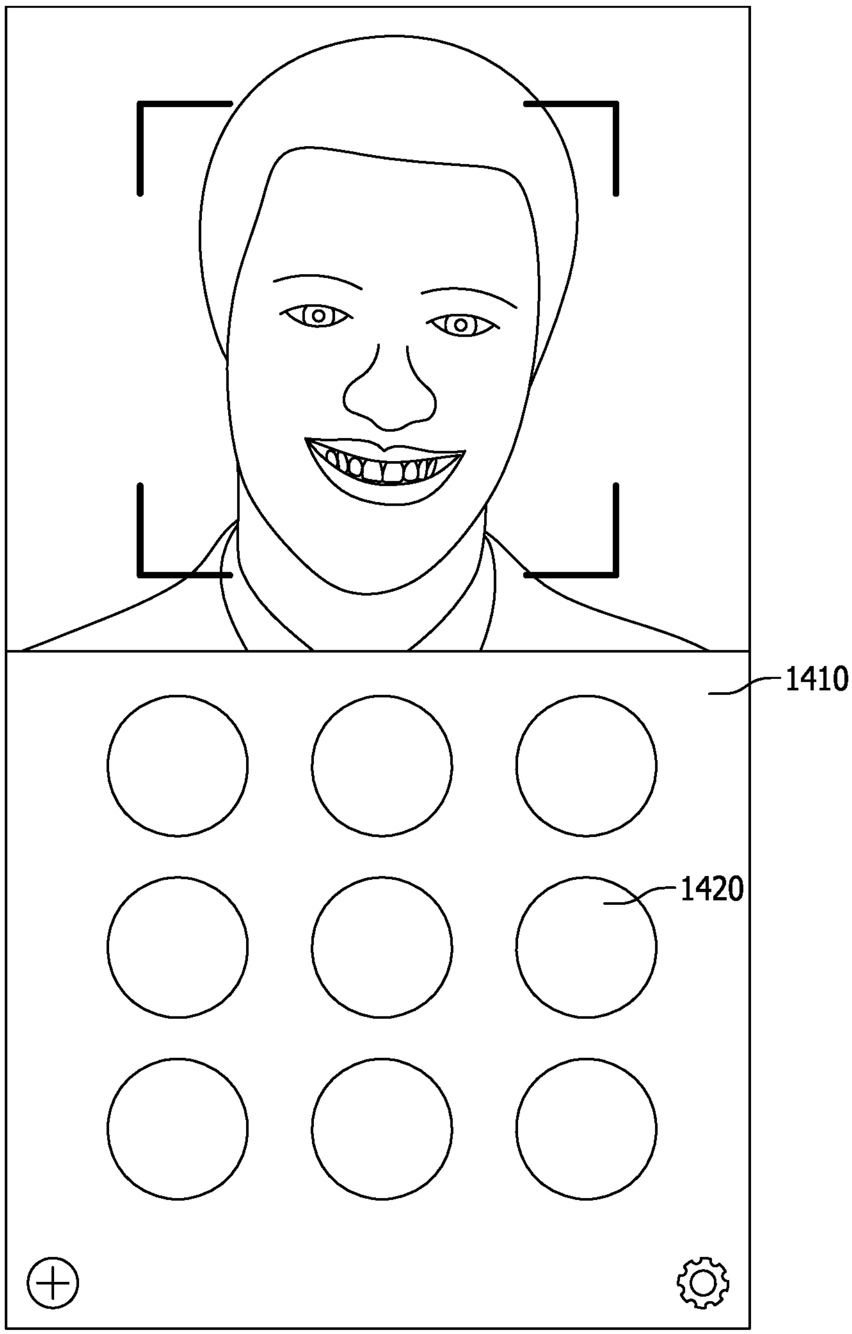


FIG. 15

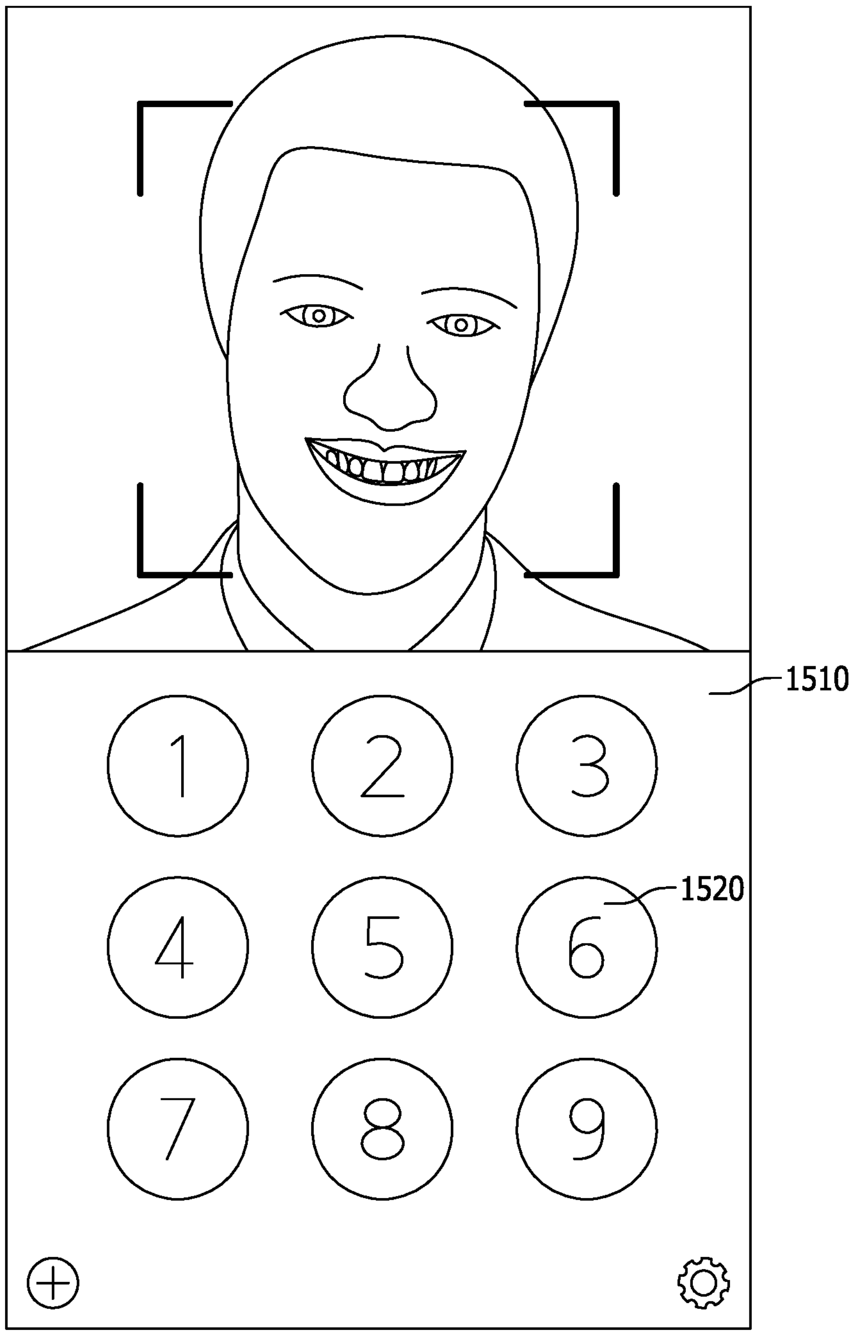


FIG. 16

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS
First Named Inventor/Applicant Name:	Kevin Alan Tussy
Filer:	Chad W. Miller
Attorney Docket Number:	FACETC.0082P

Filed as Small Entity

Filing Fees for **Utility under 35 USC 111(a)**

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
UTILITY FILING FEE (ELECTRONIC FILING)	4011	1	80	80
UTILITY SEARCH FEE	2111	1	350	350
UTILITY EXAMINATION FEE	2311	1	400	400
Pages:				
Claims:				
CLAIMS IN EXCESS OF 20	2202	1	50	50
Miscellaneous-Filing:				
Petition:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**880**

Electronic Acknowledgement Receipt

EFS ID:	44106025
Application Number:	17508887
International Application Number:	
Confirmation Number:	9577
Title of Invention:	FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS
First Named Inventor/Applicant Name:	Kevin Alan Tussy
Customer Number:	32856
Filer:	Chad W. Miller
Filer Authorized By:	
Attorney Docket Number:	FACETC.0082P
Receipt Date:	22-OCT-2021
Filing Date:	
Time Stamp:	20:22:01
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$880
RAM confirmation Number	E20210LK22343011
Deposit Account	502200
Authorized User	Chad Miller

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.21 (Miscellaneous fees and charges)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.16 (National application filing, search, and examination fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	FACETC0082PADS.pdf	103335 b479552e8ae082aaaa57e3ff7eb9f803f5c4888c	no	9

Warnings:

Information:

This is not an USPTO supplied ADS fillable form

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
2	Oath or Declaration filed	FACETC0082PPRNTDECBYINV.pdf	76866 ce9d4b0ff22a38c373a534e49b7edcf0f97dc1e2	no	1

Warnings:

Information:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
3	Power of Attorney	FACETC0082PPOAPDF.pdf	221725 42dc84fd1f3cd382c64787b3c924fc0b30ac4719	no	2

Warnings:

Information:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
4		CWMW16015SPEC.pdf	417362 47965ceca9c8563cdfb5c3b2d8533cfe4c8088c4	yes	82

Multipart Description/PDF files in .zip description

Document Description	Start	End
Specification	1	76
Claims	77	81
Abstract	82	82

Warnings:

Information:

5	Drawings-only black and white line drawings	FACETC0082PPPRNTFIGS.pdf	1242731 bc2f266414038b5c202c37774295d4d3d80d54fc	no	15
Warnings:					
Information:					
6	Fee Worksheet (SB06)	fee-info.pdf	46138 827e4b1720e2935e59c7e394d6dbd25a4c2a15d2	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	2108157		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	FACETC.0082P
	Application Number	

Title of Invention	FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2:

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Kevin	Alan	Tussy	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Las Vegas	State/Province	NV	Country of Residence	US

Mailing Address of Inventor:

Address 1	1925 Village Center Circle, Suite 150		
Address 2			
City	Las Vegas	State/Province	NV
Postal Code	89134	Country	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	32856
Email Address	Add Email Remove Email

Application Information:

Title of the Invention	FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS		
Attorney Docket Number	FACETC.0082P	Small Entity Status Claimed	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	15	Suggested Figure for Publication (if any)	

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	FACETC.0082P
	Application Number	
Title of Invention	FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS	

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

- ☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)
- ☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	32856		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Continuation of	16/817428	2020-03-12

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	FACETC.0082P
	Application Number	

Title of Invention	FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
16/817428	Continuation of	15/900681	2018-02-20	10614204	2020-04-07

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
15/900681	Claims benefit of provisional	62/460670	2017-02-17

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
15/900681	Continuation in part of	14/839505	2015-08-28	9953149	2018-04-24

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
14/839505	Claims benefit of provisional	62/043224	2014-08-28

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
14/839505	Claims benefit of provisional	62/054847	2014-09-24

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
14/839505	Claims benefit of provisional	62/064415	2014-10-15

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
14/839505	Claims benefit of provisional	62/085963	2014-12-01

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
14/839505	Claims benefit of provisional	62/101317	2015-01-08

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
14/839505	Claims benefit of provisional	62/139558	2018-03-27

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	FACETC.0082P
	Application Number	

Title of Invention	FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
14/839505	Claims benefit of provisional	62/188584	2015-07-03

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)[i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

			Remove
Application Number	Country[i]	Filing Date (YYYY-MM-DD)	Access Code[i] (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button.

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	FACETC.0082P
	Application Number	
Title of Invention	FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS	

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	FACETC.0082P
	Application Number	
Title of Invention	FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS	

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

- (●) Assignee
- ( ) Legal Representative under 35 U.S.C. 117
- ( ) Joint Inventor
- ( ) Person to whom the inventor is obligated to assign.
- ( ) Person who shows sufficient proprietary interest

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor:

If the Applicant is an Organization check here. ☒

Organization Name	FaceTec, Inc.		
Mailing Address Information For Applicant:			
Address 1	1925 Village Center Circle, Suite 150		
Address 2			
City	Las Vegas	**State/Province**	NV
Country	US	Postal Code	89134
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button.

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	FACETC.0082P
	Application Number	

Title of Invention	FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.

Signature:

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). **However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).**

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/Chad W. Miller/			Date (YYYY-MM-DD)	2021-10-22
First Name	Chad	Last Name	Miller	Registration Number	44943

Additional Signature may be generated within this form by selecting the Add button.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	FACETC.0082P
	Application Number	
Title of Invention	FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS	

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1 The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3 A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent CooperationTreaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [x] The attached application, or
- [ ] United States application or PCT international application number ____________

filed on ____________.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: KEVIN ALAN TUSSY   Date (Optional) : ____________

Signature: ____________

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.