

010606

20427 U.S. PT

PTO/SB/16 (07-05)

Approved for use through 07/31/2006. 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.

**PROVISIONAL APPLICATION FOR PATENT COVER SHEET**

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

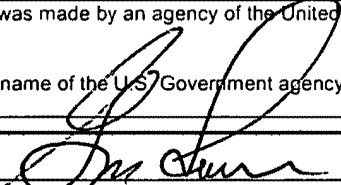
Express Mail Label No. EV 769159590 US

42960 U.S. PTO  
60757075

010606

INVENTOR(S)		
Given Name (first and middle (if any))	Family Name or Surname	Residence (City and either State or Foreign Country)
Michael F.	Malone	McKinney, Texas
Additional inventors are being named on the _____ separately numbered sheets attached hereto		
TITLE OF THE INVENTION (500 characters max):		
APPARATUS AND METHOD FOR EMBEDDING META-TAGS INTO MEDIA FILES		
Direct all correspondence to: <b>CORRESPONDENCE ADDRESS</b>		
<input checked="" type="checkbox"/> The address corresponding to Customer Number: <div style="border: 1px solid black; padding: 2px; display: inline-block;">25883</div>		
<b>OR</b>		
<input type="checkbox"/> Firm or Individual Name		
Address		
City	State	Zip
Country	Telephone	Email
<b>ENCLOSED APPLICATION PARTS (check all that apply)</b>		
<input checked="" type="checkbox"/> Application Data Sheet. See 37 CFR 1.76		
<input type="checkbox"/> CD(s), Number of CDs _____		
<input checked="" type="checkbox"/> Specification Number of Pages <u>23</u>		
<input type="checkbox"/> Other (specify) _____		
<input checked="" type="checkbox"/> Drawing(s) Number of Sheets <u>8</u>		
<b>Fees Due:</b> Filing Fee of \$200 (\$100 for small entity). If the specification and drawings exceed 100 sheets of paper, an application size fee is also due, which is \$250 (\$125 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).		
<b>METHOD OF PAYMENT OF FILING FEES AND APPLICATION SIZE FEE FOR THIS PROVISIONAL APPLICATION FOR PATENT</b>		
<input checked="" type="checkbox"/> Applicant claims small entity status. See 37 CFR 1.27.		
<input checked="" type="checkbox"/> A check or money order is enclosed to cover the filing fee and application size fee (if applicable). <div style="border: 1px solid black; padding: 2px; display: inline-block;">100.00</div>		
<input type="checkbox"/> Payment by credit card. Form PTO-2038 is attached		
<b>TOTAL FEE AMOUNT (\$)</b>		
<input checked="" type="checkbox"/> The Director is hereby authorized to charge the filing fee and application size fee (if applicable) or credit any overpayment to Deposit Account Number: <u>20-0780/MPOR-27490</u> . A duplicative copy of this form is enclosed for fee processing.		
The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.		
<input checked="" type="checkbox"/> No.		
<input type="checkbox"/> Yes, the name of the U.S. Government agency and the Government contract number are: _____		

SIGNATURE



Date

1/6/06

TYPED or PRINTED NAME Gregory M. Howison

REGISTRATION NO. 30,646

(if appropriate)

TELEPHONE 972-479-0462

Docket Number: MPOR - 27,490

**USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT**

This collection of information is required by 37 CFR 1.51. 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 1.11 and 1.14. This collection is estimated to take 8 hours 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, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

**PROVISIONAL APPLICATION COVER SHEET**  
**Additional Page**

PTO/SB/16 (07-05)

Approved for use through 07/31/2006. 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.

<b>First Named Inventor</b>	Michael F. Malone	<b>Docket Number</b>	MPOR - 27,490
<b>INVENTOR(S)/APPLICANT(S)</b>			
<b>Given Name (first and middle [if any])</b>	<b>Family or Surname</b>	<b>Residence (City and either State or Foreign Country)</b>	
Michael F.	Malone	McKinney, Texas	

Number 2 of 2

**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.

**APPARATUS AND METHOD FOR EMBEDDING META-TAGS INTO MEDIA FILES**

Inventor:

Michael F. Malone

FILE NO. MPOR-27,490  
Express Mail No. EV 769159590 US

PATENT

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

**APPARATUS AND METHOD FOR EMBEDDING META-TAGS INTO MEDIA FILES**

**TECHNICAL FIELD OF THE INVENTION**

**[0001]** This invention is related in general to recording of audio, video, images and other information, converting unique audio and speech into “keys” similar to meta-tags, which become index keys to the audio, video, images and other information, to search, sort, display, play and print the audio, video, images and other information along with their specific “keys”. In addition, this invention provides for the ability to capture an image, a video clip, audio, and other information, convert the audio elements into “keys”, which are permanently secured within the image, video, audio and other information. These element (meta-tags) keys, refer to the elements within the image, video, audio and other information such as a person, an animal, an event, date, time and location which allows the user to store, search, retrieve, display, play and print these images on their computer or other device, based on these embedded element keys.

**CROSS-REFERENCE TO RELATED APPLICATIONS**

## BACKGROUND OF THE INVENTION

[0002] With the popularity of “digital” recording devices to capture image(s), audio and video, such as, Personal Digital Assistants (PDA’s) cell camera phones, cameras, video recorders, audio recorders and other digital recorders, users have been afforded the ability to capture, transmit, and store digital media within seconds.

[0003] With the advent of digital media, it has become increasingly difficult to store these images, video, audio and other information on ones PC or on a remote server, such as AOL, Yahoo, with the functionality to store and retrieve these images, video clips, audio or other information in such a way as to allow the user(s) to search, sort, display, play or print these images based upon the elements or meta-tags within the file such as, date, time, location, events, people, pets, surroundings or other information composed within the image(s), video clips, audio or other information . . . This includes digital photographs, video clips & audio recordings of speech or musical performances, motion pictures and recordings of physical phenomena, such as meter readings or “black box” records.

[0004] An attendant problem is that of secure storage and keys to permanently store and search of specific elements (meta-tags) within an image, video clip, audio file, and other information. While a flash memory card within these digital recoding devices (in any of its currently popular forms) can hold hundreds of pictures, images, video and audio, the problem with securely storing, indexing and retrieving thousands of media files has still not been solved. When the works of intellectual property (music, software, images and movies, to name a few) are much more valuable than the equipment on which they reside, the temptation for theft and alteration becomes great.

[0005] Furthermore, this invention provides for the ability to capture an image, a video clip, audio, and other information, convert the audio elements into “keys”, which are secured within the image, video, audio, other information. These element keys, refer to the elements within the image, video or audio, such as a person, an animal, an event, which allows the user to store, retrieve, display, play and print these images on their computer or other device, and become these element keys.

**[0006]** This works for any kind of media file – photographs, images, music, audio spoken word, video, physical phenomena – anything. Obvious applications range from taking a photograph, video clip to “black boxes” embedded in transportation facilities. Following an incident, information could be transmitted using the above schemes to a storage facility. Only authorized personnel could then retrieve the encrypted messages and return the data to clear text form.

## SUMMARY OF THE INVENTION

[0007] The world of recoding images, audio, video and photography is moving from recording images and audio using layers of photosensitive chemicals on a transparent film stock and other analog recording processes - to recording image, video, audio and other information using solid-state image and audio detectors coupled with digital storage devices.

[0008] This means that the methods of storing, searching, sorting, cataloging, viewing, playback and printing of images, video, audio change as well. Instead of relying on photo finishers, anyone with an inexpensive printer can reproduce images, anyone with a CD reader/writer can reproduce audio, and anyone with a DVD player/recorder can reproduce both images and audio, anyone with a PC and store the images, video or audio files

[0009] Instead of a fireproof safe, images, video, audio and photographs storage and retrieval of images, audio and video based on searchable element keys or indexes involves digital media. And instead of couriers and the mail, transmitting images, video, audio and photographs from one place to another is likely to involve the Internet. While these images, video clips and audio files are stored on ones PC or remotely at an Internet Service Provider, such as AOL, Yahoo or others, it is increasingly difficult to sort and retrieve these images, video clips and audio based upon the elements captured within each image, video or audio.

[0010] Another problem is that of storage and retrieval of the unique elements within an image(s), video, audio file or other information. For many users (photographers, musicians, forensic, video / audio personnel, governmental, military personnel, public service, professional and non professional personnel and others) it is impossible to automate at the moment of capturing the images, video, and audio and in parallel record the elements or keys within the image, video or audio and automatically convert these elements into searchable and retrievable elements from a digital storage medium.

[0011] It is equally important that the images, video, audio and photographs not be disclosed to an unauthorized third party. While traditional analog film images, video and audio recordings can be physically locked into a secure facility, digital images, audio, and video reside on



computers. These computers can be the subjects of network attacks and information on them can be compromised in two ways. First, a knowledgeable opponent can read information from an internet-connected computer – that is, an opponent can view images, video, audio and photographs he or she is unauthorized to view. Second, a knowledgeable opponent can obtain write permission and modify the images, video, audio and photographs in a way that is difficult to detect.

[0012] Finally, it is critical that the user have a means to attach, mix, and modify media files easily and indelibly mark each image, video, audio, photograph or media file as his or her own work, to eliminate the possibility of plagiarism and to provide a certificate authority while wirelessly transmitting said media files for secure storage or to another recipient or source.

[0013] In the days of film cameras (analog), security usually meant placing the negatives into a photo safe. Prints made from the negatives could be marked with an identifier that clearly indicated the pedigree of the photograph. Those who would use the photograph without permission of the owner would be subject to a copyright infringement suit – and it would be sufficient evidence in court for the user to produce the negatives and testify that, in fact, he or she took the photographs.

[0014] With the advent of digital media and the proliferation of the Internet, images, video, audio, photographs and other forms of digital documents stored on digital computers, which are increasingly difficult to search on the key elements within an image, video or audio. This invention provides a mechanism for recording, attaching, mixing, appending to, modifying images, video, audio and photographs, storing, identifying the key elements, and provides a searchable engine to search, sort, display, play or print specific images, video, audio and photographs which have these embedded key elements. It then provides a means to transport the images, video, audio and photographs to a secure, off-site storage facility and to obtain positive confirmation that the transmission occurred error-free.

**BRIEF DESCRIPTION OF THE DRAWINGS**

[0015] For a more complete understanding of the present invention and the advantages thereof, reference is now made to the following description taken in conjunction with the accompanying Drawings in which:

[0016] Fig. 1 illustrates a block diagram of the overall operation of the system in accordance with the present disclosure.

[0017] Fig. 2 illustrates a diagrammatic view of the captured and encrypted file;

[0018] Fig. 3 illustrates a flow chart depicting the overall operation of the capture operation;

[0019] Fig. 4 illustrates a flow chart depicting the operation of the request operation for the start certificate;

[0020] Fig. 5 illustrates a flow chart depicting the operation of requesting information from the GPS; and;

[0021] Fig. 6 illustrates a flow chart depicting the operation of embedding information into the captured file;

[0022] Fig. 7 illustrates a flow chart depicting the operation of requesting the stop certificate;

[0023] Fig. 8 illustrates a flow chart depicting the encryption algorithm operation

**DETAILED DESCRIPTION OF THE INVENTION**

[0024] Referring now to Fig. 1, there is illustrated a block diagram of the overall operation of the system in accordance with the present disclosure. The system generally is directed toward a capture device 102 that is operable to capture, in this embodiment, an image of an individual; for example, the individual denoted by the reference numeral 104. As referenced by the numeral 105 (A = Audible) and to capture the audible recorded by the user, such as, "This is a picture of Dan Smith on his 45<sup>th</sup> birthday, at Sue Jones house in Burlington, WI. This can represent any type of scene, audio or any type of information that is captured. This could be a video segment, a still picture or an audio segment. It should be understood that the capture device 104 could capture any type of information, not just video information, As will be described herein below, the purpose of the system of the present disclosure will be to not only capture information, create unique elements key about the contents of the image, video or audio but to store the information in a secure and certifiable manner such that allows users to search, sort, display, play or print based upon the key elements. The capture device is controlled by a user through an input/output (I/O) interface 106. The image 104, in this example, will be captured in the form of a capture file 108 and 109 stored in a storage area 110, this being a buffer area. The capture device 102 could be a cell phone that has a video camera associated therewith; any type of device having a digital camera associated therewith, an audio system for capturing an audio file, etc. The phone, in one example, can capture and digitize the image, or even a video segment.

[0025] Once the captured image 108 is formed and temporarily stored, it then goes to the next step of the operation. In this step of the operation, a process block 112 is provided to obtain local certification. Local certification, in this example, is some certification that is viewed as providing information in such a manner that there is a high level of confidence in that information which is to be associated with the image and element keys are an integral part thereof and will, as described herein below, follow the image. For example, the information that is captured will be an audio file which corresponds to the image(s) or video clips that is received from the person or device taking the picture, video clip or audio, the time and date information and longitude and latitude information that is received from a GPS system (global positioning system), a conventional system. The time information, the date information and the longitude and latitude information are provided in such a manner that, when associated with the capture file 108, this provides some current

validation that the file was created at that particular time and, at a later time, it could be identified by the fact that it has that information associated therewith. Furthermore, as referenced in 125 of Figure 1, the GPS coordinates will be converted to address, city, state, postal code and country and be permanently embedded in the image, video, audio or other information for purposes of storage, searching, retrieval and printing as referenced at 160 and 162. For example, a user could make a log, either printed or electronic of the image captured and, at a later time, by merely knowing what the time and data information was and the longitude and latitude information was, this would provide a higher degree of confidence that the later viewed file and the original captured file was the same and had not been tampered with or had not been reproduced at a later time and location.

[0026] In order to provide this verification, the trusted entity is the GPS system, since this is a system that provides a time stamp and a longitude and latitude from the calibrated system. If this is implemented in such a manner that it is an integral part of the capture operation, i.e., it is integrated into the phone, for example, then a high degree of confidence is maintained that this was obtained basically at the time the capture was complete. The GPS system, as noted herein above, is a conventional system that utilizes a GPS receiver 114 that has an antenna 116 that is operable to receive information from a plurality of satellites 118. Typically, there can be anywhere from three to ten or more satellites from which information can be received to obtain an accurate location. Alternate techniques for recovering time, date and position information includes differential and Doppler analysis of very precise timing signals coming from a plurality of cellular/PCS base stations. A third technique for recovering time, date and position information includes retrieving information directly from the Mobility Management (MM) sub layer of the cellular protocol, where the mobile telephone service provider is a party to the transactions. Finally, another technique of retrieving accurate time and date information include use of a network timeserver.

[0027] The result of the local certification is a locally certified captured image 120 which is illustrated with the image and a time stamp, "TS," disposed on the edge thereof, this location by way of example only, as other methods of disposing this information are described herein below. This "TS" indicates that there is some information that is "embedded" into the captured file or captured image that is now part of the file. For example, as will be described in more detail herein below, there is a science of embedding information referred to as "Steganography" that allows information to be embedded in some expression of intellectual property (a photograph, a musical

recording, or other expression,) such that (a) the information is hidden from casual observers and (b) the information is not easily altered or destroyed. One such type is a “water mark” that basically is disposed in the background of a document, for example. In images, there are encoding techniques such as “glifs” that can be disposed in the image which is an optical type encoding that appears as a random background to a viewer, but actually contains digitized information. The result is that the document, file image, etc., is indelibly marked with the date, the time and the location, in addition to associating therewith information about the user in the form of a user ID, which is provided in a user ID block 122. The local certification block 112, therefore, is operable to merge the captured file 108, the GPS information as to time stamp and location and the user information into the single document 120. At this point, the document 120 is still a “clear” document such that any individual can view it. The image 120 is stored in a temporary image buffer 121.

[0028] After the document 120 has been created with the local certification, the system then compresses the file using any of a number of well-known methods. In the case of an image, the compression technique may be a lossy algorithm such as JPEG or (in the case of motion pictures) MPEG, or for a data set, the compression technique may be a lossless method such as Lempel-Ziv-Welch.

[0029] After compression, the file 120 is processed through an encryption operation wherein the file is first encrypted in accordance with predetermined encryption algorithms, this being performed in a block 124. The encryption, as will be described herein below, is a double encryption operation, which wraps the local certified captured file with a first level of encryption 126 and a second level of encryption 128 to provide an encrypted document 130. This is then stored in a temporary storage buffer 132. The file 130 is then subjected to a non-repudiation certification process to acquire a Certificate of Authenticity (CA) from a certification authority 135, this certification authority 135 being a trusted third party that can “digitally sign” a file, image, etc. and provide a level of authenticity to that file. This is conventional technology. The document 130, in its encrypted form, is converted to a “hash” file and this hash file, which is a representation of the encrypted file, is sent to the certification authority 135 via a transmitter and antenna 136 along a wireless path, and received by an antenna 137 at the certification authority 135 location. Again, this is a wireless operation. The hash file is then signed and a combination hash file and certificate of authenticity is then sent back to the antenna 136, which is then stored in a temporary memory 133 as

a certified document. This is illustrated with the attached certification authority certificate 139. This is the file that is sent to the secure storage facility, this being a file 130'.

[0030] After encryption, certification by the CA and compression, the encrypted file is then passed to the transmitter 134 for transmission via the antenna 136 along a wireless path to a secure storage facility 138 having a receiving antenna 140 associated therewith. The secure storage facility 138 is a repository. In one embodiment, this repository 138 does nothing more than to store the image 130 in a large database 142 for access at a later time. Additionally, the secure storage facility 138 could be a trusted storage facility, which trusted storage facility has the ability to "unwrap" the encryption from the document 120 such that it can transmit the document 120 at a later time upon request. Alternatively, the secure storage facility 138 could merely be a place to store the information with secure measures as to restricting access to only authorized individuals. In that scenario, the secure storage facility 138 would not be able to decrypt the image 130 and would merely be able to transfer the image to the individual or entity authorized to access that information.

[0031] For access, a remote access site 144 is operable to send requests to the secure storage facility 138, identify themselves with the appropriate passwords to comply with the security procedures of the secure storage facility 138 and then have the image requested sent thereto. This image can then be stored in a memory 146 and decrypted with a decryption algorithm in a block 148 for storage of the decrypted file 120 in a storage space 150. This can then be extracted by a user for whatever purpose. In general, all of the encryption ensures that there has been no "tampering" with the file before it is decrypted. Once decrypted, then the time date stamp and location information, in addition to the user information, is still embedded in the picture, document, audio file, etc. that makes up the captured file to show that there was some local indelible certification that verifies the captured file as being authentic and which was embedded at the time of creation.

[0032] At 123, on figure 1, the audio file which was previously captured at 102 and directly corresponds to the tagged image, video clip, audio or other information is converted from spoken word into recordable key elements or meta-tags and permanently embedded into the image, video clip, audio or other information for storage, searching, retrieval, display or printing. Once these images, video clips, audio or other information have their permanently embedded key elements (meta-tags), these files can be sent to others and devices for searching, storing, retrieving,

displaying, play or printing based upon these key elements (meta-tags).

[0033] Referring now to Fig. 2, there is illustrated a diagrammatic view of the captured and encrypted file 130 which, as noted herein above, is comprised of the locally certified captured file 120 wrapped by the first layer of encryption 126 and the second layer of encryption 128. As will be described herein below, the first layer of encryption is a symmetrical encryption algorithm and the second layer 128 is an asymmetrical encryption layer 128. The symmetrical encryption layer is something that can be unwrapped merely by having access to various public keys. This is a fairly conventional PKI system. The second layer of encryption, the asymmetrical encryption layer, is a layer that requires a private key in order to extract this layer. Therefore, in order to gain access to the file at the second layer of encryption, the individual must have the private key to unwrap the first layer and the other key to unwrap the second layer. Again, this will be described in more detail herein below.

[0034] Referring now to Fig. 3, there is illustrated a flow chart depicting the overall operation of the capture operation, which is initiated at a start block 302 and then proceeds to a function block 304 in order to allow the user to activate the capture device 102. The user activates the capture device 102 and then a capture operation is initiated at a block 306. Upon initiation of a capture, there is, in one embodiment, a "start" request sent out to the certification authority 135. The certification authority 135 receives the request generated at the block 308 for a certification certificate as to the "start" information that was sent to it. This can merely be the text "start" that is certified. This is sent back to the system during the capture operation. A decision block 310 indicates that this operation which will wait for the receipt of the certificate. However, during the time that this certificate is being generated, the capture is continuing. Once the program, after the start request is generated, then flows to a decision block 310 to wait for the completion of the capture operation. As soon as this is complete, the program flows along a "Y" path to a function block 312 in order to request the time, date, longitude, latitude information and then embed this information along with user information, as indicated by a function block 314. This is embedded into the captured file as described herein above. The program then flows to a function block 316 in order to request a "stop" certificate from the certification authority 135. In this operation, the certificate is requested prior to encryption such that the "clear" file can be certified prior to encryption with the certificate 139. However, the file could be encrypted first and then certified.

The program then flows to an encryption block 318 to encrypt the file and then to a function block 320 to compress the file. This compressed file is then transmitted to the repository, as indicated by a function block 322 and then the program proceeds to an End block 324.

[0035] Referring now to Fig. 4, there is illustrated a flow chart depicting the operation of the request operation for the start certificate, as initiated at a block 402. The program then proceeds to decision block 404 in order to initiate the capture operation. When the capture operation is initiated, the program flows along a "Y" path to a function block 406 to send the "start" text to the certification authority 135. Of course, this could be a "hash" of a certain initial part of the capture file, but just the text would be sufficient. The program then flows to a decision block 410 to determine if the certificate has been received for this "start" text and, when it has been received, the program will flow along the "Y" path to a function block 412 to store this received certificate in association with the captured file. Of course, this may not be disposed in association therewith until the capture is complete. Additionally, although not illustrated in this flow chart, the start time could also have time and date information as well as longitude and latitude information associated therewith such that there would be local certification of both the start time and the stop time which is received from a trusted authority, i.e., the GPS system. Once this information is determined as stored in association with the captured file, the program flows to a return block 414. Again, this information may merely be stored in a temporary buffer until the capture is complete.

[0036] Referring now to Fig. 5, there is illustrated a flow chart depicting the operation of requesting information from the GPS, which is initiated at a block 502. The program then flows to a function block 504 in order to access the GPS system. This, again, is a conventional operation which will obtain both accurate time information and location information. This access of information is indicated in a function block 506. The program then stores this information and flows back to a Return block 508.

[0037] Referring now to Fig. 6, there is illustrated a flow chart depicting the operation of embedding information into the captured file, which is initiated at a block 602. The program then flows to a function block 604 to initiate a steganography algorithm. The steganography operation is operable to permanently modify the captured file with the time/date information and longitude and latitude information as well as user ID information, this indicated at a function block 606. The



program then flows to a function block 608 to store a modified captured file with this local certification information embedded therein. Again, this local certification information provides some level of authenticity to a “clear” file. The program then flows to a Return block 610.

[0038] Referring now to Fig. 7, there is illustrated a function block or a flow chart depicting the operation of requesting the stop certificate, which is initiated at a start block 702 and then proceeds to a function block 704 to create the “hash” file of a modified capture file. This hash file is then sent to the certification authority 135, as indicated by a function block 706. The program then flows to decision block 708 to wait for the receipt of the certificate and, once received, flows to a function block 710 to basically sign the modified capture file and associate with the modified capture file a certificate of authority. Since the hash file is a digital representation of the actual captured file, the actual capture file does not have to be transmitted to the certification authority 135. The reason for this is that one would like to prevent the transmission over any wireless link of “clear” information. As such, the hash file has no discernable information associated therewith and, as such, it only has meaning when associated with the original file from which it was generated, since the algorithm for generating a hash file will clearly identify the two. As such, the certificate generated by the certification authority 135 is sufficient to ensure that a trusted authority has in fact verified the authenticity of the file, this indicated by a function block 712 wherein the captured file is signed and then the program flows to a Return block 716.

[0039] Referring now to Fig. 8, there is illustrated a flow chart depicting the encryption algorithm operation, which is initiated at a block 802 and then proceeds to a function block 804. This is the operation wherein symmetrical encryption is utilized with a “public and private key system.” The symmetrical encryption is an operation in which a plaintext message is transformed by a well-known algorithm operating under control of a key. The key is a short (less than 1000 bits, usually) data string that instructs the encryption algorithm how to transform the plaintext into an unreadable form called ciphertext. This type of encryption is called “symmetrical” because the same key that is used to encrypt the plaintext is used to decrypt the cyphertext, resulting in a plaintext file once again.

[0040] After encryption in the “first layer,” the program then flows to function block 806 to create the first cyphertext file. This first cyphertext file is then processed with an asymmetrical

encryption algorithm, as indicated by a function block 808 to further encrypt or protect the captured file. The second general type of cryptosystem is asymmetrical encryption. This encryption scheme uses mathematical functions called one-way or trapdoor functions that are easy to perform but extremely difficult to reverse. Examples of these one-way functions are factoring large composite numbers (two large numbers are easy to multiply, but finding the two large numbers given the product alone is difficult) and the discrete logarithm problem (raising a number to a power modulo some value is easy, but finding the number given the result is difficult.) In an asymmetrical cryptosystem, one key (referred to as the public key) is used to encrypt the plaintext and a second, related key (called the private key) is used to decrypt the ciphertext. In a public key encryption scheme, it is common to publish the public key. In this way, anyone can send a secure message, but only the holder of the private key can decrypt the message and reveal the plaintext.

[0041] Asymmetrical cryptosystems have another use as well: by encrypting a file under his or her private key, a party can prove that he or she is the author of the message. If others can decrypt the file using the associated public key, then nobody but the holder of the private key could have created the message. This leads to properties favorable to the present invention: proof of ownership and non-repudiation. The result of the asymmetrical encryption step will be the creation of the second cyphertext file as an encrypted stamped and certified captured file, as indicated by function block 810. The program then proceeds to a Return block 812.

[0042] To illustrate how the system of the present disclosure operates, one example of an application of the capture device 102– a wireless digital camera – will be described.

[0043] The user takes a picture, video, records audio or spoken word, or acquires any other data set, or any combination of these. The apparatus then sends a request to a certificate authority to obtain a certification of the time and date of the recording. This certificate, as well as time, date and location information obtained from the GPS receiver or other techniques for determining this information, as well as an identifying number unique to the wireless digital video camera, is steganographically encoded onto the image and/or audio files.

[0044] The image is now marked, but it is still “in the clear.” That is, anyone who gains access to the image file will be able to reproduce the image. It must now be secured so that

unauthorized parties cannot view the image.

[0045] After compression, the next step is to encrypt the file in such a way that the file cannot be used without access to a secret key.

[0046] Once the image file has been indelibly marked and compressed, and it is about to be encrypted using a symmetrical cryptosystem, a decision must be made as to what key to use. There are several methods of establishing a key. The first is to have a single, fixed key assigned to the wireless digital recorder (i.e. camera) at the factory. The problem with this method is that if this key becomes compromised, then all images taken by the wireless digital recorder (i.e. camera) are compromised. A second method is to create a new, random key each time a photograph is taken, and store the table of keys in the wireless digital recorder (i.e. camera) for subsequent download. This, although feasible, may be undesirable for the same reason that storing the images themselves in the wireless digital recorder (i.e. camera) is undesirable: memory in the wireless digital recorder (i.e. camera) is fragile, and if the keys are lost, the images are useless.

[0047] Instead, a preferred method of key management is used. In this scheme, the serial number of the wireless digital recorder (i.e. camera) and other pertinent information that can be recovered without recovering the file (like the filename, the time and date, etc.) are securely hashed. Hashing refers to a practice of creating a short dataset that represents a larger dataset. For example, if one were to assign all the letters in a document a number (A=1, B=2, etc.), add those numbers together modulo 26, one would come up with a single number between 0 and 25. If any letter in the document changed, the result of the function would change as well, and thus could be used as an indication that the document had changed. In a way, the short dataset (the modulo sum) would stand in for the larger dataset (the document). Note that the short dataset cannot be used to reproduce the document, but that changing the document in a way that doesn't affect the modulo sum is difficult.

[0048] Hashing works in just this way, but with much larger numbers. In the disclosed system, the serial number is hashed with other information to create a key. If the key is compromised (by technical or legal means) then no other photograph taken by the wireless digital recorder (i.e. camera) is compromised. It is impossible – not just difficult – to go from the hashed key to the source material, in the same way it is impossible to deduce this document from one modulo sum

character.

**[0049]** Now the file is encrypted, and only the holder of the secret key can unlock the file. Two more steps remain before the file is transmitted to the secure storage facility. First, the entire encrypted file is passed through a message authentication algorithm, which produces a hash (similar to the way the symmetrical encryption key was calculated, above) over the whole file. In this way, if any byte of the message file is corrupted in transmission, it will be discovered. The file is then encrypted using an asymmetrical cryptosystem under the user's private key, effectively signing the file.

**[0050]** Finally, identifying information is added to the (now doubly) encrypted file, and the file is encrypted again – this time, under the storage facility's public key. Now, observe the properties of the file thus created:

- The file is secure. Nobody but the storage facility can open the outer wrapper.
- The file is anonymous to casual observers. There is no identifying information outside of the outer wrapper.
- The file is signed. The storage facility can open the outer wrapper and discover an identifier of the party who claims to have created the file.
- The signature is irrefutable and cannot be repudiated. The storage facility can look up the public key of the party claiming to be the author of the file, and can attempt to open the middle wrapper. Inside, they will find an encrypted file and a hash of the file. If the calculated hash matches the given hash, then the photograph without question belongs to that party.
- Even after two wrappers have been removed, the picture is still secret. The storage facility keeps only encrypted files. They have no means of removing the final wrapper.

**[0051]** Should it become necessary to prove the authenticity of the photograph, video, audio or other information, the storage facility 138 can testify to all the above facts. Additionally, the originator of the photograph is the only one who can unlock the inner wrapper and produce the photograph. Finally, the photograph itself is steganographically marked, and this final information is clinching proof that the provenance of the photograph is accurate.

**[0052]** To return to the example wherein the picture is ready for transmission at this point,

the wireless digital recorder (i.e. camera) attempts to connect to the server at the secure storage facility 138 or other recipients who have access the network (i.e. PDA's, other wireless digital devices) using any of a number of well-known wireless methods. Among these are data channels associated with IS-95 CDMA, IS-136 TDMA, CDPD, GSM as well as purely data paths such as 802.11b. The exact mechanism of data transmission is not germane.

**[0053]** However the data is transmitted, the storage facility 138 receives the triply-encrypted data file and performs the following steps:

1. Remove the outer wrapper and extract an encrypted file and plain-text subscriber identification.
2. Look up the subscriber information and recover his/her public key.
3. Remove the middle wrapper using the public key to reveal an encrypted file and a hash value.
4. Pass the encrypted file through a message digest algorithm to produce a computed hash.
5. If the computed hash does not match the received hash, send a negative acknowledge and discard the file; otherwise...
6. Calculate a message digest of (1) the received hash, (2) the time and date, and (3) a random number.
7. Return an affirmative acknowledgment and a certificate containing the message digest calculated in (6), above.
8. Store the encrypted photograph along with the received time and date and the random number produced in (6). In this way, if the certificate is ever challenged, the storage facility will be able to verify that it sent the certificate.

**[0054]** The user can also transmit these files over various networks to other recipients (PDA's, cell camera phones, "IP Addresses, E-mail to name a few) for their review and storage. However the users' unique identity and other certificates described in this document are embedded within the file(s).

The wireless digital recorder (i.e. camera), upon receipt of the certificate, transmits an acknowledgment and removes the photograph from its temporary store. The certificate can be stored or discarded – it is not required to retrieve the photograph. If stored, it becomes further evidence of the provenance of the photograph.

**[0055]** Image retrieval from the storage facility 138 is simple. At login, the storage facility presents a random string encrypted under the user's public key. The user must decrypt the string and re-encrypt it under the storage facility's public key. Only the holder of the secret key can do this...and it proves beyond doubt to the storage facility that they are communicating with the owner of the photograph.

**[0056]** Once identity is established, the user can download any file from the storage facility. Once downloaded, the user can open the final wrapper and extract the image.

**[0057]** Again, this works for any kind of media file – photographs, images, music, audio spoken word, video, physical phenomena – anything. An obvious application would be in “black boxes” embedded in transportation facilities. Following an accident, information could be transmitted using the above schemes to a storage facility. Only authorized personnel could then retrieve the encrypted messages and return the data to cleartext form.

**[0058]** Although the preferred embodiment has been described in detail, it should be understood that various changes, substitutions and alterations can be made therein without departing from the spirit and scope of the invention as defined by the following claims.

**WHAT IS CLAIMED IS:**

Claim 1: An apparatus that captures and records audio and image data, interprets the received audio as speech, converts the speech to text, parses the text into a set of searchable tags, and embeds the tags into the image.

Claim 2: The apparatus of claim 1 in which the apparatus stores the image and speech information in a storage medium.

Claim 3: The apparatus of claim 2 in which the apparatus uses a well-known algorithm to identify speech elements in the recorded audio and convert those elements into text.

Claim 4: The apparatus of claim 3 in which the apparatus converts the text to searchable tags.

Claim 5: The apparatus of claim 4 in which the apparatus utilizes a method to combine the searchable tags with the actual image data in such a way that the tag information can be recovered at a later time.

Claim 6: The apparatus of claim 1 that includes captures of audio data in addition to other information, interprets the received audio as speech, converts the speech to text, parses the text into a set of searchable tags, and embeds the tags into the image.

Claim 7: The apparatus of claim 6 in which the apparatus stores the recorded information and speech in a storage medium.

Claim 8: The apparatus of claim 7 in which the apparatus uses a well-known algorithm to identify speech elements in the recorded audio and convert those elements into text.

Claim 9: The apparatus of claim 8 in which the apparatus converts the text to searchable tags.

Claim 10: The apparatus of claim 9 in which the apparatus utilizes a method to combine the searchable tags with the recorded data in such a way that the tag information can be recovered at a later time.

Claim 11: The apparatus of claim 5 in which the date, time, location and user data are similarly converted to tags and stored in the image dataset, such that the data contained in the tags can be recovered at a later time.

Claim 12: The apparatus of claim 5 in which the date, time, location and user data are similarly converted to tags and stored in the information dataset, such that the data contained in the tags can be recovered at a later time.



**ABSTRACT OF THE DISCLOSURE**

The present invention discloses an Apparatus and Method recording of audio, video, images, or other information and converting unique audible into “keys” similar to meta-tags, which become embedded and permanent index keys of the audio, video, images, or other information, to search, sort, store, retrieve, display, play and print the images along with the audio or other information based on these specific “keys” (meta-tags).

In addition, this invention discloses an Apparatus and Method for the Capture and Transport of Digital Images, Audio Files and other data across public and private Voice and Data transmissions networks to include but not limited to; PSTN, Wireless, VSAT and Packet Switched and more specifically for the secure non-repudiation of said images, audio files and other data for forensic and other evidentiary purposes that are sent and received across said transmission networks.

In the first embodiment of the invention a device capable of connecting to the transmission network(s) with a digital image, audio, and or video capture device, attached or embedded, captures images, audio files and other data, stores the images audio files and other data in volatile and/or non volatile memory, obtains a time, date and location stamp from a GPS system and/or a networked time server and/or by utilizing a MM or MM like method and means, attaches a time, date and location stamp to the images, audio files and other data at the moment of capture in a plurality of methods, attaches a Certificate Authorities non-repudiation Digital Certificate stored in the memory of the apparatus or retrieved directly from the CA, encrypts the stamped images using any number of encryption methods to include those that may be provided within the Certificates Signing Algorithm, compresses the stamped images utilizing any number of CODEC algorithms, and transmits the stamped encrypted and compressed images to a secure store forward / real-time server(s) resident on a packet switched network or point to point to another location for electronic retrieval by authorized personnel.

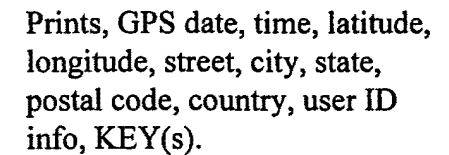


FIG 2

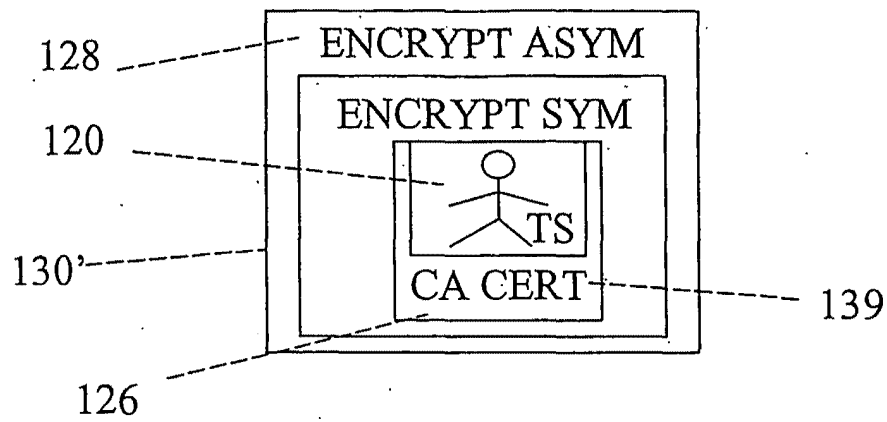


FIG 3

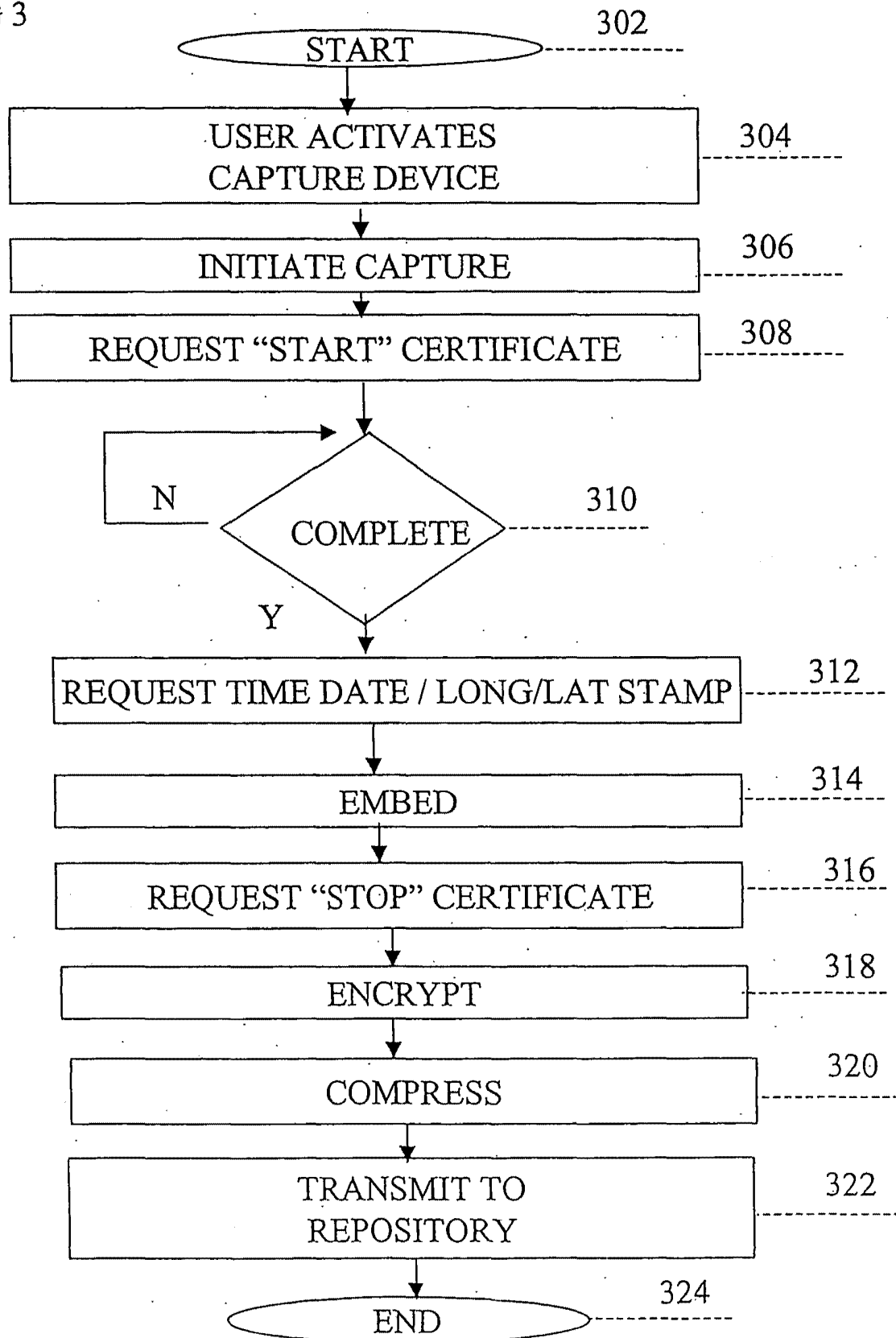


FIG 4

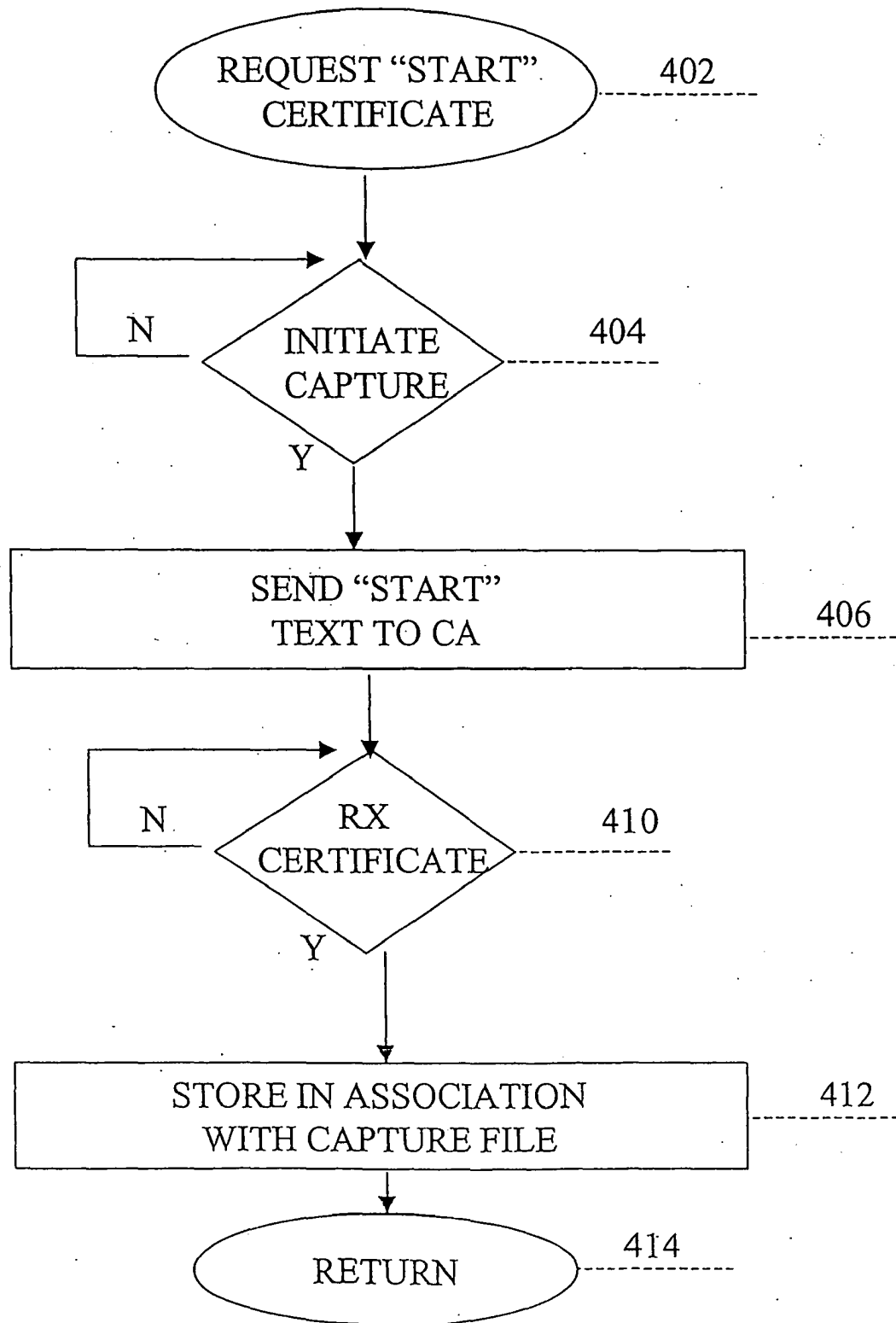


FIG 5

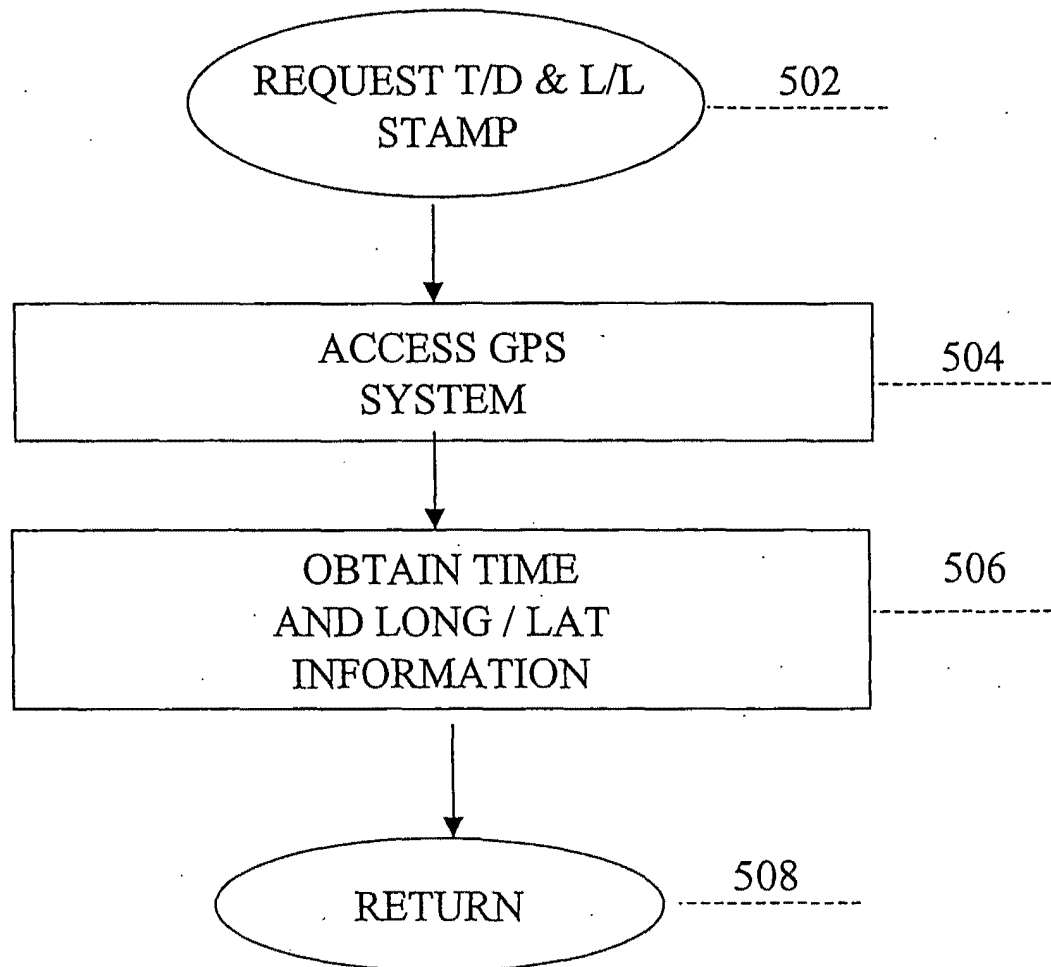


FIG 6

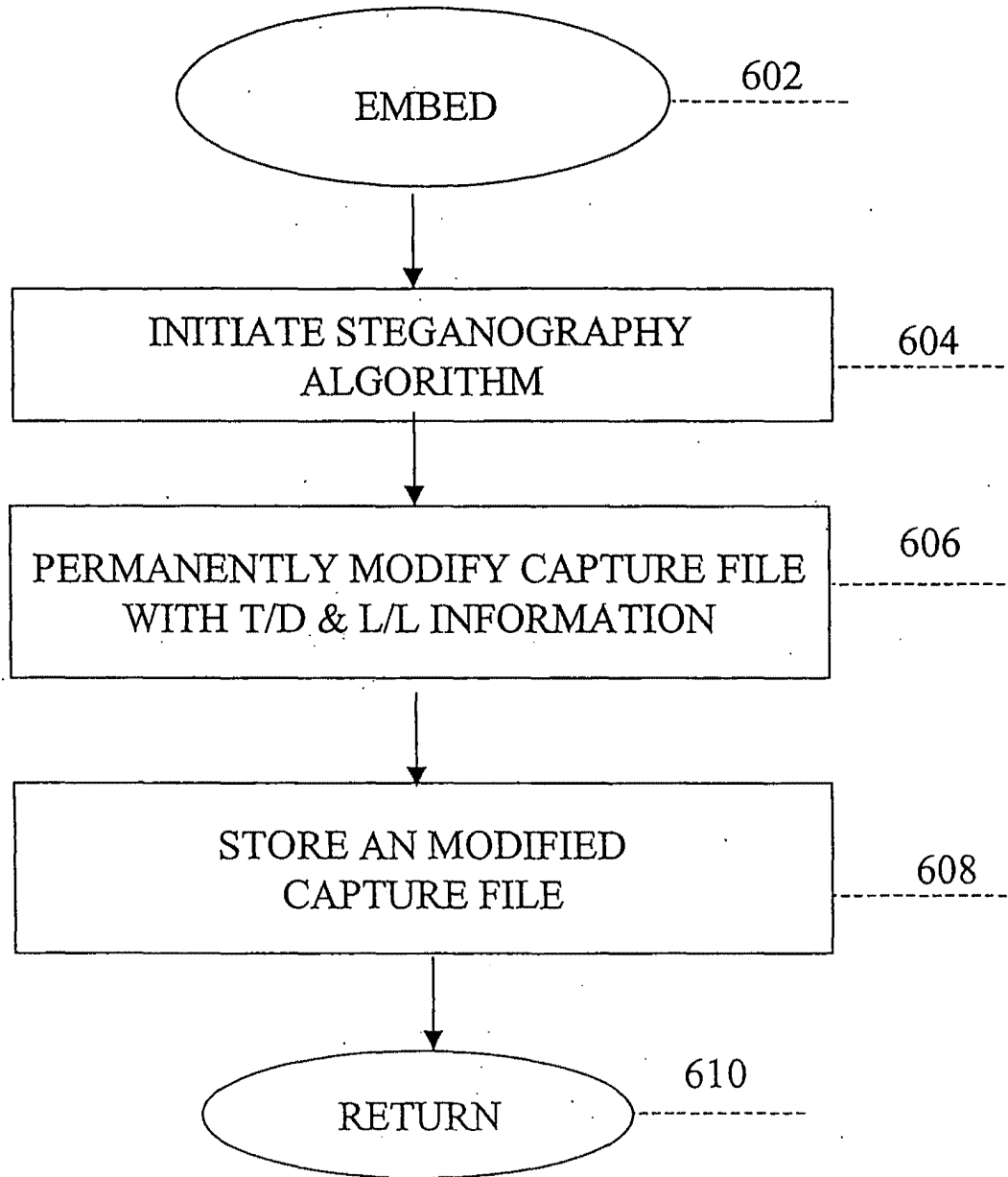


FIG 7

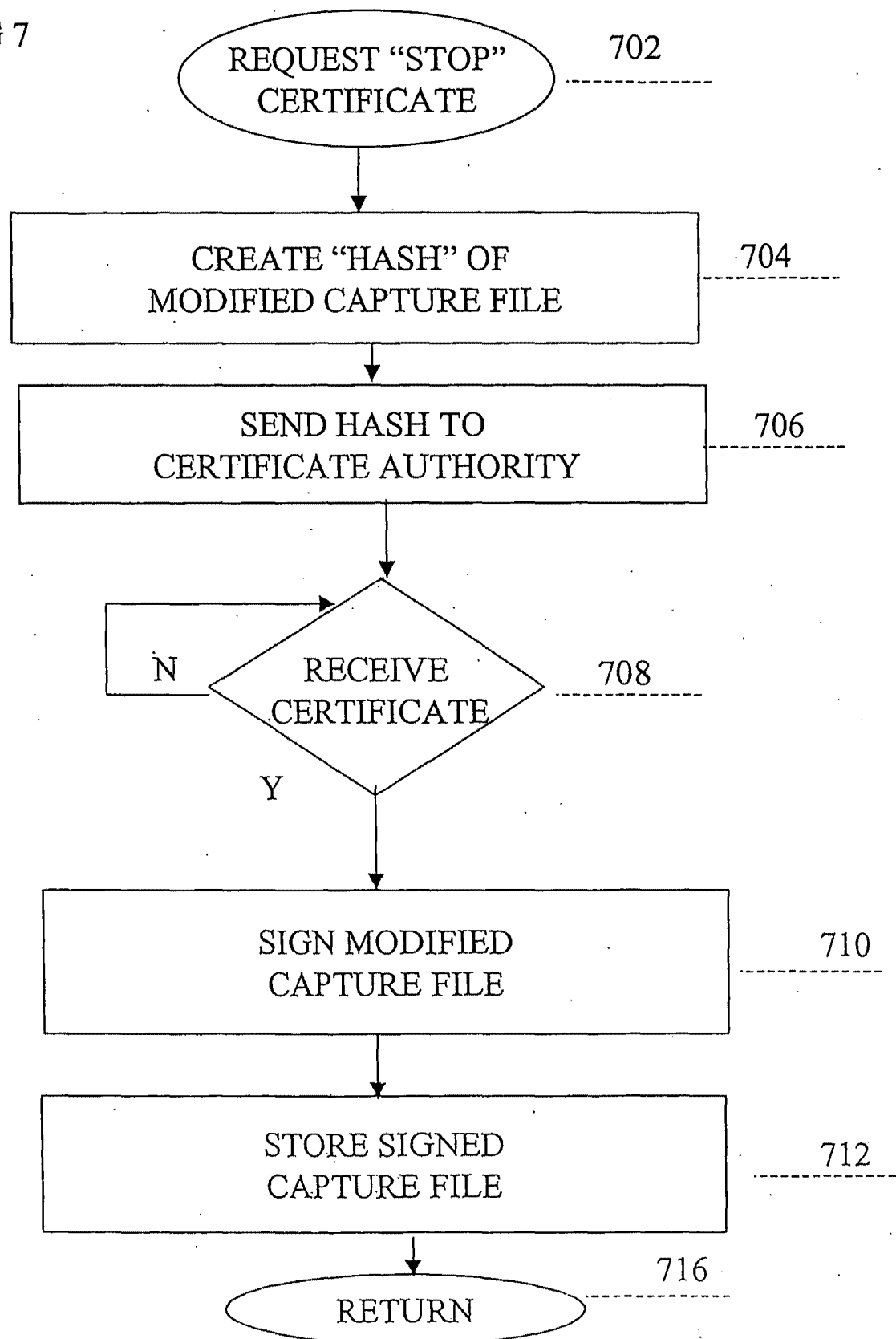
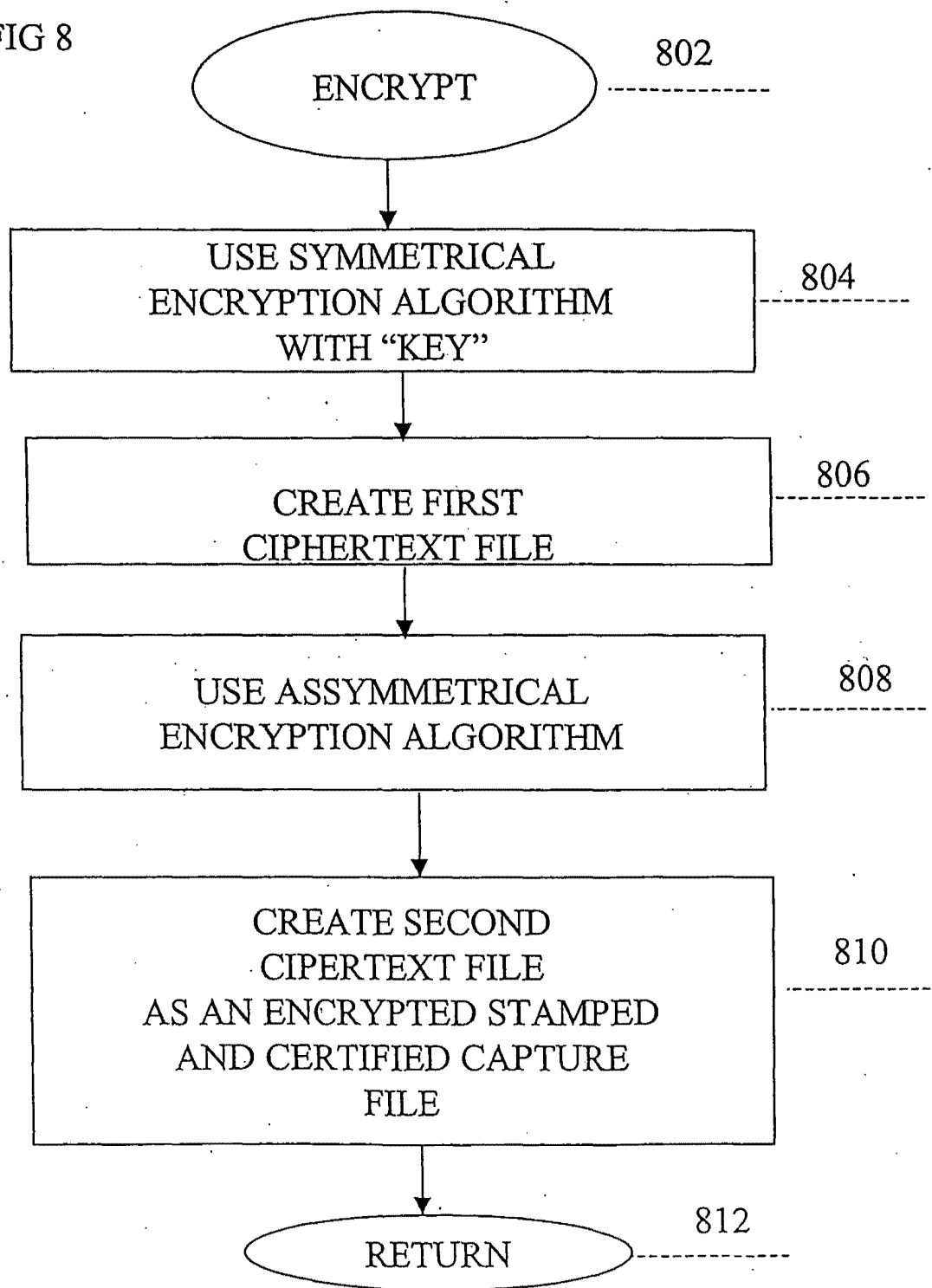




FIG 8



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☐ **BLACK BORDERS**

☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**

☐ **FADED TEXT OR DRAWING**

☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**

☐ **SKEWED/SLANTED IMAGES**

☒ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**

☐ **GRAY SCALE DOCUMENTS**

☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**

☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**

☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

PATENT APPLICATION SERIAL NO \_\_\_\_\_

U.S. DEPARTMENT OF COMMERCE  
PATENT AND TRADEMARK OFFICE  
FEE RECORD SHEET

01/11/2006 MBERHE 00000137 60757075

01 FC:2005 100.00 DP

PTO-1556  
(5/87)