

(19) World Intellectual Property Organization
International Office



(43) International Publication Date
July 13, 2006 (13.07.2006)

PCT

(10) International Publication Number
WO 2006/073040 A1

- (51) International Patent Classification:
G06F 21/24 (2006.01) H04N 5/91 (2006.01)
G11B 20/10 (2006.01) H04N 7/167 (2006.01)
G11B 27/00 (2006.01) H04N 7/173 (2006.01)
- (21) International Application No.: PCT/JP2005/022772
- (22) International Filing Date:
December 12, 2005 (12.12.2005)
- (25) Language of International Application: Japanese
- (26) Language of International Publication: Japanese
- (30) Priority Data:
JP 2005-003152 January 7, 2005 (07.01.2005) JP
- (71) Applicant (for all designated countries except the United States): Matsushita Electric Industrial Co., Ltd. (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 1006 Kadoma, Kadoma-shi, Osaka-fu 5718501 Osaka (JP).
- (72) Inventor; and
- (75) Inventor/Applicant (United States only): Yoshikatsu Ito

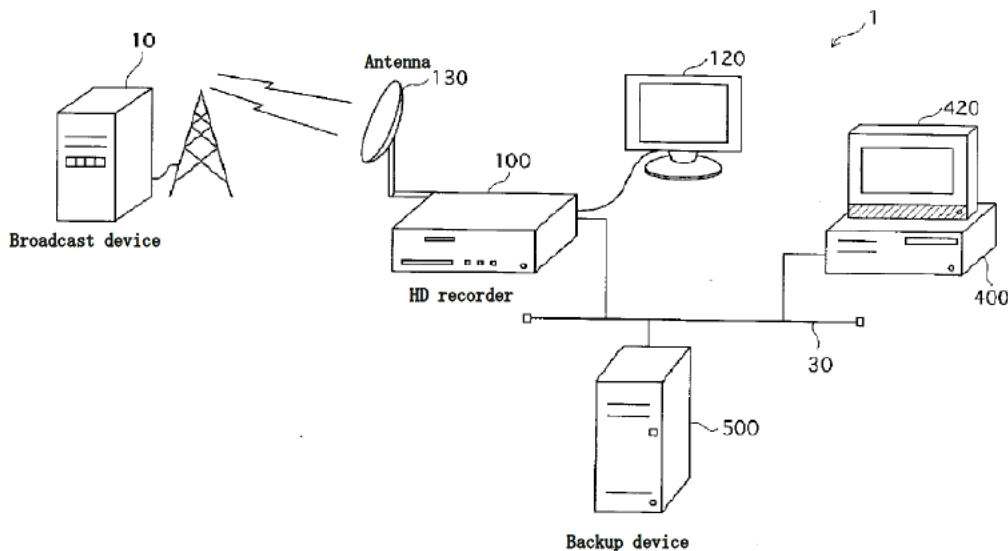
(ITO, Yoshikatsu). Shunji Harada (HARADA, Shunji). Yuko Tsusaka (TSUSAKA, Yuko). Soichiro Fujioka (FUJIOKA, Soichiro). Motoji Ohmori (OHMORI, Motoji). Toshihisa Nakano (NAKANO, Toshihisa).

- (74) Agent: Shiro Nakajima, et al. (NAKAJIMA, Shiro et al.); 6F Bldg 5, 3-2-1 Toyosaki, Kita-ku, Osaka-shi, Osaka-fu 5310072 Osaka (JP).
- (81) Designated countries (all types of domestic protections possible unless expressly noted): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (84) Designated countries (all types of domestic protections possible unless expressly noted): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD,

[Continued]

(54) Title: BACKUP SYSTEM, RECORDING/REPRODUCTION DEVICE, BACKUP DEVICE, BACKUP METHOD, PROGRAM, AND INTEGRATED CIRCUIT

(54) Title of Invention: BACKUP SYSTEM, RECORDING AND PLAYBACK DEVICE, BACKUP DEVICE, BACKUP METHOD, PROGRAM, AND INTEGRATED CIRCUIT



- 10.. BROADCAST DEVICE
- 130.. ANTENNA
- 100.. HD RECORDER
- 500.. BACKUP DEVICE

(57) Abstract: It is impossible to copy a CopyOnce content in an external device even for backup because there is a danger of unauthorized copy if copy for backup is enabled. There is provided an HD recorder (100) for transmitting a content to a backup device (500) and setting an expiration date for the content stored in the HD recorder (100) itself and deleting the content stored in itself upon expiration.

[Continued]

WO 2006/073040 A1



SL, SZ, TZ, UG, ZM, ZW), Eurasia (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), Europe (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI, (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Attached Publications:

- International Search Report

For two-letter codes and other abbreviations, refer to the Guidance Notes for Codes and Abbreviations at the beginning of each regularly issued PCT Gazette.

(57) Summary: Copy Once content cannot be copied to external equipment and the like, even to make a backup which is inconvenient for users, but when copying for backup purposes is permitted, there is a risk of unauthorized copying. The present invention provides an HD recorder 100 that transmits content to a backup device 500, and at the same time sets an expiration date for the content stored in the HD recorder 100 itself, and deletes the content stored in the HD recorder 100 when the expiration date has passed.

Specification

BACKUP SYSTEM, RECORDING AND PLAYBACK DEVICE, BACKUP DEVICE, BACKUP METHOD, PROGRAM, AND INTEGRATED CIRCUIT

[Technical Field]

[0001] The present invention relates to art for generating a backup of digital content while taking into consideration copyright protection of the digital content.

Background Art

[0002] In recent years, digital broadcasting has begun, in which digital content is broadcast. Digital content is less susceptible to deterioration with use, so copy control information (CCI: copy control information) indicating whether copies can be produced and the permitted copy number to be produced are added to protect copyright. This CCI often indicates that only one copy is permitted (Copy Once). When content including a CCI indicating Copy Once is recorded onto a recording medium, the CCI added to this content is rewritten to a CCI indicating that further copying is prohibited (No More Copy). Content containing a No More Copy CCI cannot be copied but is permitted to be moved (MOVE) to other media.

[0003] Even when the content has a CCI attached, there is a possibility that there will be unauthorized access, for example, when a hard disk recorder (hereinafter referred to as HD recorder) is turned off and the content stored on the HDD (hard disk drive) is manipulated using a personal computer or other device. In order to prevent such unauthorized copying, there has been conventional art in which unauthorized use of content is detected by substituting content stored on an HDD in advance into a one-way function, calculating and storing the unauthorized detection information, and when the HD recorder is powered on, substituting the content stored on the HDD into a one-way function, generating verification information, and comparing the generated verification information with the stored unauthorized detection information.

[0004] There is also art for temporarily storing content and erasing the content after a predetermined time has elapsed or after it has been played, thereby enabling shift playback of content that includes a CCI indicating that copying is not permitted, thereby improving user convenience.

However, HDDs have large capacity and permit random access, so users can store digitally broadcasted content in their HD recorders without worrying about storage capacity, and can view the stored content with simple operations.

Disclosure of Invention

Problem to Be Solved by Invention

[0005] Although HDDs are convenient, the incidence of failures increases with frequency of use because writing and reading information involves rotation operations and seek operations. When the HDD fails, there is a risk of losing data. In order to prevent such data loss due to HDD failure, it is considered effective to back up the content on other storage media, recording devices, and the like. However, even when the purpose is to make a backup, once content containing a CCI indicating Copy Once is moved to other media, the content stored in the HD recorder is deleted, resulting in a problem of reduced convenience for the user.

[0006] Furthermore, when copying of content to make a backup is permitted, there is a possibility that a malicious user may illegally copy the content, giving rise to the problem that the rights of copyright holders cannot be adequately protected.

The present invention has been configured in consideration of such problems, and an object thereof is to provide a backup system, a recording and playback device, a backup device, a backup method, an integrated circuit, a backup program, and a recording medium that are capable of backing up content while reaching a balance between copyright protection and user convenience.

Means for Solving Problem

[0007] In order to achieve the foregoing object, the present invention is a backup system composed of a recording and playback device for recording and playing back content and a backup device, wherein the recording and playback device is provided with storage means for storing the content, reception means for receiving an instruction to back up the content, content transmission means for, upon receiving the instruction, reading the content from the storage means and transmitting the read content to the backup device, writing means for, upon receiving the instruction, writing period information indicating a period in which playback of the content that is subject to the

backup is permitted to the storage means in association with the content, and playback control means for permitting playback of the content during a period indicated by the period information and prohibiting playback of the content when the period indicated by the period information ends.

[0008] In the present Specification, "backup" refers to storing a copy of content in a backup device in case the content stored in the authorized equipment is lost due to an operational error or a malfunction. A recording and playback device normally uses the content stored in itself, and when the content stored in the recording and playback device is lost, the recording and playback device obtains a copy from a backup device and restores the lost content. When "content is lost," recovery may be applicable not only for failures on the recording and playback device and the network to which the recording and playback device is connected, deletion due to insufficient memory of the recording and playback device, and erroneous operation, but also when deleted at a user's discretion. However, when the content is lost due to being moved to another recording medium, the recording and playback device cannot obtain the content from the backup device.

Effect of Invention

[0009] According to the above configuration, the content is transmitted to the backup device, and period information indicating a period during which playback of the backed up content is permitted is associated with the content and written to the storage means, and thus the period during which the content stored in the storage means can be played back in the recording and playback device is limited to the period indicated by the period information, permitting users to view the content while protecting the rights of the copyright holder. Therefore, it is possible to balance copyright protection and user convenience while backing up content as a countermeasure against failures.

[0010] Furthermore, the present invention is a recording and playback device for performing recording and playback of content, the recording and playback device being provided with storage means for storing the content, reception means for receiving an instruction to back up the content; content transmission means for, upon receiving the instruction, reading the content from the storage means and transmitting the read content to the backup device if backup of the read content is permitted; writing means for, upon receiving the instruction, writing period

information indicating a period in which playback of the content that is subject to the backup is permitted to the storage means in association with the content; and playback control means for permitting playback of the content during a period indicated by the period information and prohibiting playback of the content when the period indicated by the period information ends.

[0011] According to this configuration, the content is transmitted to the backup device, period information indicating a period during which playback of the backed up content is permitted is associated with the content and written to the storage means, and the playback control means prohibits playback of the content when the period indicated by the period information ends; thus, the period during which the content stored in the storage means can be played back in the recording and playback device is limited to the period indicated by the period information. Therefore, it is possible to reach a balance between copyright protection and user convenience while backing up content as a countermeasure against failures.

[0012] The recording and playback device is further provided with: extension request means for transmitting, to the backup device, an extension request requesting an extension permission for the period indicated by the period information; and extension means for receiving extension permission information indicating permission for the extension from the backup device and extending the period indicated by the period information.

According to this configuration, the extension means receive extension permission information indicating permission for the extension from the backup device, and extends the period indicated by the period information. This permits the user to view the content stored in the recording and playback device even after the end of the period indicated by the period information at the beginning of the backup.

[0013] Furthermore, the recording and playback device transmits the extension request to the backup device, and when extension permission information is received, extends the period information. Here, it is assumed that the backup device is configured to send extension permission information only when the extension request satisfies a predetermined condition, for example, that it is sent from equipment that complies with a specific standard. In this way, the equipment that can extend the period information can be limited to only those that satisfy the predetermined condition.

[0014] In the recording and playback device, the extension request means transmit the extension request a predetermined time before an ending point of the period indicated by the period information.

In this configuration, the extension request means send the extension request a predetermined time before the ending point of the period indicated by the period information, and thus the period during which viewing of the content is permitted is not interrupted on the recording and playback device.

[0015] In the recording and playback device, the extension request means repeatedly transmit the extension request means request periodically within the period indicated by the period information.

According to this configuration, even when transmission fails due to some kind of malfunction, the extension request means repeatedly transmits the extension request, and thus the period indicated by the period information can be reliably extended.

[0016] In the recording and playback device, the extension means receive the extension permission information indicating a period after the period information stored in the storage means and rewrite the period indicated by the period information to the period indicated by the received extension permission information to extend the period information.

According to this configuration, the extension means can quickly and easily extend the period information by simply replacing the period indicated by the period information with the period indicated by the received extension permission information.

[0017] The extension means constituting the recording and playback device store an extension time in advance and extend the period information by adding the extension time to the period indicated by the period information.

In the case of a home network, an in-house LAN, or the like, the backup device receives the extension request from each device connected to the network, determines whether to permit the extension, and transmits extension permission information.

[0018] In the above configuration, the extension means extend the period information by adding an extension time stored in advance to the period indicated by the period information. In this way, by performing a computation to add the extension period to the period in the recording and playback device, the processing executed by the backup device can be reduced. Furthermore, in the present invention, the recording and playback device performs computations related to management and extension of the valid period, and thus the backup device need not be provided with a clock that is protected from external manipulation.

[0019] The period information indicates an ending point of the period in which playback of the

content stored in the storage means is permitted, and the playback control means constituting the recording and playback device permit playback of the content when the current time is before the point indicated by the period information and prohibit playback of the content when the current time is after the point indicated by the period information.

[0020] According to this configuration, the playback control means can easily determine whether to permit or prohibit playback of the content by comparing the current time with the end time.

The period information is a permitted time indicating a length of time in which playback of the content stored in the storage means is permitted and a starting time indicating a starting point of a period in which playback of the content is permitted, and the playback control means of the recording and playback device acquire an elapsed time from the starting time, permit playback of the content when the acquired elapsed time is equal to or less than the permitted time, and prohibit playback of the content when the elapsed time from the starting time exceeds the permitted time.

[0021] According to this configuration, the period information is a permitted time indicating the length of time during which playback of the content stored in the storage means is permitted, and a starting time indicating the starting point of the period during which playback of the content is permitted. The period indicated by the period information is considered to be a predetermined time period from the time the content is backed up to the backup device. The writing means obtain the current time at the time the instruction is received and set the obtained current time as the starting time, thereby easily obtaining the starting time and writing such to the storage means.

[0022] In the recording and playback device, the playback control means prohibit playback of the content by deleting the content from the storage means.

In this configuration, the playback control means deletes the content from the storage means, thus reliably prohibiting playback of the content after the end of the period indicated by the time limit information.

[0023] The recording and playback device of the present invention is further provided with restore instruction acquisition means for acquiring a restore instruction indicating acquisition of the content stored by the backup device, restore request means for transmitting a transmission request for the content stored by the backup device to the backup device, and restoring means for receiving the content from the backup device and writing the received content to the storage

means, wherein when the content is written, the writing means further write period information indicating a period in which playback of the content written by the restoring means is permitted to the storage means in association with the content.

[0024] According to this configuration, the restoring means receive the content from the backup device, and write the received content to the storage means. This permits the user to view the content again.

Furthermore, when the content is received, the writing means write to the storage means period information indicating the period during which playback of the content written to the restoring means is permitted in association with the content, and thus the period during which playback of the obtained content is possible can be limited in the recording and playback device.

[0025] In the recording and playback device, the content stored in the storage means include an encrypted work generated by encrypting a digital work based on an encryption key and a decryption key used to decrypt the encrypted work, and the playback control means prohibit playback of the content by deleting the decryption key included in the content.

[0026] In this configuration, the encrypted work included in the content is generated by encrypting a digital work with an encryption key, and thus, even when the encrypted work is copied by an unauthorized user, the digital work cannot be generated without the decryption key, thereby preventing unauthorized playback of the content.

The recording and playback device is further provided with restore instruction acquisition means for acquiring a restore instruction indicating acquisition of the encryption key stored by the backup device, restore request means for transmitting a transmission request for the decryption key stored by the backup device to the backup device, and restoring means for receiving the decryption key from the backup device and writing the received decryption key to the storage means, wherein when the decryption key is written, the writing means further includes write period information indicating a period in which playback of the content stored by the storage means is permitted to the storage means in association with the content.

- [0027] In this configuration, the restoring means receive the decryption key and write the received decryption key to the storage means. This permits the user to view the content stored in the recording and playback device again. In addition, the writing means write period information indicating the period during which playback of the content stored in the storage means is permitted into the storage means in association with the content, and thus the period during which playback of the content is permitted can be limited in the recording and playback device.
- [0028] In the recording and playback device of the present invention, the content stored in the storage means includes an encrypted work generated by encrypting a digital work using an encryption key, and an encryption key generated by encrypting a decryption key used to decrypt the encrypted work using a unique key that is unique to the recording and playback device, and the playback control means prohibit playback of the content by deleting the encryption key from the storage means.
- [0029] According to this configuration, the content stored in the storage means includes an encryption key generated by encrypting the decryption key using the unique key, and the encrypted work generated by encrypting the digital work using the encryption key. Therefore, even when the content is copied, the content cannot be reproduced without the unique key, and thus unauthorized playback of the content by a third party can be prevented.
- [0030] The content stored in the storage means includes backup information indicating permission or prohibition of backup, the content transmission means constituting the recording and playback device determine whether the backup information indicates permission for backup and transmit the content when it is determined that permission is indicated, and the writing means determine whether the backup information indicates permission for backup and write the period information when it is determined that permission is indicated.
- [0031] In this configuration, backup information indicating whether backup is possible is added to the content in advance by the creator, and the content transmission means transmit the content only when the backup information indicates that backup is permitted. Therefore, the intention of the creator of the content can be reflected with regard to the backup of the content.

[0032] The content transmission means constituting the recording and playback device encrypt the content using a communication key and transmit the encrypted content securely.

This configuration makes it possible to prevent the content from being intercepted by an unauthorized third party.

The recording and playback device is further provided with detection information storage means for storing detection information generated by performing a predetermined computation on the content and fraud prohibition means for reading the content from the storage means, performing the predetermined computation on the read content to generate inspection information, comparing the generated inspection information to the detection information, and prohibiting unauthorized use of the content that is determined not to match.

[0033] According to this configuration, the fraud prohibition means compare the detection information and the inspection information generated by the same computation. When a one-way function is used for this computation, even a partial change in the content will result in the detection information not matching the inspection information. Therefore, any falsification of the content can be easily detected, and playback of content that has been illegally falsified by a malicious third party can be prevented.

[0034] The backup device stores other content in response to a backup instruction by equipment other than the recording and playback device, the recording and playback device being further provided with restore instruction acquisition means for acquiring a restore instruction indicating acquisition of the other content, content request means for transmitting a transmission request for the other content to the backup device when the list instruction is acquired, and restoring means for receiving the other content from the backup device and writing the received other content to the storage means, and when the other content is received, the writing means further write period information indicating a period in which playback of the other content is permitted to the storage means in association with the other content.

[0035] According to this configuration, the restoring means receive the other content from the backup device and write the received other content to the storage means, and thus the same content can be shared among equipment belonging to the same network, for example, a home network or an

company internal LAN. This permits users to view the same content on any equipment installed in different rooms, improving user convenience.

[0036] Furthermore, when the other content is written to the storage means, the writing means associate period information indicating a period in which playback of the other content is permitted with the other content and write such to the storage means, whereby the period in which the content can be reproduced can be limited in each device having the content.

Moreover, the present invention is a backup device provided with: storage means for storing the content; extension reception means for receiving, from the recording and playback device, an extension request seeking permission to extend period information indicating a period during which playback of the content stored by the recording and playback device is permitted; determination means for determining whether to permit the extension; and permission means for outputting, to the recording and playback device, extension permission information indicating permission of the extension when such is determined to be permitted.

[0037] In this configuration, when the determination means determine that the extension is permitted, the permission means output extension permission information indicating that the extension is permitted. This permits only devices that satisfy a certain condition to extend the period information relating to the playback of the content, and unauthorized equipment that does not satisfy the conditions cannot extend the period information. Therefore, in equipment that does not satisfy the conditions, it is possible to stop the playback of the content after the period indicated by the period information has ended.

[0038] The storage means constituting the backup device further store identification information indicating the content in correspondence with the content, the extension reception means receive the extension request including content identification information indicating the content stored by the recording and playback device, and the determination means compare the content identification information to the identification information stored by the storage means, and when both match, make a determination to permit the extension.

[0039] In this configuration, the determination means determine that the content is permitted when the content identification information matches the identification information stored in the storage means. Therefore, when the content stored in the backup device is moved and is no longer a backup for malfunctions, the period indicated by the period information is not extended, and when the period ends, it becomes impossible to play back the content on the recording and

playback device. This prevents a malicious user from being able to view both the content moved from the backup device and the content on the recording and playback device.

[0040] The extension request includes device identification information indicating the recording and playback device to which the extension request was output, and in the backup device, the determination means store one or more pieces of permitted device identification information indicating a specific piece of equipment in advance, and when the device identification information included in the received extension request matches any of the permitted device identification information, make a determination to permit the extension.

[0041] In this configuration, the determination means determine to grant permission when the device identification information included in the received extension request matches any of the permitted device identification information indicating specific equipment that has been stored in advance. This makes it possible to extend the period information and extend the period during which playback of the content is permitted only on specific equipment, and the period during which playback of the content is permitted cannot be extended on other equipment.

[0042] In the backup device, the storage means further store detection information generated by performing a predetermined computation on the content in correspondence with the content; and the determination means read the content from the storage means, perform the predetermined computation on the read content to generate verification information, compare generated verification information to the detection information, and, when both match, make a determination to permit the extension.

[0043] In this configuration, the determination means compare verification information generated by performing the same computation on the content via the detection information stored in the storage means, and when they match, permits the extension. When a one-way function is used for the computation, any falsification of the content can be easily detected. Therefore, when the content backed up by the backup device is illegally tampered with, the recording and playback device is not permitted to extend the period during which playback of the content is permitted, and the period during which the content can be played back can be limited.

[0044] In the backup device, the permission means output the extension permission information indicating a later period than the period indicated by the period information.

According to this configuration, the permission means output the extended period information as the extension permission information, and thus the recording and playback device can quickly extend the period by replacing the period information with the extended period information.

[0045] Furthermore, the backup device sets the extended period information, and thus the backup device can collectively manage the period during which playback of the content of each device is permitted.

The backup device is further provided with restore receiving means for receiving a transmission request for the content stored by the storage means, restore determination means for determining whether to transmit the content, and restore transmission means for reading the content from the storage means and transmitting the read content when it is determined that the content is to be transmitted.

[0046] In this configuration, when the restore determination means determine to transmit the content, the restore transmission means read the content from the storage means, and transmits the read content. Therefore, equipment that satisfies certain conditions can acquire the content, and users can enjoy viewing the content. In addition, it is possible to prevent the content from being played back on equipment that does not satisfy predetermined conditions.

[0047] The transmission request includes restore equipment identification information indicating restore equipment device which is the transmission source of the transmission request, the restore determination means constituting the backup device store one or more pieces of permitted device identification information indicating a specific piece of equipment in advance, and when the restore equipment identification information matches any of the permitted device identification information, make a determination to transmit the content.

[0048] According to this configuration, the restore determination means determine to transmit the content when the restore equipment identification information is included in permitted device identification information stored in advance. Therefore, equipment that can acquire the content can be limited to only specific equipment that has been set in advance.

The permitted device identification information indicates a backup source device that instructed backup of the content stored by the storage means, and in the backup device, the restore determination means make a determination to transmit the content when the restore

equipment identification information matches the permitted device identification information.

[0049] According to this configuration, the equipment capable of retrieving the content can be limited to only the backup source device that has been instructed to back up the content stored in the storage means.

In the backup device of the present invention, the restore determination means have a copy number indicating the total number of pieces of equipment storing content that is identical to the content stored in the storage means and that is permitted to be played back by the backup device, and a permitted copy number indicating an upper limit of the copy number, and when the copy number is less than the permitted copy number, a determination is made for the content to be transmitted.

[0050] In this configuration, the restore determination means determine to transmit the content when the number of copies is less than the permitted copy number. Therefore, the total number of devices having the same content as the content can be limited to less than the permitted copy number.

The backup device is further provided with: equipment identification information indicating equipment storing content that is identical to the content stored by the storage means and that is permitted to be played back by the backup device; period information storage means for associating and storing copy period information indicating a period in which playback of the content is permitted in the equipment; and copy number management means for subtracting one from the copy number when the period indicated by the copy period information ends.

[0051] In this configuration, the copy number management means or the backup device subtracts 1 from the copy number when the period indicated by the copy period information ends. Therefore, when the period during which viewing of the content is permitted on certain equipment ends, the backup device can output the content to another device.

In the backup device, the content stored by the storage means includes the permitted copy number in advance, and the determination means acquire the permitted copy number from the content.

[0052] The creator of the content can generate content containing any permitted copy number, so in this configuration, the determination means can make a determination that reflects the intention

of the creator of the content by using the permitted copy number obtained from the content.

The restore transmission means constituting the backup device encrypt the content using a communication key and safely transmit encrypted content.

[0053] This configuration makes it possible to prevent the content from being intercepted by an unauthorized third party.

Furthermore, the recording and playback device outputs startup instruction information instructing startup to the backup device prior to the extension request, and the backup device is further provided with power control means for starting power supply to each circuit constituting the backup device upon receiving the startup instruction.

[0054] The backup device has a role of storing content as a countermeasure against malfunctions, and thus it is desirable that its operation time be short. According to the above configuration, upon receiving the startup instruction, the power control means start supplying power to each circuit constituting the backup device. Therefore, the operating time of the backup device can be shortened, and the probability of occurrence of a breakdown in the hard disk unit constituting the storage means can be reduced.

Brief Description of Drawings

[0055] [FIG. 1] A diagram illustrating the configuration of a backup system 1 according to embodiment 1.

[FIG. 2] A block diagram illustrating the configuration of an HD recorder 100.

[FIG. 3] Illustrates one example of information stored in an information storage unit 110.

[FIG. 4] Illustrates details of a content management table 121.

[FIG. 5] A block diagram illustrating the configuration of a control unit 107.

[FIG. 6] Illustrates one example of a menu screen 181 and a playback list screen 211 displayed on a monitor 120.

[FIG. 7] Illustrates one example of an initial setup screen 191 and a restore information screen 221 displayed on the monitor 120.

[FIG. 8] A block diagram illustrating the configuration of a backup device 500.

[FIG. 9] Illustrates one example of information stored in a content storage unit 510.

[FIG. 10] Illustrates one example of information stored in a secure information storage unit 511.

[FIG. 11] Illustrates the details of a backup management table 521.

[FIG. 12] A flowchart illustrating operation of the HD recorder 100.

[FIG. 13] A flowchart illustrating a recording process by the HD recorder 100.

[FIG. 14] A flowchart illustrating a recording process by the HD recorder 100. Continued from FIG. 13.

[FIG. 15] A flowchart illustrating a content playback process.

[FIG. 16] A flowchart illustrating a restore process by the HD recorder 100 and the backup device 500.

[FIG. 17] A flowchart illustrating a restore process by the HD recorder 100 and the backup device 500. Continued from FIG. 16.

[FIG. 18] A flowchart illustrating a backup process by the HD recorder 100 and the backup device 500.

[FIG. 19] A flowchart illustrating a backup process by the HD recorder 100 and the backup device 500. Continued from FIG. 18.

[FIG. 20] A flowchart illustrating a backup process by the HD recorder 100 and the backup device 500. Continued from FIG. 18.

[FIG. 21] A flowchart illustrating an expiration date extension process by the HD recorder 100 and the backup device 500.

[FIG. 22] A flowchart illustrating an expiration date extension process by the HD recorder 100 and the backup device 500. Continued from FIG. 21.

[FIG. 23] A flowchart illustrating an expiration date extension process by the HD recorder 100 and the backup device 500. Continued from FIG. 21.

[FIG. 24] A flowchart illustrating an equipment authentication process by the HD recorder 100 and the backup device 500.

[FIG. 25] A flowchart illustrating an equipment authentication process by the HD recorder 100 and the backup device 500. Continued from FIG. 24.

Description of Reference Numerals

[0056]	1	Backup system
	10	Broadcast device
	100	HD recorder

- 101 Transmitting and receiving unit
- 102 Authentication unit
- 103 Input unit
- 104 Playback control unit
- 105 Decoding unit
- 106 Key generation unit
- 107 Control unit
- 108 Unique information storage unit
- 109 Encryption processing unit
- 110 Information storage unit
- 112 Input and output unit
- 113 Secure storage unit
- 114 Broadcast receiving unit
- 120 Monitor
- 400 HD recorder
- 500 Backup device
- 501 Transmitting and receiving unit
- 502 Authentication unit
- 503 Power source unit
- 504 Unique information storage unit
- 507 Control unit
- 509 Encryption processing unit
- 510 Content storage unit
- 511 Secure information storage unit
- 512 Input unit
- 513 Display unit

Best Mode for Carrying Out Invention

[0057] 1. Embodiment 1

The backup system 1 according to embodiment 1 of the present invention will be described below with reference to the drawings.

1.1 Overview of Backup System 1

The backup system 1 of the present invention is provided with a hard disk recorder (hereinafter referred to as HD recorder) 100, an HD recorder 400, and a backup device 500, as illustrated in FIG. 1. The HD recorder 100, the HD recorder 400, and the backup device 500 are connected via a LAN (Local Area Network) 30.

[0058] The HD recorder 100 receives broadcast waves transmitted from the broadcast device 10, acquires content composed of video and audio, and stores the acquired content. The HD recorder 100 can also receive content from an external recording medium such as a DVD that is attached thereto.

Based on a user operation, the HD recorder 100 transmits the stored content to the backup device 500 and sets an expiration date for the content stored within itself.

[0059] The backup device 500 receives the content from the HD recorder 100 and stores the received content.

Furthermore, when the expiration date approaches, the HD recorder 100 makes a request to the backup device 500 to postpone the expiration date.

The backup device 500 receives the request to postpone the expiration date of the content from the HD recorder 100, confirms that the content corresponding to the received request is properly stored, and permits the HD recorder 100 to postpone the expiration date.

[0060] When the postponement is permitted by the backup device 500, the HD recorder 100 postpones the expiration date stored therein. When the extension is not permitted or when communication with the backup device 500 cannot be established due to a malfunction of the LAN 30, the HD recorder 100 deletes the content whose expiration date has passed. After the deletion, the HD recorder 100, in response to a user operation or the like, acquires from the backup device 500 the content backed up in the backup device 500 and sets a new expiration date.

[0061] Furthermore, the HD recorder 100 can obtain not only the content that the HD recorder 100

itself has transmitted to the backup device 500, but also the content that the HD recorder 400 has transmitted to the backup device 500.

Similarly to the HD recorder 100, the HD recorder 400 receives, stores, and plays back content including broadcast programs, and transmits the received content to the backup device 500.

1.2 HD Recorder 100 and HD Recorder 400

As illustrated in FIG. 2, the HD recorder 100 is composed of a transmitting and receiving unit 101, an authentication unit 102, an input unit 103, a playback control unit 104, a decoding unit 105, a key generation unit 106, a control unit 107, a unique information storage unit 108, an encryption processing unit 109, an information storage unit 110, an input and output unit 112, a secure storage unit 113, a broadcast receiving unit 114, and an antenna 130.

[0062] Specifically, the HD recorder 100 is a computer system including a microprocessor, a RAM, and a ROM, and a computer program are stored in the RAM and ROM. The microprocessor operates according to the computer program, whereby the HD recorder 100 achieves part of its functions.

The configuration and operation of the HD recorder 400 are similar to those of the HD recorder 100, and therefore a detailed description thereof will be omitted.

(1) Unique information storage unit 108

The unique information storage unit 108 is composed of ROM and stores a device identifier 115 "ID_A" and a device-unique key 116 "Key_A." Furthermore, the unique information storage unit 108 is provided with a protection mechanism and is protected from access by external equipment.

[0063] The device identifier 115 "ID_A" is information that uniquely identifies the HD recorder 100. The device-unique key 116 "Key_A" is key information unique to the HD recorder 100. These are written in advance to the unique information storage unit 108 when the HD recorder 100 is shipped.

(2) Information storage unit 110

The information storage unit 110 is composed of a hard disk unit, and stores, as one example, a backup history table 131 and content files 134, 139, and so on, as illustrated in FIG. 3. Each content file includes a content ID, encrypted content, and an encrypted content key. The content ID is identification information that uniquely identifies the encrypted content. The encrypted content is generated by applying an encryption algorithm E1 to the content acquired from the

broadcast device 10 or an external recording medium using a content key. In this case, the content includes image data and audio data compressed by a compression method such as MPEG2.

[0064] The encrypted content key is generated by applying the encryption algorithm E1 to the content key used to encrypt the content, using the device-unique key 116 "Key_A" stored in the unique information storage unit 108. Content keys and content correspond one-to-one. In this case, one example of the encryption algorithm E1 is DES (Data Encryption Standard) or the like.

[0065] For example, a content file 134 includes a content ID 136 "A001," encrypted content 137, and an encrypted content key 138 "Enc(Key_A,Key_1a)," wherein the content ID 136 "A001" is identification information indicating the encrypted content 137. The encrypted content 137 is generated by applying the encryption algorithm E1 to the content including the video using the content key "Key_1a." The encrypted content key 138 "Enc(Key_A, Key_1a)" is generated by applying the encryption algorithm E1 to the content key "Key_1a" using the device-unique key 116 "Key_A" stored in the unique information storage unit 108. The content key "Key_1a" has a one-to-one correspondence with the content on which the encrypted content 137 is based.

[0066] The backup history table 131 includes the date and time when the HD recorder 100 performed backup to the backup device 500 and the content ID of each content file stored in the information storage unit 110 at that time, in association with each other.

In addition, various image data such as a menu screen, an initial setup screen, and the like is stored.

(3) Secure storage unit 113

A secure storage unit 113 includes a flash memory and is protected from access by external equipment.

[0067] The secure storage unit 113 stores, as one example, a content management table 121 illustrated in FIG. 4. As illustrated in FIG. 4, the content management table 121 includes a plurality of pieces of content information 122, 123, 124, and so on. Each piece of content information management information is composed of a content ID, a title, a recording date and time, a hash value, a type, a compression method, an expiration date, a backup flag, and a priority

level and corresponds one-to-one to a content file stored in the information storage unit 110.

[0068] The content ID is information for identifying the encrypted content included in the corresponding content file and is the same as the content ID included in the corresponding content file.

The title is a name indicating the corresponding encrypted content, and is not written as of the time when the content on which the encrypted content is based is acquired from the broadcast device 10 or an external recording medium.

[0069] The recording date and time indicate the date and time when the original encrypted content included in the corresponding content file was acquired from the broadcast device 10 or the recording medium. The type is information indicating the route by which the content was obtained, and examples include "broadcast program" indicating that the content was received from broadcast device 10, and "photograph" indicating that the content is image data captured by a digital camera or the like. The compression method is the name of the compression method used to compress the video and audio that constitute the content.

[0070] The hash value is generated by linking the encrypted content contained in the corresponding content file to the encrypted content key and substituting them into a hash function. The hash function used here is, as one example, SHA-1.

The expiration date indicates the date and time at which the period during which the corresponding encrypted content can be used in the HD recorder 100 ends.

[0071] The backup flag is a flag indicating whether the corresponding encrypted content has been backed up in the backup device 500 and has a value of "1" or "0." A "1" indicates that it is backed up, and a "0" indicates that it is not backed up.

The priority level is information indicating the priority level of saving the content and has a value of "1" or "2." While writing new encrypted content to the information storage unit 110, when the information storage unit 110 does not have enough free space, the control unit 107 deletes content files corresponding to content information that includes a priority level of "2" to secure storage space. Even when free space in the information storage unit 110 becomes insufficient, content files corresponding to content information including a priority level of "1" are not deleted. The priority level is automatically set to "1" when the content is acquired but can be changed by user operation.

[0072] For example, the content information 122 corresponds to the content file 134 stored in the

information storage unit 110. A content ID 151 "A001" is identification information indicating the encrypted content 137, and is the same as the content ID 136 "A001." A title 152 "variety show" is a name entered by the user for the encrypted content 137. Furthermore, a recording date and time 153 "04.10.10.17:00" indicates that the encrypted content 137 was generated by encrypting content acquired at 17:00 on Oct. 10, 2004. A hash value 154 "01a" is generated by substituting a combination of the encrypted content 137 and the encrypted content key 138 "Enc(Key_A, Key_1a)" into a hash function. Moreover, an expiration date 157 "04.12.15.17" indicates that the corresponding encrypted content 137 can be decrypted and played back on the HD recorder 100 until 17:00 on Dec. 15, 2004.

(4) Antenna 130, broadcast receiving unit 114, decoding unit 105

An antenna 130 receives broadcast waves transmitted from a broadcast device 10.

[0073] The broadcast receiving unit 114 includes a tuner, a modulation and demodulation unit, a transport decoder, and the like and selects one broadcast wave from the received broadcast waves of the antenna 130, converts the selected broadcast wave into a digital signal, and generates TS (transport stream) packets. Next, the generated TS packets are output to the decoding unit 105 in the order in which they were generated.

Also, a recording instruction indicating to record the content currently being received is received from the control unit 107. When the recording instruction is received, the generated TS packets are output to the control unit 107 consecutively in the order in which they were generated. The output of TS packets continues until an end notification is received from the control unit 107.

[0074] In this case, the content that the HD recorder 100 obtains from the broadcast device 10 is composed of a plurality of TS packets. In the following description, unless otherwise necessary, the TS packets that constitute the content will not be mentioned and will simply be referred to as content.

Due to the instruction of the control unit 107, the decoding unit 105 decompresses the content acquired by the broadcast receiving unit 114 and content generated by an encryption processing unit 109 (described later) according to the compression method of each set of content, such as MPEG (Moving Picture Experts Group) 2 or JPEG (Joint Photographic Experts Group), to generate image data and audio data, and outputs the generated image data and audio data to the

playback control unit 104.

[0075] MPEG2 and JPEG are well-known art, so description thereof will be omitted.

(5) Transmitting and receiving unit 101

The transmitting and receiving unit 101 is connected to the LAN 30 and transmits and receives information between the control unit 107 and authentication unit 102 and external equipment. In this case, the external equipment is the backup device 500.

(6) Authentication unit 102

The authentication unit 102 stores in advance a private key SK_A unique to the HD recorder 100, a public key certificate Cert_A, a public key PK_CA of a certification authority, and a CRL (Certificate Revocation List). The public key certificate Cert_A certifies the validity of the private key SK_A and the corresponding public key PK_A, and includes a certificate identification number, the public key PK_A, and signature data of the certification authority. The signature data of the certification authority is generated by applying a signature generation algorithm S to at least the public key PK_A using the private key SK_CA of the certification authority. One example of the signature generation algorithm S is an Elgamal signature over a finite field. Elgamal signatures are well known, so description thereof will be omitted.

[0076] In this case, the certificate authority is an impartial third party organization, and issues a public key certificate for each device constituting the backup system 1 of embodiment 1.

CRLs contain certificate identification numbers of revoked public key certificates.

The public key PK_CA of the certification authority is a public key that pairs with the private key SK_CA of the certification authority.

The authentication unit 102 performs equipment authentication between itself and the external equipment according to DTCP (Digital Transmission Content Protection) in response to an instruction from the control unit 107, and when the authentication fails, prohibits communication between the control unit 107 and the external device. When the authentication is successful, a common session key is generated between itself and the external equipment, and the generated session key is output to the control unit 107. Operations of equipment authentication will be described in detail later.

(7) Input unit 103

The input unit 103 includes various buttons such as a power button, a record button, a menu button, and a selection button, as well as a receiving circuit for a remote controller.

[0077] A button operation and a remote controller operation by the user are accepted, and operation

instruction information indicating the accepted button operation and remote controller operation is output to the control unit 107.

(8) Key generation unit 106 and encryption processing unit 109

The key generation unit 106 receives an instruction to generate a content key from the control unit 107. When an instruction to generate a content key is received, a pseudo-random number is generated, and a 56-bit content key is generated using the generated pseudo-random number. The generated content key is output to the control unit 107. The content key may be generated using other methods.

[0078] The encryption processing unit 109 receives plaintext information and the key from the control unit 107 and is instructed to encrypt the information. Also, it receives ciphertext and the key from the control unit 107 and is instructed to decrypt such.

When encryption is instructed, the encryption algorithm E1 is applied to the received plaintext using the received key to generate ciphertext, and the generated ciphertext is output to the control unit 107.

When instructed to decrypt, a decryption algorithm D1 is applied to the ciphertext received using the received key to generate decrypted text, and the generated decrypted text is output to the control unit 107.

[0079] Examples of combinations of the plaintext and the key received by the encryption processing unit 109 include content and a content key, and a content key and a device-unique key "Key_A." Furthermore, combinations of the ciphertext and the key received by the encryption processing unit 109 are encrypted content and a content key, and an encrypted content key and a device-unique key "Key_A."

The decryption algorithm D1 is an algorithm for decrypting the ciphertext generated by the encryption algorithm E1.

(9) Control unit 107

As illustrated in FIG. 5, the control unit 107 includes a secure clock 117, a main control unit 118, and an expiration date management unit 119.

[0080] (a) Secure clock 117

The secure clock 117 is a clock that measures the passage of time and calculates the current time. The calculated current time includes the date, day of the week, and time of day.

Furthermore, the secure clock 117 is provided with a protection mechanism and is protected from external manipulation.

[0081] (b) Expiration date management unit 119

The expiration date management unit 119 stores an extension execution time "24 hours" in advance. The extension execution time "24 hours" is a criterion for determining whether to request an extension of the expiration date of the encrypted content stored in HD recorder 100, and in this case, when the time remaining until the expiration date is less than "24 hours," the expiration date management unit 119 makes a request to the backup device 500 to extend the expiration date.

[0082] The expiration date management unit 119 receives an expiration date extension instruction from the main control unit 118, which instructs extension of the expiration date of each content. Also, a deletion instruction is received which indicates deletion of expired content.

(b-1) Expiration date extension processing

When an instruction to extend the expiration date is received, the expiration date management unit 119 selects each piece of content information constituting the content management table 121 stored in the secure storage unit 113 one by one in order and performs the processing described below on the selected content information.

[0083] The expiration date management unit 119 reads out the expiration date from the selected content information. When no expiration date is written in the selected content information, the process moves to the next content information.

After reading the expiration date, the expiration date management unit 119 next obtains the current time from the secure clock. The difference between the read expiration date and the obtained current time is calculated. In this case, the calculated difference is called the remaining time.

[0084] When the calculated remaining time is equal to or greater than the extension execution time "24 hours," the expiration date management unit 119 ends the process for the selected content information and moves to the process for the next content information.

When the calculated remaining time is less than the update execution time of "24 hours," the expiration date management unit 119 transmits a startup instruction indicating startup to the backup device 500 via the transmitting and receiving unit 101.

Next, the expiration date management unit 119 receives a startup notification from the backup device 500 indicating that it has started up. When the startup notification is not received within a certain period of time, the process for the selected content information is terminated, and the process moves to the next content information.

[0085] Upon receiving the startup notification, the expiration date management unit 119 instructs the authentication unit 102 to perform equipment authentication with the backup device 500. When the equipment authentication by the authentication unit 102 is successful, a session key generated

in the equipment authentication is received from the authentication unit 102. In the following process, the expiration date management unit 119 uses a session key to encrypt and decrypt information sent and received between the backup device 500 and performs secret communication, but for the sake of simplicity, description of these encryption and decryption processes is omitted.

[0086] When the equipment authentication by the authentication unit 102 fails, the process for the selected content information is terminated, and the process moves to the next content information.

Upon receiving the session key from the authentication unit 102, the expiration date management unit 119 reads a content ID contained in the selected content information, reads the device identifier 115 "ID_A" from the unique information storage unit 108, and transmits the read content ID and device identifier, as well as an extension request requesting an extension of the expiration date, to the backup device 500 via the transmitting and receiving unit 101.

[0087] Next, the expiration date management unit 119 receives a new term of validity or an error notification indicating that the extension request cannot be accepted, from the backup device 500 and via the transmitting and receiving unit 101.

When the error notification is received, the expiration date management unit 119 ends the process for the selected content information and moves to the process of the next content information.

When the new expiration date is received, the expiration date management unit 119 updates the expiration date included in the selected content information with the received expiration date, and moves to the process of the next content information.

[0088] When the foregoing processing is completed for all content information, an extension termination notification indicating that the extension of the expiration date has ended is output to the main control unit 118.

(b-2) Deletion processing

Upon receiving a deletion instruction from the main control unit 118, the expiration date management unit 119 selects the content information constituting the content management table 121 stored in the secure storage unit 113 one by one in order, and performs the processing described below for the selected content information.

[0089] The expiration date management unit 119 reads an expiration date from the selected content information. When no expiration date is written in the selected content information, the process moves to the next content information.

When the expiration date is read, the expiration date management unit 119 next acquires the current time from the secure clock 117. The read expiration date is compared to the acquired

current time, and when the current time indicates a point in time prior to the expiration date, the process proceeds as-is to the next content information.

[0090] When the current time indicates a point after the expiration date, the expiration date management unit 119 reads out the content ID contained in the selected content information, and deletes from the information storage unit 110 the content file that contains the content ID that matches the read content ID. Next, the selected content information is deleted, and the process moves to the next content information.

When the foregoing processing of all content information is completed, a deletion termination notification indicating that the deletion process of the expired content is completed is output to the main control unit 118.

[0091] (c) Main control unit 118

The main control unit 118 stores in advance the extension time to which the expiration date of the encrypted content stored in the information storage unit 110 is to be extended. In this case, the extension time "2:00" is stored. A time interval for deleting expired content is also stored, which is "30 minutes." These are set when the HD recorder 100 is shipped.

[0092] The main control unit 118 receives various types of operation instruction information from the input unit 103, and controls various types of processing in accordance with the received operation instruction information.

Specifically, when the operation instruction information indicating that the record button has been pressed is received, control of the (c-1) recording processing described below is performed.

Upon receiving operation instruction information indicating the pressing of the menu button, the main control unit 118 generates a menu screen 181 based on the image data stored in the information storage unit 110, outputs the generated menu screen 181 to the playback control unit 104, and instructs to display the menu screen 181. FIG. 6(a) is one example of the menu screen 181 displayed in this case. The menu screen 181 includes a playback list display button 182, a restore button 183, a timer reservation button 184, a program guide display button 185, a content list button 186, a dubbing settings item button 187, an initial setup button 188, and a content management button 189. The user uses directional keys to place a cursor on one of the buttons and presses a confirm button to select one of the buttons.

[0093] Upon receiving operation instruction information indicating selection of the playback list display button 182, the main control unit 118 controls the (c-2) playback processing described

below. Moreover, when operation instruction information indicating selection of the initial setup button 188 is received, the (c-3) initial setup processing described below is performed. When the operation instruction information indicating the selection of the restore button 183 is received, the (c-4) restore processing described below is executed.

[0094] When operation instruction information indicating the selection of other buttons is received, the main control unit 118 performs various processes according to each button, such as accepting timer reservations, displaying a program guide, and inputting and outputting information from an external recording medium.

Furthermore, the main control unit 118 periodically monitors the secure clock 117, and when it determines that the time indicated by the secure clock 117 is "2:00," which is the extension time, it outputs an instruction to the expiration date management unit 119 to extend the expiration date.

[0095] The main control unit 118 also measures time using the secure clock 117, and outputs a deletion instruction to the expiration date management unit 119 every 30 minutes, instructing the deletion of expired content.

The following describes control of (c-1) recording processing, control of (c-2) playback processing, (c-3) initial setup processing, (c-4) restore processing, and (c-5) backup processing performed by the main control unit 118.

[0096] (c-1) Control of recording processing

Upon receiving operation instruction information indicating the pressing of the record button from the input unit 103, the main control unit 118 generates a new content ID and adds content information including the generated content ID to the content management table 121 stored in the secure storage unit 113. At this time, the current time is written as the recording date and time of the added content information, "broadcast program" is written as the type, "MPEG2" is written as the compression method, "0" is written as the backup flag, and "1" is written as the priority level.

[0097] Next, the main control unit 118 outputs an instruction to generate a content key to the key generation unit 106, and receives the content key from the key generation unit 106. Upon receiving the content key, the main control unit 118 generates a new content file in the information storage unit 110.

Next, the main control unit 118 outputs a recording instruction to the broadcast receiving unit 114 and receives content from the broadcast receiving unit 114. The content key and content received are output to the encryption processing unit 109, and an instruction is given to encrypt the content. The encrypted content is received from the encryption processing unit 109. The main control unit 118 writes the received encrypted content into a new content file created in the

information storage unit 110.

[0098] As already described above, the content output from the broadcast receiving unit 114 here is composed of multiple TS packets, and the main control unit 118 repeatedly receives the content on a TS packet basis, instructs encryption, and writes the encrypted content until it receives operational instruction information indicating that the stop button has been pressed.

In parallel with this repetition, the main control unit 118 monitors free space in the information storage unit 110. When it is determined that there is insufficient free space, the content information constituting the content management table 121 is selected with a priority level of "2," the content file corresponding to the selected content information is deleted from the information storage unit 110, and the selected content information is deleted from the content management table 121.

[0099] When there is no content information with a priority level of "2" among the content management table 121, that is, when there is no content that can be deleted in the information storage unit 110, the main control unit 118 notifies the user, for example by flashing a lamp, that there is insufficient storage capacity and that recording will be stopped.

When the storage capacity of the information storage unit 110 is insufficient and recording is interrupted, or when operational instruction information indicating the pressing of the stop button is received from the input unit 103, the main control unit 118 outputs an end notification to the broadcast receiving unit 114 indicating the end of recording.

[0100] Next, the main control unit 118 reads device-unique key 116 "Key_A" from unique information storage unit 108, outputs the read device-unique key 116 "Key_A" and the content key to encryption processing unit 109, and instructs encryption of the content key. The encryption processing unit 109 receives the encrypted content key and writes the received encrypted content key and the generated content ID to the generated content file.

[0101] Next, the main control unit 118 reads the encrypted content and the encrypted content key from the generated content file, links the read encrypted content and encrypted content key, and substitutes them into a hash function to generate a 160-bit hash value. The calculated hash value is written into the added content information.

(c-2) Control of playback processing

When the user selects the playback list display button 182 by button operation, the main

control unit 118 generates a playback list screen 211 using the image data stored in the information storage unit 110 and the title and recording date and time of each piece of content information that makes up the content management table 121, and outputs the display of the generated playback list screen 211 to the playback control unit 104. The playback list screen 211 illustrated in FIG. 6(b) is the playback list screen 211 displayed in this case.

[0102] The playback list screen 211 includes content buttons 212, 213, 214, and 215, each content button corresponding to content information 122, 123, 124, and 125 constituting the content management table 121, respectively.

Next, selection of a content button by a user operation is accepted.

When any of the content buttons is selected by the user, the main control unit 118 reads from secure storage unit 113 the content ID included in the content information corresponding to the selected content button. In the information storage unit 110, a content file containing a content ID that matches the read content ID is detected. The encrypted content and the encrypted content key are read from the detected content file, the read encrypted content and the encrypted content key are linked, and a hash value is calculated by substituting them into a hash function.

[0103] The main control unit 118 reads out the hash value contained in the content information corresponding to the selected content button, compares the read hash value to the calculated hash value, and when the two do not match, generates an error screen indicating that the selected content cannot be played. The main control unit 118 outputs the generated error screen to the playback control unit 104, instructs such to display the error screen, and stops playback of the content.

[0104] When the read hash value matches the calculated hash value, the main control unit 118 reads the device-unique key 116 "Key_A" from the unique information storage unit 108, outputs the read device-unique key 116 "Key_A" and the read encrypted content key to the encryption processing unit 109, and instructs such to decrypt the encrypted content key.

Next, the main control unit 118 receives the content key from the encryption processing unit 109. When the content key is received, the encrypted content is read from the detected content file, outputs the read encrypted content and the received content key to the encryption processing unit 109, and instructs such to decrypt the encrypted content. Next, the main control unit 118 receives the content from the encryption processing unit 109 and outputs the received content to

the decoding unit 105.

(c-3) Initial setup processing

When operation instruction information indicating selection of the initial setup button 188 is received while the menu screen 181 illustrated in FIG. 6(a) is displayed on the monitor 120, the main control unit 118 generates an initial setup screen 191 and instructs the playback control unit 104 to display the generated initial setup screen 191. FIG. 7(a) illustrates the initial setup screen 191 displayed in this case. The initial setup screen 191 includes settings items 192, 193, 194, and 196. When the user moves the cursor to any of the settings items, a settings box corresponding to the settings item is displayed. In FIG. 7(a), settings boxes 197 to 201 corresponding to the settings item 196 "Backup" are displayed.

[0105] The main control unit 118 accepts input operations by the user into the settings boxes 197 to 201. In this case, "All" is entered in the settings box 197, indicating that all content is to be backed up regardless of the type of content.

In the settings box 198, "Sunday 12:30 am" is entered as a schedule for transmitting encrypted content to the backup device 500 for backup.

[0106] In the settings box 199, "New only" is entered, which indicates that, among the encrypted content stored in the information storage unit 110, only new encrypted content that has not been backed up is to be backed up.

In the settings box 201, "Manual" is entered as a method for starting the restoration of the content backed up in the backup device 500, which indicates that the restoration is to be started by a user operation. In the following description, the HD recorder 100 acquiring the encrypted content backed up in the backup device 500 is referred to as restoration.

[0107] Next, the main control unit 118 receives operational instruction information indicating that the enter button has been pressed from input unit 103, and stores the settings items input in each settings box.

Also, although not specifically illustrated, when the user places the cursor on buttons 192 to 194, input of settings relating to channel, picture quality, and disk is accepted, and the inputted settings are stored by pressing the Confirm button.

(c-4) Restore processing

When the menu screen 181 illustrated in FIG. 6(a) is displayed on the monitor 120 and operational instruction information indicating selection of the restore button 183 is received, the main control unit 118 transmits a startup instruction to the backup device 500 via the transmitting and receiving unit 101.

[0108] When a startup notification indicating normal startup is not received from the backup device 500 via the transmitting and receiving unit 101 within a specified time, the main control unit 118 generates an error screen to notify the user that restoration is not possible due to a failure in communication with the backup device 500. The generated error screen is displayed on the monitor 120 via the playback control unit 104, and the following processing is stopped.

[0109] When a startup notification is received from the backup device 500 via the transmitting and receiving unit 101 within a predetermined time, the main control unit 118 instructs the authentication unit 102 to perform equipment authentication with the backup device 500. When equipment authentication by the authentication unit 102 fails, the main control unit 118 generates an error screen to notify the user that restoration is not possible because communication with the backup device 500 has failed, displays the generated error screen on the monitor 120 via the playback control unit 104, and stops the following processing.

[0110] When the equipment authentication is successful, the main control unit 118 receives a session key from authentication unit 102. When transmitting and receiving information to and from the backup device 500, the main control unit 118 performs secret communication using the received session key by common key encryption. For simplicity, the following description will omit a description of encryption and decryption processes involved in secret communications.

The main control unit 118 reads the device identifier 115 "ID_A" from the unique information storage unit 108, and transmits a restore information request requesting information on encrypted content that can be restored along with the read device identifier 115 "ID_A" to the backup device 500 via the transmitting and receiving unit 101.

[0111] Next, the main control unit 118 receives the content ID, title, and recording date and time corresponding to each of the encrypted content stored in the backup device 500 from the backup device 500 via the transmitting and receiving unit 101. The received content ID, title, and recording date and time are temporarily stored, and the restore information screen 221 illustrated in FIG. 7(b) is generated using the image data stored in the information storage unit 110 and the received title and recording date and time, and the generated restore information screen 221 is

displayed on the monitor 120 via the playback control unit 104.

[0112] A plurality of content buttons 222 to 225 are displayed on the restore information screen 221.

The main control unit 118 receives operational instruction information indicating the selection of any of the content buttons from the input unit 103, and reads out the content ID corresponding to the received operational instruction information. Next, the main control unit 118 transmits the read content ID and a restore request for requesting restoration of the encrypted content indicated by the content ID to the backup device 500 via the transmitting and receiving unit 101.

[0113] Next, the encrypted content, the content key, and the expiration date are received from the backup device 500 via the transmitting and receiving unit 101. A new content file is generated in the information storage unit 110, and the content ID corresponding to the content button selected by the user and the received encrypted content are written to the generated content file.

Next, the main control unit 118 reads the device-unique key 116 "Key_A" from the secure storage unit 113, outputs the read device-unique key 116 "Key_A" and the received content key to the encryption processing unit 109, and instructs content key encryption. Upon receiving the encrypted content key from the encryption processing unit 109, the encrypted content key received is written to the newly generated content file.

[0114] Next, the main control unit 118 reads the encrypted content and the encrypted content key from the content file newly generated on the information storage unit 110, combines the read encrypted content and the encrypted content key, and assigns the encrypted content to a hash function, and calculates a hash value. After calculating the hash value, the main control unit 118 generates content information including the content ID, title, recording date and time, expiration date, and the calculated hash value corresponding to the content button selected by the user, and adds the generated content information to the content management table 121. At this time, a backup flag of "1" and a priority level of "2" are written to the added content information, and the restore process is terminated.

[0115] During these processes, once an error notification is received from backup device 500 indicating that restoration is not possible, an error screen indicating that restoration has failed is generated, and the generated error screen is displayed on the monitor 120 via the playback control unit 104.

In this case, the user selects the content to be restored and retrieves the selected content from

the backup device 500, but the backup history table 131 may also be used to return the state of the information storage unit 110 to the state immediately after the backup was performed. In this case, the main control unit 118 reads out dates when backups were performed from the backup history table 131 and displays the read out dates on the monitor 120. The user selects one of the displayed dates. The main control unit 118 reads out the content ID stored in the backup history table 131 in association with the selected date. Of the read content IDs, only content IDs not included in the content management table 121 are extracted, and the extracted content IDs are transmitted to the backup device 500, and a transmission of the encrypted content corresponding to the transmitted content ID is requested.

(c-5) Backup processing

The main control unit 118 stores settings related to backup operations performed by the user. In this case, it is assumed that the settings entered on the initial setup screen 191 are stored.

[0116] The main control unit 118 periodically monitors the time, and when determining that the current time is "Sunday 12:30 am," selects, in order, each piece of content information that constitutes the content management table 121 stored in the secure storage unit 113, and performs the following processing on the selected content information.

The backup flag included in the selected content information is read out. When the read backup flag is "0," the process moves to the next content information.

[0117] When not "0," the main control unit 118 detects a content file corresponding to the selected content information on information storage unit 110 based on the content ID included in the selected content information. The encrypted content and the encrypted content key included in the detected content file are read from the information storage unit 110, and the read encrypted content and the encrypted content key are combined and substituted into a hash function to calculate a hash value. The calculated hash value is compared to the hash value included in the selected content information. When the two do not match, the process moves to the next content information.

[0118] When the two do match, the main control unit 118 transmits a startup instruction to the backup device 500 via the transmitting and receiving unit 101. When the startup notification is not

received from the backup device 500 via the transmitting and receiving unit 101 within a predetermined time, the main control unit 118 stops subsequent processing.

Upon receiving the startup notification via the transmitting and receiving unit 101 within a predetermined time, the main control unit 118 instructs the authentication unit 102 to perform equipment authentication with the backup device 500. When the equipment authentication by the authentication unit 102 fails, the main control unit 118 stops subsequent processing.

[0119] When the equipment authentication by the authentication unit 102 is successful, the main control unit 118 receives a session key from the authentication unit 102. When transmitting and receiving information to and from the backup device 500, the main control unit 118 performs secret communication using a common key encryption method using the received session key. For simplicity, the following description will omit a description of encryption and decryption processes involved in secret communications.

[0120] The main control unit 118 reads the device-unique key 116 "Key_A" from the unique information storage unit 108, outputs the read device-unique key 116 "Key_A" and the encrypted content key read from the information storage unit 110 to the encryption processing unit 109, and instructs decryption of the encrypted content key.

The main control unit 118 receives the content key from the encryption processing unit 109. When the content key is received, the encrypted content contained in the detected content file is read, the device identifier 115 "ID_A" is read from the unique information storage unit 108, and the content ID, title, and recording date and time contained in the selected content information are read from the secure storage unit 113. Next, the main control unit 118 transmits a backup request instructing a backup, the read device identifier 115 "ID_A", the content ID, the title, the recording date and time, the content key, and the encrypted content to the backup device 500 via the transmitting and receiving unit 101.

[0121] Next, the main control unit 118 receives an error notification or expiration date indicating that the backup request cannot be accepted from the backup device 500 via the transmitting and receiving unit 101.

When the error notification is received, the main control unit 118 stops subsequent processing.

When the expiration date is received, the main control unit 118 writes the received expiration date into the selected content information and changes the backup flag to "1." Next, the priority level is set to "2," and the process moves to the next content information.

[0122] When the foregoing processing is completed for all content information, the main control unit 118 reads out the content ID from each piece of content information included in the content

management table 121 and writes the read content ID and the current date to the backup history table 131.

Note that when the user presses the backup button provided on the input unit 103, the main control unit 118 starts the above backup process regardless of the backup schedule set in the initial setup processing.

(10) Playback control unit 104 and monitor 120

The playback control unit 104 includes an image signal processing unit and an audio signal processing unit. The playback control unit 104 receives image data and audio data from the decoding unit 105. The image signal processing unit generates an image signal from the received image data. A vertical synchronizing signal, A horizontal synchronizing signal, and the generated image signal are output to the monitor 120. Also, in response to an instruction from the control unit 107, an image signal from various screen data is generated and output to the monitor 120.

[0123] The audio signal processing unit generates an analog audio signal from the received audio data, and outputs the generated analog audio signal to the monitor 120.

The monitor 120 has a built-in speaker, receives a horizontal sync signal, a vertical sync signal, and an image signal from the image signal processing unit, and displays an image based on the received horizontal sync signal, vertical sync signal, and image signal. The speaker also receives an analog audio signal from the audio signal processing unit, converts the received analog audio signal into audio, and outputs the audio.

(11) Input and output unit 112

The input and output unit 112 has installed, as one example, a recording medium such as a DVD or a memory card. As instructed by the control unit 107, information recorded on the recording medium is read and information is written to the recording medium.

1.3 Backup Device 500

As illustrated in FIG. 8, the backup device 500 is composed of a transmitting and receiving unit 501, an authentication unit 502, a power source unit 503, a control unit 507, an encryption processing unit 509, a unique information storage unit 504, a content storage unit 510, a secure information storage unit 511, an input unit 512, and a display unit 513.

[0124] The backup device 500 is specifically a computer system including a microprocessor, a RAM, and a ROM. Computer programs stored in the RAM and ROM, and the backup device 500 achieves a portion of the function thereof by the microprocessor operating in accordance with

the computer programs.

(1) Unique information storage unit 504

The unique information storage unit 504 is composed of a ROM and stores a device-unique key 516 "Key_C" as illustrated in FIG. 8. The device-unique key 516 "Key_C" is key data unique to the backup device 500 and is written when the backup device 500 is shipped.

[0125] (2) Content storage unit 510

The content storage unit 510 is composed of a hard disk unit, and stores, as one example, content files 529, 534, 539, and so on, as illustrated in FIG. 9.

Each content file includes a content ID, encrypted content, and an encrypted content key. The content ID is identification information corresponding to the encrypted content. The encrypted content is generated by applying the encryption algorithm E1 to the content using the content key. The encrypted content key is generated by applying the encryption algorithm E1 to the content key used for encrypting the content by using the device-unique key 516 "Key_C" stored in the unique information storage unit 508.

[0126] For example, the content file 529 includes a content ID 531 "A001," encrypted content 532, and encrypted content key 533 "Enc(Key_C,Key_1a)."

A content ID 531 "A001" is information that uniquely identifies the encrypted content 532, which is the same as the content ID 136 "A001" stored in the information storage unit 110 of the HD recorder 100. The encrypted content 532 is generated by applying the encryption algorithm E1 to the content by using the content key "Key_1a." The encrypted content 532 is the same as the encrypted content 137 stored in the information storage unit 110 of the HD recorder 100.

[0127] The encrypted content key 533 "Enc(Key_C, Key_1a)" is generated by applying the encryption algorithm E1 to the content key "Key_1a" by using the device-unique key 516 "Key_C" stored in the unique information storage unit 504.

(3) Secure information storage unit 511

The secure information storage unit 511 includes a flash memory. Furthermore, the secure information storage unit 511 is provided with a protection mechanism and is protected from

access by external equipment.

[0128] As one example, the secure information storage unit 511 stores a backup management table 521 and permitted device identification information 551, as illustrated in FIG. 10.

As illustrated in FIG. 11, the backup management table 521 includes a plurality of backup information 522, 523, 524, 525, and so on. Each piece of backup information is composed of a content ID, a title, a recording date and time, a backup source device identifier, and a hash value. Each piece of content information has a one-to-one correspondence with a content file stored in the content storage unit 510.

[0129] The content ID is the same as the content ID contained in the corresponding content file and is identification information that indicates the encrypted content. The title is the name of the corresponding encrypted content.

The recording date and time are the date and time as of the time when the HD recorder 100 or the HD recorder 400 obtained the original content of the encrypted content from the broadcast device 10 or the external recording medium. The backup source device identifier is the device identifier of the device that requested the backup of the encrypted content included in the corresponding content file. The hash value is generated by linking the encrypted content included in the corresponding content file to the encrypted content key and substituting them into a hash function.

[0130] The permitted device identification information 551 includes identification information of equipment from which the backup device 500 accepts various instructions such as a backup request. In this embodiment, the backup system 1 includes a device identifier 552 "ID_A" indicating the HD recorder 100 and a device identifier 553 "ID_B" indicating the HD recorder 400.

(4) Power source unit 503

The power source unit 503 obtains power from an external power source and supplies the obtained power to each circuit constituting the backup device 500 in accordance with an instruction from the control unit 507.

[0131] Normally, the power source unit 503 supplies power only to the transmitting and receiving unit 501 and the control unit 507.

The power source unit 503 receives an instruction from the control unit 507 to start supplying power. When an instruction to start supplying power is given, the power supply to each of the

other parts is started. Also, the control unit 507 issues an instruction to stop the power supply. When an instruction to stop the power supply is given, the power supply to each unit other than the transmitting and receiving unit 501 and the control unit 507 is stopped.

[0132] (5) Transmitting and receiving unit 501

The transmitting and receiving unit 501 is connected to the LAN 30, and transmits and receives various types of information between the external equipment connected to the LAN 30 and the control unit 507 and authentication unit 502. In this case, the external equipment is the HD recorder 100 and the HD recorder 400.

(6) Authentication unit 502

The authentication unit 502 stores in advance a private key SK_C unique to the backup device 500, a public key certificate Cert_C, a public key PK_CA of the certification authority, and a CRL. A public key certificate Cert_C certifies the legitimacy of the private key SK_C and the corresponding public key PK_C and is composed of a certificate identification number, the public key PK_C, and the signature data of the certification authority. The signature data of the certification authority is generated by applying a signature generation algorithm S to at least the public key PK_C using the private key SK_CA of the certification authority.

[0133] The CRL includes certificate identification numbers of revoked public key certificate.

The public key PK_CA of the certification authority is a public key that pairs with the private key SK_CA of the certification authority.

The authentication unit 502 performs equipment authentication between it and external equipment according to DTCP at the instruction of the control unit 507, and when authentication fails, communication between the control unit 507 and the external device is prohibited. When authentication is successful, a session key common with the external equipment is generated, and the generated session key is output to the control unit 507. Operations of equipment authentication will be described in detail later.

[0134] (7) Encryption processing unit 509

The encryption processing unit 509 receives plaintext and a key from the control unit 507, and is instructed to encrypt the plaintext. Furthermore, the ciphertext and key are received from the control unit 507, and decryption of the ciphertext is instructed.

When encryption is instructed, the encryption algorithm E1 is applied to the received plaintext using the received key to generate a ciphertext, and the generated ciphertext is output to the control unit 507.

[0135] When decoding is instructed, the decryption algorithm D1 is applied to the ciphertext received using the received key to generate decrypted text, and the generated decrypted text is output to the control unit 107.

The combination of plaintext and key received by the encryption processing unit 509 is, for

example, a content key and a device-unique key "Key_C." Furthermore, the combination of the ciphertext and the key received by the encryption processing unit 509 is the encrypted content key and the device-unique key "Key_C."

[0136] (8) Control unit 507

The control unit 507 stores a viewing time "240 hours." The viewing time is the time during which the encrypted content that has been backed up can be used by the HD recorder 100 and the HD recorder 400.

Furthermore, although not specifically illustrated, the control unit 507 is provided with a secure clock that cannot be externally manipulated.

[0137] The control unit 507 receives a startup instruction from external equipment via the transmitting and receiving unit 501. The external equipment is the HD recorder 100 and the HD recorder 400.

When the startup instruction is received, the power source unit 503 is instructed to start supplying power. Next, a startup notification indicating that the backup device 500 has started up is transmitted via the transmitting and receiving unit 501 to the external equipment.

[0138] Next, the control unit 507 instructs the authentication unit 502 to perform equipment authentication with the external equipment. When the equipment authentication by the authentication unit 502 fails, an instruction is given to the power source unit 503 to stop supplying power.

When the equipment authentication by the authentication unit 502 is successful, a session key is received from the authentication unit 502. In the following process, the control unit 507 implements secret communication with the external equipment by common key encryption using the received session key, but description of the encryption and decryption processes related to the secret communication is omitted.

[0139] Next, the control unit 507 receives the device identifier, the backup request, the content ID, the content key, the title, the recording date and time, and the encrypted content from the external equipment via the transmitting and receiving unit 501. Alternatively, the device identifier, the extension request, and the content ID are received. Alternatively, the device identifier and the restore information request are received.

(a) Backup processing

Upon receiving the device identifier, backup request, content ID, content key, title, recording date and time, and encrypted content, the control unit 507 verifies that the received device identifier is included in the permitted device identification information 551 stored in the secure information storage unit 511. When such is not included, an error notification indicating that the

backup request cannot be accepted is sent to the external equipment via the transmitting and receiving unit 501. Next, the power source unit 503 is instructed to stop supplying power.

[0140] When the received device identifier is included in the permitted device identification information 551 stored in the secure information storage unit 511, the device-unique key 516 "Key_C" is read from the unique information storage unit 504. The read device-unique key 516 "Key_C" and the received content key are output to the encryption processing unit 509, and an instruction is given to encrypt the content key.

Next, the control unit 507 receives the encrypted content key from encryption processing unit 509, generates a content file including the received content ID, encrypted content, and encrypted content key, and writes the generated content file to the content storage unit 510.

[0141] Next, the control unit 507 reads the encrypted content and the encrypted content key contained in the content file written in the content storage unit 510, substitutes the binding of the read encrypted content and the encrypted content key into a hash function, and generates a 160-bit hash value.

Next, the control unit 507 generates backup information composed of the received content ID, title, recording date and time, device identifier, and the calculated hash value, and adds the generated backup information to the backup management table 521. In this case, the received device identifier is set as the backup source device identifier.

[0142] Next, the control unit 507 obtains the current time from the secure clock, and adds a viewing time "240 hours" to the obtained current time to calculate the expiration date. Next, the calculated expiration date is transmitted to the external equipment via the transmitting and receiving unit 501.

Once the transmission is completed, the control unit 507 instructs the power source unit 503 to stop supplying power.

(b) Expiration date extension processing

Upon receiving the device identifier, extension request, and content ID via the transmitting and receiving unit 501, the control unit 507 confirms that the received device identifier matches one of the device identifiers included in the permitted device identification information 551 stored in the secure information storage unit 511. When there is no match, an error notification indicating that the extension request cannot be accepted is transmitted to the external equipment via the transmitting and receiving unit 501. Next, the power source unit 503 is instructed to stop supplying power.

[0143] When the received device identifier matches any of the device identifiers included in the permitted device identification information 551, the control unit 507 selects backup information that includes the same content ID as the received content ID.

Next, the control unit 507 detects from content storage unit 510 a content file that includes the same content ID as the received content ID, and reads the encrypted content and the encrypted content key included in the detected content file. The read encrypted content and the encrypted content key are combined and substituted into a hash function to calculate a hash value.

[0144] The calculated hash value is compared to the hash value contained in the selected backup information, and when the two do not match, the control unit 507 outputs an error notification indicating that the extension request cannot be accepted to the external equipment via the transmitting and receiving unit 501.

When the two do match, the control unit 507 acquires the current time from the secure clock, adds the viewing time "240 hours" to the acquired current time, and calculates the expiration date. Next, the calculated expiration date is transmitted to the external equipment via the transmitting and receiving unit 501.

[0145] (c) Restore processing

Upon receiving the device identifier and the restore information request from the external equipment, the control unit 507 confirms that the received device identifier is included in the permitted device identification information 551 stored in the secure information storage unit 511. Otherwise, an error notification indicating that the restore information request cannot be accepted is transmitted to the external equipment via the transmitting and receiving unit 501. Next, the power source unit 503 is instructed to stop supplying power.

[0146] When the received device identifier is included in the permitted device identification information 551, the control unit 507 reads the content ID, title, and recording time from all backup information included in the backup management table 521 stored in the secure information storage unit 511. The read content ID, title, and recording time are transmitted to external equipment via the transmitting and receiving unit 501.

Next, the control unit 507 receives the content ID and a restore request from the external equipment via the transmitting and receiving unit 501. When the content ID and the restore request are received, backup information including the same content ID as the received content ID is selected from the backup management table 521.

[0147] Next, the control unit 507 detects the content file corresponding to the selected backup

information based on the received content ID. The encrypted content and the encrypted content key are read from the detected content file. The read encrypted content and the encrypted content key are combined and substituted into a hash function to calculate a hash value. The calculated hash value to the hash value is compared included in the selected backup information.

[0148] When the two do not match, the control unit 507 sends an error notification to the external equipment via the transmitting and receiving unit 501 indicating that the restore request cannot be accepted. Next, the power source unit 503 is instructed to stop supplying power.

When the two do match, the control unit 507 reads the device-unique key 516 "Key_C" from the unique information storage unit 504, outputs the read encrypted content key and the device-unique key 516 "Key_C" to the encryption processing unit 509, and instructs to decrypt the encrypted content key. Next, the content key is received from the encryption processing unit 509. Upon receiving the content key, the control unit 507 reads the encrypted content from the detected content file.

[0149] Next, the control unit 507 acquires the current time from the secure clock, adds the viewing time "240 hours" to the acquired current time, and calculates the expiration date. The read encrypted content, the received content key, and the calculated expiration date are transmitted to the external equipment via the transmitting and receiving unit 501.

When transmission is completed, the control unit 507 instructs the power source unit 503 to stop supplying power.

[0150] (9) Input unit 512 and display unit 513

The input unit 512 receives information and instructions input by an operator and outputs the received information and operation instruction information corresponding to the received instructions to the control unit 507.

The display unit 513 displays various information under the control of the control unit 507.

1.4 Operation of Backup System 1

Operation of the backup system 1 will be described below.

[0151] (1) Operation of HD recorder 100

Operation of the HD recorder 100 will be described with reference to the flowchart illustrated in FIG. 12. For convenience of description, the description will start from step S111. The main control unit 118 stores the backup settings configured on the initial setup screen 191 illustrated in FIG. 7, including the content type "all," the backup schedule "Sunday 12:30 am," the backup

mode "new only," and the restore mode "manual."

[0152] The control unit 107 of the HD recorder 100 compares the current time indicated by the secure clock 117 to the extension time "2:00" stored in its own memory (step S111), and upon determining that the current time is "2:00" (YES in step S111), performs an expiration date extension process (step S112). When it is determined that the current time is not "2:00" (NO in step S111), step S112 is not performed and the process moves to step S113.

[0153] Next, the control unit 107 compares the current time with the stored backup schedule "Sunday 12:30 am," and upon determining that the current time is "Sunday 12:30 am" (YES in step S113), performs backup processing (step S114).

When it is determined that the current time is not "Sunday 12:30 am" (NO in step S113), the process moves to step S115.

[0154] Next, when the time elapsed since the most recent expired content deletion process exceeds "30 minutes" (YES in step S115), the control unit 107 again compares the expiration date contained in each piece of content information in the content management table 121 to the current time, deletes the content file corresponding to the expired content information from the information storage unit 110, and deletes the content information from the content management table 121 (step S116).

[0155] When the elapsed time is less than "30 minutes" (NO in step S115), the control unit 107 does not perform the process in step S116 and moves to step S117.

Next, when the power button is pressed by the user (YES in step S117), the control unit 107 accepts button operations and remote controller operations by the user via the input unit 103 (step S118) and performs various processes according to the accepted button operations.

[0156] When the power button is not pressed (NO in step S117), the process returns to step S111 and continues to monitor the current time.

When the record button is pressed in step S118, the control unit 107 executes a recording process (step S122). When the recording process is completed, the process returns to step S118, and operations from the user are accepted.

[0157] Also, in step S118, when the power button is pressed, the process returns to step S111 and

continues monitoring the time.

When another button is pressed in step S118, other processing is performed (step S123).

When it is determined in step S118 that the menu button has been pressed, the control unit 107 displays the menu screen 181 illustrated in FIG. 6(a) on the monitor 120 (step S121), and accepts a selection by the user (step S124).

[0158] When the initial setup button 188 is selected (step S124), the control unit 107 displays the initial setup screen 191 illustrated in FIG. 7(a) on the monitor 120 (step S126), and accepts various settings made by the user through button operations (step S127). When the settings acceptance is completed, the process returns to step S118.

When the playback list display button 182 is selected in step S124, playback processing is performed (step S129). When the playback processing ends, the process returns to step S118.

[0159] In step S124, when the restore button 183 is selected, the control unit 107 performs restore processing (step S131). When the restore processing is completed, the process moves to step S118. When another button is selected, other processing is performed (step S181), and the process returns to step S118.

(2) Recording process by HD recorder 100

The recording process by the HD recorder 100 will be described below with reference to the flowchart illustrated in FIG. 13. This is step S122 in FIG. 12 in detail.

[0160] Upon receiving operation instruction information indicating that the record button has been pressed, the control unit 107 generates a new content ID (step S151) and adds content information including the generated content ID to the content management table 121 (step S153). The current time is written into the recording date and time of the added content information (step S154), and "broadcast program" is written into the type (step S156). Furthermore, "MPEG2" is written into the compression method (step S157), "0" is written into the backup flag (step S158), and "1" is written into the priority level (step S161).

[0161] Next, the control unit 107 instructs the key generation unit 106 to generate a content key. The key generation unit 106 generates the content key and outputs the generated content key to the control unit 107 (step S162).

Next, the control unit 107 generates a new content file in the information storage unit 110 (step S163). Next, a recording instruction is output to the broadcast receiving unit 114. The broadcast receiving unit 114 receives the content via the antenna 130 (step S164) and outputs the received content to the control unit 107 in units of TS packets.

[0162] The processing in step S164 to step S168 below is repeated until the user presses the stop button. When the stop button is pressed (YES in step S166), the process moves to step S171.

First, the control unit 107 outputs the content received from the broadcast receiving unit 114 and the content key received from the key generation unit 106 to the encryption processing unit 109 and instructs such to encrypt the content. The encryption processing unit 109 encrypts the content using the received content key and outputs the generated encrypted content to the control unit 107 (step S167).

[0163] The control unit 107 writes the encrypted content generated by the encryption processing unit 109 to the content file generated in the information storage unit 110 (step S168), and the process returns to step S164.

When the stop button is pressed (YES in step S166), the control unit 107 reads the device-unique key 116 "Key_A" from the unique information storage unit 108 (step S171), and outputs the read device-unique key 116 "Key_A" and the content key to the encryption processing unit 109, and instructs to encrypt the content key. The encryption processing unit 109 encrypts the content key using the received device-unique key 116 "Key_A" to generate an encrypted content key. The generated encrypted content key is output to the control unit 107 (step S172).

[0164] The control unit 107 receives the encrypted content key from the encryption processing unit 109 and writes the received encrypted content key and the generated content ID to the content file (step S173).

Next, the control unit 107 links the encrypted content with the encrypted content key and substitutes them into a hash function to calculate a hash value (step S174). The calculated hash value is written into the added content information (step S176).

[0165] In parallel with step S164 to step S168, the control unit 107 executes step S181 to step S189. First, the control unit 107 monitors the free space in the information storage unit 110 (step S181).

When it is determined that there is sufficient free space (YES in step S181) and the user does not press the stop button (NO in step S182), the process returns to step S181, and the free space continues to be monitored. When the user presses the stop button (YES in step S182), the control unit 107 moves the process to step S171.

[0166] When it is determined that there is insufficient free space (NO in step S181), the control unit 107 selects content information included in the content management table 121 stored in the secure storage unit 113, starting from the top (step S184). At this time, when the processing of step S187 to step S189 has been completed for all content information included in the content management table 121, that is, when there is no deletable content in information storage unit 110 (YES in step S186), the control unit 107 notifies the user that there is insufficient storage capacity by, for example, making a lamp blink, and moves the process to step S171.

[0167] When the answer is NO in step S186, the control unit 107 reads the priority level included in the selected content information and determines whether the read priority level is "2" (step S187). When the priority level is not "2" (NO in step S187), the process returns to step S184, and the next content information is selected.

When the priority level is "2" (YES in step S187), a content file corresponding to the selected content information is detected in information storage unit 110 based on the content ID contained in the selected content information, and the detected content file is deleted from information storage unit 110 (step S188). Next, the selected content information is deleted from the content management table 121 (step S189), and the process returns to step S181.

[0168] (3) Operation of HD recorder 100 during playback

Operation of the HD recorder 100 during playback will be described below with reference to the flowchart illustrated in FIG. 15. This is step S129 in FIG. 12 in detail.

When a user selects the playback list display button 182 on the menu screen 181 illustrated in FIG. 6, the control unit 107 generates a playback list screen 211 as illustrated in FIG. 6(b) and displays the generated playback list screen 211 on the monitor 120 (step S201).

[0169] Next, selection of content by the user is accepted via the input unit 103 (step S202). In the following description, a case in which the user selects the content button 212 will be described.

The control unit 107 reads the content ID "A001" contained in content information 122 corresponding to the selected content button 212 from the secure storage unit 113 (step S203), and based on the read content ID "A001," detects a content file 134 corresponding to the content information 122 on the information storage unit 110 (step S204). The encrypted content 137 and the encrypted content key 138 "Enc(Key_A, Key_1a)" are read from the detected content file 134 (step S205). The read encrypted content 137 and the encrypted content key 138 "Enc(Key_A, Key_1a)" are linked and substituted into a hash function, and a hash value is calculated (step S206).

[0170] Next, the control unit 107 reads the hash value "Ola" from the content information 122 that includes the content ID "A001" (step S207). The calculated hash value is compared to the read hash value (step S208), and when the two do not match (NO in step S208), an error screen indicating that the selected content cannot be played back is generated, the generated error screen is displayed (step S209), and the playback process is terminated.

[0171] When the calculated hash value matches the read hash value (YES in step S208), the control unit 107 reads the device-unique key 116 "Key_A" from the unique information storage unit 108, outputs the encrypted content key 138 "Enc(Key_A, Key_1a)" and the read device-unique key 116 "Key_A" to the encryption processing unit 109, and instructs to decrypt the encrypted content key 138 "Enc(Key_A, Key_1a)."

[0172] The encryption processing unit 109 receives the encrypted content key "Enc(Key_A, Key_1a)" and the device-unique key 116 "Key_A" from the control unit 107. The received device-unique key 116 "Key_A" is used to decrypt the encrypted content key "Enc(Key_A, Key_1a)" to generate a content key "Key_1a," and the generated content key "Key_1a" is output to the control unit 107 (step S211).

[0173] The control unit 107 receives the content key "Key_1a" from the encryption processing unit 109. Upon receiving the content key "Key_1a," the encrypted content 137 is read from the content file 134 (step S212), the read encrypted content 137 and the content key "Key_1a" are output to the encryption processing unit 109, and decryption of the encrypted content is instructed.

[0174] In accordance with the instruction from the control unit 107, the encryption processing unit 109 decrypts the encrypted content using the content key "Key_1a," generates content, and outputs the generated content to the control unit 107 (step S213).

The control unit 107 receives the content from the encryption processing unit 109 and outputs the received content to the playback control unit 104. The playback control unit 104 receives the content from the control unit 107, decompresses the received content to generate image and audio signals (step S214), and outputs the generated image and audio signals to the monitor 120, and the monitor 120 plays back the image and audio (step S216).

[0175] (4) Restore processing by HD recorder 100 and backup device 500

Restore processing by the HD recorder 100 and the backup device 500 will be described with reference to the flowcharts illustrated in FIGS. 16 and 17. This is step S131 in FIG. 12 in detail.

When the user selects the restore button 183 on the menu screen 181 illustrated in FIG. 6, the control unit 107 transmits a startup instruction to the backup device 500 via the transmitting and receiving unit 101 (step S231).

[0176] The control unit 507 of the backup device 500 receives the startup instruction via the transmitting and receiving unit 501 and instructs the power source unit 503 to start supplying power. The power source unit 503 starts supplying power to each unit constituting the backup device 500 (step S232).

Next, the control unit 507 transmits a startup notification to the HD recorder 100 via the transmitting and receiving unit 501 (step S233).

[0177] When the control unit 107 of the HD recorder 100 does not receive a startup notification from the backup device 500 within a specified time period via the transmitting and receiving unit 101 (NO in step S234), it generates an error screen indicating that restoration is not possible and displays the error screen generated via the playback control unit 104 on the monitor 120 (step S236).

When startup notification is received within the predetermined time (YES in step S234), the authentication unit 102 is instructed to perform equipment authentication with the backup device 500. In response to the instruction from the control unit 107, the authentication unit 102 performs equipment authentication with the backup device 500 (step S237).

[0178] When the equipment authentication by the authentication unit 102 has failed (NO in step

S239), the control unit 107 moves the process to step S236.

When the equipment authentication is successful (YES in step S239), the device identifier 115 "ID_A" is read from the unique information storage unit 108 (step S241), and the read device identifier 115 "ID_A" and a restore information request are sent to the backup device 500 via the transmitting and receiving unit 101 (step S244).

[0179] When equipment authentication with the HD recorder 100 has failed (NO in step S242), the control unit 507 of the backup device 500 instructs the power source unit 503 to stop supplying power, and the power source unit 503 stops supplying power to each unit other than the transmitting and receiving unit 501 and the control unit 507 (step S243).

When equipment authentication with HD recorder 100 is successful (YES in step S242), then a restore information request and device identifier "ID_A" are received from HD recorder 100 via the transmitting and receiving unit 501. It is determined whether the received device identifier "ID_A" is registered in the permitted device identification information 551 stored in the secure information storage unit 511 (step S246). When it is determined that such is not registered (NO in step S246), the control unit 507 moves the process to step S263.

[0180] When it is determined that such has been registered (YES in step S246), the content ID, title, and recording date and time are read from each piece of backup information constituting the backup management table 521 (step S247), and the read content ID, title, and recording date and time are transmitted to the HD recorder 100 via the transmitting and receiving unit 501 (step S248).

The control unit 107 of the HD recorder 100 receives the content ID, the title, and the recording date and time from the backup device 500 via the transmitting and receiving unit 101. The restore information screen 221 illustrated in FIG. 7 is generated using the received title and recording date and time (step S251), and the generated restore information screen 221 is displayed on the monitor 120 via the playback control unit 104 (step S252).

[0181] When the control unit 107 receives the selection of the content to be restored by the user via the input unit 103 (step S253).

The control unit 107 reads the content ID corresponding to the selected content button (step S254) and transmits the read content ID and a restore request to the backup device 500 via the

transmitting and receiving unit 101 (step S256).

[0182] The control unit 507 constituting the backup device 500 receives the restore request and the content ID via the transmitting and receiving unit 501. When the restore request is received, the control unit 507 selects backup information including the received content ID from the backup management table 521 stored in the secure information storage unit 511 (step S257).

Next, the control unit 507 detects a content file corresponding to the selected backup information in the content storage unit 510 based on the received content ID and reads the encrypted content and encrypted content key contained in the detected content file (step S259). The control unit 507 links the read encrypted content and the encrypted content key and substitutes them into a hash function to calculate a hash value (step S260).

[0183] Next, the hash value contained in the selected backup information (step S261) is read, the calculated hash value is compared to the read hash value, and when the two do not match (NO in step S262), the control unit 507 generates an error notification indicating that the restore request for the content corresponding to the received content ID cannot be accepted and transmits the generated error notification to the HD recorder 100 via the transmitting and receiving unit 501 (step S263). When the error notification is received, the control unit 107 of the HD recorder 100 displays an error screen on the monitor to notify the user that restoration is not possible and ends the restore processing.

[0184] Next, the control unit 507 instructs the power source unit 503 to stop supplying power. The power source unit 503 receives the instruction from the control unit 507 and stops supplying power to each unit other than the transmitting and receiving unit 501 and the control unit 507 (step S264).

When it is determined that the calculated hash value and the read hash value match (YES in step S262), the control unit 507 reads the device-unique key 516 "Key_C" from the unique information storage unit 504 (step S266), outputs the read device-unique key 516 "Key_C" and the encrypted content key to the encryption processing unit 509, and instructs to decrypt the encrypted content key. The encryption processing unit 509 decrypts the encrypted content key and generates the content key using the device-unique key 516 "Key_C" at the instruction of the control unit 507, and outputs the generated content key to the control unit 507 (step S267).

[0185] The control unit 507 receives the content key from the encryption processing unit 509 and

then reads the encrypted content included in the detected content file (step S268).

Next, the control unit 507 acquires the current time from the secure clock, adds the viewing time "240 hours" to the acquired current time, and calculates the expiration date (step S269). The encrypted content read to the HD recorder 100, the received content key, and the calculated expiration date are transmitted via the transmitting and receiving unit 501 (step S271). Once such is transmitted, the control unit 507 instructs the power source unit 503 to stop power supply, and the power source unit 503 receives the instruction from the control unit 507 and stops supplying power to each unit other than the transmitting and receiving unit 501 and the control unit 507 (step S272).

[0186] The control unit 107 of the HD recorder 100 receives the encrypted content, the content key, and the expiration date from the backup device 500 via the transmitting and receiving unit 101. When the encrypted content, the content key, and the expiration date are received, a new content file is generated on the information storage unit 110, and the received encrypted content and the content ID are written to the generated content file (step S274).

[0187] Next, the device-unique key 116 "Key_A" is read from the unique information storage unit 108 (step S276), the read device-unique key 116 "Key_A" and the received content key are output to the encryption processing unit 109, and encryption of the content key is instructed. The encryption processing unit 109 receives the device-unique key 116 "Key_A" and the content key from the control unit 107. The content key is encrypted using the received device-unique key "Key_A," the encrypted content key is generated, and the generated encrypted content key is output to the control unit 107 (step S277).

[0188] The control unit 107 receives the encrypted content key from the encryption processing unit 109 and writes the received encrypted content key to the content file generated on the information storage unit 110 (step S278).

Next, the control unit 107 links the received encrypted content with the received encrypted content key, substitutes them to a hash function, and calculates a hash value (step S279).

[0189] The control unit 107 adds content information including the content ID corresponding to the selected content button, the title, the recording date and time, the received expiration date, and the calculated hash value to the content management table 121 (step S281). A "1" is written to the backup flag of the added content information (step S284), and a priority level of "2" is written

(step S286).

[0190] (5) Backup processing by HD recorder 100 and backup device 500

Backup processing by the HD recorder 100 and the backup device 500 will be described with reference to the flowcharts illustrated in FIGS. 18 to 20. This is step S114 in FIG. 12 in detail.

When the current time indicated by the secure clock 117 reaches "Sunday 12:30 am" set as the backup schedule by the user, the control unit 107 selects each piece of content information constituting the content management table 121 stored in the secure storage unit 113 one by one in order (step S301). At this time, when all content information has been selected and there is no new content information to be selected (YES in step S302), the backup process ends. When all content information has not been selected (NO in step S302), the control unit 107 determines whether the backup flag included in the selected content information is "0," that is, whether the content corresponding to the selected content information has already been backed up (step S303). When the backup flag is not "0" (NO in step S303), the process returns to step S301 and the next content information is selected.

[0191] When the backup flag is "0" (YES in step S303), the control unit 107 reads the content ID from the selected content information (step S304), and detects the content file corresponding to the selected content information based on the read content ID (step S306). The encrypted content and the encrypted content key from the detected content file are read from the information storage unit 110 (step S307).

[0192] The control unit 107 links the read encrypted content and the encrypted content key and substitutes them into a hash function to calculate a hash value (step S308). Next, the hash value included in the selected content information is read (step S309), and the read hash value is compared to the calculated hash value (step S311). When the two do not match, the process returns to step S301 and moves to the process of the next content information.

[0193] When the read hash value matches the calculated hash value, the control unit 107 transmits a startup instruction to the backup device 500 via the transmitting and receiving unit 101 (step S313).

The control unit 507 of the backup device 500 receives the startup instruction from the HD recorder 100 via the transmitting and receiving unit 501 and instructs the power source unit 503 to start supplying power. The power source unit 503 starts supplying power to each unit constituting the backup device 500 under the instruction of the control unit 507 (step S316).

[0194] The control unit 507 transmits a startup notification to the HD recorder 100 via the transmitting and receiving unit 501 (step S317).

When the control unit 107 of the HD recorder 100 does not receive the startup notification from the backup device 500 within a predetermined time (NO in step S318), the control unit 107 ends the backup processing.

When the startup notification is received within the predetermined time via the transmitting and receiving unit 101 (YES in step S318), the control unit 107 instructs the authentication unit 102 to perform equipment authentication with the backup device 500.

[0195] The authentication unit 102 performs equipment authentication with the backup device 500 at the instruction of the control unit 107 (step S321). When the equipment authentication by the authentication unit 102 has failed (NO in step S322), the control unit 107 ends the backup process.

When the equipment authentication is successful (YES in step S322), the control unit 107 reads the device-unique key 116 "Key_A" from the unique information storage unit 108, outputs the read device-unique key 116 "Key_A" and the encrypted content key included in the selected content information to the encryption processing unit 109, and instructs to decrypt the encrypted content key. The encryption processing unit 109 receives an instruction from the control unit 107 and decrypts the encrypted content key and generates the content key using the received device-unique key 116 "Key_A," and outputs the generated content key to the control unit 107 (step S323).

[0196] The control unit 107 receives the content key from the encryption processing unit 109. When the content key is received, the content ID, title, and recording date and time included in the selected content information are read (step S324).

Next, the control unit 107 reads the device identifier 115 "ID_A" from the unique information storage unit 108 and reads the encrypted content corresponding to the selected content information from the information storage unit 110 (step S326). The backup request, the read device identifier 115 "ID_A," the content ID, the title, the recording date and time, the encrypted content, and the received content key are transmitted to the backup device 500 via the

transmitting and receiving unit 101 (step S327).

[0197] When the equipment authentication with the HD recorder 100 has failed (NO in step S328), the control unit 507 instructs the power source unit 503 to stop supplying power, and the power source unit 503 stops supplying power to each unit other than the transmitting and receiving unit 501 and the control unit 507 (step S329).

When the equipment authentication is successful (YES in step S328), the control unit 507 receives the backup request, the device identifier "ID_A," the content ID, the title, the recording date and time, the encrypted content, and the content key from the HD recorder 100 via the transmitting and receiving unit 101. It is determined whether the received device identifier "ID_A" is registered in the permitted device identification information 551 stored in the secure information storage unit 511 (step S331). When it is determined that the backup request is not registered (NO in step S331), the control unit 507 transmits an error notification to the HD recorder 100 via the transmitting and receiving unit 501, indicating that the backup request cannot be accepted (step S332), and stops supplying power to each circuit constituting the backup device 500 via the power source unit 503 (step S333). Then, the HD recorder 100, having received the error notification, ends the backup processing.

[0198] When it is determined that the received device identifier "ID_A" is registered in the permitted device identification information 551 (YES in step S331), the device-unique key 516 "Key_C" is read from the unique information storage unit 504, the read device-unique key 516 "Key_C" and the received content key are output to the encryption processing unit 509, and an instruction is given to encrypt the content key. The encryption processing unit 509 encrypts the content key and generates the encrypted content key using the received device-unique key 516 "Key_C" in accordance with the instructions of the control unit 507 and outputs the generated encrypted content key to the control unit 507 (step S336).

[0199] The control unit 507 receives the encrypted content key from the encryption processing unit 509. Upon receiving the encrypted content key, a new content file is generated on the content storage unit 510, and the received content ID, the encrypted content, and the encrypted content key received from the encryption processing unit 509 are written to the generated content file (step S337).

Next, the control unit 507 links the received encrypted content with the received encrypted content key, substitutes them to a hash function, and calculates a hash value (step 339). Backup information including the received content ID, title, recording date and time, device identifier

"ID_A," and calculated hash value is generated, and the generated backup information is added to the backup management table 521 (step S341). In this case, the received device identifier "ID_A" is set to the backup source device identifier.

[0200] The control unit 507 obtains the current time from the secure clock, adds the viewing time of "240 hours" to the obtained current time to calculate the expiration date (step S342), and transmits the calculated expiration date to the HD recorder 100 via the transmitting and receiving unit 501 (step S343). When the transmission is completed, power supply to each circuit constituting the backup device 500 is stopped via the power source unit 503 (step S344).

[0201] The control unit 107 of the HD recorder 100 receives the expiration date from the backup device 500 via the transmitting and receiving unit 101 and writes the received expiration date into the selected content information (step S346).

Next, the control unit 107 changes the backup flag of the selected content information to "1" (step S347), changes the priority level to "2" (step S348), and returns to step S301.

[0202] (6) HD Recorder 100 expiration date extension operation

An operation of extending the expiration date by the HD recorder 100 will be described using the flowchart of FIG. 21. This is step S112 in FIG. 12 in detail.

When the time indicated by secure clock 117 reaches the extension time of "2:00" set in advance, the main control unit 118 constituting the control unit 107 outputs an instruction to expiration date management unit 119 to extend the expiration date.

[0203] The expiration date management unit 119 receives the expiration date extension instruction and selects each piece of content information constituting content management table 121 stored in the secure storage unit 113 one by one in order (step S361). At this time, when all content information has been selected and there is no content information to be newly selected (YES in step S362), the process of extending the expiration date is terminated.

[0204] When selection of all content information has not been completed (NO in step S362), the expiration date management unit 119 reads the expiration date from the selected content information (step S363). In this case, when no expiration date is written in the selected content information (NO in step S366), the process returns to step S361 and the next content information is selected.

When an expiration date is written in the selected content information (YES in step S366), expiration date management unit 119 then obtains the current time from secure clock 117 (step S367), and calculates the difference between the read expiration date and the obtained current time to calculate the remaining time (step S368). The expiration date management unit 119 compares the calculated remaining time to the extension execution time "24 hours," and upon determining that the remaining time is 24 hours or more (NO in step S371), returns to step S361, and moves to the process of the next content information.

[0205] When it is determined that the calculated remaining time is less than 24 hours (YES in step S371), the expiration date management unit 119 transmits a startup instruction to the backup device 500 via the transmitting and receiving unit 101 (step S372).

The control unit 507 of the backup device 500 receives the startup instruction via the transmitting and receiving unit 501 and instructs the power source unit 503 to start supplying power. The power source unit 503 starts supplying power to each unit constituting the backup device 500 (step S373).

[0206] Next, the control unit 507 transmits a startup notification to the HD recorder 100 via the transmitting and receiving unit 501 (step S374).

When the expiration date management unit 119 of the HD recorder 100 does not receive the startup notification from the backup device 500 within the predetermined time via the transmitting and receiving unit 101 (NO in step S376), the process returns to step S361.

[0207] When the startup notification is received within the predetermined time (YES in step S376), the expiration date management unit 119 instructs the authentication unit 102 to perform equipment authentication with the backup device 500. The authentication unit 102 performs equipment authentication with the backup device 500 at the instruction of the expiration date management unit 119 constituting the control unit 107 (step S381).

When the equipment authentication by the authentication unit 102 has failed (NO in step S382), the expiration date management unit 119 returns to step S361.

[0208] When the equipment authentication is successful (YES in step S382), the expiration date management unit 119 reads the device identifier 115 "ID_A" from the unique information storage unit 108 and reads the content ID from the selected content information (step S383).

Next, the expiration date management unit 119 transmits the extension request, the read device identifier 115 "ID_A" and the content ID to the backup device 500 via the transmitting and

receiving unit 101 (step S386).

[0209] When the equipment authentication with the HD recorder 100 has failed (NO in step S389), the control unit 507 of the backup device 500 instructs the power source unit 503 to stop supplying power, and the power source unit 503 stops supplying power to each unit other than the transmitting and receiving unit 501 and the control unit 507 (step S391).

When the equipment authentication with the HD recorder 100 is successful (YES in step S389), the control unit 507 receives the extension request, the device identifier "ID_A," and the content ID via the transmitting and receiving unit 501.

[0210] Next, the control unit 507 determines whether the received device identifier "ID_A" is included in the permitted device identification information 551 stored in the secure information storage unit 511 (step S392). When it is determined that such is not included (NO in step S392), the control unit 507 transmits an error notification to the HD recorder 100 via the transmitting and receiving unit 501 (step S393), and instructs the power source unit 503 to stop supplying power. The power source unit 503 stops supplying power to each unit other than the transmitting and receiving unit 501 and the control unit 507 (step S394). When the error notification is received, the expiration date management unit 119 of the HD recorder 100 moves the process to step S361.

[0211] In step S392, when it is determined that the received device identifier "ID_A" is included in the permitted device identification information 551 (YES in step S392), the control unit 507 selects backup information including the received content ID from the backup management table 521 stored in the secure information storage unit 511 (step S396).

Next, based on the received content ID, the control unit 507 detects a content file corresponding to the selected content information, reads the encrypted content and the encrypted content key from the detected content file (step S397), links the read encrypted content and encrypted content key, and substitutes them into a hash function to calculate a hash value (step S398).

[0212] Next, the control unit 507 reads the hash value included in the selected backup information (step S401) and compares the read hash value to the calculated hash value (step S402). When the two do not match (NO in step S402), the control unit 507 transmits an error notification to the HD recorder 100 via the transmitting and receiving unit 501 (step S403) and instructs the power source unit 503 to stop supplying power. The power source unit 503 stops supplying

power to each unit other than the transmitting and receiving unit 501 and the control unit 507 (step S404). When the error notification is received, the expiration date management unit 119 of the HD recorder 100 moves the process to step S361.

[0213] When the read hash value matches the calculated hash value (YES in step S402), the control unit 507 obtains the current time from the secure clock and adds the viewing time "240 hours" to the obtained current time to calculate the expiration date (step S406).

Next, the control unit 507 transmits the calculated expiration date to the HD recorder 100 via the transmitting and receiving unit 501 (step S407). Once the expiration date is transmitted, the control unit 507 instructs the power source unit 503 to stop supplying power. The power source unit 503 stops supplying power to each unit other than the transmitting and receiving unit 501 and the control unit 507 (step S408).

[0214] The expiration date management unit 119 receives the expiration date from the backup device 500 via the transmitting and receiving unit 101. The expiration date included in the selected content information is updated based on the received expiration date (step S411), and the process moves to step S361.

(7) Equipment authentication

An operation of equipment authentication between the HD recorder 100 and the backup device 500 will be described with reference to FIG. 24 and FIG. 25.

[0215] Note that this equipment authentication method is one example, and other authentication methods and key sharing methods may also be used. *In this case*, Gen() is a key generation function and Y is a system-unique parameter. The key generation function Gen() satisfies a relationship $\text{Gen}(x, \text{Gen}(z, Y)) = \text{Gen}(z, \text{Gen}(x, Y))$. The key generation function may be implemented by any known technique and will not be described in detail here.

[0216] The authentication unit 102 of the HD recorder 100 reads the public key certificate Cert_A (step S501), and transmits the read public key certificate Cert_A to the backup device 500 via the transmitting and receiving unit 101 (step S502).

The authentication unit 502 of the backup device 500, having received the public key certificate Cert_A, uses the public key PK_CA of the certification authority to perform a signature verification algorithm V on a received signature data Sig_CA of the certification authority included in the public key certificate Cert_A to verify the signature (step S503). In this case, the signature verification algorithm V is an algorithm for verifying signature data generated

by the signature generation algorithm S. When the signature verification has failed (NO in step S504), the process ends.

[0217] When the signature verification is successful (YES in step S504), the authentication unit 502 reads the CRL (step S505) and determines whether the received certificate identification number ID_a included in the public key certificate Cert_A is registered in a read CRL (step S506). When it is determined that such has been registered (YES in step S506), the process ends.

When it is determined that such is not registered (NO in step S506), the authentication unit 502 reads the public key certificate Cert_C (step S507) and transmits the read public key certificate Cert_C to the HD recorder 100 (step S508).

[0218] The authentication unit 102 of the HD recorder 100, having received the public key certificate Cert_C, uses the public key PK_CA of the certification authority to apply the signature verification algorithm V to the received signature data Sig_CA of the certification authority included in the public key certificate Cert_C (step S509). When the result of signature verification is a failure (NO in step S510), the process ends.

When the result of signature verification is successful (YES in step S510), the authentication unit 102 reads the CRL (step S511) and determines whether the received certificate identification number ID_b included in the public key certificate Cert_C is registered in the read CRL (step S512). When it is determined that such is registered (YES in step S512), the process ends. When it is determined that such is not registered (NO in step S512), the process continues.

[0219] The authentication unit 502 of the backup device 500 generates a random number Cha_C (step S513) and transmits the generated random number Cha_C to the HD recorder 100 (step S514).

The authentication unit 102 of the HD recorder 100 receives the random number Cha_C, uses the private key SK_A of the HD recorder 100 to apply the signature generation algorithm S to the received random number Cha_C to generate signature data Sig_A (step S515), and transmits the generated signature data Sig_A to the backup device 500 (step S516).

[0220] Upon receiving the signature data Sig_A, the authentication unit 502 of the backup device 500 verifies the signature by using the public key PK_A of the HD recorder 100 to apply the signature verification algorithm V to the received signature data Sig_A included in the public key certificate Cert_A (step S517). When the result of signature verification is determined to be

a failure (NO in step S518), the process ends. When the result of signature verification is determined to be a success (YES in step S518), the process continues.

[0221] The authentication unit 102 of the HD recorder 100 generates a random number Cha_A (step S519) and transmits the generated random number Cha_A to the backup device 500 (step S520).

The backup device 500 receives the random number Cha_A, applies the signature generation algorithm S to the received random number Cha_A using the secret key S K_B of the backup device 500 to generate the signature data Sig_C (step S521), and transmits the generated signature data Sig_C to the HD recorder 100 (step S522).

[0222] When the HD recorder 100 receives the signature data Sig_C, the received signature data Sig_C is verified by using the public key PK_B of the backup device 500 to apply the signature verification algorithm V to the received signature data Sig_C included in the public key certificate Cert_C (step S523). When the result of signature verification is determined to be a failure (NO in step S524), the process ends. When the result of signature verification is determined to be a success (YES in step S524), the authentication unit 102 then generates a random number "a" (step S525), generates the Key_a = Gen(a, Y) using the generated random number "a" (step S526), and transmits the generated Key_a to the backup device 500 (step S527).

[0223] Upon receiving the Key_a, the authentication unit 502 of the backup device 500 generates a random number "c" (step S528), uses the generated random number "c" to generate the Key_c = Gen(c, Y) (step S529), and transmits the generated Key_c to the HD recorder 100 (step S530).

Also, using the generated random number "c" and the received Key_a, Key_ac = Gen(c, Key_A) = Gen(c, Gen(a, Y)) is generated and used as the session key (step S531).

[0224] The HD recorder 100 receives Key_c, and generates Key_ac = Gen(a, Key_c) = Gen(a, Gen(c, Y)) from the generated random number "a" and the received Key_c and uses this as the session key (step S532).

1.5 Summary and Effect

As described above, in the backup system 1 of the present invention, the HD recorder 100 transmits encrypted content stored in the information storage unit 110 to the backup device 500 to request backup, and the backup device 500 backs up the received encrypted content. At this

time, an expiration date is set for the encrypted content stored in HD recorder 100, which is the sender of the encrypted content. The HD recorder 100 requests an extension of the expiration date from the backup device 500 before the expiration date.

[0225] When the expiration date cannot be extended due to a reason such as an inability to communicate with the backup device 500 and the expiration date passes, the HD recorder 100 deletes the encrypted content whose expiration date has passed from the information storage unit 110.

After being deleted, the encrypted content stored in the backup device 500 can be acquired by a user operation or the like.

[0226] The backup device 500 stores permitted device identification information in advance and accepts backup requests, extension requests, and restore requests from devices having device identifiers registered in the permitted device identification information.

In this way, even after the backup device 500 backs up the encrypted content, the HD recorder 100 stores the encrypted content until the expiration date, and thus the user can view the content by a simple operation.

[0227] Furthermore, when the expiration date has passed, the HD recorder 100 deletes the stored encrypted content, thereby preventing copies of the encrypted content from existing indefinitely, and protecting the rights of the copyright holder of the content.

In the backup system 1 of the present invention, the backup device 500 also stores content that the HD recorder 400 requests be backed up. The HD recorder 100 can also obtain and play back the backed up content in response to an instruction from the HD recorder 400, thereby making it possible to further improve convenience for the user.

[0228] Furthermore, the backup device 500 receives a startup instruction from the HD recorder 100 and supplies power to each component of the backup device 500 only while various processes are being performed. Therefore, the operating time of the hard disk unit constituting the content storage unit 510 can be minimized, and the risk of failure of the hard disk unit can be reduced.

2. Modifications

Note that the present invention has been described based on the foregoing embodiment, but it goes without saying that the present invention is not limited to the foregoing embodiment. The

following cases are also included in the present invention.

[0229] (1) In embodiment 1, the expiration date management unit 119 deletes content files including encrypted content whose expiration date has passed from the information storage unit 110, but it is also possible to delete only the encrypted content key.

In this case, the expiration date management unit 119 deletes only the encrypted content key from the information storage unit 110 and deletes the hash value and expiration date included in the corresponding content information.

[0230] While the playback list screen 211 is displayed on the monitor, when a hash value is not present in the content information corresponding to a content button selected by a user's button operation, the main control unit 118 reads the content ID included in the content information and transmits a content key request and the read content ID to the backup device 500 via the transmitting and receiving unit 101.

[0231] The backup device 500 receives the content key request and transmits the corresponding content key and expiration date to the HD recorder 100.

The main control unit 118 of the HD recorder 100 receives the content key and the expiration date and instructs the encryption processing unit 109 to generate an encrypted content key and write the generated encrypted content key to the information storage unit 110. Next, the encrypted content included in the content file corresponding to the content information corresponding to the selected content button is read from the information storage unit 110, a hash value is generated based on the read encrypted content and the generated encrypted content key, and the generated hash value and the received expiration date are written into the content information. Then, the encrypted content is decrypted and played back in the same manner as in the foregoing generation process.

(2) In the foregoing modification (1), the hash value and the expiration date of the content information for which the expiration date could not be updated may be all that is deleted.

[0232] In this case, the main control unit 118 transmits a request for the expiration date to the backup device 500 instead of a request for the content key. Only when the expiration date has been received from the backup device 500, the received expiration date is written into the content information, and a hash value is calculated again from the encrypted content and encrypted content key corresponding to the content information.

(3) In the foregoing embodiment 1, the backup device 500 calculates the expiration date and

transmits the calculated expiration date to the HD recorder 100, but the expiration date may be calculated by the HD recorder 100.

[0233] For example, in backup processing, the backup device 500 transmits a completion notification indicating that the backup has been completed normally to the HD recorder 100, instead of transmitting the expiration date.

Upon receiving the completion notification, the main control unit 118 of the HD recorder 100 acquires the current time from the secure clock 117, adds the viewing time "240 hours" to the acquired current time, and calculates the expiration date.

[0234] Also, in the process of extending the expiration date, the backup device 500 transmits an extension permission indicating that the expiration date can be extended to the HD recorder 100, instead of the expiration date itself.

When the extension permission is received, the expiration date management unit 119 of the HD recorder 100 acquires the current time from the secure clock 117, adds the viewing time "240 hours" to the acquired current time, and calculates the expiration date.

[0235] Alternatively, instead of the current time, the viewing time "240 hours" may be added to the expiration date included in each piece of content information, and the result of the addition may be used as the new expiration date.

In such a configuration, the control unit 507 constituting the backup device 500 does not need to have a secure clock.

(4) In the foregoing embodiment, the HD recorder 100 extends the expiration date and deletes expired content based on the expiration date included in the content information for each content, but each content may be managed based on the start date and time of the period during which playback of the encrypted content is permitted and the period for which playback is permitted.

[0236] In this case, each piece of content information constituting content management table 121 includes, instead of an expiration date, a start date and time of a period during which playback of the content is permitted.

The main control unit 118 stores the period during which playback of the content is permitted, which is "240 hours." In the backup process, the backup device 500 transmits a backup completion notification, instead of an expiration date, indicating that the content has been successfully backed up.

[0237] The main control unit 118 receives the backup completion notification from backup device

500 via the transmitting and receiving unit 101, obtains the current time from secure clock 117, and writes the obtained current time as the start date and time in the content information.

In the process of extending the expiration date, the expiration date management unit 119 acquires the current time from the secure clock 117 and, when the time elapsed since the start date and time is 216 hours or more, transmits an extension request to the backup device 500.

[0238] In the deletion process, the expiration date management unit 119 obtains the current time from the secure clock 117 and, when the elapsed time from the start date and time is 240 hours or more, deletes the corresponding content file from the information storage unit 110 and deletes the content information.

In such a configuration, the control unit 507 constituting the backup device 500 does not need to have a secure clock.

(5) In the foregoing embodiment 1 and variations thereof, the HD recorder 100 transmits an extension request to the backup device 500 when there is less than 24 hours left until the expiration date of each encrypted content, but may be configured to transmit the extension request periodically regardless of the time remaining until the expiration date.

(6) Content may also be managed based on a number of viewings, instead of the expiration date.

[0239] For example, each piece of content information in the content management table 121 includes the available number of viewings instead of the expiration date. Each time a content is played back, the control unit 107 subtracts 1 from the available number of viewings included in the content information corresponding to the content played back.

In the backup process and the expiration date extension process, the backup device 500 transmits the number of viewings "3" instead of the expiration date. The control unit 107 of the HD recorder 100 sets the received number of viewings "3" as a available number of viewings.

[0240] Also, the HD recorder 100 deletes content information having a available number of viewings of "0" and the content file corresponding to this content information.

(7) In embodiment 1, the backup device 500 stores the permitted device identification information 551 in advance and accepts a restore request from equipment having a device identifier registered in the permitted device identification information 551, but may determine whether to accept a restore request depending on the number of pieces of copied content.

[0241] For ease of description, the encrypted content stored in the backup device 500 is referred to

simply as "content," and encrypted content stored in playback equipment such as the HD recorder 100 is referred to as copied content. In addition to the HD recorders 100 and 400, other equipment having content storage and playback functions is also connected to the backup system 1.

[0242] Specifically, the control unit 507 of the backup device 500 stores, for each piece of content, the permitted copy number "3," which is the number of pieces of copy content that are permitted to exist. Furthermore, each piece of backup information constituting the backup management table 521 stored in the secure information storage unit 511 includes a copy number indicating the number of pieces of copy content that currently exist.

The secure information storage unit 511 further stores a plurality of copy management tables. Each copy management table is composed of a plurality of pieces of copy information, and each piece of copy information is composed of a content ID, a device identifier, and an expiration date. The content ID is the same as any of the content IDs included in the backup management table 521. The device identifier is information for identifying external equipment that has the copy content indicated by the content ID. The expiration date is the expiration date of the copied content of external equipment indicated by the device identifier.

[0243] (7-a) Backup processing

In the backup processing described in embodiment 1, upon receiving a backup request from the HD recorder 100, the control unit 507 writes the content, adds backup information, calculates the expiration date, and so on, as described in embodiment 1. At this time, "1" is written as the copy number of the added backup information.

[0244] Next, the control unit 507 generates copy information composed of the received content ID, the received device identifier, and the calculated expiration date, and adds the generated copy information to the copy management table. After the copy information is added, the calculated expiration date is sent to the HD recorder 100.

(7-b) Copy deletion

As already described, in control of the recording process by the main control unit 118 of the HD recorder 100, when the free space in the information storage unit 110 is insufficient while recording new content, the main control unit 118 deletes encrypted content corresponding to content information including the priority level "2" from the information storage unit 110.

[0245] At this time, the main control unit 118 transmits a copy deletion notification indicating the

deletion of the copied content, the content ID corresponding to the copied content to be deleted, and the device identifier "ID_A" of the HD recorder 100 itself to the backup device 500 .

The control unit 507 of the backup device 500 receives the copy deletion notification, the content ID, and the device identifier "ID_A" from the HD recorder 100. When the copy deletion notification is received, the copy information including the received content ID and device identifier "ID_A" is deleted, and the copy number of the backup information including the received content ID is decremented by one.

[0246] (7-c) Restore processing

In the restore process described above, upon receiving a restoration request from external equipment, the control unit 507 of the backup device 500 reads the copy number from the backup information including the content ID received together with the restoration request. When the read copy number is a permitted copy number "3," an error notification is sent to the HD recorder 100 indicating that the restore request cannot be accepted.

[0247] When the read copy number is less than the permitted copy number "3," the control unit 507 performs the procedures described in embodiment 1, such as verifying the hash value, generating the content key, and calculating the expiration date. After calculating the expiration date, the copy number included in the backup information including the received content ID in the backup management table 521 is incremented by one. Next, the control unit 507 generates copy information composed of the received content ID, the device identifier, and the calculated expiration date and adds the generated copy information to the copy management table.

[0248] Next, the content, the content key, and the expiration date are transmitted to the external equipment.

(7-d) Verification of expiration date by backup device 500

In the process of extending the expiration date, the control unit 507 selects copy information that includes the received content ID and device identifier and rewrites the expiration date of the selected copy information using the newly calculated expiration date.

[0249] The control unit 507 stores a verification time at which the expiration date included in each copy information is verified. When the verification time arrives, the control unit 507 selects one piece of copy information constituting the copy management table, reads the expiration date included in the selected copy information, and compares the read expiration date to the current time. When the current time has passed the expiration date, the copy number of the backup information that contains the content ID included in the selected copy information is

decremented by one. Next, the control unit 507 deletes the selected content information.

[0250] When the current time has not passed the expiration date, the copy number is not decremented, and the copy information is not deleted.

The control unit 507 verifies the expiration date for all backup information by a similar procedure.

(8) In modification (7), the backup device 500 stores the permitted copy number in advance, but the permitted copy number may be included in the broadcast content.

[0251] For example, the permitted copy number is included in specific bits of a TS packet that constitutes the content, and in the backup process, the backup device 500 decrypts one of the TS packets of the received encrypted content using the received content key to extract the permitted copy number and stores the extracted copy number in association with the received content ID.

Furthermore, in addition to the permitted copy number, information indicating whether backup generation is permitted may also be included in the content. The control unit 107 of the HD recorder 100 extracts information indicating whether backup generation is permitted from the received content and stores the extracted information (called backup information) in association with the content ID.

[0252] During backup processing, when the backup information corresponding to the encrypted content to be backed up indicates permission to generate a backup, the encrypted content is sent to backup device 500 in a procedure such as described in embodiment 1. When the backup information corresponding to the encrypted content to be backed up indicates that backup is prohibited, the transmission is stopped.

[0253] In particular, when the user starts the foregoing backup process by pressing the backup button, backup information indicating that backup is prohibited and the title of the corresponding encrypted content are displayed on the monitor 120, notifying the user that backup of the displayed content is prohibited.

Thereby, the intention of the copyright holder of the content can be reflected with regard to the generation of backup and copy content.

(9) In embodiment 1, the encrypted content and the encrypted content key are linked and substituted into the hash function to calculate the hash value, but it is also possible to substitute

in only the encrypted content key.

(10) In the foregoing embodiment and variations, a common key encryption method is adopted to encrypt the content and the content key, and the same key is used for encryption and decryption, but the present invention is not limited thereto. For example, a public key encryption method such as RSA or elliptic curve encryption may be adopted, and different keys may be used for encryption and decryption.

[0254] Specifically, when public key encryption is used to encrypt content, in the content recording process described using FIG. 13, the key generation unit 106 of the HD recorder 100 generates a pair of content encryption key and content decryption key instead of a single content key. The control unit 107 outputs the content received via the broadcast receiving unit 114 and the content encryption key generated by the key generation unit 106 to the encryption processing unit 109 and instructs such to encrypt the content. When instructed to encrypt the content, the encryption processing unit 109 uses the content encryption key to use an encryption algorithm conforming to a public key encryption method on the content to generate encrypted content. When recording is stopped by pressing the stop button or due to insufficient free space in the information storage unit 110, the encryption processing unit 109 encrypts the content decryption key using the device-unique key "Key_A" instead of the content key and generates an encrypted content key.

[0255] Afterward, the encryption processing unit 109 performs encryption and decryption processing by adopting a common key encryption method to encrypt the content decryption key and decrypt the encrypted content key, and adopting a public key encryption method to decrypt the encrypted content.

(11) In the foregoing embodiment and modifications, the backup device 500 and HD recorder 100 are connected via the LAN 30, but the present invention is not limited to this configuration. As another example, the present invention also includes a case in which the backup device is built into the HD recorder 100.

(12) The content storage unit 510 of the backup device 500 has been described as being composed of a hard disk unit but may instead be composed of a removable optical disk and an input and output unit that writes and reads information to and from the optical disk. In this case, the user inserts and removes optical disks as necessary.

[0256] Furthermore, such may also be configured to include a plurality of optical disks and a disk

changer for automatically changing them.

(13) The present invention may be a method as described above. Furthermore, these methods may be computer programs that are implemented by a computer or may be digital signals that include a computer program.

[0257] Furthermore, the present invention may also be configured such that the computer program or the digital signal is recorded on a computer-readable recording medium, such as a flexible disk, a hard disk, a CD-ROM, an MO, a DVD, a DVD-ROM, a DVD-RAM, a BD (Blu-ray Disc), a semiconductor memory, or the like. Moreover, the present invention may be applicable to the computer program or digital signal recorded on such a recording medium.

[0258] Furthermore, the present invention may involve transmitting the computer program or the digital signal via a telecommunications line, a wireless or wired communication line, a network such as the internet, data broadcasting, or the like.

The present invention may also be a computer system including a microprocessor and a memory, wherein the memory stores a computer program, and the microprocessor operates in accordance with the computer program.

[0259] The program or the digital signal may also be implemented by another independent computer system by recording on the recording medium and transferring such, by transferring the program or the digital signal via the network, or the like.

(14) All or some of the constituent elements constituting each of the foregoing devices may be configured as a single system LSI (Large Scale Integration: large scale integrated circuit). A system LSI is a highly multifunctional LSI manufactured by integrating multiple components onto a single chip, and specifically, is a computer system composed of a microprocessor, ROM, RAM, and the like. The RAM stores a computer program. The microprocessor operates according to the computer program, whereby the system LSI achieves part of its functions.

[0260] Note that in the foregoing, a system LSI is used, but depending on the degree of integration, an integrated circuit called an IC (Integrated Circuit), LSI, super LSI, or ultra LSI may also be used.

In addition, instead of a system LSI, such may be configured using an FPGA (Field Programmable Gate Array) or CPLD (Complex Programmable Logic Device; also known as a reconfigurable LSI) that can be programmed after being incorporated into a product. Furthermore, when new art is developed in the future that replaces the functions of the foregoing integrated circuits, some or all of the constituent elements constituting each device may be realized using that new art.

(15) The foregoing embodiment and foregoing modifications may be combined with each other.

Industrial Applicability

[0261] The present invention can be used commercially, continuously, and repeatedly in industries which generate, distribute, broadcast, and use digital content, and in industries which manufacture and sell various electrical equipment for generating content, distributing content, playing content, editing content, and the like.

[Scope of Patent Claims]

- [1] A backup system consisting of a recording and playback device for recording and playing back content and a backup device, wherein
- the recording and playback device comprises
 - storage means for storing the content;
 - reception means for receiving an instruction to back up the content;
 - content transmission means for,
 - upon receiving the instruction, reading the content from the storage means and transmitting the read content to the backup device;
 - writing means for,
 - upon receiving the instruction, writing period information indicating a period in which playback of the content that is subject to the backup is permitted to the storage means in association with the content;
 - and playback control means for permitting playback of the content during a period indicated by
 - the period information and
 - prohibiting playback of the content when the period indicated by the period information ends.
- [2] A recording and playback device for performing recording and playback of content,
- the recording and playback device comprising storage means for storing the content;
 - reception means for receiving an instruction to back up the content; content transmission means for, upon receiving
 - the instruction, reading the content from the storage means and transmitting the read content to the backup device if backup of the read content is permitted;
 - writing means for, upon receiving
 - the instruction, writing period information indicating a period in which playback of the content that is subject to the backup is permitted to the storage means in association with the content; and playback control means for permitting playback of the content during a period

indicated by

the period information and prohibiting playback of the content when the period indicated by the period information ends.

- [3] The recording and playback device according to claim 2, further comprising:
extension request means for transmitting, to the backup device, an extension request requesting an extension permission for the period indicated by the period information;
and extension means for receiving extension permission information indicating permission for the extension from the backup device and extending the period indicated by the period information.
- [4] The recording and playback device according to claim 3, wherein
the extension request means transmit the extension request a predetermined time before an ending point of the period indicated by the period information.
- [5] The recording and playback device according to claim 3, wherein
the extension request means repeatedly transmit the extension request means request periodically within the period indicated by the period information.
- [6] The recording and playback device according to claim 3,
wherein the extension means receive the extension permission information indicating a period after the period information stored in the storage means and rewrite the period indicated by the period information to the period indicated by the received extension permission information to extend the period information.
- [7] The recording and playback device according to claim 3,
wherein the extension means store an extension time in advance and extend the period information by adding the extension time to the period indicated by the period information.
- [8] The recording and playback device according to claim 3,
wherein the period information indicates an ending point of a period in which playback of the content stored in the storage means is permitted, and
the playback control means permit playback of the content when the current time is before the point indicated by the period information, and prohibit playback of the content when the current time is after the point indicated by the period information.

- [9] The recording and playback device according to claim 3,
wherein the period information is a permitted time indicating a length of time in which playback of the content stored in the storage means is permitted and a starting time indicating a starting point of a period in which playback of the content is permitted; and
the playback control means acquire an elapsed time from the starting time, permit playback of the content when the acquired elapsed time is equal to or less than the permitted time, and prohibit playback of the content when the time elapsed from the starting time exceeds the permitted time.
- [10] The recording and playback device according to claim 2, wherein
the playback control means prohibit playback of the content by deleting the content from the storage means.
- [11] The recording and playback device according to claim 10,
wherein the recording and playback device further comprise: restore instruction acquisition means for acquiring a restore instruction indicating acquisition of the content stored by the backup device;
restore request means for transmitting a transmission request for the content stored by the backup device to the backup device,
and restoring means for receiving the content from the backup device and writing the received content to the storage means,
wherein when the content is written, the writing means further write
period information indicating a period in which playback of the content written by the restoring means is permitted to the storage means in association with the content.
- [12] The recording and playback device according to claim 2, wherein the content stored in the storage means
is configured to include an encrypted work generated by encrypting a digital work based on an encryption key and a decryption key used to decrypt the encrypted work,
and the playback control means prohibit
playback of the content by deleting the decryption key included in the content.
- [13] The recording and playback device according to claim 12, wherein the recording and playback

device further comprises: restore instruction acquisition means

for acquiring a restore instruction indicating acquisition of the encryption key stored by the backup device; restore request means for transmitting a transmission request for the decryption key stored by the backup device to the backup device; and restoring means for receiving the decryption key from the backup device

and writing the received decryption key to the storage means, wherein when the decryption key is written, the writing means further write period information indicating a period in which playback of the content stored by the storage means is permitted to the storage means in association with the content.

[14] The recording and playback device according to claim 2, wherein the content stored in the storage means

includes an encrypted work generated by encrypting a digital work using an encryption key, and an encryption key generated by encrypting a decryption key used to decrypt the encrypted work using a unique key that is unique to the recording and playback device, and the playback control means

prohibit playback of the content by deleting the encryption key from the storage means.

[15] The recording and playback device according to claim 2, wherein the content stored in the storage means includes backup information indicating permission or prohibition of backup,

the content transmission means determine whether the backup information indicates permission for backup and transmit the content when it is determined that permission is indicated, and

the writing means determine whether the backup information indicates permission for backup and

write the period information when it is determined that permission is indicated.

[16] The recording and playback device according to claim 2, wherein the content transmission means encrypt the content using a communication key and safely transmit

the encrypted content.

[17] The recording and playback device according to claim 2, wherein the recording and playback

device further comprises:

detection information storage means for storing detection information generated by performing a predetermined computation on the content; and

fraud prohibition means for reading the content from the storage means, performing the predetermined computation on the read content to generate inspection information, comparing the generated inspection information to the detection information, and

prohibiting use of the content that is determined not to match.

[18] The recording and playback device according to claim 2,

wherein the backup device stores other content in response to a backup instruction by equipment other than the recording and playback device, the recording and playback device being

further comprising: restore instruction acquisition means for acquiring a restore instruction indicating acquisition of the other content;

content request means for transmitting a transmission request for the other content to the backup device when the list instruction is acquired;

and restoring means for receiving the other content from the backup device and writing the received other content to the storage means,

and when the other content is received, the writing means further write

period information indicating a period in which playback of the other content is permitted to the storage means in association with the other content.

[19] A backup device for backing up content, the backup device comprising: storage means for storing

the content; extension reception means for receiving, from the

recording and playback device, an extension request seeking permission to extend period information indicating a period during which playback of the content stored by the recording and playback device is permitted; determination means for determining whether to permit

the extension; and

permission means for outputting, to the recording and playback device, extension permission information indicating permission of the extension when

it is determined that the extension will be permitted.

[20] The backup device according to claim 19, wherein the storage means further store identification

information indicating the content in correspondence with the content,

the extension reception means receive the extension request including content identification information indicating the content stored by the recording and playback device, and

the determination means compare the content identification information to the identification information stored by the storage means, and when both match, make a determination to permit the extension.

[21] The backup device according to claim 19, wherein the extension request includes device identification information indicating the recording and playback device to which the extension request was output,

the determination means store one or more pieces of permitted device identification information indicating a specific piece of equipment in advance, and when the device identification information included in the received extension request matches any of the permitted device identification information, make a determination

to permit the extension.

[22] The backup device according to claim 19, wherein the storage means further store

detection information generated by performing a predetermined computation on the content in correspondence with the content; and

the determination means read the content from the storage means, perform the predetermined computation on the read content to generate verification information, compare generated verification information to the detection information, and, when both match, make a determination to permit the extension.

[23] The backup device according to claim 19, wherein the permission means output

the extension permission information indicating a later period than the period indicated by the period information.

[24] The backup device according to claim 19, further comprising:

restore receiving means for receiving a transmission request for the content stored by the storage means;

restore determination means for determining whether to transmit the content;

and restore transmission means for reading the content from the storage means and transmitting the read content when it is determined that the content is to be transmitted.

[25] The backup device according to claim 24, wherein the transmission request includes restore

equipment identification information indicating restore equipment that is the transmission source of the transmission request, and

the restore determination means store one or more pieces of permitted device identification information indicating a specific piece of equipment in advance, and when the restore equipment identification information matches any of the permitted device identification information, the restore determination means make a determination

to transmit the content.

[26] The backup device according to claim 25, wherein the permitted device identification information indicates a backup source device that instructed backup of the content stored by the storage means, and

the restore determination means make a determination

to transmit the content when the restore equipment identification information matches the permitted device identification information.

[27] The backup device according to claim 24, wherein the restore determination means have a copy number indicating the total number of pieces of equipment storing content that is identical to the content stored in the storage means and that is permitted to be played back by the backup device, and a permitted copy number indicating an upper limit of the copy number, and

when the copy number is less than the permitted copy number, the restore determination means make a determination to transmit the content.

[28] The backup device according to claim 27, wherein the backup device further comprises:

equipment identification information indicating equipment storing content that is identical to the content stored by the storage means and that is permitted to be played back by the backup device;

period information storage means for associating and storing copy period information indicating a period in which playback of the content is permitted in the equipment; and copy number management means for subtracting one from the copy number when the period indicated by

the copy period information ends.

[29] The backup device according to claim 27, wherein the content stored by the storage means includes the permitted copy number in advance, and the determination means acquire

the permitted copy number from the content.

[30] The backup device according to claim 24, wherein the restore transmission means encrypt the

content using a communication key and safely transmit encrypted content.

[31] The backup device according to claim 19, wherein the recording and playback device outputs startup instruction information instructing startup to the backup device prior to the extension request, and

the backup device further comprises

power control means for starting power supply to each circuit constituting the backup device upon receiving the startup instruction.

[32] A backup method used in a recording and playback device for performing recording and playback of content,

wherein the recording and playback device comprises storage means for storing the content, the backup method comprising:

a reception step of receiving an instruction to back up the content; a content transmission step of, upon receiving

the instruction, reading the content from the storage means and transmitting the read content to the backup device when backup of the read content is permitted; a writing step of, upon receiving

the instruction, writing period information indicating a period in which playback of the content that is subject to the backup is permitted to the storage means in association with the content;

and a playback control step of permitting playback of the content during the period indicated by

the period information and prohibiting playback of the content when the period indicated by the period information ends.

[33] An integrated circuit installed in a recording and playback device for performing recording and playback of content,

the integrated circuit comprising: storage means for storing the content;

reception means for receiving an instruction to back up the content; content transmission means for, upon receiving

the instruction, reading the content from the storage means and transmitting the read content to the backup device when backup of the read content is permitted;

writing means for, upon receiving

the instruction, writing period information indicating a period in which playback of the content that is subject to the backup is permitted to the storage means in association with the content; and playback control means for permitting playback of the content during the period indicated by

the period information and prohibiting playback of the content when the period indicated by the period information ends.

[34] A backup program executed in a recording and playback device for performing recording and playback of content,

wherein

the recording and playback device comprises storage means for storing the content,

the backup program comprising: a reception step of receiving an instruction to back up the content;

a content transmission step of, upon receiving

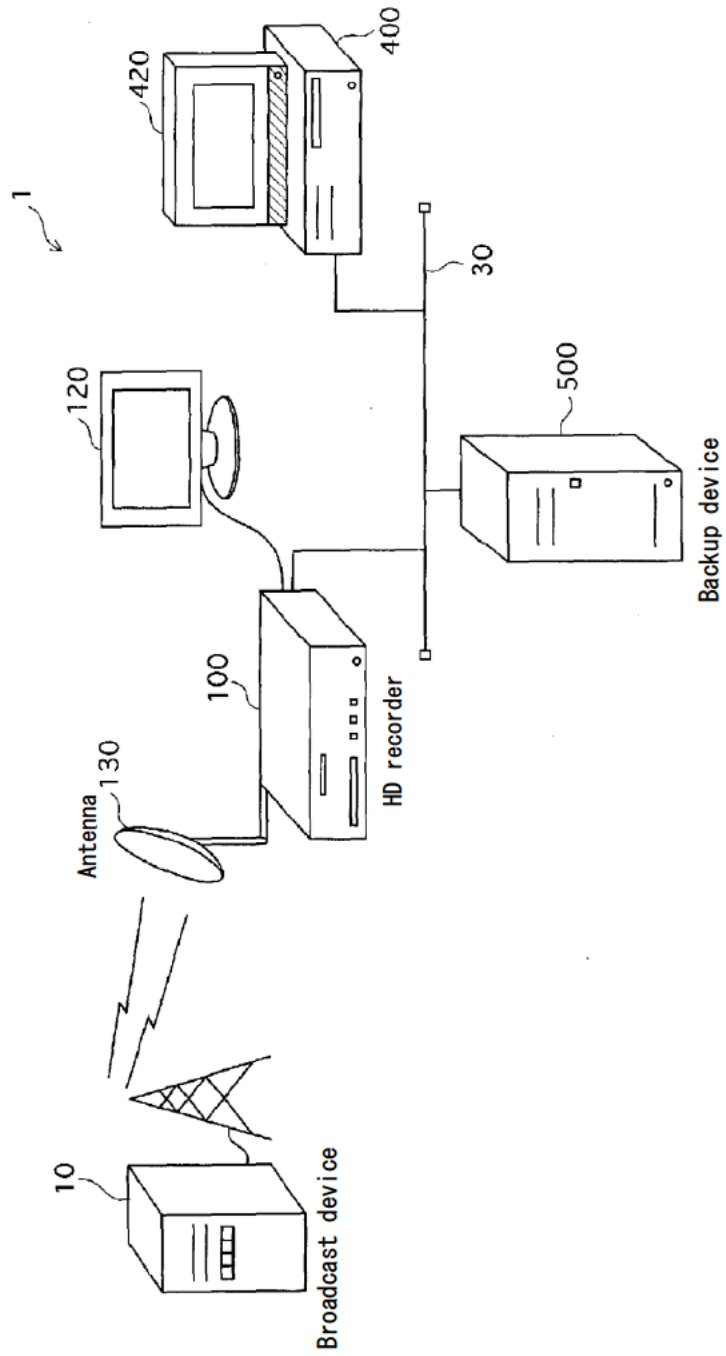
the instruction, reading the content from the storage means and transmitting the read content to the backup device when backup of the read content is permitted; a writing step of, upon receiving

the instruction, writing period information indicating a period in which playback of the content that is subject to the backup is permitted to the storage means in association with the content; and a playback control step of permitting playback of the content during the period indicated by

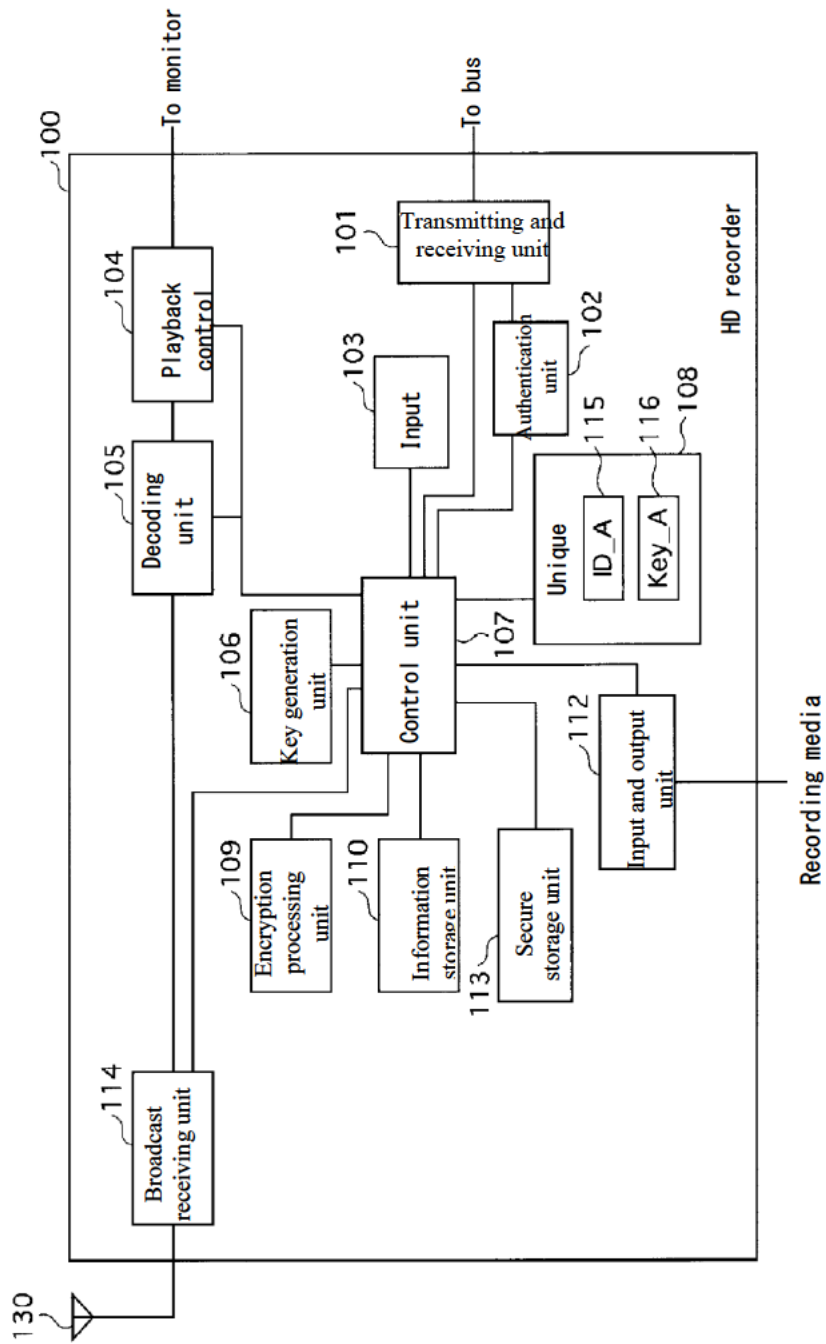
the period information and prohibiting playback of the content when the period indicated by the period information ends.

[35] The backup program according to claim 34, wherein the backup program is recorded on a computer-readable recording medium.

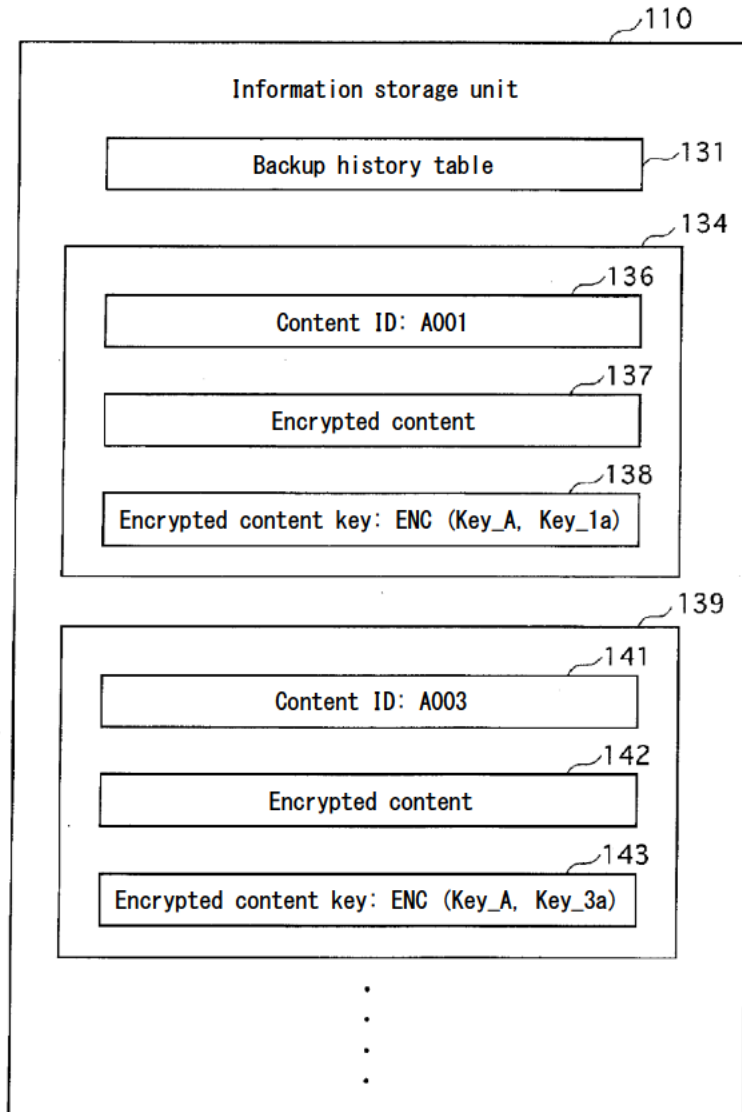
[FIG. 1]



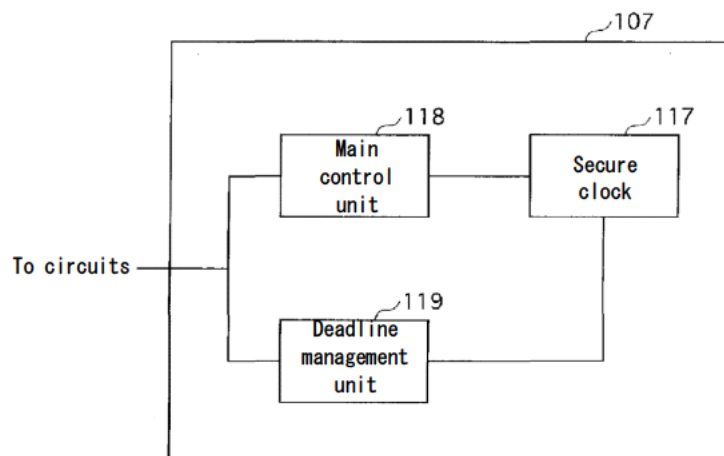
[FIG. 2]



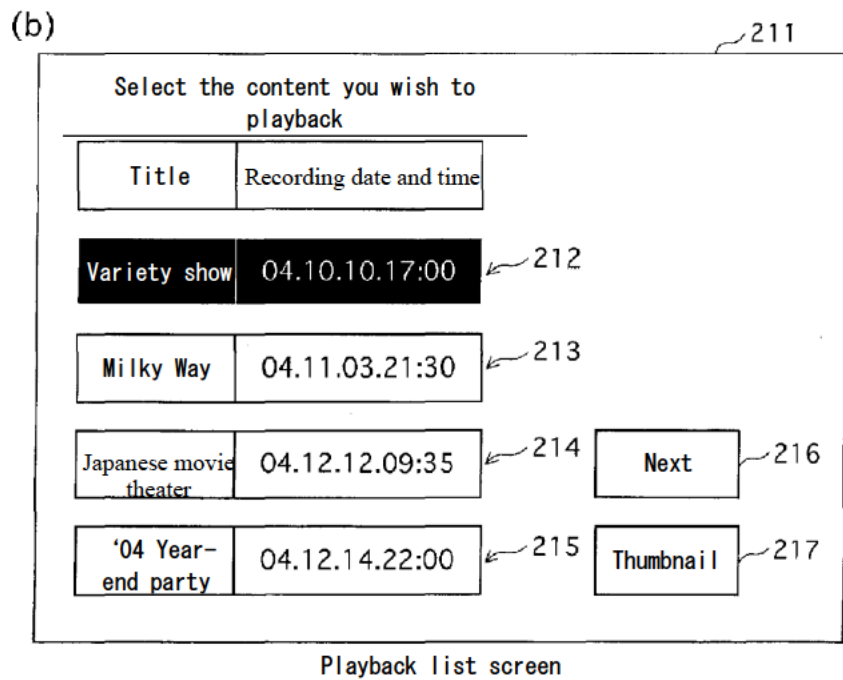
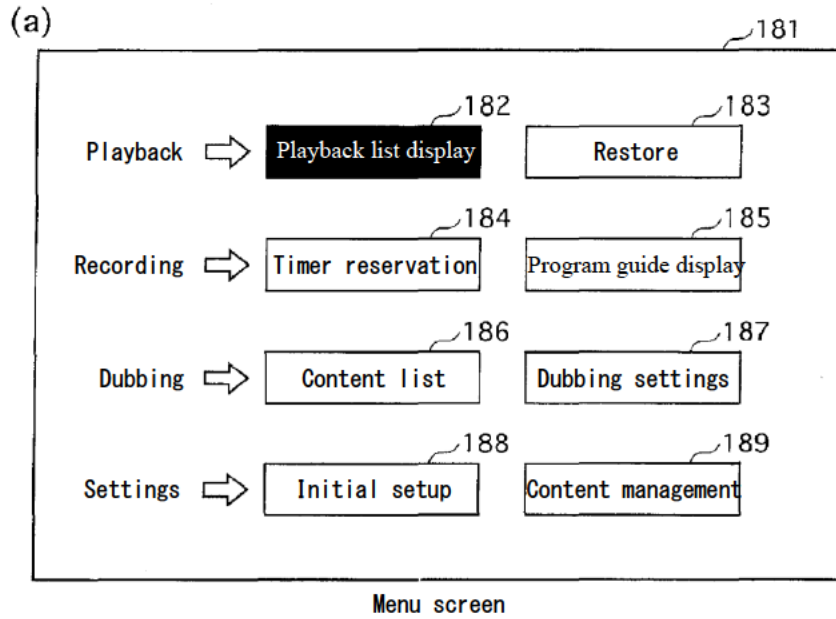
[FIG. 3]



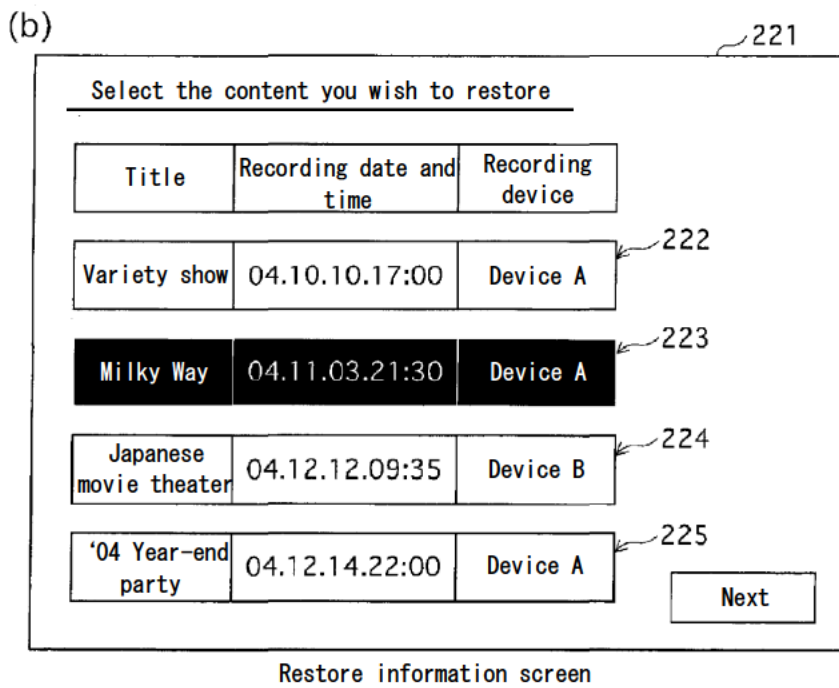
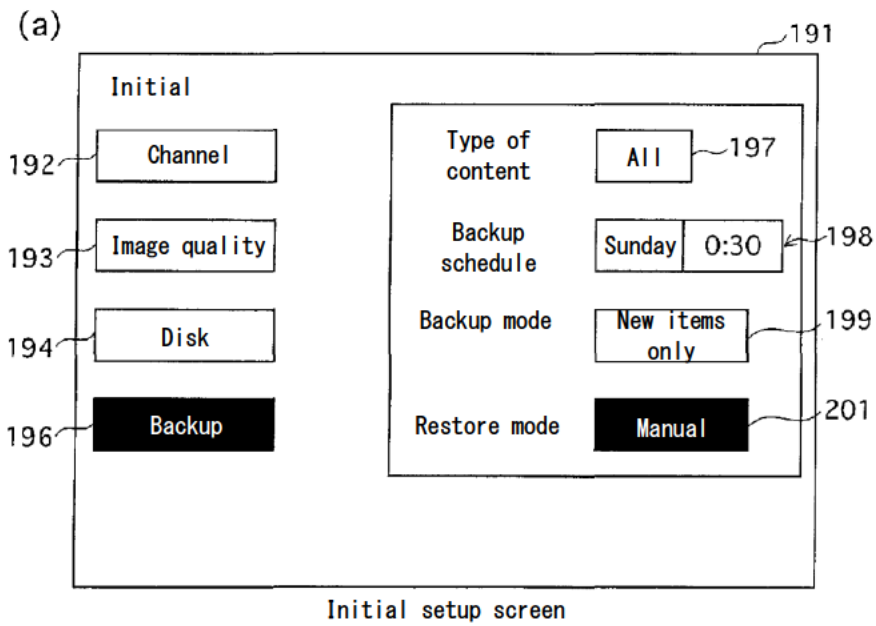
[FIG. 5]



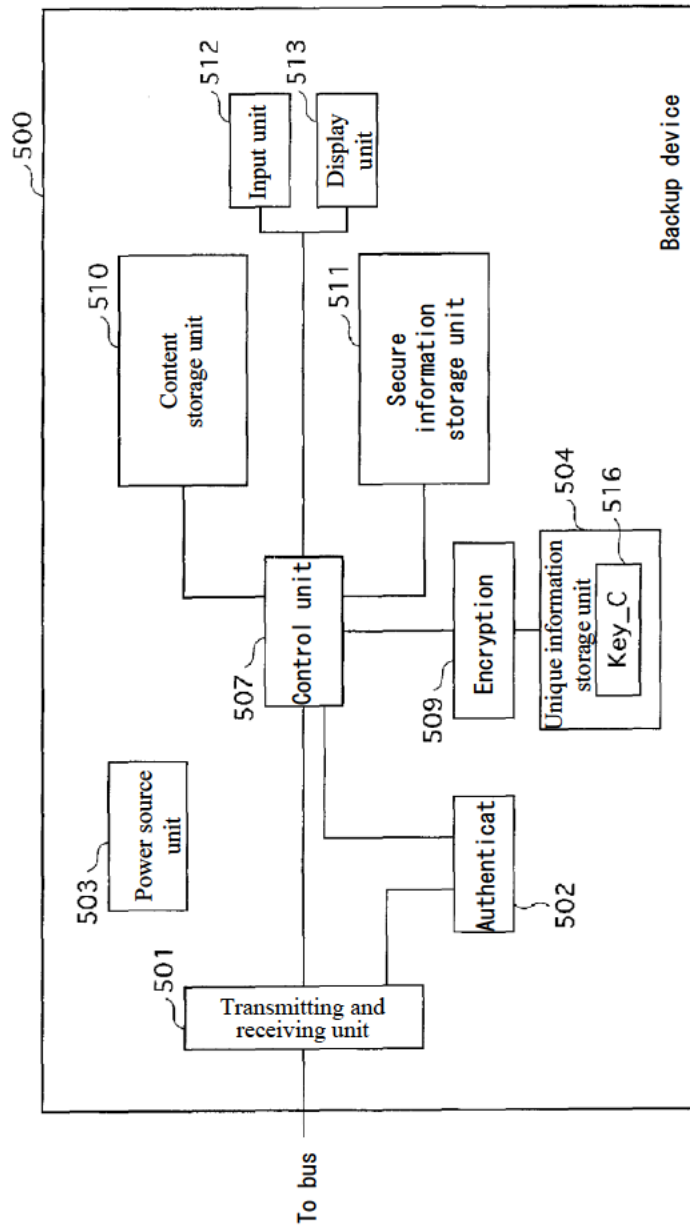
[FIG. 6]



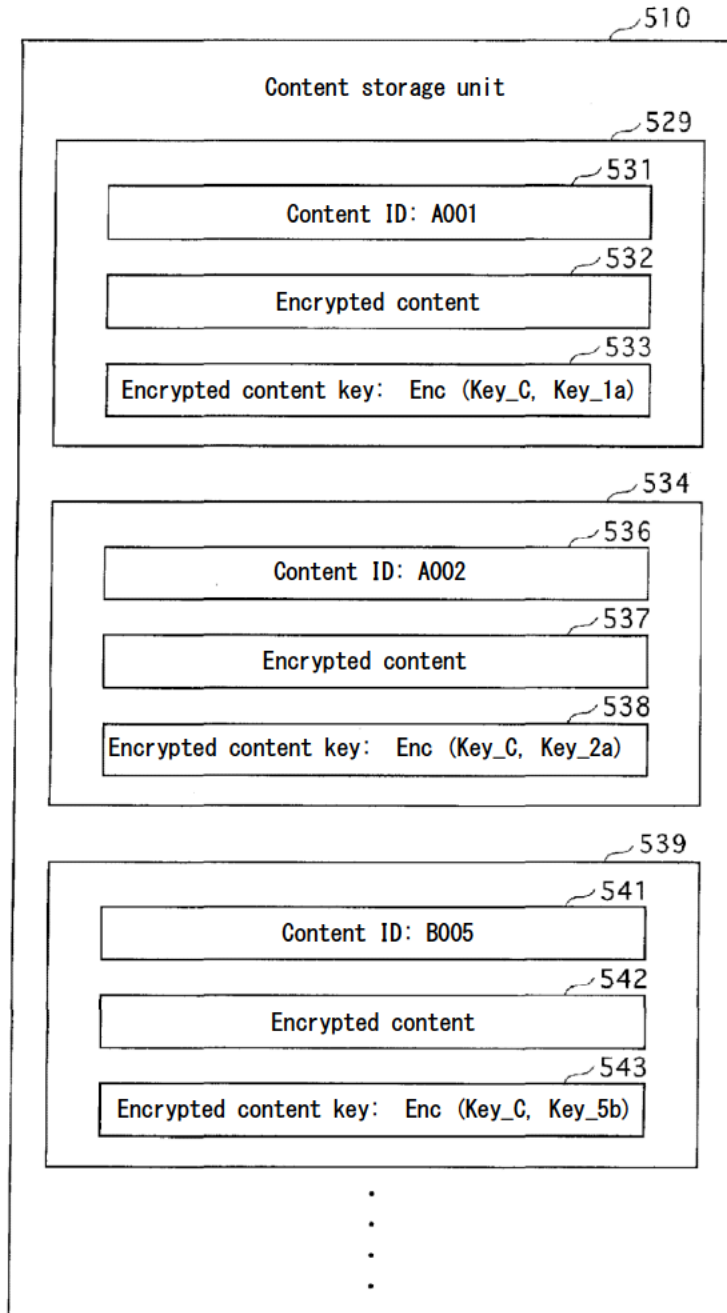
[FIG. 7]



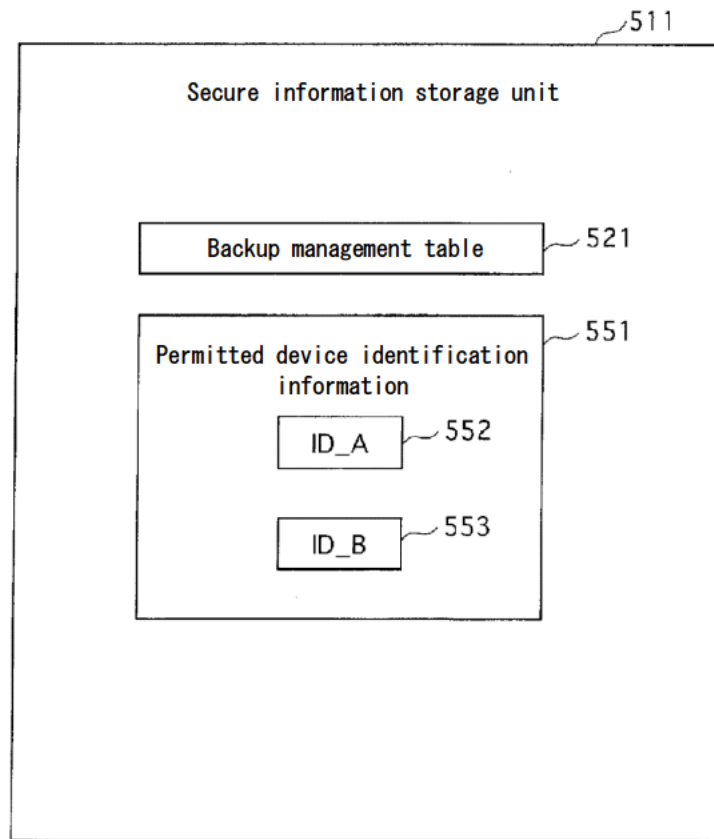
[FIG. 8]



[FIG. 9]



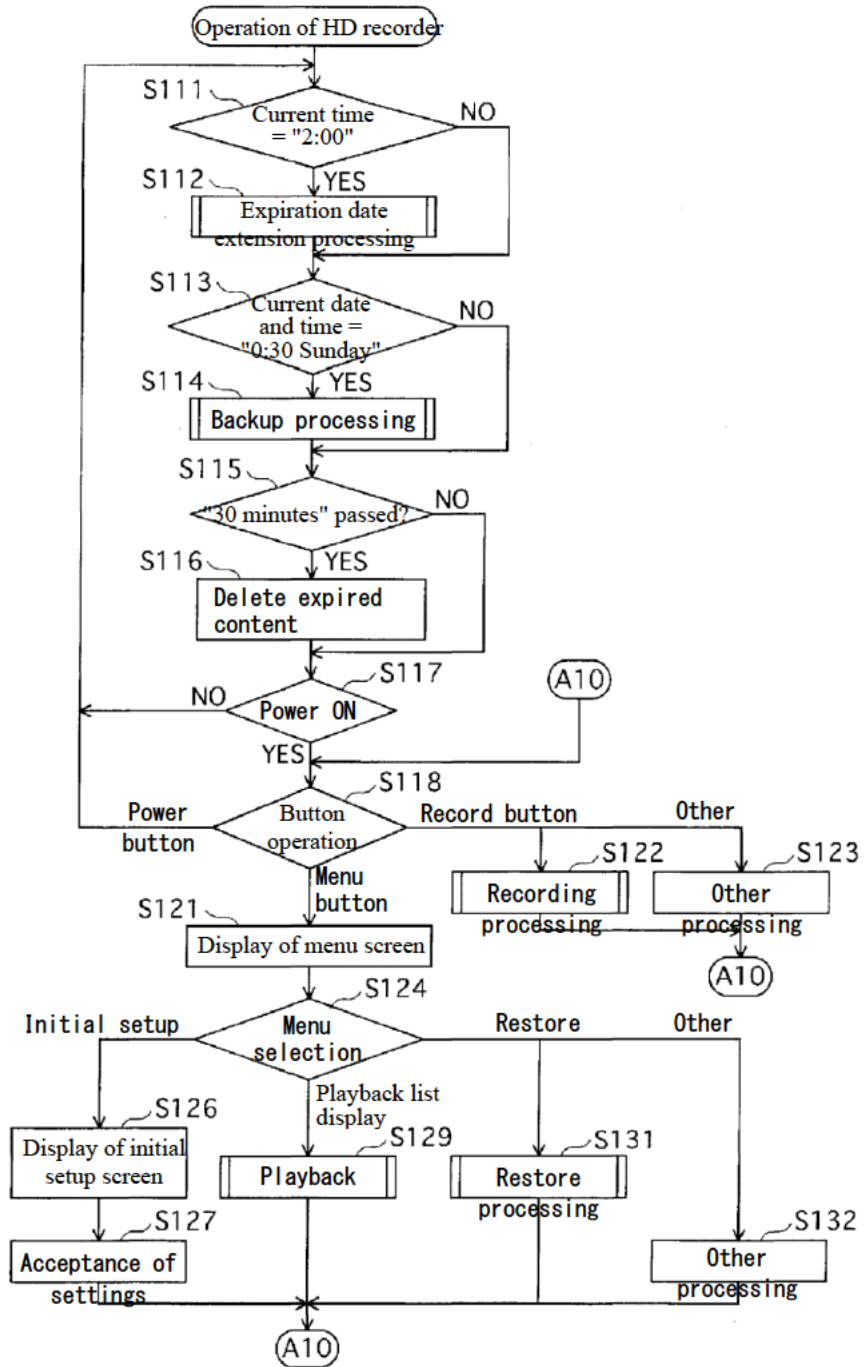
[FIG. 10]



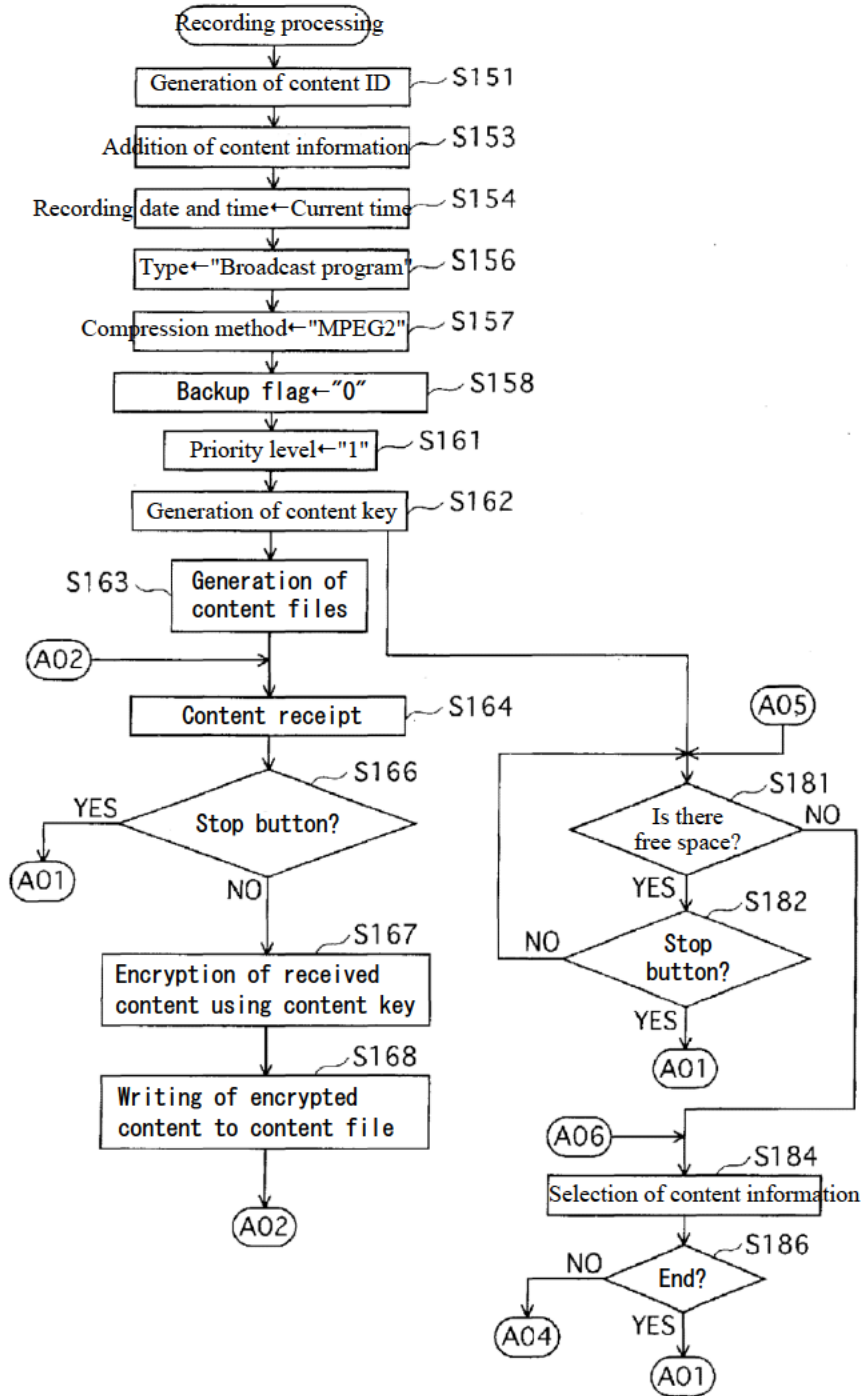
[FIG. 11]

521				
561	562	563 Backup information		565
Content ID	Title	Recording date and	Backup source device	Hash value
522 A001	Variety show	04.10.10.17:00	ID_A	01c
523 A002	Milky Way	04.11.03.21:30	ID_A	02c
524 B005	Japanese movie	04.12.12.09:35	ID_B	05c
525 A003	'04 Year-end	04.12.14.22:00	ID_A	03c
.
.
.

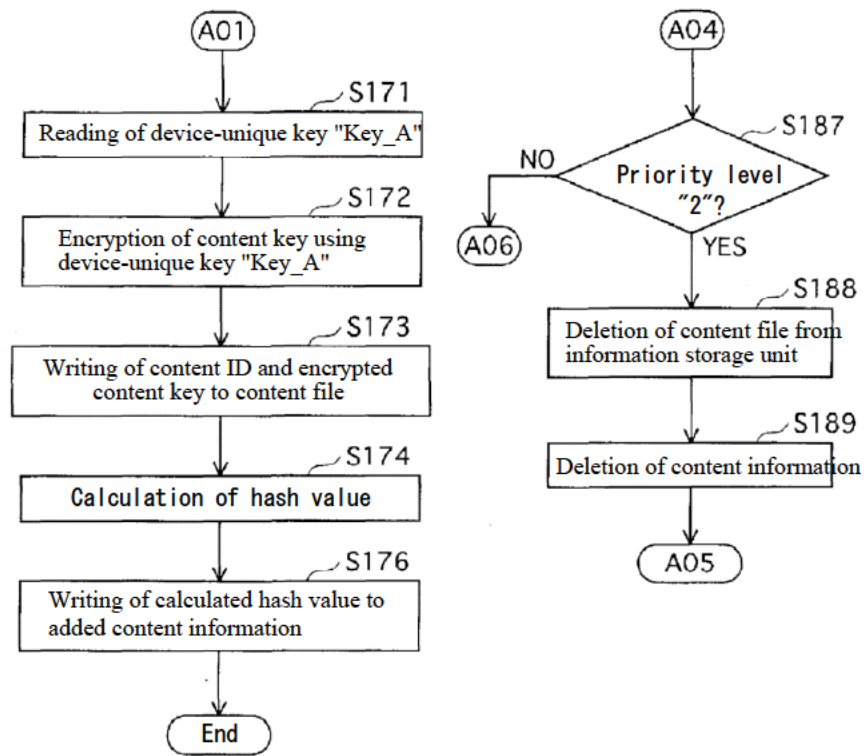
[FIG. 12]



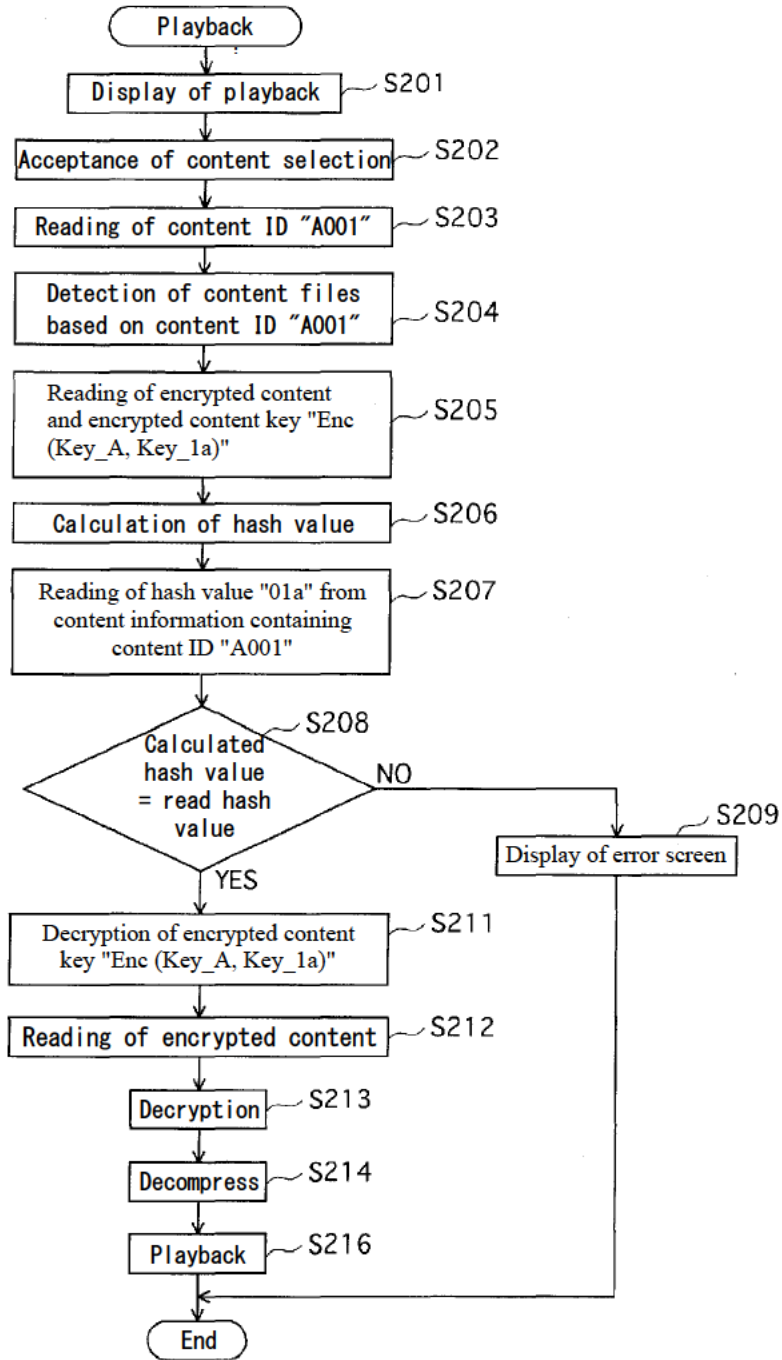
[FIG. 13]



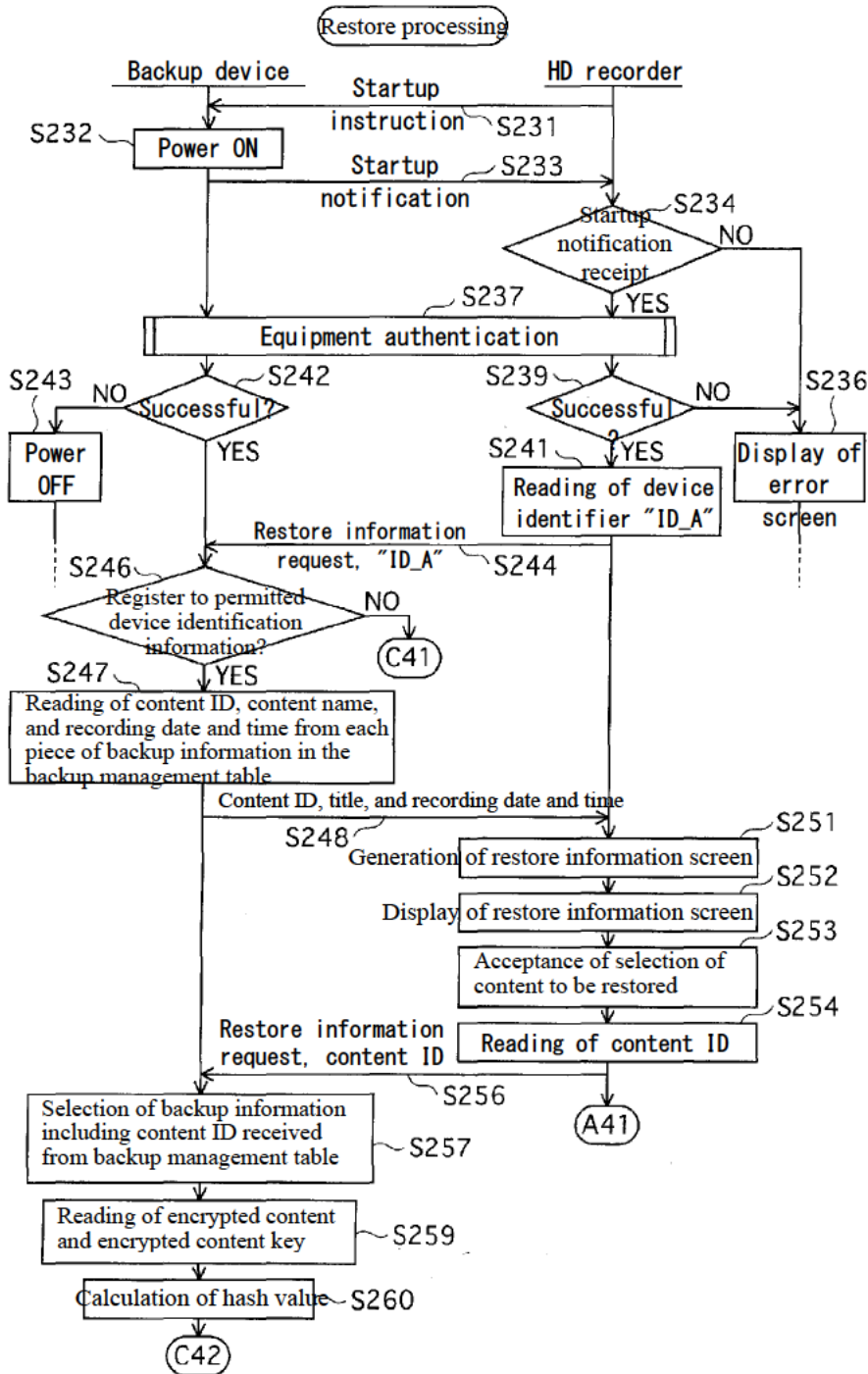
[FIG. 14]



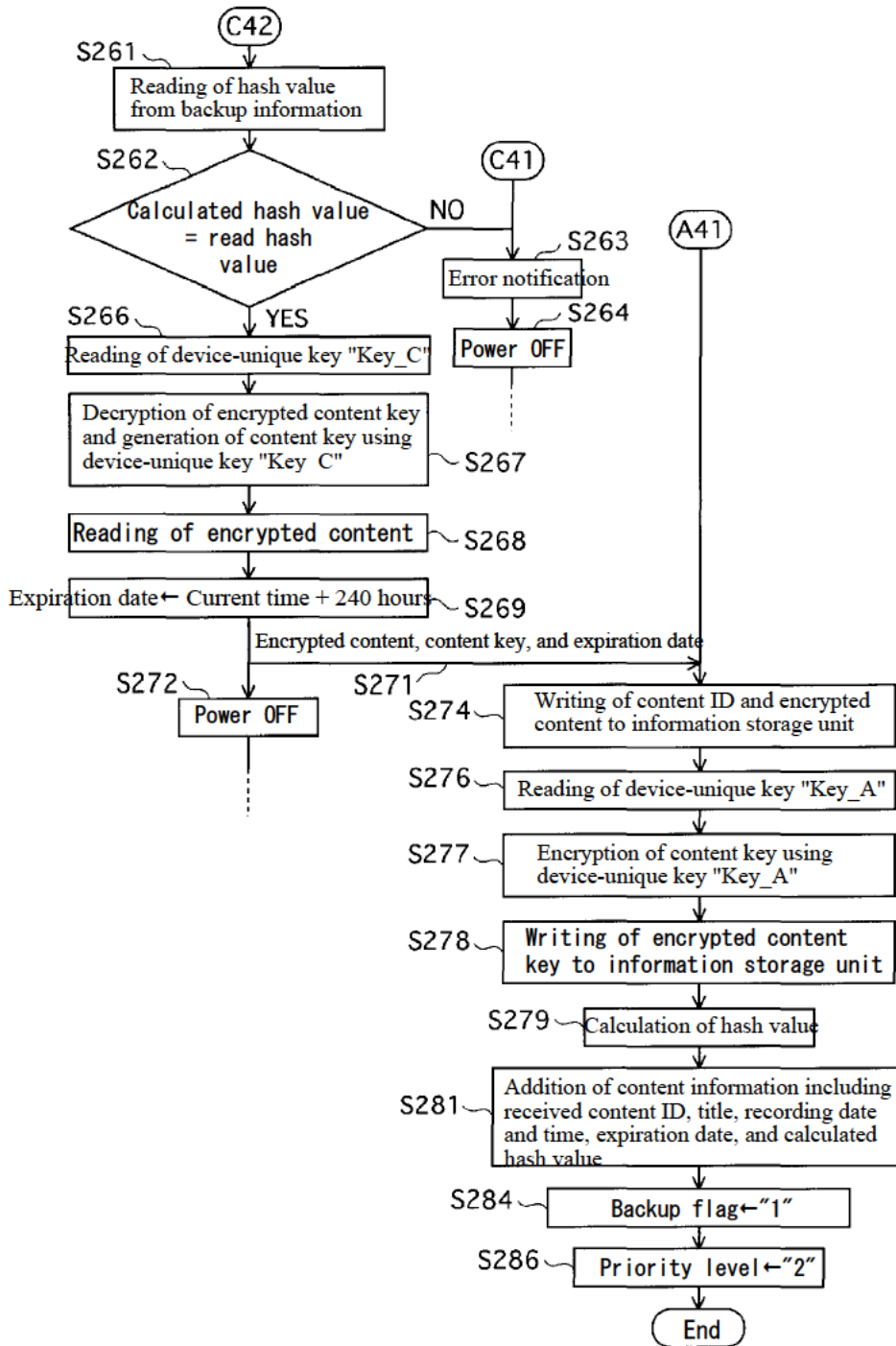
[FIG. 15]



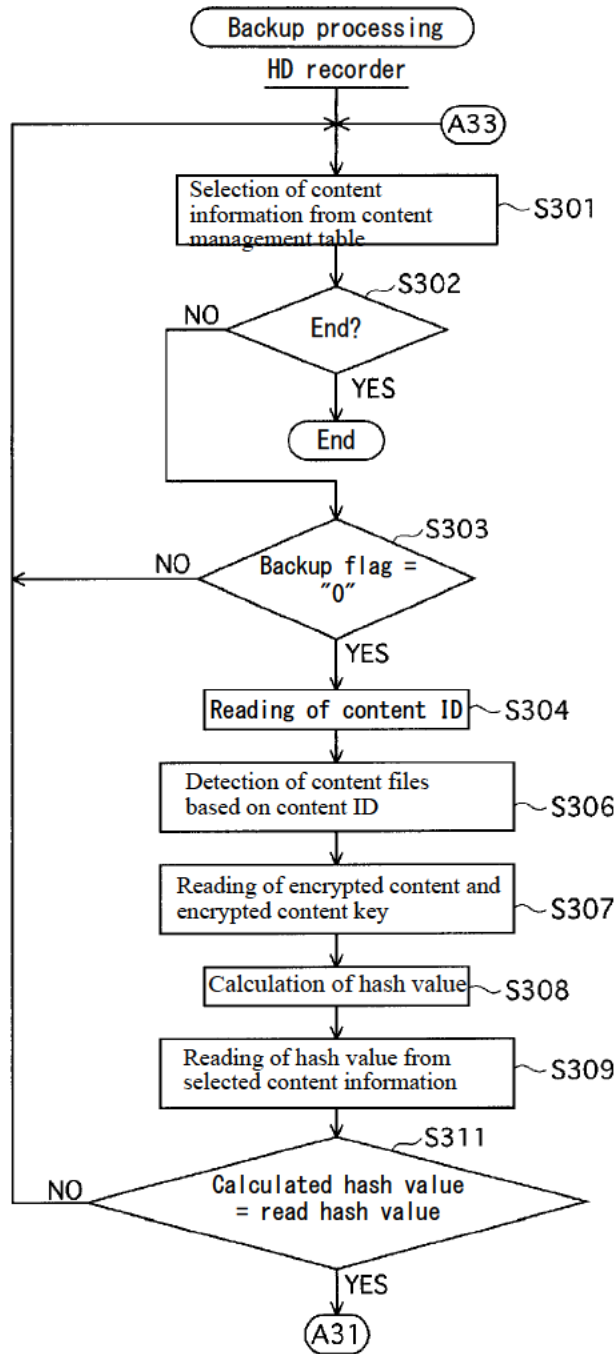
[FIG. 16]



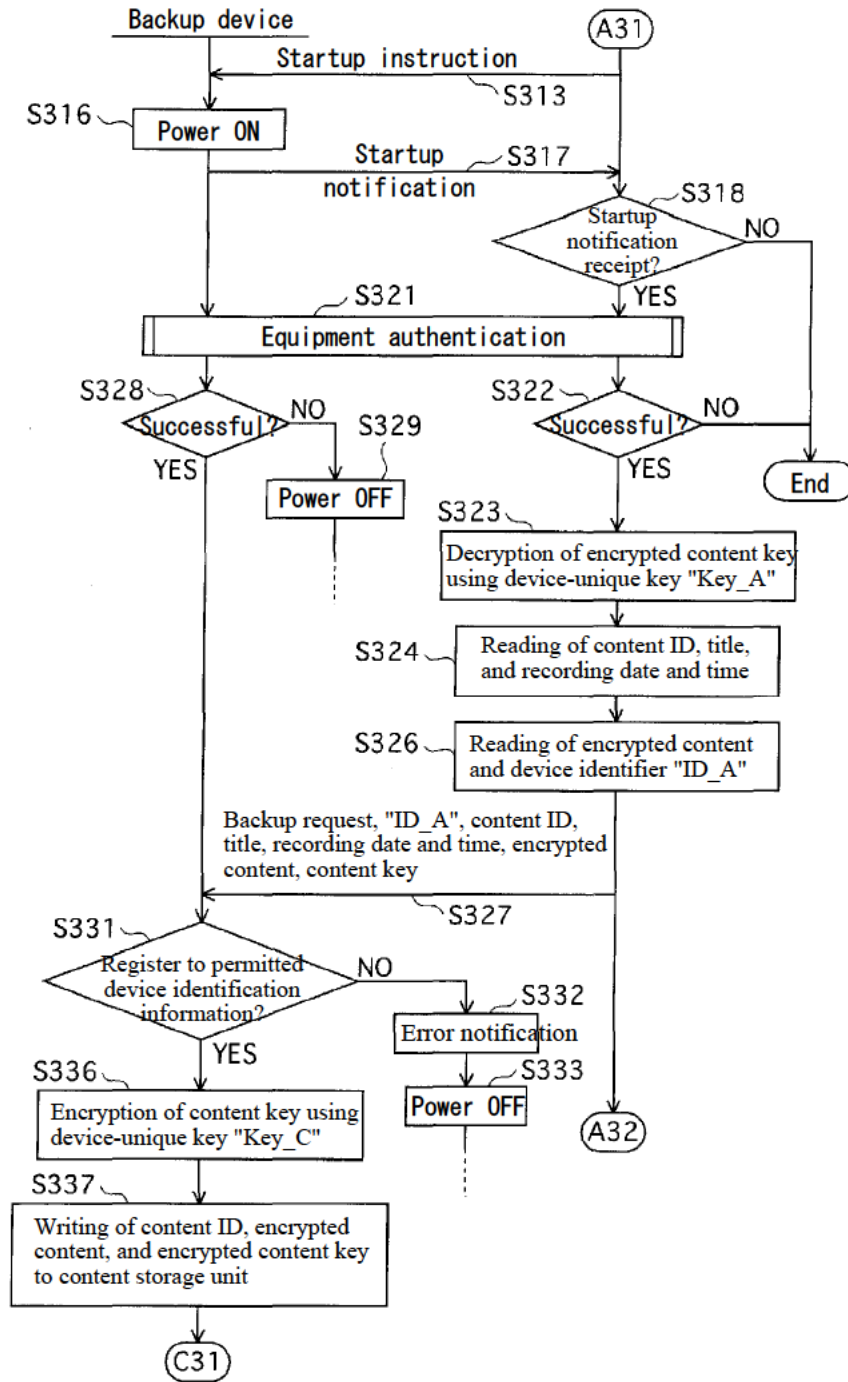
[FIG. 17]



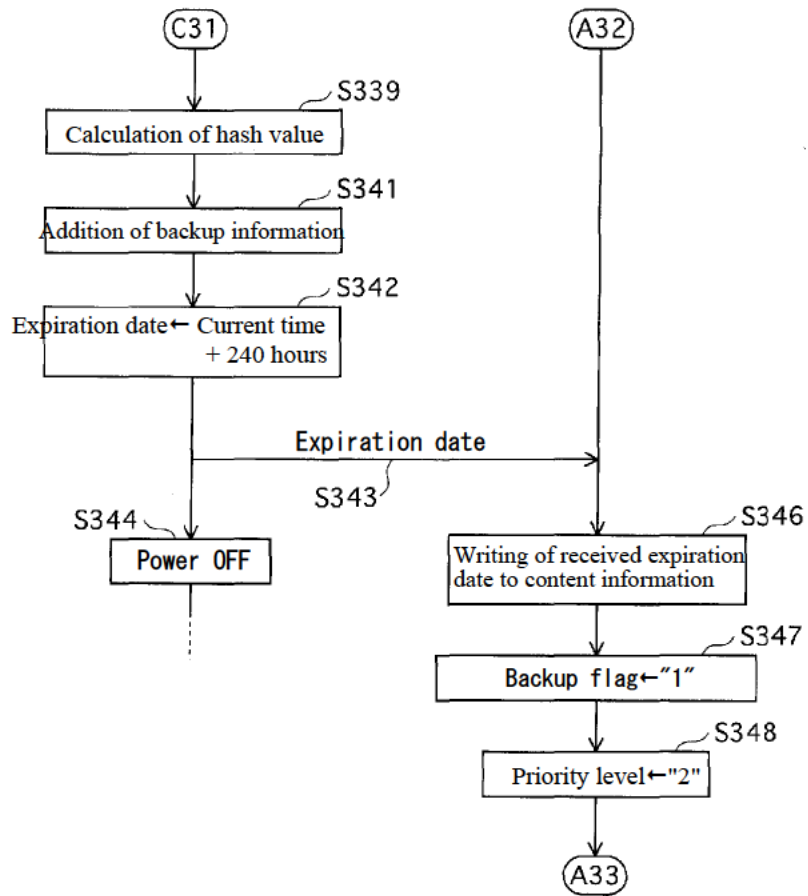
[FIG. 18]



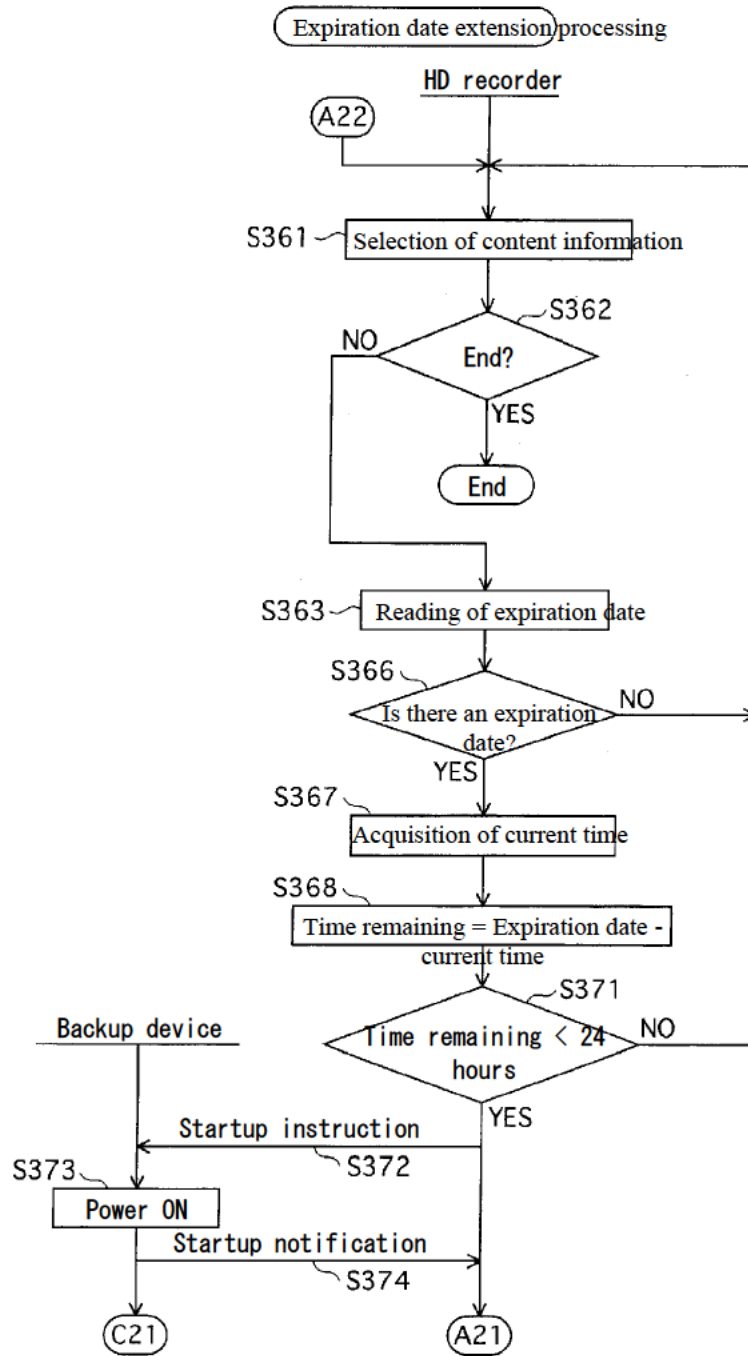
[FIG. 19]



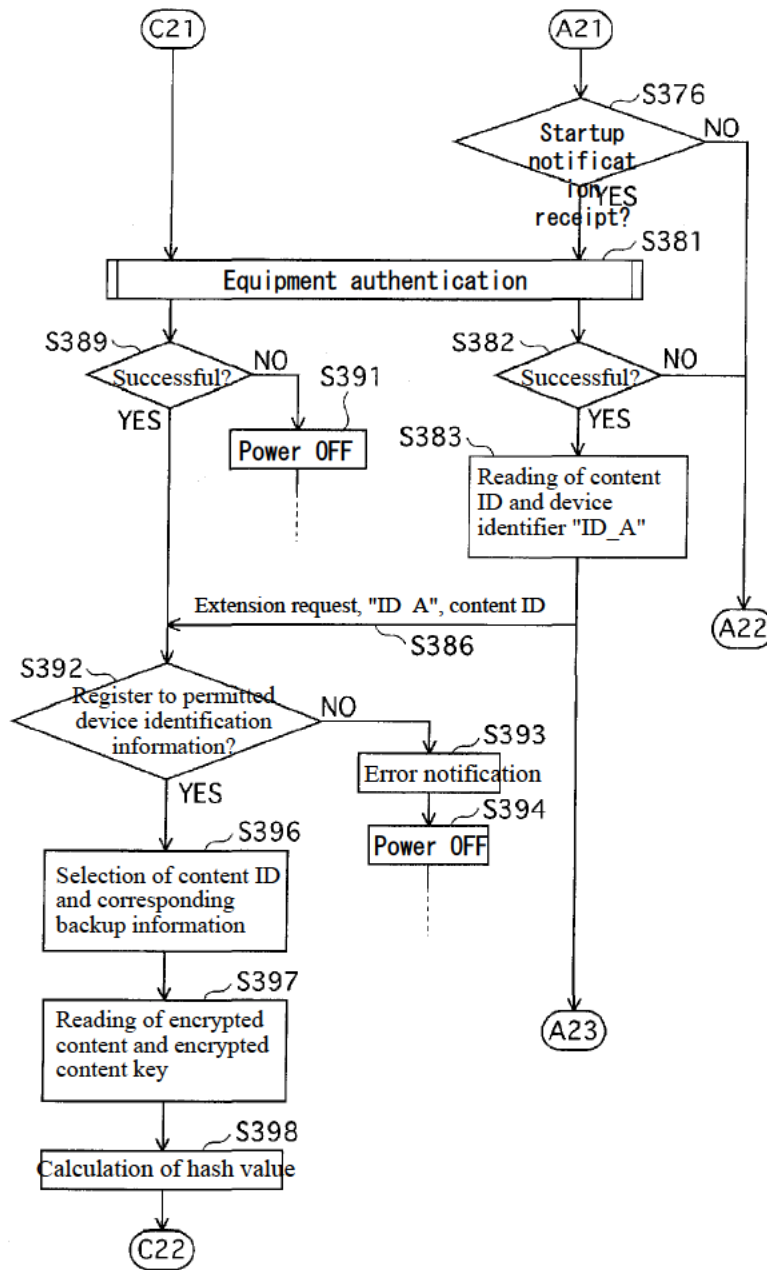
[FIG. 20]



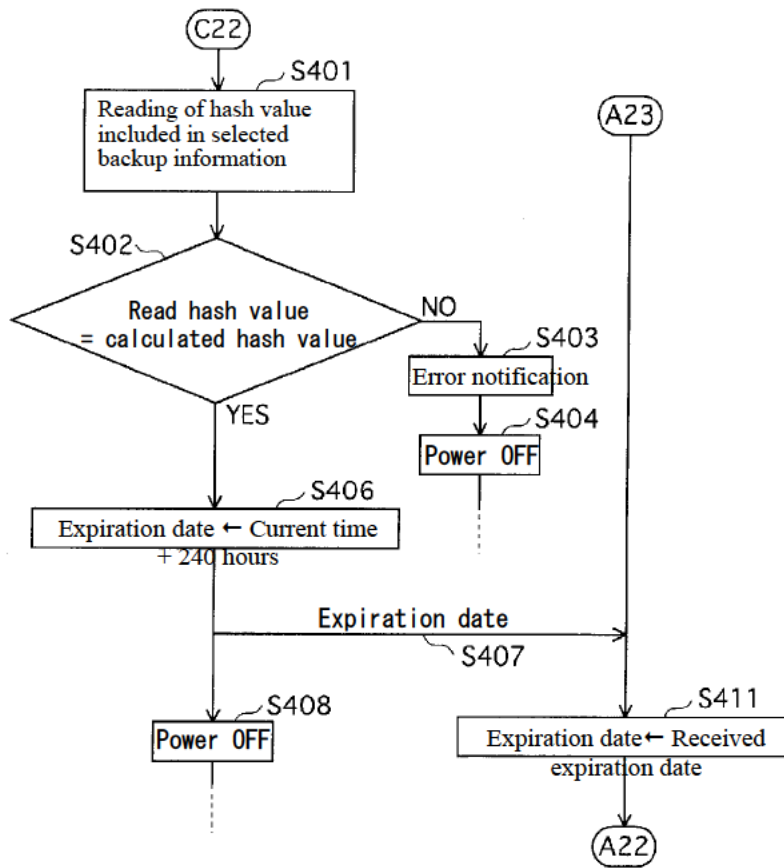
[FIG. 21]



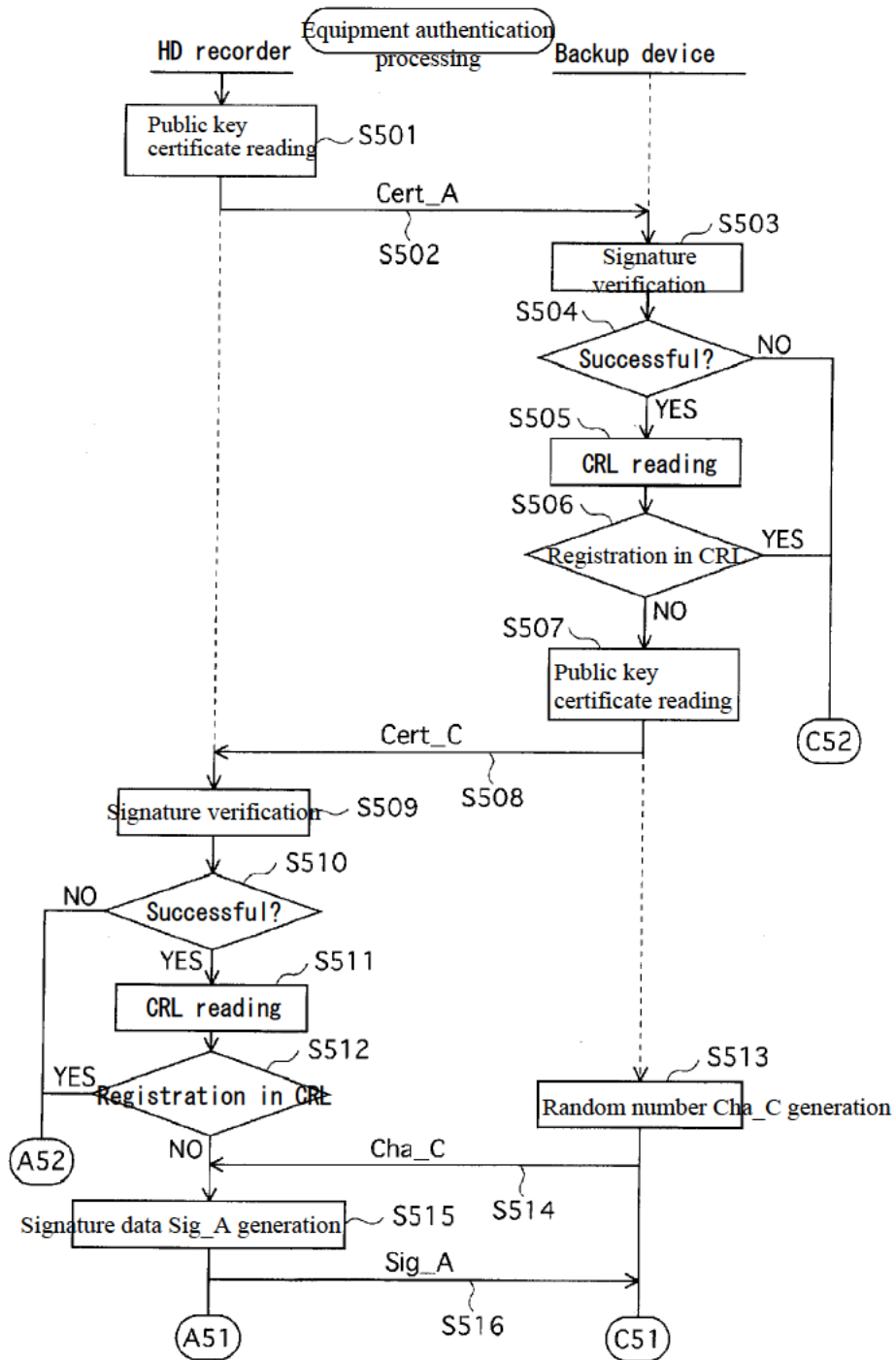
[FIG. 22]



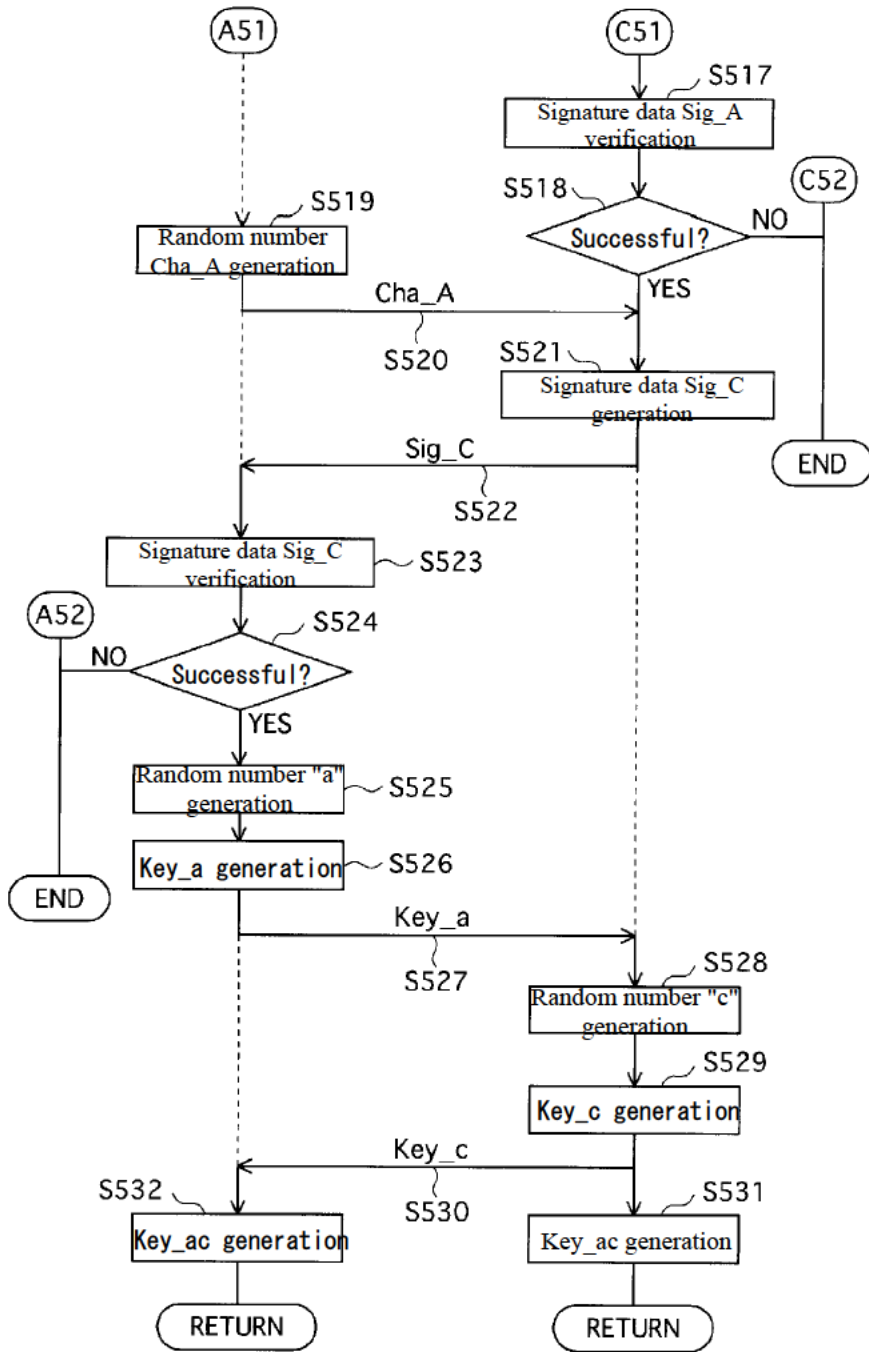
[FIG. 23]



[FIG. 24]



[FIG. 25]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2005/022

A. CLASSIFICATION OF SUBJECT MATTER
G06F21/24(2006.01), **G11B20/10**(2006.01), **G11B27/00** (2006.01), **H04N5/91**
 (2006.01), **H04N7/167** (2006.01), **H04N7/173**(2006.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F21/24(2006.01), **G11B20/10**(2006.01), **G11B27/00** (2006.01), **H04N5/91**
 (2006.01), **H04N7/167** (2006.01), **H04N7/173**(2006.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2006
 Kokai Jitsuyo Shinan Koho 1971-2006 Toroku Jitsuyo Shinan Koho 1994-2006

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to
Y	JP 2003-186751 A (Matsushita Electric Industrial Co., Ltd.), 04 July, 2003 (04.07.03), Par. No. [0298] (Family: none)	19-25
Y	JP 11-203127 A (Casio Computer Co., Ltd.), 30 July, 1999 (30.07.99), Abstract (Family: none)	19-25
A	JP 8-263440 A (Xerox Corp.), 11 October, 1996 (11.10.96), Par. Nos. [0081] to [0083], [0176] to [0180] & US 5715403 A & EP 0715244 A1	1-

Further documents are listed in the continuation of Box C.

See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"I" later document published after the international filing date and not in conflict with the application but cited to underline the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention is considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention is considered to involve an inventive step when the document is combined with one or more other such documents, such as being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

14 February, 2006 (14.02.06)

Date of mailing of the international search report

21 February, 2006 (21.02.06)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2005/022772

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to
A	JP 2001-14221 A (Victor Company Of Japan, Ltd.), 19 January, 2001 (19.01.01), Par. Nos. [0022] to [0023] & EP 1049087 A2	1-
A	JP 2004-54988 A (Sony Corp.), 19 February, 2004 (19.02.04), Abstract (Family: none)	1-
A	JP 2003-30054 A (Sharp Corp.), 31 January, 2003 (31.01.03), Full text; all drawings (Family: none)	1-

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2005/022772

A. CLASSIFICATION OF SUBJECT MATTER G06F21/24 (2006.01), G11B20/10 (2006.01), G11B27/00 (2006.01), H04N5/91 (2006.01), H04N7/167 (2006.01), H04N7/173 (2006.01)		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols) G06F21/24 (2006.01), G11B20/10 (2006.01), G11B27/00 (2006.01), H04N5/91 (2006.01), H04N7/167 (2006.01), H04N7/173 (2006.01)		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2006 Kokai Jitsuyo Shinan Koho 1971-2006 Toroku Jitsuyo Shinan Koho 1994-2006		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2003-186751 A (Matsushita Electric Industrial Co., Ltd.), 04 July, 2003 (04.07.03), Par. No. [0298] (Family: none)	19-25, 27-31
Y	JP 11-203127 A (Casio Computer Co., Ltd.), 30 July, 1999 (30.07.99), Abstract (Family: none)	19-25, 27-31
A	JP 8-263440 A (Xerox Corp.), 11 October, 1996 (11.10.96), Par. Nos. [0081] to [0083], [0176] to [0180] & US 5715403 A & EP 0715244 A1	1-35
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 14 February, 2006 (14.02.06)		Date of mailing of the international search report 21 February, 2006 (21.02.06)
Name and mailing address of the ISA/ Japanese Patent Office		Authorized officer
Facsimile No.		Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2005/022772

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2001-14221 A (Victor Company Of Japan, Ltd.), 19 January, 2001 (19.01.01), Par. Nos. [0022] to [0023] & EP 1049087 A2	1-35
A	JP 2004-54988 A (Sony Corp.), 19 February, 2004 (19.02.04), Abstract (Family: none)	1-35
A	JP 2003-30054 A (Sharp Corp.), 31 January, 2003 (31.01.03), Full text; all drawings (Family: none)	1-35