Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2594760 A1 2006/07/20

(21) 2 594 760

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2006/01/09
(87) Date publication PCT/PCT Publication Date: 2006/07/20
(85) Entrée phase nationale/National Entry: 2007/07/11
(86) N° demande PCT/PCT Application No.: EP 2006/050099
(87) N° publication PCT/PCT Publication No.: 2006/074987
(30) Priorité/Priority: 2005/01/11 (US10/905,570)

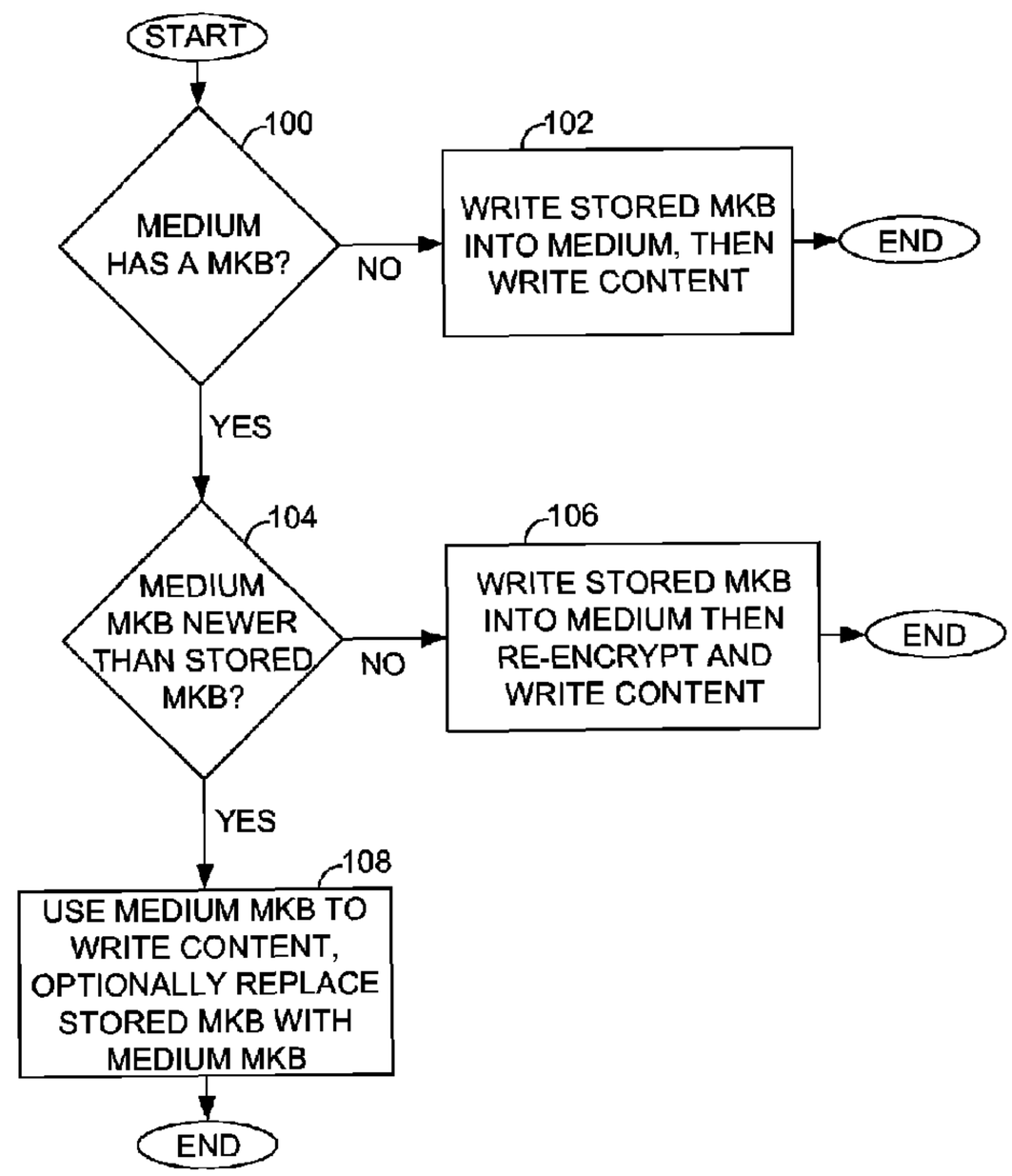
(51) Cl.Int./Int.Cl. *H04L 9/00* (2006.01),
H04L 9/08 (2006.01)

(71) Demandeurs/Applicants:
INTERNATIONAL BUSINESS MACHINES CORPORATION, US;
THE WALT DISNEY COMPANY, US

(72) Inventeurs/Inventors:
LOTSPIECH, JEFFREY BRUCE, US;
WATSON, SCOTT FRAZIER, US

(74) Agent: CHAN, BILL W.K.

(54) Titre : BLOC CLE DE SUPPORT DE LECTURE/ECRITURE
(54) Title: SYSTEM AND METHOD FOR CONTROLLING ACCES TO PROTECTED DIGITAL CONTENT BY VERIFICATION OF A MEDIA KEY BLOCK



(57) Abrégé/Abstract:
A recorder system contains a media key block (MKB) and selectively writes protected content into a recording medium according to the following content protection logic, to combat theft of the protected content: If the medium does not have a MKB, then the recorder writes its stored MKB into the medium and writes protected content into the medium. If the medium has a MKB that is older than the stored MKB in the recorder, then the recorder writes its stored MKB into the medium before re-encrypting and writing protected content into the medium. If the medium has a MKB that is newer than the stored MKB, then the MKB in the medium is used for content protection. The recorder may store the newer MKB in non-volatile memory, effectively updating its previous stored MKB, so the recorder will have the most recently observed MKB for content protection use.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 July 2006 (20.07.2006)

PCT

(10) International Publication Number
WO 2006/074987 A3

(51) International Patent Classification:
H04L 9/00 (2006.01) *H04L 9/08* (2006.01)

(21) International Application Number:
PCT/EP2006/050099

(22) International Filing Date: 9 January 2006 (09.01.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/905,570 11 January 2005 (11.01.2005) US

(71) Applicants *(for all designated States except US)*: **INTERNATIONAL BUSINESS MACHINES CORPORATION** [US/US]; New Orchard Road, Armonk, New York 10504 (US). **THE WALT DISNEY COMPANY** [US/US]; 500 South Buena Vista Street, Burbank, California 91521-0178 (US).

(71) Applicant *(for MG only)*: **IBM UNITED KINGDOM LIMITED** [GB/GB]; P.O. Box 41, North Harbour, Portsmouth, Hampshire PO6 3AU (GB).

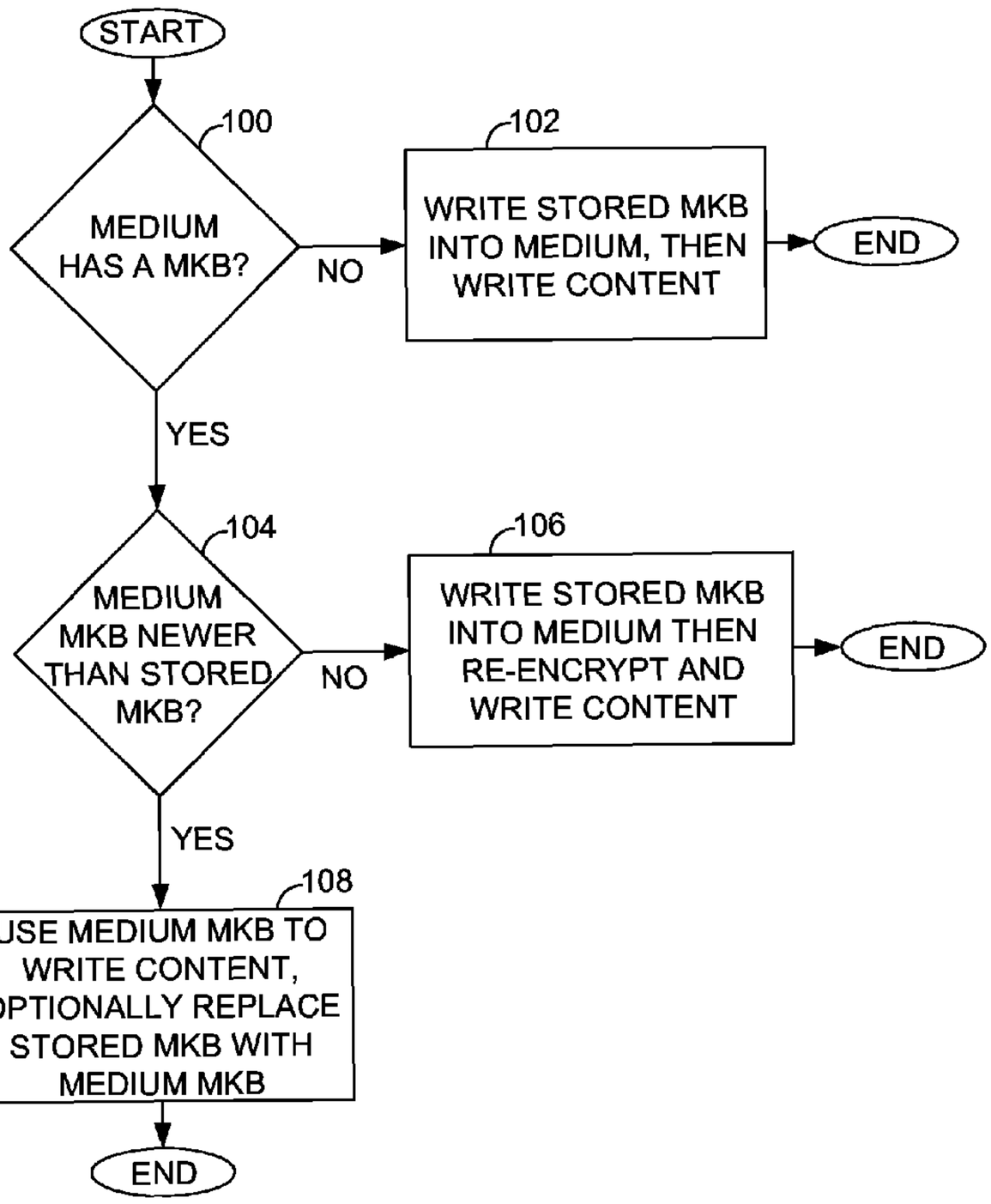
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **LOTSPIECH, Jeffrey, Bruce** [US/US]; 2858 Hartwick Pines Drive, Henderson, Nevada 89052 (US). **WATSON, Scott, Frazier** [US/US]; 15355 Michael Crest, Santa Clarita, California 91387 (US).

(74) Agent: **SEKAR, Anita**; IBM United Kingdom Limited, Intellectual Property Law, Hursley Park, Winchester, Hampshire SO21 2JN (GB).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: 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,

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR CONTROLLING ACCES TO PROTECTED DIGITAL CONTENT BY VERIFICATION OF A MEDIA KEY BLOCK



(57) Abstract: A recorder system contains a media key block (MKB) and selectively writes protected content into a recording medium according to the following content protection logic, to combat theft of the protected content: If the medium does not have a MKB, then the recorder writes its stored MKB into the medium and writes protected content into the medium. If the medium has a MKB that is older than the stored MKB in the recorder, then the recorder writes its stored MKB into the medium before re-encrypting and writing protected content into the medium. If the medium has a MKB that is newer than the stored MKB, then the MKB in the medium is used for content protection. The recorder may store the newer MKB in non-volatile memory, effectively updating its previous stored MKB, so the recorder will have the most recently observed MKB for content protection use.

WO 2006/074987 A3

WO 2006/074987 A3

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 States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (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).

Published:

— *with international search report*

(88) Date of publication of the international search report:
28 December 2006

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

READ/WRITE MEDIA KEY BLOCK

Field of the Invention

The present invention generally relates to the management of cryptographic keys for controlling access to protected content, particularly for recordable media.

Background of the Invention

The advantages of digitized video and music are numerous, but one significant drawback is that being digitized, the content is relatively easy to copy perfectly, without authorization by the copyright owner. Pirating of content currently costs content providers billions of dollars each year. Therefore, numerous schemes have been developed to address this problem, but not all are practical given the large number of content instances and devices that handle content.

U.S. Pat. No. 6,118,873 provides an encryption system for the secure broadcasting of programs, including updates to authorized in-home digital video devices. That patent discloses a system for encrypting broadcast music, videos, and other content such that only authorized player-recorders can play and/or copy the content and only in accordance with rules established by the vendor of the content. Authorized players or recorders are issued software-implemented device keys from a matrix of device keys termed a media key block (MKB). The keys can be issued simultaneously with each other or over time, but in any event, no player-recorder is supposed to have more than one device key per column of the matrix. Although two devices might share the same key from the same column, the chances that any two devices share exactly the same set of keys from all the columns of the matrix are very small when keys are randomly assigned. The keys are used to decrypt content. Devices may be 'revoked' by encrypting future protected content in various ways such that particular selected devices cannot decrypt it properly.

In the case of recordable media, content protection is conventionally based on having a media key block on each media instance (in this application, the term "media" may refer to a particular data storage item or a plurality of such data storage items). This MKB allows compliant devices to calculate a proper media key, while preventing circumvention devices from doing the same thing. Heretofore, it has been important that

the MKB be read-only, even though the rest of the medium is, of course, read/write, i.e. recordable. The MKB needs to be read-only because of the following so-called "down-level media" attack: if the MKB were read/write, an attacker could write an old broken MKB on the medium, and then ask a compliant device to encrypt and record a piece of content of interest to the attacker. Since the MKB is broken, the attacker knows the media key and can decrypt this content. The attacker thus gets the protected content in the clear, effectively defeating the goal of the content protection scheme.

However, having a read-only area on read/write media is often problematic. For example, in DVD-RAM, DVD-R, and DVD-R/W media, the MKB is pre-embossed on the lead-in area, a part of the disc not written into by recorders. The lead-in area has a limited capacity. Therefore, this approach inherently limits the size of the MKB, thereby restricting the number of circumvention devices that can be revoked. In the case of DVD+R and DVD+R/W media, the lead-in area is read/write. The approach used in that technology is to write only a digest of the MKB into the "burst cut area" (BCA), a very limited read-only area near the hub of the disc, during manufacture. Writing into the BCA adds another $0.05 to the cost of each disc, unfortunately.

A potentially more serious problem is that these approaches require the disc replicator to be involved in the process. Not all disc replicators wish to become licensees of the given content protection scheme, so to date each type of media has two versions: one with MKBs, and one without. Since only the MKB-containing media can be used to record protected content, there is substantial potential for consumer confusion. Furthermore, the disc replicators have to be constrained by license not to put too many discs out with the same MKB. If they did, the media key of that MKB could become an important global secret, the compromise of which could do serious damage to the content protection scheme. But there is a cost/security tradeoff involved, because the cost of replication is strongly dependent on the number of identical replicas that can be made. To date, that tradeoff has been made entirely to favor low cost: the replicators are allowed to use a single MKB a million times.

Disclosure of the Invention

Accordingly, there is provided a computer-implemented method for combating theft of protected digital content by verification of a media key block (MKB) in a recording medium, comprising: a) storing a MKB in a

recording device; b) if the medium does not have a MKB, then writing the stored MKB onto the medium before writing the content into the medium; c) if the medium has a MKB that is older than the stored MKB, then writing the stored MKB into the medium, re-encrypting and writing the content into the medium; and d) if the medium has a MKB that is newer than the stored MKB, then using the MKB in the medium for content protection.

The present invention provides a read-only MKB stored in each recorder device, instead of having read-only MKBs on blank media from disc replicators. The recorder device selectively writes protected digital content onto a recording medium according to the age of the stored MKB and any MKB that may be present in the recording medium. If there is no MKB in the medium, the recorder writes its stored MKB into the medium and then proceeds to write the protected content. If the MKB in the medium is older than the stored MKB, then the recorder writes the stored MKB into the medium and then re-encrypts the protected content and then writes it, eliminating the possibility that a broken older MKB can be used for piracy. If the MKB in the medium is newer than the stored MKB, then the recorder uses the newer MKB for writing protected content, but can optionally update its stored MKB with the newer MKB, eliminating the possibility that a broken older stored MKB can be used for piracy.

Preferably, there is provided a system for combating theft of protected digital content, comprising a recording device storing a media key block (MKB) and selectively writing the content into the medium according to logical rules including: if the medium does not have a MKB, then writing the stored MKB into the medium before writing the content into the medium; if the medium has a MKB that is older than the stored MKB, then writing the stored MKB into the medium, re-encrypting and writing the content into the medium; and if the medium has a MKB that is newer than the stored MKB, then using the MKB in the medium for content protection.

Any recordable medium having a unique media ID or serial number can be employed by the system to store protected content. Costly modifications to media during manufacture can be avoided, and limitations to the size of MKBs are effectively eliminated.

Brief Description of the Drawings

The present invention will now be described, by way of example only, with reference to preferred embodiments thereof, as illustrated in the following drawings:

Figure 1 is a flowchart of steps taken to combat theft of protected digital content through media key block validation, according to an embodiment of the invention.

Detailed Description of the Preferred Embodiments

In an exemplary embodiment, the present invention eliminates the difficulties described above by having a read-only MKB stored in each recorder device, instead of having read-only MKBs on blank media from disc replicators. The recorder can selectively write the stored MKB onto the media. There are several schemes known in the art for efficiently enabling a device to cryptographically determine which of two keys is the more recent, so the invention capitalizes on these schemes to help solve the problems with the conventional approaches described above. See for example U.S. Pat. No. 5,081,677 and U.S. Pat. No. 5,412,723, which describe the use of version numbers for cryptographic keys that are periodically "refreshed" for enhanced security. Note however that the invention is not limited to any specific scheme for determining the relative age of keys or MKBs.

Therefore, referring now to Figure 1 and according to the present invention, when a recorder is asked to record a piece of protected content, the content protection logic followed in the recorder is as follows:

1. If the media has no MKB, as determined in step 100, then in step 102 the recorder first writes its own MKB into the media before writing the content protected by that MKB.

2. Otherwise, the recorder compares the existing MKB on the media with its own MKB in step 104. If the MKB on the media is older, then in step 106 the recorder replaces the MKB on the media with its own. As part of that replacement, the recorder must re-encrypt all titles currently on the media with a key based on the newer (i.e. the recorder's) media key.

3. If the MKB on the media is more recent, then in step 108 the recorder uses the MKB on the media instead of its own. If the recorder has its own internal non-volatile memory, then it can store the more recent MKB in that memory, and then from that point on use the more recent MKB as its own MKB for content protection.

Thus, with the present invention, MKBs no longer have any practical restriction in size. Also, any piece of blank media can be used as content-protected media, as long as it has a unique serial number or media ID, so consumer confusion is avoided. (If cloned serial numbers were used, those pieces of identical media could be used to make unauthorized copies by just making a bit-for-bit copy.) Finally, since recorder-player devices already employ programmable read-only memory for unique device keys, having a unique MKB per device would only require slightly more programmable storage, not a new and costly disc manufacturing step. Therefore, with the present invention, the chance that media keys could become global secrets would be greatly reduced.

There are some subtleties, however. If the MKB changes, then every encrypted title key has to be updated, and recorders generally are not cognizant of all possible formats of content. They do not know where the encrypted title keys are stored for the unknown formats, and thus are not able to re-encrypt them when they change the MKB. This problem is solved simply by having different MKBs for different formats. The recorder only updates MKBs of the formats it understands. However, a "backup MKB" protocol may be defined so that content is not lost if a recorder fails during the updating. An exemplary backup MKB protocol is as follows:

If the encrypted title keys are in a single file, then the recorder renames the old encrypted title keys to a defined backup name before beginning to write the new encrypted title keys file via these logical steps:

1. Check to see if both a backup MKB and a backup encrypted title keys file exists. If they both exist then go to step 2, else erase the remaining backup file and exit.

2. If the current MKB does not exist or is corrupt then rename the backup MKB and backup encrypted title keys file to the current files and exit.

3. Decrypt the title keys in the backup title keys file using the backup MKB, and re-encrypt the title keys using the current MKB, writing the current title keys file.

4. Delete the backup MKB and the backup title keys file, modifying any nonce associated with the backup encrypted title key file.

In some applications, encrypted title keys may be found in more than one file. In that case, the recorder runs the backup protocol separately for each file, not deleting the backup MKB until all title keys files have been processed.

Further, if the MKB is simply a file in a file system, it might be difficult for the recorder to find it (i.e. for optical media, the disc drive authentication requires the disc to read the MKB, but from where?). Disc drives are not accustomed to understanding the format of the file system on the disc and would prefer to simply access data at fixed locations on the disc. This preference can be accommodated by having the disc format operation place the MKB at a pre-defined location on the disc, in addition to placing it logically in the file system. Subsequent MKBs can simply overwrite a previous MKB in the same place. Recorders must not accept discs that have not been correctly formatted, and must be able to format them themselves and then write an "authentication MKB". Recorders must undoubtedly perform the formatting for other reasons. The authentication MKB should be in addition to all the format-specific MKBs, and the recorder must be prepared to update any MKB that it knows. It always knows about the authentication MKB.

Historically, attackers who want to use circumvention programs save old media for a down-level media attack, as they hope that those MKBs will be broken. This invention changes the nature of the attacks possible against the content protection scheme. For example, in the current state of the art, the attackers employ an attack where they save media that comes out when the scheme was first introduced, before there were any revocations. Once circumvention devices (e.g. rogue recorders) appear, they will be revoked for new media, but will still be able to use the old media. Next, the attackers ask compliant recorders to record content on the old media. The attackers then use the circumvention device to make unauthorized copies. This attack is somewhat obviated by MKB extensions, which the attacker must avoid, but MKB extensions are always optional.

In the present invention, the analogous attack proceeds as follows: the attacker buys devices (instead of media) that come out when the scheme is first introduced. These old recorders format media with old media key blocks. The attackers ask the old devices to record content, and then use the circumvention devices to make unauthorized copies. The attacker has to avoid using a particular media in a new recorder - the attack becomes even more difficult if the recorders have non-volatile storage for the latest updated MKB they've seen for subsequent writing use.

What if a rogue replicator clones the supposedly unique IDs of the media? In this case, in both the prior art and in the present invention, the only recourse is legal. Consider the legal situation in the current state of the art. If the replicator has licensed the content protection scheme and built cloned media, he is in violation of that license. If he is not a licensee, then he has violated the intellectual property of the content protection scheme: the copyrighted MKB, the trade secrets, and the relevant patents. In either case, the replicator might be accused of having circumvented "technical protection means" and be liable to prosecution under the U.S. Digital Millennium Copyright Act (DMCA).

The present invention allows the possibility that replicators need not be licensees of the content protection scheme. If the replicator need not be a licensee, then all media will be usable for content protection, and there will be less chance of user confusion. In this case, the content protection scheme's owners might have no status in court if a replicator is cloning, and protection falls back on the strength of the DMCA. However, replicators must always be licensees of the particular media format. If the format license makes the reasonable demand that unique IDs must actually be unique, then the legal situation reverts to the way it was before the present invention. It is just that the format owner, not the content protection scheme owner, is now the legally injured party.

If for some reason this situation is not satisfactory, the content protection scheme can add some licensable element to the media. The media ID might be divided into two parts, for example, a unique ID and an encryption of that ID with a secret key available only with the license. Player devices would be given the key so they can check that the two halves match. Players would only play licensed media. However, this license would presumably be less onerous to the replicators, because it would no longer restrict the number of replicas, and need not require an ongoing license fee. It is possible that all replicators would choose to be licensees under these terms, and consumer confusion would be avoided.

It is also within the scope of this invention to have the replicators initially record the authentication MKB at the time of media manufacture. In that case, the consumer confusion problem returns, but the security of the content protection scheme is increased as the attack mentioned before now requires both an old media and an old player to succeed.

A general purpose computer is programmed according to the inventive steps herein. The invention can also be embodied as an article of manufacture - a machine component - that is used by a digital processing apparatus to execute the present logic. This invention is realized in a critical machine component that causes a digital processing apparatus to perform the inventive method steps herein. The invention may be embodied by a computer program that is executed by a processor within a computer as a series of computer-executable instructions. These instructions may reside, for example, in RAM of a computer or on a hard drive or optical drive of the computer, or the instructions may be stored on a DASD array, magnetic tape, electronic read-only memory, or other appropriate data storage device.

The particular READ/WRITE MEDIA KEY BLOCK as herein shown and described is the presently preferred embodiment of the present invention and is thus representative of the subject matter which is broadly contemplated by the present invention, that the scope of the present invention fully encompasses other embodiments which may become obvious to those skilled in the art, and that the scope of the present invention is accordingly to be limited by nothing other than the appended claims, in which reference to an element in the singular is not intended to mean "one and only one" unless explicitly so stated, but rather "one or more". All structural and functional equivalents to the elements of the above-described preferred embodiment that are known or later come to be known to those of ordinary skill in the art are expressly incorporated herein by reference and are intended to be encompassed by the present claims. Moreover, it is not necessary for a device or method to address each and every problem sought to be solved by the present invention, for it to be encompassed by the present claims. Furthermore, no element, component, or method step in the present disclosure is intended to be dedicated to the public regardless of whether the element, component, or method step is explicitly recited in the claims. No claim element herein is to be construed under the provisions of 35 U.S.C. 112, sixth paragraph, unless the element is expressly recited using the phrase "means for".

CLAIMS

1. A computer-implemented method for controlling access to protected digital content by verification of a media key block (MKB) in a recording medium, comprising:

a) storing a MKB in a recording device;

b) if the medium does not have a MKB, then writing the stored MKB onto the medium before writing the content into the medium;

c) if the medium has a MKB that is older than the stored MKB, then writing the stored MKB into the medium, re-encrypting and writing the content into the medium; and

d) if the medium has a MKB that is newer than the stored MKB, then using the MKB in the medium for content protection.

2. The method of claim 1 wherein the re-encrypting includes re-encrypting all titles in the medium with a key based on a new media key.

3. The method of claim 1 or claim 2 wherein step d further comprises replacing the stored MKB with the newer MKB in non-volatile memory in the recording device.

4. The method of any preceding claim wherein the recording device uses different format-specific MKBs for differently formatted content.

5. The method of any preceding claim wherein the recording device writes an authentication MKB into the medium.

6. The method of any preceding claim wherein MKBs are at pre-defined locations in the medium.

7. The method of any preceding claim wherein the recording device updates MKBs only for known formats.

8. The method of any preceding claim wherein a backup MKB protocol protects content if the recording device fails during writing.

9. The method of any preceding claim wherein an authentication MKB is written into the medium during manufacture.

10. The method of any preceding claim further comprising adding a licensable element to the medium.

11. The method of claim 10 wherein the licensable element comprises a media ID including an unencrypted unique ID and an encryption of that unique ID with a secret key available only with a license.

12. The method of claim 11 wherein the medium is validated if the decryption of the encrypted unique ID using the secret key matches the unique ID.

13. A system for controlling access to protected digital content by verification of a media key block (MKB) in a recording medium, comprising:

a) means for storing a MKB in a recording device;

b) means for, if the medium does not have a MKB, writing the stored MKB into the medium before writing the content into the medium;

c) means for, if the medium has a MKB that is older than the stored MKB, writing the stored MKB into the medium, re-encrypting and writing the content into the medium; and

d) means for, if the medium has a MKB that is newer than the stored MKB, using the MKB in the medium for content protection.

14. The system of claim 13 wherein the re-encrypting includes re-encrypting all titles in the medium with a key based on a new media key.

15. The system of claim 13 or claim 14 wherein the recording device replaces the stored MKB with the newer MKB in non-volatile memory in the recording device.

16. The system of any of claims 13 to 15 wherein the recording device uses different format-specific MKBs for differently formatted content.

17. The system of any of claims 13 to 16 wherein the recording device writes an authentication MKB into the medium.

18. The system of any of claims 13 to 17 wherein MKBs are at pre-defined locations in the medium.

19. The system of any of claims 13 to 18 wherein the recording device updates MKBs only for known formats.

20. The system of any of claims 13 to 19 wherein a backup MKB protocol protects content if the recording device fails during writing.

21. The system of any of claims 13 to 20 wherein an authentication MKB is written into the medium during manufacture.

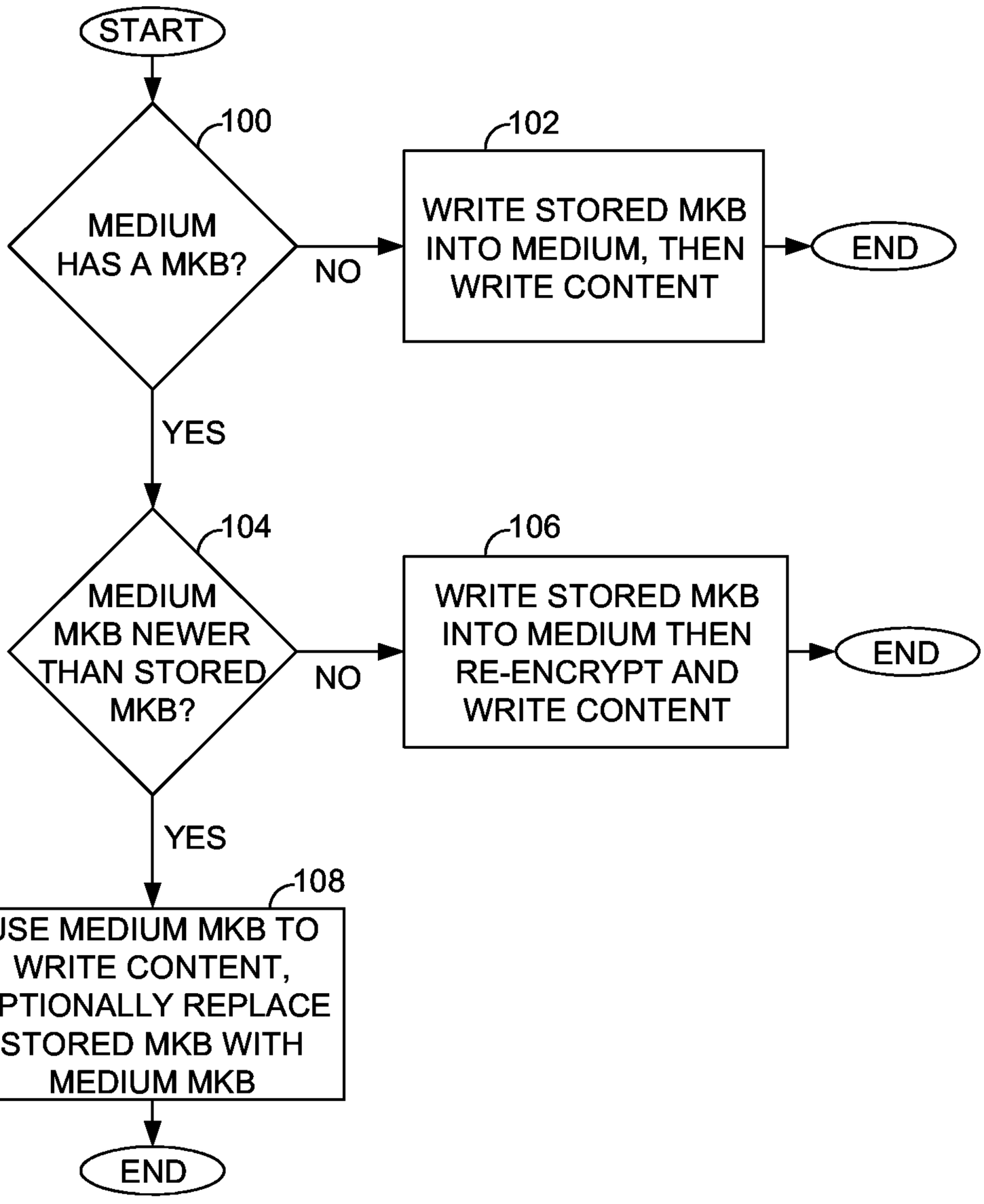
22. The system of any of claims 13 to 21 wherein a licensable element is added to the medium.

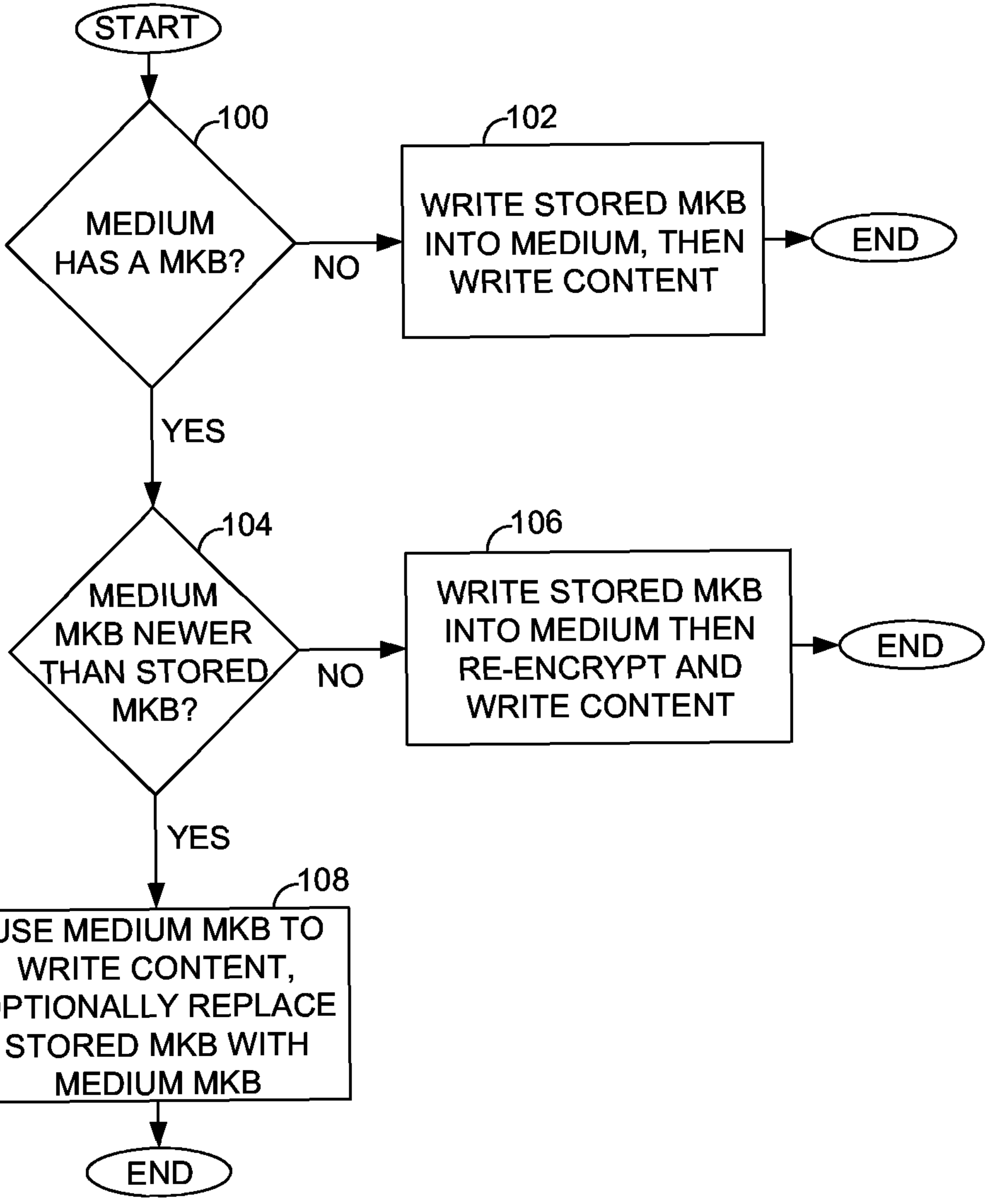
23. The system of claim 22 wherein the licensable element comprises a media ID including an unencrypted unique ID and an encryption of that unique ID with a secret key available only with a license.

24. The system of claim 23 wherein the medium is validated if the decryption of the encrypted unique ID using the secret key matches the unique ID.

25. A computer program comprising program code means adapted to perform all the steps of any of claims 1 to 12 when said program is run on a computer.

FIG. 1


START
100
MEDIUM HAS A MKB?
NO
102
WRITE STORED MKB INTO MEDIUM, THEN WRITE CONTENT
END
YES
104
MEDIUM MKB NEWER THAN STORED MKB?
NO
106
WRITE STORED MKB INTO MEDIUM THEN RE-ENCRYPT AND WRITE CONTENT
END
YES
108
USE MEDIUM MKB TO WRITE CONTENT, OPTIONALLY REPLACE STORED MKB WITH MEDIUM MKB
END


START
100
MEDIUM HAS A MKB?
NO
102
WRITE STORED MKB INTO MEDIUM, THEN WRITE CONTENT
END
YES
104
MEDIUM MKB NEWER THAN STORED MKB?
NO
106
WRITE STORED MKB INTO MEDIUM THEN RE-ENCRYPT AND WRITE CONTENT
END
YES
108
USE MEDIUM MKB TO WRITE CONTENT, OPTIONALLY REPLACE STORED MKB WITH MEDIUM MKB
END