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

(19) **World Intellectual Property Organization**
International Bureau

(43) **International Publication Date**
19 April 2007 (19.04.2007)

PCT

(10) **International Publication Number**
WO 2007/044825 A2

(51) **International Patent Classification:**
G06Q 99/00 (2006.01) ***H04K 1/00*** (2006.01)
H04L 9/00 (2006.01)

(21) **International Application Number:**
PCT/US2006/039778

(22) **International Filing Date:** 10 October 2006 (10.10.2006)

(25) **Filing Language:** English

(26) **Publication Language:** English

(30) **Priority Data:**
11/249,123 11 October 2005 (11.10.2005) US

(71) **Applicant** *(for all designated States except US)*: **APPLE COMPUTER, INC.** [US/US]; 1 Infinite Loop, Cupertino, CA 95014 (US).

(72) **Inventors; and**
(75) **Inventors/Applicants** *(for US only)*: **FARRUGIA, Augustin, J.** [FR/US]; 10411 Tula Lane, Cupertino, CA 95014 (US). **DOWDY, Thomas** [US/US]; 1610 Kamsack Drive, Sunnyvale, CA 94087 (US). **FASOLI, Gianpaolo** [US/US]; 684 Hawthorne Avenue, Pala Alto, CA 94301 (US).

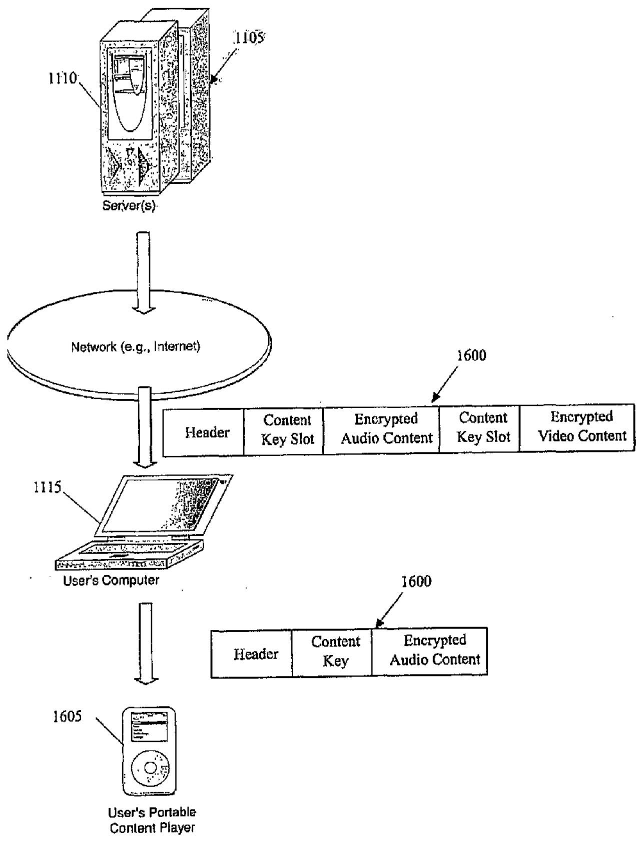
(74) **Agent: ADELI, Mani**; 1875 Century Park East, Suite 1360, Los Angeles, CA 90067 (US).

(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, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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,

[Continued on next page]

(54) **Title:** USE OF MEDIA STORAGE STRUCTURE WITH MULTIPLE PIECES OF CONTENT IN A CONTENT-DISTRIBUTION SYSTEM



(57) **Abstract:** Some embodiments of the invention provide a method for distributing content over a network. The method distributes a single media storage structure to a device (e.g., a computer, portable player, etc.) that connects to the network. The media storage structure includes first and second pieces of encrypted content. Based on whether the device is allowed to access the first piece of content, the second piece of content, or both, the method provides the device with a set of keys for decrypting the pieces of the content that the device is able to access. The provided set of keys might include one or more keys for decrypting only one of the two encrypted pieces of content. Alternatively, it might include one or more keys for decrypting both encrypted pieces of content. For instance, the selected set of keys might include a first key for decrypting the first encrypted piece and a second key for decrypting the second encrypted piece. Based on the provided set of keys, the device can then decrypt and access either one of the two pieces of content in the media storage structure or both pieces of encrypted content in the media storage structure.

RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

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.

UNITED STATES PATENT APPLICATION FOR

USE OF MEDIA STORAGE STRUCTURE WITH MULTIPLE PIECES OF CONTENT IN A CONTENT-DISTRIBUTION SYSTEM

FIELD OF THE INVENTION

The present invention relates to the use of a single media storage structure with multiple pieces of content in a digital rights management system.

BACKGROUND OF THE INVENTION

The protection of digital content transferred between computers over a network is fundamentally important for many enterprises today. Enterprises attempt to secure this protection by implementing some form of Digital Rights Management (DRM) process. The DRM process often involves encrypting the piece of content (e.g., encrypting the binary form of the content) to restrict usage to those who have been granted a right to the content.

Cryptography is the traditional method of protecting data in transit across a network. In its typical application, cryptography protects communications between two mutually trusting parties from an attack on the data in transit. However, for many digital file transfer applications today (e.g., for the transfer of audio or video content), the paradigm has shifted, as a party that receives the content (i.e., the "receiving party") might try to break the DRM encryption that the party that supplied the content (i.e., the "distributing party") applied to the content. In addition, with the proliferation of network penetration attacks, a third party may obtain access to the receiving party's computer and thus to the protected content.

Some pieces of content that are distributed in existing DRM systems are related to one another. However, existing DRM system often do not allow content recipients to flexibly purchase or license a subset of the contents from a related set of DRM contents. For instance, one existing DRM system distributes certain songs along with their associated music videos. In distributing a song along with its associated music video, this DRM system rigidly requires a recipient either (1) to purchase both the song and its associated music video, or (2) to forego access to both the song and its associated music video. Therefore, there is a need in the art for a DRM system that flexibly allows content recipients to purchase or license a subset of the content from a related set of DRM contents.

SUMMARY OF THE INVENTION

Some embodiments of the invention provide a method for distributing content over a network. The method distributes a single media storage structure to a device (e.g., a computer, portable player, etc.) that connects to the network. The media storage structure includes first and second pieces of encrypted content. Based on whether the device is allowed to access the first piece of content, the second piece of content, or both, the method provides the device with a set of keys for decrypting the pieces of the content that the device is able to access.

The provided set of keys might include one or more keys for decrypting only one of the two encrypted pieces of content. Alternatively, it might include one or more keys for decrypting both encrypted pieces of content. For instance, the selected set of keys might include a first key for decrypting the first encrypted piece and a second key for decrypting the second encrypted piece. Based on the provided set of keys, the device can then decrypt and access either one of the two pieces of content in the media storage structure or both pieces of encrypted content in the media storage structure.

The media storage structure includes a first content section that stores the first piece of encrypted content, and a second content section that stores the second piece of encrypted content. In some embodiments, the media storage structure also includes first and second key sections respectively for storing first and second keys for decrypting the first and second pieces of encrypted content. The method of some embodiments distributes the media storage structure with the encrypted first and second content pieces from a computer that is separate from the computer or computers that distribute the first and second keys. In some embodiments, the device that receives the media storage structure inserts the first and second keys in the first and second key sections of the media storage structure.

One piece of encrypted content might be audio content (e.g., an audio track, a song, a sound track, etc.) related to a particular presentation (e.g., a music video, a film, etc.), while the other piece of encrypted content might be video content (e.g., a video track, a video clip, etc.) related to the particular presentation. Alternatively, both pieces of content can be video content (e.g., video clips from different angles of one or more scenes) or audio content (e.g., different versions or mixes of a song or different languages for the dialogue in a movie). In addition, content other than audio or video might be stored in the media storage structure. For instance, one piece of content might be audio or video content, while the other piece of content might be lyrics or dialogue associate with the audio or video content piece.

The method in some embodiments distributes a media storage structure that contains more than two pieces of content. For instance, in some cases, the media storage structure includes one piece of audio content and two pieces of video content, which can be two different video clips associated with the audio content (e.g., can be two different music videos that are associated with a song).

In some embodiments, the device (e.g., the computer) that receives the media storage structure transfers the media storage structure to another device (e.g., to a portable player). In this transfer, one of the pieces of content from the media storage structure might be removed in the transfer of the media storage structure to the other device (e.g., in the portable player). In some cases, content is removed from the media storage structure in order to reduce the consumption of resources on the other device. In other cases, content is removed from the media storage structure because the other device does not have rights to access this other content.

BRIEF DESCRIPTION OF THE DRAWINGS

The novel features of the invention are set forth in the appended claims. However, for purpose of explanation, several embodiments are set forth in the following figures.

Figure 1 illustrates an example of such a media storage structure.

Figure 2 illustrates an example where the selected set of keys includes a first key for decrypting the first encrypted piece of content and a second key for decrypting the second encrypted piece of content.

Figure 3 illustrates another example of the media storage structure.

Figures 4-10 illustrate various examples of related pieces of content in a media storage structure of some embodiments.

Figure 11 illustrates a content-distribution system of some embodiments.

Figure 12 conceptually illustrates an example of one possible set of interactions between the computer, the DRM server, and the content-caching server.

Figure 13 illustrates another example of a computer acquiring a media file.

Figure 14 illustrates a computer's storage of the two keys that it receives in the example illustrated in **Figure 11**.

Figure 15 illustrates a computer's storage of the key that it receives in the example illustrated in **Figure 13**.

Figure 16 illustrates an example of the computer synchronizing its DRM content with a portable player.

Figure 17 conceptually illustrates a process that a computer performs in some embodiments to synchronize a set of content with a portable player.

DETAILED DESCRIPTION OF THE INVENTION

In the following description, numerous details are set forth for the purpose of explanation. However, one of ordinary skill in the art will realize that the invention may be practiced without the use of these specific details. In other instances, well-known structures and devices are shown in block diagram form in order not to obscure the description of the invention with unnecessary detail.

I. MEDIA STORAGE STRUCTURE

Some embodiments of the invention provide a content-distribution system for distributing unitary media storage structures to devices (e.g., computers, portable players, etc.) that connect to a network. Each unitary media storage structure includes a set of related pieces of content. In at least some unitary media storage structures of some embodiments, each piece of content is separately encrypted to protect it from unauthorized use. Examples of pieces of content include video, audio, text, sound, etc.

Figure 1 conceptually illustrates an example of a unitary media storage structure 100 of some embodiments. As shown in this figure, the media storage structure includes first and second pieces 105 and 110 of encrypted content. It also includes first and second sections 115 and 120 for containing first and second cryptographic keys for decrypting the first and second pieces 105 and 110 of content. The media storage structure also includes a header 125 that includes metadata regarding the content in the media storage structure.

Based on whether the device is allowed to access the first piece of content 105, the second piece of content 110, or both, the system provides the device with a set of keys for decrypting the pieces of the content that the device is able to access. The provided set of keys might include only one key for decrypting only one of the two encrypted pieces of content. Alternatively, it might include two keys for decrypting both encrypted pieces of content.

For instance, **Figure 2** illustrates an example where the selected set of keys includes a first key 215 for decrypting the first encrypted piece of content 105 and a second key 220 for decrypting the second encrypted piece of content 110. **Figure 3** illustrates another example of the media storage structure 100. In this example, the media storage structure 100 includes only the second key 220 for decrypting the second piece of encrypted content 110.

Based on the set of keys that the system provides to the device, the device can decrypt and access either one of the two pieces of content 105 and 110 or both pieces of encrypted content. The system of some embodiments distributes the media storage structure with the encrypted first and second content pieces 105.and 110 from a computer that is separate from the computer or computers that distribute the first and second keys 215 and 220 for decrypting the first and second pieces of encrypted content.

While this application describes receiving, storing, manipulating and using a "key," it will be understood that a host of know techniques can be used to disguise the key. For example, key hiding, key encryption, splitting the key into more than one piece to be stored separately, and obfuscation of read/write operations, can all be used and are considered within the general concept of receiving, storing, and using a "key."

As mentioned above, the single media storage structure that is distributed by some embodiments includes a set of related pieces of content. In some embodiments, two pieces of content are related when they relate to the same audio and/or video presentation (e.g., song, movie, music video, etc.). In some cases, two pieces of related content can be viewed or played simultaneously. In other cases, two pieces of related content can be viewed or player independently.

Figures 4-10 illustrate various examples of related pieces of content in a media storage structure of some embodiments. **Figure 4** illustrates an example of a storage structure 400 where one piece of encrypted content is audio content 405 (e.g., an audio track, a song, a sound track) related to a particular presentation (e.g., a music video, a film, etc.), while the other piece of encrypted content is video content 410 (e.g., a video track, a video clip, etc.) related to the particular presentation.

Figure 5 illustrates a storage structure 500 that includes two pieces of video content. One example of two such pieces of video content would be two video clips that are shot from different angles to cover one or more scenes in a movie. A piece of video content might also include audio content associated with its video content or might only include video data. **Figure 6** illustrates a storage structure 600 that includes two pieces of audio content. One example of two such pieces of audio content would be two different versions or mixes of a song.

Content other than audio or video might be stored in the media storage structure of the some embodiments of the invention. For instance, **Figure 7** illustrates a media storage structure 700 that stores one piece of audio content 705 and another piece of textual content 710, which might be lyrics, dialogue, or other data associated with the audio content 705. Similarly, **Figure 8** illustrates a media storage structure 800 that stores one piece of video content 805 and another piece of textual content 810, which might be dialogue associate with the video content 805.

In some cases, the system distributes a media storage structure that contains more than two pieces of content. For instance, **Figure 9** illustrates a media storage structure 900 that includes one piece of audio content (e.g., a song) along with two pieces of video content, which can be two different video clips associated with the audio content (e.g., can be two different music videos that are associated with the song). Similarly, **Figure 10** illustrates a media storage structure 1000 that includes one piece of video content (e.g., a movie) along with two pieces of audio content, which can be the video's audio component in two different languages.

In the various examples illustrated in **Figures 4-10**, the media storage structure includes a key for decrypting each piece of content stored in the media storage structure. As mentioned above, the content-distribution system of some embodiments allows different set of keys to be acquired (e.g., purchased or licensed) for accessing a media storage structure on a particular device. In some embodiments, the device stores the acquired set of keys in the media storage structure, and uses the acquired set of keys to decrypt and access the media storage structure's content that has been purchased or licensed for access on the device. Once decrypted, the device can individually or simultaneously view or play the decrypted pieces of content.

In some embodiments, the device (e.g., the computer) that receives the media storage structure transfers the media storage structure to another device (e.g., to a portable player). In this transfer, one of the pieces of content from the media storage structure might be removed in the transfer of the media storage structure to the other device (e.g., in the portable player). In some cases, one of the pieces of content is removed in order to reduce the consumption of resources on the other device.

Some embodiments above were illustrated by reference to a media storage structure that itself includes a plurality of sections available for storage of keys. Such storage sections can be incorporated into many media file formats, including the Quicktime file format, Windows Media file format, Real media format, ISO/IEC 14496-12, Motion JPEG, etc. One of ordinary skill will realize that in some embodiments the keys are alternatively stored and transferred separately from the unitary media files to which they pertain.

II. CONTENT-DISTRIBUTION SYSTEM

Figure 11 illustrates a content-distribution system 1100 of some embodiments. This content-distribution system distributes content in a manner that protects the digital rights (i.e., ensures the legal use) of the content. To distribute content that is related, the system distributes single media storage structures with multiple related pieces of content. In this example, the media storage structures are media files. One of ordinary skill will realize that other embodiments might use other types of storage structures.

As shown in **Figure 11**, the content-distribution system 1100 includes a content-caching server 1105, a DRM server 1110, and a content-receiving computer 1115. The computer 1115 connects to the servers 1105 and 1110 through a computer network, such as a local area network, a wide area network, a network of networks (e.g., the Internet), etc.

Through this connection, the computer 1115 communicates with the DRM server 1110 to obtain content. In some embodiments, the content-distribution system 1100 does not entail the sale or licensing of content. Accordingly, in these embodiments, the DRM server 1110 simply enforces the distribution of content to authorized computers without considering any financial objectives.

For purposes of illustration, however, several embodiments of the content-distribution system 1100 that are described below are involved in the sale or licensing of the content. Accordingly, in these embodiments, the DRM server 1110 is the server from which the user of the computer 1115 can purchase or license content. In other words, the DRM server 1110 of some embodiments is the server that handles the financial transaction for purchasing or licensing content. In some instance, certain content can be purchased or licensed free.

After the DRM server 1110 determines that the computer 1115 can obtain the content, the content-distribution system 1100 uses the content caching server 1105 to provide a media storage file that contains one or more pieces of DRM content to the computer 1115 through the network 1120. In some embodiments, the system 1100 uses multiple caching servers 1105 to cache content at various locations on the network, in order to improve the speed and efficiency of downloading content across the network. For each media storage file that the DRM server 1110 directs the caching server 1105 to provide to the computer 1115, the DRM server 1110 provides a set of keys for the computer to use to decrypt the content that is stored in the media storage file.

Figure 12 conceptually illustrates an example of one possible set of interactions between the computer 1115, the DRM server 1110, and the content-caching server 1105. This set of interactions represents a content-acquisition process 1200 of some embodiments of the invention. As shown in this figure, the acquisition process 1200 starts when the computer 1115 sends (at 1205) a request to the DRM server 1110 to purchase or license one or more pieces of content that are stored in a particular media file. At 1210, the DRM server receives this request.

The acquisition process then has the DRM server 1110 and/or purchasing computer 1115 perform one or more operations (at 1215) to complete the purchase or license transaction. After the transaction has been completed, the DRM server 1110 sends (at 1215) a request to the content-caching server 1105 to send the media file for the purchased or licensed content to the computer 1115.

The caching server 1105 receives this request at 1225, and in response, commences (at 1230) a download of the media file to the purchasing computer 1115. **Figure 11** illustrates an example of a media file 1125 that the content caching server 1105 downloads to the computer 1115. In this example, the media file has five sections. The first and second section 1145 and 1155 contain two pieces of encrypted content. Each piece of content is encrypted using a particular content key. The third and fourth sections 1150 and 1160 are empty sections in the file for the insertion of the content keys if such content keys are purchased or licensed by the computer 1115. Lastly, the fifth section 1165 is a header field, which contains metadata regarding the content and/or content keys.

The computer 1115 receives (at 1235) the media file provided by the caching server. The computer 1115 then sends (at 1240) a confirmation of the download to the DRM server 1110. After 1220, the DRM server 1110 transitions to a wait state 1245 to wait for the confirmation to be received from the computer 1115.

Once the DRM server 1110 receives the confirmation of the download at 1245, it sends (at 1250) to the computer 1115 a set of keys based on the pieces of content that the computer 1115 purchased or licensed. In the example illustrated in **Figure 11**, the computer 1115 has acquired both pieces of content that is stored in the media file. Accordingly, in this example, the DRM server 1110 sends (at 1250) a set of keys that would allow the computer 1115 to access both pieces of content in the media file 1125.

In the example illustrated in **Figure 11**, this set of keys includes two content keys 1130 and 1132. In some embodiments, each piece of content (e.g., 1145 or 1155) is encrypted based on a particular content key (e.g., 1130 or 1132). Hence, the computer 1115 uses the content key 1130 to decrypt the encrypted content 1145, and uses the content key 1132 to decrypt the encrypted content 1155.

Figure 13 illustrates another example of the computer 1115 acquiring the media file 1125. In this example, the computer 1115 has only acquired the first encrypted content 1145. Accordingly, even though the caching server 1105 supplies the computer 1115 with the media file that contains both pieces of content, the DRM server 1110 only supplies the content key 1130 for the encrypted content 1145.

Accordingly, in this example, the computer can access the encrypted content 1145 in the media file by using the content key 1130. However, since the computer 1115 has not received the encrypted content for the encrypted content 1155 in the media file 1125, the computer cannot decrypt the encrypted content 1155.

As shown in **Figure 12**, the computer 1115 receives (at 1255) the set of keys supplied by the DRM server 1110. As shown in **Figure 12**, the computer 1115 stores (at 1260) this set of keys in the media file. **Figure 14** illustrates the computer's storage of the two keys that it receives in the example illustrated in **Figure 11**. As shown in this figure, the computer 1115 initially stores the content keys 1130 and 1132 in temporary storages 1405 and 1407. It then merges these content keys with the media file 1125 that it received at 1235 and that it temporarily stored in a temporary storage 1410. The computer then stores the media file that results from this merging in a content library storage 1415.

Figure 15 illustrates the computer's storage of the key that it receives in the example illustrated in **Figure 13**. The storage operation illustrated in **Figure 15** is similar to the storage operation illustrated in **Figure 14**, except that the merge file (stored in the content media library 1415) does not contain the content key 1132 for the second encrypted content as the computer did not acquire and receive this content key.

In the embodiments described above, the content-distribution system 1100 utilizes one computer to provide the encrypted content while using another computer to provide the keys necessary for decrypting the encrypted content. One of ordinary skill will realize that in other embodiments the content-distribution system utilizes one computer to provide encrypted content and the keys for decrypting the encrypted content.

Alternatively, in other embodiments, the content-distribution system uses more than one computer to provide the cryptographic keys for the content. For example, keys for audio content may be available from one server and keys for related video content stored in the same media storage structure may be available from a separate server. The multiple servers may even be owned and administered by different parties, as may be the rights they administer.

Also, in the embodiments described above, the content-distribution system 1100 provides different cryptographic keys for decrypting different pieces of content. In other embodiments, the content-distribution system might utilize different encoding schemes for encrypting different pieces of content. For instance, the system might utilize a symmetric encoding scheme to encrypt audio content but utilize an asymmetric encrypting scheme to encrypt video content. Alternatively, the system might encrypt audio content in its entirety, while encrypting only parts of the video content.

Also, **Figure 12** illustrates one possible set of interactions between the computer 1115, the DRM server 1110, and the caching server 1105. One of ordinary skill will realize that these computers might interact differently in other embodiments. For instance, in some embodiments, the computer 1115 does not send a confirmation of the receipt of a media file to the DRM server. In some of these embodiments, the DRM server on its own sends the set of keys to the computer 1115.

Although some embodiments have been described with reference to a simplified network configuration, it will be understood that many variations exist within the framework described herein. For example, the DRM server is shown as a single computer, but for the purposes of this patent, such a server could include many interconnected computers and/or memory and/or interconnecting pieces of equipment. Similarly, the content caching server could be a single computer or a collection of networked computers and memory all forming a server. Additionally, while content may be supplied from a content caching server directly or indirectly to a specific client computer, other transfer methods may result in a computer requiring keys to unlock content available to it from a peer computer, portable storage device, or some other transfer mechanism.

III.SYNCHRONIZATION WITH A PLAYER

In some embodiments, the computer 1115 can synchronizes its DRM content with a portable player that is also allowed access to the DRM content. In some cases, this synchronization removes one or more pieces of content from a media file that the computer downloads to the portable player. In some cases, the pieces of content are removed in order to reduce the consumption of resources on the other device. In other cases, content is removed from the media storage structure because the other device does not have rights to access this other content.

Figure 16 illustrates an example of the computer 1115 synchronize its DRM content with a portable player 1605. The portable player can be a music player, audio/video player, etc. When the computer 1115 synchronizes its DRM content with the player 1605, the portable player 1605 in some embodiments receives (1) DRM content from the computer 1115, and (2) a content key for decrypting each piece of DRM content that it receives. The portable then stores the received encrypted DRM content and the associated keys.

Figure 17 conceptually illustrates a process 1700 that a computer 1115 performs in some embodiments to synchronize a set of content with a player 1605. As shown in this figure, the process 1700 starts (at 1705) when it receives a request to synchronize a set of content with the player 1605. The process then identifies (at 1710) the set of media files that is associated with a user account ID of the player.

Next, the process determines (at 1715) whether the computer 1115 is storing any media file for the player, which it has not yet downloaded to the player (i.e., whether there is any media file that needs to be synchronized between the computer and the player). If not, the process ends.

Otherwise, the process selects (at 1720) a media file that needs to be synchronized. At 1720, the process removes from the media file any piece of content that has been designated as content that should not be downloaded to the portable player. In some embodiments, the computer uses an application that allows a user to designate the content that the user wishes to synchronize with the portable player.

If the process removes (at 1720) any content from the media file, it also removes the content's associated content key and metadata from the media file in some embodiments of the invention. **Figure 16** illustrates an example of the removal of the video content and its associated content key from a media file 1600 that is downloaded to the portable player 1605.

After 1720, the process downloads (at 1725) the media file that contains only the encrypted content that has to be synchronized with the player (i.e., downloads the media file after any content that should not be downloaded to the player has been removed). In some embodiments, the downloaded media file not only contains one or more pieces of encrypted content but also contains one or more content keys that can be used to decrypt the content. In some embodiments, the set of keys that is downloaded in the media file to the player is the same set of keys that are used to decrypt the content on the computer 1115. In other embodiments, the keys in the downloaded media file are a different set of keys.

The player then stores (at 1725) the downloaded media file on its internal storage (e.g., its internal non-volatile storage, hard drive, flash memory, etc.). After 1725, the process determines (at 1730) whether there is any additional content for the player that it has not yet downloaded to the player (i.e., whether there is any additional content that needs to be synchronized between the computer and the player). If so, the process repeats 1720 and 1725 for a piece of content that needs to be synchronized. If not, the process ends.

Figure 17 provides an illustrative example of synchronizing media files between a computer and a player in some embodiments of the invention. One of ordinary skill will realize that other embodiments use other processes for synchronizing media files. Also, in some embodiments, the portable player directly communicates with the DRM server and/or the content caching server to obtain content.

IV. ENCRYPTION

As described above, several embodiments of the invention provide DRM processes and systems for distributing content. These processes and systems encrypt and decrypt content based on cryptographic keys. Encrypting content entails transforming the content from a decipherable form (called plaintext) into an indecipherable form (called ciphertext) based on one or more cryptographic keys. Decrypting content entails transforming encrypted content into a decipherable from by using one or more cryptographic keys.

An encryption key is a piece of information that controls the operation of a cryptography algorithm. In symmetrical encryption technology, the key that is used to encrypt content is the same key that is used to decrypt content. In asymmetric encryption technology, the same key is not used to encrypt and decrypt the content. For instance, in one scheme, an encrypting device uses a public key of a recipient to encrypt content, and the recipient uses its private key to decrypt the encrypted content.

Many of the features of the embodiments described above can be implemented according to a symmetrical or asymmetrical encryption approach. Also, in some embodiments, the encryption is applied to a binary format of the content. Although the unencrypted binary format of a piece of content may be hard for a human to decipher, it can be deciphered by an application or an operating system. On the other hand, encrypted binary format of a piece of content ideally should not be deciphered by any application or operating system, without first being decrypted by using one or more cryptographic keys.

While the invention has been described with reference to numerous specific details, one of ordinary skill in the art will recognize that the invention can be embodied in other specific forms without departing from the spirit of the invention. For instance, even though one set of keys are described above for the media storage files of some embodiments, other embodiments provide different sets of keys for defining different levels of access on different devices to the content of a media storage file. Thus, one of ordinary skill in the art would understand that the invention is not to be limited by the foregoing illustrative details, but rather is to be defined by the appended claims.

CLAIMS

What is claimed is:

1. A digital rights management (DRM) method for distributing content, the method comprising:

a) providing a single media storage structure to a device, wherein the media storage structure includes first and second pieces of encrypted content.

b) based on the pieces of content that the device has right to access, selecting a first set of keys from among a second set of key; and

c) providing the first set of keys to the device to control which piece of content the device can access.

2. The method of claim 1 further comprising:

storing, at the device, the first set of keys in the media storage structure.

3. The method of claim 1, wherein the first set of keys includes a cryptographic key for decrypting each piece of content in the media storage structure that the device has a right to access.

4. The method of claim 1 further comprising:

before providing a single media storage structure, completing a financial transaction in which a user of the device acquires rights to access certain pieces of content in the media storage structure.

5. A content-distribution system comprising:

a) a plurality of devices for receiving content;

b) at least one computer for distributing media storage structures, each media storage structure comprising a set of encrypted content pieces and a set of keys, wherein each particular key in the set of keys is for decrypting a particular piece of content in the set of encrypted contents, wherein the set of encrypted content pieces of one media storage structure has more than one pieces of content.

6. The content-distribution system of claim 5, wherein each media storage structure further includes metadata.

7. The content-distribution system of claim 5, wherein a plurality of the devices are computers.

8. The content-distribution system of claim 7 further comprising a plurality of portable players for synchronizing with the computers to receive media storage structures.

9. The content-distribution system of claim 8, wherein the synchronization of at least one portable player with a computer results in the removal of content from at least one media storage structure.

10. A data structure comprising:

a) header information,

b) a plurality of encrypted media portions, and

c) a plurality of keys, each key for decrypting a corresponding one of the encrypted media portions.

11. The data structure of claim 10, wherein one of the encrypted media portions is audio content and another of the encrypted media portions is video content related to the audio content.

12. The data structure of claim 11, wherein the audio content is a song and the video content is a music video associated with the song.

13. The data structure of claim 11, wherein one of the encrypted media portions is audio content and another of the encrypted media portions is text content related to the audio content.

14. The data structure of claim 11, wherein the audio content is a song and the text content is the song's lyrics.

15. The data structure of claim 11, wherein one of the encrypted media portions is video content and another of the encrypted media portions is text content related to the video content.

16. The data structure of claim 11, wherein the text content is dialogue of the video associated.

17. A method of a user receiving permission to access media content comprising:

a) receiving a unitary media storage structure with a plurality of protected media portions,

b) receiving from a license authority a key for each protected media portion that the user has permission to access,

c) using said key to access said media portions that the user has permission to access.

18. The method of claim 17 further comprising storing said received keys in said unitary media storage structure.

19. A method of granting permission to access media content comprising:

a) providing to a device a unitary media storage structure with a plurality of protected media portions;

b) providing to the device a key for each protected media portion that the device has permission to access, wherein each key is for accessing a media portion that the user has permission to access.

20. The method of claim 19, wherein the provided keys are stored in said unitary media storage structure after the keys are provided.

Figure 1

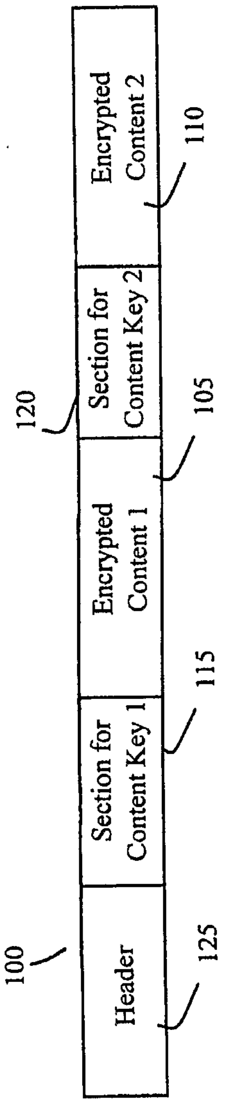


Figure 2

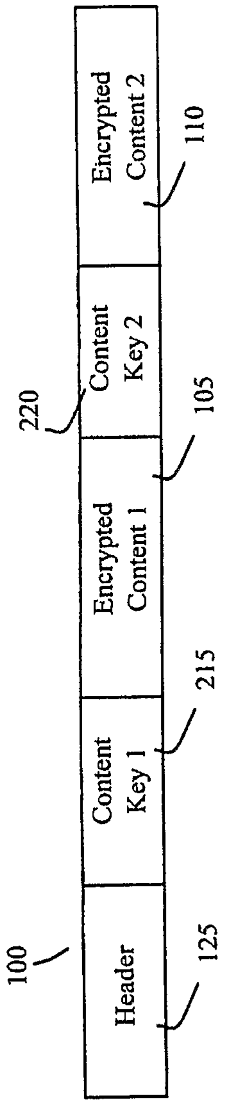
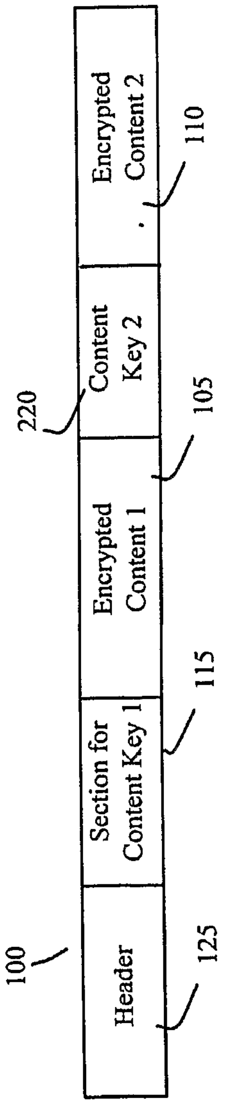


Figure 3



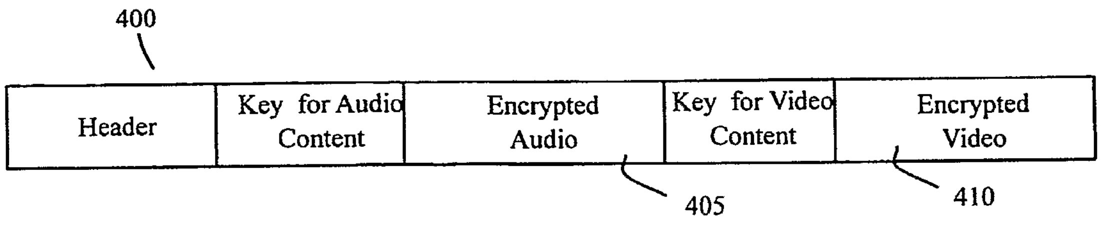


Figure 4

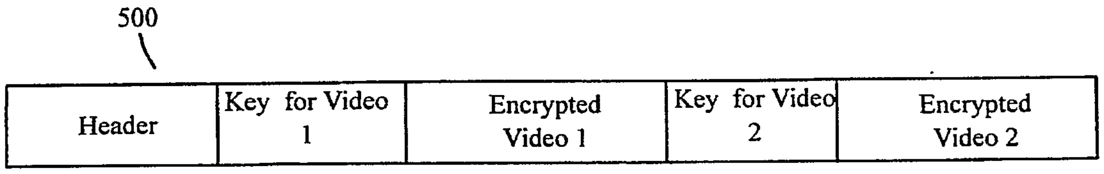


Figure 5

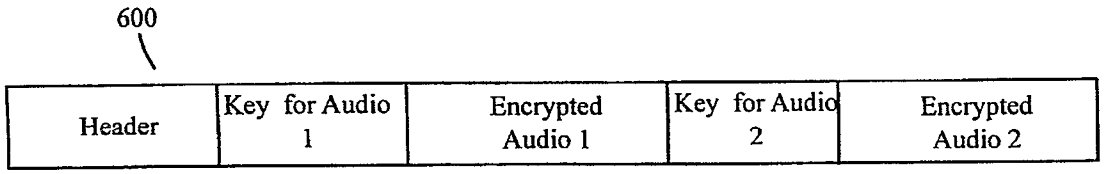


Figure 6

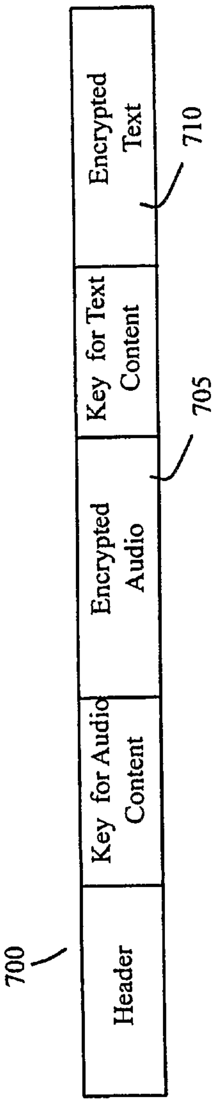


Figure 7

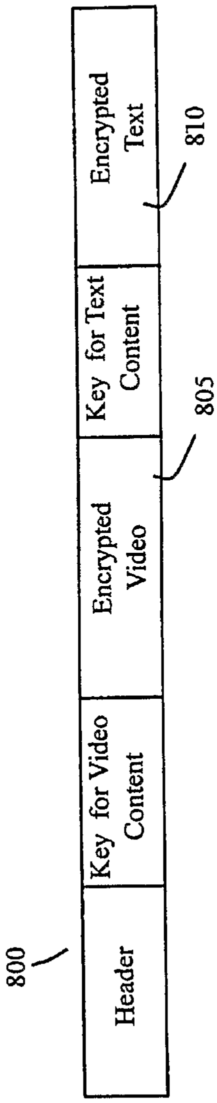


Figure 8

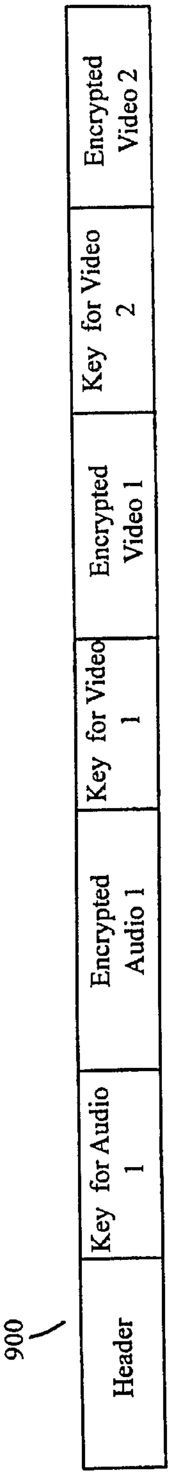


Figure 9

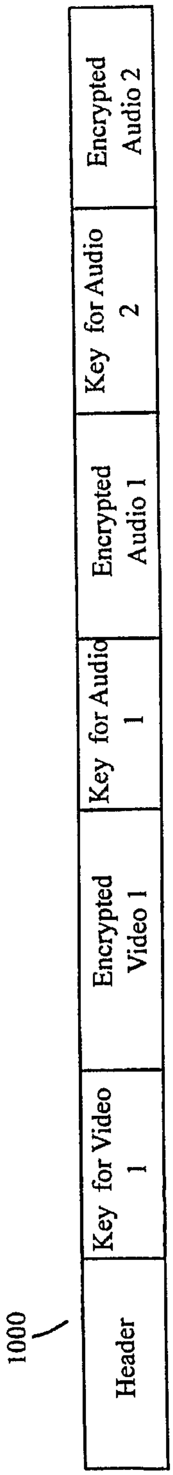


Figure 10

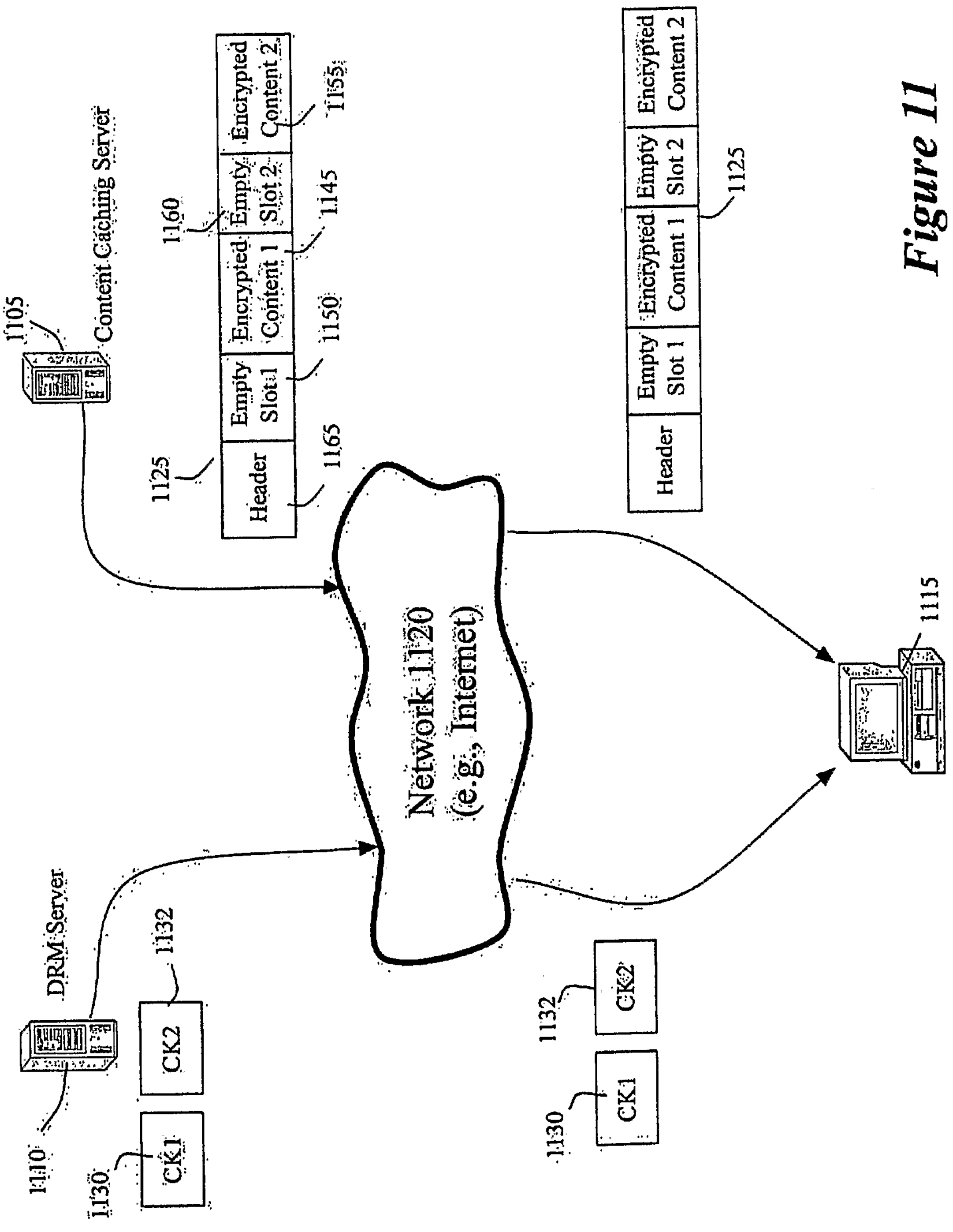

1105
Content Caching Server
1125
Header
Empty Slot 1
Encrypted Content 1
Empty Slot 2
Encrypted Content 2
1165
1150
1145
1160
1155
Network 1120 (e.g., Internet)
DRM Server
1110
1130
CK1
1132
CK2
1115
Header
Empty Slot 1
Encrypted Content 1
Empty Slot 2
Encrypted Content 2
1125
1130
CK1
1132
CK2

Figure 11

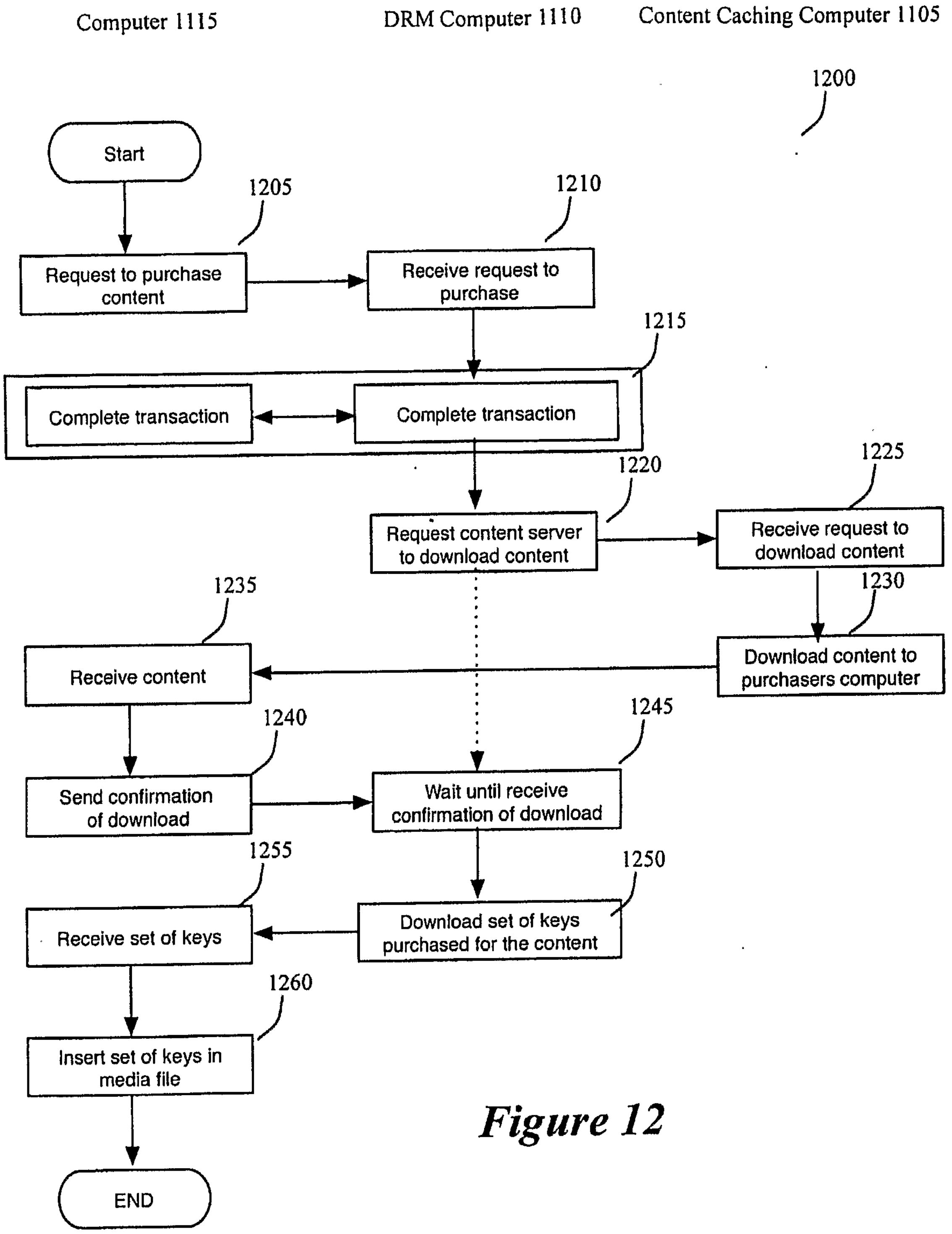

Computer 1115
DRM Computer 1110
Content Caching Computer 1105
1200
Start
1205
Request to purchase content
1210
Receive request to purchase
1215
Complete transaction
Complete transaction
1220
Request content server to download content
1225
Receive request to download content
1230
Download content to purchasers computer
1235
Receive content
1240
Send confirmation of download
1245
Wait until receive confirmation of download
1250
Download set of keys purchased for the content
1255
Receive set of keys
1260
Insert set of keys in media file
END

Figure 12

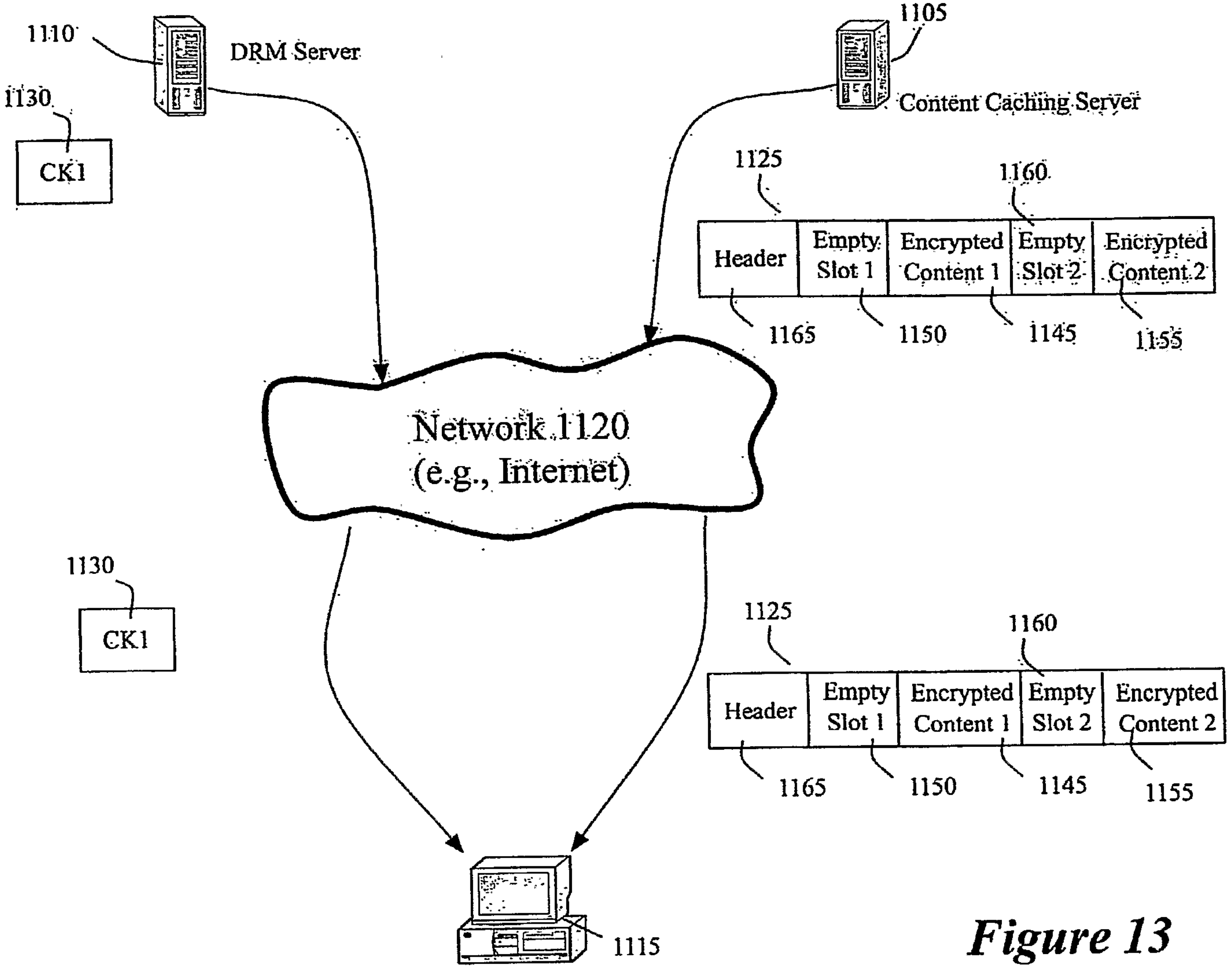

1110
DRM Server
1130
CK1
1105
Content Caching Server
1125
1160
Header
Empty Slot 1
Encrypted Content 1
Empty Slot 2
Encrypted Content 2
1165
1150
1145
1155
Network 1120 (e.g., Internet)
1130
CK1
1125
1160
Header
Empty Slot 1
Encrypted Content 1
Empty Slot 2
Encrypted Content 2
1165
1150
1145
1155
1115

Figure 13

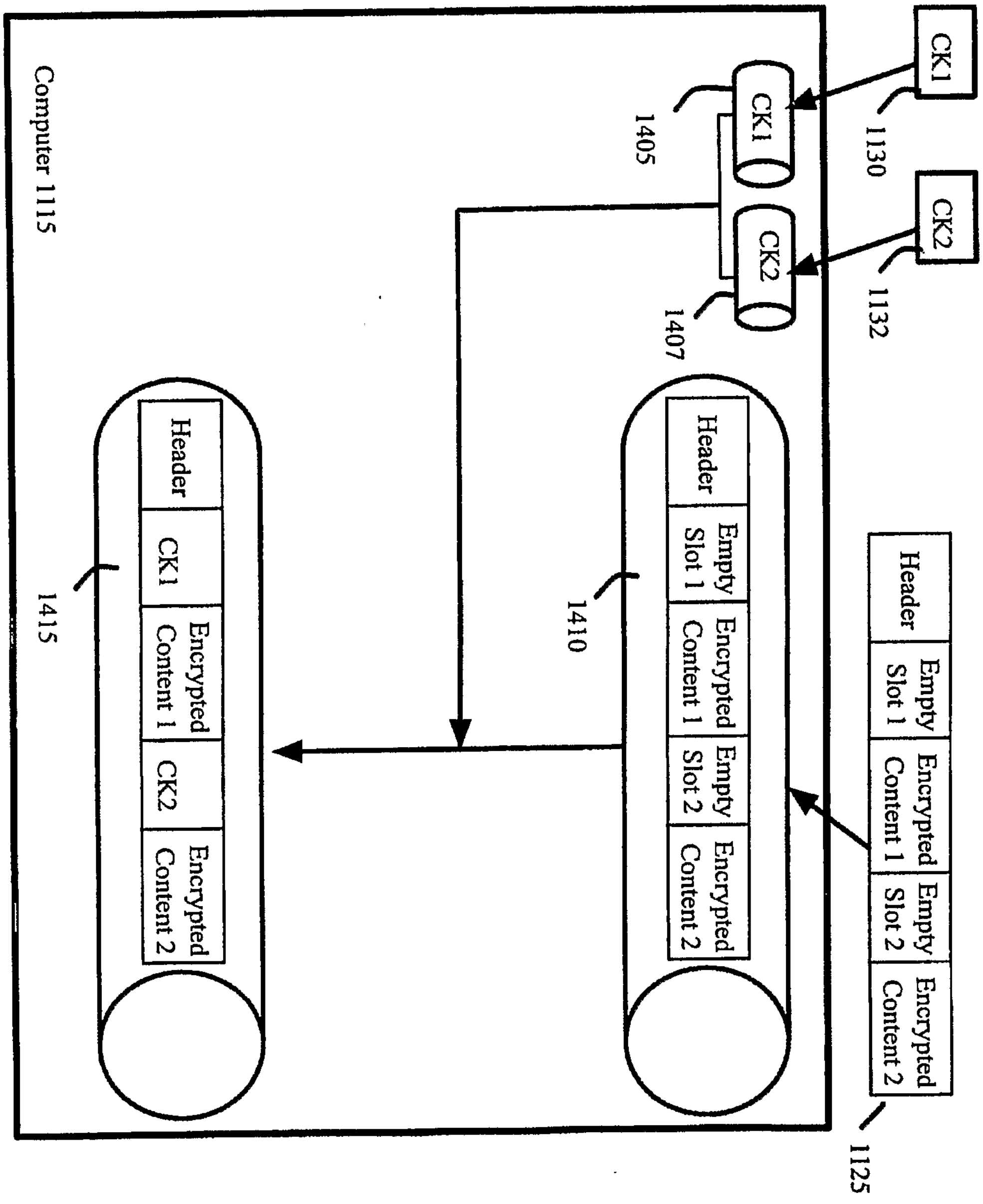

CK1
1130
CK2
1132
Header
Empty Slot 1
Encrypted Content 1
Empty Slot 2
Encrypted Content 2
1125
CK1
1405
CK2
1407
Header
Empty Slot 1
Encrypted Content 1
Empty Slot 2
Encrypted Content 2
1410
Header
CK1
Encrypted Content 1
CK2
Encrypted Content 2
1415
Computer 1115

Figure 14

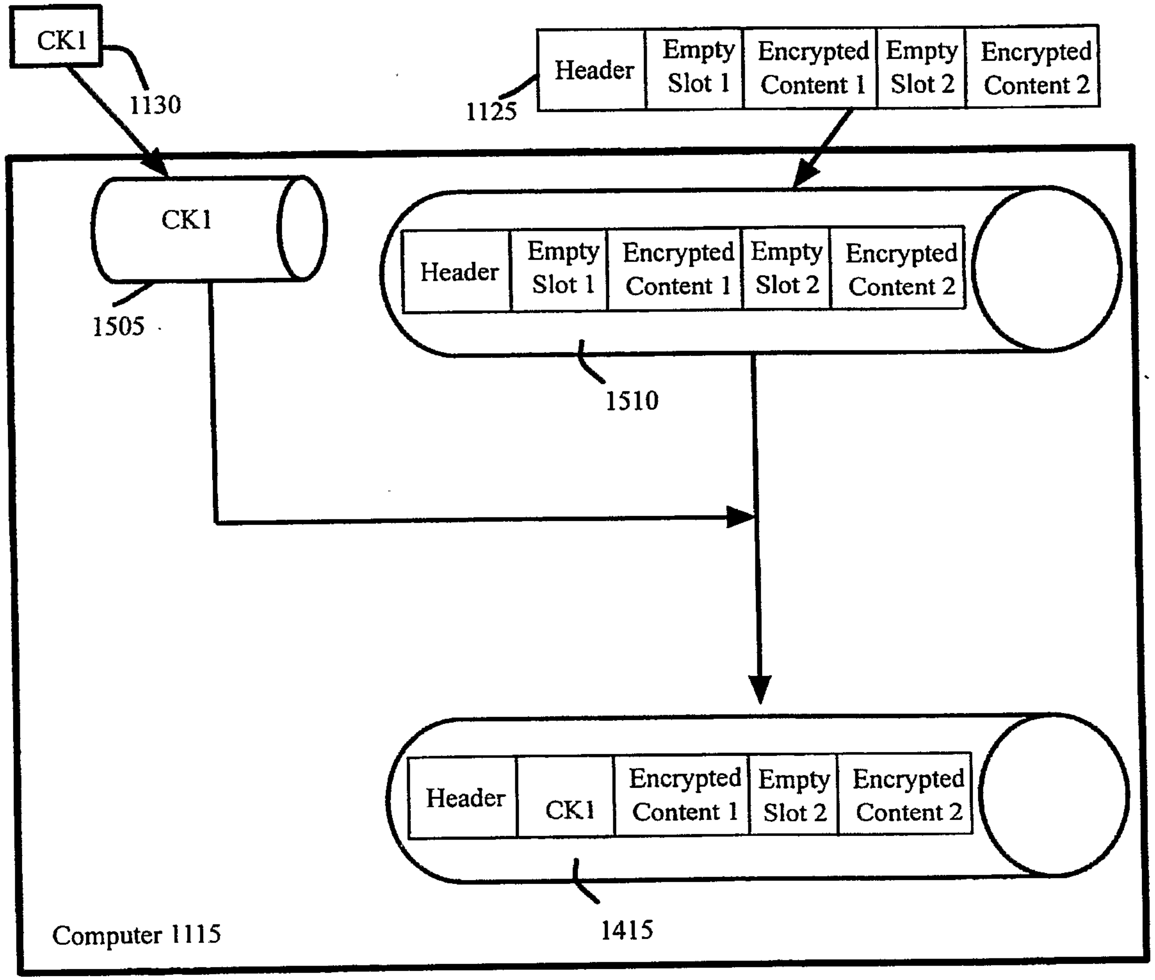

CK1
1130
1125
Header
Empty Slot 1
Encrypted Content 1
Empty Slot 2
Encrypted Content 2
CK1
1505
Header
Empty Slot 1
Encrypted Content 1
Empty Slot 2
Encrypted Content 2
1510
Header
CK1
Encrypted Content 1
Empty Slot 2
Encrypted Content 2
1415
Computer 1115

Figure 15

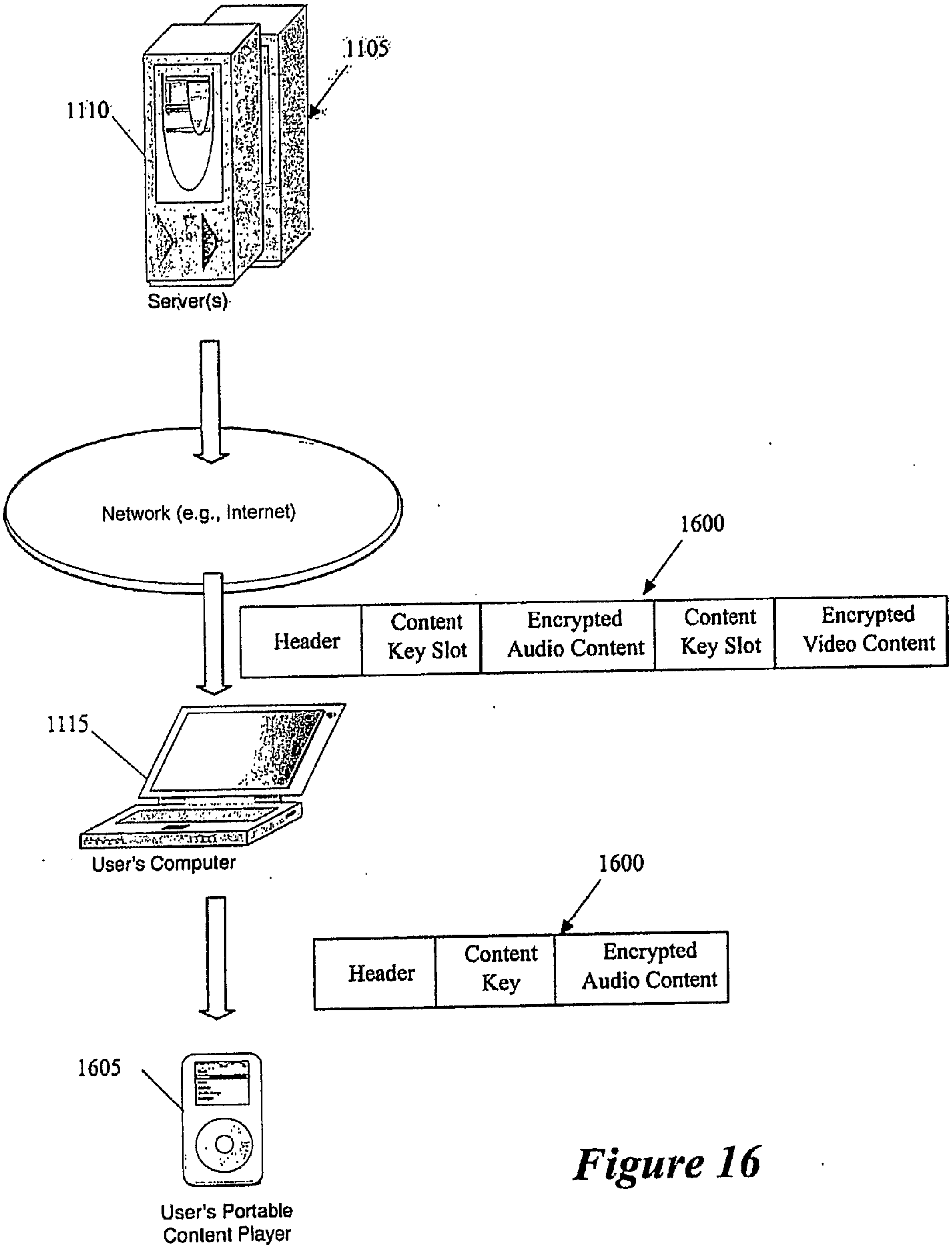

1105
1110
Server(s)
Network (e.g., Internet)
1600
Header
Content Key Slot
Encrypted Audio Content
Content Key Slot
Encrypted Video Content
1115
User's Computer
1600
Header
Content Key
Encrypted Audio Content
1605
User's Portable Content Player

Figure 16

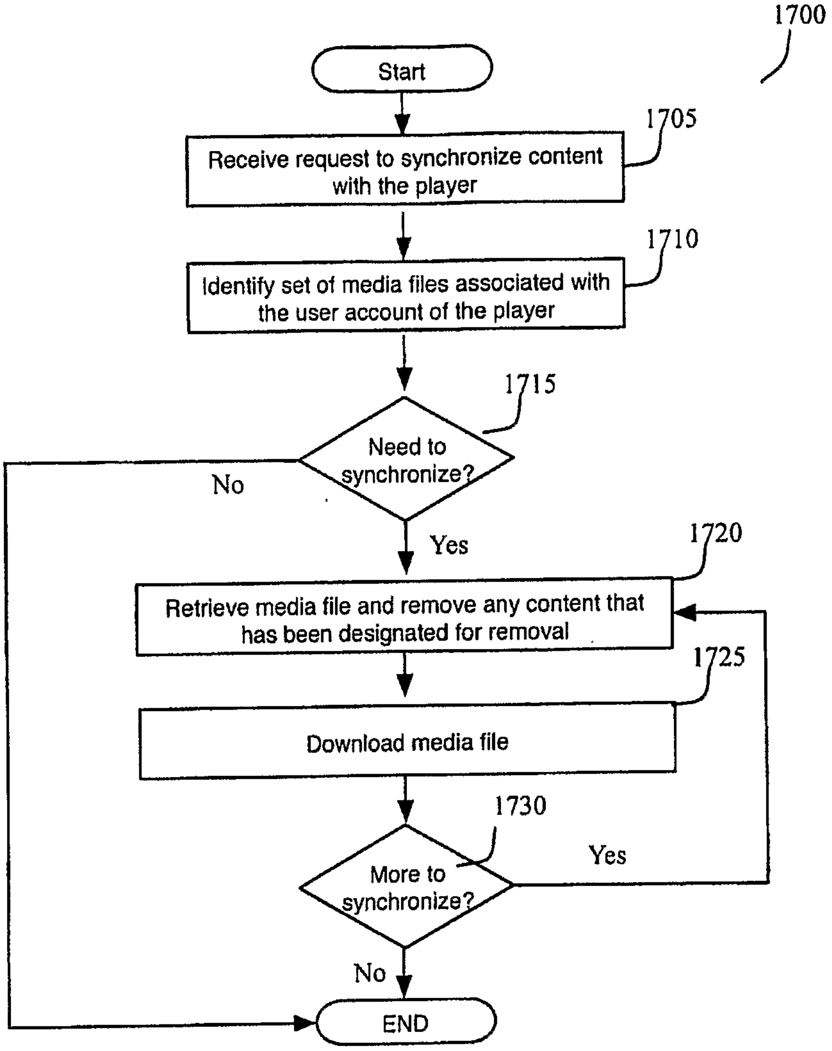

1700
Start
1705
Receive request to synchronize content with the player
1710
Identify set of media files associated with the user account of the player
1715
Need to synchronize?
No
Yes
1720
Retrieve media file and remove any content that has been designated for removal
1725
Download media file
1730
More to synchronize?
Yes
No
END

Figure 17