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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 August 2010 (12.08.2010)

PCT

(10) International Publication Number
WO 2010/090689 A1

(51) International Patent Classification:
H04L 9/14 (2006.01) *G06F 15/16* (2006.01)
G06F 21/24 (2006.01) *G06F 9/06* (2006.01)

(21) International Application Number:
PCT/US2009/069332

(22) International Filing Date:
22 December 2009 (22.12.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/146,099 21 January 2009 (21.01.2009) US
12/485,949 17 June 2009 (17.06.2009) US

(71) Applicant *(for all designated States except US)*: **MICROSOFT CORPORATION** [US/US]; One Microsoft Way, Redmond, Washington 98052-6399 (US).

(72) Inventors: **BURNS, Quintin, Swayne**; One Microsoft Way, Redmond, Washington 98052-6399 (US). **HUGHES, Robert, Kilroy, Jr.**; One Microsoft Way, Redmond, Washington 98052-6399 (US). **SIMMONS, John, Carl**; One Microsoft Way, Redmond, Washington 98052-6399 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, 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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(54) **Title**: MULTIPLE CONTENT PROTECTION SYSTEMS IN A FILE

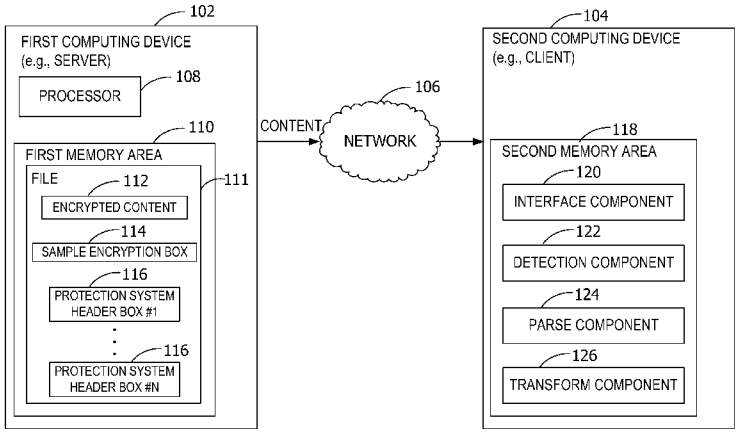

FIG. 1

(57) **Abstract**: Supporting a plurality of content protection systems in a single container file. The protection systems share an encryption method which is accessible from a sample encryption box in the file. Each of the protection systems stores, in a protection system header box, information for decrypting the content in accordance with the corresponding protection system. In some embodiments, separate protection system header boxes in the file correspond to each of the protection systems. By using the common encryption method and sharing encryption expressions across the protection systems, the multiple content protection systems are supported in the file without creating additional copies of the content. In some embodiments, aspects of the disclosure extend the International Organization for Standardization (ISO) base media file format to support multiple digital rights management (DRM) systems in the single container file.

WO 2010/090689 A1

MULTIPLE CONTENT PROTECTION SYSTEMS IN A FILE

BACKGROUND

[0001] Existing digital rights management (DRM) systems protect media content and other files from unauthorized use. To protect the content, metadata specific to one of the DRM systems is stored in the file with the media content. Devices render the content by interpreting the metadata and decrypting the content for presentation to a user. However, content encrypted according to a first DRM system cannot be decrypted by a device supporting only a second DRM system. To enable decryption of the encrypted content by such a device, existing systems create multiple versions of the content each encrypted according to a different DRM system. Alternatively, the content may be decrypted by a device supporting the first DRM system and then re-encrypted by a device supporting the second DRM system. Still other existing systems include a service that provides a rights mapping between the first and second DRM systems.

SUMMARY

[0002] Embodiments of the invention support multiple protection systems applied to a single container file. The file containing the content and one or more encryption expressions is received. The content is encrypted by the encryption expressions. A plurality of protection systems are applied to the content using the encryption expressions from the received file. Each of the protection systems protects the content using the same encryption expressions. The file with the content and the applied plurality of protection systems are transmitted to one or more computing devices for decryption. Each of the computing devices decrypts the content using at least one of the applied plurality of protection systems.

[0003] This Summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This Summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used as an aid in determining the scope of the claimed subject matter.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] FIG. 1 is an exemplary block diagram illustrating a first computing device providing content to a second computing device over a network.

[0005] FIG. 2 is an exemplary block diagram illustrating the flow of content from a content provider through an encoding provider and a service provider to a consumer.

[0006] FIG. 3 is an exemplary flow chart illustrating the application of protection systems to content.

[0007] FIG. 4 is an exemplary flow chart illustrating the decoding of content for presentation on a computing device.

[0008] FIG. 5 is an exemplary block diagram illustrating an exemplary structure representing a fragmented file structure.

[0009] FIG. 6 is an exemplary block diagram illustrating an exemplary structure representing fragmented file organization.

[0010] FIG. 7 is an exemplary block diagram illustrating an exemplary structure for storing a track box.

[0011] FIG. 8 is an exemplary block diagram illustrating an exemplary structure for storing for storing a media information box.

[0012] FIG. 9 is an exemplary block diagram illustrating an exemplary structure for storing a protected sample entry box.

[0013] Corresponding reference characters indicate corresponding parts throughout the drawings.

DETAILED DESCRIPTION

[0014] Referring to the figures, embodiments of the disclosure support, at least, multiple protection systems such as digital rights management (DRM) systems in a file 111 storing media content for presentation to a user. The file 111 stores a single copy of the media content or other content protected by the multiple protection systems. In part to enable such interoperability among the protection systems, the protection systems use or share an encryption algorithm or other encryption method common to the protection systems. Additionally, encryption expressions such as key information used by the protection systems are shared across the protection systems.

[0015] Aspects of the disclosure extend the International Organization for Standardization (ISO) base media file format to support the multiple DRM systems in a single container file such as file 111. In some embodiments, the container file includes a sample encryption box 114 and a plurality of protection system header boxes 116, each particular to one or more of the protection systems. The sample encryption box 114 stores or identifies the encryption method common to the protection systems. The protection system header boxes 116 each store data objects used to decrypt the content with the corresponding protection systems. For example, in some embodiments, the data objects in the protection system header boxes 116 are used to acquire other data objects (e.g., from a

license server) to decrypt the content. The data objects represent opaque metadata to support the multiple protection systems in the single file, simultaneously.

[0016] While aspects of the invention are described with reference to the computing device being the mobile computing device such as a mobile telephone or a netbook or ultraportable, embodiments of the invention are operable with any computing device. For example, aspects of the invention are operable with devices such as digital cameras, digital video cameras, laptop computers, set top boxes, gaming consoles (including handheld gaming consoles), portable music players, personal digital assistants, information appliances, and personal communicators.

[0017] Referring again to FIG. 1, an exemplary block diagram illustrates a first computing device 102 providing content to a second computing device 104 over a network 106. In some embodiments, the first computing device 102 is a server, the second computing device 104 is a client device, and the network 106 is the Internet. The first computing device 102 includes at least a first memory area 110 and a processor 108. The first memory area 110 stores the file 111 corresponding to, for example, media content or a media presentation. The media content includes commercial or non-commercial media data such as video, audio, images, text, and/or graphics, or sequences thereof. The first computing device 102 transmits the file 111 with the media content to the second computing device 104 over the network 106.

[0018] The exemplary block diagram in FIG. 1 describes content delivery scenarios supported by embodiments of the disclosure including, but not limited to, second session or digital delivery of standard definition or portable media content from an optical disc to a computing device (e.g., portable device or personal computer), progressive download of multimedia content, adaptive streaming over Internet Protocol (IP) networks, or side loading of multimedia content onto portable devices.

[0019] The first computing device 102, or other server, represents any known or later-developed sources of media content or information associated therewith including, but not limited to, data storage servers, DRM servers, media content servers (e.g., for music or video downloading, on-demand, broadcasting, or advertising), peer servers, and the like. The first computing device 102 may comprise one or more such devices.

[0020] The network 106 represents any digital data transmission infrastructure or technology configured to support known or future-developed media protocol. Exemplary networks include, but are not limited to, the Internet, cellular networks, satellite networks, BLUETOOTH brand wireless networks, and the like.

[0021] The second computing device 104 is any computing device, or element of such a computing device, configured to receive data from the first computing device 102. The second computing device 104 may be configured to store and/or present the received data, or alternatively pass the received data to another device for storage and/or presentation.

[0022] The first computing device 102 and the second computing device 104 may include components such as transceivers, multiplexers, demultiplexers, encoders, decoders, encrypters, decrypters, and the like.

[0023] In some embodiments, the file 111 represents a container file that stores the content in a format supports multiple protection systems. The protection systems correspond to, for example, the DRM systems. In such embodiments, the file 111 includes encrypted content 112, the sample encryption box 114, and the plurality of protection system header boxes 116 such as protection system header box #1 through protection system header box #N. The sample encryption box 114 and the protection system header boxes 116 represent object-oriented building blocks defined by a type identifier and length. A container box contains and groups related boxes. For example, a media data box is a container box holding media content for a presentation, while a movie box is a container box whose sub-boxes define metadata for a presentation. While the sample encryption box 114 and protection system header boxes 116 are shown to be included in a particular box or container box such as illustrated in the figures, the boxes sets forth information that can be conveyed via the box included therewith, or another box therein. Further, the boxes may be considered sub-boxes of other boxes in the file 111.

[0024] Each of the plurality of protection system header boxes 116 are associated with one or more of the protection systems. Any quantity of the protection system header boxes 116 may be contained within the file 111. The boxes and protection system are identified by a DRM identifier or other protection system identifier. The sample encryption box 114 identifies a key used to encrypt the encrypted content 112. In some embodiments, the sample encryption box 114 stores a key, key identifier, and/or key mapping information describing a common or standard encryption method across the protection systems. The key may be different for each sample encryption box 114. For example, the standard encryption method includes the Advanced Encryption Standard (AES) with 128-bit key size in counter (CTR) mode. The initialization vector for the AES algorithm is also common to the protection systems. The sample encryption box 114 is shared by the protection system header boxes 116. Each of the protection system header

boxes 116 includes metadata for decoding the encrypted content 112, or otherwise granting access to the content, in accordance with one or more of the protection systems.

[0025] In an example in which the file 111 corresponds to the ISO base media file format, the protection system header boxes 116 are at nesting level 1 while the sample encryption box 114 is at nesting level 2, in some embodiments.

[0026] The second computing device 104 has access to a second memory area 118. The second memory area 118, or one or more computer-readable media, stores computer-executable components for decoding and presenting the media content to a user of the second computing device 104. Exemplary components include an interface component 120, a detection component 122, a parse component 124, and a transform component 126. These components represent exemplary structure for implementing functionality associated with the second computing device 104, although other structures are contemplated for implementing the functionality described herein. Operation of the exemplary components illustrated in FIG. 1 is described below with reference to FIG. 4.

[0027] In general, the first memory area 110 is associated with the first computing device 102. For example, in FIG. 1, the first memory area 110 is within the first computing device 102. However, the first memory area 110 or any of the data stored thereon may be associated with any server or other computer, local or remote from the first computing device 102 (e.g., accessible via a network). Similarly, the second memory area 118 is associated with the second computing device 104. For example, in FIG. 1, the second memory area 118 is within the second computing device 104. However, the second memory area 118 or any of the data stored thereon may be associated with any server or other computer, local or remote from the second computing device 104 (e.g., accessible via a network).

[0028] The processor 108 includes any quantity of processing units, and is programmed to execute computer-executable instructions for implementing aspects of the disclosure. The instructions may be performed by the processor 108 or by multiple processors executing within the first computing device 102, or performed by a processor external to the first computing device 102 (e.g., by a cloud service). In some embodiments, the processor 108 is programmed to execute instructions such as those illustrated in the figures (e.g., FIG. 3 and FIG. 4).

[0029] Referring again to FIG. 2, an exemplary block diagram illustrates the flow of content from a content provider 202 through an encoding provider 204 and a service provider 206 to a consumer. The diagram of FIG. 2 represents an example of the diagram

shown in FIG. 1 in which the service provider 206 corresponds to the first computing device 102 and a consumer device 208 corresponds to the second computing device 104.

[0030] The content provider 202 generates a file containing media content. For example, the content provider 202 is a movie studio that produces a video file corresponding to a movie. The generated video file may be in the format known as a mezzanine format, which may be specific to each content provider 202. The content provider 202 transmits the video file to the encoding provider 204. The encoding provider 204 prepares the video file for distribution to one or more of the service providers 206. In this example, the encoding partner performs processing to prepare the mezzanine content for encoding, including encryption in some embodiments, and then performs the encoding and encryption. The encoding and encryption occurs using an encryption key provided by the content provider 202 or generated by the encoding provider 204. The encoded content is ready for distribution, but lacks a protection system (e.g., DRM). The encoded content is sent to the service provider 206.

[0031] The service provider 206 receives the encoded content and adds a header (e.g., one of the protection system header boxes 116) for DRM A to the video file. The video file with the applied protection system may be sent to the consumer device 208 or other devices where it is capable of being decrypted only by DRM A. Alternatively or in addition, the service provider 206 may also add another header (e.g., another one of the protection system header boxes 116) for DRM B to the video file. At this point, the video file is capable of being decoded using DRM A or DRM B. The video file is transmitted to the consumer, where the consumer device 208 may parse, decrypt, and decode the video file using DRM A or DRM B.

[0032] In an example, the content is a movie, and the user attempts to play the movie on Device One which support DRM A. Playback software on Device One determines that the movie is encrypted. The playback software finds the protection specific header box corresponding to DRM A. The playback software uses the information contained in the protection specific header box to contact a license server and retrieve a license for the movie. The retrieved license may be stored within the protection specific header box for DRM A (e.g., in extra space therein). The movie is then decrypted using DRM A and presented to the user.

[0033] In a further example, the user then copies the movie to Device Two which supports DRM B. The playback software on Device Two determines that the movie is encrypted. The playback software finds the protection specific header box corresponding

to DRM B. The playback software uses the information contained in the protection specific header box to contact a license server and retrieve a license for the movie. The retrieved license may be stored within the protection specific header box for DRM B (e.g., in extra space therein). The movie is then decrypted using DRM B and presented to the user.

[0034] Referring next to FIG. 3, an exemplary flow chart illustrates the application of protection systems to content. A computing device, such as the service provider 206 in FIG. 2, determines at 302 if a file has been received. The file includes media content and one or more encryption expressions. The media content is encrypted according to the encryption expressions. In some embodiments, the encryption expressions include, or include metadata describing, one or more encryption keys, key identifiers, and key mapping information. In other embodiments, the encryption expressions include data objects for obtaining one or more of the encryption keys, key identifiers, and key mapping information from another location (e.g., a web service). The encryption expressions may be stored in, for example, one or more of the protection system header boxes 116 and/or the sample encryption box 114 illustrated in FIG. 1.

[0035] After the file with the media content is received at 302, a plurality of protection systems is selected at 304. For example, the protection systems may be selected based on the intended recipients of the file, or represent a default selection of protection systems commonly used by consumer devices 208. At 306, the selected protection systems are applied to the content in the file using one or more of the encryption expressions to create DRM-protected content. For example, applying the protection systems includes adding or embedding metadata for the protection systems to the file. The metadata describes the protection systems and enables decryption of the content. In some embodiments, the metadata includes a rights object or license information (or a reference to the license information) related to the protection systems, along with a decryption key associated with the protection system.

[0036] The protection systems are applied to the content without creating additional copies of the content. As a result, a single container file (e.g., file 111) comprises the content and the plurality of selected, applied protection systems.

[0037] The DRM-protected content is transmitted to one or more computing devices at 308. The computing devices decrypt the content using at least one of the applied protection systems supported by the computing devices. Alternatively or in addition, the DRM-protection content is stored in a memory area for access by the computing devices.

[0038] In the example of FIG. 1, applying the protection systems includes defining one of the protection system header boxes 116 for each of the selected protection systems. The defined protection system header boxes 116 are included in the file. In this example, the sample encryption box 114 includes key information including key mapping information and a key identifier. The protection systems are applied to the content using the key information identified in the sample encryption box 114.

[0039] Referring next to FIG. 4, an exemplary flow chart illustrates the decoding of content for presentation on a computing device. A DRM-protected video file is received by the computing device at 402. A parser executing on the computing device examines metadata in the received file at 404 to determine that the file has a protection system applied thereto at 406. For example, the parser determines that the file has been protected by a stream type of encrypted video (e.g., "encv") or encrypted audio (e.g., "enca") if the file is in Moving Picture Experts Groups-4 (MP4) format. In such an example, the parser examines a scheme information box or scheme type box within a protection scheme information box to determine whether a track within the file is encrypted in accordance with aspects of the disclosure. The track corresponds to a collection of related samples in the file. In some embodiments, the parser finds in the scheme type box a four-character code and a version number identifying the protection scheme.

[0040] An application program executing on the computing device searches the protection system header boxes 116 in the received video file at 408 to find the protection system header box 116 that corresponds to a protection system supported by the computing device. The protection system header box 116 is used to ensure that any license(s) for decrypting the content is available on the computing device before playback begins. The key identifier is obtained from the sample encryption box 114. The application program obtains data from the protection system header box 116 corresponding to a supported protection system that enables the application program to obtain a license from a license server that corresponds to that key identifier at 410. The application then extracts an encrypted key from the license, and decrypts the key at 411. Decryption of the encrypted key (e.g., a private key, an individualized key, or other asymmetric key) may be performed using known public-private key systems, in some embodiments. The decrypted key is used to decrypt the track, and the decrypted content is presented to the user at 412.

[0041] In some embodiments, the operations illustrated in FIG. 4 are implemented using computer-executable components stored on one or more computer-readable media. For

example, the components illustrated in FIG. 1 perform the operations. In such an example, the interface component 120 receives the file containing content and one or more encryption expressions. The content has been encrypted by at least one of the encryption expressions. The content further has a plurality of protection systems applied thereto, and the file includes metadata for each of the plurality of protection systems. The plurality of protection systems share access to the encryption expressions. Further, the content is encoded according to an encryption algorithm. The plurality of protection systems shares the encryption expressions and the encryption algorithm.

[0042] The detection component 122 examines a scheme information box in the file to determine whether the content is protected by a protection scheme in accordance with aspects of the disclosure. The detection component 122 determines which protection systems are supported by the computing device, and selects one of the supported protection systems. The parse component 124 obtains, from the metadata, license information for the protection system selected by the detection component 122. The transform component 126 decodes and decrypts the content based on the license information obtained by the parse component 124 and based on the encryption expressions. The interface component 120 presents the decoded content to a user.

[0043] Referring next to FIG. 5, FIG. 6, FIG. 7, FIG. 8, and FIG. 9, exemplary block diagrams illustrate an example application of embodiments of the disclosure to extend a media file format to support a plurality of protection systems in a single container file. The examples below refer to various known specifications including, but not limited to, ISO 14496-12, ISO 14496-14, ISO 14496-1, ISO 14496-10, ISO 14496-3, and ISO/IEC 639-3:2007, all of which are hereby incorporated by reference herein for all purposes. While the examples next described are directed to the ISO base media file format and/or MP4 formats, embodiments of the invention are applicable to other file formats.

[0044] For the purposes of the following examples, the file format may be referred to as a movie. The movie is logically divided into tracks. Each track represents a timed sequence of media (e.g., frames of video). Within each track, each timed unit or frame of data is called a sample (e.g., a frame of video or audio, a time-contiguous series of video frames, or a time-contiguous compresses section of audio). Samples are implicitly numbered in sequence. A frame of audio may decompress into a sequence of audio samples. Each track has one or more sample descriptions. Each sample in the track is tied to a description by reference. The description defines how the sample may be decoded (e.g. identifies the compression algorithm used).

[0045] In some embodiments, neither the physical structure of the file nor the layout of the physical media is tied to the time ordering of the media content. For example, frames of video need not be laid down in the file in time order, although the frames might be laid down in such a way.

[0046] The data within the file is encapsulated in boxes. The metadata, including metadata defining the placement and timing of the media content, is contained in the boxes. The media content (e.g., frames of video) is referred to by the metadata. The media content may be in the same file (e.g., contained in one or more boxes) or can be in other files. The metadata permits referring to other files by means of references such as hyperlinks (e.g., uniform resource locators).

[0047] In the examples below, embodiments of the invention use a class-based notation with inheritance. The classes are consistently represented as structures on the disk and on the wire as follows: the fields of a class appear in the disk structure in the same order the fields are specified, and the fields in a parent class appear before the fields for derived classes. Further, when a box contains other boxes as children, the child boxes appear after any explicitly specified fields and can appear in any order (e.g., sibling boxes can be re-ordered without breaking compliance to the specification).

[0048] Referring again to FIG. 5, an exemplary block diagram illustrates an exemplary structure representing a fragmented file structure in accordance with embodiments of the disclosure. The fragmented file structure includes two top-level boxes: a movie fragment box ("moof") for metadata, and a media data ("mdat") box for samples. In this example, the sample encryption box 114 shared by the protection systems is shown as a sub-box of the movie fragment box. The sample encryption box 114 includes sample-specific encryption data. In the example of FIG. 5, the sample encryption box 114 has a type universally unique identifier (UUID), and is part of a track fragment container box or a sample table container box.

[0049] An example syntax for the sample encryption box 114 is shown below.

```
aligned(8) class SampleEncryptionBox extends
FullBox('uuid', extended_type=1, version=0, flags=0)
{
      unsigned int(8)  AlgorithmID;
      GUID             KID;
```

```
            unsigned int(32) sample_count;
            {
                unsigned int(64) SampleIdentifier;
            }[ sample_count ]
        }
```

[0050] The AlgorithmID is the identifier of the encryption algorithm (e.g., AES 128-bit in CTR mode) used to encrypt the track. KID is a key identifier that identifies the key for decrypting samples referred to by the sample encryption box 114. In this example, there is one AlgorithmID and one KID in the sample encryption box 114, meaning that there is one key per track. In other embodiments, there are multiple keys per track to, for example, allow for key rotation for broadcast content including sections of clear content within an encrypted track and to allow for insertion of content encrypted with different parameters (e.g., editing, advertisement insertion, etc).

[0051] Sample_count is the quantity of sample in this track or track fragment. SampleIdentifier is used to form an initialization vector for decrypting the sample. The AES CTR mode encryption used to encrypt the sample data uses the SampleIdentifier as the high 64 bits and a simple block counter (e.g., starting at zero from the beginning of the sample) as the low 64 bits of the 128 bit value encrypted with the AES cipher. In some embodiments, the SampleIdentiifers for a given key are unique for each sample, and the initial sample identifier is randomly generated. For each protected sample added to the file, the SampleIdentifier is incremented to provide entropy and ensure that the SampleIdentifiers are unique.

[0052] Referring again to FIG. 6, an exemplary block diagram illustrates an exemplary structure representing fragmented file organization. The movie fragment includes a particular segment of a particular sequence of media data. In this example, the disk format is fragmented MP4. The file type box in FIG. 6 identifies the file as being encoded according to embodiments of the disclosure to make the file type box fixed length. The plurality of DRM specific header boxes 602 such as DRM specific header box #1 through DRM specific header box #N (sub-boxes of the movie box) correspond to the plurality of protection system headers boxes illustrated in FIG 1. The DRM specific header boxes 602 contain data including, but not limited to, a license server reference (e.g., uniform resource locator), a list of key identifiers used by the file, embedded licenses, and the like. The DRM specific header boxes 602 may also store or pre-load any quantity of embedded

licenses (e.g., from the service provider 206 prior to the content being made available to the user).

[0053] In some embodiments, a plurality of DRM specific header boxes 602 exists for the same protection system. For example, a single file is shared by two different services both using the same protection system but each using different header parameters (e.g., different service identifiers, different license acquisition links, etc.).

[0054] An example syntax for the DRM specific header boxes 602 is shown below.

```
aligned(8) class DrmSpecificHeaderBox extends
FullBox('uuid', extended_type=1, version=0, flags=0)
 {
     GUID                          DRMID;
     unsigned int(32)              DataSize;
     unsigned int(8)[DataSize]     Data;
 }
```

[0055] DRMID specifies a UUID that uniquely identifies the protection system to which this header belongs. DataSize specifies the size in bytes of the data member. Data holds the data specific to the protection system.

[0056] Referring again to FIG. 7, an exemplary block diagram illustrates an exemplary structure for storing a track box. The track box acts as a container box storing boxes such as a media information box 702 as shown in FIG. 8.

[0057] Referring again to FIG. 8, an exemplary block diagram illustrates an exemplary structure for storing the media information box 702. The media information box 702 acts as a container box for storing boxes such as a sample description box ("stsd"). The sample description box stores boxes including a protected sample entry box 802, which stores the encrypted sample content. The sample entry box is shown again in FIG. 9.

[0058] Referring again to FIG. 9, an exemplary block diagram illustrates an exemplary structure for storing the protected sample entry box 802. The protected sample entry box 802 acts as a container box storing boxes such as a protection scheme information box. In contrast to the existing ISO base media file format, the protection scheme information box is stored in place of the sample entry in the sample description box to denote that the stream is encrypted. The protection scheme info box contains a scheme type box ('schm') so that the scheme is identifiable.

Additional Examples

[0059] The file format described herein represents a minimum file format that includes support for late binding of alternate audio and video content. This enables computing devices supporting legacy or emerging coders/decoders (codecs) to late-bind those streams at playback without burdening devices without support of those codecs with the additional download cost.

[0060] Embodiments of the disclosure support both fragmented and nonfragmented container files. For example, for adaptive streaming, the fragmented file format is used, but for digital copy from an optical disc, the nonfragmented file format is used.

Exemplary Operating Environment

[0061] By way of example and not limitation, computer readable media comprise computer storage media and communication media. Computer storage media store information such as computer readable instructions, data structures, program modules or other data. Communication media typically embody computer readable instructions, data structures, program modules, or other data in a modulated data signal such as a carrier wave or other transport mechanism and include any information delivery media. Combinations of any of the above are also included within the scope of computer readable media.

[0062] Although described in connection with an exemplary computing system environment, embodiments of the invention are operational with numerous other general purpose or special purpose computing system environments or configurations. Examples of well known computing systems, environments, and/or configurations that may be suitable for use with aspects of the invention include, but are not limited to, mobile computing devices, personal computers, server computers, hand-held or laptop devices, multiprocessor systems, gaming consoles, microprocessor-based systems, set top boxes, programmable consumer electronics, mobile telephones, network PCs, minicomputers, mainframe computers, distributed computing environments that include any of the above systems or devices, and the like.

[0063] Embodiments of the invention may be described in the general context of computer-executable instructions, such as program modules, executed by one or more computers or other devices. The computer-executable instructions may be organized into one or more computer-executable components or modules. Generally, program modules include, but are not limited to, routines, programs, objects, components, and data structures that perform particular tasks or implement particular abstract data types.

Aspects of the invention may be implemented with any number and organization of such components or modules. For example, aspects of the invention are not limited to the specific computer-executable instructions or the specific components or modules illustrated in the figures and described herein. Other embodiments of the invention may include different computer-executable instructions or components having more or less functionality than illustrated and described herein.

[0064] Aspects of the invention transform a general-purpose computer into a special-purpose computing device when configured to execute the instructions described herein.

[0065] The embodiments illustrated and described herein as well as embodiments not specifically described herein but within the scope of aspects of the invention constitute exemplary means for supporting the plurality of protection systems within a single container file in accordance with the ISO Base Media File Format, and exemplary means for storing the metadata for the plurality of protection systems in a single container file as an extension to the ISO Base Media File Format.

[0066] The order of execution or performance of the operations in embodiments of the invention illustrated and described herein is not essential, unless otherwise specified. That is, the operations may be performed in any order, unless otherwise specified, and embodiments of the invention may include additional or fewer operations than those disclosed herein. For example, it is contemplated that executing or performing a particular operation before, contemporaneously with, or after another operation is within the scope of aspects of the invention.

[0067] When introducing elements of aspects of the invention or the embodiments thereof, the articles "a," "an," "the," and "said" are intended to mean that there are one or more of the elements. The terms "comprising," "including," and "having" are intended to be inclusive and mean that there may be additional elements other than the listed elements.

[0068] Having described aspects of the invention in detail, it will be apparent that modifications and variations are possible without departing from the scope of aspects of the invention as defined in the appended claims. As various changes could be made in the above constructions, products, and methods without departing from the scope of aspects of the invention, it is intended that all matter contained in the above description and shown in the accompanying drawings shall be interpreted as illustrative and not in a limiting sense.

CLAIMS

What is claimed is:

1. A system for extending a media file format to support multiple protection systems in a single container file, said system comprising:

a memory area for storing a file (111) containing encrypted content (112), a sample encryption box (114), and a plurality of protection system header boxes (116) each associated with one or more of a plurality of protection systems, wherein the sample encryption box (114) identifies a key used to encrypt the encrypted content (112), and wherein each of the plurality of protection system header boxes (116) includes metadata for decoding the encrypted content (112) in accordance with one or more of the plurality of protection systems; and

a processor (108) programmed to:

receive, by a service provider (206), the file (111) from an encoding provider (204);

select one or more of the plurality of protection systems available to the service provider (206);

apply the selected protection systems to the content in the received file (111) using the key identified by the sample encryption box (114); and

store the file (111) with the applied protection systems in the memory area.

2. The system of claim 1, wherein the sample encryption box includes key mapping information to identify the key.

3. The system of claim 1, wherein the sample encryption box includes a key identifier.

4. The system of claim 1, wherein the sample encryption box and the plurality of protection system header boxes enable playback of the file with the plurality of protection systems.

5. The system of claim 1, wherein the file stored in the memory area conforms to the ISO Base Media File Format.

6. The system of claim 1, further comprising:

means for supporting the plurality of protection systems within a single container file in accordance with the ISO Base Media File Format; and

means for storing the metadata for the plurality of protection systems in a single container file as an extension to the ISO Base Media File Format.

7. A method comprising:

receiving a file (111) containing content and one or more encryption expressions, said content being encrypted by the encryption expressions;

applying a plurality of protection systems to the content using the encryption expressions from the received file (111); and

transmitting the file (111) with the content and the applied plurality of protection systems to one or more computing devices for decryption, wherein each of the computing devices decrypts the content using at least one of the applied plurality of protection systems.

8. The method of claim 7, wherein applying the plurality of protection systems to the content comprises adding metadata for each of the plurality of protection systems to the received file, said metadata defining one or more of the following: a decryption key, a rights object, and license information.

9. The method of claim 7, wherein receiving the file comprises receiving a file containing key mapping information, said content being encrypted using said key mapping information.

10. The method of claim 7, wherein applying the plurality of protection systems to the content comprises:

defining a protection system header box for each of the plurality of protection systems; and

including the defined protection system header box in the received file.

11. The method of claim 10, further comprising embedding license information into the protection system header box.

12. The method of claim 10, further comprising embedding in the protection system header box a reference to license information.

13. The method of claim 7, wherein applying the plurality of protection systems to the content comprises applying the plurality of protection systems to said content without creating another copy of the content.

14. The method of claim 7, wherein receiving the file comprises receiving, from a movie studio, a file corresponding to a movie.

15. The method of claim 7, wherein one or more computer-readable storage media have computer-executable components, said components comprising:

an interface component that, when executed by at least one processor, causes the at least one processor to receive, by a computing device, a file containing content and one or

more encryption expressions, said content being encrypted by the encryption expressions, said content further having a plurality of protection systems applied thereto, said file including metadata for each of the plurality of protection systems;

a detection component that, when executed by at least one processor, causes the at least one processor to select one of the plurality of protection systems supported by the computing device;

a parse component that, when executed by at least one processor, causes the at least one processor to obtain, from the metadata, license information for said one of the plurality of protection systems selected by the detection component; and

a transform component that, when executed by at least one processor, causes the at least one processor to decode the content based on the license information obtained by the parse component and based on the encryption expressions, wherein the interface component presents the decoded content to a user.

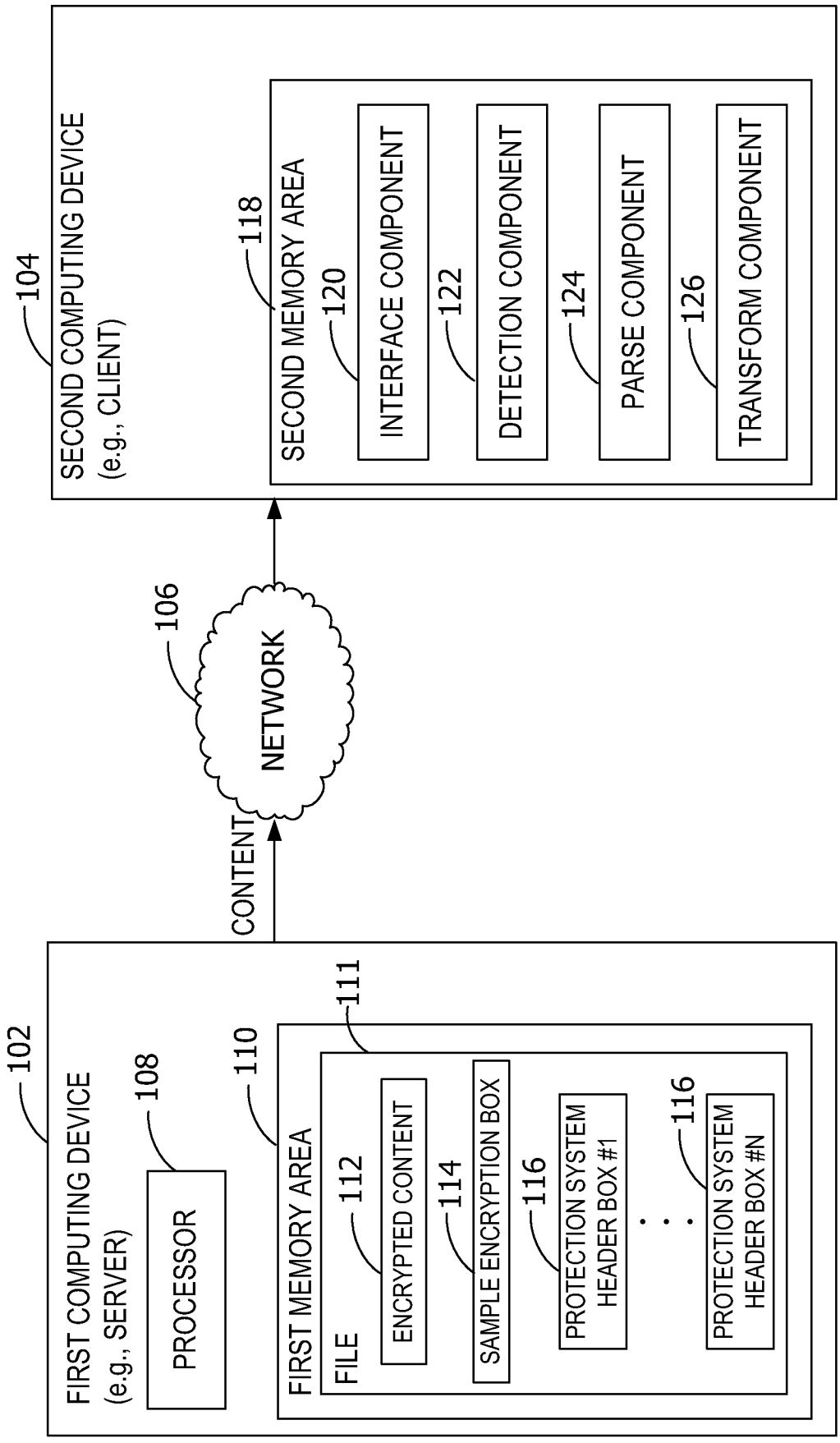
102
FIRST COMPUTING DEVICE
(e.g., SERVER)
108
PROCESSOR
110
FIRST MEMORY AREA
111
FILE
112
ENCRYPTED CONTENT
114
SAMPLE ENCRYPTION BOX
116
PROTECTION SYSTEM HEADER BOX #1
116
PROTECTION SYSTEM HEADER BOX #N
CONTENT
106
NETWORK
104
SECOND COMPUTING DEVICE
(e.g., CLIENT)
118
SECOND MEMORY AREA
120
INTERFACE COMPONENT
122
DETECTION COMPONENT
124
PARSE COMPONENT
126
TRANSFORM COMPONENT

FIG. 1

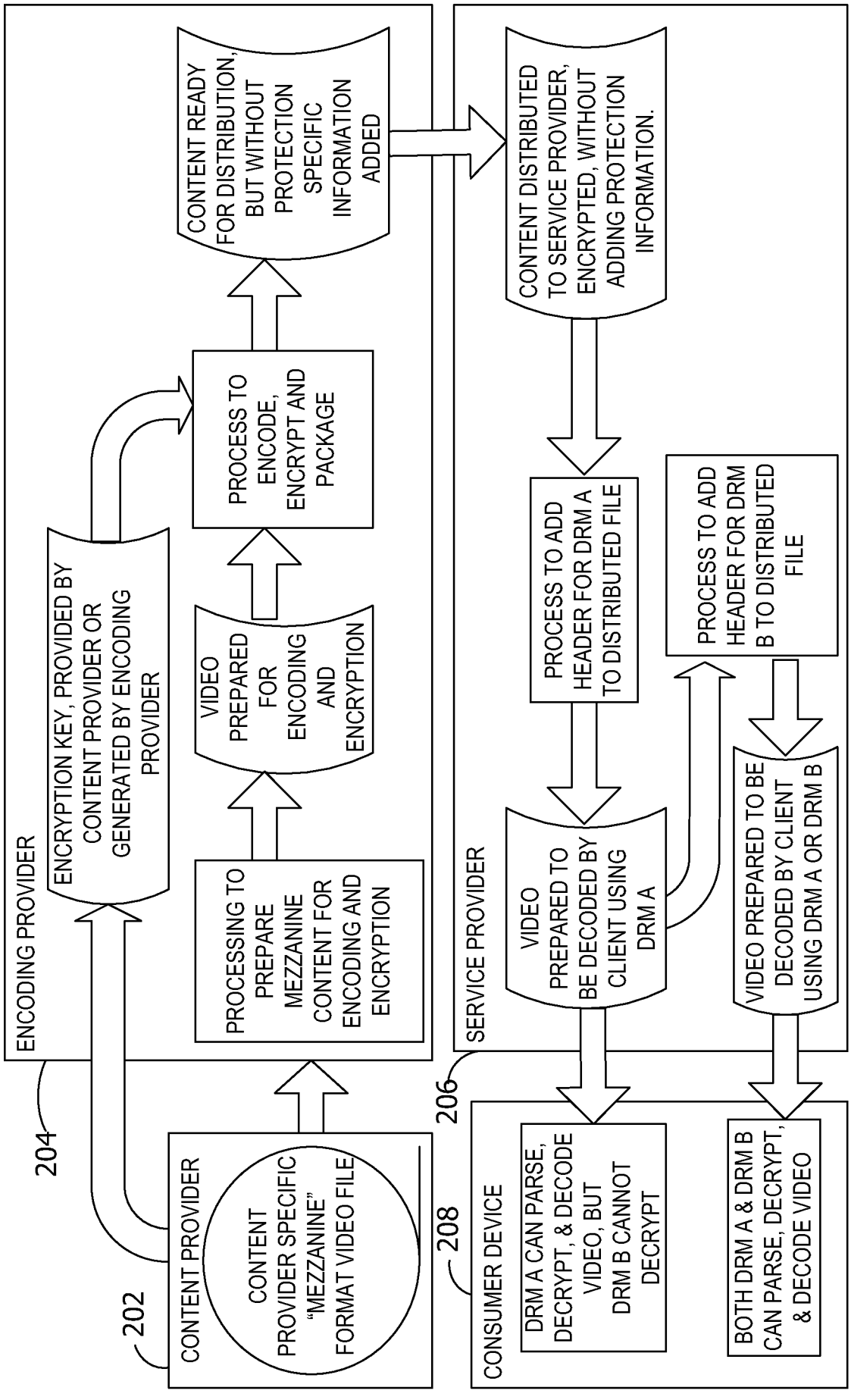
ENCODING PROVIDER
ENCRYPTION KEY, PROVIDED BY CONTENT PROVIDER OR GENERATED BY ENCODING PROVIDER
PROCESSING TO PREPARE MEZZANINE CONTENT FOR ENCODING AND ENCRYPTION
VIDEO PREPARED FOR ENCODING AND ENCRYPTION
PROCESS TO ENCODE, ENCRYPT AND PACKAGE
CONTENT READY FOR DISTRIBUTION, BUT WITHOUT PROTECTION SPECIFIC INFORMATION ADDED
204
CONTENT PROVIDER
CONTENT PROVIDER SPECIFIC "MEZZANINE" FORMAT VIDEO FILE
202
SERVICE PROVIDER
CONTENT DISTRIBUTED TO SERVICE PROVIDER, ENCRYPTED, WITHOUT ADDING PROTECTION INFORMATION.
PROCESS TO ADD HEADER FOR DRM A TO DISTRIBUTED FILE
PROCESS TO ADD HEADER FOR DRM B TO DISTRIBUTED FILE
VIDEO PREPARED TO BE DECODED BY CLIENT USING DRM A
VIDEO PREPARED TO BE DECODED BY CLIENT USING DRM A OR DRM B
206
CONSUMER DEVICE
208
DRM A CAN PARSE, DECRYPT, & DECODE VIDEO, BUT DRM B CANNOT DECRYPT
BOTH DRM A & DRM B CAN PARSE, DECRYPT, & DECODE VIDEO

FIG. 2

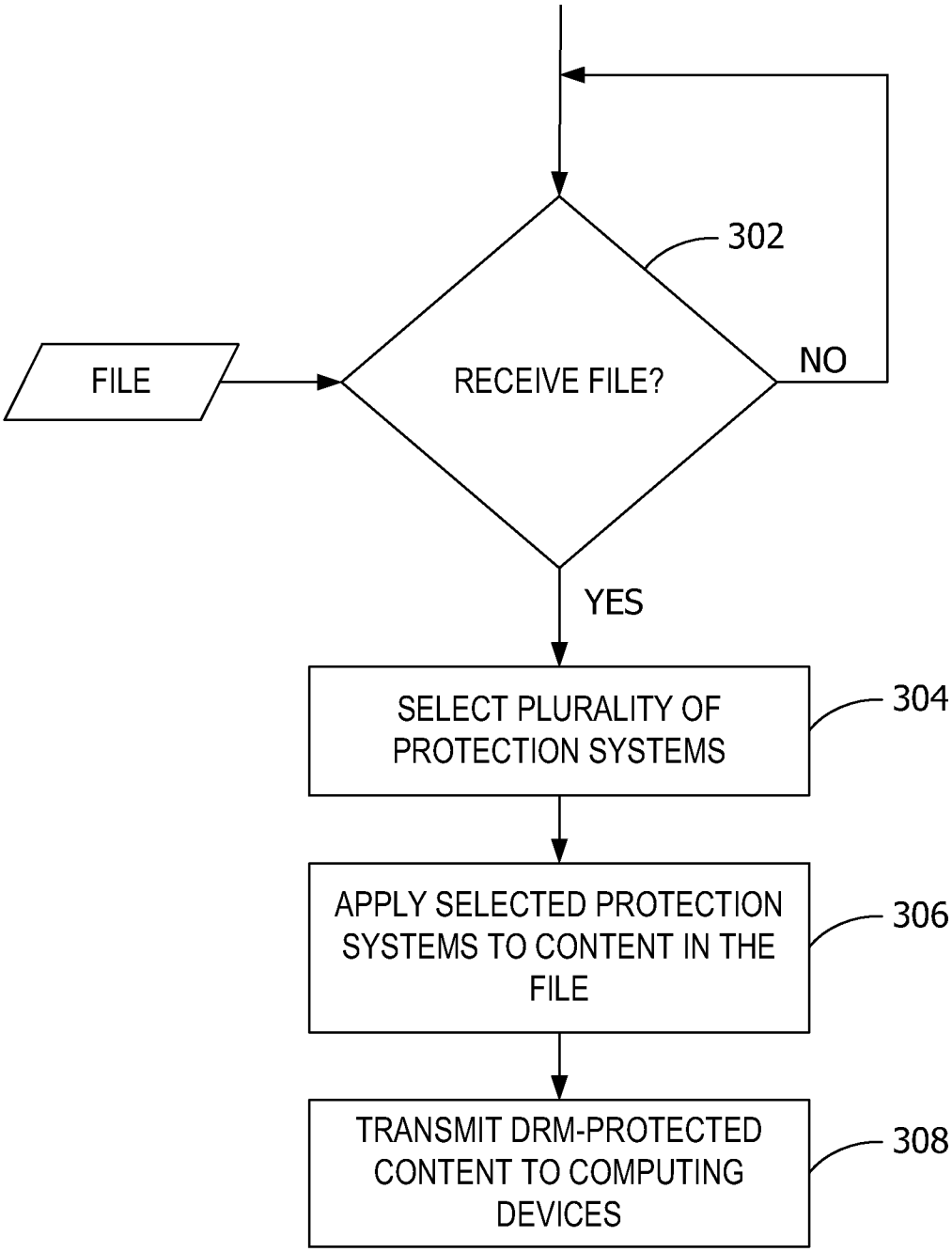
FILE
RECEIVE FILE?
302
NO
YES
SELECT PLURALITY OF PROTECTION SYSTEMS
304
APPLY SELECTED PROTECTION SYSTEMS TO CONTENT IN THE FILE
306
TRANSMIT DRM-PROTECTED CONTENT TO COMPUTING DEVICES
308

FIG. 3

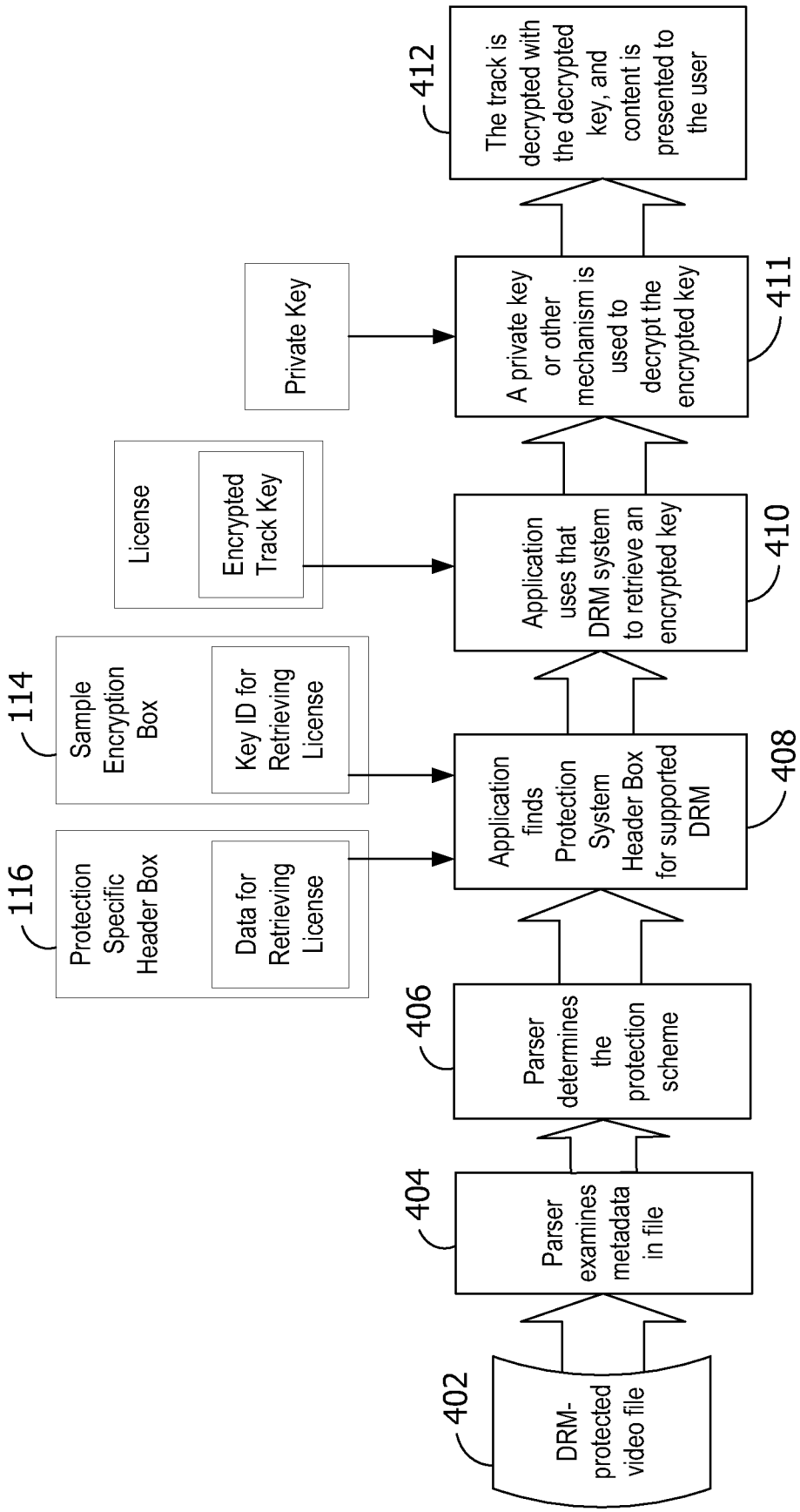
402
DRM-protected video file
404
Parser examines metadata in file
406
Parser determines the protection scheme
408
Application finds Protection System Header Box for supported DRM
410
Application uses that DRM system to retrieve an encrypted key
411
A private key or other mechanism is used to decrypt the encrypted key
412
The track is decrypted with the decrypted key, and content is presented to the user
Private Key
License
Encrypted Track Key
114
Sample Encryption Box
Key ID for Retrieving License
116
Protection Specific Header Box
Data for Retrieving License

FIG. 4

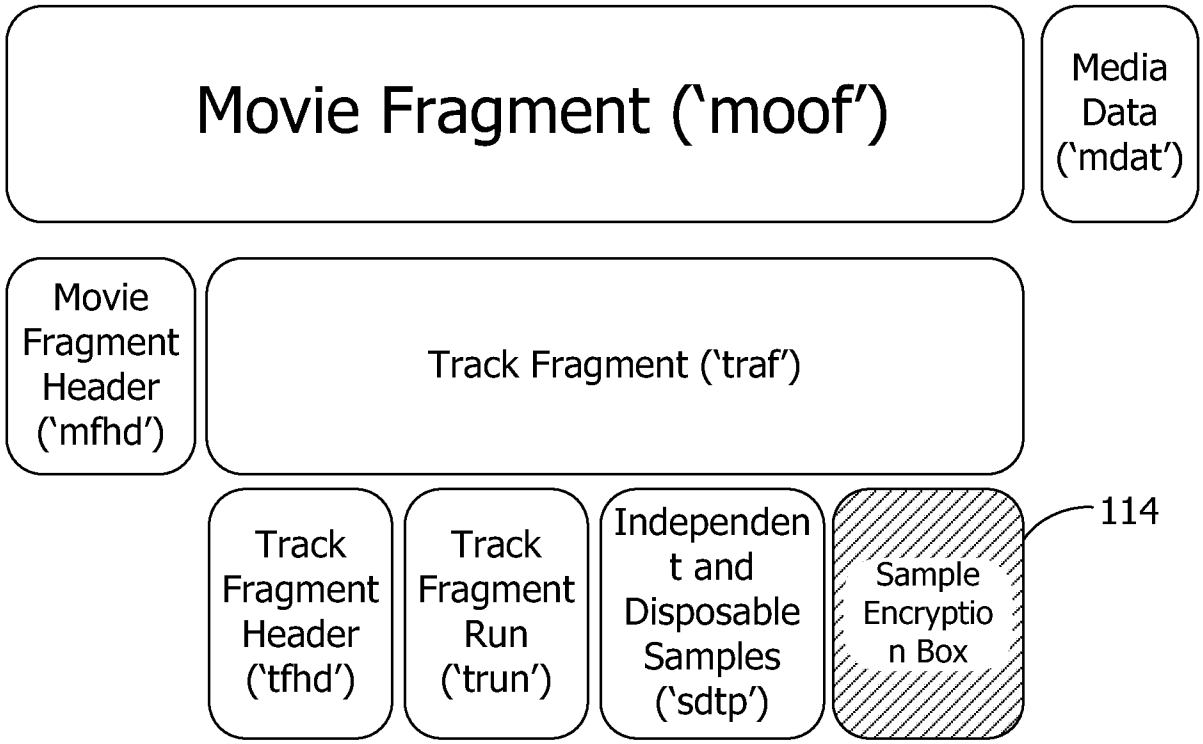
Movie Fragment ('moof')
Media Data ('mdat')
Movie Fragment Header ('mfhd')
Track Fragment ('traf')
Track Fragment Header ('tfhd')
Track Fragment Run ('trun')
Independent and Disposable Samples ('sdtp')
Sample Encryption Box
114

FIG. 5

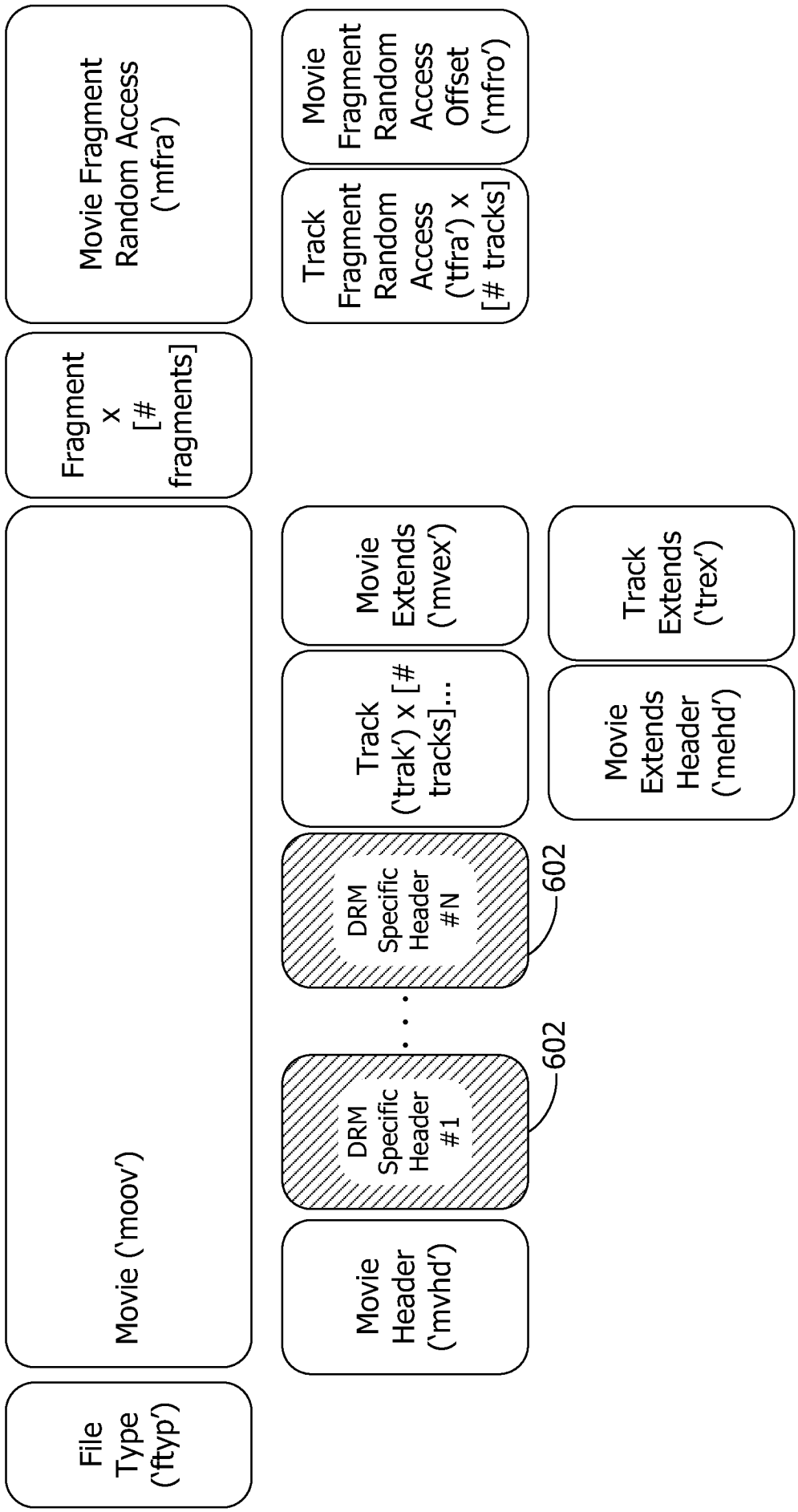
File Type ('ftyp')
Movie ('moov')
Movie Header ('mvhd')
DRM Specific Header #1
602
DRM Specific Header #N
602
Track ('trak') x [# tracks]...
Movie Extends ('mvex')
Movie Extends Header ('mehd')
Track Extends ('trex')
Fragment x [# fragments]
Movie Fragment Random Access ('mfra')
Track Fragment Random Access ('tfra') x [# tracks]
Movie Fragment Random Access Offset ('mfro')

FIG. 6

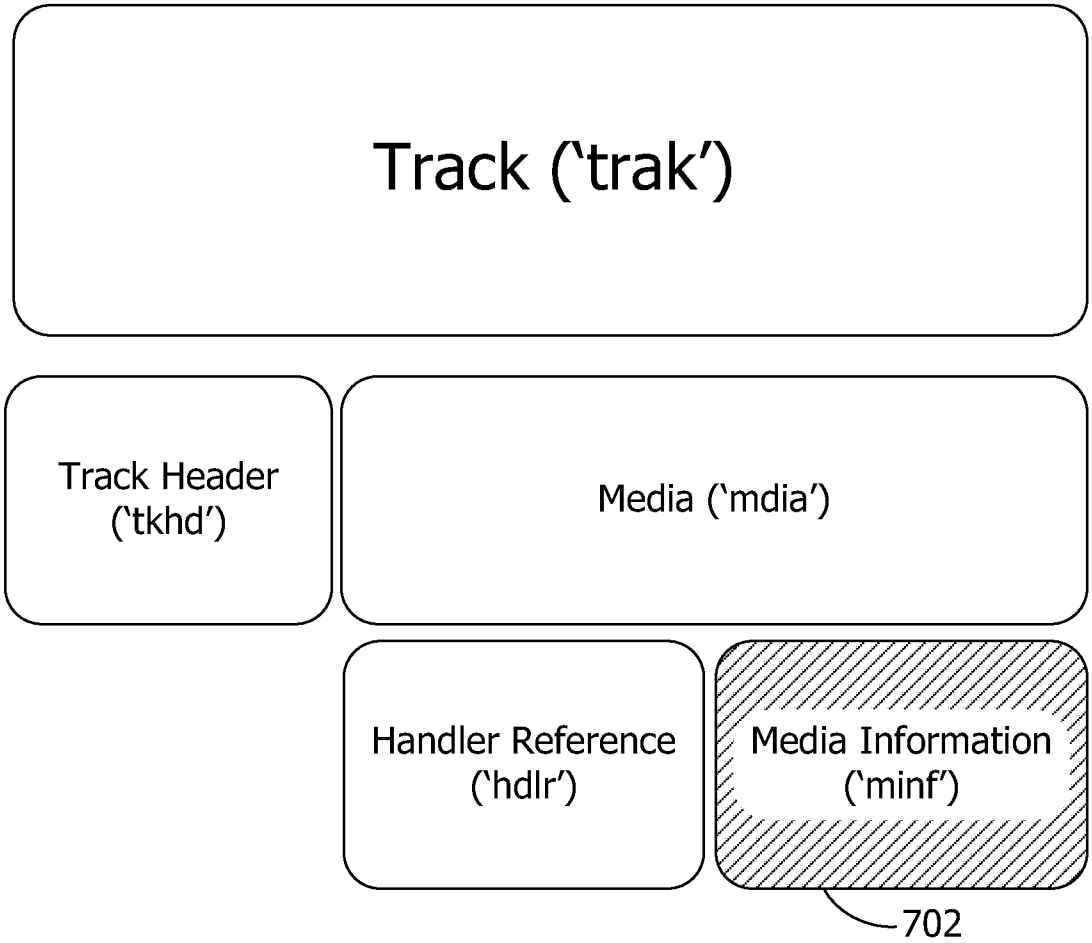
Track ('trak')
Track Header ('tkhd')
Media ('mdia')
Handler Reference ('hdlr')
Media Information ('minf')
702

FIG. 7

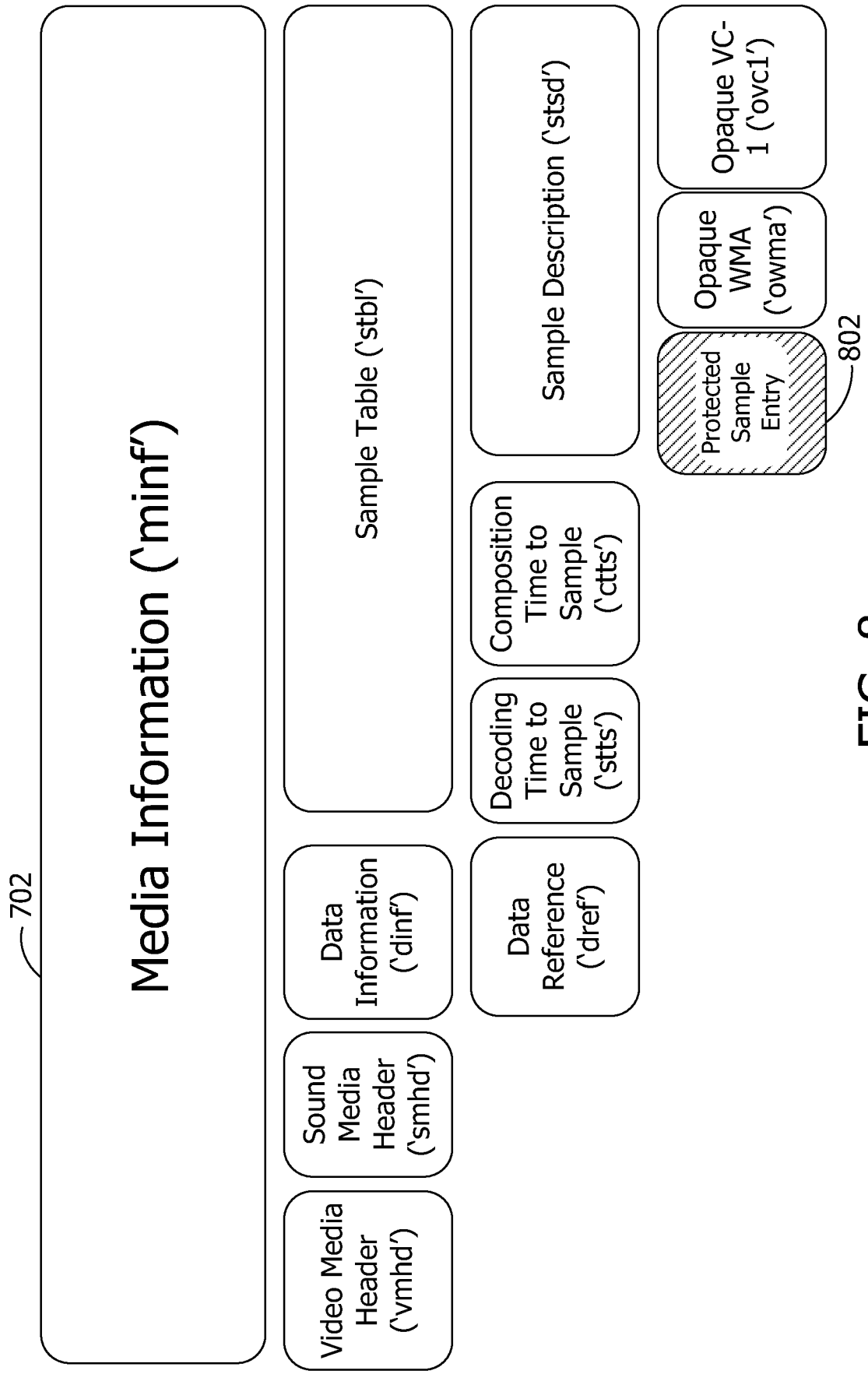
Media Information ('minf')
702
Video Media Header ('vmhd')
Sound Media Header ('smhd')
Data Information ('dinf')
Sample Table ('stbl')
Data Reference ('dref')
Decoding Time to Sample ('stts')
Composition Time to Sample ('ctts')
Sample Description ('stsd')
Protected Sample Entry
802
Opaque WMA ('owma')
Opaque VC-1 ('ovc1')

FIG. 8

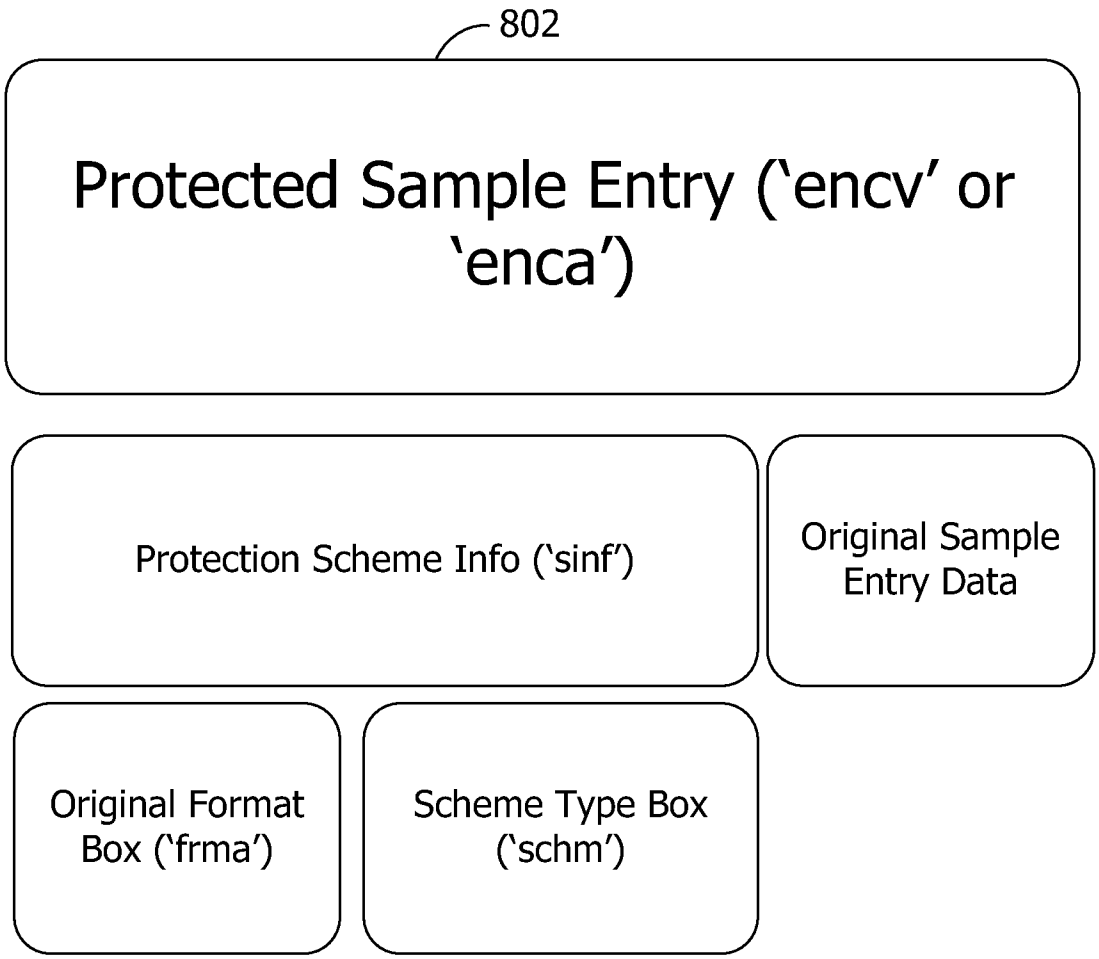
802
Protected Sample Entry ('encv' or 'enca')
Protection Scheme Info ('sinf')
Original Sample Entry Data
Original Format Box ('frma')
Scheme Type Box ('schm')

FIG. 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2009/069332

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/14(2006.01)i, G06F 21/24(2006.01)i, G06F 15/16(2006.01)i, G06F 9/06(2006.01)i

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)

H04L 9/14; G06F 12/14; G06F 15/16; G06F 17/60; H04L 9/00

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

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & Keywords: multiple, protection, content and protection

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2006-0090082 A1 (JOHN G. APOSTOLOPOULOS) 27 April 2006. See abstract, figs.1,3 and claims 1-21.	1-15
A	US 2008-0313264 A1 (FLORIAN PESTONI) 18 December 2008. See abstract, figs.1-3 and claims 1-12.	1-15
A	US 2006-0095382 A1 (JAMES M. MAHLBACHER) 04 May 2006. See abstract, figs.2A,3 and claims 1-9,17-26.	1-15

☐ 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 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

"T" 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	Date of mailing of the international search report
22 JULY 2010 (22.07.2010)	**22 JULY 2010 (22.07.2010)**

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex-Daejeon, 139 Seonsa-ro, Seo-gu, Daejeon 302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

Yang, Jong Phil

Telephone No. 82-42-481-8595

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2009/069332

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006-0090082 A1	27.04.2006	EP 1803048 A1	04.07.2007
		KR 10-2007-0054734 A	29.05.2007
		WO 2006-047368 A1	04.05.2006
US 2008-0313264 A1	18.12.2008	None	
US 2006-0095382 A1	04.05.2006	CN 1770170 A	10.05.2006
		CN 1770170 C0	10.05.2006