PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being electronically filed with the United States Patent and Trademark Office on May 27, 2014 at or before 11:59 p.m. Pacific Time under the Rules of 37 CFR § 1.8.

/Katrina Lee/
Katrina Lee

Appl No.	: 13/340,623	Confirmation No. 1094
Applicant	: Michael George Kiefer et al.	
Filed	: December 29, 2011	
Title	: Systems and Methods for Playing Back Alternative Streams of Protected Content Protected Using Common Cryptographic Information	
TC/A.U.	: 2434	
Examiner	: Abiy Getachew	
Docket No.	: D1-02359A	
Customer No.	: 71897	

AMENDMENT

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

2400 E. Katella, Suite 1050
Anaheim, CA 92806
May 27, 2014

Commissioner:

In response to the Office action mailed November 27, 2013, please amend the above-identified application as follows:

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 15 of this paper.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0900
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A playback device, comprising:

a processor;

memory containing a client application;

wherein the client application configures the processor to:

obtain ~~request~~ a top level index file identifying a plurality of separate container files each containing one of a plurality of alternative streams of protected video ~~content~~, ~~where~~ wherein each of the alternative streams of protected video ~~content~~ includes video frames that are encrypted using a common set of frame keys comprising a plurality of different frame keys ~~cryptographic information~~, wherein each of the container files containing the alternative streams of protected video comprises (i) an encrypted copy of the common set of frame keys and (ii) a set of DRM information that identifies encrypted portions of the video frames and frame keys to utilize in accessing the encrypted portions of the video frames, and wherein the set of DRM information in each of the plurality of alternative streams of protected video references the same common set of frame keys;

obtain ~~the common cryptographic information~~ an encrypted copy of the common set of frame keys from a given container file and decrypt the encrypted copy of the common set of frame keys using a content key;

obtain a set of DRM information from the given container file;

~~request~~ obtain portions of protected video ~~content~~ from the given container file containing ~~at least~~ one of the plurality of alternative streams of protected video ~~content~~;

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0901
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

~~access the~~ decrypt encrypted video frames from the obtained portions of video ~~protected content~~ using the decrypted copy of the common set of frame keys according to the obtained set of DRM information ~~cryptographic information~~; and

playback the obtained portions of video ~~content~~.

2. (Currently Amended) The playback device of claim 1, wherein:

the alternative streams of protected video ~~content are alternative streams of protected video~~ are encoded at different maximum bitrates using different sets of encoding parameters; and

~~each of the alternative streams of protected video includes DRM information indicating portions of frames of video that are encrypted and identifying at least a portion of the common cryptographic information used to access the encrypted portions of the frames of video; and~~

the client application further configures the processor to~~:~~

~~obtain a protected frame of video from one of the alternative streams of protected video;~~

~~obtain DRM information indicating a portion of the protected frame of video that is encrypted;~~

~~identify at least a portion of the common cryptographic information that is used to access the encrypted portion of the protected frame using the DRM information;~~

~~decrypt the encrypted portion of the protected frame of video using the identified portion of the common cryptographic information; and~~

decode the encoded frames ~~frame~~ of video prior to playback of the obtained portions of video.

3. (Cancelled)

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0902
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

4. (Currently Amended) The playback device of claim 1[[3]], wherein:

the container files containing each of the alternative streams of protected video ~~content~~ comprise at least one header that includes ~~including the common cryptographic information and~~ information that describes the encoding of the stream of protected video ~~content~~; and

the top level index file identifies the location of the at least one header within each container file.

5. (Currently Amended) The playback device of claim 1[[4]], wherein the common ~~cryptographic information is a~~ set of frame ~~encryption~~ keys is part of a frame key table that is common to each of the plurality of alternative streams.

6. (Currently Amended) The playback device of claim 1[[5]], wherein:

~~the common set of encryption keys is encrypted; and~~

the client application further configures the processor to securely receive the content key ~~cryptographic information used to unencrypt the common set of encryption keys~~.

7. (Cancelled)

8. (Currently Amended) The playback device of claim 1[[7]], wherein:

each container file containing one of the alternative streams of protected video ~~content~~ further comprises an index; and

the client application further configures the processor to ~~request a portion of content from one of the container files by configuring the processor to~~:

request at least a portion of an index from the given container file;

identify the portion of the given container file containing a specific portion of video ~~content~~ using the index; and

request the identified portion of the given container file.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0903
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

9. (Currently Amended) The playback device of claim 1[[4]], wherein the container files are Matroska container files.

10. (Currently Amended) The playback device of claim 9, wherein the encrypted copy of the common set of frame keys ~~cryptographic information~~ is stored in a common DRM Header element contained within a Tracks element within each of the Matroska container files containing the alternative streams of protected video ~~content~~.

11. (Cancelled)

12. (Currently Amended) The playback device of claim 10[[11]], wherein the client application further configures the processor to:

obtain the content key ~~cryptographic information~~ that can be used to decrypt ~~unencrypt~~ the encrypted copy of the set of ~~encryption~~ frame keys stored within the common DRM Header element; and

decrypt ~~unencrypt~~ the encrypted copy of the set of ~~encryption~~ frame keys stored within the common DRM Header element using the obtained content key ~~cryptographic information~~.

13. (Currently Amended) The playback device of claim 10, wherein the client application configures the processor to obtain the common DRM Header element by requesting a Tracks element from one of the Matroska container files identified in the top level index file.

14. (Currently Amended) The playback device of claim 13, wherein:

each Mastroska container file containing an alternative stream of protected video ~~content~~ further comprises an index contained within a Cues element; and

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0904
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

the client application further configures the processor to request a portion of video ~~content~~ from one of the Matroska container files by configuring the processor to:

request at least a portion of a Cues element from a Matroska container file containing one of the alternative streams of protected video ~~content~~;

identify a portion of the Matroska container file containing a specific portion of video ~~content~~ using at least one CueTrackPosition element within the Cues element; and

request the portion of the Matroska container file identified by the at least one CueTrackPosition element.

15. (Original) The playback device of claim 14, wherein the index comprises a plurality of CueTrackPosition elements that identify the location of a plurality of Cluster elements within the Matroska container file.

16. (Currently Amended) The playback device of claim 15, wherein:

each Cluster element contains a plurality of BlockGroup elements including encoded portions of video ~~content~~;

a CueTrack Position element indexes each Cluster element; and

each CueTrackPosition element includes the size of the Cluster element that it indexes.

17. (Currently Amended) The playback device of claim 14, wherein:

~~the alternative streams of protected content are alternative streams of protected video;~~

each of the Matroska container files containing an alternative stream of protected video includes a set of BlockGroup elements that each contain a DRMInfo element ~~in a BlockGroup element containing a~~ and an encrypted ~~protected~~ frame of video, where the DRMInfo element is a part of the set of DRM information for each of the Matroska container files ~~indicates at least a portion of the protected frames of video~~

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0905
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

~~that is encrypted and identifies at least a portion of the common cryptographic information used to access the at least one encrypted portion of the protected frame of video~~; and

the client application further configures the processor to ~~access~~ decrypt encrypted video frames of the obtained portions of video ~~in a stream of protected video~~ using the decrypted copy of the common set of frame keys ~~cryptographic information~~ by configuring the processor to:

obtain a BlockGroup containing ~~a protected~~ an encrypted frame of video;

parse the BlockGroup element to obtain a DRMInfo element indicating at least a portion of the encrypted ~~protected~~ frame of video that is encrypted using ~~an encryption~~ a frame key from the common set of frame ~~encryption~~ keys;

decrypt the at least one encrypted portion of the encrypted ~~protected~~ frame of video using the identified frame ~~encryption~~ key; and

decode the frame of video.

18. (Currently Amended) A method of performing adaptive bitrate streaming using a plurality of alternative streams of protected video ~~content~~, ~~where each of the streams of protected content is protected using common cryptographic information,~~ the method comprising:

obtaining ~~requesting~~ a top level index file identifying a plurality of separate container files each containing one of a plurality of alternative streams of protected video ~~content~~ using a playback device, ~~where~~ wherein each of the alternative streams of protected video ~~content~~ include video frames that are encrypted using a common set of frame keys comprising a plurality of different frame keys ~~cryptographic information~~, and wherein each of the container files containing the alternative streams of protected video comprises (i) an encrypted copy of the common set of frame keys and (ii) a set of DRM information that identifies encrypted portions of the video frames and frame keys to utilize in accessing the encrypted portions of the video frames, and wherein the set of

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0906
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

DRM information in each of the plurality of alternative streams of protected video references the same common set of frame keys;

obtaining ~~the common cryptographic information~~ an encrypted copy of the common set of frame keys from a given container file and decrypting the encrypted copy of the common set of frame keys using a content key using the playback device;

obtaining a set of DRM information from the given container file using the playback device;

~~requesting~~ obtaining portions of video ~~content~~ from the given container file containing ~~at least~~ one of the plurality of alternative streams of protected video ~~content~~ using the playback device;

~~accessing the~~ decrypting encrypted video frames from the obtained portions of video ~~protected content~~ using the playback device and the decrypted copy of the common set of frame keys according to the obtained set of DRM information ~~cryptographic information~~; and

playing back the obtained portions of video ~~content~~ using the playback device.

19. (Currently Amended) The method of claim 18, wherein:

the alternative streams of protected video ~~content~~ are encoded at different maximum bitrates using different sets of encoding parameters ~~alternative streams of protected video~~; and

~~each of the alternative streams of protected video includes DRM information indicating portions of frames of video that are encrypted and identifying at least a portion of the common cryptographic information used to access the encrypted portions of the frames of video; and~~

the method further comprises~~:~~

~~obtaining a protected frame of video from one of the alternative streams of protected video using the playback device;~~

~~obtaining DRM information indicating a portion of the protected frame of video that is encrypted using the playback device;~~

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0907
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

~~identify at least a portion of the common cryptographic information that is used to access the encrypted portion of the protected frame using the playback device and the DRM information;~~

~~decrypting the encrypted portion of the protected frame of video using the playback device and the identified portion of the common cryptographic information; and~~

decoding the encoded frames ~~frame~~ of video using the playback device prior to playback of the obtained portions of video.

20. (Cancelled)

21. (Currently Amended) The method of claim 18[[20]], wherein:

the container files containing each of the alternative streams of protected video ~~content~~ comprise at least one header that includes ~~including the common cryptographic information and~~ information that describes the encoding of the stream of protected video ~~content~~; and

the top level index file identifies the location of the at least one header within each container file.

22. (Currently Amended) The method of claim 18[[21]], wherein the common ~~cryptographic information is a~~ set of frame ~~encryption~~ keys is part of a frame key table that is common to each of the plurality of alternative streams.

23. (Currently Amended) The method of claim 18[[22]], wherein:

~~the set of encryption keys is encrypted so that it is accessible using cryptographic information obtained by the playback device; and~~

the method further ~~comprising~~ comprises securely obtaining the content key ~~cryptographic information~~ using the playback device.

24. (Cancelled)

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0908
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

25. (Currently Amended) The method of claim 18[[24]], wherein the ~~at least one encryption~~ content key is ~~encrypted using at least one encryption key included in the cryptographic information~~ bound to the playback device.

26. (Currently Amended) The method of claim 21[[23]], further comprising obtaining[[the]] an encrypted copy of the common set of frame keys ~~cryptographic information~~ by requesting at least one header of a container file identified in the top level index file using the playback device.

27. (Currently Amended) The method of claim 26, wherein:

each container file containing one of the alternative streams of protected video ~~content~~ further comprises an index; and

the method further comprising:

requesting at least a portion of an index from the given container file using the playback device;

identify the portion of the given container file containing a specific portion of video ~~content~~ using the playback device and the index; and

requesting the identified portion of the given container file using the playback device.

28. (Original) The method of claim 21, wherein the container files are Matroska container files.

29. (Currently Amended) The method of claim 28, wherein the encrypted copy of the common set of frame keys ~~cryptographic information~~ is stored in a common DRM Header element contained within a Tracks element within each of the Matroska container files containing the alternative streams of protected video ~~content~~.

30. (Cancelled)

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0909
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

31. (Cancelled)

32. (Currently Amended) The method of claim 29[[30]], further comprising obtaining the common DRM Header element by requesting a Tracks element from one of the Matroska container files identified in the top level index file.

33. (Currently Amended) The method of claim 32, wherein:

each Mastroska container file containing an alternative stream of protected video ~~content~~ further comprises an index contained within a Cues element; [[and]]

the method further comprises:

requesting at least a portion of a Cues element from a Matroska container file containing one of the alternative streams of protected video ~~content~~ using the playback device;

identifying a portion of the Matroska container file containing a specific portion of video ~~content~~ using the playback device and at least one CueTrackPosition element within the Cues element; and

requesting the portion of the Matroska container file identified by the at least one CueTrackPosition element.

34. (Original) The method of claim 33, wherein the index comprises a plurality of CueTrackPosition elements that identify the location of a plurality of Cluster elements within the Matroska container file.

35. (Currently Amended) The method of claim 34, wherein:

each Cluster element contains a plurality of BlockGroup elements including encoded portions of video ~~content~~;

a CueTrack Position element indexes each Cluster element; and

each CueTrackPosition element includes the size of the Cluster element that it indexes.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0910
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

36. (Currently Amended) The method of claim 33, wherein:

~~the alternative streams of protected content are alternative streams of protected video;~~

each of the Matroska container files containing an alternative stream of protected video includes a set of BlockGroup elements that each contain a DRMInfo element ~~in a BlockGroup element containing a protected~~ and an encrypted frame of video, where the DRMInfo element is a part of the set of DRM information for each of the Matroska container files ~~indicates at least a portion of the protected frames of video that is encrypted and identifies at least a portion of the common cryptographic information used to access the at least one encrypted portion of the protected frame of video~~; and

the method further comprising:

obtaining a BlockGroup containing ~~a protected~~ an encrypted frame of video using the playback device;

parsing the BlockGroup element to obtain a DRMInfo element indicating at least a portion of the encrypted ~~protected~~ frame of video that is encrypted using the playback device and ~~an encryption~~ a frame key from the common set of frame ~~encryption~~ keys;

decrypting the at least one encrypted portion of the encrypted ~~protected~~ frame of video using the playback device and the identified frame ~~encryption~~ key; and

decoding the frame of video using the playback device.

37. (Currently Amended) A non-transitory machine readable medium containing processor instructions, where execution of the instructions by a processor causes the processor to perform a process comprising:

obtaining ~~requesting~~ a top level index file identifying a plurality of separate container files each containing one of a plurality of alternative streams of protected video ~~content~~, ~~where~~ wherein each of the alternative streams of protected video ~~content~~

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0911
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

include video frames that are encrypted using a common set of frame keys comprising a plurality of different frame keys ~~cryptographic information~~, and wherein each of the container files containing the alternative streams of protected video comprises (i) an encrypted copy of the common set of frame keys and (ii) a set of DRM information that identifies encrypted portions of the video frames and frame keys to utilize in accessing the encrypted portions of the video frames, and wherein the set of DRM information in each of the plurality of alternative streams of protected video references the same common set of frame keys;

obtaining ~~the common cryptographic information~~ an encrypted copy of the common set of frame keys from a given container file and decrypting the encrypted copy of the common set of frame keys using a content key;

obtaining a set of DRM information from the given container file;

~~requesting~~ obtaining portions of video ~~content~~ from the given container file containing ~~at least~~ one of the plurality of alternative streams of protected video ~~content~~;

~~accessing the~~ decrypting encrypted video frames from the obtained portions of video ~~protected content~~ using the decrypted copy of the common set of frame keys according to the obtained set of DRM information ~~cryptographic information~~; and

playing back the obtained portions of video ~~content~~.

38. (Currently Amended) The non-transitory machine readable medium of claim 37, wherein:

the alternative streams of protected video ~~content~~ are encoded at different maximum bitrates using different sets of encoding parameters ~~alternative streams of protected video~~; and

~~each of the alternative streams of protected video includes DRM information indicating portions of frames of video that are encrypted and identifying at least a portion of the common cryptographic information used to access the encrypted portions of the frames of video; and~~

execution of the instructions by a processor also causes the processor to perform a process comprising~~:~~

~~obtaining a protected frame of video from one of the alternative streams of protected video;~~

~~obtaining DRM information indicating a portion of the protected frame of video that is encrypted;~~

~~identify at least a portion of the common cryptographic information that is used to access the encrypted portion of the protected frame using the DRM information;~~

~~decrypting the encrypted portion of the protected frame of video using and the identified portion of the common cryptographic information; and~~

decoding the <u>encoded frames</u> ~~frame~~ of video <u>prior to playback of the obtain portions of video</u>.

39. (Cancelled)

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0913
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

REMARKS/ARGUMENTS

Summary of the Amendments

Claims 1, 2, 4-6, 8-10, 12-14, 16-19, 21-23, 25-27, 29, 32, 33, and 35-38 are amended. Claims 3, 7, 11, 20, 24, 30, 31, and 39 are cancelled. After entry of these amendments, claims 1, 2, 4-6, 8-10, 12-19, 21-23, 25-29, and 32-38 will be pending. Support for all the amendments can be found throughout the specification, including in paragraphs [0083], [0084], [0089], [00107], [00115], [00118], and [00120].

Summary of the Office Action

The Office action dated November 27, 2013 contained the following objections and rejections:

- claims 37 and 38 are rejected under 35 U.S.C. § 101 because the claimed invention is allegedly directed to a non-statutory subject matter;
- claims 1, 18, and 37 are rejected under pre-AIA 35 U.S.C. § 103(a) as allegedly being unpatentable over U.S. Patent Publication No. 2009/0290706 to Amini et al. (the Amini publication) in view of PCT Patent Publication No. 2011/103364 to Thorwirth (the Thorwirth publication);
- claims 2-8, 19-20, and 38-39 are rejected under pre-AIA 35 U.S.C. § 103(a) as allegedly being unpatentable over the Amini et al. publication in view of the Thorwirth publication and further in view of U.S. Patent Publication No. 2009/0328228 to Schnell (the Schnell publication); and
- claims 9-17 and 21-36 are rejected under pre-AIA 35 U.S.C. § 103(a) as allegedly being unpatentable over the Amini et al. publication in view of the Thorwirth publication and further in view of the Schnell publication and further in view of U.S. Patent Publication No. 2009/0132721 to Soroushian et al. (the Soroushian publication).

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0914
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

The Amini Publication

The Amini publication generally describes "[t]echniques for securely and adaptively delivering multimedia content are disclosed in which a set of alternate access units for each time slot is obtained" (Amini publication [abstract]). As illustrated in Figure 2 of the Amini publication, "data processing system 200 of FIG. 2 generates a stream that offers a choice from multiple access units for a single time slot within which the access units are to be encrypted" (Amini publication, ¶ [0030]). "Multimedia stream source 210 offers unencoded access units (e.g., frames) to a multi-encoder platform 220" (Amini publication, ¶ [0031]). "Platform 220 generates multiple encoded access units for each offered unencoded access unit and passes off the multiple encoded access units to a stream thinner 230" (Amini publication, ¶ [0031]). "The thinned access unit streams are input into encryptor 240, where they are encrypted. The output of encryptor 240 is finally sent to an output device 250, such as a network protocol formatter or a file writer" (Amini publication, ¶ [0032]). As explained in the Amini publication, "the problem of encrypting a multimedia stream that may have multiple access units for each time slot is overcome by selecting the encryption index for each access unit such that the encryption index always increases, regardless of which access unit the delivery system (e.g., server) selects for transmission" (Amini publication, ¶ [0043]). The Amini publication describes three methods to overcome its stated problem, "Method 1: Each Stream has a Different Key", "Method 2: Each Stream Uses the Same Key", and "Method 3: One Stream may not have Index Gaps" (Amini publication, pages 4 and 5).

Rejection of Claims 37 and 38 for Non-Statutory Subject Matter

Claims 37 and 38 are rejected under 35 U.S.C. § 101 because the claimed invention is allegedly directed to a non-statutory subject matter. Applicant respectfully disagrees, but adopts the recommendation in the Office action and has amended claims 37 and 38 to recite "non-transitory machine readable medium". Applicant therefore requests withdrawal of the rejection.

Patentability of Claim 1

In the Office action dated November 27, 2013, claim 1 is rejected under pre-AIA 35 U.S.C. § 103(a) as being unpatentable over the Amini publication in view of the Thorwirth publication. Applicant respectfully disagrees with this rejection. However, in order to advance prosecution, Applicant has amended claim 1. Applicant respectfully submits that claim 1 as amended is not disclosed or taught by the combination of the cited references.

The Amini publication generally describes "[t]echniques for securely and adaptively delivering multimedia content are disclosed in which a set of alternate access units for each time slot is obtained" (Amini publication [abstract]). As explained in the Amini publication, "the problem of encrypting a multimedia stream that may have multiple access units for each time slot is overcome by selecting the encryption index for each access unit such that the encryption index always increases, regardless of which access unit the delivery system (e.g., server) selects for transmission" (Amini publication, ¶ [0043]). The Amini publication describes three methods to overcome its stated problem, "Method 1: Each Stream has a Different Key", "Method 2: Each Stream Uses the Same Key", and "Method 3: One Stream may not have Index Gaps". The Office action specifically cites paragraph 0054 of the Amini publication which states that, per Method 2, "In case a very simple key management system is used that allows only a single key per stream, then all alternate streams must use the same key. In that situation, the same index should not be used more than once …".

As far as Applicant can tell from reviewing the Amini publication, Amini only describes the three methods of using keys for streams listed above (see Method 1, Method 2, and Method 3). Method 1 of the Amini publication uses a different key for each stream, whereas amended claim 1 recites that "wherein the set of DRM information in each of the plurality of alternative streams of protected video references the same common set of frame keys". Method 2 of the Amini publication has each stream use the same key, whereas amended claim 1 recites that "each of the alternative streams of protected video includes video frames that are encrypted using a common set of frame keys comprising a plurality of different frame keys" (i.e. several

keys). Method 3 of the Amini publication relates to "where a multimedia stream is self-contained, is delivered in a loss free environment (e.g., downloaded), and played back as is. An example of such a case is an MP3 audio file" (Amini publication, ¶ [0060]). Similarly to Method 1 and Method 2 of the Amini publication, Method 3 fails to disclose the above recited aspects of amended claim 1.

In addition, Applicant could find no mention within the Amini publication of an operation involving "obtain an encrypted copy of the common set of frame keys from a given container file and decrypt the encrypted copy of the common set of frame keys using a content key" or "decrypt encrypted video frames from the obtained portions of video using the decrypted copy of the common set of frame keys according to the obtained set of DRM information" as recited in amended claim 1. Furthermore, Applicant respectfully submits that the other cited references (e.g., the Thorwirth publication, the Schnell publication, and the Soroushian publication) do not satisfy these deficiencies. For at least the reasons discussed above, Applicant respectfully submits that claim 1 is allowable over the cited art of record and requests withdrawal of the rejection.

Patentability of Claims 2, 4-6, 8-10, and 12-17

Claims 2, 4-6, 8-10, and 12-17 depend from claim 1. Applicant respectfully submits that claims 2, 4-6, 8-10, 12-17 are allowable for at least the reasons provided above with respect to claim 1.

Patentability of Claim 18

The Office action rejects claim 18 based upon the same combination of references as cited with respect to claim 1. For reasons similar to those outlined above with respect to claim 1, Applicant respectfully submits that the prior art of record does not disclose or suggest at least the following from claim 18: "each of the alternative streams of protected video include video frames that are encrypted using a common set of frame keys comprising a plurality of different frame keys", "wherein the set of DRM information in each of the plurality of alternative streams of protected video references

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0917
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

the same common set of frame keys", "obtaining an encrypted copy of the common set of frame keys from a given container file and decrypting the encrypted copy of the common set of frame keys using a content key", and "decrypting encrypted video frames from the obtained portions of video using the playback device and the decrypted copy of the common set of frame keys according to the obtained set of DRM information". Accordingly, Applicant respectfully submits that claim 18 is allowable over the cited art of record and requests withdrawal of the rejection.

Patentability of Claims 19, 21-23, 25-29, and 32-36

Claims 19, 21-23, 25-29, and 32-36 depend from claim 18. Applicant respectfully submits that claims 19, 21-23, 25-29, and 32-36 are allowable for at least the reasons provided above with respect to claim 18.

Patentability of Claim 37

The Office action rejects claim 37 based upon the same combination of references as cited with respect to claim 1. For reasons similar to those outlined above with respect to claim 1, Applicant respectfully submits that the prior art of record does not disclose or suggest at least the following from claim 37: "each of the alternative streams of protected video include video frames that are encrypted using a common set of frame keys comprising a plurality of different frame keys", "wherein the set of DRM information in each of the plurality of alternative streams of protected video references the same common set of frame keys", "obtaining an encrypted copy of the common set of frame keys from a given container file and decrypting the encrypted copy of the common set of frame keys using a content key", and "decrypting encrypted video frames from the obtained portions of video using the decrypted copy of the common set of frame keys according to the obtained set of DRM information". Accordingly, Applicant respectfully submits that claim 37 is allowable over the cited art of record and requests withdrawal of the rejection.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0918
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Patentability of Claim 38

Claim 38 depends from claim 37. Applicant respectfully submits that claim 38 is allowable for at least the reasons provided above with respect to claim 37.

CONCLUSION

In view of the foregoing amendments and remarks, it is respectfully submitted that this application is in condition for allowance. Accordingly, reconsideration of the application and allowance of the claims are respectfully requested. Although the present paper may include a combination of alterations to the application or claims, or characterizations of claim scope or referenced art, Applicants are not conceding that previously pending claims in this application are not patentable over the cited references. Rather, any alterations and/or characterizations are made to strictly facilitate prosecution of this application. As such, reviewers of this or any parent, child, or related prosecution history shall not reasonably infer that Applicants have made any disclaimers or disavowals of any subject matter supported by the present application.

Applicants have submitted amendments and arguments believed to be sufficient to overcome all of the outstanding rejections. Consequently, Applicants have not advanced every argument for the allowability of the claims over the references of record. As such, Applicants do not acquiesce to any of the Examiner's statements or characterizations not specifically traversed. If the Examiner should have any remaining questions or objections, a telephone interview to discuss and resolve these issues is respectfully requested.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0919
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

The Commissioner is authorized to charge any fee under 37 CFR 1.16 and 1.17 which may be required during the **entire pendency** of the application to Deposit Account No. 50-4407. Please show our docket number with any transaction to the Deposit Account.

Respectfully submitted,

KPPB LLP

By /Jason D. Wolfe/
Jason D. Wolfe
Registration No. 71,327
949.852.0000

JDW/kl

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0920
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

PTO/SB/22 (03-13)
Approved for use through 3/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)

Docket Number (Optional): D1-02359A

Application Number: 13/340,623 | Filed: December 29, 2011

For: Systems and Methods for Playing Back Alternative Streams of Protected Content Protected Using Common Cryptographic Information

Art Unit: 2434 | Examiner: Abiy Getachew

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

		Fee	Small Entity Fee	Micro Entity Fee	
☐	One month (37 CFR 1.17(a)(1))	$200	$100	$50	$
☐	Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$
☑	Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$ 1,400
☐	Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐	Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☐ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 504407.

☑ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest. See 37 CFR 3.71. 37 CFR 3.73(b) statement is enclosed (Form PTO/SB/96).

☑ attorney or agent of record. Registration number 71,327.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/Jason D. Wolfe/ — Signature

05-27-2014 — Date

Jason D. Wolfe — Typed or printed name

949.852.0000 — Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☑ * Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Electronic Patent Application Fee Transmittal

Application Number:	13340623
Filing Date:	29-Dec-2011
Title of Invention:	Systems and Methods for Playing Back Alternative Streams of Protected Content Protected Using Common Cryptographic Information
First Named Inventor/Applicant Name:	Michael George Kiefer
Filer:	Jason Daniel Wolfe
Attorney Docket Number:	D1:02359A

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 3 months with $0 paid	1253	1	1400	1400

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**1400**

Electronic Acknowledgement Receipt

EFS ID:	19138453
Application Number:	13340623
International Application Number:	
Confirmation Number:	1094
Title of Invention:	Systems and Methods for Playing Back Alternative Streams of Protected Content Protected Using Common Cryptographic Information
First Named Inventor/Applicant Name:	Michael George Kiefer
Customer Number:	71897
Filer:	Jason Daniel Wolfe/Katrina Lee
Filer Authorized By:	Jason Daniel Wolfe
Attorney Docket Number:	D1:02359A
Receipt Date:	27-MAY-2014
Filing Date:	29-DEC-2011
Time Stamp:	18:56:55
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$1400
RAM confirmation Number	6797
Deposit Account	504407
Authorized User	BAILEY, DAVID

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		02359aamendment.pdf	169415 316badd09a3848da61587e49579035f9369262a9	yes	21

Multipart Description/PDF files in .zip description

Document Description	Start	End
Amendment/Req. Reconsideration-After Non-Final Reject	1	1
Claims	2	14
Applicant Arguments/Remarks Made in an Amendment	15	21

Warnings:

Information:

2	Extension of Time	02359aextoftime.pdf	130257 7a03c4d154bece42d15e19417503847b95ddb174	no	1

Warnings:

Information:

3	Fee Worksheet (SB06)	fee-info.pdf	30400 dc690a70b8dfcce279e68fd95c1cf15cf9693-7e5	no	2

Warnings:

Information:

Total Files Size (in bytes):	330072

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/340,623	Filing Date 12/29/2011	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 05/27/2014

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 31	Minus	** 39	= 0	X $80 =	0
Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $420 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/DORRETTA BROOKS/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/340,623
	Filing Date	Dec 29, 2011
	First Named Inventor	Michael George Kiefer
	Art Unit	2434
	Examiner Name	Abiy Getachew
	Attorney Docket Number	D1-02359A

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		5715403	A	1998-02-03	Stefik, Mark	
		6141754	A	2000-10-31	Choy, David	

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
		"IBM Closes Cryptolopes Unit," December 17, 2007, CNET News, Retrieved from http://news.cnet.com/IBM-closes-Cryptolopes-unit/2100-1001_3206465.html, 3pgs.	
		"IBM Spearheading Intellectual Property Protection Technology for Information on the Internet; Cryptolope Containers Have Arrived," May 1, 1996, Business Wire, Retrieved from http://www.thefreelibrary.com/IBM+Spearheading+Intellectual+Property+Protection+Technology+for...-a018239381, 1pg.	
		Nelson, Michael, "IBM's Cryptolopes," Complex Objects in Digital Libraries Course, Spring 2001, Retrieved from http://www.cs.odu.edu/~mln/teaching/unc/inls210/?method=display&pkg_name=cryptolopes.pkg&element_name=cryptolopes.ppt, 12 pgs.	

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document.
[4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

Electronic Acknowledgement Receipt

EFS ID:	19105409
Application Number:	13340623
International Application Number:	
Confirmation Number:	1094
Title of Invention:	Systems and Methods for Playing Back Alternative Streams of Protected Content Protected Using Common Cryptographic Information
First Named Inventor/Applicant Name:	Michael George Kiefer
Customer Number:	71897
Filer:	Jason Daniel Wolfe/Agnes Poon
Filer Authorized By:	Jason Daniel Wolfe
Attorney Docket Number:	D1:02359A
Receipt Date:	22-MAY-2014
Filing Date:	29-DEC-2011
Time Stamp:	16:53:05
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	02359aidsxtml.pdf	92547 ff4308f687755b81f749fba86425c73d947e07d4	no	2

Warnings:	
Information:	

2	Information Disclosure Statement (IDS) Form (SB08)	02359aids1449.pdf	88203 a3de1edd741c6f262c8ecfafbf960db4abdd2ed6	no	1
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Non Patent Literature	IBMclosesCryptolopesunit.pdf	92883 e22f2c47a2a9e3608583ec169d89f6e274ba7133	no	3
Warnings:					
Information:					
4	Non Patent Literature	IBMsCryptolopes.pdf	150153 dd03c2be313f4b9d92e0a40fcad71422e42b60aa	no	12
Warnings:					
Information:					
5	Non Patent Literature	IBMSpearheadingIntellectualProperty.pdf	468428 8c8828f37e68b81d78a4256c21d9ab907aff0016	no	1
Warnings:					
Information:					
			Total Files Size (in bytes):	892214	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being electronically filed with the United States Patent and Trademark Office on May 22, 2014 at or before 11:59 p.m. Pacific Time under the Rules of 37 C.F.R. 1.8.

/Agnes Poon/
Agnes Poon

Appl No.	: 13/340,623	Confirmation No. 1094
Applicant	: Michael George Kiefer et al.	
Filed	: December 29, 2011	
Title	: Systems and Methods for Playing Back Alternative Streams of Protected Content Protected Using Common Cryptographic Information	
TC/A.U.	: 2434	
Examiner	: Abiy Getachew	
Docket No.	: D1-02359A	
Customer No.	: 71897	

INFORMATION DISCLOSURE STATEMENT § 1.97(c)

MAIL STOP AMENDMENT
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

2400 E. Katella, Suite 1050
Anaheim, CA 92806
May 22, 2014

Commissioner

In compliance with the duty of disclosure under 37 C.F.R. §§ 1.56, 1.97 and 1.98, and in accordance with the provisions in the MPEP §§ 609 and 707.05(b), enclosed is FORM PTO/SB/08A/B with a listing of references that are known to applicant. Copies of each of the references listed under "Non-Patent Literature Documents" are enclosed.

It is respectfully requested that these references be considered in the examination of this application and identified on the list of references cited on the patent issuing on this application. Applicant also requests that an initialed copy of said FORM PTO/SB/08A/B be entered in the application file, and returned to the Applicant with the next official communication from the Office in accordance with MPEP § 609.

Applicant's undersigned attorney hereby certifies, in accordance 37 CFR § 1.97(e)(2), that no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

It is believed that there are no fees due in connection with this filing. If there are any fees due in connection with this filing, the Commissioner is authorized to charge Deposit Account 50-4407. Please show our docket number with any charge to the Deposit Account.

Respectfully submitted,

KPPB LLP

/Jason D. Wolfe/
Jason D. Wolfe
Registration No. 71,327
949.852.0000

JDW/ap

Enclosure(s)

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0932
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/340,623	12/29/2011	Michael George Kiefer	D1:02359A	1094

71897 7590 11/27/2013

KPPB LLP
2400 EAST KATELLA AVENUE
SUITE 1050
ANAHEIM, CA 92806

EXAMINER	
GETACHEW, ABIY	
ART UNIT	PAPER NUMBER
2434	

NOTIFICATION DATE	DELIVERY MODE
11/27/2013	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@cpaglobal.com
PAIR@KPPB.COM

Office Action Summary	Application No. 13/340,623	Applicant(s) KIEFER ET AL.	
	Examiner ABIY GETACHEW	Art Unit 2434	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12/29/2011*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-39* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-39* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *12/29/2011* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some * c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *09/19/2013*.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0934
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

DETAILED ACTION

1. The present application is being examined under the pre-AIA first to invent provisions.

2. This is in reply to an original application filed on 12/29/2011.

Information Disclosure Statement

3. The information disclosure statements (IDS) submitted on 09/19/2013 has been considered. The submission is in compliance with the provisions of 37 CFR 1.97. Form PTO-1449 is signed and attached hereto.

Oath/Declaration

4. The oath filed 03/20/2012 complies with all the requirements set forth in MPEP 602 and therefore is accepted.

Drawings

5. The drawings filed on 12/29/2011 are accepted.

Specification

6. The specification filed on 12/29/2011 is also accepted.

Claim Rejections - 35 USC § 101

7. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

8. **Claims 37-38** are rejected under 35 U.S.C. 101 because the claimed invention is directed to a non-statutory subject matter.

9. Claim 37 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claim is directed to non-statutory subject matter, which do not fall into the categories of "process", "machine", "manufacture" and "composition of matter".

Claim 37 recites, "The machine **readable medium** ..." *the machine* ***readable medium*** *could be a "transmission type" medium, which renders the claim non-statutory. The above claim can be fixed by inserting the word "non-transitory" before the word medium.*

Claim 38 inherit the deficiencies of the base claim 37 respectively and therefore are non-transitory by virtue of their dependency.

Claim Rejections - 35 USC § 103

10. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

12. Claims 1, 18 and 37 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Amini et al. (US Pat. App. US 6,005,621) hereafter refers as to Amini in view of Thorwirth (WO 2011/103364 A1).

Regarding claim 1, Amini discloses a device ***(fig. 2 a multi-encoder platform 220 i.e. "a device")***, comprising: a memory containing a client application, wherein the client application configures the processor ***(Fig. 11 processor 1110 and furthermore Para 0068, 0069)*** a plurality of alternative streams of protected content ***(fig. 2 a multimedia stream source 210 i.e. "a plurality of alternative")***, where each of the alternative streams of protected content are encrypted using common cryptographic information; obtain the common cryptographic information ***(fig. 2 encryptor 240 discloses same key is used for different streams i.e. "common cryptographic information" para 0054 discloses "...a single key per stream, then all alternate streams must use the same key")***; request portions of content from at least the plurality of alternative streams of protected content ***(fig. 2 and para 0031 discloses multi-encoder 220 generates multiple encoded access units and gives alternate or multiple streams)***; access the protected content using the common cryptographic information; and playback the content. ***(Para 0032 discloses encryptor 240 where the streams are encrypted and fig, 2 and***

para 0054 discloses same key is used for different streams i.e. "common cryptographic information").

Amini does not explicitly request a top level index file.

However, Thorwirth discloses a top level index file **(para 0009 discloses top level Index file pointing to a number of alternate streams that contain actual video and audio data)**.

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the teachings of Thorwirth with the teachings of Amini in order for providing a playlist with a list of URLS pointing to TS container files that contain alternative chunks for the sections of a piece of content (Thorwirth, para 0010).

Regarding claim 18, Amini discloses a method of performing adaptive bitrate streaming using a plurality of alternative streams of protected content, where each of the streams of protected content is protected using common cryptographic information, the method comprising:
identifying a plurality of alternative streams of protected content using a payback device ***(Fig. 2 a multimedia stream source 210 i.e. "a plurality of alternative")*** where each of the alternative streams of protected content are encrypted using common cryptographic information ***(Fig. 2 a multimedia stream source 210 i.e. "a plurality of alternative")*** obtaining the common cryptographic information using the payback device; requesting portions of

content from at least the plurality of alternative streams of protected content using the payback device; accessing the protected content using the payback device and the common cryptographic information; and praying back the content using the payback device. ***(Fig. 2 encryptor 240 discloses same key is used for different streams i.e. "common cryptographic information" para 0054 discloses "...a single key per stream, then all alternate streams must use the same key")***;

Amini does not explicitly request a top level index file.

However, Thorwirth discloses a top level index file ***(para 0009 discloses top level Index file pointing to a number of alternate streams that contain actual video and audio data).***

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the teachings of Thorwirth with the teachings of Amini in order for providing a playlist with a list of URLS pointing to TS container files that contain alternative chunks for the sections of a piece of content (Thorwirth, para 0010).

Regarding claim 37, Amini discloses a machine readable medium containing processor instructions, where execution of the instructions by a processor causes the processor to perform a process ***(Fig. 11 processor 1110 and furthermore Para 0068, 0069)*** comprising:

alternative streams of protected content ***(Fig. 2 a multimedia stream source 210 i.e. "a plurality of alternative")***, where each of the alternative streams

of protected content are encrypted using common cryptographic information; obtaining the common cryptographic information***(Fig. 2 encryptor 240 discloses same key is used for different streams i.e. "common cryptographic information" para 0054 discloses "...a single key per stream, then all alternate streams must use the same key")***; requesting portions of content from at [east the plurality of alternative streams of protected content ***fig. 2 and para 0031 discloses multi-encoder 220 generates multiple encoded access units and gives alternate or multiple streams)***; accessing the protected content using the common cryptographic information; and praying back the content. ***(Para 0032 discloses encryptor 240 where the streams are encrypted and fig, 2 and para 0054 discloses same key is used for different streams i.e. "common cryptographic information").***

Amini does not explicitly request a top level index file.

However, Thorwirth discloses a top level index file **(para 0009 discloses top level Index file pointing to a number of alternate streams that contain actual video and audio data)**.

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the teachings of Thorwirth with the teachings of Amini in order for providing a playlist with a list of URLS pointing

to container files that contain alternative chunks for the sections of a piece of content (Thorwirth, para 0010).

13. Claims 2-8, 19-20 and 38-39 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Amini et al. (US Pat. App. US 6,005,621) hereafter refers as to Amini in view of Thorwirth (WO 2011/103364 A1) as applied to claim 1 above, and further in view of Schnell (US 2009/0328228 A1).

Regarding claim 2 Amini as modified by Thorwirth discloses wherein: the alternative streams of protected content are alternative streams of protected video ***(Para 0052 of Thorwirth discloses alternative streams of protected content)***; and identifying at least a portion of the common cryptographic information used to access the encrypted portions of the frames of video **(para 0054 of Amini discloses a stream source 210 offers unencoded 13ccess units (i.e. frames) to the encoder, pars 0031 t see fig. 2; encryptor 240 where the streams are encrypted, para 0032, see fig. 2; same keys used for different streams (i.e. "common cryptographic Information"));** and the client application configures the processor to: obtain a protected frame of video from one of the alternative streams of protected video ***(figs 4 and 5 of Thorwirth discloses Encryption is a sort of a content protecting method of preventing illegal copy redistribution, editing and the like of contents provided by a content provider (CP) in a manner of transforming data using a specific algorithm)***; decrypt the encrypted portion of the protected

frame of video using the identified portion of the common cryptographic information; and decode the frame of video. ***(Para 0059 of Thorwirth discloses decryption of streamed file utilizes the content keys based on the sections).***

Though Amini as modified by Thorwirth teaches a stream is encrypted with an indexed stream (para 0060 of Amini, for example) However, Amini as modified by Thorwirth does not explicitly discloses each of the alternative streams of protected video includes DRM information indicating portions of frames of video that are encrypted and obtain DRM information indicating a portion of the protected frame of video that is encrypted; identify at least a portion of the common cryptographic information that is used to access the encrypted portion of the protected frame using the DRM information;

Schnell discloses each of the alternative streams of protected video includes DRM information indicating portions of frames of video that are encrypted ***(para 0034 OF discloses media device 202 also includes DRM platform 21 to receive the ORM license)*** and obtain DRM information indicating a portion of the protected frame of video that is encrypted ***(para 0002 discloses digital rights management (DRM) system, various devices that obtain or download digital media content can perform actions on the protected media content as permitted by a DRM license and furthermore para);*** identify at least a portion of the common cryptographic

information that is used to access the encrypted portion of the protected frame using the DRM information ***(para 0028-0031 discloses content server 122 and a DRM system 118 distribute protected media content 120 to various wireless media devices 106).***

It would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Schnell to Incorporate the DRM system with the teachings of Amini as modified by Thorwirth for the purpose of providing DRM associated features such as licenses that correspond to the media segments of the protected media (Schnell para 0004).

Regarding claim 3 Amini as modified by Thorwirth further in view of Schnell discloses wherein: each of the alternative streams of protected content is contained within a separate container file; and the top level index file identifies a container file containing each of the alternative streams. ***(Para 0004 of Thorwirth discloses sections of files in a container file and para 0009 and 0010 of Thorwirth discloses different media containers for adaptive streaming).***

The examiner supplies the same rationale for the combination of Amini as modified by Thorwirth further in view of Schnell as in claim 2 which is set forth above.

Regarding claim 4 Amini as modified by Thorwirth further in view of Schnell discloses wherein: the container files containing each of the alternative

streams of protected content ***(Para 0004 of Thorwirth discloses sections of files in a container file para 0009 and 0010 of Thorwirth discloses different media containers for adaptive streaming)*** comprise at least one header including the common cryptographic information and information that describes the encoding of the stream of protected content; and the top level index file identifies the location of the at least one header within each container file. ***(fig. 2 and para 0037 of Schnell discloses file header object 218 [DRM header element} has the ORM licenses for the protected media content, para 0036, written in a file segment 160, which has track objects 222 associated with the tracks or video tracks).***

The examiner supplies the same rationale for the combination of Amini as modified by Thorwirth further in view of Schnell as in claim 2 which is set forth above.

Regarding claim 5 Amini as modified by Thorwirth further in view of Schnell discloses wherein the common cryptographic information is a set of encryption keys. ***(Para 0054 of Amini discloses encryptor 240 where the streams are encrypted and para 0032. Also see. fig, 2; same key is used for different streams i.e. ("common cryptographic Information").***

The examiner supplies the same rationale for the combination of Amini as modified by Thorwirth further in view of Schnell as in claim 2 which is set forth above.

Regarding claim 6 Amini as modified by Thorwirth further in view of Schnell discloses wherein: the common set of encryption keys is encrypted; and the client application configures the processor to securely receive cryptographic information used to unencrypt the common set of encryption keys. ***(Para 0058 of Thorwirth discloses the content keys used to encrypt the content are encrypted using a key unique to a specific user or client device However, Thorwirth lacks the teaching of common cryptographic information. However, Amini teaches a content distribution with common cryptographic information for the alternate streams of content (para 0054, 0044 of Amini discloses multi-encoder 220 generates multiple encoded access units and gives alternate or multiple streams, para 0031, see fig. 2; same key is used for different streams, (protecting the content)).***

The examiner supplies the same rationale for the combination of Amini as modified by Thorwirth further in view of Schnell as in claim 2 which is set forth above.

Regarding claim 7 Amini as modified by Thorwirth further in view of Schnell discloses wherein the client application configures the processor to obtain the common cryptographic information by requesting at least one header of a container file identified in the top level index file. ***(Para 0004 of Thorwirth discloses sections of files in a container file and para 0004 of Thorwirth, different media containers for adaptive streaming).***

The examiner supplies the same rationale for the combination of Amini as modified by Thorwirth further in view of Schnell as in claim 2 which is set forth above.

Regarding claim 8 Amini as modified by Thorwirth further in view of Schnell discloses wherein: each container file containing one of the alternative streams of protected content further comprises an index; and the client application configures the processor to request a portion of content from one of the container files by configuring the processor to: request at least a portion of an index from the container file; identify the portion of the container file containing a specific portion of content using the index; and request the identified portion of the container file. ***(Para 0053 Thorwirth server provides access to the client based on the selection or chunks requested).***

The examiner supplies the same rationale for the combination of Amini as modified by Thorwirth further in view of Schnell as in claim 2 which is set forth above.

Regarding claim 19 Amini as modified by Thorwirth further in view of Schnell discloses wherein: the alternative streams of protected content are alternative streams of protected video; each of the alternative streams of protected video ***(Para 0052 of Thorwirth discloses alternative streams of protected content)***; includes DRM information indicating portions of frames of video that are encrypted and identifying at least a portion of the common cryptographic information used to access the encrypted portions of the frames

of video; and the method further comprises: obtaining a protected frame of video from one of the alternative streams of protected video using the playback device ***figs 4 and 5 of Thorwirth discloses Encryption is a sort of a content protecting method of preventing illegal copy redistribution, editing and the like of contents provided by a content provider (CP) in a manner of transforming data using a specific algorithm)*** obtaining DRM information indicating a portion of the protected frame of video that is encrypted using the playback device; identify at least a portion of the common cryptographic information that is used to access the encrypted portion of the protected frame using the playback device and the DRM information; decrypting the encrypted portion of the protected frame of video using the playback device and the identified portion of the common cryptographic information; and decoding the frame of video using the playback device. ***(Para 0028-0031 of Schnell discloses content server 122 and a ORM system 118 distribute protected media content 120 to various wireless media devices 106).***

The examiner supplies the same rationale for the combination of Amini as modified by Thorwirth further in view of Schnell as in claim 2 which is set forth above.

Regarding claim 20 Amini as modified by Thorwirth further in view of Schnell discloses wherein: each of the alternative streams of protected content is contained within a separate container file; and the top level index file

identifies a container file containing each of the alternative streams. ***(Para 0004 of Thorwirth discloses sections of files in a container file and para 0009 and 0010 of Thorwirth discloses different media containers for adaptive streaming).***

The examiner supplies the same rationale for the combination of Amini as modified by Thorwirth further in view of Schnell as in claim 2 which is set forth above.

Regarding claim 38 Amini as modified by Thorwirth further in view of Schnell discloses wherein: the alternative streams of protected content are alternative streams of protected video; each of the alternative streams of protected video **(*Para 0052 of Thorwirth discloses alternative streams of protected content)***; includes DRM information indicating portions of frames of video that are encrypted and identifying at least a portion of the common cryptographic information used to access the encrypted portions of the frames of video; and execution of the instructions by a processor also causes the processor to perform a process comprising: obtaining a protected frame of video from one of the alternative streams of protected video (***figs 4 and 5 of Thorwirth discloses Encryption is a sort of a content protecting method of preventing illegal copy redistribution, editing and the like of contents provided by a content provider (CP) in a manner of transforming data using a specific algorithm***)obtaining DRM information indicating a portion of the protected frame of video that is encrypted; identify at least a portion of the

common cryptographic information that is used to access the encrypted portion of the protected frame using the DRM information; decrypting the encrypted portion of the protected frame of video using and the identified portion of the common cryptographic information; and decoding the frame of video. ***(Para 0028-0031 of Schnell discloses content server 122 and a ORM system 118 distribute protected media content 120 to various wireless media devices 106).***

The examiner supplies the same rationale for the combination of Amini as modified by Thorwirth further in view of Schnell as in claim 2 which is set forth above.

Regarding claim 39 Amini as modified by Thorwirth further in view of Schnell discloses wherein the machine readable medium is non-volatile memory. ***(fig. 11 and para 0068, 0069 of Amini memory 1104 with ROM i.e. "non-volatile").***

The examiner supplies the same rationale for the combination of Amini as modified by Thorwirth further in view of Schnell as in claim 2 which is set forth above.

14. Claims 9-17 and 21-36 rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Amini et al. (US Pat. App. US 6,005,621) hereafter refers as to Amini in view of Thorwirth (WO 2011/103364 A1) and further in view of Schnell (US 2009/0328228 A1) in view of as applied to claim 2 above and

further in view of Soroushian et al. (US 2009/0132721 A1) herein after refer as to Soroushian.

Regarding claim 9 Amini as modified by Thorwirth further in view of Schnell discloses all claimed limitations except for wherein the container files are Matroska container files.

However, Soroushian discloses wherein the container files are Matroska container files. ***(see fig, 1c and para 0031, Matroska is MKV, discloses Soroushian is in the field of playback and distribution systems (abstract) and further teaches wherein the content is stored as chunks or elements in a Matroska container (MKV container composed of lists, chunks and/or elements).***

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the Invention to use the teachings of Soroushian to incorporate with the teaching of Amini as modified by Thorwirth modified Schnell in order for the purpose of providing a MKV container for distributing high-definition downloadable content on the internet and peer-to-peer networks (Soroushian, para 0003).

Regarding claim 10 Amini as modified by Thorwirth modified Schnell and further modified Soroushian discloses wherein the common cryptographic information is stored in a common DRM Header element contained within a Tracks element within each of the Matroska container files containing the alternative streams of protected content. ***(Para 0052 of Thorwirth discloses***

the chunks are protected using different watermark payloads, i.e. "alternative streams of protected content")

The examiner supplies the same rationale for the combination of Amini as modified by Thorwirth further in view of Schnell and further in view of Soroushian as in claim 9 which is set forth above.

Regarding claim 11 Amini as modified by Thorwirth modified Schnell and further modified Soroushian discloses wherein: the common cryptographic information is a set of encryption keys; and the set of encryption keys is encrypted and stored within the DRM Header element. ***(para 0036 0037 of Schnell file header object 218 (DRM header element) has the DRM licenses for the protected media content,; tracks objects 22 which has the track attributes and segment data to identify the content).***

The examiner supplies the same rationale for the combination of Amini as modified by Thorwirth further in view of Schnell and further in view of Soroushian as in claim 9 which is set forth above.

Regarding claim 12 Amini as modified by Thorwirth modified Schnell and further modified Soroushian discloses wherein the client application configures the processor to: obtain cryptographic information that can be used to unencrypt the set of encryption keys stored within the DRM Header element; and unencrypt the set of encryption keys stored within the DRM Header element using the obtained cryptographic information. ***(Para 0036 of Schnell***

file header object 218 (DRM header element) has the DRM licenses for the protected media content).

The examiner supplies the same rationale for the combination of Amini as modified by Thorwirth further in view of Schnell and further in view of Soroushian as in claim 9 which is set forth above.

Regarding claim 13 Amini as modified by Thorwirth modified Schnell and further modified Soroushian discloses wherein the client application configures the processor to obtain the DRM Header element by requesting a Tracks element from one of the Matroska container files identified in the top level index file. ***(See para 0004 of Thorwirth, different media containers for adaptive streaming, para 0009 of Thorwirth [background]) and a top level index file identifies a container file containing each of the alternative streams and furthermore para 0009 of Thorwirth top level Index file pointing to a number of alternate streams that contain actual video and audio data,).***

The examiner supplies the same rationale for the combination of Amini as modified by Thorwirth further in view of Schnell and further in view of Soroushian as in claim 9 which is set forth above.

Regarding claim 14 Amini as modified by Thorwirth modified Schnell and further modified Soroushian discloses wherein: each Matroska container file containing an alternative stream of protected content further comprises an index contained within a Cues element ; and the client application configures

the processor to request a portion of content from one of the Matroska container files by configuring the processor to: request at least a portion of a Cues element from a Matroska container file containing one of the alternative streams of protected content; identify a portion of the Matroska container file containing a specific portion of content using at least one CueTrackPosition element within the Cues element; and request the portion of the Matroska container file identified by the at least one CueTrackPosition element. ***(Schnell teaches file index 158 for each me and the corresponding segments, para 0031, see fig. 2; and (track objects 222 has the attributes and information included in a track ("Cues element"), para 0036, 0037 see fig. 2 and includes size, type, mode 10, Index, 'Algorithm 10 with index. para 0041 and table under it).***

The examiner supplies the same rationale for the combination of Amini as modified by Thorwirth further in view of Schnell and further in view of Soroushian as in claim 9 which is set forth above.

Regarding claim 15 Amini as modified by Thorwirth modified Schnell and further modified Soroushian discloses wherein the index comprises a plurality of CueTrackPosition elements that identify the location of a plurality of Cluster elements within the Matroska container file. ***(See fig. 1c and Para 0031, discloses (Matroska is MKV) and furthermore Para 0037 of Soroushian table with hierarchical index Identifiers with CUEPOS_ID, table above).***

The examiner supplies the same rationale for the combination of Amini as modified by Thorwirth further in view of Schnell and further in view of Soroushian as in claim 9 which is set forth above.

Regarding claim 16 Amini as modified by Thorwirth modified Schnell and further modified Soroushian discloses wherein: each Cluster element contains a plurality of BlockGroup elements including encoded portions of content; a CueTrack Position element indexes each Cluster element; and each CueTrackPosition element includes the size of the Cluster element that it indexes. ***(fig, 2 para 0031 of Schnell file index 158 for each file, and the corresponding segments (segments can be interpreted as track elements or comprising of cluster element and furthermore fig 2 and para 0036, 0037 and para 9041 of Schnell teaches size, type, mode ID. index, Algorithm ID with index).***

The examiner supplies the same rationale for the combination of Amini as modified by Thorwirth further in view of Schnell and further in view of Soroushian as in claim 9 which is set forth above.

Regarding claim 17 Amini as modified by Thorwirth modified Schnell and further modified Soroushian discloses wherein the alternative streams of protected content are alternative streams of protected video ***(para 0052 of Thorwirth discloses CDN stores six alternative chunks [video] created for each section with different encoding parameters and two different watermark payloads [alternative streams of protected content);*** each of

the Matroska container files containing an alternative stream of protected video includes a DRMInfo element in a BlockGroup element containing a protected frame of video ***(para 0052 of Thorwirth discloses the chunks are protected using different watermark payloads),*** where the DRMInfo element indicates at least a portion of the protected frames of video that is encrypted and identifies at least a portion of the common cryptographic information used to access the at least one encrypted portion of the protected frame of video ***(para 0036 of Schnell file header object 218 i.e. "DRM header Element" has the DRM licenses for the protected media content);*** and the client application configures the processor to access video frames in a stream of protected video using the common cryptographic information by configuring the processor to: obtain a BlockGroup containing a protected frame of video; parse the BlockGroup element to obtain a DRMInfo element indicating at least a portion of the protected frame of video that is encrypted using an encryption key from the set of encryption keys; decrypt the at least one encrypted portion of the protected frame of video using the identified encryption key; and decode the frame of video. ***(figs 4 and 5 of Thorwirth discloses Encryption is a sort of a content protecting method of preventing illegal copy redistribution, editing and the like of contents provided by a content provider (CP) in a manner of transforming data using a specific algorithm*)**;

The examiner supplies the same rationale for the combination of Amini as modified by Thorwirth further in view of Schnell and further in view of Soroushian as in claim 9 which is set forth above.

Regarding claim 21 Amini as modified by Thorwirth modified Schnell and further modified Soroushian discloses wherein: the container files containing each of the alternative streams of protected content comprise at least one header including the common cryptographic information and information that describes the encoding of the stream of protected content; and the top level index file identifies the location of the at least one header within each container file. ***(fig. 2 and para 0037 of Schnell discloses file header object 218 [DRM header element} has the ORM licenses for the protected media content, para 0036, written in a file segment 160, which has track objects 222 associated with the tracks or video tracks).***

The examiner supplies the same rationale for the combination of Amini as modified by Thorwirth further in view of Schnell and further in view of Soroushian as in claim 9 which is set forth above.

Regarding claim 22 Amini as modified by Thorwirth modified Schnell and further modified Soroushian discloses, wherein the common cryptographic information is a set of encryption keys. ***(Para 0054 of Amini discloses encryptor 240 where the streams are encrypted and para 0032. Also see. fig, 2; same key is used for different streams i.e. ("common cryptographic Information").***

The examiner supplies the same rationale for the combination of Amini as modified by Thorwirth further in view of Schnell and further in view of Soroushian as in claim 9 which is set forth above.

Regarding claim 23 Amini as modified by Thorwirth modified Schnell and further modified Soroushian discloses wherein: the set of encryption keys is encrypted so that it is accessible using cryptographic information obtained by the playback device (***para 0058 of Thorwirth discloses the content keys used to encrypt the content are encrypted using a key unique to a specific user or client device);*** and the method further comprising obtaining cryptographic information using the playback device ***(para 0054, 0044 of Amini same key Is used for different streams i.e. ("protecting the content")).***

The examiner supplies the same rationale for the combination of Amini as modified by Thorwirth further in view of Schnell and further in view of Soroushian as in claim 9 which is set forth above.

Regarding claim 24 Amini as modified by Thorwirth modified Schnell and further modified Soroushian discloses wherein the set of encryption keys is encrypted using at least one encryption key; and the playback device securely obtains the at least one encryption key ***(para 0058 of Thorwirth discloses copy of the encryption key used for the encryption of the content key is delivered securely to the specific user or client device, and furthermore***

para 0064 of Thorwirth discloses, hashing or encrypting the encrypted content and key).

The examiner supplies the same rationale for the combination of Amini as modified by Thorwirth further in view of Schnell and further in view of Soroushian as in claim 9 which is set forth above.

Regarding claim 25 Amini as modified by Thorwirth modified Schnell and further modified Soroushian discloses wherein the at least one encryption key is encrypted using at least one encryption key included in the cryptographic information bound to the playback device. ***(Para 0058 of Thorwirth the content keys used to encrypt the content are encrypted using a key unique to a specific user or client device and furthermore para 0058 of Thorwirth discloses copy of the encryption key used for the encryption of the content key is delivered securely to the specific user or client device)***

The examiner supplies the same rationale for the combination of Amini as modified by Thorwirth further in view of Schnell and further in view of Soroushian as in claim 9 which is set forth above.

Regarding claim 26 Amini as modified by Thorwirth modified Schnell and further modified Soroushian discloses obtaining the common cryptographic information by requesting at least one header of a container file identified in the top level index file using the playback device. ***(Para 0004 of Thorwirth discloses sections of files in a container file, different media containers for adaptive streaming, and a top level index file identifies a container***

file containing each of the alterative streams (top level index file pointing to a number of alternate streams that contain actual video and audio data, para 0009 of Thorwirth).

The examiner supplies the same rationale for the combination of Amini as modified by Thorwirth further in view of Schnell and further in view of Soroushian as in claim 9 which is set forth above.

Regarding claim 27 Amini as modified by Thorwirth modified Schnell and further modified Soroushian discloses wherein: each container file containing one of the alternative streams of protected content further comprises an index; and the method further comprising: requesting at least a portion of an index from the container file using the playback device; identify the portion of the container file containing a specific portion of content using the playback device and the index; and requesting the identified portion of the container file using the playback device. ***(Para 0058 of Thorwirth discloses a copy of the encryption key used for the encryption of the content key is delivered securely to the specific user or client device and furthermore para 0064 of Thorwirth discloses hashing or encrypting the encrypted content and key).***

The examiner supplies the same rationale for the combination of Amini as modified by Thorwirth further in view of Schnell and further in view of Soroushian as in claim 9 which is set forth above.

Regarding claim 28 Amini as modified by Thorwirth modified Schnell and further modified Soroushian discloses wherein the container files are Matroska container files. ***(Soroushian teaches see fig, 1c and para 0031, Matroska is MKV, discloses Soroushian is in the field of playback and distribution systems (abstract) and further teaches wherein the content is stored as chunks or elements in a Matroska container (MKV container composed of lists, chunks and/or elements).***

The examiner supplies the same rationale for the combination of Amini as modified by Thorwirth further in view of Schnell and further in view of Soroushian as in claim 9 which is set forth above.

Regarding claim 29 Amini as modified by Thorwirth modified Schnell and further modified Soroushian discloses wherein the common cryptographic information is stored in a common DRM Header element contained within a Tracks element within each of the Matroska container files containing the alternative streams of protected content. ***(Para 0052 of Thorwirth discloses the chunks are protected using different watermark payloads, i.e. "alternative streams of protected content")***

The examiner supplies the same rationale for the combination of Amini as modified by Thorwirth further in view of Schnell and further in view of Soroushian as in claim 9 which is set forth above.

Regarding claim 30 Amini as modified by Thorwirth modified Schnell and further modified Soroushian discloses wherein: the common cryptographic

information is a set of encryption keys; and the set of encryption keys is encrypted and stored within the DRM Header element. ***(para 0036 0037 of Schnell file header object 218 (DRM header element) has the DRM licenses for the protected media content,; tracks objects 22 which has the track attributes and segment data to identify the content).***

The examiner supplies the same rationale for the combination of Amini as modified by Thorwirth further in view of Schnell and further in view of Soroushian as in claim 9 which is set forth above.

Regarding claim 31 Amini as modified by Thorwirth modified Schnell and further modified Soroushian discloses wherein: the set of encryption keys is encrypted so that it is accessible using cryptographic information obtained by the playback device and the method further comprising obtaining cryptographic information using the playback device. (***Para 0058 of Thorwirth discloses the content keys used to encrypt the content are encrypted using a key unique to a specific user or client device);***

The examiner supplies the same rationale for the combination of Amini as modified by Thorwirth further in view of Schnell and further in view of Soroushian as in claim 9 which is set forth above.

Regarding claim 32 Amini as modified by Thorwirth modified Schnell and further modified Soroushian discloses further comprising obtaining the DRM Header element by requesting a Tracks element from one of the Matroska container files identified in the top level index file. ***(See para 0004 of***

Thorwirth, different media containers for adaptive streaming, para 0009 of Thorwirth [background]) and a top level index file identifies a container file containing each of the alternative streams and furthermore para 0009 of Thorwirth top level Index file pointing to a number of alternate streams that contain actual video and audio data,).

The examiner supplies the same rationale for the combination of Amini as modified by Thorwirth further in view of Schnell and further in view of Soroushian as in claim 9 which is set forth above.

Regarding claim 33 Amini as modified by Thorwirth modified Schnell and further modified Soroushian discloses wherein: each Matroska container file containing an alternative stream of protected content further comprises an index contained within a Cues element and the method further comprises: requesting at least a portion of a Cues element from a Matroska container file containing one of the alternative streams of protected content using the playback device; identifying a portion of the Matroska container file containing a specific portion of content using the playback device and at least one CueTrackPosition element within the Cues element; and requesting the portion of the Matroska container file identified by the at least one CueTrackPosition element. ***(Schnell teaches file index 158 for each me and the corresponding segments, para 0031, see fig. 2; and (track objects 222 has the attributes and information included in a track ("Cues element"),***

para 0036, 0037 see fig. 2 and includes size, type, mode 10, Index, 'Algorithm 10 with index. para 0041 and table under it).

The examiner supplies the same rationale for the combination of Amini as modified by Thorwirth further in view of Schnell and further in view of Soroushian as in claim 9 which is set forth above.

Regarding claim 34 Amini as modified by Thorwirth modified Schnell and further modified Soroushian discloses wherein the index comprises a plurality of CueTrackPosition elements that identify the location of a plurality of Cluster elements within the Matroska container file. ***(See fig. 1c and Para 0031, discloses (Matroska is MKV) and furthermore Para 0037 of Soroushian table with hierarchical index Identifiers with CUEPOS_ID, table above).***

The examiner supplies the same rationale for the combination of Amini as modified by Thorwirth further in view of Schnell and further in view of Soroushian as in claim 9 which is set forth above.

Regarding claim 35 Amini as modified by Thorwirth modified Schnell and further modified Soroushian discloses wherein: each Cluster element contains a plurality of BlockGroup elements including encoded portions of content; a CueTrack Position element indexes each Cluster element; and each CueTrackPosition element includes the size of the Cluster element that it indexes. ***(fig, 2 para 0031 of Schnell file index 158 for each file, and the corresponding segments (segments can be interpreted as track elements or comprising of cluster element and furthermore fig 2 and para 0036,***

0037 and para 9041 of Schnell teaches size, type, mode ID. index, Algorithm ID with index).

The examiner supplies the same rationale for the combination of Amini as modified by Thorwirth further in view of Schnell and further in view of Soroushian as in claim 9 which is set forth above.

Regarding claim 36 Amini as modified by Thorwirth modified Schnell and further modified Soroushian discloses, wherein the alternative streams of protected content are alternative streams of protected video **(*Para 0052 of Thorwirth discloses alternative streams of protected content)*;** each of the Matroska container files containing an alternative stream of protected video includes a DRMInfo element in a BlockGroup element containing a protected frame of video ***(fig, 2 para 0031 of Schnell file index 158 for each file, and the corresponding segments (segments can be interpreted as track elements or comprising of cluster element and furthermore fig 2 and para 0036, 0037 and para 9041 of Schnell teaches size, type, mode ID. index, Algorithm ID with index)*** where the DRMInfo element indicates at least a portion of the protected frames of video that is encrypted and identifies at least a portion of the common cryptographic information used to access the at least one encrypted portion of the protected frame of video; and the method further comprising: obtaining a BlockGroup containing a protected frame of video using the playback device; parsing the BlockGroup element to obtain a DRMInfo element indicating at least a portion of the protected frame of video

that is encrypted using the playback device and an encryption key from the set of encryption keys; decrypting the at least one encrypted portion of the protected frame of video using the playback device and the identified encryption key; and decoding the frame of video using the playback device. ***(para 0003 of Soroushian discloses decoding multimedia and present audio, video and subtitle information in a synchronized manner and furthermore para 0028-0031 of Schnell discloses content server 122 and a ORM system 118 distribute protected media content 120 to various wireless media devices 106).***

The examiner supplies the same rationale for the combination of Amini as modified by Thorwirth further in view of Schnell and further in view of Soroushian as in claim 9 which is set forth above.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ABIY GETACHEW whose telephone number is (571)272-6932. The examiner can normally be reached on Monday to Friday 8Am to 4:30Pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571)272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/William S. Powers/
Primary Examiner, Art Unit 2434

/Abiy Getachew/
Examiner, Art Unit 2434

A.G.
October 16, 2013

Notice of References Cited	Application/Control No. 13/340,623	Applicant(s)/Patent Under Reexamination KIEFER ET AL.	
	Examiner ABIY GETACHEW	Art Unit 2434	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2010/0107260 A1	04-2010	Orrell et al.	726/27
*	B	US-2012/0260277 A1	10-2012	Kosciewicz, Pawel	725/14
*	C	US-2011/0135090 A1	06-2011	Chan et al.	380/210
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

+You Search Images Maps Play YouTube News Gmail More Sign in

Google index file and streams of protected content and alternative streams of prot

Web Images Maps Shopping Patents More Search tools

About 19,900 results (0.68 seconds)

Systems and methods for **protecting alternative streams** in adaptiv...
www.google.com/patents/WO2013032518A2?cl=en
App. - Filed Dec 31, 2011 - Published Mar 7, 2013 - Michael George KIEFER - Divx, Llc
protect the plurality of **alternative streams** of **content using** the **common** ... the **common cryptographic information** is a set of **encryption** keys; ... generate an **index** for each Matroska container **file** during the encoding of each of ...
Overview - Related - Discuss

Systems and methods for automatically generating top level **index files**
www.google.com/patents/WO2013032517A1?cl=en
App. - Filed Dec 31, 2011 - Published Mar 7, 2013 - Jason Braness - Divx, Llc
generating a top level **index file** describing each asset in the filtered list of ... from a database of **cryptographic information** and is **encrypted** so that the ..... **Alternative Streams of Protected Content** Protected **Using Common** ...
Overview - Related - Discuss

Methods and apparatus for continuous control and **protection** of ...
www.google.com/patents/EP1343318A2?cl=en
App. - Filed Mar 18, 1998 - Published Sep 10, 2003 - Talal G. Shamoon - Intertrust Technologies Corp.
the media player reading first header **information** identifying a ... The digital bit **stream** includes **content**, which is **encrypted** at least in part, and ... in which a **protected** MPEG-4 **file** may be created consistent **with** the present invnetion;; FIG. .... include **cryptographic** keys and rules governing the **use** of **content**
Overview - Related - Discuss

Methods and apparatus for continuous control and **protection** of ...
www.google.com/patents/EP1521467A2?cl=en
App. - Filed Mar 18, 1998 - Published Apr 6, 2005 - Ralph D. Hill - Intertrust Technologies Corp.
A **streaming** media player providing **content protection** and digital rights ... a key for decryption of at least a portion of the **encrypted content information** .... in which a **protected** MPEG-4 **file** may be created consistent **with** the present ..... **Stream** Flow Controllers 17 and 18 contain **Cryptographic** Engines 19 ...
Overview - Related - Discuss

Digital **content** distribution system
www.google.com/patents/CA2434883C?cl=en
Grant - Filed Dec 18, 2002 - Issued Apr 2, 2013 - Ivan Hugh Mclean - Irdeto Access B.V.
At least one of the message sections is **encrypted** in such a way as to be ... A method of generating **cryptographically protected** digital data encoding **content** and arranged ..... Intellectual Property Management and **Protection** (IPMP) **information** is ... Keys are associated **with** the **content** or other **streams via** ...
Overview - Related - Discuss

Streaming media player **with** continuous control and **protection** of ...
www.google.com/patents/EP1062128B1?cl=en
Grant - Filed Mar 18, 1999 - Issued May 25, 2005 - Ralph D. Hill - Intertrust Technologies Corp.
The digital bit **stream** includes **content**, which is **encrypted** at least in part, ... in which a **protected** MPEG-4 **file** may be created consistent **with** the present invnetion;; FIG. .... In an **alternate** embodiment, the association of control to **content** ... **Stream** Flow Controllers 17 and 18 contain **Cryptographic** Engines ...
Overview - Related - Discuss

Streaming video server **with** virtual **file** system and methods for ...
www.google.com/patents/WO2012145822A1?cl=en
App. - Filed Apr 23, 2012 - Published Nov 1, 2012 - King Chiu TAM - Morega Systems Inc.
A **streaming** video server generates a virtual **file** system that includes ... The plurality of **encrypted** segments of the selected one of the plurality ... As an **alternative** .... This allows the keys to not be saved to a storage device, **protecting** the ... For example, (a) responding **with** the **content index**, variant playlist, ...

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0968
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Overview - Related - Discuss

Help Send feedback Privacy & Terms

Compression and decompression techniques for drm license ...



www.google.com/patents/WO2012048996A1?cl=en

App. - Filed Oct 14, 2011 - Published Apr 19, 2012 - Daniel Catrein - Telefonaktiebolaget L M Ericsson (Publ)

The table comprises at least one first license part **common** to licenses ... The method of claim 15 or 16, wherein the **content stream** conforms to the ... a second table associating a reference **index with** each placeholder, ... the one or more **cryptographic content** keys are **encrypted** for a specific ..... **Protection** ...

Overview - Related - Discuss

Protection of digital data **content**



www.google.com/patents/EP2230622B1?cl=en

Grant - Filed Feb 2, 2005 - Issued Dec 12, 2012 - Gidon Elazar - SanDisk Secure Content Solutions, Inc.

sending the at least two units of data as a single data **stream** over a network (230) in ... said accessed at least one of the units of data are in an **encrypted** form. ... A Digital **Content File** is data which has an end **use** of being either viewed, ... DRM systems typically involve **cryptographic** methods for the secure ...

Overview - Related - Discuss

Methods and systems for generating transcodable **encrypted content**



www.google.com/patents/WO2005099163A1?cl=en

App. - Filed Mar 22, 2005 - Published Oct 20, 2005 - John G. Apostolopoulos - John G. Apostolopoulos

The transcodable **encrypted** content is transcodable without requiring ... transcodable **encrypted** content has **information** associated **with** it to direct ... Providing effective security in order to **protect content** from ... Intermediate nodes in the system may be used to perform **stream** ..... a **cryptographic** checksum

Overview - Related - Discuss

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0969
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

CONSIDERED: /A.G./ (10/16/2013)

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Field

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/340,623
	Filing Date	Dec 29, 2011
	First Named Inventor	Michael George Kiefer
	Art Unit	2434
	Examiner Name	Abiy Getachew
	Attorney Docket Number	D1:02359A

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
/A.G./		20090132721	A1	2009- 05-21	Soroushian, Kourosh et al.	
/A.G./		20090290706	A1	2009-11-26	Amini, Lisa D., et al.	
/A.G./		20090328228	A1	2009-12-31	Schnell, Patrik	
/A.G./		20130061040	A1	2013-03-07	Kiefer, Michael G., et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
/A.G./		2011103364	WO	A1	2011-08-25	Thorwirth, Niels		
/A.G./		2013032518	WO	A2	2013-03-07	Kiefer, Michael, et al.		
/A.G./		2013032518	WO	A3	2013-09-06	Kiefer, Michael, et al.		

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
/A.G./		International Search Report and Written Opinion for International Application PCT/US2011/068276, International Filing Date December 31, 2011, Report completed June 19, 2013, Mailed July 8, 2013, 24 pgs.	

CONSIDERED: /A.G./ (10/16/2013)

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Field

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	**Application Number**	13/340,623
	Filing Date	Dec 29, 2011
	First Named Inventor	Michael George Kiefer
	Art Unit	2434
	Examiner Name	Abiy Getachew
	Attorney Docket Number	D1:02359A

EXAMINER SIGNATURE			
Examiner Signature	/Abiy Getachew/ (10/16/2013)	Date Considered	10/16/2013

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document.
[4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	2	("20090013195").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/07 11:23
S2	8	(("20090132721") or ("20090290706") or ("20090328228") or ("20130061040")).PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/07 11:27
S3	1	(13/340623).APP.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/07 11:28
S4	18	(playback with device) with (processor with memory with client with application)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/08 09:49
S5	2	("20070024706").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/08 10:03
S8	2	("20090290706").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/08 10:38
S9	8	(("20090132721") or ("20090290706") or ("20090328228") or ("20130061040")).PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/08 10:56
S10	17797	(playback with device)	USPAT	OR	OFF	2013/10/08 11:02
S11	0	(playback with device) with (processor) with (memoory with client with application) same (index with file) same (Streams with content with encryp$3)	USPAT	OR	OFF	2013/10/08 11:05
S12	0	(playback with device) with (processor) with (memoory with client with application) same (index with file) same (Streams with content with encryp$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/08 11:05
S13	0	(processor) with (memoory with client with application) same (index	US-PGPUB; USPAT; USOCR;	OR	OFF	2013/10/08 11:05

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0972
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

		with file) same (Streams with content with encryp$3)	FPRS; EPO; JPO; DERWENT; IBM_TDB			
S14	1	(processor) with (memory with client with application) same (index with file) same (Streams with content with encryp$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/08 11:05
S15	3	(processor) near20 (index with file) same (Streams with content with encryp$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/08 11:06
S16	1	((plurality with streams) with (encrypt$3 adj key)) same (index$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/08 12:26
S17	4	((plurality with streams) with (encrypt$3 adj key)) same (index$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/10/08 12:27
S18	11	((plurality with streams) with (encrypt$3 adj key)) same (index$3 list$3 or index)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/10/09 11:02
S22	4	((plurality with streams) with (encrypt$3 adj key)) same (index$3 list$3 or index) and (playback with content)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/10/09 11:04
S23	2	((plurality with streams) near20 (index$3 list$3 or index)) near20 (identify or identifying or identified) same (plurality with alternative with streams)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/10/09 11:18
S25	2	("20130032518").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 11:32
S26	2	("20090290706").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 11:48
S27	2	("20130061040").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 11:51
S29	2	("20130061040").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 11:55
S30	2	("20130061045").PN.	US-PGPUB; USPAT; USOCR;	OR	OFF	2013/10/09 11:55

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0973
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S32	2	(request with index with file with identifying with alternative with streams)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 12:33
S33	4	("2003030324").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 12:39
S34	0	("20090387258").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 12:39
S35	0	("200900387258").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 12:39
S36	2	("20090307258").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 12:40
S37	2	("20090132599").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 12:41
S38	0	(index with file) with (alternative streams of protected content)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	WITH	OFF	2013/10/09 12:55
S39	1	(index with file) with (alternative streams protected content)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	WITH	OFF	2013/10/09 12:55
S40	1	(index) with (alternative streams protected content)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	WITH	OFF	2013/10/09 12:55
S41	9	(index) with (streams protected content)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	WITH	OFF	2013/10/09 12:55
S42	2	("20080301734").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 12:59
S43	5	(index) near20 (streams protected content)	US-PGPUB; USPAT; USOCR;	WITH	OFF	2013/10/09 13:02

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0974
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S44	2	(index) near20 (streams protected content).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	WITH	OFF	2013/10/09 13:04
S46	5	(index or indexing or indexed) near20 (streams with content with protect$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	WITH	OFF	2013/10/09 13:41
S47	2	(index or indexing or indexed) near20 (streams with content with protect$3).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	WITH	OFF	2013/10/09 13:42
S48	30	(index or indexing or indexed) near20 (streams with content).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	WITH	OFF	2013/10/09 13:43
S49	2	S48 and (streams with protected with content)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	WITH	OFF	2013/10/09 13:44
S50	2	S48 and (streams same encrypted same cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	WITH	OFF	2013/10/09 13:45
S51	3	S48 and (encrypted same cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	WITH	OFF	2013/10/09 13:46
S52	4	(index or indexing or indexed) near20 (streams with content) near20 (protected with content with cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	WITH	OFF	2013/10/09 14:05
S53	2	("20030078930").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 14:06
S54	4	(index or indexing or indexed) near20 (protected with content with cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	WITH	OFF	2013/10/09 14:08
S55	60	(index or indexing or indexed) near20 (content with cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	WITH	OFF	2013/10/09 14:08
S56	4	(index or indexing or indexed) near20 (streams with content)	US-PGPUB; USPAT; USOCR;	WITH	OFF	2013/10/09 14:08

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0975
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

		near20 (content with cryptographic)	FPRS; EPO; JPO; DERWENT; IBM_TDB			
S57	4	(index or indexing or indexed) near20 (streams) near20 (content with cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	WITH	OFF	2013/10/09 14:08
S58	4	(index or indexing or indexed) near20 (streams) near20 (cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	WITH	OFF	2013/10/09 14:09
S59	4	(index or indexing or indexed) near20 (streams) with (content with cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	WITH	OFF	2013/10/09 14:10
S60	13	(index or indexing or indexed) near20 (streams same protect$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	WITH	OFF	2013/10/09 14:11
S61	58	("5465353" | "5613004" | "5664016" | "5689639" | "5809498" | "6101602" | "6363463").PN. OR ("6671407").URPN.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/10/09 14:21
S62	6	(streams with content) near20 (protected with content with cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	WITH	OFF	2013/10/09 14:41
S63	20490	(client with application same processor)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	WITH	OFF	2013/10/09 15:13
S64	1	(client with application same processor) with (index or indexing or indexed) near20 (Streams with content with encryp$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 15:16
S65	48	(client with application same processor) with (index or indexing or indexed)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 15:16
S66	1	(client with application same processor) with (index or indexing or indexed) near20 (Streams with encryp$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 15:17
S67	1	(client with application same processor) with (index or indexing or indexed) near20 (Streams with cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 15:17
S68	2	(client with application same processor) with (index or indexing	US-PGPUB; USPAT; USOCR;	OR	OFF	2013/10/09 15:18

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0976
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

		or indexed) near20 (cryptographic)	FPRS; EPO; JPO; DERWENT; IBM_TDB			
S69	12	(client with application same processor) with (index or indexing or indexed) near20 (Stream$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 15:19
S70	1	(client with application same processor) with (index or indexing or indexed) near20 (protect with Stream$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 15:19
S71	1	(client with application same processor) with (index or indexing or indexed) near20 (protect same Stream$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 15:20
S72	2	(client with application same processor) with (index or indexing or indexed) near20 (Stream$3) and (cryptographic with information)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 15:21
S73	2	(client with application same processor) with (index or indexing or indexed) near20 (Stream$3) and (cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 15:21
S74	6	(application same processor) with (index or indexing or indexed) near20 (Stream$3) and (cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 15:21
S75	3	(processor) with (index or indexing or indexed) near20 (Stream$3) same (protected with content)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 15:23
S76	4	(processor) with (index or indexing or indexed) near20 (Stream$3) same (protected)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 15:24
S77	69	(index or indexing or indexed) near20 (Stream$3) same (protected)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 15:24
S78	5	S55 and S77	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 15:25
S79	2	(plurality with alternative with streams with protected with content)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 17:50
S80	308	(plurality with alternative with streams)	US-PGPUB; USPAT; USOCR;	OR	OFF	2013/10/09 17:50

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0977
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S81	2	(plurality with alternative with streams)same (cryptographic with information)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 17:51
S82	2	(plurality with alternative with streams)same (cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 17:51
S83	2	(plurality with alternative with streams) near20 (content with encryp$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 17:52
S84	2	(plurality with alternative with streams) near20 (encryp$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 17:52
S85	4	(plurality with alternative with streams) near20 (key or encryption or decryption or code or encryp$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 17:54
S86	2	(plurality with alternative with streams) near20 (protect$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 17:56
S87	49731	(plurality with streams)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 17:56
S88	51	(plurality with streams)same (cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 17:56
S89	27	(plurality with streams) near20 (cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 17:56
S90	2	(plurality with streams) near20 (protect$3 same cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 17:57
S91	27	S88 and S89	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 17:57
S92	9	(Request) with (index) near20 (plurality with streams)	US-PGPUB; USPAT; USOCR;	OR	OFF	2013/10/09 18:01

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0978
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S93	1	(Request) with (index) near20 (plurality with streams)same (cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 18:02
S94	1	(index) near20 (plurality with streams)same (cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 18:02
S95	3	(Request) with (index) near20 (protect$3 same cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 18:03
S96	17	(index) near20 (protect$3 same cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 18:03
S97	1	(plurality with streams) near20 (index) near20 (protect$3 same cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 18:03
S98	4	(streams) near20 (index) near20 (protect$3 same cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 18:04
S99	18	(streams) near20 (protect$3 same cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 18:04
S101	13	(streams with protected with video same DRM)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 10:15
S102	9	(streams with protected with video same DRM) same (DRM same encrypt$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 10:15
S103	3	(streams with protected with video same DRM) near20 (encrypt$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 10:16
S104	0	(memory with client with application) near20 (streams with protected with video same DRM)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 10:18
S105	0	(memory same application) near20 (streams with protected with video	US-PGPUB; USPAT; USOCR;	OR	OFF	2013/10/10 10:19

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0979
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

		same DRM)	FPRS; EPO; JPO; DERWENT; IBM_TDB			
S106	1	(client with application) near20 (streams with protected with video same DRM)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 10:19
S107	1	(Application) near20 (streams with protected with video same DRM)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 10:20
S108	3	(Application) same (streams with protected with video same DRM)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 10:20
S109	3	(processor) same (streams with protected with video same DRM)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 10:23
S111	1	(application with configures with processor) same (streams with protected with video same DRM)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 10:24
S112	1	(application same processor) same (streams with protected with video same DRM)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 10:25
S113	4	(application same processor) and (streams with protected with video same DRM)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 10:25
S114	2	"13235729"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 12:26
S115	2	(streams with protected with video same DRM) near20 (Matroska)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 14:14
S116	2	(streams same video same DRM) near20 (Matroska)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 14:15
S117	20	(streams same video) near20 (Matroska)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 14:15
S118	1	S117 and (DRM with Header same Tracks)	US-PGPUB; USPAT; USOCR;	OR	OFF	2013/10/10 14:16

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0980
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S119	10	(DRM with Header same Tracks)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 14:16
S120	1	S119 and (streams same video) near20 (Matroska)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 14:17
S121	1	S119 and (streams) near20 (Matroska)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 14:17
S122	1	S119 and (Matroska)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 14:17
S123	2	("20060245727").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 14:21
S124	2	DRM same (streams same video) near20 (Matroska)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 14:27
S125	9	index same (streams same video) near20 (Matroska)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 14:28
S126	20	(Matroska with container with files)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 14:34
S127	2	S126 and (index or indexing or indexed) near20 (content with cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	WITH	OFF	2013/10/10 14:35
S128	17	S126 and (index or indexing or indexed)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	WITH	OFF	2013/10/10 14:35
S129	20	S117 and (streams same video) near20 (Matroska)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 14:52
S130	3	S129 and (index or indexing or indexed) near20 (Stream$3) same	US-PGPUB; USPAT; USOCR;	OR	OFF	2013/10/10 14:55

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0981
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

		(protected)	FPRS; EPO; JPO; DERWENT; IBM_TDB			
S131	3	S129 and (index or indexing or indexed) same (Stream$3) same (protected)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 14:56
S132	3	S129 and (Stream$3) same (protected)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 14:56
S133	16	S129 and (index or indexing or indexed)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 14:56
S134	7	S129 and (processor) with (index or indexing or indexed)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 14:57
S135	2	(streams with protected) near20 (Matroska)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 14:57
S136	9	S125 and (streams same video) near20 (Matroska)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 14:58
S137	9	S125 and (streams) near20 (Matroska)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 14:59
S138	21	(streams) near20 (Matroska)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 15:00
S139	2	(DRM with Header) near20 (Matroska)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 15:01
S140	2	(DRM) near20 (Matroska)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 15:01
S141	3	(DRM) same (Matroska)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 15:02
S142	7	(DRM with Header same cryptographic)	US-PGPUB; USPAT; USOCR;	OR	OFF	2013/10/10 15:49

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0982
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S143	20	(DRM same Header same cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 15:50
S144	2	(streams) near20 (Matroska) near20 (DRM same Header same cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 15:50
S145	2	(Matroska) near20 (DRM same Header same cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 15:51
S146	2	(DRM same Header same cryptographic) near20 (Matroska)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 15:51
S147	2	(DRM same cryptographic) near20 (Matroska)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 15:51
S148	2	(DRM same Header same cryptographic) same (Matroska)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 15:51
S149	4	(DRM same Header same cryptographic) and (Matroska)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 15:52
S150	54	(bitrate with stream$4) same (alternative with streams)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/15 10:46
S151	6	(bitrate with stream$4) same (alternative with streams) same (protected with content)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/15 10:46
S152	8	(bitrate with stream$4) same (alternative with streams) same (protected cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/15 10:47
S153	6	(bitrate with stream$4) same (alternative with streams) same (protected crypto$5)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/15 10:47
S154	1	713/160.ccls. and (bitrate with stream$4) same (alternative with	US-PGPUB; USPAT; USOCR;	OR	OFF	2013/10/16 15:16

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0983
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

		streams) same (protected crypto$5)	FPRS; EPO; JPO; DERWENT; IBM_TDB			

EAST Search History (Interference)

<This search history is empty>

10/16/2013 5:57:25 PM
C:\Users\agetachew\Documents\EAST\Workspaces\13340623.wsp

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0984
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 1094

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/340,623	12/29/2011 RULE	713	2434	D1:02359A

APPLICANTS

Michael George Kiefer, Scottsdale, AZ;
Eric William Grab, San Diego, CA;
Jason Braness, San Diego, CA;

**** CONTINUING DATA ***************************

This appln claims benefit of 61/530,305 09/01/2011

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****

01/13/2012

Foreign Priority claimed	35 USC 119(a-d) conditions met	Verified and Acknowledged	Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
☑ Yes ☐ No	☑ Yes ☐ No	/ABIY GETACHEW/ Examiner's Signature	☑ A.G. Initials	AZ	19	39	3

ADDRESS

KPPB LLP
2400 EAST KATELLA AVENUE
SUITE 1050
ANAHEIM, CA 92806
UNITED STATES

TITLE

Systems and Methods for Playing Back Alternative Streams of Protected Content Protected Using Common Cryptographic Information

FILING FEE RECEIVED	FEES: Authority has been given in Paper	
2520	No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

BIB (Rev. 05/07).

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13340623	KIEFER ET AL.
	Examiner	Art Unit
	ABIY GETACHEW	2434

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
713	160	10/16/2013	A.G.

SEARCH NOTES		
Search Notes	Date	Examiner
Class/subclass, Text search and google keyword search	10/16/2013	A.G.

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13340623	KIEFER ET AL.
	Examiner	Art Unit
	ABIY GETACHEW	2434

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	10/16/2013								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								
	22	✓								
	23	✓								
	24	✓								
	25	✓								
	26	✓								
	27	✓								
	28	✓								
	29	✓								
	30	✓								
	31	✓								
	32	✓								
	33	✓								
	34	✓								
	35	✓								
	36	✓								

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0987
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13340623	KIEFER ET AL.
	Examiner	Art Unit
	ABIY GETACHEW	2434

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	10/16/2013								
	37	✓								
	38	✓								
	39	✓								

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0988
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/340,623
	Filing Date	Dec 29, 2011
	First Named Inventor	Michael George Kiefer
	Art Unit	2434
	Examiner Name	Abiy Getachew
	Attorney Docket Number	D1:02359A

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		20090132721	A1	2009- 05-21	Soroushian, Kourosh et al.	
		20090290706	A1	2009-11-26	Amini, Lisa D., et al.	
		20090328228	A1	2009-12-31	Schnell, Patrik	
		20130061040	A1	2013-03-07	Kiefer, Michael G., et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
		2011103364	WO	A1	2011-08-25	Thorwirth, Niels		
		2013032518	WO	A2	2013-03-07	Kiefer, Michael, et al.		
		2013032518	WO	A3	2013-09-06	Kiefer, Michael, et al.		

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
		International Search Report and Written Opinion for International Application PCT/US2011/068276, International Filing Date December 31, 2011, Report completed June 19, 2013, Mailed July 8, 2013, 24 pgs.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13/340,623
	Filing Date	Dec 29, 2011
	First Named Inventor	Michael George Kiefer
	Art Unit	2434
	Examiner Name	Abiy Getachew
	Attorney Docket Number	D1:02359A

EXAMINER SIGNATURE			
Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document.
[4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference D1:02359AB.PCT	FOR FURTHER ACTION	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US2011/068276	International filing date *(day/month/year)* 31 December 2011	(Earliest) Priority Date *(day/month/year)* 01 September 2011
Applicant DIVX, LLC		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 2 sheets.

☐ It is also accompanied by a copy of each prior art document cited in this report.

1. Basis of the report

a. With regard to the language, the international search was carried out on the basis of:

☒ the international application in the language in which it was filed.

☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

b. ☐ This international search report has been established taking into account the rectification of an obvious mistake authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).

c. ☐ With regard to any nucleotide and/or amino acid sequence disclosed in the international application, see Box No. I.

2. ☐ Certain claims were found unsearchable (see Box No. II).

3. ☐ Unity of invention is lacking (see Box No. III).

4. With regard to the title,

☒ the text is approved as submitted by the applicant.

☐ the text has been established by this Authority to read as follows:

5. With regard to the abstract,

☒ the text is approved as submitted by the applicant.

☐ the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the drawings,

a. the figure of the drawings to be published with the abstract is Figure No. 1A

☐ as suggested by the applicant.

☐ as selected by this Authority, because the applicant failed to suggest a figure.

☒ as selected by this Authority, because this figure better characterizes the invention.

b. ☐ none of the figures is to be published with the abstract.

Form PCT/ISA/210 (first sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2011/068276

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - H04L 9/18 (2013.01)
USPC - 380/255
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)
IPC(8) - H04L 9/00, 9/08, 9/14, 9/18, (2013.01)
USPC - 380/1, 45, 255, 269, 277, 281

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
CPC- H04L 9/00, 9/08, 9/14, 9/18, (2013.01)

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X -- Y	US 2009/0290706 A1 (AMINI et al) 26 November 2009 (26.11.2009) entire document	1, 2, 14, 15, 27, 28 ----- 3-13, 16-26, 29-105
Y	WO 2011/103364 A1 (THORWIRTH) 25 August 2011 (25.08.2011) entire document	4-13, 17-26, 29-105
Y	US 2009/0328228 A1 (SCHNELL) 31 December 2009 (31.12.2009) entire document	3, 10-13, 16, 23-26, 29-66, 68, 70-83, 85, 87-102, 104
Y	US 2009/0132721 A1 (SOROUSHIAN et al) 21 May 2009 (21.05.2009) entire document	9-13, 22-26, 34, 35, 41-48, 54, 55, 59-66, 68, 75-83, 85, 94-102, 104

☐ Further documents are listed in the continuation of Box C ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"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
19 June 2013	08 JUL 2013
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To: DAVID J. BAILEY
KAUTH, POMEROY, PECK & BAILEY LLP
2400 E. KATELLA, SUITE 1050
ANAHEIM, CA 92806

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	08 JUL 2013
Applicant's or agent's file reference D1:02389AB.PCT	FOR FURTHER ACTION See paragraph 2 below

International application No	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2011/068276	31 December 2011	01 September 2011

International Patent Classification (IPC) or both national classification and IPC
IPC(8) - H04L 9/18 (2013.01)
USPC - 380/255

Applicant DIVX, LLC

1. This opinion contains indications relating to the following items.

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/US	Date of completion of this opinion	Authorized officer:
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	19 June 2013	Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/237 (cover sheet) (July 2011)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2011/066276

Box No. I Basis of this opinion

1. With regard to the language, this opinion has been established on the basis of:

☒ the international application in the language in which it was filed.

☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. ☐ This opinion has been established taking into account the rectification of an obvious mistake authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a)).

3. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:

a. (means)

☐ on paper

☐ in electronic form

b. (time)

☐ in the international application as filed

☐ together with the international application in electronic form

☐ subsequently to this Authority for the purposes of search

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0994
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2011/066276

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	3-13, 16-26, 29-105	YES
	Claims	1, 2, 14, 15, 27, 28	NO
Inventive step (IS)	Claims	None	YES
	Claims	105	NO
Industrial applicability (IA)	Claims	105	YES
	Claims	None	NO

2. Citations and explanations:

Claims 1, 2, 14, 15, 27, 28 lack novelty under PCT Article 33(2) as being anticipated by Amini et al., hereinafter referred to as Amini.

Regarding claim 1, Amini discloses a source encoder (multi-encoder platform 220, para 0031, see fig. 2 [whose components are shown in the computing system of fig. 11, para 0068]), comprising: a processor (processor 1102, para 0068, 0069, see fig. 11); non-volatile storage containing an encoding application (memory 1104 [RAM or ROM (nonvolatile)], para 0068, 0069, see fig. 11), wherein the encoding application configures the processor to: receive source content (a stream source 210 offers unencoded access units [frames] to the encoder, para 0031, see fig. 2); obtain common cryptographic information (encryptor 240 where the streams are encrypted, para 0032, see fig. 2, same key is used for different streams [common cryptographic information], para 0054), encode the source content as a plurality of streams including a plurality of alternative streams of content (multi-encoder 220 generates multiple encoded access units and gives alternate or multiple streams, para 0031, see fig. 2); and protect the plurality of alternative streams of content using the common cryptographic information (same key is used for different streams, para 0054, 0044 [protecting the content]).

Regarding claim 14, Amini discloses a method of encoding source content as a plurality of protected streams using common cryptographic information (multi-encoder 220 generates multiple encoded access units and gives alternate or multiple streams, para 0031, see fig. 2), comprising: receiving source content using a source encoder (a stream source 210 offers unencoded access units [frames] to the encoder, para 0031, see fig. 2); obtaining common cryptographic information using a source encoder (encryptor 240 where the streams are encrypted, para 0032, see fig. 2; same key is used for different streams [common cryptographic information], para 0054); encoding the source content as a plurality of streams including a plurality of alternative streams of content using the source encoder (multi-encoder 220 generates multiple encoded access units and gives alternate or multiple streams, para 0031, see fig. 2); and protecting the plurality of alternative streams of content using the source encoder and the common cryptographic information (same key is used for different streams, para 0054, 0044 [protecting the content]).

Regarding claim 27, Amini discloses a machine readable medium containing processor instructions (machine readable medium, claim 26; multi-encoder platform 220, para 0031, see fig. 2 [whose components are shown in the computing system of fig. 11, para 0068]), where execution of the instructions by a processor causes the processor to perform a process (processor 1102, para 0068, 0069, see fig. 11) comprising receiving source content using a source encoder (a stream source 210 offers unencoded access units [frames] to the encoder, para 0031, see fig. 2); obtaining common cryptographic information using a source encoder (encryptor 240 where the streams are encrypted, para 0032, see fig. 2, same key is used for different streams [common cryptographic information], para 0054); encoding the source content as a plurality of streams including a plurality of alternative streams of content using the source encoder (multi-encoder 220 generates multiple encoded access units and gives alternate or multiple streams, para 0031, see fig. 2); and protecting the plurality of alternative streams of content using the source encoder and the common cryptographic information (same key is used for different streams, para 0054, 0044 [protecting the content]).

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0995
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2011/063276

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of

Regarding claims 2 and 15, Amini teaches wherein the encoding application configures the processor to encode and protect the source content by configuring the processor to: encode a portion of source content (multi-encoder 220 generates multiple encoded access units and gives alternate or multiple streams, para 0031, see fig. 2); and encrypt at least one portion of the encoded portion of content so that the at least one encrypted portion can be accessed using the common cryptographic information (same key is used for different streams (which are encrypted using the encryptor 220, para 0032, see fig. 2], para 0054, 0044 [protecting the content]).

Regarding claim 28, Amini discloses wherein the machine readable medium is non-volatile memory (memory 1104 with ROM [non-volatile], para 0068, 0069, see fig. 11).

Claims 29-33, 36-40, 48-53, 56-58 lack an inventive step under PCT Article 33(3) as being obvious over Thorwirth and in view of Schnell and further in view of Amini.

Regarding claim 29, Thorwirth discloses a content distribution system (system for enhancing security of content distribution, para 0018), comprising a content distribution server (content ingested on server 301 part of a content distribution network, para 0052),where the content distribution server stores a plurality of content files containing alternative streams of protected content associated with a title (CDN stores six alternative chunks created for each section with different encoding parameters and two different watermark payloads [alternative streams of protected content], para 0052),the alternative streams of protected content are protected using cryptographic information (the chunks are protected using different watermark payloads, para 0052), and each content file includes a copy of the cryptographic information encrypted using at least one encryption key (the content keys used to encrypt the content are encrypted using a key unique to a specific user or client device, para 0058); wherein a server is configured to: receive a request for access to the alternative streams of protected content associated with the title from a playback device (client device authenticated requests access to choose content choice for playback, para 0053; link has a part that identifies the chunk to be accessed [part that identifies the chunk is the title with a unique identifier, para 0057]);and securely provide a copy of the at least one encryption key used to encrypt the cryptographic information to the playback device (a copy of the encryption key used for the encryption of the content key is delivered securely to the specific user or client device, para 0058, hashing or encrypting the encrypted content and key, para 0064);and wherein the content distribution server is configured to grant the playback device access to the alternative streams of protected content (server provides access to the client based on the selection or chunks requested, para 0053). Thorwirth lacks the teaching of comprising: a DRM server; a container file; common cryptographic information. However, Thorwirth shows how well known in the art are container files (sections of files in a container file, para 0004, different media containers for adaptive streaming, para 0009 [background]). Further, Schnell is in the field of segmented media content rights management (abstract, title) and teaches a content distributor with a DRM system (content server 122 and a DRM system 118 distribute protected media content 120 to various wireless media devices 108, para 0026-0031). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Schnell to incorporate the DRM system in the invention of Thorwirth for the purpose of providing DRM associated features such as licenses that correspond to the media segments of the protected media (Schnell, para 0004). Furthermore, Amini teaches a content distribution with common cryptographic information for the alternate streams of content (multi-encoder 220 generates multiple encoded access units and gives alternate or multiple streams, para 0031, see fig. 2; same key is used for different streams, para 0054, 0044 [protecting the content]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Amini to incorporate the common cryptographic information in the invention of Thorwirth for the purpose of encrypting and protecting the alternate streams of source content and allowing random access and joining a broadcasted multimedia stream at a point somewhere other than at the beginning of the stream (Amini, para 0041, 0064).

Regarding claim 49, Thorwirth discloses a method of distributing content encoded as a plurality of alternative streams of protected content (CDN stores six alternative chunks created for each section with different encoding parameters and two different watermark payloads [alternative streams of protected content], para 0052), where the alternative streams of protected content are protected using cryptographic information (the chunks are protected using different watermark payloads, para 0052) and each stream of protected content includes a copy of the cryptographic information encrypted using at least one encryption key (the content keys used to encrypt the content are encrypted using a key unique to a specific user or client device, para 0058), the method comprising: receiving a request for access to the alternative streams of protected content associated with the title from a playback device using a server (client device authenticated requests access to choose content choice for playback, para 0053; link has a part that identifies the chunk to be accessed [part that identifies the chunk is the title with a unique identifier, para 0057]); securely providing to the playback device at least one encryption key using the server (a copy of the encryption key used for the encryption of the content key is delivered securely to the specific user or client device, para 0058, hashing or encrypting the encrypted content and key, para 0064), where the at least one encryption key is used to access the encrypted cryptographic information (the content keys used to encrypt the content are encrypted using a key unique to a specific user or client device, para 0058); and granting the playback device access to the alternative streams of protected content using a content distribution server (content ingested on server 301 part of a content distribution network, para 0052; server provides access to the client based on the selection or chunks requested, para 0053).Thorwirth lacks the teaching of comprising: a DRM server; a container file; common cryptographic information. However, Thorwirth shows how well known in the art are container files (sections of files in a container file, para 0004, different media containers for adaptive streaming, para 0009 [background]). Further, Schnell is in the field of segmented media content rights management (abstract, title) and teaches a content distributor with a DRM system (content server 122 and a DRM system 118 distribute protected media content 120 to various wireless media devices 108, para 0026-0031). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Schnell to incorporate the DRM system in the invention of Thorwirth for the purpose of providing DRM associated features such as licenses that correspond to the media segments of the protected media (Schnell, para 0004). Furthermore, Amini teaches a content distribution with common cryptographic information for the alternate streams of content (multi-encoder 220 generates multiple encoded access units and gives alternate or multiple streams, para 0031, see fig. 2; same key is used for different streams, para 0054, 0044 [protecting the content]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Amini to incorporate the common cryptographic information in the invention of Thorwirth for the purpose of encrypting and protecting the alternate streams of source content and allowing random access and joining a broadcasted multimedia stream at a point somewhere other than at the beginning of the stream (Amini, para 0041, 0064).

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0996
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2011/068276

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of

Regarding claim 30, Thorwirth as modified teaches wherein the server is configured to associate a title ID with the title (client device authenticated requests access to choose content choice for playback, para 0053; link has a part that identifies the chunk to be accessed [part that identifies the chunk is the title with a unique identifier, para 0057]; the chunks are protected using different watermark payloads, para 0052). Thorwirth lacks the teaching of a DRM server. Schnell teaches a content distributor with a DRM system (content server 122 and a DRM system 118 distribute protected media content 120 to various wireless media devices 106, para 0028-0031). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Schnell to incorporate the DRM system in the invention of Thorwirth for the purpose of providing DRM associated features such as licenses that correspond to the media segments of the protected media (Schnell, para 0004).

Regarding claim 31, Thorwirth teaches wherein server is configured to associate the cryptographic information with the title ID (client device authenticated requests access to choose content choice for playback, para 0053; link has a part that identifies the chunk to be accessed [part that identifies the chunk is the title with a unique identifier, para 0057]; the chunks are protected using different watermark payloads, para 0052). Thorwirth lacks the teaching of a DRM server and a common cryptographic information. Schnell teaches a content distributor with a DRM system (content server 122 and a DRM system 118 distribute protected media content 120 to various wireless media devices 106, para 0028-0031). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Schnell to incorporate the DRM system in the invention of Thorwirth for the purpose of providing DRM associated features such as licenses that correspond to the media segments of the protected media (Schnell, para 0004). Furthermore, Amini teaches a content distribution with common cryptographic information for the alternate streams of content (multi-encoder 220 generates multiple encoded access units and gives alternate or multiple streams, para 0031, see fig. 2; same key is used for different streams, para 0054, 0044 [protecting the content]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Amini to incorporate the common cryptographic information in the invention of Thorwirth for the purpose of encrypting and protecting the alternate streams of source content and allowing random access and joining a broadcasted multimedia stream at a point somewhere other than at the beginning of the stream (Amini, para 0041, 0054).

Regarding claim 32, Thorwirth teaches wherein the request for access to the alternative streams of protected content associated with the title comprises a request identifying a title ID (client device authenticated requests access to choose content choice for playback, para 0053; link has a part that identifies the chunk to be accessed [part that identifies the chunk is the title with a unique identifier, para 0057]; the chunks are protected using different watermark payloads, para 0052).

Regarding claim 33, Thorwirth teaches wherein the content distribution server is further configured to: receive requests for portions of at least one container file from the playback device (client device authenticated requests access to choose content choice for playback, para 0053; link has a part that identifies the chunk to be accessed [part that identifies the chunk is the title with a unique identifier, para 0057]), and provide the requested portions of the at least one container file to the playback device (server provides access to the client based on the selection or chunks requested para 0053).

Regarding claim 38, Thorwirth teaches obtain common cryptographic information from the server (the chunks are protected using different watermark payloads, para 0052); receive source content, encode the source content as a plurality of streams including a plurality of alternative streams of content (CDN stores six alternative chunks created for each section with different encoding parameters and two different watermark payloads [alternative streams of protected content], para 0052); protect the plurality of alternative streams of content using cryptographic information (the chunks are protected using different watermark payloads, para 0052); protect the cryptographic information using at least one encryption key (the content keys used to encrypt the content are encrypted using a key unique to a specific user or client device, para 0058); and provide a plurality of content files containing the plurality of alternative streams of protected content to the content distribution server (CDN stores six alternative chunks created for each section with different encoding parameters and two different watermark payloads [alternative streams of protected content], para 0052). However, Thorwirth lacks the teaching of a source encoder, common cryptographic information and a DRM server, container files. However, Thorwirth shows how well known in the art are container files (sections of files in a container file, para 0004, different media containers for adaptive streaming, para 0009 [background]). Further, Schnell is in the field of segmented media content rights management (abstract, title) and teaches a content distributor with a DRM system (content server 122 and a DRM system 118 distribute protected media content 120 to various wireless media devices 106, para 0028-0031). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Schnell to incorporate the DRM system in the invention of Thorwirth for the purpose of providing DRM associated features such as licenses that correspond to the media segments of the protected media (Schnell, para 0004). Furthermore, Amini teaches a content distribution source encoder (multi-encoder platform 220, para 0031, see fig. 2 [whose components are shown in the computing system of fig. 11, para 0068]) with common cryptographic information for the alternate streams of content (multi-encoder 220 generates multiple encoded access units and gives alternate or multiple streams, para 0031, see fig. 2, same key is used for different streams, para 0054, 0044 [protecting the content]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Amini to incorporate the common cryptographic information in the invention of Thorwirth for the purpose of encrypting and protecting the alternate streams of source content and allowing random access and joining a broadcasted multimedia stream at a point somewhere other than at the beginning of the stream (Amini, para 0041, 0054).

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0997
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2011/068276

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

Regarding claim 37, Thorwirth lacks the teaching wherein the source encoder is configured to: encode a portion of content; and encrypt at least one portion of the encoded content so that the at least one encrypted portion can be accessed using the common cryptographic information. Amini teaches wherein the source encoder is configured to: encode a portion of content (multi-encoder 220 generates multiple encoded access units and gives alternate or multiple streams, para 0031, see fig. 2); and encrypt at least one portion of the encoded portion of content so that the at least one encrypted portion can be accessed using the common cryptographic information (same key is used for different streams [which are encrypted using the encryptor 220, para 0032, see fig. 2], para 0054, 0044 [protecting the content]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Amini to incorporate the common cryptographic information in the invention of Thorwirth for the purpose of encrypting and protecting the alternate streams of source content and allowing random access and joining a broadcasted multimedia stream at a point somewhere other than at the beginning of the stream (Amini, para 0041, 0054).

Regarding claim 38, Thorwirth lacks the teaching wherein the source encoder is configured to write each of the alternative streams of protected content to a separate container file. However, Thorwirth shows wherein the alternative streams of protected content are written into a container file is well known in the art (sections of multiple files are created with pointers within a container file, para 0004, 0010). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Thorwirth to incorporate the container file feature in the invention for the purpose of providing a playlist with a list of URLS pointing to TS container files that contain alternative chunks for the sections of a piece of content (Thorwirth, para 0010).

Regarding claim 39, Thorwirth teaches each stream of protected content includes a copy of the cryptographic information encrypted using at least one encryption key (the content keys used to encrypt the content are encrypted using a key unique to a specific user or client device, para 0058), but lacks the teaching wherein the source encoder is configured to process common cryptographic information. Amini teaches wherein the encoding application configures the processor to write at least a portion of the common cryptographic information (a stream source 210 offers unencoded access units [frames] to the encoder, para 0031, see fig. 2; encryptor 240 where the streams are encrypted, para 0032, see fig. 2, same key is used for different streams [common cryptographic information], para 0054). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Amini to incorporate the common cryptographic information in the invention of Thorwirth for the purpose of encrypting and protecting the alternate streams of source content and allowing random access and joining a broadcasted multimedia stream at a point somewhere other than at the beginning of the stream (Amini, para 0041, 0054).

Regarding claim 40, Thorwirth teaches wherein the source encoder is configured to encrypt at least a portion of the cryptographic information using a single encryption key and write the encrypted information to each of the container files containing the alternative streams of protected content (the content keys used to encrypt the content are encrypted using a key unique to a specific user or client device, para 0058), but lacks the teaching wherein the source encoder is configured to process common cryptographic information. Amini teaches wherein the encoding application configures the processor to write at least a portion of the common cryptographic information (a stream source 210 offers unencoded access units [frames] to the encoder, para 0031, see fig. 2; encryptor 240 where the streams are encrypted, para 0032, see fig. 2; same key is used for different streams [common cryptographic information], para 0054). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Amini to incorporate the common cryptographic information in the invention of Thorwirth for the purpose of encrypting and protecting the alternate streams of source content and allowing random access and joining a broadcasted multimedia stream at a point somewhere other than at the beginning of the stream (Amini, para 0041, 0054).

Regarding claim 50, Thorwirth teaches wherein the title is identified using a title ID (client device authenticated requests access to choose content choice for playback, para 0053; link has a part that identifies the chunk to be accessed [part that identifies the chunk is the title with a unique identifier, para 0057]; the chunks are protected using different watermark payloads, para 0052).

Regarding claim 51, Thorwirth teaches wherein the common cryptographic information is associated with the title ID (client device authenticated requests access to choose content choice for playback, para 0053; link has a part that identifies the chunk to be accessed [part that identifies the chunk is the title with a unique identifier, para 0057]; the chunks are protected using different watermark payloads, para 0052). Thorwirth lacks the teaching of common cryptographic information. Amini teaches a content distribution with common cryptographic information for the alternate streams of content (multi-encoder 220 generates multiple encoded access units and gives alternate or multiple streams, para 0031, see fig. 2; same key is used for different streams, para 0054, 0044 [protecting the content]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Amini to incorporate the common cryptographic information in the invention of Thorwirth for the purpose of encrypting and protecting the alternate streams of source content and allowing random access and joining a broadcasted multimedia stream at a point somewhere other than at the beginning of the stream (Amini, para 0041, 0054).

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0998
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of

Regarding claim 52, Thorwirth teaches wherein the request for access to the alternative streams of protected content associated with the title comprises a request identifying a title ID (client device authenticated requests access to choose content choice for playback, para 0053; link has a part that identifies the chunk to be accessed (part that identifies the chunk is the title with a unique identifier, para 0057); the chunks are protected using different watermark payloads, para 0052).

Regarding claim 53, Thorwirth teaches receiving requests for portions of at least one container file from the playback device using the content distribution server (client device authenticated requests access to choose content choice for playback, para 0053; link has a part that identifies the chunk to be accessed (part that identifies the chunk is the title with a unique identifier, para 0057)); and providing the requested portions of the at least one container file to the playback device using the content distribution server (server provides access to the client based on the selection or chunks requested para 0053).

Regarding claim 56, Thorwirth teaches obtain common cryptographic information from the server (the chunks are protected using different watermark payloads, para 0052); receive source content, encode the source content as a plurality of streams including a plurality of alternative streams of content (CDN stores six alternative chunks created for each section with different encoding parameters and two different watermark payloads (alternative streams of protected content), para 0052); protect the plurality of alternative streams of content using cryptographic information (the chunks are protected using different watermark payloads, para 0052); protect the cryptographic information using at least one encryption key (the content keys used to encrypt the content are encrypted using a key unique to a specific user or client device, para 0058); and provide a plurality of content files containing the plurality of alternative streams of protected content to the content distribution server (CDN stores six alternative chunks created for each section with different encoding parameters and two different watermark payloads (alternative streams of protected content), para 0052). However, Thorwirth lacks the teaching of a source encoder, common cryptographic information and a DRM server, container files. However, Thorwirth shows how well known in the art are container files (sections of files in a container file, para 0004, different media containers for adaptive streaming, para 0009 (background)). Further, Schnell is in the field of segmented media content rights management (abstract, title) and teaches a content distributor with a DRM system (content server 122 and a DRM system 118 distribute protected media content 120 to various wireless media devices 106, para 0028-0031). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Schnell to incorporate the DRM system in the invention of Thorwirth for the purpose of providing DRM associated features such as licenses that correspond to the media segments of the protected media (Schnell, para 0004). Furthermore, Amini teaches a content distribution source encoder (multi-encoder platform 220, para 0031, see fig. 2 (whose components are shown in the computing system of fig. 11, para 0068)) with common cryptographic information for the alternate streams of content (multi-encoder 220 generates multiple encoded access units and gives alternate or multiple streams, para 0031, see fig. 2; same key is used for different streams, para 0054, 0044 (protecting the content)). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Amini to incorporate the common cryptographic information in the invention of Thorwirth for the purpose of encrypting and protecting the alternate streams of source content and allowing random access and joining a broadcasted multimedia stream at a point somewhere other than at the beginning of the stream (Amini, para 0041, 0054).

Regarding claim 57, Thorwirth lacks the teaching of encoding a portion of content using the source encoder; and encrypting at least one portion of the encoded content using the source encoder so that the at least one encrypted portion can be accessed using the common cryptographic information. Amini teaches wherein the source encoder is configured to: encode a portion of content (multi-encoder 220 generates multiple encoded access units and gives alternate or multiple streams, para 0031, see fig. 2); and encrypt at least one portion of the encoded portion of content so that the at least one encrypted portion can be accessed using the common cryptographic information (same key is used for different streams (which are encrypted using the encryptor 220, para 0032, see fig. 2], para 0054, 0044 [protecting the content]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Amini to incorporate the common cryptographic information in the invention of Thorwirth for the purpose of encrypting and protecting the alternate streams of source content and allowing random access and joining a broadcasted multimedia stream at a point somewhere other than at the beginning of the stream (Amini, para 0041, 0054).

Regarding claim 58, Thorwirth lacks the teaching wherein the source encoder is configured to write each of the alternative streams of protected content to a separate container file. However, Thorwirth shows wherein the alternative streams of protected content are written into a container file is well known in the art (sections of multiple files are created with pointers within a container file, para 0004, 0010). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Thorwirth to incorporate the container file feature in the invention for the purpose of providing a playlist with a list of URLS pointing to TS container files that contain alternative chunks for the sections of a piece of content (Thorwirth, para 0010).

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0999
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

Claims 67, 69, 84, 86, 103, 105 lack an inventive step under PCT Article 33(3) as being obvious over Thorwirth and in view of Amini.

Regarding claim 67, Thorwirth discloses a playback device (client device or user requests access for playback, para 0053), comprising: a processor (client device is a personal computer 404, mobile phone 406 or consumer electronics device 408 [a processor is inherent], para 0056, see fig. 4); memory containing a client application (client device is a personal computer 404, mobile phone 406 or consumer electronics device 408 [a memory is inherent], para 0056, see fig. 4); wherein the client application configures the processor to: request a file identifying a plurality of alternative streams of protected content (CDN stores six alternative chunks created for each section with different encoding parameters and two different watermark payloads [alternative streams of protected content], para 0052; link has a part that identifies the chunk to be accessed [part that identifies the chunk is the title with a unique identifier, para 0057]),where each of the alternative streams of protected content are encrypted using cryptographic information (the chunks are protected using different watermark payloads, para 0052); request portions of content from at least the plurality of alternative streams of protected content (client device authenticated requests access to choose content choice for playback, para 0053; link has a part that identifies the chunk to be accessed [part that identifies the chunk is the title with a unique identifier, para 0057]); access the protected content using the cryptographic information (content ingested on server 301 part of a content distribution network, para 0052; server provides access to the client based on the selection or chunks requested, para 0053); and playback the content (playback of content on the client device, para 0053). Thorwirth lacks the teaching of a top level index file obtain the common cryptographic information. However, Thorwirth teaches a top level index file is well known in the art (top level index file pointing to a number of alternate streams that contain actual video and audio data, para 0009). Further, Amini teaches a content distribution with common cryptographic information for the alternate streams of content (multi-encoder 220 generates multiple encoded access units and gives alternate or multiple streams, para 0031, see fig. 2; same key is used for different streams, para 0054, 0044 [protecting the content]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Amini to incorporate the common cryptographic information in the invention of Thorwirth for the purpose of encrypting and protecting the alternate streams of source content and allowing random access and joining a broadcasted multimedia stream at a point somewhere other than at the beginning of the stream (Amini, para 0041, 0054).

Regarding claim 84, Thorwirth discloses a method of performing adaptive bitrate streaming using a plurality of alternative streams of protected content (CDN stores six alternative chunks created for each section with different encoding parameters and two different watermark payloads [alternative streams of protected content], para 0052 [chunks differ in encoding and bit rat . adaptive bitrate streaming system, para 0005]), where each of the streams of protected content is protected using cryptographic information (), the method comprising: requesting a file identifying a plurality of alternative streams of protected content using a playback device (CDN stores six alternative chunks created for each section with different encoding parameters and two different watermark payloads [alternative streams of protected content], para 0052; link has a part that identifies the chunk to be accessed [part that identifies the chunk is the title with a unique identifier, para 0057]), where each of the alternative streams of protected content are encrypted using cryptographic information (the chunks are protected using different watermark payloads, para 0052); obtaining the cryptographic information using the playback device (the content keys used to encrypt the content are encrypted using a key unique to a specific user or client device, para 0056); requesting portions of content from at least the plurality of alternative streams of protected content using the playback device (client device authenticated requests access to choose content choice for playback, para 0053; link has a part that identifies the chunk to be accessed [part that identifies the chunk is the title with a unique identifier, para 0057]); accessing the protected content using the playback device and the cryptographic information (content ingested on server 301 part of a content distribution network, para 0052; server provides access to the client based on the selection or chunks requested, para 0053); and playing back the content using the playback device (playback of content on the client device, para 0053);Thorwirth lacks the teaching of a top level index file obtain the common cryptographic information. However, Thorwirth teaches a top level index file is well known in the art (top level index file pointing to a number of alternate streams that contain actual video and audio data, para 0009). Further, Amini teaches a content distribution with common cryptographic information for the alternate streams of content (multi-encoder 220 generates multiple encoded access units and gives alternate or multiple streams, para 0031, see fig. 2; same key is used for different streams, para 0054, 0044 [protecting the content]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Amini to incorporate the common cryptographic information in the invention of Thorwirth for the purpose of encrypting and protecting the alternate streams of source content and allowing random access and joining a broadcasted multimedia stream at a point somewhere other than at the beginning of the stream (Amini, para 0041, 0054).

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1000
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

International application No.
PCT/US2011/068276

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:

Regarding claim 103, Thorwirth discloses a machine readable medium containing processor instructions, where execution of the instructions by a processor causes the processor to perform a process (implementation process, para 0047 [CDN stores six alternative chunks created for each section with different encoding parameters and two different watermark payloads [alternative streams of protected content], para 0052]) comprising: request a file identifying a plurality of alternative streams of protected content (link has a part that identifies the chunk to be accessed [part that identifies the chunk is the title with a unique identifier, para 0057]), where each of the alternative streams of protected content are encrypted using cryptographic information (the chunks are protected using different watermark payloads, para 0052), obtaining the cryptographic information (the content keys used to encrypt the content are encrypted using a key unique to a specific user or client device, para 0058), requesting portions of content from at least the plurality of alternative streams of protected content (client device authenticated requests access to choose content choice for playback, para 0053; link has a part that identifies the chunk to be accessed [part that identifies the chunk is the title with a unique identifier, para 0057]), accessing the protected content using the cryptographic information (content ingested on server 301 part of a content distribution network, para 0052, server provides access to the client based on the selection or chunks requested, para 0053), and playing back the content (playback of content on the client device, para 0053).Thorwirth lacks the teaching of a top level index file obtain the common cryptographic information. However, Thorwirth teaches a top level index file is well known in the art (top level index file pointing to a number of alternate streams that contain actual video and audio data, para 0009). Further, Amini teaches a content distribution with common cryptographic information for the alternate streams of content (multi-encoder 220 generates multiple encoded access units and gives alternate or multiple streams, para 0031, see fig. 2; same key is used for different streams, para 0054, 0044 [protecting the content]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Amini to incorporate the common cryptographic information in the invention of Thorwirth for the purpose of encrypting and protecting the alternate streams of source content and allowing random access and joining a broadcasted multimedia stream at a point somewhere other than at the beginning of the stream (Amini, para 0041, 0054).

Regarding claims 69 and 86, Thorwirth lacks the teaching wherein each of the alternative streams of protected content is contained within a separate container file, and the top level index file identifies a container file containing each of the alternative streams. However, Thorwirth shows how well known in the art are container files (sections of files in a container file, para 0004, different media containers for adaptive streaming, para 0009 [background]) and a top level index file identifies a container file containing each of the alternative streams (top level index file pointing to a number of alternate streams that contain actual video and audio data, para 0009). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Thorwirth to incorporate the container file and top level index file in the invention for the purpose of providing a playlist with a list of URLS pointing to TS container files that contain alternative chunks for the sections of a piece of content (Thorwirth, para 0010).

Regarding claim 105, Thorwirth lacks the teaching wherein the machine readable medium is non-volatile memory. Amini teaches wherein the machine readable medium is non-volatile memory (memory 1104 with ROM [non-volatile], para 0068, 0069, see fig. 11). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Amini to incorporate the non-volatile memory for storing the common cryptographic information in the invention of Thorwirth for the purpose of encrypting and protecting the alternate streams of source content and allowing random access and joining a broadcasted multimedia stream at a point somewhere other than at the beginning of the stream (Amini, para 0041, 0054).

Claims 3, 16 lack an inventive step under PCT Article 33(3) as being obvious over Amini and in view of Schnell.

Regarding claims 3 and 16, Amini lacks the teaching wherein the encoding application configures the processor to obtain common cryptographic information by configuring the processor to: send a request to a DRM server for common cryptographic information; and receive the common cryptographic information from the DRM server. However, Amini teaches a content distribution with common cryptographic information for the alternate streams of content (multi-encoder 220 generates multiple encoded access units and gives alternate or multiple streams, para 0031, see fig. 2; same key is used for different streams, para 0054, 0044 [protecting the content]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Amini to incorporate the common cryptographic information in the invention of Thorwirth for the purpose of encrypting and protecting the alternate streams of source content and allowing random access and joining a broadcasted multimedia stream at a point somewhere other than at the beginning of the stream (Amini, para 0041, 0054). Further, Schnell teaches a DRM system that sends cryptographic information to the media device (DRM system 118 with domain controller 124 and license server 126, where the DRM system encrypts the media content, licenser server can issue DRM licenses before media content by various media devices, para 0022, 0023 [media device 202 also includes DRM platform 21 to receive the DRM license, para 0034]).Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Schnell to incorporate the DRM system in the invention of Thorwirth for the purpose of providing DRM associated features such as licenses that correspond to the media segments of the protected media (Schnell, para 0004).

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1001
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2011/058276

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

Claims 4-8, 17-21 lack an inventive step under PCT Article 33(3) as being obvious over Amini and in view of Thorwirth.

Regarding claims 4 and 17, Amini teaches the common cryptographic content and the plurality of alternative streams of protected content (a stream source 210 offers unencoded access units (frames) to the encoder, para 0031, see fig. 2; encryptor 240 where the streams are encrypted, para 0032, see fig. 2; same key is used for different streams (common cryptographic information), para 0054), but lacks the teaching wherein a title is associated with the common cryptographic content and the plurality of alternative streams of protected content. Thorwirth teaches a title is associated with the cryptographic content and the plurality of alternative streams of protected content (client device authenticated requests access to choose content choice for playback, para 0053; link has a part that identifies the chunk to be accessed (part that identifies the chunk is the title with a unique identifier, para 0067); the chunks are protected using different watermark payloads, para 0062). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Thorwirth to incorporate the title feature in the invention of Amini for the purpose of providing the content distribution server a link that includes a unique identifier that enables the server to determine the information to be embedded in the chunk (Thorwirth, para 0067).

Regarding claims 5 and 18, Amini lacks the teaching wherein the encoding application configures the processor to write each of the alternative streams of protected content to a separate container file. However, Thorwirth shows wherein the alternative streams of protected content are written into a container file is well known in the art (sections of multiple files are created with pointers within a container file, para 0004, 0010). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Thorwirth to incorporate the container file feature in the invention of Amini for the purpose of providing a playlist with a list of URLS pointing to TS container files that contain alternative chunks for the sections of a piece of content (Thorwirth, para 0010).

Regarding claims 6 and 19, Amini teaches wherein the encoding application configures the processor to write at least a portion of the common cryptographic information (a stream source 210 offers unencoded access units (frames) to the encoder, para 0031, see fig. 2; encryptor 240 where the streams are encrypted, para 0032, see fig. 2, same key is used for different streams (common cryptographic information), para 0054), but lacks the teaching of the cryptographic information encrypted using at least one encryption key to each of the container files containing the alternative streams of protected content. Thorwirth teaches each stream of protected content includes a copy of the cryptographic information encrypted using at least one encryption key (the content keys used to encrypt the content are encrypted using a key unique to a specific user or client device, para 0058). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Thorwirth to incorporate the encryption key in the invention of Amini for the purpose of providing an encryption key unique to a specific user or client device and the encrypted data is delivered securely and individually to the user and/or client device (Thorwirth, para 0058).

Regarding claims 7 and 20, Amini teaches wherein writing the at least a portion of the common cryptographic information (a stream source 210 offers unencoded access units (frames) to the encoder, para 0031, see fig. 2; encryptor 240 where the streams are encrypted, para 0032, see fig. 2; same key is used for different streams (common cryptographic information), para 0054), but lacks the teaching of writing to the container files containing the alternative streams of protected content comprises encrypting the at least a portion of the common cryptographic information written to each of the container files using at least one encryption key. Thorwirth teaches each stream of protected content includes a copy of the cryptographic information encrypted using at least one encryption key (the content keys used to encrypt the content are encrypted using a key unique to a specific user or client device, para 0058). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Thorwirth to incorporate the encryption key in the invention of Amini for the purpose of providing an encryption key unique to a specific user or client device and the encrypted data is delivered securely and individually to the user and/or client device (Thorwirth, para 0058).

Regarding claims 8 and 21, Amini teaches wherein writing the at least a portion of the common cryptographic information (a stream source 210 offers unencoded access units (frames) to the encoder, para 0031, see fig. 2; encryptor 240 where the streams are encrypted, para 0032, see fig. 2; same key is used for different streams (common cryptographic information), para 0054), but lacks the teaching of writing to the container files containing the alternative streams of protected content comprises encrypting the at least a portion of the common cryptographic information written to each of the container files using the same encryption key. However, Thorwirth teaches each stream of protected content includes a copy of the cryptographic information encrypted using at least one encryption key (the content keys used to encrypt the content are encrypted using a key unique to a specific user or client device, para 0058). Further, encrypting the content for protection is well known in the art and the specifics (using same encryption key) would have been a matter of design choice. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Thorwirth to incorporate the encryption key in the invention of Amini for the purpose of providing an encryption key unique to a specific user or client device and the encrypted data is delivered securely and individually to the user and/or client device (Thorwirth, para 0058).

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1002
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of

Claims 9, 22 lack an inventive step under PCT Article 33(3) as being obvious over Amini and in view of Thorwirth and further in view of Soroushian et al., hereinafter referred to as Soroushian.

Regarding claims 9 and 22, Amini lacks the teaching wherein the container files are Matroska container files. Soroushian is in the field of playback and distribution systems (abstract) and further teaches wherein the content is stored as chunks or elements in a Matroska container (MKV container composed of lists, chunks and/or elements, para 0031, see fig. 1c [Matroska is MKV, para 003]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Soroushian to incorporate the Matroska container files in the invention of Amini for the purpose of providing a MKV container for distributing high-definition downloadable content on the internet and peer-to-peer networks (Soroushian, para 0003).

Claims 10-13, 23-26 lack an inventive step under PCT Article 33(3) as being obvious over Amini and in view of Thorwirth and further in view of Soroushian and even further in view of Schnell.

Regarding claims 10 and 23, Amini teaches common cryptographic information (a stream source 210 offers unencoded access units [frames] to the encoder, para 0031, see fig. 2; encryptor 240 where the streams are encrypted, para 0032, see fig. 2; same key is used for different streams [common cryptographic information], para 0054) wherein, but lacks the teaching wherein the encoding application configures the processor to write a DRMHeader element to the TracksData element in a Tracks element within each of the Matroska container files, where the DRMHeader element includes an encrypted copy of the common cryptographic information. Soroushian teaches wherein the content is stored as chunks or elements in a Matroska container (MKV container composed of lists, chunks and/or elements, para 0031, see fig. 1c [Matroska is MKV, para 003]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Soroushian to incorporate the Matroska container files in the invention of Amini for the purpose of providing a MKV container for distributing high-definition downloadable content on the internet and peer-to-peer networks (Soroushian, para 0003). Schnell teaches writing a DRMHeader element to the tracksDATA element in a Tracks element within each of the content files, wherein the DRMHeader element includes an encrypted copy of the cryptographic information (file header object 218 [DRM header element] has the DRM licenses for the protected media content, para 0036, written in a file segment 160, which has track objects 222 associated with the tracks or video tracks, para 0037, see fig. 2). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Schnell to incorporate the DRM elements in the invention of Amini for the purpose of seamlessly rendering all of the segments of a movie, without managing a multitude of DRM licenses for the different versions of the median content segments (Schnell, para 0036).

Regarding claims 11 and 24, Amini teaches common cryptographic information (a stream source 210 offers unencoded access units [frames] to the encoder, para 0031, see fig. 2; encryptor 240 where the streams are encrypted, para 0032, see fig. 2, same key is used for different streams [common cryptographic information], para 0054) wherein, but lacks the teaching wherein the common cryptographic information is a set of encryption keys, the encoding application configures the processor to: encrypt the set of encryption keys using at least one encryption key; and write the encrypted set of encryption keys to the DRMHeader element of each of the Matroska container files. Thorwirth teaches a set of encryption keys for each chunk of content ((the chunks are protected using different watermark payloads, para 0052) and encrypt the set of encryption keys using one encryption key (the content keys used to encrypt the content are encrypted using a key unique to a specific user or client device, para 0058). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Thorwirth to incorporate the encryption key in the invention of Amini for the purpose of providing an encryption key unique to a specific user or client device and the encrypted data is delivered securely and individually to the user and/or client device (Thorwirth, para 0058). Soroushian teaches wherein the content is stored as chunks or elements in a Matroska container (MKV container composed of lists, chunks and/or elements, para 0031, see fig. 1c [Matroska is MKV, para 003]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Soroushian to incorporate the Matroska container files in the invention of Amini for the purpose of providing a MKV container for distributing high-definition downloadable content on the internet and peer-to-peer networks (Soroushian, para 0003). Further, Schnell teaches writing encrypted set of encryption keys to the DRMHeader element (file header object 218 [DRM header element] has the DRM licenses for the protected media content, para 0036). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Schnell to incorporate the DRM elements in the invention of Amini for the purpose of seamlessly rendering all of the segments of a movie, without managing a multitude of DRM licenses for the different versions of the median content segments (Schnell, para 0036).

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

Regarding claims 12 and 25, Amini teaches wherein: the source content includes a stream of video (bitstreams are series of compressed data units (video frames), para 0037); and the encoding application configures the processor to: encode a frame of video (encoding parameters generate several compressed data units of the original, para 0037); protect the encoded frame of video by encrypting at least a portion of the encoded frame of video (encryption is done, para 0041, encryptor 240 where the streams are encrypted, para 0032, see fig. 2, same key is used for different streams (common cryptographic information), para 0054). Amini lacks the teaching to write a BlockGroup element to a Matroska container file including a DRMinfo element identifying the at least one portion of the encoded frame of video that is encrypted and at least one encryption key from the set of encryption keys used to access the at least one encrypted portion of the encoded frame of video. Soroushian teaches wherein the content is stored as chunks or elements in a Matroska container (MKV container composed of lists, chunks and/or elements, para 0031, see fig. 1c [Matroska is MKV, para 003]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Soroushian to incorporate the Matroska container files in the invention of Amini for the purpose of providing a MKV container for distributing high-definition downloadable content on the internet and peer-to-peer networks (Soroushian, para 0003). Schnell teaches a DRMinfo element identifying the protected encoded element and using an encryption key from the set of encryption keys used to access the encrypted encoded content (file header object 218 [DRM header element] has the DRM licenses for the protected media content, para 0036; tracks objects 22 which has the track attributes and segment data to identify the content, para 0037).Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Schnell to incorporate the DRM elements in the invention of Amini for the purpose of seamlessly rendering all of the segments of a movie, without managing a multitude of DRM licenses for the different versions of the median content segments (Schnell, para 0036).

Regarding claims 13 and 26, Amini lacks the teaching wherein the encoding application further configures the processor to: generate an index for each Matroska container file during the encoding of each of the streams of protected content; and write a Cues element containing the index to the indexed Matroska container file. Soroushian teaches wherein the content is stored as chunks or elements in a Matroska container (MKV container composed of lists, chunks and/or elements, para 0031, see fig. 1c [Matroska is MKV, para 003]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Soroushian to incorporate the Matroska container files in the invention of Amini for the purpose of providing a MKV container for distributing high-definition downloadable content on the internet and peer-to-peer networks (Soroushian, para 0003). Schnell teaches an index for each content field for the streams of protected content (file index 158 for each file and the corresponding segments, para 0031, see fig. 2); and write a Cues element containing the index to the indexed file (track objects 222 has the attributes and information included in a track [Cues element], para 0036, 0037, see fig. 2 and includes size, type, mode ID, index, Algorithm ID with index, para 0041 and table under it).Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Schnell to incorporate the DRM elements in the invention of Amini for the purpose of seamlessly rendering all of the segments of a movie, without managing a multitude of DRM licenses for the different versions of the median content segments (Schnell, para 0036).

Claims 34, 35, 41-46, 54, 55, 59-66 lack an inventive step under PCT Article 33(3) as being obvious over Thorwirth and in view of Schnell and further in view of Amini and even further in view of Soroushian.

Regarding claim 34, Thorwirth lacks the teaching wherein the plurality of container files are Matroska container files. Soroushian teaches wherein the content is stored as chunks or elements in a Matroska container (MKV container composed of lists, chunks and/or elements, para 0031, see fig. 1c [Matroska is MKV, para 003]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Soroushian to incorporate the Matroska container files in the invention of Thorwirth for the purpose of providing a MKV container for distributing high-definition downloadable content on the internet and peer-to-peer networks (Soroushian, para 0003).

Regarding claim 35, Thorwirth teaches wherein: a set of encryption keys for each chunk of content (the chunks are protected using different watermark payloads, para 0052) and encrypt the set of encryption keys using one encryption key (the content keys used to encrypt the content are encrypted using a key unique to a specific user or client device, para 0058). However, Thorwirth lacks the teaching of common cryptographic information. Amini teaches a content distribution with common cryptographic information for the alternate streams of content (multi-encoder 220 generates multiple encoded access units and gives alternate or multiple streams, para 0031, see fig. 2; same key is used for different streams, para 0054, 0044 [protecting the content]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Amini to incorporate the common cryptographic information in the invention of Thorwirth for the purpose of encrypting and protecting the alternate streams of source content and allowing random access and joining a broadcasted multimedia stream at a point somewhere other than at the beginning of the stream (Amini, para 0041, 0054).

Regarding claim 41, Thorwirth lacks the teaching wherein the container files are Matroska container files. Soroushian is in the field of playback and distribution systems (abstract) and further teaches wherein the content is stored as chunks or elements in a Matroska container (MKV container composed of lists, chunks and/or elements, para 0031, see fig. 1c [Matroska is MKV, para 003]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Soroushian to incorporate the Matroska container files in the invention of Thorwirth for the purpose of providing a MKV container for distributing high-definition downloadable content on the internet and peer-to-peer networks (Soroushian, para 0003).

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1004
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2011/068278

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:

Regarding claim 42, Thorwirth lacks the teaching wherein the source encoder is configured to write a DRMHeader element to a TracksData element in a Tracks element within each of the Matroska container files, where the DRMHeader element includes an encrypted copy of the common cryptographic information. Amini teaches wherein the encoding application configures the processor to write at least a portion of the common cryptographic information (a stream source 210 offers unencoded access units [frames] to the encoder, para 0031, see fig. 2; encryptor 240 where the streams are encrypted, para 0032, see fig. 2; same key is used for different streams [common cryptographic information], para 0054). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Amini to incorporate the common cryptographic information in the invention of Thorwirth for the purpose of encrypting and protecting the alternate streams of source content and allowing random access and joining a broadcasted multimedia stream at a point somewhere other than at the beginning of the stream (Amini, para 0041, 0064). Soroushian teaches wherein the content is stored as chunks or elements in a Matroska container (MKV container composed of lists, chunks and/or elements, para 0031, see fig. 1c [Matroska is MKV, para 003]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Soroushian to incorporate the Matroska container files in the invention of Thorwirth for the purpose of providing a MKV container for distributing high-definition downloadable content on the internet and peer-to-peer networks (Soroushian, para 0003). Schnell teaches writing a DRMHeader element to the trackDATA element in a Tracks element within each of the content files, wherein the DRMHeader element includes an encrypted copy of the cryptographic information (file header object 218 [DRM header element] has the DRM licenses for the protected media content, para 0036, written in a file segment 160, which has track objects 222 associated with the tracks or video tracks, para 0037, see fig. 2). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Schnell to incorporate the DRM elements in the invention of Thorwirth for the purpose of seamlessly rendering all of the segments of a movie, without managing a multitude of DRM licenses for the different versions of the median content segments (Schnell, para 0036).

Regarding claim 43, Thorwirth teaches wherein a set of encryption keys for each chunk of content (the chunks are protected using different watermark payloads, para 0052) and encrypt the set of encryption keys using one encryption key (the content keys used to encrypt the content are encrypted using a key unique to a specific user or client device, para 0058). However, Thorwirth lacks the teaching of common cryptographic information and write the encrypted set of encryption keys to the DRMHeader element of each of the Matroska container files. Amini teaches a content distribution with common cryptographic information for the alternate streams of content (multi-encoder 220 generates multiple encoded access units and gives alternate or multiple streams, para 0031, see fig. 2; same key is used for different streams, para 0054, 0044 [protecting the content]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Amini to incorporate the common cryptographic information in the invention of Thorwirth for the purpose of encrypting and protecting the alternate streams of source content and allowing random access and joining a broadcasted multimedia stream at a point somewhere other than at the beginning of the stream (Amini, para 0041, 0064). Soroushian teaches wherein the content is stored as chunks or elements in a Matroska container (MKV container composed of lists, chunks and/or elements, para 0031, see fig. 1c [Matroska is MKV, para 003]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Soroushian to incorporate the Matroska container files in the invention of Thorwirth for the purpose of providing a MKV container for distributing high-definition downloadable content on the internet and peer-to-peer networks (Soroushian, para 0003). Further, Schnell teaches writing encrypted set of encryption keys to the DRMHeader element (file header object 218 [DRM header element] has the DRM licenses for the protected media content, para 0036). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Schnell to incorporate the DRM elements in the invention of Thorwirth for the purpose of seamlessly rendering all of the segments of a movie, without managing a multitude of DRM licenses for the different versions of the median content segments (Schnell, para 0036).

Regarding claim 44, Thorwirth wherein: the source content includes a stream of video (content ingested on server 301 part of a content distribution network, para 0052 [video]), and configured to: encode a frame from the stream of video (CDN stores six alternative chunks created for each section with different encoding parameters and two different watermark payloads [alternative streams of protected content], para 0052), protect the encoded frame of video by encrypting at least a portion of the encoded frame of video (the chunks are protected using different watermark payloads, para 0052), but lacks the teaching wherein to write a BlockGroup element to a Matroska container file including a DRMInfo element identifying the at least one portion of the encoded frame of video that is encrypted and at least one encryption key from the set of encryption keys used to access the at least one encrypted portion of the encoded frame of video. Soroushian teaches wherein the content is stored as chunks or elements in a Matroska container (MKV container composed of lists, chunks and/or elements, para 0031, see fig. 1c [Matroska is MKV, para 003]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Soroushian to incorporate the Matroska container files in the invention of Thorwirth for the purpose of providing a MKV container for distributing high-definition downloadable content on the internet and peer-to-peer networks (Soroushian, para 0003). Schnell teaches a DRMInfo element identifying the protected encoded element and using an encryption key from the set of encryption keys used to access the encrypted encoded content (file header object 218 [DRM header element] has the DRM licenses for the protected media content, para 0036; tracks objects 22 which has the track attributes and segment data to identify the content, para 0037).Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Schnell to incorporate the DRM elements in the invention of Thorwirth for the purpose of seamlessly rendering all of the segments of a movie, without managing a multitude of DRM licenses for the different versions of the median content segments (Schnell, para 0036).

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1005
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:

Regarding claim 45, Thorwirth lacks the teaching wherein the source encoder is configured to: generate an index for each Matroska container file during the encoding of each of the streams of protected content; and write a Cues element containing the index to the indexed Matroska container file. Soroushian teaches wherein the content is stored as chunks or elements in a Matroska container (MKV container composed of lists, chunks and/or elements, para 0031, see fig. 1c [Matroska is MKV, para 003]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Soroushian to incorporate the Matroska container files in the invention of Thorwirth for the purpose of providing a MKV container for distributing high-definition downloadable content on the internet and peer-to-peer networks (Soroushian, para 0003). Schnell teaches an index for each content field for the streams of protected content (file index 158 for each file and the corresponding segments, para 0031, see fig. 2); and write a Cues element containing the index to the indexed file (track objects 222 has the attributes and information included in a track [Cues element], para 0036, 0037, see fig. 2 and includes size, type, mode ID, index, Algorithm ID with index, para 0041 and table under it).Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Schnell to incorporate the DRM elements in the invention of Thorwirth for the purpose of seamlessly rendering all of the segments of a movie, without managing a multitude of DRM licenses for the different versions of the median content segments (Schnell, para 0036).

Regarding claim 46, Thorwirth lacks the teaching wherein the container files are Matroska container files. Soroushian is in the field of playback and distribution systems (abstract) and further teaches wherein the content is stored as chunks or elements in a Matroska container (MKV container composed of lists, chunks and/or elements, para 0031, see fig. 1c [Matroska is MKV, para 003]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Soroushian to incorporate the Matroska container files in the invention of Thorwirth for the purpose of providing a MKV container for distributing high-definition downloadable content on the internet and peer-to-peer networks (Soroushian, para 0003).

Regarding claim 47, Thorwirth lacks the teaching wherein the source encoder is configured to write a DRMHeader element to a TracksData element in a Tracks element within each of the Matroska container files, where the DRMHeader element includes an encrypted copy of the common cryptographic information. Amini teaches wherein the encoding application configures the processor to write at least a portion of the common cryptographic information (a stream source 210 offers unencoded access units [frames] to the encoder, para 0031, see fig. 2; encryption 240 where the streams are encrypted, para 0032, see fig. 2; same key is used for different streams [common cryptographic information], para 0054). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Amini to incorporate the common cryptographic information in the invention of Thorwirth for the purpose of encrypting and protecting the alternate streams of source content and allowing random access and joining a broadcasted multimedia stream at a point somewhere other than at the beginning of the stream (Amini, para 0041, 0054). Soroushian teaches wherein the content is stored as chunks or elements in a Matroska container (MKV container composed of lists, chunks and/or elements, para 0031, see fig. 1c [Matroska is MKV, para 003]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Soroushian to incorporate the Matroska container files in the invention of Thorwirth for the purpose of providing a MKV container for distributing high-definition downloadable content on the internet and peer-to-peer networks (Soroushian, para 0003). Schnell teaches writing a DRMHeader element to the tracksDATA element in a Tracks element within each of the content files, wherein the DRMHeader element includes an encrypted copy of the cryptographic information (file header object 218 [DRM header element] has the DRM licenses for the protected media content, para 0036, written in a file segment 160, which has track objects 222 associated with the tracks or video tracks, para 0037, see fig. 2). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Schnell to incorporate the DRM elements in the invention of Thorwirth for the purpose of seamlessly rendering all of the segments of a movie, without managing a multitude of DRM licenses for the different versions of the median content segments (Schnell, para 0036).

Regarding claim 48, Thorwirth teaches wherein a set of encryption keys for each chunk of content (the chunks are protected using different watermark payloads, para 0052) and encrypt the set of encryption keys using one encryption key (the content keys used to encrypt the content are encrypted using a key unique to a specific user or client device, para 0058). However, Thorwirth lacks the teaching of common cryptographic information. Amini teaches a content distribution with common cryptographic information for the alternate streams of content (multi-encoder 220 generates multiple encoded access units and gives alternate or multiple streams, para 0031, see fig. 2; same key is used for different streams, para 0054, 0044 [protecting the content]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Amini to incorporate the common cryptographic information in the invention of Thorwirth for the purpose of encrypting and protecting the alternate streams of source content and allowing random access and joining a broadcasted multimedia stream at a point somewhere other than at the beginning of the stream (Amini, para 0041, 0054).

Regarding claim 54, Thorwirth lacks the teaching wherein the plurality of container files are Matroska container files. Soroushian teaches wherein the content is stored as chunks or elements in a Matroska container (MKV container composed of lists, chunks and/or elements, para 0031, see fig. 1c [Matroska is MKV, para 003]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Soroushian to incorporate the Matroska container files in the invention of Thorwirth for the purpose of providing a MKV container for distributing high-definition downloadable content on the internet and peer-to-peer networks (Soroushian, para 0003).

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2011/068276

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

Regarding claim 55, Thorwirth teaches wherein: a set of encryption keys for each chunk of content (the chunks are protected using different watermark payloads, para 0052) and encrypt the set of encryption keys using one encryption key (the content keys used to encrypt the content are encrypted using a key unique to a specific user or client device, para 0058). However, Thorwirth lacks the teaching of common cryptographic information. Amini teaches a content distribution with common cryptographic information for the alternate streams of content (multi-encoder 220 generates multiple encoded access units and gives alternate or multiple streams, para 0031, see fig. 2; same key is used for different streams, para 0054, 0044 [protecting the content]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Amini to incorporate the common cryptographic information in the invention of Thorwirth for the purpose of encrypting and protecting the alternate streams of source content and allowing random access and joining a broadcasted multimedia stream at a point somewhere other than at the beginning of the stream (Amini, para 0041, 0054)

Regarding claim 59, Thorwirth lacks the teaching wherein the container files are Matroska container files. Soroushian is in the field of playback and distribution systems (abstract) and further teaches wherein the content is stored as chunks or elements in a Matroska container (MKV container composed of lists, chunks and/or elements, para 0031, see fig. 1c [Matroska is MKV, para 003]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Soroushian to incorporate the Matroska container files in the invention of Thorwirth for the purpose of providing a MKV container for distributing high-definition downloadable content on the internet and peer-to-peer networks (Soroushian, para 0003)

Regarding claim 60, Thorwirth lacks the teaching wherein the source encoder is configured to write a DRMHeader element to a TracksData element in a Tracks element within each of the Matroska container files, where the DRMHeader element includes an encrypted copy of the common cryptographic information. Amini teaches wherein the encoding application configures the processor to write at least a portion of the common cryptographic information (a stream source 210 offers unencoded access units (frames) to the encoder, para 0031, see fig. 2; encryptor 240 where the streams are encrypted, para 0032, see fig. 2; same key is used for different streams [common cryptographic information], para 0054). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Amini to incorporate the common cryptographic information in the invention of Thorwirth for the purpose of encrypting and protecting the alternate streams of source content and allowing random access and joining a broadcasted multimedia stream at a point somewhere other than at the beginning of the stream (Amini, para 0041, 0054). Soroushian teaches wherein the content is stored as chunks or elements in a Matroska container (MKV container composed of lists, chunks and/or elements, para 0031, see fig. 1c [Matroska is MKV, para 003]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Soroushian to incorporate the Matroska container files in the invention of Thorwirth for the purpose of providing a MKV container for distributing high-definition downloadable content on the internet and peer-to-peer networks (Soroushian, para 0003). Schnell teaches writing a DRMHeader element to the tracksDATA element in a Tracks element within each of the content files, wherein the DRMHeader element includes an encrypted copy of the cryptographic information (file header object 218 [DRM header element] has the DRM licenses for the protected media content, para 0036, written in a file segment 160, which has track objects 222 associated with the tracks or video tracks, para 0037, see fig. 2). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Schnell to incorporate the DRM elements in the invention of Thorwirth for the purpose of seamlessly rendering all of the segments of a movie, without managing a multitude of DRM licenses for the different versions of the median content segments (Schnell, para 0036)

Regarding claim 61, Thorwirth teaches wherein: a set of encryption keys for each chunk of content (the chunks are protected using different watermark payloads, para 0052) and encrypt the set of encryption keys using one encryption key (the content keys used to encrypt the content are encrypted using a key unique to a specific user or client device, para 0058). However, Thorwirth lacks the teaching of common cryptographic information and write the encrypted set of encryption keys to the DRMHeader element of each of the Matroska container files. Amini teaches a content distribution with common cryptographic information for the alternate streams of content (multi-encoder 220 generates multiple encoded access units and gives alternate or multiple streams, para 0031, see fig. 2; same key is used for different streams, para 0054, 0044 [protecting the content]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Amini to incorporate the common cryptographic information in the invention of Thorwirth for the purpose of encrypting and protecting the alternate streams of source content and allowing random access and joining a broadcasted multimedia stream at a point somewhere other than at the beginning of the stream (Amini, para 0041, 0054). Soroushian teaches wherein the content is stored as chunks or elements in a Matroska container (MKV container composed of lists, chunks and/or elements, para 0031, see fig. 1c [Matroska is MKV, para 003]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Soroushian to incorporate the Matroska container files in the invention of Thorwirth for the purpose of providing a MKV container for distributing high-definition downloadable content on the internet and peer-to-peer networks (Soroushian, para 0003). Further, Schnell teaches writing encrypted set of encryption keys to the DRMHeader element (file header object 218 [DRM header element] has the DRM licenses for the protected media content, para 0036). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Schnell to incorporate the DRM elements in the invention of Thorwirth for the purpose of seamlessly rendering all of the segments of a movie, without managing a multitude of DRM licenses for the different versions of the median content segments (Schnell, para 0036).

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1007
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2011/068276

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

Regarding claim 62, Thorwirth wherein the source content includes a stream of video (content ingested on server 301 part of a content distribution network, para 0052 [video]); and configured to: encode a frame from the stream of video (CDN stores six alternative chunks created for each section with different encoding parameters and two different watermark payloads [alternative streams of protected content], para 0052), protect the encoded frame of video by encrypting at least a portion of the encoded frame of video (the chunks are protected using different watermark payloads, para 0052), but lacks the teaching wherein to write a BlockGroup element to a Matroska container file including a DRMInfo element identifying the at least one portion of the encoded frame of video that is encrypted and at least one encryption key from the set of encryption keys used to access the at least one encrypted portion of the encoded frame of video. Soroushian teaches wherein the content is stored as chunks or elements in a Matroska container (MKV container composed of lists, chunks and/or elements, para 0031, see fig. 1c [Matroska is MKV, para 003]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Soroushian to incorporate the Matroska container files in the invention of Thorwirth for the purpose of providing a MKV container for distributing high-definition downloadable content on the internet and peer-to-peer networks (Soroushian, para 0003). Schnell teaches a DRMInfo element identifying the protected encoded element and using an encryption key from the set of encryption keys used to access the encrypted encoded content (file header object 218 [DRM header element] has the DRM licenses for the protected media content, para 0036, tracks objects 22 which has the track attributes and segment data to identify the content, para 0037) Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Schnell to incorporate the DRM elements in the invention of Thorwirth for the purpose of seamlessly rendering all of the segments of a movie, without managing a multitude of DRM licenses for the different versions of the median content segments (Schnell, para 0036).

Regarding claim 63, Thorwirth lacks the teaching wherein the source encoder is configured to: generate an index for each Matroska container file during the encoding of each of the streams of protected content; and write a Cues element containing the index to the indexed Matroska container file. Soroushian teaches wherein the content is stored as chunks or elements in a Matroska container (MKV container composed of lists, chunks and/or elements, para 0031, see fig. 1c [Matroska is MKV, para 003]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Soroushian to incorporate the Matroska container files in the invention of Thorwirth for the purpose of providing a MKV container for distributing high-definition downloadable content on the internet and peer-to-peer networks (Soroushian, para 0003). Schnell teaches an index for each content field for the streams of protected content (file index 158 for each file and the corresponding segments, para 0031, see fig. 2), and write a Cues element containing the index to the indexed file (track objects 222 has the attributes and information included in a track [Cues element], para 0036, 0037, see fig. 2 and includes size, type, mode ID, index, Algorithm ID with index, para 0041 and table under it) Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Schnell to incorporate the DRM elements in the invention of Thorwirth for the purpose of seamlessly rendering all of the segments of a movie, without managing a multitude of DRM licenses for the different versions of the median content segments (Schnell, para 0036).

Regarding claim 64, Thorwirth lacks the teaching wherein the container files are Matroska container files. Soroushian is in the field of playback and distribution systems (abstract) and further teaches wherein the content is stored as chunks or elements in a Matroska container (MKV container composed of lists, chunks and/or elements, para 0031, see fig. 1c [Matroska is MKV, para 003]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Soroushian to incorporate the Matroska container files in the invention of Thorwirth for the purpose of providing a MKV container for distributing high-definition downloadable content on the internet and peer-to-peer networks (Soroushian, para 0003).

Regarding claim 65, Thorwirth lacks the teaching wherein the source encoder is configured to write a DRMHeader element to a TracksData element in a Tracks element within each of the Matroska container files, where the DRMHeader element includes an encrypted copy of the common cryptographic information. Amini teaches wherein the encoding application configures the processor to write at least a portion of the common cryptographic information (a stream source 210 offers unencoded access units [frames] to the encoder, para 0031, see fig. 2; encryptor 240 where the streams are encrypted, para 0032, see fig. 2; same key is used for different streams [common cryptographic information], para 0054). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Amini to incorporate the common cryptographic information in the invention of Thorwirth for the purpose of encrypting and protecting the alternate streams of source content and allowing random access and joining a broadcasted multimedia stream at a point somewhere other than at the beginning of the stream (Amini, para 0041, 0054). Soroushian teaches wherein the content is stored as chunks or elements in a Matroska container (MKV container composed of lists, chunks and/or elements, para 0031, see fig. 1c [Matroska is MKV, para 003]) Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Soroushian to incorporate the Matroska container files in the invention of Thorwirth for the purpose of providing a MKV container for distributing high-definition downloadable content on the internet and peer-to-peer networks (Soroushian, para 0003). Schnell teaches writing a DRMHeader element to the tracksDATA element in a Tracks element within each of the content files, wherein the DRMHeader element includes an encrypted copy of the cryptographic information (file header object 218 [DRM header element] has the DRM licenses for the protected media content, para 0036, written in a file segment 160, which has track objects 222 associated with the tracks or video tracks, para 0037, see fig. 2). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Schnell to incorporate the DRM elements in the invention of Thorwirth for the purpose of seamlessly rendering all of the segments of a movie, without managing a multitude of DRM licenses for the different versions of the median content segments (Schnell, para 0036).

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1008
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

Regarding claim 66, Thorwirth teaches wherein a set of encryption keys for each chunk of content (the chunks are protected using different watermark payloads, para 0052) and encrypt the set of encryption keys using one encryption key (the content keys used to encrypt the content are encrypted using a key unique to a specific user or client device, para 0058). However, Thorwirth lacks the teaching of common cryptographic information. Amini teaches a content distribution with common cryptographic information for the alternate streams of content (multi-encoder 220 generates multiple encoded access units and gives alternate or multiple streams, para 0031, see fig. 2; same key is used for different streams, para 0054, 0044 (protecting the content)). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Amini to incorporate the common cryptographic information in the invention of Thorwirth for the purpose of encrypting and protecting the alternate streams of source content and allowing random access and joining a broadcasted multimedia stream at a point somewhere other than at the beginning of the stream (Amini, para 0041, 0054).

Claims 70-74, 87-93 lack an inventive step under PCT Article 33(3) as being obvious over Thorwirth and in view of Amini and Schnell.

Regarding claims 70 and 87, Thorwirth lacks the teaching wherein the container files containing each of the alternative streams of protected content comprise at least one header including the common cryptographic information and information that describes the encoding of the stream of protected content; and the top level index file identifies the location of the at least one header within each container file. However, Thorwirth shows how well known in the art are container files (sections of files in a container file, para 0004, different media containers for adaptive streaming, para 0009 (background)) and a top level index file identifies a container file containing each of the alternative streams (top level index file pointing to a number of alternate streams that contain actual video and audio data, para 0009). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Thorwirth to incorporate the container file and top level index file in the invention for the purpose of providing a playlist with a list of URLS pointing to TS container files that contain alternative chunks for the sections of a piece of content (Thorwirth, para 0010). Further, Schnell teaches one header including the cryptographic information and information that describes the encoding of the stream of the protected content and identifies the location of one header within each container file (file header object 216 [DRM header element] has the DRM licenses for the protected media content, para 0036, written in a file segment 160, which has track objects 222 associated with the tracks or video tracks, para 0037, see fig. 2) Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Schnell to incorporate the DRM system in the invention of Thorwirth for the purpose of providing DRM associated features such as licenses that correspond to the media segments of the protected media (Schnell, para 0004). Further, Amini teaches a content distribution with common cryptographic information for the alternate streams of content (multi-encoder 220 generates multiple encoded access units and gives alternate or multiple streams, para 0031, see fig. 2; same key is used for different streams, para 0054, 0044 (protecting the content)).

Regarding claims 71 and 88, Thorwirth teaches wherein cryptographic information is a set of encryption keys (the chunks are protected using different watermark payloads, para 0052). However, Thorwirth lacks the teaching of common cryptographic information. Amini teaches a content distribution with common cryptographic information for the alternate streams of content (multi-encoder 220 generates multiple encoded access units and gives alternate or multiple streams, para 0031, see fig. 2; same key is used for different streams, para 0054, 0044 (protecting the content)). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Amini to incorporate the common cryptographic information in the invention of Thorwirth for the purpose of encrypting and protecting the alternate streams of source content and allowing random access and joining a broadcasted multimedia stream at a point somewhere other than at the beginning of the stream (Amini, para 0041, 0054).

Regarding claim 72, Thorwirth teaches wherein set of encryption keys is encrypted (the content keys used to encrypt the content are encrypted using a key unique to a specific user or client device, para 0058); and the client application configures the processor to securely receive cryptographic information used to unencrypt the set of encryption keys (the content keys used to encrypt the content are encrypted using a key unique to a specific user or client device, para 0058). However, Thorwirth lacks the teaching of common cryptographic information. Amini teaches a content distribution with common cryptographic information for the alternate streams of content (multi-encoder 220 generates multiple encoded access units and gives alternate or multiple streams, para 0031, see fig. 2; same key is used for different streams, para 0054, 0044 (protecting the content)). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Amini to incorporate the common cryptographic information in the invention of Thorwirth for the purpose of encrypting and protecting the alternate streams of source content and allowing random access and joining a broadcasted multimedia stream at a point somewhere other than at the beginning of the stream (Amini, para 0041, 0054).

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1009
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2011/068276

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:

Regarding claims 73 and 92, Thorwirth lacks the teaching wherein the client application configures the processor to obtain the common cryptographic information by requesting at least one header of a container file identified in the top level index file. However, Thorwirth shows how well known in the art are container files (sections of files in a container file, para 0004, different media containers for adaptive streaming, para 0009 [background]) and a top level index file identifies a container file containing each of the alternative streams (top level index file pointing to a number of alternate streams that contain actual video and audio data, para 0009). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Thorwirth to incorporate the container file and top level index file in the invention for the purpose of providing a playlist with a list of URLS pointing to TS container files that contain alternative chunks for the sections of a piece of content (Thorwirth, para 0010). Further, Schnell teaches one header including the cryptographic information and information that describes the encoding of the stream of the protected content and identifies the location of one header within each container file (file header object 218 [DRM header element] has the DRM licenses for the protected media content, para 0036, written in a file segment 160, which has track objects 222 associated with the tracks or video tracks, para 0037, see fig. 2). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Schnell to incorporate the DRM system in the invention of Thorwirth for the purpose of providing DRM associated features such as licenses that correspond to the media segments of the protected media (Schnell, para 0004). Further, Amini teaches a content distribution with common cryptographic information for the alternate streams of content (multi-encoder 220 generates multiple encoded access units and gives alternate or multiple streams, para 0031, see fig. 2; same key is used for different streams, para 0054, 0044 [protecting the content]).

Regarding claims 74 and 93, Thorwirth lacks the teaching wherein: each container file containing one of the alternative streams of protected content further comprises an index; and the client application configures the processor to request a portion of content from one of the container files by configuring the processor to: request at least a portion of an index from the container file; identify the portion of the container file containing a specific portion of content using the index; and request the identified portion of the container file. However, Thorwirth shows how well known in the art are container files (sections of files in a container file, para 0004, different media containers for adaptive streaming, para 0009 [background]) and a top level index file identifies a container file containing each of the alternative streams (top level index file pointing to a number of alternate streams that contain actual video and audio data, para 0009), request a portion of content from one of the container files (client device authenticated requests access to choose content choice for playback, para 0053); identify the portion of the container file containing a specific portion of content (link has a part that identifies the chunk to be accessed [part that identifies the chunk is the title with a unique identifier, para 0057]); and request the identified portion of the container file (server provides access to the client based on the selection or chunks requested, para 0050). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Thorwirth to incorporate the container file and top level index file in the invention for the purpose of providing a playlist with a list of URLS pointing to TS container files that contain alternative chunks for the sections of a piece of content (Thorwirth, para 0010). Further, Schnell teaches one header including the cryptographic information and information that describes the encoding of the stream of the protected content and identifies the location of one header within each container file (file header object 218 [DRM header element] has the DRM licenses for the protected media content, para 0036, written in a file segment 160, which has track objects 222 associated with the tracks or video tracks, para 0037, see fig. 2) Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Schnell to incorporate the DRM system in the invention of Thorwirth for the purpose of providing DRM associated features such as licenses that correspond to the media segments of the protected media (Schnell, para 0004).

Regarding claim 88, Thorwirth teaches wherein: the set of encryption keys is encrypted so that it is accessible using cryptographic information obtained by the playback device (the content keys used to encrypt the content are encrypted using a key unique to a specific user or client device, para 0058); and the method further comprising obtaining cryptographic information using the playback device (a copy of the encryption key used for the encryption of the content key is delivered securely to the specific user or client device, para 0058, hashing or encrypting the encrypted content and key, para 0064).

Regarding claim 90, Thorwirth teaches wherein the set of encryption keys is encrypted using at least one encryption key (the content keys used to encrypt the content are encrypted using a key unique to a specific user or client device, para 0058); and the playback device securely obtains the at least one encryption key (copy of the encryption key used for the encryption of the content key is delivered securely to the specific user or client device, para 0058, hashing or encrypting the encrypted content and key, para 0064).

Regarding claim 91, Thorwirth lacks the teaching wherein the at least one encryption key is encrypted using at least one encryption key included in the cryptographic information bound to the playback device. However, Thorwirth teaches wherein the set of encryption keys is encrypted using at least one encryption key (the content keys used to encrypt the content are encrypted using a key unique to a specific user or client device, para 0058); and the playback device securely obtains the at least one encryption key (copy of the encryption key used for the encryption of the content key is delivered securely to the specific user or client device, para 0058, hashing or encrypting the encrypted content and key, para 0064). Furthermore, defining multiple encryptions is well known in the art and the specifics would have been a matter of design choice. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Thorwirth to incorporate the encryption features in the invention for the purpose of providing protection against unauthorized used and distribution of content (Thorwirth, para 0058).

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1010
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2011/068276

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

Claims 68, 75-83, 85, 94-102, 104 lack an inventive step under PCT Article 33(3) as being obvious over Thorwirth and in view of Amini and further in view of Schnell and further in view of Soroushian.

Regarding claims 68 and 85, Thorwirth teaches wherein the alternative streams of protected content are alternative streams of protected video (CDN stores six alternative chunks [video] created for each section with different encoding parameters and two different watermark payloads [alternative streams of protected content], para 0052); each of the alternative streams of protected video includes information indicating portions of frames of video that are encrypted and identifying at least a portion of the cryptographic information used to access the encrypted portions of the frames of video (CDN stores six alternative chunks created for each section with different encoding parameters and two different watermark payloads [alternative streams of protected content], para 0052; link has a part that identifies the chunk to be accessed [part that identifies the chunk is the title with a unique identifier, para 0057]); and the client application configures the processor to: obtain a protected frame of video from one of the alternative streams of protected video (client device authenticated requests access to choose content choice for playback, para 0053; link has a part that identifies the chunk to be accessed [part that identifies the chunk is the title with a unique identifier, para 0057]); obtain information indicating a portion of the protected frame of video that is encrypted (the chunks are protected using different watermark payloads, para 0052; link has a part that identifies the chunk to be accessed [part that identifies the chunk is the title with a unique identifier, para 0057]); identify at least a portion of the cryptographic information that is used to access the encrypted portion of the protected frame using the information (a copy of the encryption key used for the encryption of the content key is delivered securely to the specific user or client device [this encryption key identifies the encrypted content to be sent], para 0058, hashing or encrypting the encrypted content and key, para 0064); decrypt the encrypted portion of the protected frame of video using the identified portion of the common cryptographic information (decryption of streamed file utilizes the content keys based on the sections, para 0059). Thorwirth lacks the teaching of common cryptographic information and a DRM server and decoding the frames of video. Schnell teaches a content distributor with a DRM system (content server 122 and a DRM system 118 distribute protected media content 120 to various wireless media devices 106, para 0028-0031). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Schnell to incorporate the DRM system in the invention of Thorwirth for the purpose of providing DRM associated features such as licenses that correspond to the media segments of the protected media (Schnell, para 0004). Further, Amini teaches a content distribution with common cryptographic information for the alternate streams of content (multi-encoder 220 generates multiple encoded access units and gives alternate or multiple streams, para 0031, see fig. 2; same key is used for different streams, para 0054, 0044 [protecting the content]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Amini to incorporate the common cryptographic information in the invention of Thorwirth for the purpose of encrypting and protecting the alternate streams of source content and allowing random access and joining a broadcasted multimedia stream at a point somewhere other than at the beginning of the stream (Amini, para 0041, 0054). Furthermore, Soroushian teaches a playback can identify and decode the data (decode the appropriate data, para 0037). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Soroushian to incorporate the decoder in the invention of Thorwirth for the purpose of decoding multimedia and present audio, video and subtitle information in a synchronized manner (Soroushian, para 0003).

Regarding claims 75 and 94, Thorwirth lacks the teaching wherein the plurality of container files are Matroska container files. Soroushian teaches wherein the content is stored as chunks or elements in a Matroska container (MKV container composed of lists, chunks and/or elements, para 0031, see fig. 1c [Matroska is MKV, para 003]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Soroushian to incorporate the Matroska container files in the invention of Thorwirth for the purpose of providing a MKV container for distributing high-definition downloadable content on the internet and peer-to-peer networks (Soroushian, para 0003).
Regarding claims 76 and 95, Thorwirth lacks the teaching wherein the common cryptographic information is stored in a common DRM Header element contained within a Tracks element within each of the Matroska container files containing the alternative streams of protected content. Amini teaches wherein the encoding application configures the processor to write at least a portion of the common cryptographic information (a stream source 210 offers unencoded access units [frames] to the encoder, para 0031, see fig. 2; encryptor 240 where the streams are encrypted, para 0032, see fig. 2; same key is used for different streams [common cryptographic information], para 0054). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Amini to incorporate the common cryptographic information in the invention of Thorwirth for the purpose of encrypting and protecting the alternate streams of source content and allowing random access and joining a broadcasted multimedia stream at a point somewhere other than at the beginning of the stream (Amini, para 0041, 0054). Soroushian teaches wherein the content is stored as chunks or elements in a Matroska container (MKV container composed of lists, chunks and/or elements, para 0031, see fig. 1c [Matroska is MKV, para 003]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Soroushian to incorporate the Matroska container files in the invention of Thorwirth for the purpose of providing a MKV container for distributing high-definition downloadable content on the internet and peer-to-peer networks (Soroushian, para 0003). Schnell teaches writing a DRMHeader element to the tracksDATA element in a Tracks element within each of the content files, wherein the DRMHeader element includes an encrypted copy of the cryptographic information (file header object 218 [DRM header element] has the DRM licenses for the protected media content, para 0036, written in a file segment 160, which has track objects 222 associated with the tracks or video tracks, para 0037, see fig. 2). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Schnell to incorporate the DRM elements in the invention of Thorwirth for the purpose of seamlessly rendering all of the segments of a movie, without managing a multitude of DRM licenses for the different versions of the median content segments (Schnell, para 0036).

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1011
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2011/066276

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

Regarding claims 77 and 96, Thorwirth teaches wherein: a set of encryption keys for each chunk of content (the chunks are protected using different watermark payloads, para 0052) and encrypt the set of encryption keys using one encryption key (the content keys used to encrypt the content are encrypted using a key unique to a specific user or client device, para 0056). However, Thorwirth lacks the teaching of common cryptographic information and write the encrypted set of encryption keys to the DRMHeader element. Amini teaches a content distribution with common cryptographic information for the alternate streams of content (multi-encoder 220 generates multiple encoded access units and gives alternate or multiple streams, para 0031, see fig. 2; same key is used for different streams, para 0054, 0044 [protecting the content]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Amini to incorporate the common cryptographic information in the invention of Thorwirth for the purpose of encrypting and protecting the alternate streams of source content and allowing random access and joining a broadcasted multimedia stream at a point somewhere other than at the beginning of the stream (Amini, para 0041, 0054). Schnell teaches writing encrypted set of encryption keys to the DRMHeader element (file header object 218 [DRM header element] has the DRM licenses for the protected media content, para 0036). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Schnell to incorporate the DRM elements in the invention of Thorwirth for the purpose of seamlessly rendering all of the segments of a movie, without managing a multitude of DRM licenses for the different versions of the median content segments (Schnell, para 0036).

Regarding claims 78 and 97, Thorwirth teaches wherein set of encryption keys is encrypted (the content keys used to encrypt the content are encrypted using a key unique to a specific user or client device, para 0056); and the client application configures the processor to securely receive cryptographic information used to unencrypt the set of encryption keys (the content keys used to encrypt the content are encrypted using a key unique to a specific user or client device, para 0056). However, Thorwirth lacks the teaching of cryptographic information stored in a DRM header element. Schnell teaches writing encrypted set of encryption keys to the DRMHeader element (file header object 218 [DRM header element] has the DRM licenses for the protected media content, para 0036). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Schnell to incorporate the DRM elements in the invention of Thorwirth for the purpose of seamlessly rendering all of the segments of a movie, without managing a multitude of DRM licenses for the different versions of the median content segments (Schnell, para 0036).

Regarding claims 79 and 98, Thorwirth lacks the teaching wherein the client application configures the processor to obtain the DRM Header element by requesting a Tracks element from one of the Matroska container files identified in the top level index file. However, Thorwirth shows how well known in the art are container files (sections of files in a container file, para 0004, different media containers for adaptive streaming, para 0008 [background]) and a top level index file identifies a container file containing each of the alternative streams (top level index file pointing to a number of alternate streams that contain actual video and audio data, para 0009). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Thorwirth to incorporate the container file and top level index file in the invention for the purpose of providing a playlist with a list of URLS pointing to TS container files that contain alternative chunks for the sections of a piece of content (Thorwirth, para 0010). Soroushian teaches wherein the content is stored as chunks or elements in a Matroska container (MKV container composed of lists, chunks and/or elements, para 0031, see fig. 1c [Matroska is MKV, para 003]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Soroushian to incorporate the Matroska container files in the invention of Thorwirth for the purpose of providing a MKV container for distributing high-definition downloadable content on the internet and peer-to-peer networks (Soroushian, para 0003). Schnell teaches writing a DRMHeader element to the tracksDATA element in a Tracks element within each of the content files, wherein the DRMHeader element includes an encrypted copy of the cryptographic information (file header object 218 [DRM header element] has the DRM licenses for the protected media content, para 0036, written in a file segment 160, which has track objects 222 associated (with the tracks or video tracks, para 0037, see fig. 2). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Schnell to incorporate the DRM elements in the invention of Thorwirth for the purpose of seamlessly rendering all of the segments of a movie, without managing a multitude of DRM licenses for the different versions of the median content segments (Schnell, para 0036).

Regarding claims 80 and 99, Thorwirth lacks the teaching wherein: each Matroska container file containing an alternative stream of protected content further comprises an index contained within a Cues element; and the client application configures the processor to request a portion of content from one of the Matroska container files by configuring the processor to: request at least a portion of a Cues element from a Matroska container file containing one of the alternative streams of protected content; identify a portion of the Matroska container file containing a specific portion of content using at least one CueTrackPosition element within the Cues element; and request the portion of the Matroska container file identified by the at least one CueTrackPosition element. However, Thorwirth shows how well known in the art are container files (sections of files in a container file, para 0004, different media containers for adaptive streaming, para 0008 [background]) and a top level index file identifies a container file containing each of the alternative streams (top level index file pointing to a number of alternate streams that contain actual video and audio data, para 0009). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Thorwirth to incorporate the container file and top level index file in the invention for the purpose of providing a playlist with a list of URLS pointing to TS container files that contain alternative chunks for the sections of a piece of content (Thorwirth, para 0010).
Soroushian teaches wherein the content is stored as chunks or elements in a Matroska container (MKV container composed of lists, chunks and/or elements, para 0031, see fig. 1c [Matroska is MKV, para 003]) and identifying a portion of the MKV container using CueTrackPosition element (table with hierarchical index identifiers with CUEPOS_ID, table above para 0037). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Soroushian to incorporate the Matroska container files in the invention of Thorwirth for the purpose of providing a MKV container for distributing high-definition downloadable content on the internet and peer-to-peer networks (Soroushian, para 0003). Schnell teaches an index for each content field for the streams of protected content (file index 158 for each file and the corresponding segments, para 0031, see fig. 2), and write a Cues element containing the index to the indexed file (track objects 222 has the attributes and information included in a track [Cues element], para 0036, 0037, see fig. 2 and includes size, type, mode ID, index, Algorithm ID with index, para 0041 and table under it).Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Schnell to incorporate the DRM elements in the invention of Thorwirth for the purpose of seamlessly rendering all of the segments of a movie, without managing a multitude of DRM licenses for the different versions of the median content segments (Schnell, para 0036).

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1012
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

Regarding claims 81 and 100, Thorwirth lacks the teaching wherein the index comprises a plurality of CueTrackPosition elements that identify the location of a plurality of Cluster elements within the Matroska container file. Soroushian teaches wherein the content is stored as chunks or elements in a Matroska container (MKV container composed of lists, chunks and/or elements, para 0031, see fig. 1c [Matroska is MKV, para 003]) and identifying a portion of the MKV container using CueTrackPosition element (table with hierarchical index identifiers with CUEPOS_ID, table above para 0037). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Soroushian to incorporate the Matroska container files in the invention of Thorwirth for the purpose of providing a MKV container for distributing high-definition downloadable content on the internet and peer-to-peer networks (Soroushian, para 0003). Schnell teaches an index for each content field for the streams of protected content (file index 158 for each file and the corresponding segments [segments can be interpreted as track elements or comprising of cluster elements], para 0031, see fig. 2); and write a Cues element containing the index to the indexed file (track objects 222 has the attributes and information included in a track [Cues element], para 0036, 0037, see fig. 2 and includes size, type, mode ID, index, Algorithm ID with index, para 0041 and table under it).Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Schnell to incorporate the DRM elements in the invention of Thorwirth for the purpose of seamlessly rendering all of the segments of a movie, without managing a multitude of DRM licenses for the different versions of the median content segments (Schnell, para 0036).

Regarding claims 82 and 101, Thorwirth lacks the teaching wherein: each Cluster element contains a plurality of BlockGroup elements including encoded portions of content; a Cue Track Position element indexes each Cluster element; and each CueTrackPosition element includes the size of the Cluster element that it indexes. Schnell teaches an index for each content field for the streams of protected content (file index 158 for each file and the corresponding segments [segments can be interpreted as track elements or comprising of cluster elements], para 0031, see fig. 2); and write a Cues element containing the index to the indexed file (track objects 222 has the attributes and information included in a track [Cues element], para 0036, 0037, see fig. 2 and includes size, type, mode ID, index, Algorithm ID with index, para 0041 and table under it). Furthermore, defining the specifics of file headers and clusters would have been a matter of design choice. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Schnell to incorporate the DRM elements in the invention of Thorwirth for the purpose of seamlessly rendering all of the segments of a movie, without managing a multitude of DRM licenses for the different versions of the median content segments (Schnell, para 0036).
Regarding claims 83 and 102, Thorwirth teaches wherein the alternative streams of protected content are alternative streams of protected video (CDN stores six alternative chunks [video] created for each section with different encoding parameters and two different watermark payloads [alternative streams of protected content], para 0052); each of the alternative streams of protected video includes information indicating portions of frames of video that are encrypted and identifying at least a portion of the cryptographic information used to access the encrypted portions of the frames of video (CDN stores six alternative chunks created for each section with different encoding parameters and two different watermark payloads [alternative streams of protected content], para 0052; link has a part that identifies the chunk to be accessed [part that identifies the chunk is the title with a unique identifier, para 0057]); and the client application configures the processor to: obtain a protected frame of video from one of the alternative streams of protected video (client device authenticated requests access to choose content choice for playback, para 0053; link has a part that identifies the chunk to be accessed [part that identifies the chunk is the title with a unique identifier, para 0057]); obtain information indicating a portion of the protected frame of video that is encrypted (the chunks are protected using different watermark payloads, para 0052; link has a part that identifies the chunk to be accessed [part that identifies the chunk is the title with a unique identifier, para 0057]); identify at least a portion of the cryptographic information that is used to access the encrypted portion of the protected frame using the information (a copy of the encryption key used for the encryption of the content key is delivered securely to the specific user or client device [this encryption key identifies the encrypted content to be sent], para 0058, hashing or encrypting the encrypted content and key, para 0064); decrypt the encrypted portion of the protected frame of video using the identified portion of the common cryptographic information (decryption of streamed file utilizes the content keys based on the sections, para 0059). Thorwirth lacks the teaching of common cryptographic information, a Matroska container file and a DRM server and decoding the frames of video. Schnell teaches a content distributor with a DRM system (content server 122 and a DRM system 118 distribute protected media content 120 to various wireless media devices 106, para 0028-0031). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Schnell to incorporate the DRM system in the invention of Thorwirth for the purpose of providing DRM associated features such as licenses that correspond to the media segments of the protected media (Schnell, para 0004). Further, Amini teaches a content distribution with common cryptographic information for the alternate streams of content (multi-encoder 220 generates multiple encoded access units and gives alternate or multiple streams, para 0031, see fig. 2; same key is used for different streams, para 0054, 0044 [protecting the content]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Amini to incorporate the common cryptographic information in the invention of Thorwirth for the purpose of encrypting and protecting the alternate streams of source content and allowing random access and joining a broadcasted multimedia stream at a point somewhere other than at the beginning of the stream (Amini, para 0041, 0064). Furthermore, Soroushian teaches wherein the content is stored as chunks or elements in a Matroska container (MKV container composed of lists, chunks and/or elements, para 0031, see fig. 1c [Matroska is MKV, para 003]) and further teaches a playback can identify and decode the data (decode the appropriate data, para 0037). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Soroushian to incorporate the decoder in the invention of Thorwirth for the purpose of decoding multimedia and present audio, video and subtitle information in a synchronized manner (Soroushian, para 0006).

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1013
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2011/068276

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

Regarding claim 104, Thorwirth teaches wherein the alternative streams of protected content are alternative streams of protected video (CDN stores six alternative chunks [video] created for each section with different encoding parameters and two different watermark payloads [alternative streams of protected content], para 0052), each of the alternative streams of protected video includes information indicating portions of frames of video that are encrypted and identifying at least a portion of the cryptographic information used to access the encrypted portions of the frames of video (CDN stores six alternative chunks created for each section with different encoding parameters and two different watermark payloads [alternative streams of protected content], para 0052; link has a part that identifies the chunk to be accessed [part that identifies the chunk is the title with a unique identifier, para 0057]); and the client application configures the processor to: obtain a protected frame of video from one of the alternative streams of protected video (client device authenticated requests access to choose content choice for playback, para 0053; link has a part that identifies the chunk to be accessed [part that identifies the chunk is the title with a unique identifier, para 0057]); obtain information indicating a portion of the protected frame of video that is encrypted (the chunks are protected using different watermark payloads, para 0052; link has a part that identifies the chunk to be accessed [part that identifies the chunk is the title with a unique identifier, para 0057]); identify at least a portion of the cryptographic information that is used to access the encrypted portion of the protected frame using the information (a copy of the encryption key used for the encryption of the content key is delivered securely to the specific user or client device [this encryption key identifies the encrypted content to be sent], para 0058, hashing or encrypting the encrypted content and key, para 0064); decrypt the encrypted portion of the protected frame of video using the identified portion of the common cryptographic information (decryption of streamed file utilizes the content keys based on the sections, para 0059). Thorwirth lacks the teaching of common cryptographic information and a DRM server and decoding the frames of video. Schnell teaches a content distributor with a DRM system (content server 122 and a DRM system 118 distribute protected media content 120 to various wireless media devices 106, para 0028-0031). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Schnell to incorporate the DRM system in the invention of Thorwirth for the purpose of providing DRM associated features such as licenses that correspond to the media segments of the protected media (Schnell, para 0004). Further, Amini teaches a content distribution with common cryptographic information for the alternate streams of content (multi-encoder 220 generates multiple encoded access units and gives alternate or multiple streams, para 0031, see fig. 2; same key is used for different streams, para 0054, 0044 [protecting the content]). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Amini to incorporate the common cryptographic information in the invention of Thorwirth for the purpose of encrypting and protecting the alternate streams of source content and allowing random access and joining a broadcasted multimedia stream at a point somewhere other than at the beginning of the stream (Amini, para 0041, 0054). Furthermore, Soroushian teaches a playback can identify and decode the data (decode the appropriate data, para 0037). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Soroushian to incorporate the decoder in the invention of Thorwirth for the purpose of decoding multimedia and present audio, video and subtitle information in a synchronized manner (Soroushian, para 0003).

Claims 1-105 meet the criteria set out in PCT Article 33(4), and thus have industrial applicability because the subject matter claimed can be made or used in industry.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1014
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 August 2011 (25.08.2011)

PCT

(10) International Publication Number
WO 2011/103364 A1

(51) International Patent Classification:
G06F 21/00 (2006.01)

(21) International Application Number:
PCT/US2011/025341

(22) International Filing Date:
17 February 2011 (17.02.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/305,398 17 February 2010 (17.02.2010) US
61/333,909 12 May 2010 (12.05.2010) US

(71) Applicant *(for all designated States except US)*: **VERIMATRIX, INC.** [US/US]; 6825 Flanders Drive, San Diego, CA 92121 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **THORWIRTH, Niels** [DE/US]; 630 1/2 Diamond Street, San Diego, CA 92109 (US).

(74) Agent: **BAILEY, David, J.**; Keith, Pomeroy, Pack & Bailey LLP, 2875 Michelle Drive, Suite 110, Irvine, CA 92606 (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, TH, 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, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, 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, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

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

(54) Title: SYSTEMS AND METHODS FOR SECURING CONTENT DELIVERED USING A PLAYLIST

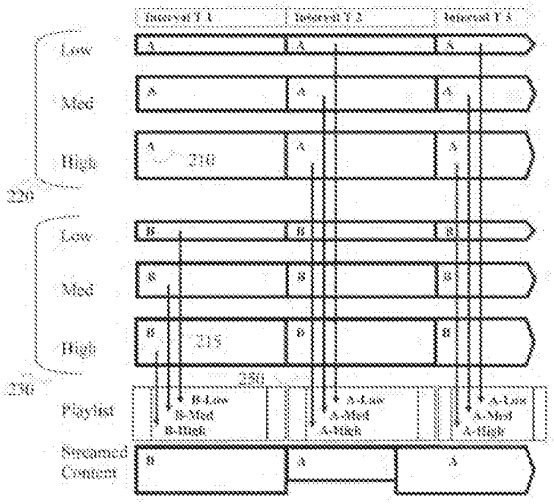


Fig. 2

(57) Abstract: Systems and methods in accordance with embodiments of the invention enhance the security of content distribution using individualized playlists. In many embodiments, a playlist is individually composed for a client device so that the selection of content included in the playlist encodes information. One embodiment includes generating a watermark sequence, where each watermark sequence is a unique identifier, selecting between alternative chunks of encoded content based upon the watermark sequence, where each of the alternative chunks of encoded content includes the same perceptual content and differs in the way it is watermarked, and listing the selected chunks in a playlist, where content assembled using the playlist includes a unique watermark sequence.

WO 2011/103364 A1

SYSTEMS AND METHODS FOR SECURING CONTENT DELIVERED USING A PLAYLIST

FIELD OF THE INVENTION

[0001] The present invention generally relates to securing digital content and more specifically relates to securing digital content accessible via a playlist using digital watermarking and encryption.

BACKGROUND

[0002] The term "content" can be used to describe digital media such as audio, video, an image, a collection of images or a combination thereof. A digital content file can include several streams of audio, video and text in different tracks. Different tracks may contain different video programs, alternative audio tracks for different languages, and/or text for subtitles. Content is typically encoded or compressed for efficient transmission and storage. Common encoding formats include MPEG-2, VC-1 and H.264 for video and mp3 (i.e. MPEG-1 Audio Layer 3), AAC and Ogg Vorbis for audio.

[0003] "Sections" are parts of a content file. Typically, they contain temporal sections (i.e. a subsection of a piece of content in time such as a number of video frames, group of pictures or audio samples). In many instances, sections contain several seconds of encoded content and the sections in a content file are of similar duration. Other variations include sections that contain the entire media file. Sections can also be created from a partition of a file including but not limited to in areas of an image or video frame, pages of a text document, channels of video in a multi channel video stream, channels of a multi channel audio stream (such as stereo, surround sound, multi language versions), channels of a stereo or 3D video, and/or groups of bytes in a bitstream.

[0004] Sections may be created by actual separation of a file into multiple files or they may be created within a file. Creation of sections within a file can be realized by creating pointers to sections or an index within a container file that allow for fast random access to individual sections. The creation of sections within a file can be further enhanced by grouping content within separate structures within the file. Sections can also be created on the fly where the section is determined just before it is requested or used.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1016
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

[0005] Chunks are sections that are prepared to be retrieved by a client via a "playlist". Typically, several alternative chunks are created from every section. These chunks contain the same perceptual content (e.g. the same 2 seconds of content in a video file). Commonly those chunks differ in their encoding and/or bitrate (e.g. in adaptive bitrate streaming systems). Different bitrates are typically created by compressing using different levels of lossy compression, and different video resolutions. Other variations to create chunks from sections include: variation in compression codecs or number of channels, video 2D/3D video, bit depth of audio samples, bit depth of video samples, additional channels for audio such as stereo surround sound channels, compression codecs that differ in decoding complexity in order to support adaption to processing performance of the playback client and DRM systems and different content that can be chosen by or targeted to an individual as is the case in targeted advertisement.

[0006] A "client device" typically is an electronic device that implements a media player. It typically retrieves content from a server via a network but may also play back content from a local storage device or physical media such as a DVD, a Blu-ray disc, other optical discs, a USB memory stick, or another storage device. Client devices can include Set Top Boxes, desktop and laptop computers, cell phones, tablet devices, game consoles, mp3 players, portable media players and other media players. The client device is interpreting the playlist and as such may reside on the head-end where the playlist is executed to assemble content according to its destination.

[0007] The term "streaming" describes the playback of content on a client device, where the content is stored on a server and continuously sent to the client device over a network during playback. Typically, the client device stores a sufficient quantity of content in a buffer at any given time during playback to prevent disruption of playback due to the playback device completing playback of all the buffered content prior to receipt of the next portion of content. The client may also store the streamed content locally for later playback. Adaptive bit rate streaming or "adaptive streaming" involves detecting the present streaming conditions (e.g. the user's network bandwidth and CPU capacity) in real time and adjusting the quality of the streamed media accordingly. Typically, the source media is encoded at multiple bit rates and the client device switches between streaming the different encodings depending on available

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1017
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

resources. Alternatively this choice may be made by the server as it evaluates the connection quality of an individual connection.

[0008] Adaptive streaming may use common protocols like the Hypertext Transfer Protocol (HTTP), published by the Internet Engineering Task Force and the World Wide Web Consortium as RFC 2616, or Real Time Streaming Protocol (RTSP), published by the Internet Engineering Task Force as RFC 2326, to stream media between a server and a playback device. HTTP is a stateless protocol that enables a playback device to request a file or a byte range within a file. HTTP is described as stateless, because the server is not required to record information concerning the state of the playback device requesting information or the byte ranges requested by the playback device in order to respond to requests received from the playback device. RTSP is a network control protocol used to control streaming media servers. Playback devices issue control commands, such as "play" and "pause", to the server streaming the media to control the playback of media files. When RTSP is utilized, the media server records the state of each client device and determines the media to stream based upon the instructions received from the client device.

[0009] In adaptive streaming systems, the source media is often organized on a media server with the help of a top level index file pointing to a number of alternate streams that contain the actual video and audio data. Different adaptive streaming solutions can utilize different index and media containers. The Synchronized Multimedia Integration Language (SMIL) developed by the World Wide Web Consortium is utilized to create indexes in several adaptive streaming solutions including IIS Smooth Streaming developed by Microsoft Corporation of Redmond, Washington, and Flash Dynamic Streaming developed by Adobe Systems Incorporated of San Jose, California. HTTP Adaptive Bitrate Streaming developed by Apple Computer Incorporated of Cupertino, California organizes media files via an extended M3U playlist file (.M3U8), which is a text file containing a list of URIs that typically identify media chunks. Today's most commonly used media container formats are the MP4container format specified in MPEG-4 Part 14 (i.e. ISO/IEC 14496-14) and the MPEG transport stream (TS) container specified in MPEG-2 Part 1 (i.e. ISO/IEC Standard 13818-1). The MP4 container format is utilized in IIS Smooth Streaming and Flash Dynamic Streaming. The TS container is used in HTTP Adaptive Bitrate Streaming.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1018
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

[0010] The term "playlist" can be used to describe a list of chunks or links to chunks for playback. A playlist may also contain a selection that allows adapting to user preferences such as playback order, language settings or bandwidth consumption or device capabilities such as 3D display, surround sound and DRM support. The M3U playlist file utilized in HTTP Adaptive Bitrate Streaming is an example of a file containing a playlist (i.e. a list of URLs pointing to TS container files that contain alternative chunks for the sections of a piece of content). A playlist can also be distributed across multiple files. For example, in IIS Smooth Streaming a list of URLs is provided as a SMIL file and each container referenced in the SMIL file contains an index. Together the SMIL top level index file and the indexes within in each of the container files can provide a complete index to all of the alternative chunks for the different sections of a piece of content. A playlist is typically used by a media player running on a client device but can also be used to assemble content in preparation for further distribution. Common formats for playlists include: M3U, RAM, Winamp B4S, Advanced Stream Redirector (ASX) with variation of ASX and WVX, WPL, PLS, Kapsule and KPL, SMIL, iTunes Library, DAAP, Creative Commons RDF and XML Shareable Playlist Format (XSPF).

[0011] A playlist is typically interpreted on the client but may also be used on the server to assemble content before final delivery to a client (e.g. Flash Dynamic Streaming). Examples where a playlist is interpreted on the server also include individual content composition for each client, or server side adaption to the available bitrate and client capabilities.

[0012] A "link" is an entry in a playlist pointing to a content file or content chunk. A link can be expressed as a URL or filename. It may point to a local or remote file and/or a location within a local or remote file. The file may be an existing file or it may be created and prepared on the fly while it is requested via the client.

[0013] A process that can be used to prepare content for use in a typical adaptive streaming system is illustrated in FIG. 1. The content is divided into temporal sections, depicted as T1, T2 and T3 (100). Each section is compressed with three different bitrates Low (131), Medium (132) and High (133). A first chunk 120 is a chunk for the low bitrate of section T3. The Low bitrate has the smallest data size and lowest quality. Consecutive chunks of different bitrates can be played consecutively without duplicated or skipped content.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1019
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

[0014] For adaptive streaming, links (160) to all three chunks of each temporal section can be provided in a playlist (150) to the client device. The client device adapts the bitrate during playback according to its playback environment by selecting the best chunk for each section. The best chunk typically is the chunk with the highest bitrate that can be played without interruption. In the example shown in Fig. 1, the content (170) streamed to the client device is composed of High, Med, High bitrate for corresponding Sections T1, T2, T3. The client device may have chosen to reduce the bitrate for section T2, because it did not have sufficient bandwidth to download the chunk with the High bitrate fast enough to play without interruption.

[0015] The term "digital watermarking" can be used to describe processes that embeds imperceptible, robust and secure information in content. One application is embedding recipient information in the content in order to identify individuals that receive the content and distribute the content in an unauthorized manner.

[0016] There are different approaches to applying digital watermarks to content files. One application is to embed the mark on the server before the content is delivered to a client device. One possibility is to mark the content "on the fly" as the file is requested from the client. For example, by using an approach as described in U.S. Patent No. 13/002,280, entitled "Efficient Watermarking Approaches of Compressed Media", filed December 30, 2010, the disclosure of which is incorporated by reference herein. Another approach is to prepare the content with different sections that are perceptually identical but contain different information and to assemble the sections during delivery in a way that represents the information to be embedded as described in U.S. Patent No. 7,555,630, entitled "Techniques for reducing the computational cost of embedding information in digital representations", filed March 17, 2003. Several watermark systems that embed information in content files and that can be applied to sections and chunks have been described in the prior art. Such systems apply noise patterns, DCT transformation or luminance variations in the content in order to embed information. An overview can be found in Cox et al., "Digital Watermarking and Steganography" (2nd Ed., 2007). The information that is embedded using a digital watermark is called the payload. It often represents a number that relates to a user, device or content owner. Transformations are typically applied to the payload for security and reliability such as encryption, error correction and/or error detection codes.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1020
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Payloads are often stored repeatedly within the content in order to enhance the robustness with an increase in redundancy.

[0017] If content is delivered using a playlist and adaptive streaming, it is not known prior to streaming what parts of the content will be accessed. If the content is prepared for each client in all available bitrates and maintained for the entire duration of possible access by the client, the resulting overhead in processing storage created is significant if not prohibitive.

SUMMARY OF THE INVENTION

[0018] Systems and methods in accordance with embodiments of the invention enhance the security of content distribution using individualized playlists. In many embodiments, a playlist is individually composed for a client device so that the selection of content included in the playlist encodes information. One embodiment includes generating a watermark sequence, where each watermark sequence is a unique identifier, selecting between alternative chunks of encoded content based upon the watermark sequence, where each of the alternative chunks of encoded content includes the same perceptual content and differs in the way it is watermarked, and listing the selected chunks in a playlist, where content assembled using the playlist includes a unique watermark sequence.

[0019] In a further embodiment, at least one of the alternative chunks includes an imperceptibly embedded watermark, and one of the alternative chunks is unmodified.

[0020] In another embodiment, each of the alternative chunks includes a different imperceptibly embedded watermark.

[0021] In a still further embodiment, each of the alternative chunks includes a different amount of embedded information.

[0022] In still another embodiment, the number of alternative chunks differs for different sections of the content.

[0023] In a yet further embodiment, selecting between alternative chunks of encoded content based upon the watermark sequence further includes selecting between alternative groups of chunks based upon the watermark sequence, where each chunk in a group of chunks includes the same perceptual content encoded using different encoding parameters and is watermarked in the same way, and alternative groups of chunks encode the same perceptual content and differ in the

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1021
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

way they are watermarked, and listing the selected chunks in the playlist further includes listing the chunks from the selected groups of chunks in the playlist.

[0024] In yet another embodiment, the selected chunks are listed in the playlist using links to the selected chunks of encoded content.

[0025] In a further embodiment again, at least one of the links is a single use link.

[0026] In another embodiment again, each single use link includes a unique token.

[0027] In a further additional embodiment, at least one of the links is a destination link.

[0028] In another additional embodiment, each destination link includes a token indicative of a client device.

[0029] A still yet further embodiment also includes inserting a playlist-bound key into the playlist.

[0030] In still yet another embodiment, selecting between alternative chunks of encoded content based upon the watermark sequence further includes selecting between chunks where each of the alternative chunks is encrypted in a different way.

[0031] In a still further embodiment again, each of the alternative chunks is encrypted using a different encryption key.

[0032] In still another embodiment again, selection between alternative chunks of encoded content is performed as the watermark sequence is generated.

[0033] A still further additional embodiment includes generating a sequence of content keys, selecting between alternative chunks of encrypted content based upon the sequence of content keys, where each of the alternative chunks of encrypted content includes the same perceptual content and is encrypted using a different content key, and listing the selected chunks in a playlist, where content assembled using the playlist requires the sequence of content keys for decryption.

[0034] In still another additional embodiment, selection between alternative chunks of encrypted content is performed as the sequence of content keys is generated.

[0035] A yet further embodiment again also includes modifying the sequence of content keys by modifying at least one of the content keys using information derived from one of the selected chunks of encrypted content.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1022
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

[0036] In yet another embodiment again, the number of alternative chunks of encrypted content differs for different sections of the content.

[0037] A yet further additional embodiment includes encoding sections of the content as alternative chunks of encoded content, where each of the alternative chunks of encoded content includes the same perceptual content and differs in the way it is watermarked, generating a plurality of unique playlists, where each playlist is generated by generating a watermark sequence, where each watermark sequence is a unique identifier, selecting between the alternative chunks of encoded content based upon the watermark sequence, and listing the selected chunks in a playlist, where content assembled using the playlist includes a unique watermark sequence, and providing chunks of content to client devices in accordance with requests made using the plurality of unique playlists, where the content assembled by each client device includes a unique watermark sequence.

[0038] Another further embodiment includes a server configured to generate a watermark sequence, where each watermark sequence is a unique identifier. In addition, the server is also configured to select between alternative chunks of encoded content based upon the watermark sequence, where each of the alternative chunks of encoded content includes the same perceptual content and differs in the way it is watermarked, and the server is configured to list the selected chunks in a playlist, where content assembled using the playlist includes a unique watermark sequence.

[0039] Still another further embodiment includes a server configured to generate a sequence of content keys. In addition, the server is configured to select between alternative chunks of encrypted content based upon the sequence of content keys, where each of the alternative chunks of encrypted content includes the same perceptual content and is encrypted using a different content key, and the server is configured to list the selected chunks in a playlist, where content assembled using the playlist requires the sequence of content keys for decryption.

[0040] Yet another further embodiment includes an encoder configured to encode sections of the content as alternative chunks of encoded content, where each of the alternative chunks of encoded content includes the same perceptual content and differs in the way it is watermarked, a server configured to generate a plurality of unique playlists, where each playlist is generated by generating a watermark sequence, where each watermark sequence is a unique identifier,

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1023
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

selecting between alternative chunks of encoded content based upon the watermark sequence, and listing the selected chunks in a playlist, where content assembled using the playlist includes a unique watermark sequence, and a server configured to provide chunks of content to client devices in accordance with requests made using the plurality of unique playlists, where the content assembled by each client device includes a unique watermark sequence.

BRIEF DESCRIPTION OF THE DRAWINGS

[0041] In the drawings, like reference characters generally refer to the same parts throughout the different views. Also, the drawings are not necessarily to scale, emphasis instead generally being placed upon illustrating the principles of the invention.

[0042] Fig. 1 illustrates prior processes for preparing content for adaptive streaming .

[0043] Fig. 2 illustrates process for preparing content for adaptive streaming alternative chunks watermarked with alternative payloads so that each stream includes an individualized watermarking sequence in accordance with an embodiment of the invention.

[0044] Fig.3 illustrates a processing sequence and communication between a client and a server for content preparation and delivery via an individualized playlist in accordance with an embodiment of the invention.

[0045] Fig. 4 illustrates a network diagram showing a system for playing back content using an individualized playlist in accordance with an embodiment of the invention.

DETAILED DESCRIPTION

[0046] Turning now to the drawings, systems and methods for enhancing the security of content distribution using individualized playlists are illustrated. In many embodiments, a playlist is individually composed for a client device so that the selection of content included in the playlist encodes information. In a number of embodiments, the playlist encodes information using a sequence of links that refer to chunks, where the referenced chunks include chunks selected from a plurality of alternative chunks that differ in digital watermark information. In several embodiments, the content retrieved using a playlist exhibits an individual sequence of watermarked chunks that encodes information. In a number of embodiments, the playlists includes an individual sequence of links that refer to selections between alternative chunks

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1024
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

encrypted with different encryption keys. Accordingly, playback of the content referenced by the playlist involves accessing the content using a unique sequence of content keys.

[0047] A playlist in accordance with embodiments of the invention can be utilized in order to avoid the overhead of assembling a unique stream on a server in response to a request for playback by a client device. Instead, a unique playlist can be utilized by the client device or the server (depending on the streaming protocol) to transmit selected chunks of content that result in a uniquely marked and/or encrypted piece of content at the client. The approach is secure, because the client device does not possess information enabling access to the alternative chunks stored on the server that are not referenced by the playlist. The approach can also be efficiently implemented in adaptive streaming systems, because the systems already support the selection of alternative chunks of information in order to adapt to the processing environment and the implementation logic of assembling content from different chunks is already present (either on the client device or the server depending upon the adaptive streaming implementation). Although much of the following discussion relates to adaptive streaming, many embodiments of the invention select between alternative chunks that include the same encoded content (i.e. the content is only available at one bitrate), but include different embedded payload information.

[0048] Systems and methods for generating individualized playlists and playing back content using individualized playlists in accordance with embodiments of the invention are discussed further below.

Watermarking Content Using Playlists

[0049] A process for performing user or client device specific watermarking of content using a playlist in accordance with embodiments of the invention is illustrated in Fig. 2. In this example, for each chunk in Fig. 1 two alternative versions of the chunk are created with different embedded digital watermark information. As a result, two groups 220 and 230 of perceptually similar chunks of content marked with different information A (210) and B (215) are created.

[0050] A playlist can be generated such that for each section only chunks with information A or chunks with information B are accessible via the links in the playlist. The watermark sequence (i.e. the sequence of A and B marked chunks) in a file assembled using the playlist is dependent on the links provided in the playlist and not on the specific bitrate of the chunks requested by the client device. In other words, no matter which bandwidth the client is choosing, the sequence of

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1025
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

A and B in the resulting file will only depend on the playlist. The specific watermark sequence present in the content file assembled using the playlist provides information that can be used to uniquely identify the user and/or client device that assembled the content. In this way a unique playlist with a unique sequence of chunks marked with A and B watermarking can be generated for each client device or user, and the content streamed using the playlist will include a unique sequence of watermarks. In the illustrated embodiment, the sequence determined by the playlist is B, A, A.

[0051] In the embodiment illustrated in Fig. 2, two sets of payload information are used, A and B. In many embodiments, three or more sets of payload information are utilized (e.g. A,B,C,D). In several embodiments, information is embedded using chunks that include one or more alternative embedded payloads and chunks that contain no modification. Yet other embodiments create many alternative chunks in which different payload information is embedded for selected sections, and other sections are not marked. These embodiments vary in complexity and provide different numbers of alternative chunks for different sections of the content and the amount of different information that can be created with a fixed number of sections of content. The sections may be adjusted in length depending on an optimal length to embed the information or depending on other chunking optimization such as imposed by the compression system. The provision of sequences of chunks including marked chunks to client devices for playback in accordance with embodiments of the invention is discussed further below.

Provision of Marked Content to Playback Devices

[0052] The sequence diagram of Fig. 3 shows a process for preparing and streaming content using an individual playlist assembled for a specific client device or user in accordance with an embodiment of the invention. Initially, the content is ingested (310) on the server (301). The server may be operated by a retailer for online video or may be part of a content distribution network (CDN). The ingest (310) typically includes preparing the content for re-distribution with steps including but not limited to localization, adding meta information for ad insertion, program guides, and/or compression. Next, the content is separated into sections and chunks (320) are created from each section. Each chunk can then be used to create (330) multiple alternative watermarked chunks, where each alternative watermarked chunk contains the same encoded

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1026
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

content but a different watermark payload. In the illustrated embodiment, six alternative chunks are created from each section of content utilizing three different sets of encoding parameters and two different watermark payloads. In a number of embodiments, the steps (310-330) are performed once per piece of content.

[0053] Next, the content is offered for download, typically against a fee, to a known client device or user. The client device or user is authenticated. For example, by providing login information to a website (350) via her client device (302) and the server verifies her credential (355). She makes a content choice that she would like to download and/or playback. This will trigger the client device to first request (370) a playlist. A playlist is assembled on the server in a manner unique to the requesting client or user (365). The individualized playlist is then provided to the client device to enable the download/streaming (370) of the content. During playback, the client device can dynamically select chunks to download (375) from the links provided in the playlist. The server does not require any processing for a specific connection to the client but provides the chunks requested by the client (380). The client device can then play back the chunks after download (390).

[0054] Although the client device utilizes the playlist in the process illustrated in Fig. 3, in embodiments where the server determines the chunks to stream in response to a request to switch streams from the client, the server can utilize a unique playlist to select chunks of content to stream to the client device. In addition, the preparation of chunks in different bitrates or different watermarked chunks can be performed after the client has requested the playlist. This will reduce the amount of data that is permanently kept as stored chunks at the expense of increasing the processing load for each playlist request. In several embodiments, the unique playlist is assembled (365) before a client request and supplied to the next client upon request. The unique information associated with the playlist is then associated with the client by storing a record of the playlist that the client received. In yet further embodiments, the steps are performed on different servers. In many embodiments, the content preparation (310, 320, 330) is performed on a first server(s) and the delivery steps (355, 365, 380) are performed on a second server(s).

[0055] In yet further embodiments, a playlist is delivered and contains all links to differently marked chunks and the client selects the links that correspond to the content it should assemble.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1027
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

This will reduce the processing required on the server. This is particularly interesting, if the execution and interpretation at the client can be secured against readout and manipulation.

System Architecture

[0056] A system that can be used to prepare and download content for playback in accordance with an embodiment of the invention is illustrated in Fig. 4. The system 400 includes a server 402 connected to a variety of client devices via a network 403, such as the Internet. In the illustrated embodiment, the client devices include a personal computer 404, a mobile phone 406, and a consumer electronics device 408 such as a set top box, a DVD player, a Blu-ray player, a game console or an Internet connected television. Although specific playback devices are illustrated in FIG. 4, any of a variety of client devices capable of communicating with a server and downloading content can be utilized in accordance with embodiments of the invention. Although a specific system architecture is illustrated in Fig. 4, any of a variety of architectures appropriate to the streaming or downloading of content to a playback device can be utilized in accordance with embodiments of the invention.

Embedding Payload Information in Real Time

[0057] In several embodiments, alternative chunks containing different payload information for different sections of a piece of content are not preprocessed prior to being accessed but are marked upon receipt of a request for a specific chunk from the client (i.e. on the fly). In order to do so, the server is aware of the information that is used to prepare every chunk that is requested. In a number of embodiments, the information that is embedded is transmitted to the server with the link that is used to access the chunk of content. The link, therefore, includes several parts. One part of the link identifies the chunk to be accessed and another part contains information indicative of the data to be embedded. The payload to be embedded in the chunk can be inserted into the link by the client, or the link can include a unique identifier that enables the server to determine the information to be embedded in the chunk. The preparation of the chunk on the fly can include the marking, encryption and/or transcoding of a section of content.

Encryption of Alternative Chunks of Content

[0058] Encryption can be used to obfuscate and scramble digital content such that the encrypted file is not useful unless the decryption mechanism and keys used for decryption are

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1028
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

known. Encryption is often used to provide protection against unauthorized use and distribution of content. Typically the content is encrypted once using one or more content keys and the same file is distributed to all users. The content key(s) is encrypted using one or more keys that are unique to a specific user or client device and the encrypted content key(s) is delivered securely and individually to the user and/or client device. A potential problem with using a single content key or set of content keys to encrypt a widely distributed piece of content is that the security of the content is compromised if the content key(s) are obtained in the clear (i.e. unencrypted) by a user, who then shares the content keys with other users. The unencrypted content key(s) can then be used to decrypt the content by users, who have not been granted permission to play back the content by the content creators or owners of the content.

[0059] In many embodiments, chunks of content corresponding to the same section of a piece of content can be encrypted with different encryption keys and/or encryption algorithms. The encrypted chunks can be used to specify the assembly of uniquely encrypted files without individually encrypting the content for each client device. Referring back to the embodiment illustrated in Fig. 2, each group of chunks 220, 230 in each section can be encrypted with a different content key or different set of encryption keys. For example, a first group of chunks (220) can be encrypted with a set of content keys K_A and a second group of chunks (230) can be encrypted with set of content keys K_B. In which case, decryption of the entire streamed file (B, A, A) utilizes the following content keys: K_{B1} for section T1, K_{A2} for section T2 and K_{A3} for section T3. Different content keys can be used to encrypt each section of the content. For example, a first group of chunks (220) corresponding to three sections of a piece of content can be encrypted using a set of three content keys K_{A1}, K_{A2}, and K_{A3}, and a second group of chunks (230) corresponding to the three sections of content can be encrypted using a second set of content keys K_{B1}, K_{B2}, and K_{B3}. Accordingly, decryption of the same file could involve the following content keys: K_{B1} for section T1, K_{A2} for section T2 and K_{A3} for section T3. The keys between sets (A and B) as well as within sets (A1, A2) are commonly different to provide the maximal variation in keys and provide a higher level of security. In the event that a first client obtained the content keys in the clear, another client would receive chunks in accordance with a different playlist configured so that different keys are utilized during decryption. This enhances the security of the resulting delivered file because the keys required can be unique for every

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1029
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

client and simply sharing the content keys amongst different clients is unlikely to enable decryption of content obtained from a server in its entirety. When encryption is performed in a manner similar to that outlined above, the playlist and a content key table can be assembled uniquely for every client; an operation that can be performed very efficiently. As can be readily appreciated, individualized playlists can be utilized to enable adaptive streaming, variation in content key sequence, and/or watermarking. In many embodiments, the length of the chunks may be different for each of the applications.

[0060] In the embodiment illustrated in Fig. 2, two sets of keys are used, A and B. In many embodiments, three or more keys are utilized (e.g. A,B,C,D). In several embodiments, information is embedded using chunks that are encrypted using one or more keys and chunks that remain unencrypted. Yet other embodiments create many alternative chunks in which different keys are used for selected sections, and other sections are encrypted with a single key only. Some sections may also be encrypted with keys unique to an individual client. These embodiments vary in complexity and provide different numbers of alternative chunks for different sections of the content and effectively increase the difficulty to decrypt the content by combining different playlists. And keys may change over time and different representations of the same content on different servers may use different keys (e.g. in a content distribution network). The sections may be adjusted in length depending on an optimal length to archive the maximal impact of the key selection or depending on other chunking optimization such as imposed by the compression system. The number of keys may also be temporarily reduced in order to increase delivery performance by enabling improved caching for a limit time.

[0061] Another variation to enhance the security of the delivery is to use different keys for different quality levels of the content. While there is a risk that the client is manipulated to always retrieve the same content and therefore maximize the probability of matching keys between the content retrieved by two clients, this represents another hurdle at the client and makes an attack harder, since typically the sequence of quality levels is determined by client capabilities and network conditions. Referring to Fig. 2 the keys for section T1 of Low, Med and High segments would be different and even if a second client uses the same group (e.g. A), that client would not be able to use the keys from the first client if they requested different chunks of this segment.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1030
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Incorporating Single Use Links in Individualized Playlists

[0062] The security of distributed content can be enhanced by utilizing single use or "one-time" links in a playlist in accordance with embodiments of the invention. The single use link is created and recorded when a user and/or a client device requests a piece of content. In several embodiments, the link includes several parts. One part of the link indicates the chunk to be accessed and another part contains a token that is a piece of information that is unique to any link pointing to this chunk. After that chunk has been access using this token, the server registers that the token has been used to retrieve the chunk and does not allow access to this chunk using the same token again. The token can also be secured such that a random piece of information will not be considered a valid token by the server, because it has not been presented before. This can be accomplished with a token white list or by digitally signing the token. Single use links can be useful for identifying alternative chunks in which watermarking is utilized to embed payload information and/or alternative chunks that are encrypted using different content keys or different sets of content keys in accordance with embodiments of the invention.

Incorporating Destination Links in Individualized Playlists

[0063] The security of content distribution can be further enhanced by using destination links (i.e. links in the playlist that can only be used from a specific destination) in accordance with embodiments of the invention. Destination links are described in detail in U.S. Provisional Patent Application No. 61/333,909 entitled "Securing Content Access Using Destination Links", filed May 12, 2010, the disclosure of which is incorporated by reference above. A destination link can be created when a client requests playback of a specific piece of content. The destination link can incorporate destination properties of the requesting clients such as its IP address or port or a combination of HTTP request components, MAC address, cookie, device ID / serial number or user credentials. Accordingly, the link includes several parts. One part of the Link indicates the chunk to be accessed and another part contains information indicative of a destination property. In several embodiments, the destination property is secured against tampering by obfuscation (e.g. using a secure hash). When a chunk is accessed using a destination link, the server will only provide the requested data if the request from the client device matches the destination encoded in the link. Destination links can be useful for identifying alternative chunks in which watermarking is utilized to embed payload information

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1031
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

and/or alternative chunks that are encrypted using different content keys or different sets of content keys in accordance with embodiments of the invention.

Incorporating Obfuscated Links in Individualized Playlists

[0064] The security of distributed content can also be enhanced using obfuscated links (i.e. links that have no obvious connection to the data that is retrieved) in accordance with embodiments of the invention. Instead of using a link that can be interpreted, such as:

http://server.com/movie=content1.mp4&chunk=10&key=B10

an obfuscated link can be generated and utilized, such as:

http://server.com/movie=content1.mp4&token=x12ywe23e

where the token x12ywe23e points to the requested chunk (e.g. chunk=10 and encryption key = B10) in a way that can only be resolved on the server by a lookup or process such as encryption or hashing. Although obfuscation using tokens is described above, obfuscations using any of a variety of techniques that provide information to a server as part of a link can be utilized in accordance with embodiments of the invention.

Encrypted Playlists

[0065] Security can be further enhanced by encrypting individualized playlists distributed to client devices, so that the playlist can only be read and executed by a specific client device or user qualified by the possession of a key bound to the client device or specific to the user. The key may be symmetric or asymmetric.

Playlist-Bound Keys

[0066] Security can also be enhanced using playlist-bound keys, which contain information unique to the playlist such that the server can verify the identity of playlist from which content requests originate. A playlist-bound key can be a number embedded in the playlist during the creation of the playlist, or a hash code of the playlist or a portion of the playlist stored by or capable of being re-generated by the server. The number can be embedded in a single location within the playlist and utilized by the client device to generate content requests or can be a part of every link contained in the playlist. When the playlist-bound key is present in each link

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1032
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

within the playlist, the playlist-bound key is typically a separate parameter in the link or combined with, for example, a token in the link or other already existing elements in the link. Although tokens are described above, any technique for binding a key to a playlist that is appropriate to a specific application can be utilized in accordance with embodiments of the invention.

Chunk-Bound Keys

[0067] Security may also be enhanced using chunk-bound keys, which are keys that are modified/obfuscated based upon the content of a chunk and can only be used if the appropriate content chunk is present. This binding can occur by a process of an XOR combination with one or several sections of the chunk or a hash code of the chunk. Consequently, the key cannot be used in a different context on another chunk. One scenario where this is relevant is where the same key is used for differently marked content, such that the content varies while the key used to encrypt the alternative chunks of content does not vary. By using the marked content (or unmarked content) to modify the key, the keys received by the client device vary for every variation of the chunk even though the same key is used to encrypt the content. The process used to modify the key can be undone at the client device using information derived from the received chunk. The process reduces the likelihood that modified, delivered keys can be shared between differently marked or compressed chunks.

Applications

[0068] The systems and techniques described above can be used in several different applications. In many embodiments, the system is used to track unauthorized distribution of secret or copyrighted information. A problem that faces many industries is the unauthorized distribution of information. Systems and processes in accordance with embodiments of the present invention can be used to embed marks in media information at the time of delivery of the content. Each distributed copy can be uniquely marked with information such as a recipient identification number and a time stamp. If the copy is publicly available or in the possession of an entity or individual that is not authorized to possess the information, the information can be uncovered and the entity or person that is the recipient of the media and the likely source of the unauthorized distribution can be identified.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1033
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

[0069] In many instances, the secret or copyrighted information is passed between several different entities and/or individuals during production and authorized distribution. In several embodiments, the point from which the information was distributed without authorization can be ascertained by embedding a mark associated with the last recipient of the information prior to delivery or display. The entity or individual that is responsible for the unauthorized distribution can then be identified based upon the last mark added to the content.

[0070] A common instance, in which copyrighted information is communicated, is the distribution of copyrighted media via a network to a media player. In many embodiments, the player is a consumer electronics device such as a set top box or a personal computer. A mark can be embedded in the media in accordance with embodiments of the invention. The mark can contain information relating to the owner of the player and information identifying the time of transmission or playback. If the recipient of the information is known, the information to be embedded can be generated by the server (or head end) providing the media. The embedded information can also be stored by the server in a database that contains additional information about the transaction, such as the user's billing information and details about the receiving device. In other embodiments, the player maintains information such as player identification number and time, which is embedded as a mark during storage and/or playback.

[0071] Another instance in which unauthorized distribution is a common problem is in the production of media. During production, content is particularly vulnerable to unauthorized distribution that can cause considerable damage to the producer of the media. In many embodiments, marks are embedded in the media during various stages of production that identify the recipient of the media and the time of the receipt of the media. If the copy is made publicly available, the mark can be uncovered and the responsible person or entity can be identified.

[0072] Although the present invention has been described in certain specific aspects, many additional modifications and variations would be apparent to those skilled in the art. It is therefore to be understood that the present invention may be practiced otherwise than specifically described, including various changes in the implementation. Thus, embodiments of the present invention should be considered in all respects as illustrative and not restrictive.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1034
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

WHAT IS CLAIMED:

1. A method of generating a plurality of unique playlists, where content assembled using each playlist includes a unique watermark sequence, and the method of generating each of the plurality of unique playlists comprises:

generating a watermark sequence, where each watermark sequence is a unique identifier;

selecting between alternative chunks of encoded content based upon the watermark sequence, where each of the alternative chunks of encoded content includes the same perceptual content and differs in the way it is watermarked; and

listing the selected chunks in a playlist, where content assembled using the playlist includes a unique watermark sequence.

2. The method of claim 1, wherein at least one of the alternative chunks includes an imperceptibly embedded watermark, and one of the alternative chunks is unmodified.

3. The method of claim 1, wherein each of the alternative chunks includes a different imperceptibly embedded watermark.

4. The method of claim 3, wherein each of the alternative chunks includes a different amount of embedded information.

5. The method of claim 1, wherein the number of alternative chunks differs for different sections of the content.

6. The method of claim 1, wherein:

selecting between alternative chunks of encoded content based upon the watermark sequence further comprises selecting between alternative groups of chunks based upon the watermark sequence, where each chunk in a group of chunks includes the same perceptual content encoded using different encoding parameters and is watermarked in the same

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1035
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

way, and alternative groups of chunks encode the same perceptual content and differ in the way they are watermarked; and

listing the selected chunks in the playlist further comprises listing the chunks from the selected groups of chunks in the playlist.

7. The method of claim 1, wherein the selected chunks are listed in the playlist using links to the selected chunks of encoded content.

8. The method of claim 7, wherein at least one of the links is a single use link.

9. The method of claim 8, wherein each single use link includes a unique token.

10. The method of claim 7, wherein at least one of the links is a destination link.

11. The method of claim 10, wherein each destination link includes a token indicative of a client device.

12. The method of claim 1, further comprising inserting a playlist-bound key into the playlist.

13. The method of claim 1, wherein selecting between alternative chunks of encoded content based upon the watermark sequence further comprises selecting between chunks where each of the alternative chunks is encrypted in a different way.

14. The method of claim 13, wherein each of the alternative chunks is encrypted using a different encryption key.

15. The method of claim 1, wherein selection between alternative chunks of encoded content is performed as the watermark sequence is generated.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1036
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

16. A method of generating a plurality of playlists, where content assembled using each playlist is encrypted using a different sequence of content keys, and the method of generating each playlist comprises:

generating a sequence of content keys;

selecting between alternative chunks of encrypted content based upon the sequence of content keys, where each of the alternative chunks of encrypted content includes the same perceptual content and is encrypted using a different content key; and

listing the selected chunks in a playlist, where content assembled using the playlist requires the sequence of content keys for decryption.

17. The method of claim 16, wherein selection between alternative chunks of encrypted content is performed as the sequence of content keys is generated.

18. The method of claim 16, further comprising modifying the sequence of content keys by modifying at least one of the content keys using information derived from one of the selected chunks of encrypted content.

19. The method of claim 16, wherein the number of alternative chunks of encrypted content differs for different sections of the content.

20. A method of providing content for downloading using a plurality of unique playlists, where content assembled using each playlist includes a unique watermark sequence, comprising:

encoding sections of the content as alternative chunks of encoded content, where each of the alternative chunks of encoded content includes the same perceptual content and differs in the way it is watermarked;

generating a plurality of unique playlists, where each playlist is generated by:

generating a watermark sequence, where each watermark sequence is a unique identifier;

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1037
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

selecting between the alternative chunks of encoded content based upon the watermark sequence; and

listing the selected chunks in a playlist, where content assembled using the playlist includes a unique watermark sequence; and

providing chunks of content to client devices in accordance with requests made using the plurality of unique playlists, where the content assembled by each client device includes a unique watermark sequence.

21. A system configured to generate a plurality of unique playlists, where content assembled using each playlist includes a unique watermark sequence, the system comprising:

a server configured to generate a watermark sequence, where each watermark sequence is a unique identifier;

wherein the server is also configured to select between alternative chunks of encoded content based upon the watermark sequence, where each of the alternative chunks of encoded content includes the same perceptual content and differs in the way it is watermarked; and

wherein the server is configured to list the selected chunks in a playlist, where content assembled using the playlist includes a unique watermark sequence.

22. A system configured to generate a plurality of playlists, where content assembled using each playlist is encrypted using a different sequence of content keys, the system comprising:

a server configured to generate a sequence of content keys;

wherein the server is configured to select between alternative chunks of encrypted content based upon the sequence of content keys, where each of the alternative chunks of encrypted content includes the same perceptual content and is encrypted using a different content key; and

wherein the server is configured to list the selected chunks in a playlist, where content assembled using the playlist requires the sequence of content keys for decryption.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1038
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

23. A system configured to provide content for downloading using a plurality of unique playlists, where content assembled using each playlist includes a unique watermark sequence, the system comprising:

an encoder configured to encode sections of the content as alternative chunks of encoded content, where each of the alternative chunks of encoded content includes the same perceptual content and differs in the way it is watermarked;

a server configured to generate a plurality of unique playlists, where each playlist is generated by:

generating a watermark sequence, where each watermark sequence is a unique identifier;

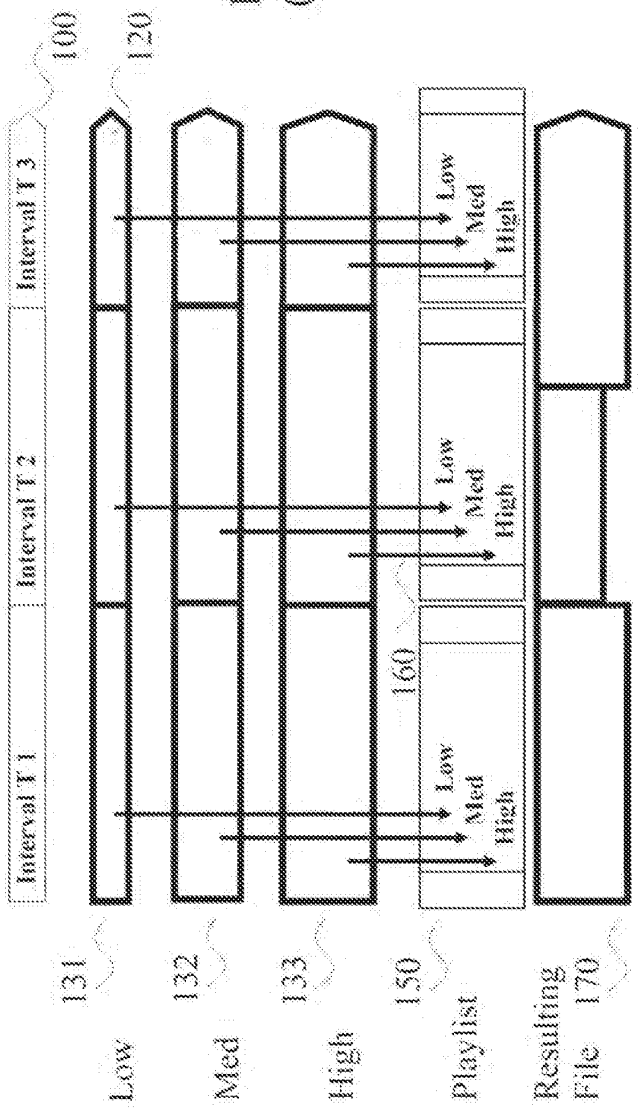
selecting between alternative chunks of encoded content based upon the watermark sequence; and

listing the selected chunks in a playlist, where content assembled using the playlist includes a unique watermark sequence; and

a server configured to provide chunks of content to client devices in accordance with requests made using the plurality of unique playlists, where the content assembled by each client device includes a unique watermark sequence.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1039
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Fig. 1
(Prior Art)



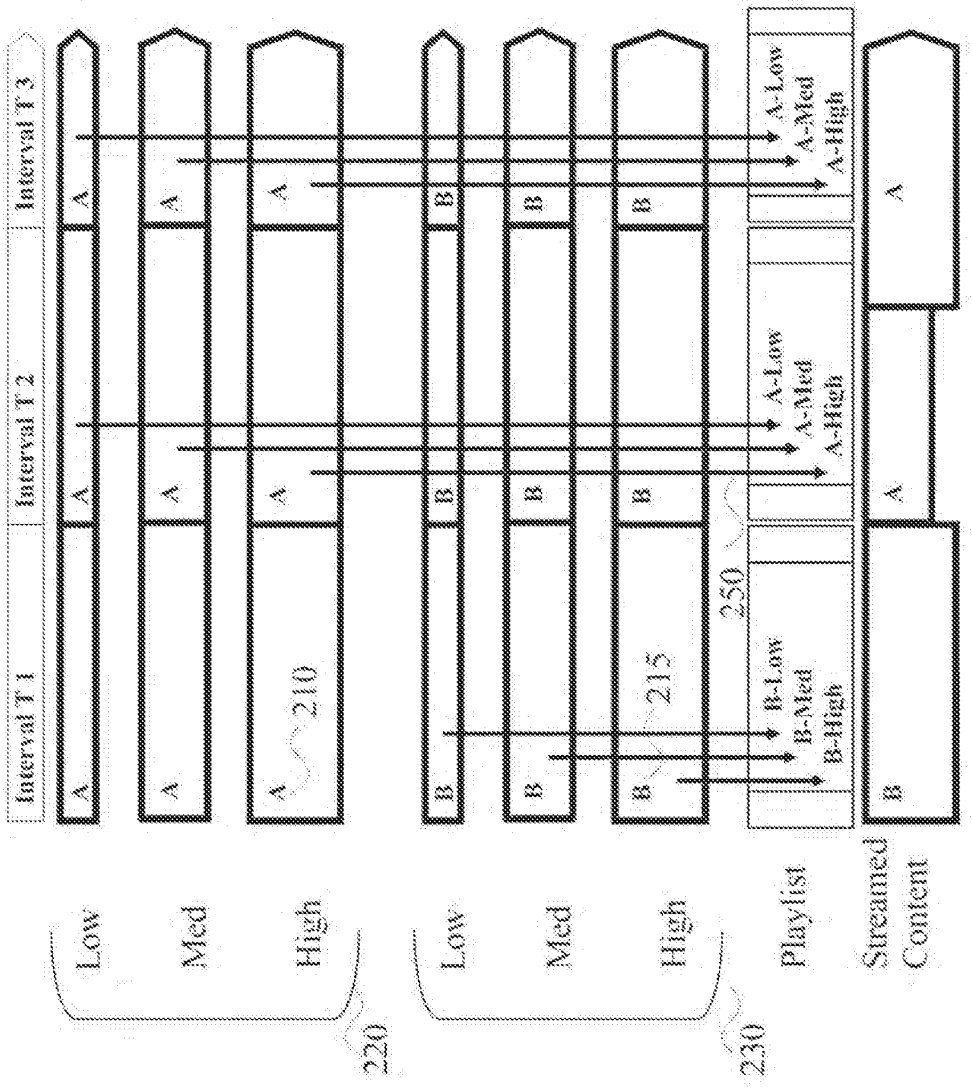

Interval T 1
Interval T 2
Interval T 3
A
B
210
215
250
A-Low
A-Med
A-High
B-Low
B-Med
B-High
Low
Med
High
220
230
Playlist
Streamed Content

Fig. 2

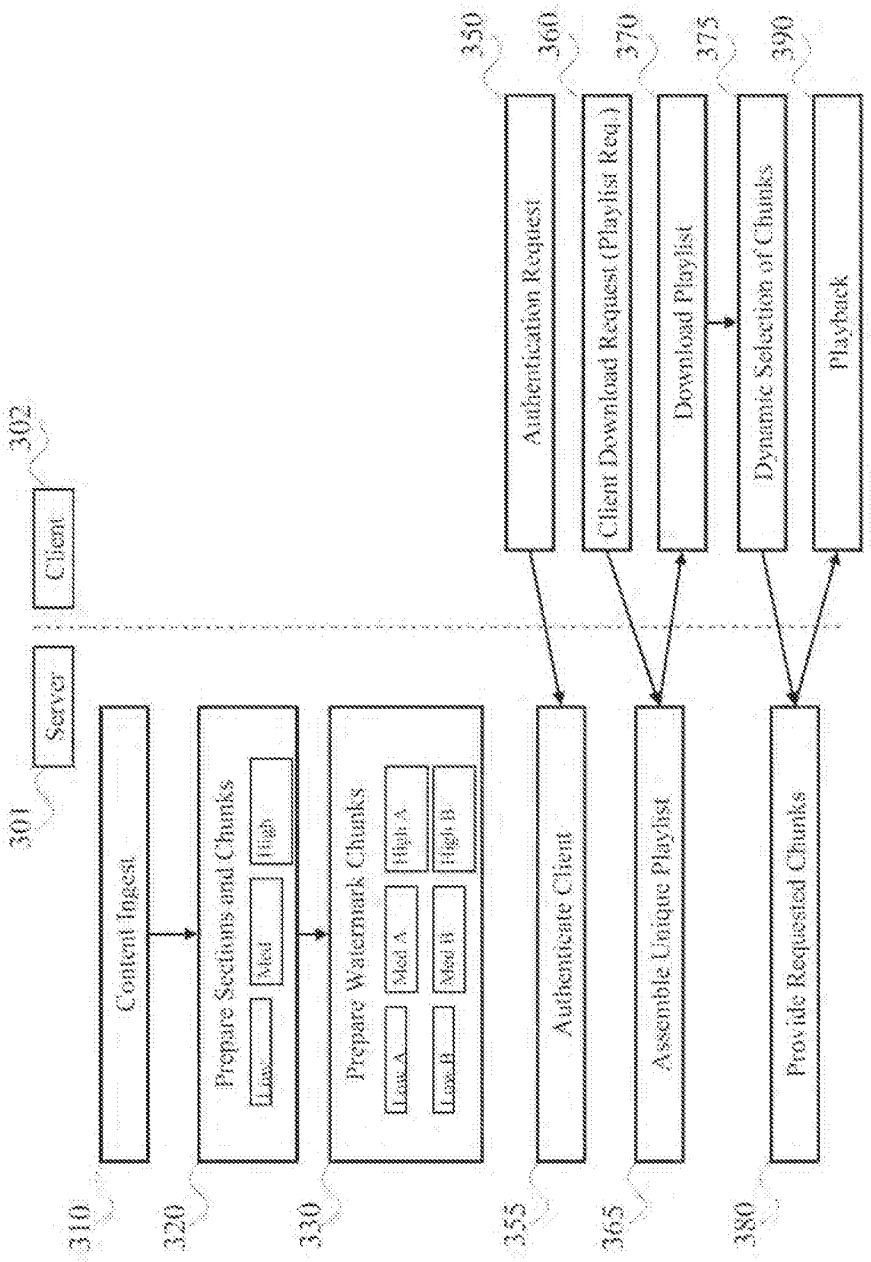

301
Server
302
Client
Content Ingest
Prepare Sections and Chunks
Low
Med
High
Prepare Watermark Chunks
Low A
Low B
Med A
Med B
High A
High B
Authentication Request
Client Download Request (Playlist Req.)
Download Playlist
Dynamic Selection of Chunks
Playback
Authenticate Client
Assemble Unique Playlist
Provide Requested Chunks
310
320
330
350
360
370
375
390
355
365
380

Fig. 3

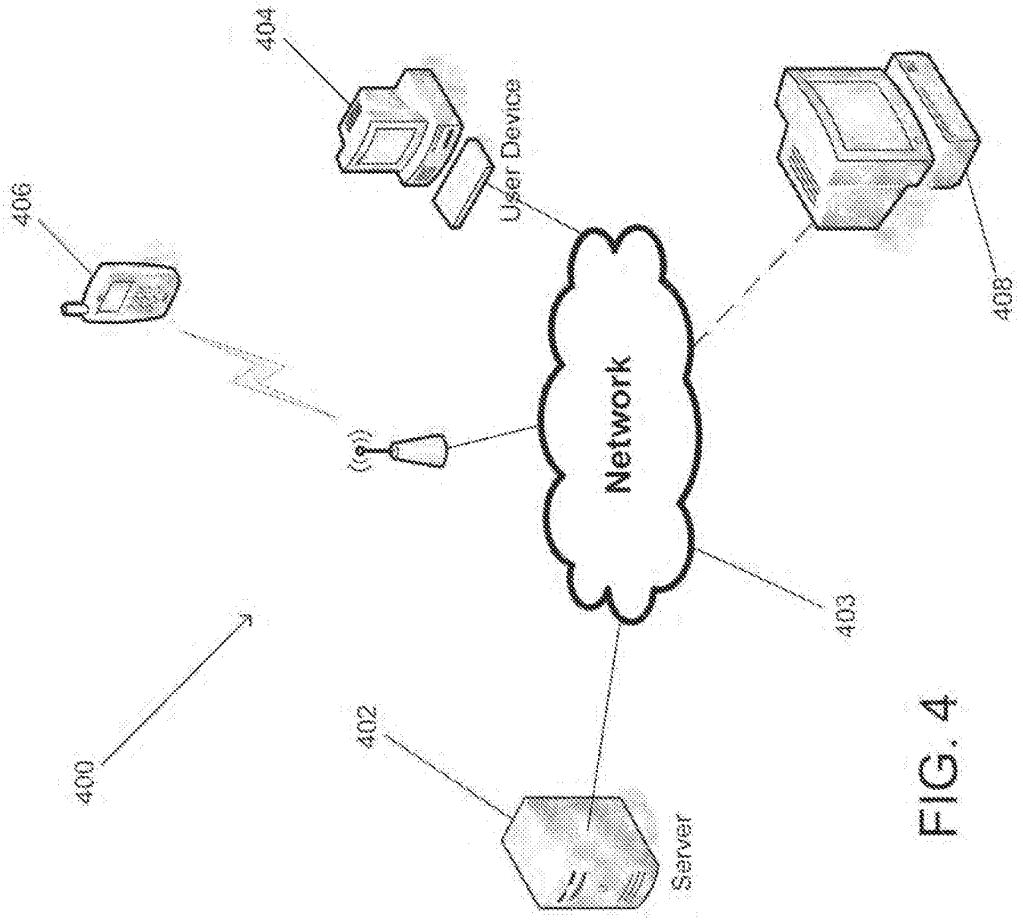


FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 11/25341

A CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F 21/00 (2011.01)
USPC - 705/51
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)
USPC: 705/51

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 705/54; 705/50 (keyword limited - see search terms below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PubWEST (PGPB, USPT, USOC, EPAB, JPAB); GOOGLE; Google Scholar
Terms: playlist, order, security, music, media, video, watermark, sequence, identifier, chunk, sections, linking, token, encoding, streaming, channel, alternating, unique

C DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 2009/0158318 A1 (Levy) 18 June 2009 (18.06.2009), entire document, especially abstract, para [0049], [0053], [0076], [0124], [0151], [0250], [0268], [0272], [0277], [0291], [0298], [0312], [0343], [0361], [0366]	1, 7-12, 15-23 --- 2-6, 13-14
Y	US 2006/0101269 A1 (Moskowitz et al.) 11 May 2006 (11.05.2006), entire document, especially abstract, para [0007], [0008], [0021], [0036], [0040], [0116], [0117].	2-6, 13-14
A	US 2007/0283449 A1 (Green) 06 December 2007 (06.12.2007), entire document, especially abstract, para [0001], [0006], [0010], [0011], [0041], [0044], [0050].	1-23

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"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
08 April 2011 (08.04.2011)	19 APR 2011
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 March 2013 (07.03.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/032518 A2

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

(21) International Application Number:
PCT/US2011/068276

(22) International Filing Date:
31 December 2011 (31.12.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/530,305 1 September 2011 (01.09.2011) US
13/340,623 29 December 2011 (29.12.2011) US
13/341,265 30 December 2011 (30.12.2011) US

(71) Applicant *(for all designated States except US)*: **DIVX, LLC** [US/US]; 2830 De La Cruz Boulevard, Santa Clara, CA 95050 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **KIEFER, Michael, George** [US/US]; 7007 E. Gold Dust Ave., Apt. 1053, Scottsdale, AZ 85253 (US). **GRAB, Eric, William** [US/US]; 5387 Channing Street, San Diego, CA 92117 (US). **BRANESS, Jason** [US/US]; 15885 Concord Ridge Terrace, San Diego, CA 92127 (US).

(74) Agent: **BAILEY, David, J.**; Kaufi, Pomeroy, Peck & Bailey LLP, 2400 E. Katella, Suite 1050, Anaheim, CA 92806 (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, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, 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, RS, SE, SI, SK, SM, 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 (Rule 48.2(g))*

(54) Title: SYSTEMS AND METHODS FOR PROTECTING ALTERNATIVE STREAMS IN ADAPTIVE BITRATE STREAMING SYSTEMS

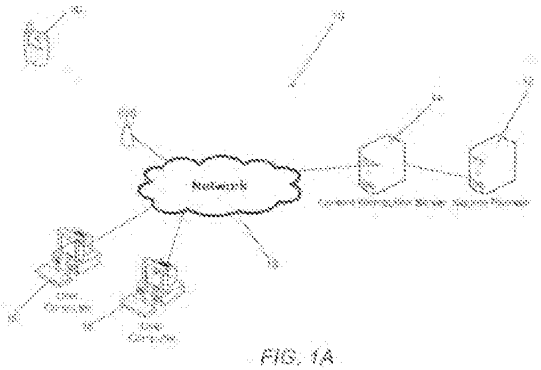


FIG. 1A

(57) Abstract: Systems and methods for performing adaptive bitrate streaming using alternative streams of protected content in accordance with embodiments of the invention are described. One embodiment includes a processor, and non-volatile storage containing an encoding application. In addition, the encoding application configures the processor to: receive source content; obtain common cryptographic information; encode the source content as a plurality of streams including a plurality of alternative streams of content; and protect the plurality of alternative streams of content using the common cryptographic information.

WO 2013/032518 A2

Systems and Methods For Protecting Alternative Streams in Adaptive Bitrate Streaming Systems

FIELD OF THE INVENTION

[0001] The present invention generally relates to adaptive streaming and more specifically to adaptive bitrate streaming of encoded media contained within Matroska container files using Hypertext Transfer Protocol.

BACKGROUND

[0002] The term streaming media describes the playback of media on a playback device, where the media is stored on a server and continuously sent to the playback device over a network during playback. Typically, the playback device stores a sufficient quantity of media in a buffer at any given time during playback to prevent disruption of playback due to the playback device completing playback of all the buffered media prior to receipt of the next portion of media. In many instances, content is divided into multiple streams. For example, content can be divided into audio, video, and subtitle streams and some streams can be encoded as alternative streams that are suitable for different network connection bandwidths or comply with specific geographic restrictions and/or other restrictions.

[0003] Adaptive bit rate streaming or adaptive streaming involves detecting the present streaming conditions (e.g. the user's network bandwidth and CPU capacity) in real time and adjusting the quality of the streamed media accordingly by selecting between different streams encoded for use at different network connection data rates. Typically, the source media is encoded at multiple bitrates and the playback device or client switches between streaming the different encodings depending on available resources.

[0004] Adaptive streaming solutions typically utilize either Hypertext Transfer Protocol (HTTP), published by the Internet Engineering Task Force and the World Wide Web Consortium as RFC 2616 to stream media between a server and a playback device.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1046
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

HTTP is a stateless protocol that enables a playback device to request a byte range within a file. HTTP is described as stateless, because the server is not required to record information concerning the state of the playback device requesting information or the byte ranges requested by the playback device in order to respond to requests received from the playback device.

[0005] In adaptive streaming systems, the source media is typically stored on a media server as a top level index file pointing to a number of alternate streams that contain the actual video and audio data. Each stream is typically stored in one or more container files. Different adaptive streaming solutions typically utilize different index and media containers. The Synchronized Multimedia Integration Language (SMIL) developed by the World Wide Web Consortium is utilized to create indexes in several adaptive streaming solutions including IIS Smooth Streaming developed by Microsoft Corporation of Redmond, Washington, and Flash Dynamic Streaming developed by Adobe Systems Incorporated of San Jose, California. HTTP Adaptive Bitrate Streaming developed by Apple Computer Incorporated of Cupertino, California implements index files using an extended M3U playlist file (.M3U8), which is a text file containing a list of URIs that typically identify a media container file. The most commonly used media container formats are the MP4 container format specified in MPEG-4 Part 14 (i.e. ISO/IEC 14496-14) and the MPEG transport stream (TS) container specified in MPEG-2 Part 1 (i.e. ISO/IEC Standard 13818-1). The MP4 container format is utilized in IIS Smooth Streaming and Flash Dynamic Streaming. The TS container is used in HTTP Adaptive Bitrate Streaming.

[0006] The Matroska container is a media container developed as an open standard project by the Matroska non-profit organization of Aussonne, France. The Matroska container is based upon Extensible Binary Meta Language (EBML), which is a binary derivative of the Extensible Markup Language (XML). Decoding of the Matroska container is supported by many consumer electronics (CE) devices. The DivX Plus file format developed by DivX, LLC of San Diego, California utilizes an extension of the

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1047
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Matroska container format (i.e. is based upon the Matroska container format, but includes elements that are not specified within the Matroska format).

[0007] The term Digital Rights Management (DRM) is utilized to describe access control technologies that are used to control access to and/or copying of digital content. DRM systems typically involve the use of cryptographic information to control access to or protect a piece of content. Content protection is typically achieved using cryptographic information such as (but not limited to) one or more encryption keys to encrypt some or all of the content. An important component of most DRM systems is a mechanism for securely providing cryptographic information to authorized playback devices for use in accessing protected content. The protected content cannot be accessed without the cryptographic data and ideally the cryptographic data is bound to specific playback devices and cannot be readily used by unauthorized playback devices or is securely provided to the playback devices (often on a session basis).

SUMMARY OF THE INVENTION

[0008] Systems and methods in accordance with embodiments of the invention perform adaptive bitrate streaming using alternative streams of protected content. One embodiment includes a processor, and non-volatile storage containing an encoding application. In addition, the encoding application configures the processor to: receive source content; obtain common cryptographic information; encode the source content as a plurality of streams including a plurality of alternative streams of content; and protect the plurality of alternative streams of content using the common cryptographic information.

[0009] An embodiment of the method of the invention includes receiving source content using a source encoder, obtaining common cryptographic information using a source encoder, encoding the source content as a plurality of streams including a plurality of alternative streams of content using the source encoder, and protecting the

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1048
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

plurality of alternative streams of content using the source encoder and the common cryptographic information.

[0010] Another embodiment of the invention includes a machine readable medium containing processor instructions, where execution of the instructions by a processor causes the processor to perform a process including receiving source content, obtaining common cryptographic information, encoding the source content as a plurality of streams including a plurality of alternative streams of content, and protecting the plurality of alternative streams of content and the common cryptographic information.

[0011] A further embodiment includes a DRM server, and a content distribution server, where the content distribution server stores a plurality of container files containing alternative streams of protected content associated with a title, the alternative streams of protected content are protected using common cryptographic information, and each container file includes a copy of the common cryptographic information encrypted using at least one encryption key. In addition, the DRM server is configured to receive a request for access to the alternative streams of protected content associated with the title from a playback device, and securely provide a copy of the at least one encryption key used to encrypt the common cryptographic information to the playback device. Furthermore, the content distribution server is configured to grant the playback device access to the alternative streams of protected content.

[0012] A further embodiment of the method of the invention includes receiving a request for access to the alternative streams of protected content associated with the title from a playback device using a DRM server, securely providing to the playback device at least one encryption key using the DRM server, where the at least one encryption keys is used to access the encrypted common cryptographic information, and granting the playback device access to the alternative streams of protected content using a content distribution server.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1049
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

[0013] Another further embodiment of the invention includes a processor, and memory containing a client application. In addition, the client application configures the processor to: request a top level index file identifying a plurality of alternative streams of protected content, where each of the alternative streams of protected content are encrypted using common cryptographic information; obtain the common cryptographic information; request portions of content from at least the plurality of alternative streams of protected content; access the protected content using the common cryptographic information; and playback the content.

[0014] An embodiment of the method of the invention includes requesting a top level index file identifying a plurality of alternative streams of protected content using a playback device, where each of the alternative streams of protected content are encrypted using common cryptographic information, obtaining the common cryptographic information using the playback device, requesting portions of content from at least the plurality of alternative streams of protected content using the playback device, accessing the protected content using the playback device and the common cryptographic information, and playing back the content using the playback device.

[0015] Another further embodiment includes a machine readable medium containing processor instructions, where execution of the instructions by a processor causes the processor to perform a process including request a top level index file identifying a plurality of alternative streams of protected content, where each of the alternative streams of protected content are encrypted using common cryptographic information, obtaining the common cryptographic information, requesting portions of content from at least the plurality of alternative streams of protected content, accessing the protected content using the common cryptographic information, and playing back the content.

BRIEF DESCRIPTION OF THE DRAWINGS

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1050
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

[0016] FIG. 1A is a network diagram of an adaptive bitrate streaming system in accordance with an embodiment of the invention.

[0017] FIG. 1B is a block diagram illustrating a source encoder in accordance with an embodiment of the invention.

[0018] FIG. 1C is a block diagram illustrating a content distribution server in accordance with an embodiment of the invention.

[0019] FIG. 1D is a block diagram illustrating a playback device in accordance with an embodiment of the invention.

[0020] FIG. 2 conceptually illustrates a top level index file and Matroska container files generated by the encoding of source media in accordance with embodiments of the invention.

[0021] FIG. 3 conceptually illustrates a specialized Matroska container file incorporating a TracksData Payload containing cryptographic information in accordance with an embodiment of the invention.

[0022] FIGS. 4a - 4c conceptually illustrate the insertion of different types of protected media into the Clusters element of a Matroska container file subject to various constraints that facilitate adaptive bitrate streaming in accordance with embodiments of the invention.

[0023] FIG. 4d conceptually illustrates the multiplexing of different types of protected media into the Clusters element of a Matroska container file subject to various constraints that facilitate adaptive bitrate streaming in accordance with an embodiment of the invention.

[0024] FIG. 4e conceptually illustrates the inclusion of a protected trick play track into the Clusters element of a Matroska container file subject to various constraints that facilitate adaptive bitrate streaming in accordance with an embodiment of the invention.

[0025] FIG. 5 conceptually illustrates a modified Cues element of a specialized Matroska container file, where the Cues element includes information enabling the

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1051
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

retrieval of Cluster elements using HTTP byte range requests in accordance with an embodiment of the invention.

[0026] FIG. 5a conceptually illustrates a modified Cues element of a specialized Matroska container file in accordance with an embodiment of the invention, where the Cues element is similar to the Cues element shown in FIG. 5 with the exception that attributes that are not utilized during adaptive bitrate streaming are removed.

[0027] FIG. 6 conceptually illustrates the indexing of Cluster elements within a specialized Matroska container file utilizing modified CuePoint elements within the container file in accordance with embodiments of the invention.

[0028] FIG. 7 conceptually illustrates the use of a hierarchical index to index CuePoint elements within a Matroska container file in accordance with embodiments of the invention.

[0029] FIG. 8 is a flow chart illustrating a process for encoding and protecting source media for adaptive bitrate streaming in accordance with an embodiment of the invention.

[0030] FIG. 9 is a flow chart illustrating a process for encoding and encrypting frames of source video in accordance with an embodiment of the invention.

[0031] FIG. 10 conceptually illustrates a DRM header element that can be included in a Matroska container file in accordance with an embodiment of the invention.

[0032] FIG. 11 conceptually illustrates communication between a playback device and an HTTP server associated with the commencement of streaming of encoded media contained within Matroska container files indexed by a top level index file in accordance with an embodiment of the invention.

[0033] FIGS. 12a and 12b conceptually illustrate communication between a playback device and an HTTP server associated with switching between streams in response to the streaming conditions experienced by the playback device prior to the decision to switch streams in accordance with embodiments of the invention.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1052
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

DETAILED DISCLOSURE OF THE INVENTION

[0034] Turning now to the drawings, systems and methods for performing adaptive bitrate streaming using alternative streams of protected content in accordance with embodiments of the invention are illustrated. In a number of embodiments, source media is encoded as a number of alternative streams and the alternative streams are protected using a common set of cryptographic information. In many embodiments, the alternative streams are video streams and each stream is protected by encrypting at least a portion of a plurality of video frames within the stream using the common set of cryptographic information. In several embodiments, the common set of cryptographic information is a set of frame keys. In order to protect a video frame, a frame key can be selected from the set of frame keys and used to encrypt at least a portion of the encoded frame and DRM information can be provided with the protected frame indicating the frame key utilized to perform the encryption and the location of the encrypted portion within the frame. By encrypting each of the alternative streams using the same set of cryptographic information, a playback device can switch between streams without the need to maintain or acquire multiple sets of cryptographic information in memory or to reinitialize the decryption engine of the playback device with a different set of cryptographic information.

[0035] In many embodiments, each of the alternative streams is stored in a separate container file referenced by a top level index file. In several embodiments, the common cryptographic information is embedded in each of the container files so that a playback device has access to the cryptographic information irrespective of which alternative is initially select to commence playback of the media. The common cryptographic information can be stored on a content distribution system and associated with a title identifier or title ID that uniquely identifies the source content used to create the alternative streams. When a new alternative stream is generated, a source encoder can utilize the title ID to request the common cryptographic information from the content distribution system and the common cryptographic information can be utilized

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1053
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

to encrypt the new alternative stream and embedded in a container file created to contain the new encrypted alternative stream.

[0036] In several embodiments, each stream associated with a piece of source content and/or title ID is stored in a Matroska (MKV) container file. In many embodiments, the Matroska container file is a specialized Matroska container file in that the manner in which the media in each stream is encoded and stored within the container is constrained to improve streaming performance. In several embodiments, the Matroska container file is further specialized in that additional DRM elements (i.e. elements that are not specified as part of the Matroska container format) can be included within the file to facilitate the distribution of protected media during adaptive bitrate streaming. In a number of embodiments, common cryptographic information is included within a DRM header element in each of the Matroska container files and references to the common cryptographic information are made using DRMInfo elements within a BlockGroup element corresponding to a specific frame of encrypted video. In other embodiments, any of a variety of mechanisms can be utilized to store DRM information within a Matroska container in accordance with embodiments of the invention. In several embodiments, each stream (i.e. audio, video, or subtitle) is stored within a separate Matroska container file. In other embodiments, an encoded video stream is multiplexed with one or more encoded audio, and/or subtitle streams in each Matroska container file.

[0037] A top level index file containing an index to the streams contained within each of the container files is also generated to enable adaptive bitrate streaming of the encoded media. In many embodiments, the top level index file is a Synchronized Multimedia Integration Language (SMIL) file containing URIs for each of the Matroska container files. In other embodiments, any of a variety of file formats can be utilized in the generation of the top level index file.

[0038] The performance of an adaptive bitstrate streaming system in accordance with embodiments of the invention can be significantly enhanced by encoding each

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1054
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

portion of the source video at each bit rate in such a way that the portion of video is encoded in each stream as a single (or at least one) closed group of pictures (GOP) starting with an Instantaneous Decoder Refresh (IDR) frame. The GOP for each stream can then be stored as a Cluster element within the Matroska container file for the stream. In this way, the playback device can switch between streams at the completion of the playback of a Cluster and, irrespective of the stream from which a Cluster is obtained the first frame in the Cluster will be an IDR frame and can be decoded without reference to any encoded media other than the encoded media contained within the Cluster element. In many embodiments, the sections of the source video that are encoded as GOPs are all the same duration. In a number of embodiments each two second sequence of the source video is encoded as a GOP.

[0039] Adaptive streaming of source media encoded in the manner outlined above can be coordinated by a playback device in accordance with embodiments of the invention. The playback device obtains information concerning each of the available streams from the top level index file and selects one or more streams to utilize in the playback of the media. The playback device can then obtain header information from the Matroska container files containing the one or more bitstreams or streams, and the headers provide information concerning the decoding of the streams including a DRM header, which contains the cryptographic information utilized to protect the stream. The playback device can also request index information that indexes the encoded media stored within the relevant Matroska container files. The index information can be stored within the Matroska container files or separately from the Matroska container files in the top level index or in separate index files. The index information enables the playback device to request byte ranges corresponding to Cluster elements within the Matroska container file containing specific portions of encoded media via HTTP from the server. As the playback device receives the Cluster elements from the HTTP server, the playback device can evaluate current streaming conditions to determine whether to increase or decrease the bitrate of the streamed media. In the event that the playback

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1055
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

device determines that a change in bitrate is necessary, the playback device can obtain header information and index information for the container file(s) containing the desired stream(s) (assuming the playback device has not already obtained this information). The playback device need not perform the computationally intensive process of accessing the encrypted cryptographic information in the header of the new stream, because each of the alternative streams uses common cryptographic information. The index information can then be used to identify the byte range of the Cluster element containing the next portion of the source media encoded at the desired bit rate and the identified Cluster element can be retrieved from the server via HTTP. The next portion of the source media that is requested is typically identified based upon the Cluster elements already requested by the playback device and the Cluster elements buffered by the playback device. The next portion of source media requested from the alternative stream is requested to minimize the likelihood that the buffer of the playback device will underflow (i.e. run out media to playback) prior to receipt of the Cluster element containing the next portion of source media by the playback device. In this way, the playback device can achieve adaptive bitrate streaming by retrieving sequential Cluster elements from the various streams as appropriate to the streaming conditions using the top level index and index information describing the Cluster elements within each of the Matroska container files.

[0040] In a number of embodiments, variation in the bitrate between different streams can be achieved by modifying the encoding parameters for each stream including but not limited to the bitrate, frame rate, resolution and sample aspect ratio. The encoding and protection of source video using common cryptographic information for use in adaptive bitrate streaming and the playback of alternative streams of protected content via adaptive bitrate streaming in accordance with embodiments of the invention is discussed further below.

ADAPTIVE STREAMING SYSTEM ARCHITECTURE

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1056
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

[0041] An adaptive bitrate streaming system in accordance with an embodiment of the invention is illustrated in FIG. 1. The adaptive streaming system 10 includes a source encoder 12 configured to encode source media as a number of alternative streams and to protect the encoded streams using common cryptographic information. Alternative streams are streams that encode the same media content in different ways. In several embodiments, the source encoder 12 ingests source content and obtains a title ID and common cryptographic information from a content distribution server 14 that the content distribution server assigns to the source content. The source encoder encodes the alternative streams and protects the streams using the common cryptographic information received from the content distribution server. In many instances, alternative streams encode media content (such as but not limited to video) at different maximum bitrates. In a number of embodiments, the alternative streams are encoded with different resolutions, sample aspect ratios and/or frame rates. When the streams are written to file(s), the common cryptographic information is also written to the file(s). The content distribution server 14 can receive request to access the alternative streams of content (i.e. the title) via the Internet from a playback device such as (but not limited to) a user computer 18 or a mobile phone 20 and can commence streaming content. In several embodiments, the common cryptographic information is protected by encrypting at least a portion of the common cryptographic information using at least one encryption key. The playback device can securely obtain the cryptographic key using a process such as (but not limited to) Hypertext Transfer Protocol Secure or HTTPS. Other processes for securely obtaining cryptographic information to obtain access to encrypted common cryptographic information in accordance with embodiments of the invention are discussed below.

[0042] In many embodiments, a playback device commences playback by requesting a top level index file from the content distribution server. The source encoder 12, the content distribution server 14, or another server can generate the top level index to the file(s) containing the streams, at least a plurality of which are alternative streams, at

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1057
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

the time the request is made or at the time the streams are generated by the source encoder. The playback device can then use HTTP or another appropriate stateless protocol to request portions of the top level index file and the file(s) containing the protected streams via a network 16 such as the Internet.

[0043] In many embodiments, the top level index file is a SMIL file and the media is stored in Matroska container files. As is discussed further below, the media can be stored within the Matroska container file in a way that facilitates the protection of the content using common cryptographic information. In many embodiments, the Matroska container files are specialized Matroska container files that include enhancements (i.e. elements that do not form part of the Matroska file format specification) that facilitate retrieval and decryption using common cryptographic information of specific portions of media during adaptive bitrate streaming.

[0044] Although a specific content distribution system configured to support adaptive bitrate streaming is illustrated in FIG. 1A, any of a variety of content distribution system architectures can be utilized to implement an adaptive bitrate streaming system in accordance with embodiments of the invention. Source encoders, content distribution server systems, and playback devices in accordance with embodiments of the invention are discussed further below.

SOURCE ENCODERS

[0045] In many embodiments, a source encoder can be implemented using a server. In other embodiments, the source encoder can be any processing device including a processor and sufficient resources to perform the transcoding and encryption of source media (including but not limited to video, audio, and/or subtitles). A source encoder in accordance with an embodiment of the invention is illustrated in FIG. 1B. The source encoder 12 is implemented on a computing platform including a processor 12a, volatile memory 12b and non-volatile storage 12c. An encoder application 12d is stored in non-volatile storage 12c. The encoder application includes the machine readable

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1058
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

instructions that configure the processor to encode source content 12e as a plurality of streams. In a number of embodiments, the encoder application also configures the source encoder to obtain common cryptographic information 12g that can be utilized to protect alternative streams generated using the source content 12e. In many embodiments, the source encoder obtains the common cryptographic information and a title ID from a content distribution system. In other embodiments, the source encoder generates a title ID and/or cryptographic data and provides the generated information to a content distribution system.

[0046] Although a specific source encoder in accordance with embodiments of the invention is illustrated in FIG. 1B, any of a variety of computing platforms can be utilized to implement a source encoder that is configured to encode at least one stream of source content as a plurality of alternative streams and to protect each of the alternative streams using common cryptographic information in accordance with embodiments of the invention.

CONTENT DISTRIBUTION SERVERS

[0047] Content distribution servers in accordance with embodiments of the invention can be responsible for storing protected streams of content for streaming to playback devices using adaptive bitrate streaming processes. Content distribution servers can also store common cryptographic information utilized to protect the alternative streams of protected content. In several embodiments, the common cryptographic information is identified utilizing a title ID associated with the common cryptographic information and a set of streams that form part of a specific title or piece of content. A content distribution server in accordance with an embodiment of the invention is illustrated in FIG. 1C. The content distribution server is implemented using a computing platform including a processor 14a, volatile memory 14b, and non-volatile storage 14c. In the illustrated embodiment, a plurality of container files 14d are stored on the content distribution server. Playback devices can stream content from the content distribution

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1059
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

server utilizing adaptive bitrate streaming processes in accordance with embodiments of the invention. To facilitate the creation of new streams with respect to a specific piece of content, the content distribution server also stores title IDs 14e for specific pieces of content and common cryptographic information 14f associated with each title ID. A source encoder can request common cryptographic information to protect a new stream related to a specific piece of content, by providing a request to the content distribution server that identifies the specific piece of content using the title ID assigned to it.

[0048] Although a specific content distribution server is illustrated in FIG. 1C, any of a variety of computational platform including (but not limited to) platforms in which container files and common cryptographic information are stored on separate servers can be utilized in content distribution systems in accordance with embodiments of the invention.

PLAYBACK DEVICES

[0049] Referring back to FIG. 1A, the illustrated playback devices include personal computers 18 and mobile phones 20. In other embodiments, playback devices can include consumer electronics devices such as DVD players, Blu-ray players, televisions, set top boxes, video game consoles, tablets, and other devices that are capable of playing back protected media stored on a content distribution server using adaptive bitrate streaming. A playback device in accordance with an embodiment of the invention is illustrated in FIG. 1D. The playback device is implemented on a processing platform 20 including a processor 20a, volatile memory 20b, and non-volatile memory (or other non-volatile storage) 20c. The non-volatile memory 20c contains a client application 20d, which includes machine readable instructions that can be utilized to configure the processor to register with a content distribution system to obtain cryptographic data 20e bound to the playback device. The playback device can then use the bound cryptographic data 20e to request adaptive bitrate streaming of protected

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1060
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

content. As is discussed further below, the alternative streams of protected content utilized to perform adaptive bitrate streaming are protected using common cryptographic information. Once the client application 20d has obtained the common cryptographic information, which can be a time consuming and/or computationally intensive process, the playback device can use the same cryptographic information to access content in any of the alternative streams of protected content within a single instance of a title.

[0050] Although a specific architecture for a playback device is shown in FIG. 1D any of a variety of architectures can be utilized that enable playback devices to request portions of the top level index file and the container files in accordance with embodiments of the invention.

FILE STRUCTURE

[0051] Files generated by a source encoder and/or stored on an HTTP server for streaming to playback devices in accordance with embodiments of the invention are illustrated in FIG. 2. The files utilized in the adaptive bitrate streaming of the source media include a top level index 30 and a plurality of container files 32 that each contain at least one stream. The top level index file describes the content of each of the container files. As is discussed further below, the top level index file can take a variety of forms including an SMIL file and the container files can take a variety of forms including a specialized Matroska container file.

[0052] In many embodiments, each Matroska container file contains a single protected stream. For example, the stream could be one of a number of alternate video streams protected using common cryptographic information, an audio stream, one of a number of alternate audio streams, a subtitle stream, one of a number of alternate subtitle streams, a trick play stream, or one of a number of alternate trick play streams protected using common cryptographic information. In several embodiments, the Matroska container file includes multiple multiplexed streams. For example, the

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1061
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Matroska container could include a video stream, and one or more audio streams, one or more subtitle streams, and/or one or more trick play streams. As is discussed further below, in many embodiments the Matroska container files are specialized files. The encoding of the media and the manner in which the media is stored within Cluster elements within the Matroska container file can be subject to constraints designed to enhance the performance of an adaptive bitrate streaming system. In a number of embodiments, common cryptographic information is included within a DRM header element in each of the Matroska container files and references to the common cryptographic information are made using DRMInfo elements included within BlockGroup elements of protected (not all frames need be protected to protect the stream). In addition, the Matroska container file can include index elements that facilitate the location and downloading of Cluster elements from the various Matroska container files during the adaptive streaming of the media. Top level index files and Matroska container files that can be used in adaptive bitrate streaming systems in accordance with embodiments of the invention are discussed below.

TOP LEVEL INDEX FILES

[0053] Playback devices in accordance with many embodiments of the invention utilize a top level index file to identify the container files that contain the streams available to the playback device for use in adaptive bitrate streaming. In many embodiments, the top level index files can include references to container files that each include an alternative stream of encoded media. The playback device can utilize the information in the top level index file to retrieve encoded media from each of the container files according to the streaming conditions experienced by the playback device.

[0054] In several embodiments, the top level index file provides information enabling the playback device to retrieve information concerning the encoding of the media in each of the container files and an index to encoded media within each of the container

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1062
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

files. In a number of embodiments, each container file includes information concerning the encoded media contained within the container file and an index to the encoded media within the container file and the top level index file indicates the portions of each container file containing this information. Therefore, a playback device can retrieve the top level index file and use the top level index file to request the portions of one or more of the container files that include information concerning the encoded media contained within the container file and an index to the encoded media within the container file. A variety of top level index files that can be utilized in adaptive bitrate streaming systems in accordance with embodiments of the invention are discussed further below.

[0055] In a number of embodiments, the top level index file utilized in the adaptive bitrate streaming of media is a SMIL file, which is an XML file that includes a list of URIs describing each of the streams and the container files that contain the streams. The URI can include information such as the "system-bitrate" of the stream contained within the stream and information concerning the location of specific pieces of data within the container file. The top level index SMIL file can be generated when the source media is encoded for playback via adaptive bitrate streaming. Alternatively, the top level index SMIL file can be generated when a playback device requests the commencement of playback of the encoded media. When the playback device receives the top level index SMIL file, the playback device can parse the SMIL file to identify the available streams. The playback device can then select the streams to utilize to playback the content and can use the SMIL file to identify the portions of the container file to download to obtain information concerning the encoding of a specific stream and/or to obtain an index to the encoded media within the container file.

[0056] Although top level index SMIL files are described above, any of a variety of top level index file formats can be utilized to create top level index files as appropriate to a specific application in accordance with an embodiment of the invention. The use of top level index files to enable playback of encoded media using adaptive bitrate streaming in accordance with embodiments of the invention is discussed further below.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1063
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

STORING PROTECTED MEDIA IN MKV FILES FOR ADAPTIVE BITRATE STREAMING

[0057] A Matroska container file used to store encoded video in accordance with an embodiment of the invention is illustrated in FIG. 3. The container file 32 is an Extensible Binary Markup Language (EBML) file that is an extension of the Matroska container file format. The specialized Matroska container file 32 includes a standard EBML element 34, and a standard Segment element 36 that includes a standard Seek Head element 40, a standard Segment Information element 42, and a standard Tracks element 44 including a tracks data payload that is a non-standard EBML element containing cryptographic information utilized to access the protected stream(s) contained within the Matroska container file. In many embodiments, the cryptographic data takes the form of a DRMHeaders element (discussed below) that includes a set of keys utilized to access encrypted portions of the stream contained within the Matroska container file. In many embodiments, the set of keys is encrypted in such a way that a playback device can only access the set of keys in the clear using a specific piece or set of cryptographic information.

[0058] The Segment element 36 also includes a standard Clusters element 46. As is described below, the manner in which encoded media is inserted within individual Cluster elements 48 within the Clusters element 46 is constrained to improve the playback of the media in an adaptive streaming system. In many embodiments, the constraints imposed upon the encoded video are consistent with the specification of the Matroska container file format and involve encoding the video so that each cluster includes at least one closed GOP commencing with an IDR frame. In addition to the above elements, the Segment element 36 can optionally include a modified version of the standard Cues element. As is discussed further below, the Cues element includes specialized CuePoint elements (i.e. non-standard CuePoint elements) that facilitate the retrieval of the media contained within specific Cluster elements via HTTP. The Segment element 36 can optionally include a non-standard Hierarchical Index element

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1064
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

54. The Hierarchical Index element is an extension to the Matroska file format proposed by DivX, LLC of San Diego, California. The Hierarchical Index element is described in U.S. Patent Application Serial No. 12/272,631, the disclosure of which is incorporated by reference above in its entirety.

[0059] The constraints imposed upon the encoding of media and the formatting of the encoded media within the Clusters element of a Matroska container file for adaptive bitrate streaming of protected streams and the additional DRM and index information inserted within the container file in accordance with embodiments of the invention are discussed further below.

ENCODING MEDIA FOR INSERTION IN CLUSTER ELEMENTS

[0060] An adaptive bitrate streaming system provides a playback device with the option of selecting between different protected streams of encoded media during playback according to the streaming conditions experienced by the playback device. In many embodiments, switching between protected streams is facilitated by separately pre-encoding discrete portions of the source media in accordance with the encoding parameters of each stream and then including each separately encoded portion in its own Cluster element within the stream's container file. Furthermore, the media contained within each Cluster is encoded so that the media is capable of playback without reference to media contained in any other Cluster within the stream. In this way, each stream includes a Cluster element corresponding to the same discrete portion of the source media and, at any time, the playback device can select the Cluster element from the stream that is most appropriate to the streaming conditions experienced by the playback device and can commence playback of the media contained within the Cluster element. Accordingly, the playback device can select clusters from different streams as the streaming conditions experienced by the playback device change over time. In several embodiments, the Cluster elements are further constrained so that each Cluster element contains a portion of encoded media from the

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1065
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

source media having the same duration. In a number of embodiments, each Cluster element includes two seconds of encoded media. The specific constraints applied to the media encoded within each Cluster element depending upon the type of media (i.e. video, audio, or subtitles) are discussed below.

[0061] A Clusters element of a Matroska container file containing a video stream in accordance with an embodiment of the invention is illustrated in FIG. 4a. The Clusters element 46 includes a plurality of Cluster elements 48 that each contains a discrete portion of encoded video. In the illustrated embodiment, each Cluster element 48 includes two seconds of encoded video. In other embodiments, the Cluster elements include encoded video having a greater or lesser duration than two seconds. In several embodiments, the encoded video sequences in the Cluster elements have different durations.

[0062] Each Cluster element 48 includes a Timecode element 60 indicating the start time of the encoded video within the Cluster element and a plurality of BlockGroup elements. As noted above, the encoded video stored within the Cluster is constrained so that the encoded video can be played back without reference to the encoded video contained within any of the other Cluster elements in the container file. In many embodiments, encoding the video contained within the Cluster element as a GOP in which the first frame is an IDR frame enforces the constraint. In the illustrated embodiment, the first BlockGroup element 62 contains an IDR frame. Therefore, the first BlockGroup element 62 does not include a ReferenceBlock element. The first BlockGroup element 62 includes a Block element 64, which specifies the Timecode attribute of the frame encoded within the Block element 64 relative to the Timecode of the Cluster element 48 and a DRMInfo element 65 that identifies a portion of the frame that is encrypted and the cryptographic information that can be utilized to access the encrypted portion of the frame. In a number of embodiments, only a small portion of the video frame is encrypted and the DRMInfo includes a reference to the start of an encrypted block of data and the size of the encrypted block of data. As is discussed

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1066
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

further below, the common cryptographic information utilized to protect alternative streams of video content is a set of frame keys in many embodiments of the invention and the DRMInfo element can also include an index to a specific frame key in the set of frame keys that can be utilized to access the encrypted block of data in the clear. In other embodiments, any of a variety of information appropriate to identifying encrypted data within a video frame and decrypting the encrypted data can be stored within a DRMInfo element.

[0063] Subsequent BlockGroup elements 66 are not restricted in the types of frames that they can contain (other than that they cannot reference frames that are not contained within the Cluster element). Therefore, subsequent BlockGroup elements 66 can include ReferenceBlock elements 68 referencing other BlockGroup element(s) utilized in the decoding of the frame contained within the BlockGroup or can contain IDR frames and are similar to the first BlockGroup element 62. In addition, subsequent BlockGroup elements 66 can also include DRMInfo elements to describe the manner in which the frame of video contained within the BlockGroup element is protected. As noted above, the manner in which encoded video is inserted within the Cluster elements of the Matroska file conforms with the specification of the Matroska file format.

[0064] The insertion of encoded audio and subtitle information within a Clusters element 46 of a Matroska container file in accordance with embodiments of the invention is illustrated in FIGS. 4b and 4c. In the illustrated embodiments, the encoded media is inserted within the Cluster elements 48 subject to the same constraints applied to the encoded video discussed above with respect to FIG. 4a. In addition, the duration of the encoded audio and subtitle information within each Cluster element corresponds to the duration of the encoded video in the corresponding Cluster element of the Matroska container file containing the encoded video. In other embodiments, the Cluster elements within the container files containing the audio and/or subtitle streams need not correspond with the start time and duration of the Cluster elements in the container files containing the alternative video streams. In many embodiments, audio,

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1067
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

and/or subtitle tracks are protected and information identifying the protected portions of the stream can be included in an element in a manner similar to that described above with respect to protected video streams.

MULIPLEXING STREAMS IN A SINGLE MKV CONTAINER FILE

[0065] The Clusters elements shown in FIGS. 4a – 4c assume that a single stream is contained within each Matroska container file. In several embodiments, media from multiple streams is multiplexed within a single Matroska container file. In this way, a single container file can contain a video stream multiplexed with one or more corresponding audio streams, and/or one or more corresponding subtitle streams. Storing the streams in this way can result in duplication of the audio and subtitle streams across multiple alternative video streams. However, the seek time to retrieve encoded media from a video stream and an associated audio, and/or subtitle stream can be reduced due to the adjacent storage of the data on the server. The Clusters element 46 of a Matroska container file containing multiplexed video, audio and subtitle data in accordance with an embodiment of the invention is illustrated in FIG. 4d. In the illustrated embodiment, each Cluster element 48 includes additional BlockGroup elements for each of the multiplexed streams. The first Cluster element includes a first BlockGroup element 62v for encoded video that includes a Block element 64v containing an encoded video frame and indicating the Timecode attribute of the frame relative to the start time of the Cluster element (i.e. the Timecode attribute 60). A second BlockGroup element 62a includes a Block element 64a including an encoded audio sequence and indicating the timecode of the encoded audio relative to the start time of the Cluster element, and a third BlockGroup element 62s including a Block element 64s containing an encoded subtitle and indicating the timecode of the encoded subtitle relative to the start time of the Cluster element. In the illustrated embodiment, only the video stream is protected. Therefore, the BlockGroup elements 62v containing the video stream include DRMInfo elements 65v to identify the portions of the frames within

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1068
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

the video stream that are encrypted. In other embodiments, the audio, and/or subtitle streams can also be protected. Although not shown in the illustrated embodiment, each Cluster element 48 likely would include additional BlockGroup elements containing additional encoded video, audio or subtitles. Despite the multiplexing of the encoded video, audio, and/or subtitle streams, the same constraints concerning the encoded media apply.

INCORPORATING TRICK PLAY STREAMS IN MKV CONTAINER FILES FOR USE IN ADAPTIVE BITRATE STREAMING SYSTEMS

[0066] The incorporation of trick play tracks within Matroska container files is proposed by DivX, LLC in U.S. Patent Application No. 12/260,404 entitled "Application Enhancement Tracks", filed October 29, 2008, the disclosure of which is hereby incorporated by reference in its entirety. Trick play tracks similar to the trick play tracks described in U.S. Patent Application No. 12/260,404 can be used to provide a trick play stream in an adaptive bitrate streaming system in accordance with an embodiment of the invention to provide smooth visual search through source content encoded for adaptive bitrate streaming. A separate trick play stream can be encoded that appears to be an accelerated visual search through the source media when played back, when in reality the trick play stream is simply a separate stream encoding the source media at a lower frame rate. In several embodiments, a trick play stream is generated in the manner outlined in U.S. Patent Application No. 12/260,404 and inserting the trick play stream into a Matroska container file subject to the constraints mentioned above with respect to insertion of a video stream into a Matroksa container file. In many embodiments, the trick play stream is also subject to the further constraint that every frame in the GOP of each Cluster element in the trick play stream is encoded as an IDR frame. As with the other video streams, each Cluster element contains a GOP corresponding to the same two seconds of source media as the corresponding Cluster elements in the other streams. There are simply fewer frames in the GOPs of the trick

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1069
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

play stream and each frame has a longer duration. In this way, transitions to and from a trick play stream can be treated in the same way as transitions between any of the other encoded streams are treated within an adaptive bitrate streaming system in accordance with embodiments of the invention. In embodiments where the trick play stream(s) are protected, the same common cryptographic information utilized to encrypt the primary video stream(s) is utilized to protect the trick play stream(s). Playback of the frames contained within the trick play stream to achieve accelerated visual search typically involves the playback device manipulating the timecodes assigned to the frames of encoded video prior to providing the frames to the playback device's decoder to achieve a desired increase in rate of accelerated search (e.g. x2, x4, x6, etc.).

[0067] A Clusters element containing encoded media from a trick play stream is shown in FIG. 4e. In the illustrated embodiment, the encoded trick play stream is inserted within the Cluster elements 48 subject to the same constraints applied to the encoded video discussed above with respect to FIG. 4a including the constraint that frames are protected using the common cryptographic information. However, each BlockGroup element contains an IDR. In other embodiments, the Cluster elements within the container files containing the trick play streams need not correspond with the start time and duration of the Cluster elements in the container files containing the alternative video streams.

[0068] In many embodiments, source content can be encoded to provide a single trick play stream or multiple trick play streams for use by the adaptive bit rate streaming system. When a single trick play stream is provided, the trick play stream is typically encoded at a low bitrate. When multiple alternative trick play streams are provided, adaptive streaming can also be performed with respect to the trick play streams. In several embodiments, multiple trick play streams are provided to support different rates of accelerated visual search through the encoded media.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1070
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

INCORPORATING INDEXING INFORMATION WITHIN MKV CONTAINER FILES

[0069] The specification for the Matroska container file format provides for an optional Cues element that is used to index Block elements within the container file. A modified Cues element that can be incorporated into a Matroska container file in accordance with an embodiment of the invention to facilitate the requesting of clusters by a playback device using HTTP is illustrated in FIG. 5. The Cues element 52 is similar to a standard Cues element 52 in that it includes a plurality of standard CuePoint elements 70 that each include a standard CueTime attribute 72. Each CuePoint element includes a CueTrackPositions element 74 containing the standard CueTrack 76 and CueClusterPosition 78 attributes. In many embodiments, the CuePoint element is mainly configured to identify a specific Cluster element as opposed to a specific Block element within a Cluster element. Although, in several applications the ability to seek to specific Block elements within a Cluster element is required and additional index information is included in the Cues element.

[0070] The use of a modified Cues element to index encoded media within a Clusters element of a Matroska file in accordance with an embodiment of the invention is illustrated in FIG. 6. A CuePoint element is generated to correspond to each Cluster element within the Matroska container file. The CueTime attribute 72 of the CuePoint element 70 corresponds to the Timecode attribute 60 of the corresponding Cluster element 48. In addition, the CuePoint element contains a CueTrackPositions element 74 having a CueClusterPosition attribute 78 that points to the start of the corresponding Cluster element 48. The CueTrackPositions element 74 can also include a CueBlockNumber attribute, which is typically used to indicate the Block element containing the first IDR frame within the Cluster element 48.

[0071] As can readily be appreciated the Cues element 52 forms an index to each of the Cluster elements 48 within the Matroska container file. Furthermore, the CueTrackPosition elements provide information that can be used by a playback device to request the byte range of a specific Cluster element 48 via HTTP or another suitable

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1071
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

protocol from a remote server. The Cues element of a conventional Matroska file does not directly provide a playback device with information concerning the number of bytes to request from the start of the Cluster element in order to obtain all of the encoded video contained within the Cluster element. The size of a Cluster element is, therefore, inferred by using the CueClusterPosition attribute of the CueTrackPositions element that indexes the first byte of the next Cluster element. Alternatively, additional CueTrackPosition elements could be added that index the last byte of the Cluster element (in addition to the CueTrackPositions elements that index the first byte of the Cluster element), and/or a non-standard CueClusterSize attribute that specifies the size of the Cluster element pointed to by the CueClusterPosition attribute is included in each CueTrackPosition element to assist with the retrieval of specific Cluster elements within a Matroska container file via HTTP byte range requests or a similar protocol.

[0072] The modification of the Cues element in the manner outlined above significantly simplifies the retrieval of Cluster elements from a Matroska container file via HTTP or a similar protocol during adaptive bitrate streaming. In addition, by only indexing the first frame in each Cluster the size of the index is significantly reduced. Given that the index is typically downloaded prior to playback, the reduced size of the Cues element (i.e. index) means that playback can commence more rapidly. Using the CueClusterPosition elements, a playback device can request a specific Cluster element from the stream most suited to the streaming conditions experienced by the playback device by simply referencing the index of the relevant Matroska container file using the Timecode attribute for the desired Cluster element.

[0073] A number of the attributes within the Cues element are not utilized during adaptive bitrate streaming. Therefore, the Cues element can be further modified by removing the unutilized attributes to reduce the overall size of the index for each Matroska container file. A modified Cues element that can be utilized in a Matroska container file that includes a single encoded stream, where portions of the encoded stream having the same duration are contained in each Cluster element within the

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1072
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Matroska file in accordance with an embodiment of the invention is illustrated in FIG. 5a. The Cues element 52' shown in FIG. 5a is similar to the Cues element 52 shown in FIG. 5 with the exception that the CuePoint elements 70' do not include a CueTime attribute (see 72 in FIG. 5) and/or the CueTrackPositions elements 74' do not include a CueTrack attribute (76 in FIG. 5). When the portions of encoded media in each Cluster element in the Matroska container file have the same duration, the CueTime attribute is not necessary. When the Matroska contain file includes a single encoded stream, the CueTrack attribute is not necessary. In other embodiments, the Cues element and/or other elements of the Matroska container file can be modified to remove elements and/or attributes that are not necessary for the adaptive bitrate streaming of the encoded stream contained within the Matroska container file, given the manner in which the stream is encoded and inserted in the Matroska container file.

[0074] Although various modifications to the Cues element to include information concerning the size of each of the Cluster elements within a Matroska container file and to eliminate unnecessary attributes are described above, many embodiments of the invention utilize a conventional Matroska container. In several embodiments, the playback device simply determines the size of Cluster elements on the fly using information obtained from a conventional Cues element, and/or relies upon a separate index file containing information concerning the size and/or location of the Cluster elements within the MKV container file. In several embodiments, the additional index information is stored in the top level index file. In a number of embodiments, the additional index information is stored in separate files that are identified in the top level index file. When index information utilized to retrieve Cluster elements from a Matroska container file is stored separately from the container file, the Matroska container file is still typically constrained to encode media for inclusion in the Cluster elements in the manner outlined above. In addition, wherever the index information is located, the index information will typically index each Cluster element and include (but

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1073
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

not be limited to) information concerning at least the starting location and, in many instances, the size of each Cluster element.

INCORPORATING HIERARCHICAL INDEXES INTO MKV CONTAINERS

[0075] Retrieval of media using HTTP during adaptive streaming can be improved by adding additional index information to the Matroska container files used to contain each of the encoded streams. In a number of embodiments, the index is a reduced index in that the index only points to the IDRs at the start of each cluster. In many embodiments, the index of the Matroska container file includes additional non-standard attributes (i.e. attributes that do not form part of the Matroska container file format specification) that specify the size of each of the clusters so that a playback device can retrieve a Cluster element from the Matroska container file via HTTP using a byte range request. In several embodiments, the Matroska container file includes a hierarchical index using a HierarchicalIndex element similar to the hierarchical indexes disclosed in U.S. Patent Application Serial No. 12/272,631 entitled "Hierarchical and Reduced Index Structures for Multimedia Files" to Soroushian et al. filed November 17, 2008 to increase the speed with which a playback device can seek to a specific Cluster element containing encoded media within the container file. The disclosure of U.S. Patent Application Serial No. 12/272,631 is herby incorporated by reference in its entirety.

[0076] A hierarchical index included in a Matroska container file using a HierarchicalIndex element in accordance with an embodiment of the invention is illustrated in FIG. 7. The HierarchicalIndex element 54 includes a plurality of HierarchicalIndexPointer elements 80 that each point to a CuePoint element 70 within the Cues element 52. In this way, the hierarchical index can be utilized to rapidly locate specific Cluster elements within a Matroska file using the Timecode attribute of the Cluster element. Furthermore, the entire index (i.e. the entire Cues element) need not be downloaded in order to locate a specific Cluster element. The playback device can

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1074
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

simply download the hierarchical index and download the specific CuePoint elements that enable the location of a desired Cluster element within the Matroska container file.

[0077] In several embodiments, the HierarchicalIndex element is generated so that the HierarchicalIndexPointer elements point to CuePoint elements indexing Cluster elements that are a predetermined time period apart. For example, the HierarchicalIndexPointer elements can point to CuePoint elements indexing Cluster elements that are spaced 30 seconds apart. In other implementations, any of a variety of implementations can be utilized to determine the interval between the CuePoint elements referenced by the higher layers of the hierarchical index. In addition, although a two layer hierarchical index is illustrated in FIG. 7, hierarchical indexes including three or more layers can also be incorporated within Matroska container files generated for use in adaptive bitrate streaming systems in accordance with embodiments of the invention.

[0078] As noted above, index information can be stored in a separate file to the Matroska container file in accordance with embodiments of the invention. In embodiments where the index information is stored separately, the index can be hierarchical to prevent the need to download the entire index for a container file prior to playback and to facilitate seeking within the index.

ENCODING AND PROTECTING SOURCE MEDIA FOR ADAPTIVE BITRATE STREAMING

[0079] A process for encoding source media as a top level index file and a plurality of Matroska container files for use in an adaptive bitrate streaming system in accordance with an embodiment of the invention is illustrated in FIG. 8. The encoding process 100 commences by writing headers for each of the MKV files that will contain the streams of content generated using the source content. In the illustrated embodiment, the source content includes a stream of video that is encoded as a plurality of protected streams. The frames of the source video are encoded (104) using the encoding parameters associated with each of the alternative streams and portions of the encoded frames can

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1075
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

be encrypted using a frame key selected from a set of frame keys. When the encoding and encryption of the streams is complete, an index is inserted (106) into each Matroska container file containing an alternative stream of protected video. The common set of frame keys is also encrypted (108) and the process writes (110) a DRM header including the encrypted set of frame keys to each container file. DRM headers and processes for restricting access to cryptographic information stored within the DRM header of a Matroska container file in accordance with embodiments of the invention are discussed further below.

[0080] A process for encoding and protecting frames of video to create a plurality of alternative streams of protected video in accordance with embodiments of the invention is illustrated in FIG. 9. The process 120 includes selecting (122) a first portion of the source media and encoding (123) the source media using the encoding parameters for each alternative stream. Assuming that the resulting frame is to be encrypted, a frame key can be selected (124) from a common set of frame keys and utilized to encrypt at least a portion of the frame of video. A DRMInfo element can then be written (125) to a BlockGroup element. The DRMInfo element identifies the portion of the frame that is encrypted and the frame key that can be utilized by a playback device to access the encrypted portion of the frame. The encoded and/or encrypted frame can then be written (126) to the BlockGroup element. When the entire source video stream is determined (127) as being encoded and protected, then the process is complete.

[0081] Each portion of source video that is encoded (123) can be encoded as a single GOP commencing with an IDR frame. In many embodiments, encoding parameters used to create the alternative GOPs vary based upon bitrate, frame rate, encoding parameters and resolution. In this way, the portion of media is encoded as a set of interchangeable alternatives and a playback device can select the alternative most appropriate to the streaming conditions experienced by the playback device. When different resolutions are supported, the encoding of the streams is constrained so that each stream has the same display aspect ratio. A constant display aspect ratio can be

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1076
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

achieved across different resolution streams by varying the sample aspect ratio with the resolution of the stream. In many instances, reducing resolution can result in higher quality video compared with higher resolution video encoded at the same bit rate.

[0082] Although specific processes involving the encoding and protection of a source video stream as a set of alternative streams are illustrated in FIGS. 8 and 9, any of a variety of processes can be utilized to protect audio, video, and/or subtitle streams using common cryptographic information in accordance with embodiments of the invention. Following the encoding of the source media to create Matroska container files containing each of the protected streams, which can include trick play streams, the Matroska container files can be uploaded to a content distribution server for adaptive bitrate streaming to playback devices. The adaptive bitrate streaming of protected media encoded in accordance with embodiments of the invention using HTTP requests is discussed further below.

DRM HEADERS

[0083] Common cryptographic information utilized in protecting alternative streams can be inserted into container files containing each of the alternative streams. When the container files are Matroska container files, the common cryptographic information can be inserted into the container file as a DRMHeader element. A DRMHeader element configured to contain a set of keys in accordance with an embodiment of the invention is illustrated in FIG. 10. The DRM Header element 130 includes a plurality of pieces of information 132 including a frame keys record 134 that can be utilized to contain a set of frame keys or frame key table common to each of a plurality of alternative streams.

[0084] If the frame key record 134 is communicated in the clear, then any playback device can access the protected streams. Therefore, the frame keys record 134 is typically encrypted using one or more encryption keys. The encryption key(s) used to encrypt the frame key record 134 can be securely provided to an individual playback

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1077
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

device using any of a variety of techniques appropriate to a specific application. In the context of streaming systems that also support the downloading of content.

[0085] Although a specific format for storing common cryptographic information in a Matroska container file is illustrated in FIG. 10, any format can be utilized to store common cryptographic information in a Matroska container file and/or any other container file appropriate to a specific application in accordance with an embodiment of the invention. Adaptive bitrate streaming of protected content in accordance with embodiments of the invention is discussed further below.

ADAPTIVE BITRATE STREAMING FROM MKV CONTAINER FILES USING HTTP

[0086] When source media is encoded so that there are alternative streams of protected media contained in separate Matroska container files for at least one of video, audio, and subtitle content, adaptive streaming of the media contained within the Matroska container files can be achieved using HTTP requests or a similar stateless data transfer protocol. In many embodiments, a playback device requests a top level index file from a content distribution server and uses the index information to identify the streams that are available to the playback device and the cryptographic information required to access any protected streams. The playback device can then retrieve the indexes for one or more of the Matroska files and can use the indexes to request media from one or more of the protected streams contained within the Matroska container files using HTTP requests or using a similar stateless protocol. As noted above, many embodiment of the invention implement the indexes for each of the Matroska container files using a modified Cues element. In several embodiments, the index is a hierarchical index and is also includes a HierarchicalIndex element contained within the Matroska container file. In a number of embodiments, however, the encoded media for each stream is contained within a standard Matroska container file and separate index file(s) can also be provided for each of the container files.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1078
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

[0087] Based upon the streaming conditions experienced by the playback device, the playback device can select media from alternative protected streams encoded at different bitrates. When the media from each of the streams is protected using common cryptographic information and inserted into the Matroska container files in the manner outlined above, transitions between streams can occur upon the completion of playback of media within a Cluster element without the need to retrieve additional cryptographic information. As noted above, the size of the Cluster elements (i.e the duration of the encoded media within the Cluster elements) is typically chosen so that the playback device is able to respond quickly enough to changing streaming conditions and to instructions from the user that involve utilization of a trick play track. The smaller the Cluster elements (i.e. the smaller the duration of the encoded media within each Cluster element) the higher the overhead associated with requesting each Cluster element. Therefore, a tradeoff exists between the responsiveness of the playback device to changes in streaming conditions and the effective data rate of the adaptive streaming system for a given set of streaming conditions (i.e. the portion of the available bandwidth actually utilized to transmit encoded media). In many embodiments, the size of the Cluster elements is chosen so that each Cluster element contains two seconds of encoded media. In other embodiments, the duration of the encoded media can be greater or less than two seconds and/or the duration of the encoded media can vary from Cluster element to Cluster element.

[0088] Communication between a playback device or client and an HTTP server during the playback of media encoded in separate streams contained within Matroska container files indexed by a top level index file in accordance with an embodiment of the invention is illustrated in FIG. 11. In the illustrated embodiment, the playback device 200 commences playback by requesting the top level index file from the server 202 using an HTTP request or a similar protocol for retrieving data. The server 202 provides the bytes corresponding to the request. The playback device 200 then parses the top level index file to identify the URIs of each of the Matroska container files containing the

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1079
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

streams of encoded media derived from a specific piece of source media. The playback device can then request the byte ranges corresponding to headers of one or more of the Matroska container files via HTTP or a similar protocol, where the byte ranges are determined using the information contained in the URI for the relevant Matroska container files (see discussion above). The server returns the following information in response to a request for the byte range containing the headers of a Matroska container file:

```
ELEM("EBML")
 ELEM("SEEKHEAD")
 ELEM("SEGMENTINFO")
 ELEM("TRACKS")
```

[0089] The EBML element is typically processed by the playback device to ensure that the file version is supported. The SeekHead element is parsed to find the location of the Matroska index elements and the SegmentInfo element contains two key elements utilized in playback: TimecodeScale and Duration. The TimecodeScale specifies the timecode scale for all timecodes within the Segment of the Matroska container file and the Duration specifies the duration of the Segment based upon the TimecodeScale. The Tracks element contains the information used by the playback device to decode the encoded media contained within the Clusters element of the Matroska file including the common cryptographic information, which can take a variety of forms including but not limited to a DRMHeader element. As noted above, adaptive bitrate streaming systems in accordance with embodiments of the invention can support different streams encoded using different encoding parameters including but not limited to frame rate, and resolution. Therefore, the playback device can use the information contained within the Matroska container file's headers to configure the decoder every time a transition is made between encoded streams. Due to the fact that alternative protected streams utilize the same cryptographic information, the engine

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1080
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

utilized to decrypt the content on the client 200 (i.e. the software process used to decrypt encrypted portions of frames of video) does not require reconfiguration using different cryptographic information with each stream switch.

[0090] In many embodiments, the playback device does not retrieve the headers for all of the Matroska container files indexed in the top level index file. Instead, the playback device determines the stream(s) that will be utilized to initially commence playback and requests the headers from the corresponding Matroska container files. Depending upon the structure of the URIs contained within the top level index file, the playback device can either use information from the URIs or information from the headers of the Matroska container files to request byte ranges from the server that contain at least a portion of the index from relevant Matroska container files. The byte ranges can correspond to the entire index or can correspond to the top level of a hierarchical index and a portion of a lower level index (i.e. a HierarchicalIndex element and one or more CuePoint elements). The server provides the relevant byte ranges containing the index information to the playback device, and the playback device can use the index information to request the byte ranges of Cluster elements containing encoded media using this information. When the Cluster elements are received, the playback device can extract encoded media from the BlockGroup elements within the Cluster element, and can decode and playback the media within the BlockGroup elements in accordance with their associated Timecode attributes. Prior to decoding the encoded media, the playback device can check for the presence of a DRMInfo element within each BlockGroup of a video stream to identify whether the encoded media is protected. The playback device can use the information within the DRMInfo element to decrypt encrypted portions of the video prior to decoding.

[0091] In the illustrated embodiment, the playback device 200 requests sufficient index information from the HTTP server prior to the commencement of playback that the playback device can stream the entirety of each of the selected streams using the index information. In other embodiments, the playback device continuously retrieves

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1081
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

index information as media is played back. In several embodiments, all of the index information for the lowest bitrate steam is requested prior to playback so that the index information for the lowest bitrate stream is available to the playback device in the event that streaming conditions deteriorate rapidly during playback.

SWITCHING BETWEEN STREAMS

[0092] The communications illustrated in FIG. 11 assume that the playback device continues to request media from the same streams (i.e. Matroska container files) throughout playback of the media. In reality, the streaming conditions experienced by the playback device are likely to change during the playback of the streaming media and the playback device can request media from alternative streams (i.e. different Matroska container files) to provide the best picture quality for the streaming conditions experienced by the playback device. In addition, the playback device may switch streams in order to perform a trick play function that utilizes a trick play track stream.

[0093] Communication between a playback device and a server when a playback device switches to a new stream in accordance with embodiments of the invention are illustrated in FIG. 12a. The communications illustrated in FIG. 12a assume that the index information for the new stream has not been previously requested by the playback device and that downloading of Cluster elements from the old stream proceeds while information is obtained concerning the Matroska container file containing the new stream. When the playback device 200 detects a change in streaming conditions, determines that a higher bitrate stream can be utilized at the present streaming conditions, or receives a trick play instruction from a user, the playback device can use the top level index file to identify the URI for a more appropriate alternative stream to at least one of the video, audio, or subtitle streams from which the playback device is currently requesting encoded media. The playback device can save the information concerning the current stream(s) and can request the byte ranges of the headers for the Matroska container file(s) containing the new stream(s) using the parameters of the

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1082
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

corresponding URIs. Caching the information in this way can be beneficial when the playback device attempts to adapt the bitrate of the stream downward. When the playback device experiences a reduction in available bandwidth, the playback device ideally will quickly switch to a lower bitrate stream. Due to the reduced bandwidth experienced by the playback device, the playback device is unlikely to have additional bandwidth to request header and index information. Ideally, the playback device utilizes all available bandwidth to download already requested higher rate Cluster elements and uses locally cached index information to start requesting Cluster elements from Matroska container file(s) containing lower bitrate stream(s). When a hierarchical index is used, the playback device typically will download additional index information. However, the amount of index information that is downloaded is significantly reduced as the headers of the Matroska container file are already cached on the playback device and the playback device only needs a portion of the index in order commence requesting Cluster elements from the Matroska container file(s) containing the new stream(s).

[0094] Byte ranges for index information for the Matroska container file(s) containing the new stream(s) can be requested from the HTTP server 202 in a manner similar to that outlined above with respect to FIG. 11. At which point, the playback device can stop downloading of cluster elements from the previous streams and can commence requesting the byte ranges of the appropriate Cluster elements from the Matroska container file(s) containing the new stream(s) from the HTTP server, using the index information from the Matroska container file(s) to identify the Cluster element(s) containing the encoded media following the encoded media in the last Cluster element retrieved by the playback device. As noted above, the encoding of the alternative streams so that corresponding Cluster elements within alternative streams (i.e. Cluster elements containing the same portion of the source media encoded in accordance with different encoding parameters) start with the same Timecode element and an IDR frame facilitates the smooth transition from one stream to another. In addition, the use

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1083
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

of common cryptographic information further facilitates smooth switching between alternative streams.

[0095] When the Matroska file includes a hierarchical index, the process for switching between streams can involve downloading less than the entire index of the new streams. The index information can be downloaded by requesting the byte range for the hierarchical index and then using the Timecode attribute of media played back by the playback device 200 to identify the location of CuePoint elements within the Matroska container file(s) containing the new stream(s) that reference Cluster elements containing sequential encoded media and requesting the byte ranges of the CuePoint elements from the HTTP server 202. After the HTTP server has provided the byte ranges including the CuePoint elements, the playback device can use the information within the CuePoint elements to request byte ranges containing desired Cluster elements from the HTTP server. At which point, playback of the encoded media contained within the Cluster elements proceeds in the manner discussed above.

[0096] When the playback device caches the header and the entire index for each stream that has be utilized in the playback of the media, the process of switching back to a previously used stream can be simplified. The playback device already has the header and index information for the Matroska file containing the previously utilized stream and the playback device can simply use this information to start requesting Cluster elements from the Matroska container file of the previously utilized stream via HTTP. Communication between a playback device and an HTTP server when switching back to a stream(s) for which the playback device has cached header and index information in accordance with an embodiment of the invention is illustrated in FIG. 12b. The process illustrated in FIG. 12b is ideally performed when adapting bitrate downwards, because a reduction in available resources can be exacerbated by a need to download index information in addition to media. The likelihood of interruption to playback is reduced by increasing the speed with which the playback device can switch between streams and reducing the amount of overhead data downloaded to achieve the

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1084
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

switch. When a hierarchical index is utilized, the playback device requests the appropriate portion of the index from the Matroska container file(s) containing the lower bitrate stream(s) prior to requesting Cluster elements from the Matroska container file.

[0097] Although the present invention has been described in certain specific aspects, many additional modifications and variations would be apparent to those skilled in the art. It is therefore to be understood that the present invention may be practiced otherwise than specifically described, including various changes in the implementation such as utilizing encoders and decoders that support features beyond those specified within a particular standard with which they comply, without departing from the scope and spirit of the present invention. Thus, embodiments of the present invention should be considered in all respects as illustrative and not restrictive.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1085
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

WHAT IS CLAIMED:

1. A source encoder, comprising:

a processor;

non-volatile storage containing an encoding application;

wherein the encoding application configures the processor to:

receive source content;

obtain common cryptographic information;

encode the source content as a plurality of streams including a plurality of alternative streams of content; and

protect the plurality of alternative streams of content using the common cryptographic information.

2. The source encoder of claim 1, wherein the encoding application configures the processor to encode and protect the source content by configuring the processor to:

encode a portion of source content; and

encrypt at least one portion of the encoded portion of content so that the at least one encrypted portion can be accessed using the common cryptographic information.

3. The source encoder of claim 1, wherein the encoding application configures the processor to obtain common cryptographic information by configuring the processor to:

send a request to a DRM server for common cryptographic information; and

receive the common cryptographic information from the DRM server.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1086
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

4. The source encoder of claim 1, wherein a title ID is associated with the common cryptographic content and the plurality of alternative streams of protected content.

5. The source encoder of claim 1, wherein the encoding application configures the processor to write each of the alternative streams of protected content to a separate container file.

6. The source encoder of claim 5, wherein the encoding application configures the processor to write at least a portion of the common cryptographic information encrypted using at least one encryption key to each of the container files containing the alternative streams of protected content.

7. The source encoder of claim 6, wherein writing the at least a portion of the common cryptographic information to the container files containing the alternative streams of protected content comprises encrypting the at least a portion of the common cryptographic information written to each of the container files using at least one encryption key.

8. The source encoder of claim 6, wherein writing the at least a portion of the common cryptographic information to the container files containing the alternative streams of protected content comprises encrypting the at least a portion of the common cryptographic information written to each of the container files using the same encryption key.

9. The source encoder of claim 5, wherein the container files are Matroska container files.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1087
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

10. The source encoder of claim 9, wherein the encoding application configures the processor to write a DRMHeader element to the TracksData element in a Tracks element within each of the Matroska container files, where the DRMHeader element includes an encrypted copy of the common cryptographic information.

11. The source encoder of claim 10, wherein:

the common cryptographic information is a set of encryption keys;

the encoding application configures the processor to:

encrypt the set of encryption keys using at least one encryption key; and

write the encrypted set of encryption keys to the DRMHeader element of each of the Matroska container files.

12. The source encoder of claim 11, wherein:

the source content includes a stream of video; and

the encoding application configures the processor to:

encode a frame of video;

protect the encoded frame of video by encrypting at least a portion of the encoded frame of video; and

write a BlockGroup element to a Matroska container file including a DRMInfo element identifying the at least one portion of the encoded frame of video that is encrypted and at least one encryption key from the set of encryption keys used to access the at least one encrypted portion of the encoded frame of video.

13. The source encoder of claim 9, wherein the encoding application further configures the processor to:

generate an index for each Matroska container file during the encoding of each of the streams of protected content; and

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1088
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

write a Cues element containing the index to the indexed Matroska container file.

14. A method of encoding source content as a plurality of protected streams using common cryptographic information, comprising:

receiving source content using a source encoder;

obtaining common cryptographic information using a source encoder;

encoding the source content as a plurality of streams including a plurality of alternative streams of content using the source encoder; and

protecting the plurality of alternative streams of content using the source encoder and the common cryptographic information.

15. The method of claim 14, further comprising:

encoding a portion of source content using the source encoder; and

encrypting at least one portion of the encoded content using the source encoder so that the at least one encrypted portion can be accessed using the common cryptographic information.

16. The method of claim 14, wherein obtaining common cryptographic information comprises:

sending a request to a DRM server for common cryptographic information using the source encoder; and

receiving the common cryptographic information from the DRM server.

17. The method of claim 14, further comprising associating a title ID with the common cryptographic content and the plurality of alternative streams of protected content.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1089
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

18. The method of claim 14, further comprising writing each of the alternative streams of protected content to a separate container file using the source encoder.

19. The method of claim 18, further comprising writing at least a portion of the common cryptographic information encrypted using at least one encryption key to each of the container files containing the alternative streams of protected content using the source encoder.

20. The method of claim 19, wherein writing the at least a portion of the common cryptographic information to the container files containing the alternative streams of protected content comprises encrypting the at least a portion of the common cryptographic information written to each of the container files using at least one encryption key.

21. The method of claim 19, wherein writing the at least a portion of the common cryptographic information to the container files containing the alternative streams of protected content comprises encrypting the at least a portion of the common cryptographic information written to each of the container files using the same encryption key.

22. The method of claim 18, wherein the container files are Matroska container files.

23. The method of claim 22, further comprising writing a DRMHeader element to a TracksData element in a Tracks element within each of the Matroska container files using the source encoder, where the DRMHeader element includes an encrypted copy of the common cryptographic information.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1090
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

24. The method of claim 23, wherein the common cryptographic information is a set of encryption keys and the method further comprises:

encrypting the set of encryption keys using at least one encryption key using the source encoder; and

writing the encrypted set of encryption keys to the DRMHeader element of each of the Matroska container files using the source encoder.

25. The method of claim 24, wherein the source content includes a stream of video and the method further comprises:

encoding a frame of video using the source encoder;

protecting the encoded frame of video by encrypting at least a portion of the encoded frame of video using the source encoder; and

writing a BlockGroup element to a Matroska container file including a DRMInfo element identifying the at least one portion of the encoded frame of video that is encrypted and at least one encryption key from the set of encryption keys used to access the at least one encrypted portion of the encoded frame of video using the source encoder.

26. The method of claim 22, further comprising:

generating an index for each Matroska container file using the source encoder during the encoding of each of the streams of protected content; and

writing a Cues element containing the index to the indexed Matroska container file using the source encoder.

27. A machine readable medium containing processor instructions, where execution of the instructions by a processor causes the processor to perform a process comprising:

receiving source content;

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1091
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

obtaining common cryptographic information;

encoding the source content as a plurality of streams including a plurality of alternative streams of content; and

protecting the plurality of alternative streams of content and the common cryptographic information.

28. The machine readable medium of claim 27, wherein the machine readable medium is non-volatile memory.

29. A content distribution system, comprising:

a DRM server;

a content distribution server, where the content distribution server stores a plurality of container files containing alternative streams of protected content associated with a title, the alternative streams of protected content are protected using common cryptographic information, and each container file includes a copy of the common cryptographic information encrypted using at least one encryption key;

wherein the DRM server is configured to:

receive a request for access to the alternative streams of protected content associated with the title from a playback device; and

securely provide a copy of the at least one encryption key used to encrypt the common cryptographic information to the playback device; and

wherein the content distribution server is configured to grant the playback device access to the alternative streams of protected content.

30. The content distribution system of claim 29, wherein the DRM server is configured to associate a title ID with the title.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1092
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

31. The content distribution system of claim 30, wherein the DRM server is configured to associate the common cryptographic information with the title ID.

32. The content distribution system of claim 30, wherein the request for access to the alternative streams of protected content associated with the title comprises a request identifying a title ID.

33. The content distribution system of claim 29, wherein the content distribution server is further configured to:

receive requests for portions of at least one container file from the playback device; and

provide the requested portions of the at least one container file to the playback device.

34. The content distribution system of claim 29, wherein the plurality of container files are Matroska container files.

35. The content distribution system of claim 34, wherein:

the common cryptographic information includes a set of encryption keys; and

the set of encryption keys are encrypted using the at least one encryption key.

36. The content distribution system of claim 29, further comprising:

a source encoder configured to:

receive source content;

obtain common cryptographic information from the DRM server;

encode the source content as a plurality of streams including a plurality of alternative streams of content;

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1093
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

protect the plurality of alternative streams of content using the common cryptographic information;

protect the common cryptographic information using at least one encryption key; and

provide a plurality of container files containing the plurality of alternative streams of protected content to the content distribution server.

37. The content distribution system of claim 36, wherein the source encoder is configured to:

encode a portion of content; and

encrypt at least one portion of the encoded content so that the at least one encrypted portion can be accessed using the common cryptographic information.

38. The content distribution system of claim 37, wherein the source encoder is configured to write each of the alternative streams of protected content to a separate container file.

39. The content distribution system of claim 38, wherein the source encoder is configured to encrypt at least a portion of the common cryptographic information using at least one encryption key and write the encrypted information to each of the container files containing the alternative streams of protected content.

40. The content distribution system of claim 38, wherein the source encoder is configured to encrypt at least a portion of the common cryptographic information using a single encryption key and write the encrypted information to each of the container files containing the alternative streams of protected content.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1094
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

41. The content distribution system of claim 38, wherein the container files are Matroska container files.

42. The content distribution system of claim 41, wherein the source encoder is configured to write a DRMHeader element to a TracksData element in a Tracks element within each of the Matroska container files, where the DRMHeader element includes an encrypted copy of the common cryptographic information.

43. The source encoder of claim 42, wherein:

the common cryptographic information includes a set of encryption keys; and

the source encoder is configured to:

encrypt the set of encryption keys using at least one encryption key;

write the encrypted set of encryption keys to the DRMHeader element of each of the Matroska container files.

44. The content distribution system of claim 43, wherein:

the source content includes a stream of video; and

the source encoder is configured to:

encode a frame from the stream of video;

protect the encoded frame of video by encrypting at least a portion of the encoded frame of video; and

write a BlockGroup element to a Matroska container file including a DRMInfo element identifying the at least one portion of the encoded frame of video that is encrypted and at least one encryption key from the set of encryption keys used to access the at least one encrypted portion of the encoded frame of video.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1095
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

45. The content distribution system of claim 41, wherein the source encoder is configured to:

generate an index for each Matroska container file during the encoding of each of the streams of protected content; and

write a Cues element containing the index to the indexed Matroska container file.

46. The content distribution system of claim 36, wherein the plurality of container files are Matroska container files.

47. The content distribution system of claim 46, wherein the source encoder is configured to write a DRMHeader element to a TracksData element in a Tracks element within each of the Matroska container files, where the DRMHeader element includes an encrypted copy of the common cryptographic information.

48. The content distribution system of claim 47, wherein:

the common cryptographic information includes a set of encryption keys; and

the source encoder is configured to encrypt the set of encryption keys using the at least one encryption key.

49. A method of distributing content encoded as a plurality of alternative streams of protected content, where the alternative streams of protected content are protected using common cryptographic information and each stream of protected content includes a copy of the common cryptographic information encrypted using at least one encryption key, the method comprising:

receiving a request for access to the alternative streams of protected content associated with the title from a playback device using a DRM server;

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1096
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

securely providing to the playback device at least one encryption key using the DRM server, where the at least one encryption keys is used to access the encrypted common cryptographic information; and

granting the playback device access to the alternative streams of protected content using a content distribution server.

50. The method of claim 49, wherein the title is identified using a title ID.

51. The method of claim 50, wherein the common cryptographic information is associated with the title ID.

52. The method of claim 50, wherein the request for access to the alternative streams of protected content associated with the title comprises a request identifying a title ID.

53. The method of claim 49, further comprising:

receiving requests for portions of at least one container file from the playback device using the content distribution server; and

providing the requested portions of the at least one container file to the playback device using the content distribution server.

54. The method of claim 49, wherein the plurality of container files are Matroska container files.

55. The method of claim 54, wherein:

the common cryptographic information includes a set of encryption keys; and

the set of encryption keys is encrypted using the at least one encryption key.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1097
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

56. The method of claim 49, further comprising:

receiving source content using a source encoder;

obtaining common cryptographic information from the DRM server using a source encoder;

encoding the source content as a plurality of streams including a plurality of alternative streams of content using the source encoder;

protecting the plurality of alternative streams of content using the source encoder and the common cryptographic information;

encrypting the common cryptographic information using the source encoder and at least one encryption key; and

providing the plurality of alternative streams of content and the encrypted common cryptographic information to a content distribution server using the source encoder.

57. The method of claim 56, further comprising

encoding a portion of content using the source encoder; and

encrypting at least one portion of the encoded content using the source encoder so that the at least one encrypted portion can be accessed using the common cryptographic information.

58. The method of claim 57, further comprising writing each of the alternative streams of protected content to a separate container file.

59. The method of claim 58, wherein the container files are Matroska container files.

60. The method of claim 59, further comprising writing a DRMHeader element to a TracksData element in a Tracks element within each of the Matroska container files

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1098
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

using the source encoder, where the DRMHeader element includes an encrypted copy of the common cryptographic information.

61. The method of claim 59, wherein the common cryptographic information includes a set of encryption keys, the method further comprising:

encrypting the set of encryption keys using the at least one encryption key; and

writing the encrypted set of encryption keys to the DRMHeader element of each of the Matroska container files using the source encoder.

62. The method of claim 61, wherein the source content includes a stream of video, the method further comprising:

encoding a frame from the stream of video using the source encoder;

protecting the encoded frame of video by encrypting at least a portion of the encoded frame of video using the source encoder; and

writing a BlockGroup element to a Matroska container file including a DRMInfo element identifying the at least one portion of the encoded frame of video that is encrypted and at least one encryption key from the set of encryption keys used to access the at least one encrypted portion of the encoded frame of video using the source encoder.

63. The method of claim 59, further comprising:

generating an index for each Matroska container file during the encoding of each of the streams of protected content using the source encoder; and

writing a Cues element containing the index to the indexed Matroska container file using the source encoder.

64. The method of claim 56, wherein the plurality of container files are Matroska container files.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1099
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

65. The method of claim 64, further comprising writing a DRMHeader element to a TracksData element in a Tracks element within each of the Matroska container files using the source encoder, where the DRMHeader element includes an encrypted copy of the common cryptographic information.

66. The method of claim 65, wherein:

the common cryptographic information includes a set of encryption keys; and

the method further comprising encrypting the set of encryption keys using the source encoder and at least one encryption key.

67. A playback device, comprising:

a processor;

memory containing a client application;

wherein the client application configures the processor to:

request a top level index file identifying a plurality of alternative streams of protected content, where each of the alternative streams of protected content are encrypted using common cryptographic information;

obtain the common cryptographic information;

request portions of content from at least the plurality of alternative streams of protected content;

access the protected content using the common cryptographic information; and

playback the content.

68. The playback device of claim 67, wherein:

the alternative streams of protected content are alternative streams of protected video;

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1100
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

each of the alternative streams of protected video includes DRM information indicating portions of frames of video that are encrypted and identifying at least a portion of the common cryptographic information used to access the encrypted portions of the frames of video; and

the client application configures the processor to:

obtain a protected frame of video from one of the alternative streams of protected video;

obtain DRM information indicating a portion of the protected frame of video that is encrypted;

identify at least a portion of the common cryptographic information that is used to access the encrypted portion of the protected frame using the DRM information;

decrypt the encrypted portion of the protected frame of video using the identified portion of the common cryptographic information; and

decode the frame of video.

69. The playback device of claim 67, wherein:

each of the alternative streams of protected content is contained within a separate container file; and

the top level index file identifies a container file containing each of the alternative streams.

70. The playback device of claim 69, wherein:

the container files containing each of the alternative streams of protected content comprise at least one header including the common cryptographic information and information that describes the encoding of the stream of protected content; and

the top level index file identifies the location of the at least one header within each container file.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1101
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

71. The playback device of claim 70, wherein the common cryptographic information is a set of encryption keys.

72. The playback device of claim 71, wherein:

the common set of encryption keys is encrypted; and

the client application configures the processor to securely receive cryptographic information used to unencrypt the common set of encryption keys.

73. The playback device of claim 70, wherein the client application configures the processor to obtain the common cryptographic information by requesting at least one header of a container file identified in the top level index file.

74. The playback device of claim 73, wherein:

each container file containing one of the alternative streams of protected content further comprises an index; and

the client application configures the processor to request a portion of content from one of the container files by configuring the processor to:

request at least a portion of an index from the container file;

identify the portion of the container file containing a specific portion of content using the index; and

request the identified portion of the container file.

75. The playback device of claim 70, wherein the container files are Matroska container files.

76. The playback device of claim 75, wherein the common cryptographic information is stored in a common DRM Header element contained within a Tracks

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1102
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

element within each of the Matroska container files containing the alternative streams of protected content.

77. The playback device of claim 76, wherein:

the common cryptographic information is a set of encryption keys; and

the set of encryption keys is encrypted and stored within the DRM Header element.

78. The playback device of claim 77, wherein the client application configures the processor to:

obtain cryptographic information that can be used to unencrypt the set of encryption keys stored within the DRM Header element; and

unencrypt the set of encryption keys stored within the DRM Header element using the obtained cryptographic information.

79. The playback device of claim 76, wherein the client application configures the processor to obtain the DRM Header element by requesting a Tracks element from one of the Matroska container files identified in the top level index file.

80. The playback device of claim 79, wherein:

each Mastroska container file containing an alternative stream of protected content further comprises an index contained within a Cues element; and

the client application configures the processor to request a portion of content from one of the Matroska container files by configuring the processor to:

request at least a portion of a Cues element from a Matroska container file containing one of the alternative streams of protected content;

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1103
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

identify a portion of the Matroska container file containing a specific portion of content using at least one CueTrackPosition element within the Cues element; and

request the portion of the Matroska container file identified by the at least one CueTrackPosition element.

81. The playback device of claim 80, wherein the index comprises a plurality of CueTrackPosition elements that identify the location of a plurality of Cluster elements within the Matroska container file.

82. The playback device of claim 81, wherein:

each Cluster element contains a plurality of BlockGroup elements including encoded portions of content;

a CueTrack Position element indexes each Cluster element; and

each CueTrackPosition element includes the size of the Cluster element that it indexes.

83. The playback device of claim 80, wherein

the alternative streams of protected content are alternative streams of protected video;

each of the Matroska container files containing an alternative stream of protected video includes a DRMInfo element in a BlockGroup element containing a protected frame of video, where the DRMInfo element indicates at least a portion of the protected frames of video that is encrypted and identifies at least a portion of the common cryptographic information used to access the at least one encrypted portion of the protected frame of video; and

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1104
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

the client application configures the processor to access video frames in a stream of protected video using the common cryptographic information by configuring the processor to:

obtain a BlockGroup containing a protected frame of video;

parse the BlockGroup element to obtain a DRMInfo element indicating at least a portion of the protected frame of video that is encrypted using an encryption key from the set of encryption keys;

decrypt the at least one encrypted portion of the protected frame of video using the identified encryption key; and

decode the frame of video.

84. A method of performing adaptive bitrate streaming using a plurality of alternative streams of protected content, where each of the streams of protected content is protected using common cryptographic information, the method comprising:

requesting a top level index file identifying a plurality of alternative streams of protected content using a playback device, where each of the alternative streams of protected content are encrypted using common cryptographic information;

obtaining the common cryptographic information using the playback device;

requesting portions of content from at least the plurality of alternative streams of protected content using the playback device;

accessing the protected content using the playback device and the common cryptographic information; and

playing back the content using the playback device.

85. The method of claim 84, wherein:

the alternative streams of protected content are alternative streams of protected video;

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1105
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

each of the alternative streams of protected video includes DRM information indicating portions of frames of video that are encrypted and identifying at least a portion of the common cryptographic information used to access the encrypted portions of the frames of video; and

the method further comprises:

obtaining a protected frame of video from one of the alternative streams of protected video using the playback device;

obtaining DRM information indicating a portion of the protected frame of video that is encrypted using the playback device;

identify at least a portion of the common cryptographic information that is used to access the encrypted portion of the protected frame using the playback device and the DRM information;

decrypting the encrypted portion of the protected frame of video using the playback device and the identified portion of the common cryptographic information; and

decoding the frame of video using the playback device.

86. The method of claim 84, wherein:

each of the alternative streams of protected content is contained within a separate container file; and

the top level index file identifies a container file containing each of the alternative streams.

87. The method of claim 86, wherein:

the container files containing each of the alternative streams of protected content comprise at least one header including the common cryptographic information and information that describes the encoding of the stream of protected content; and

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1106
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

the top level index file identifies the location of the at least one header within each container file.

88. The method of claim 87, wherein the common cryptographic information is a set of encryption keys.

89. The method of claim 88, wherein:

the set of encryption keys is encrypted so that it is accessible using cryptographic information obtained by the playback device; and

the method further comprising obtaining cryptographic information using the playback device.

90. The method of claim 89, wherein

the set of encryption keys is encrypted using at least one encryption key; and

the playback device securely obtains the at least one encryption key.

91. The method of claim 90, wherein the at least one encryption key is encrypted using at least one encryption key included in the cryptographic information bound to the playback device.

92. The method of claim 89, further comprising obtaining the common cryptographic information by requesting at least one header of a container file identified in the top level index file using the playback device.

93. The method of claim 92, wherein:

each container file containing one of the alternative streams of protected content further comprises an index; and

the method further comprising:

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1107
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

requesting at least a portion of an index from the container file using the playback device;

identify the portion of the container file containing a specific portion of content using the playback device and the index; and

requesting the identified portion of the container file using the playback device.

94. The method of claim 87, wherein the container files are Matroska container files.

95. The method of claim 94, wherein the common cryptographic information is stored in a common DRM Header element contained within a Tracks element within each of the Matroska container files containing the alternative streams of protected content.

96. The method of claim 95, wherein:

the common cryptographic information is a set of encryption keys; and

the set of encryption keys is encrypted and stored within the DRM Header element.

97. The method of claim 96, wherein:

the set of encryption keys is encrypted so that it is accessible using cryptographic information obtained by the playback device; and

the method further comprising obtaining cryptographic information using the playback device.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1108
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

98. The method of claim 97, further comprising obtaining the DRM Header element by requesting a Tracks element from one of the Matroska container files identified in the top level index file.

99. The method of claim 98, wherein:

each Mastroska container file containing an alternative stream of protected content further comprises an index contained within a Cues element; and

the method further comprises:

requesting at least a portion of a Cues element from a Matroska container file containing one of the alternative streams of protected content using the playback device;

identifying a portion of the Matroska container file containing a specific portion of content using the playback device and at least one CueTrackPosition element within the Cues element; and

requesting the portion of the Matroska container file identified by the at least one CueTrackPosition element.

100. The method of claim 99, wherein the index comprises a plurality of CueTrackPosition elements that identify the location of a plurality of Cluster elements within the Matroska container file.

101. The method of claim 100, wherein:

each Cluster element contains a plurality of BlockGroup elements including encoded portions of content;

a CueTrack Position element indexes each Cluster element; and

each CueTrackPosition element includes the size of the Cluster element that it indexes.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1109
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

102. The method of claim 99, wherein

the alternative streams of protected content are alternative streams of protected video;

each of the Matroska container files containing an alternative stream of protected video includes a DRMInfo element in a BlockGroup element containing a protected frame of video, where the DRMInfo element indicates at least a portion of the protected frames of video that is encrypted and identifies at least a portion of the common cryptographic information used to access the at least one encrypted portion of the protected frame of video; and

the method further comprising:

obtaining a BlockGroup containing a protected frame of video using the playback device;

parsing the BlockGroup element to obtain a DRMInfo element indicating at least a portion of the protected frame of video that is encrypted using the playback device and an encryption key from the set of encryption keys;

decrypting the at least one encrypted portion of the protected frame of video using the playback device and the identified encryption key; and

decoding the frame of video using the playback device.

103. A machine readable medium containing processor instructions, where execution of the instructions by a processor causes the processor to perform a process comprising:

request a top level index file identifying a plurality of alternative streams of protected content, where each of the alternative streams of protected content are encrypted using common cryptographic information;

obtaining the common cryptographic information;

requesting portions of content from at least the plurality of alternative streams of protected content;

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1110
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

accessing the protected content using the common cryptographic information; and

playing back the content.

104. The machine readable medium of claim 103, wherein:

the alternative streams of protected content are alternative streams of protected video;

each of the alternative streams of protected video includes DRM information indicating portions of frames of video that are encrypted and identifying at least a portion of the common cryptographic information used to access the encrypted portions of the frames of video; and

execution of the instructions by a processor also causes the processor to perform a process comprising:

obtaining a protected frame of video from one of the alternative streams of protected video;

obtaining DRM information indicating a portion of the protected frame of video that is encrypted;

identify at least a portion of the common cryptographic information that is used to access the encrypted portion of the protected frame using the DRM information;

decrypting the encrypted portion of the protected frame of video using and the identified portion of the common cryptographic information; and

decoding the frame of video.

105. The machine readable medium of claim 103, wherein the machine readable medium is non-volatile memory.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1111
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

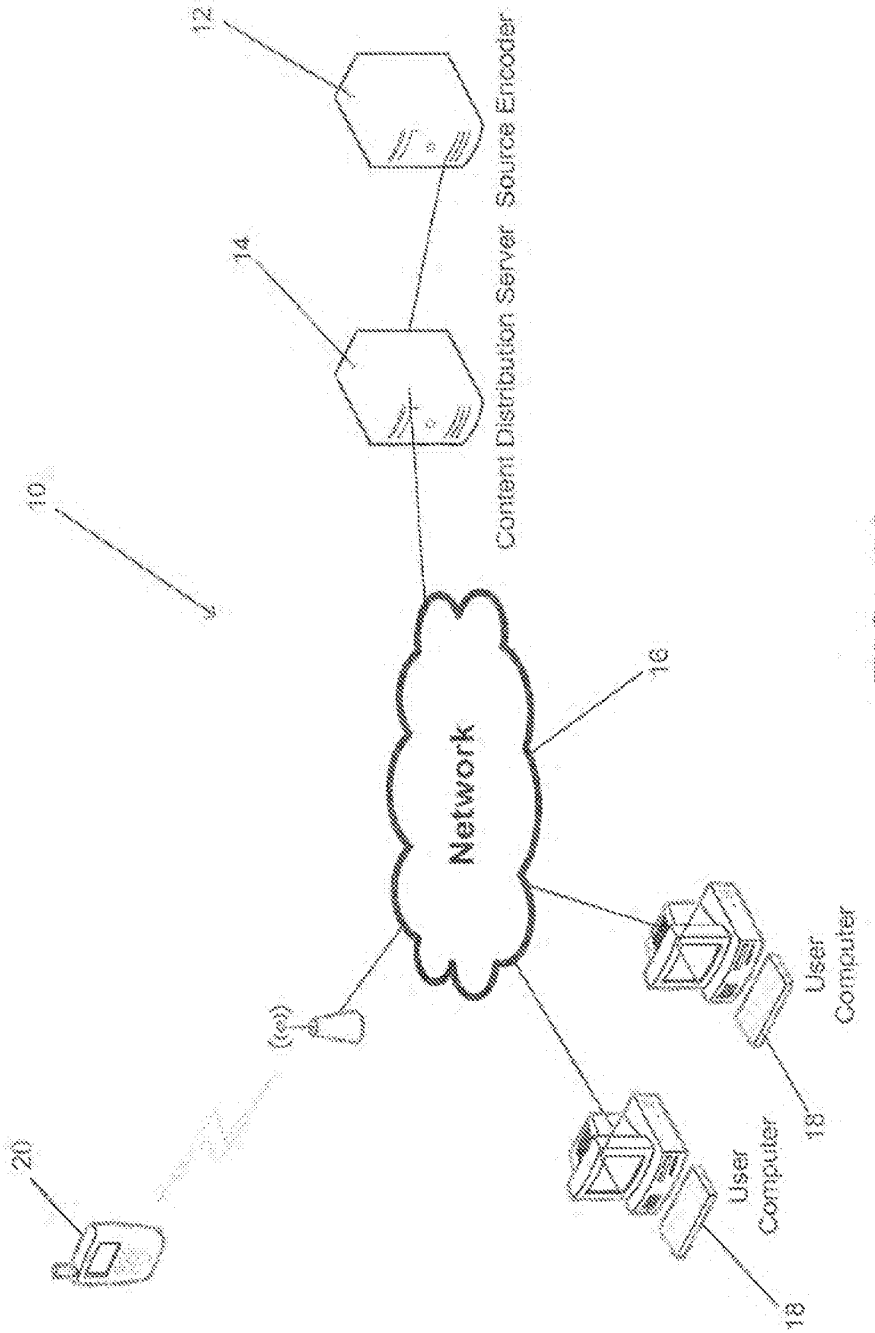


FIG. 1A

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1112
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

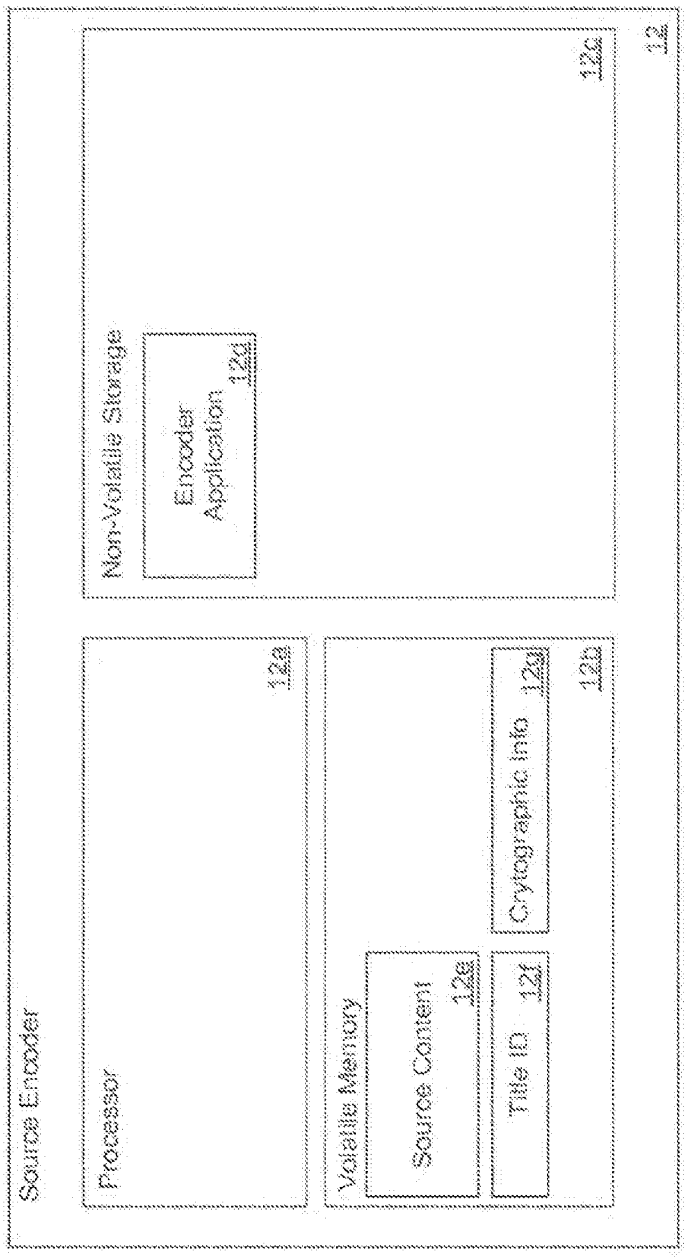


FIG. 1B

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1113
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

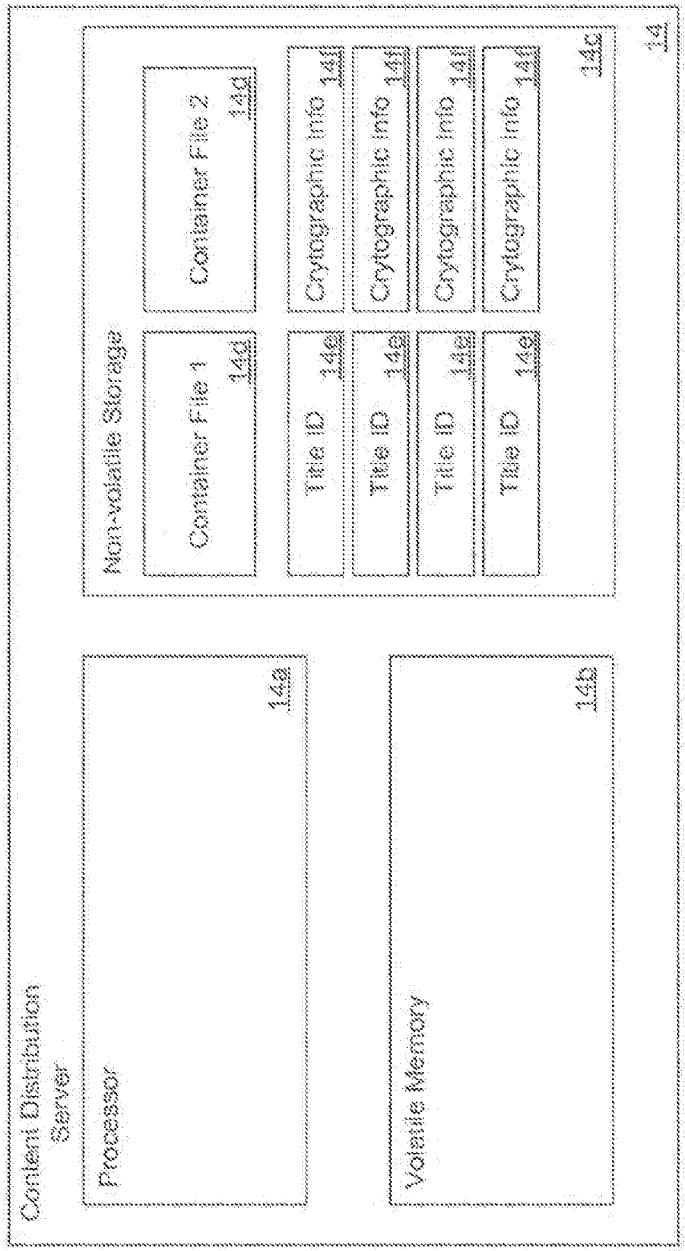


FIG. 1C

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1114
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

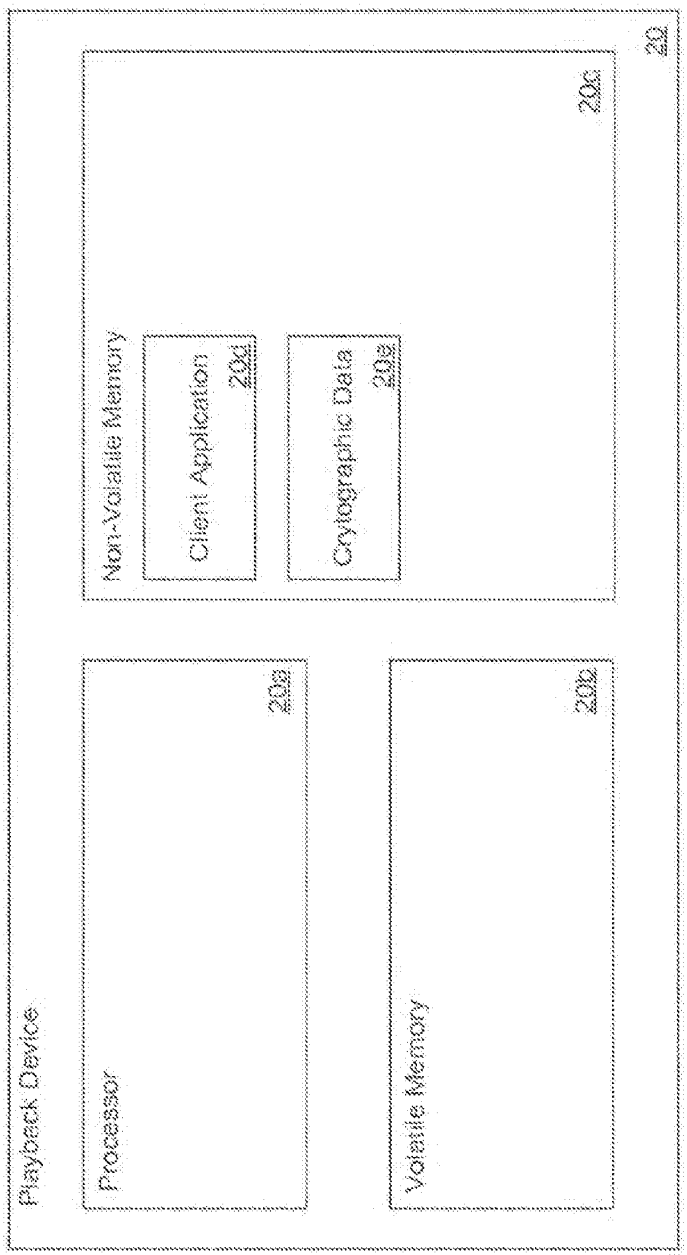


FIG. 1D

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1115
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

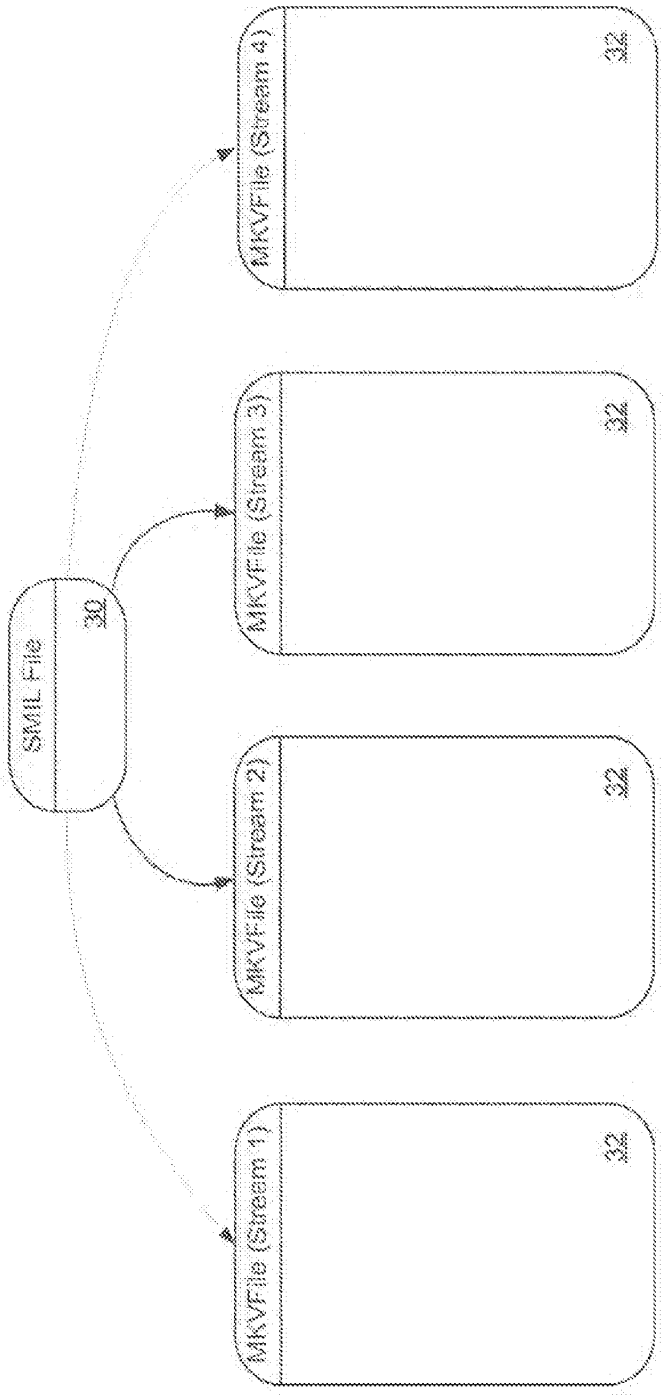


FIG. 2

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1116
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

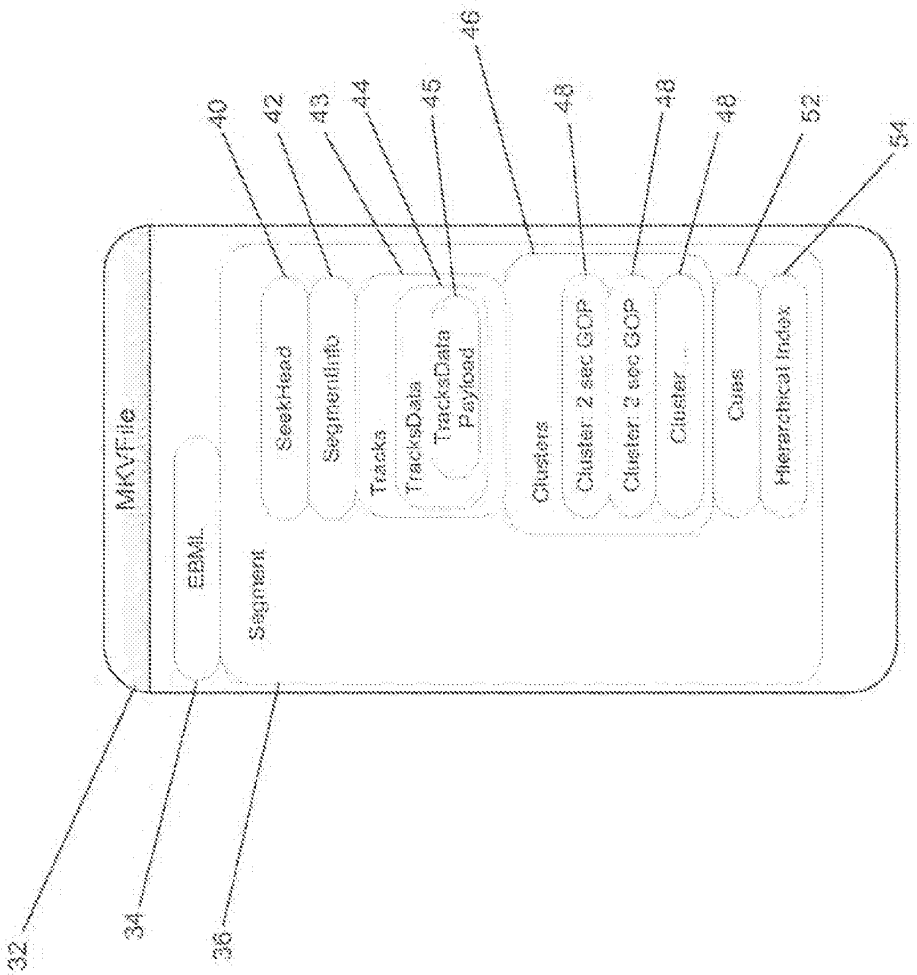


FIG. 3

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1117
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

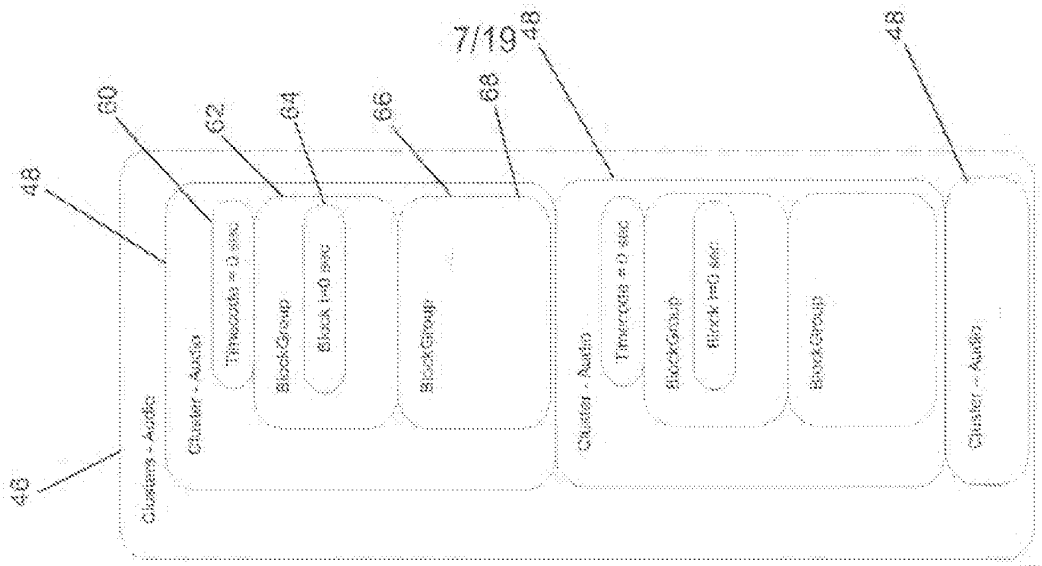


FIG 4b

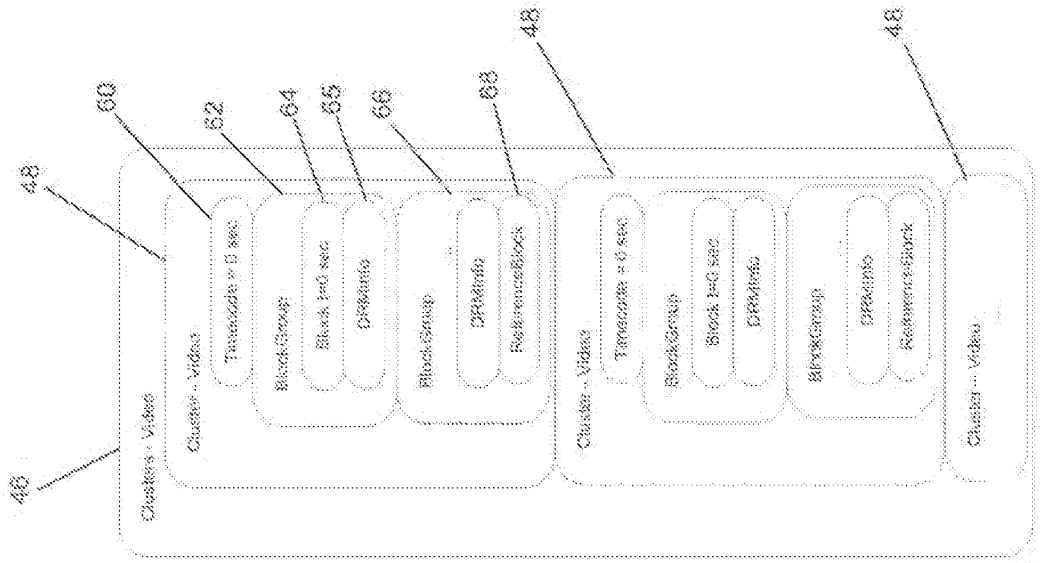


FIG 4a

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1118
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

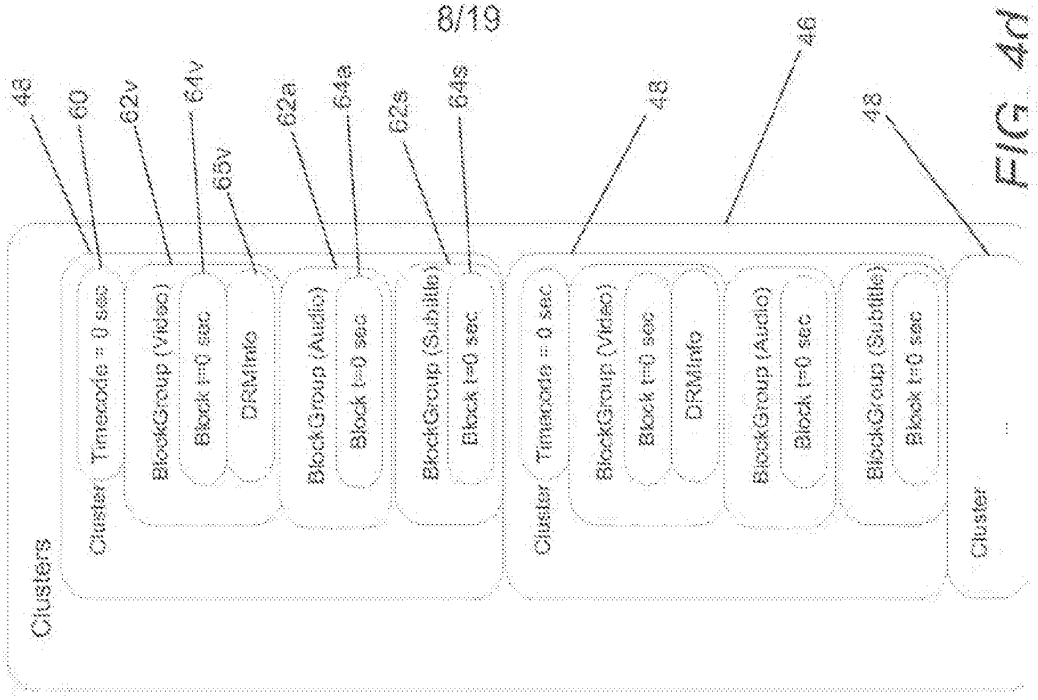


FIG. 4d

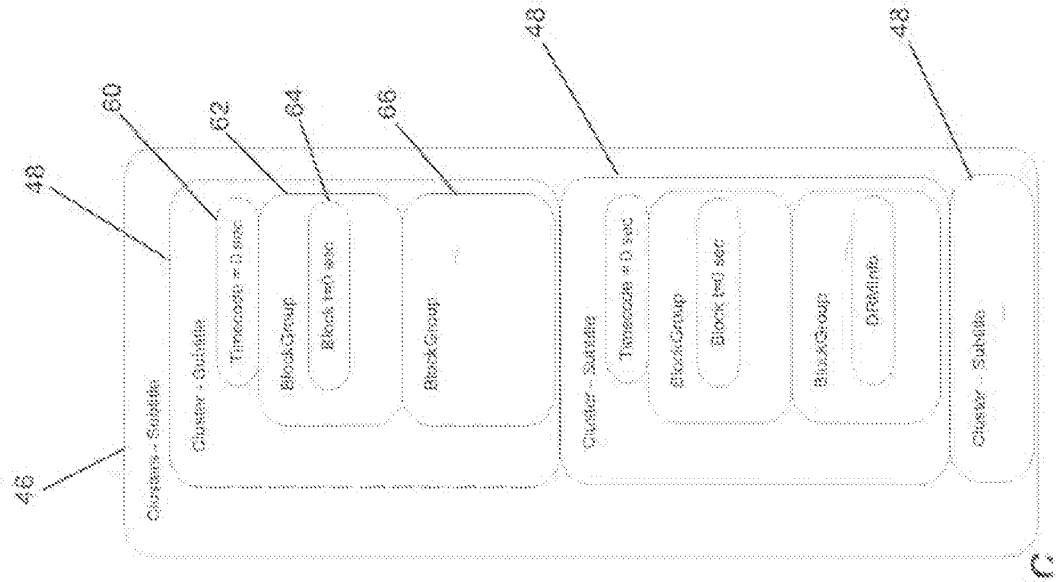


FIG. 4c

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1119
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

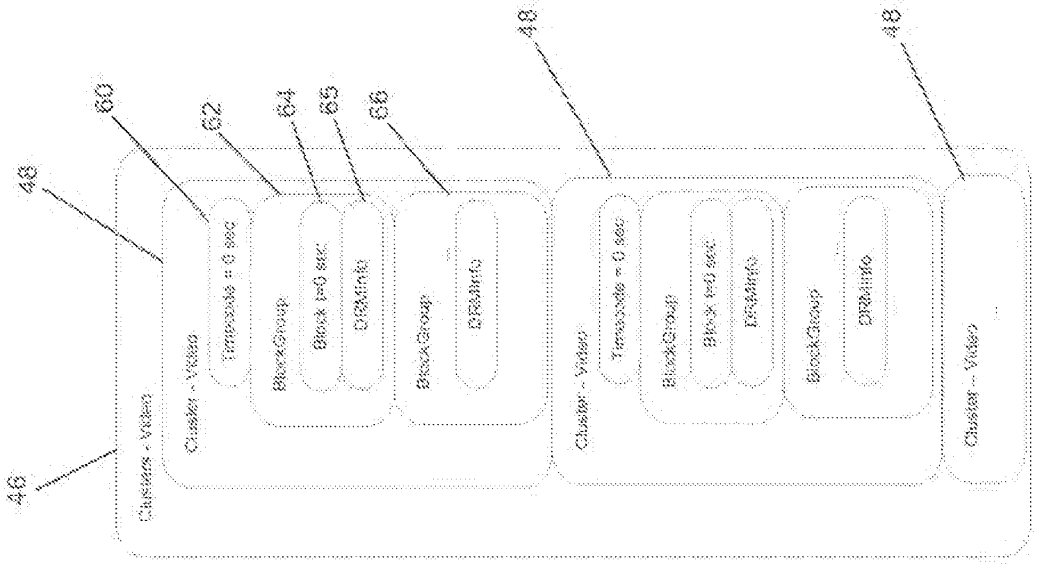


FIG. 4e

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1120
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

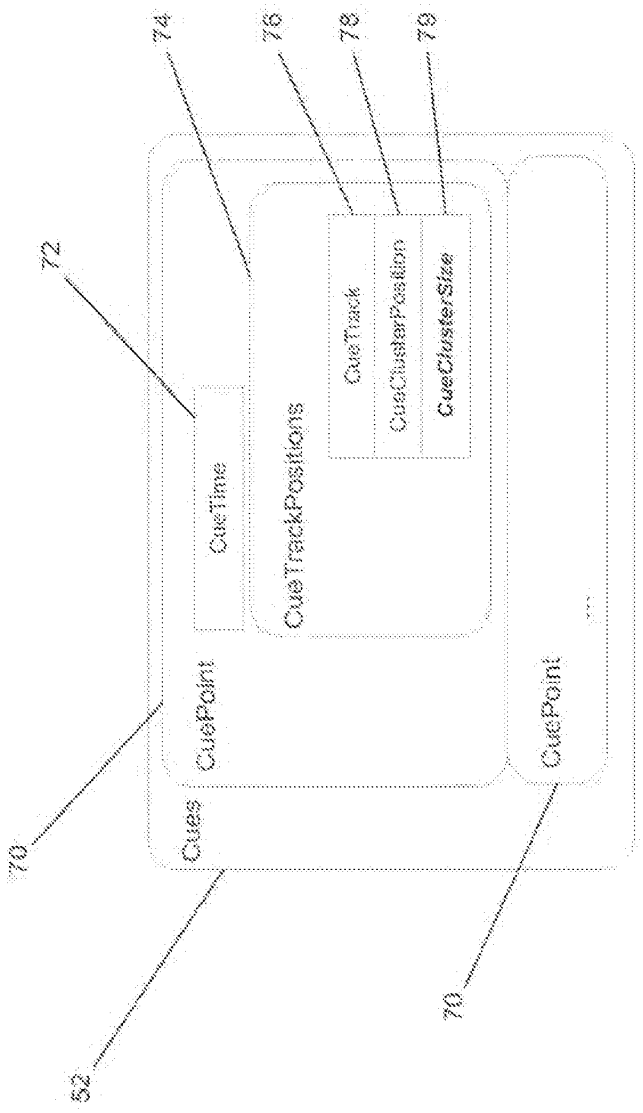


FIG. 5

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1121
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

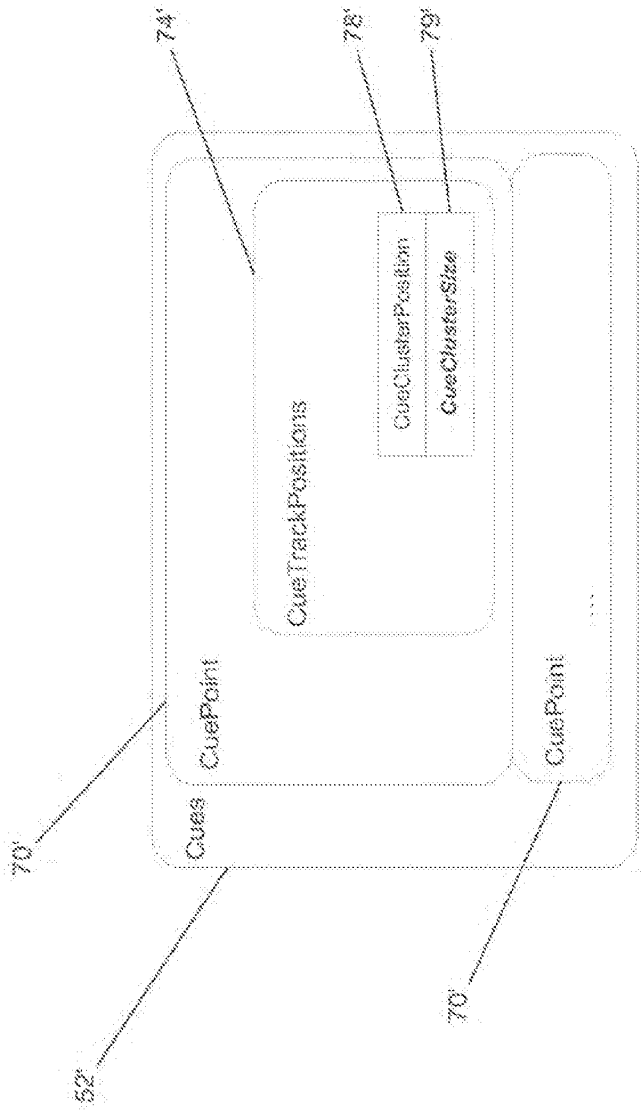


FIG. 5a

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1122
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

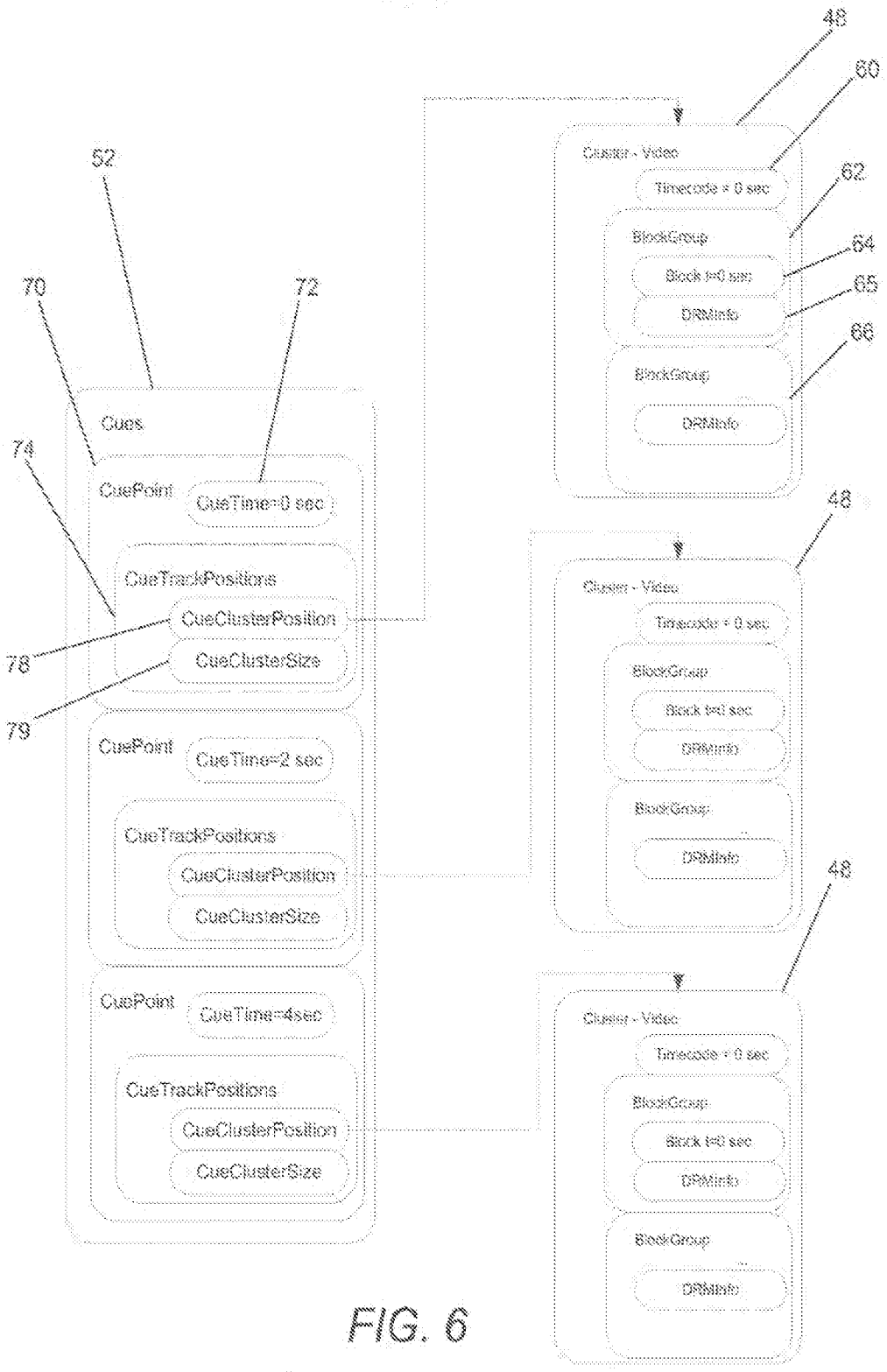


FIG. 6

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1123
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

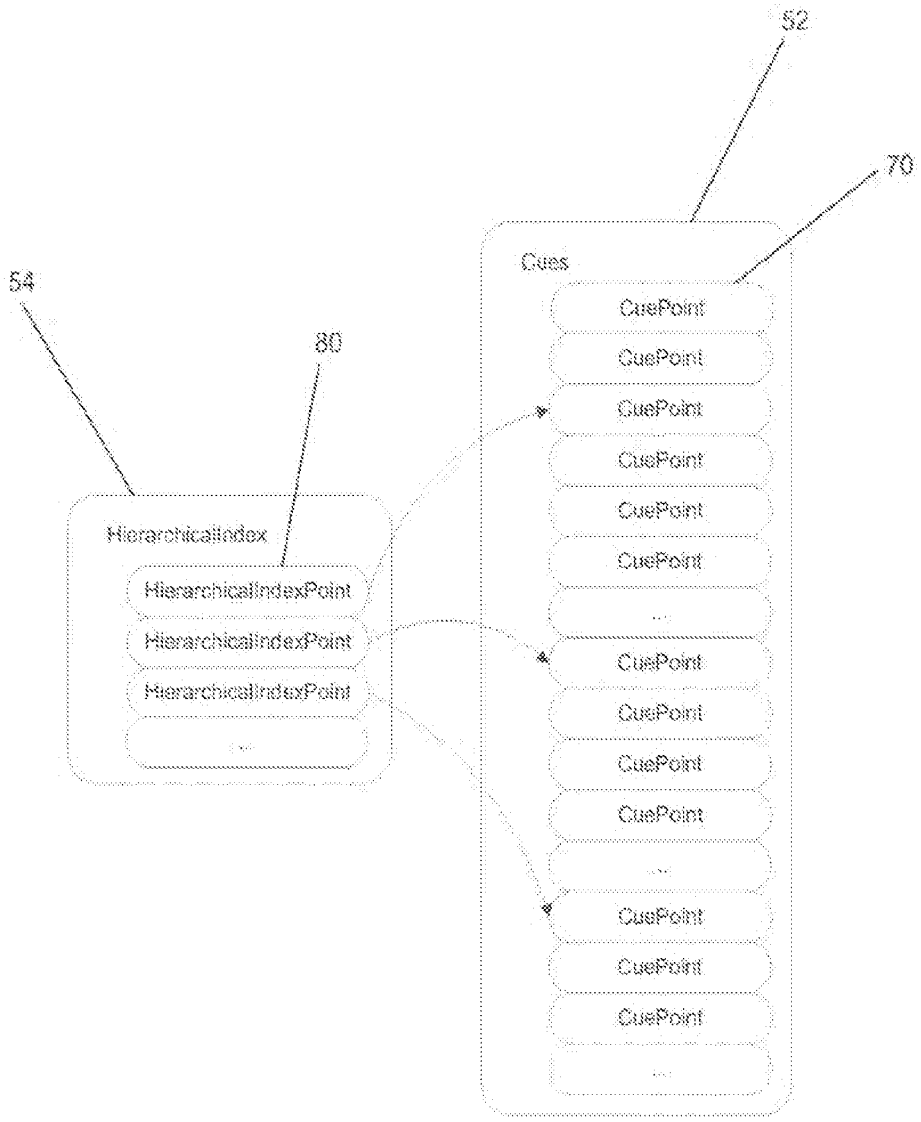


FIG. 7

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1124
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

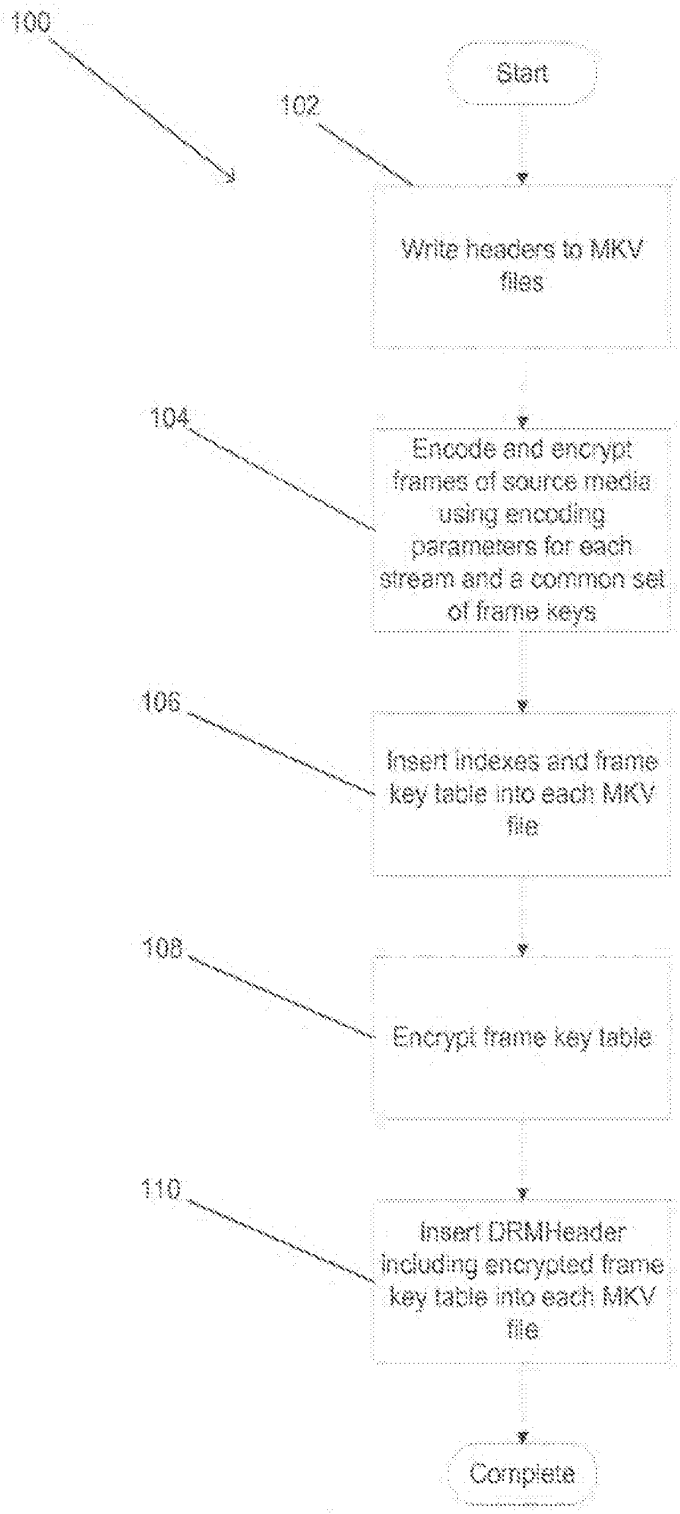


FIG. 8

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1125
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

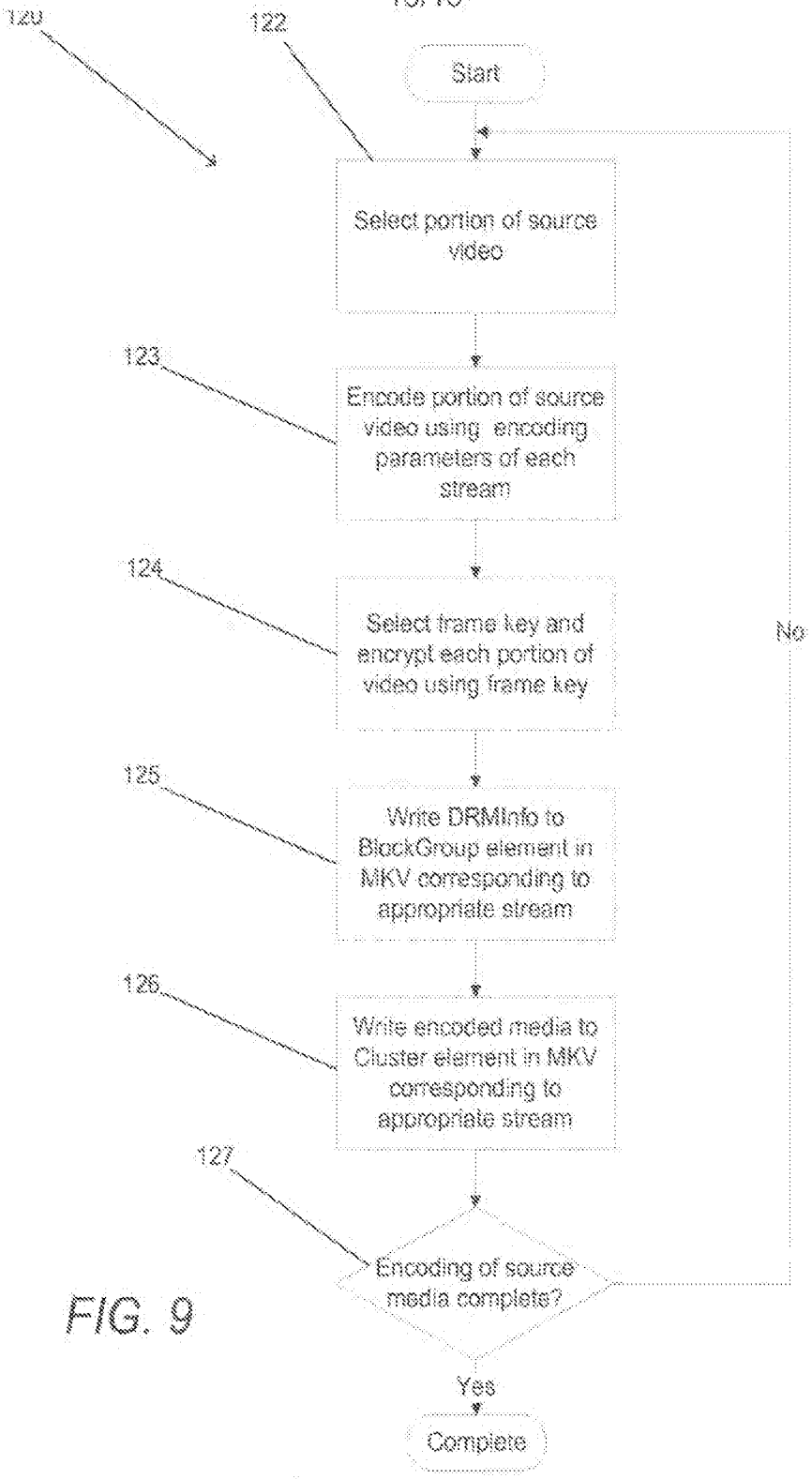


FIG. 9

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1126
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

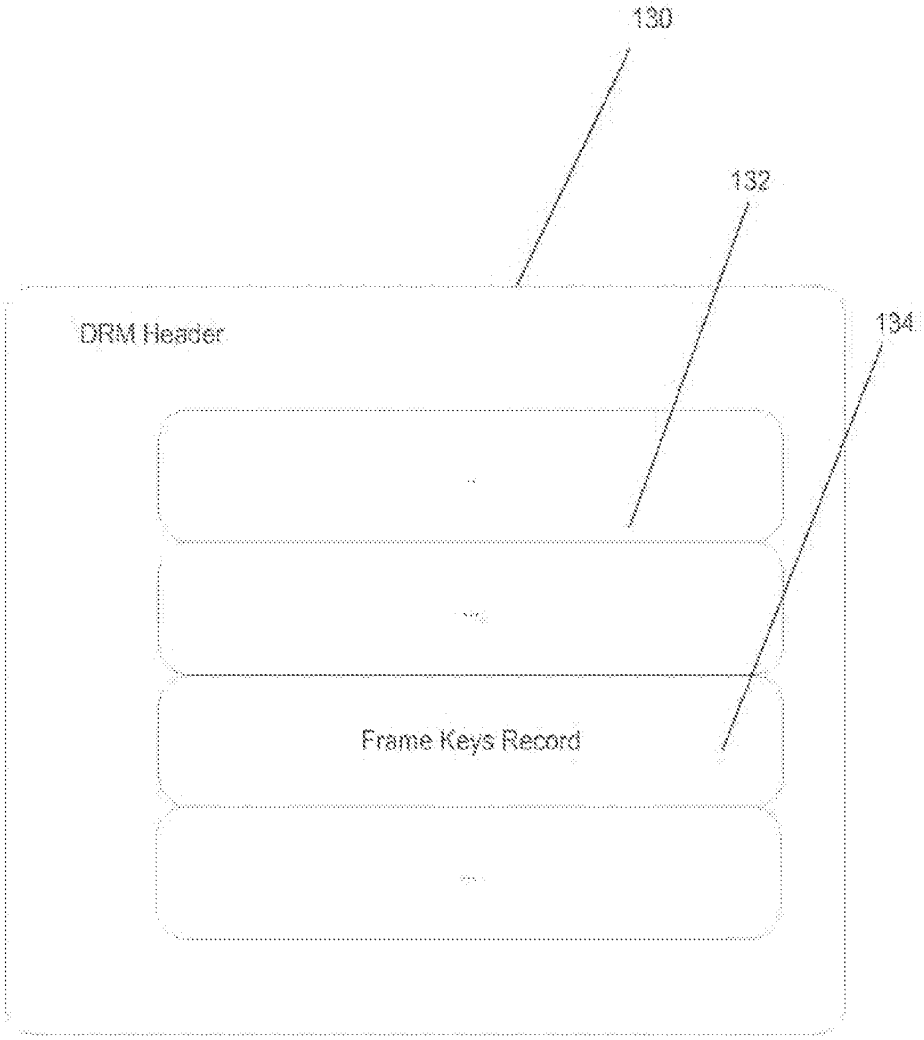


FIG. 10

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1127
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

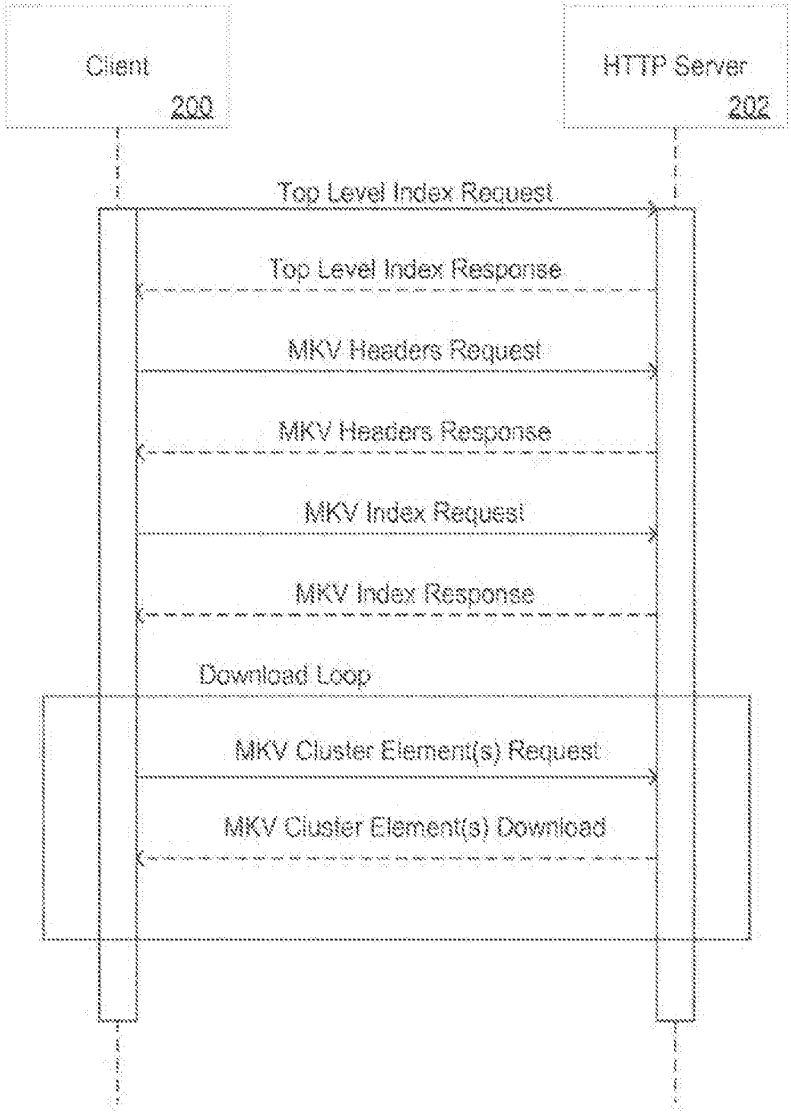


FIG. 11

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1128
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

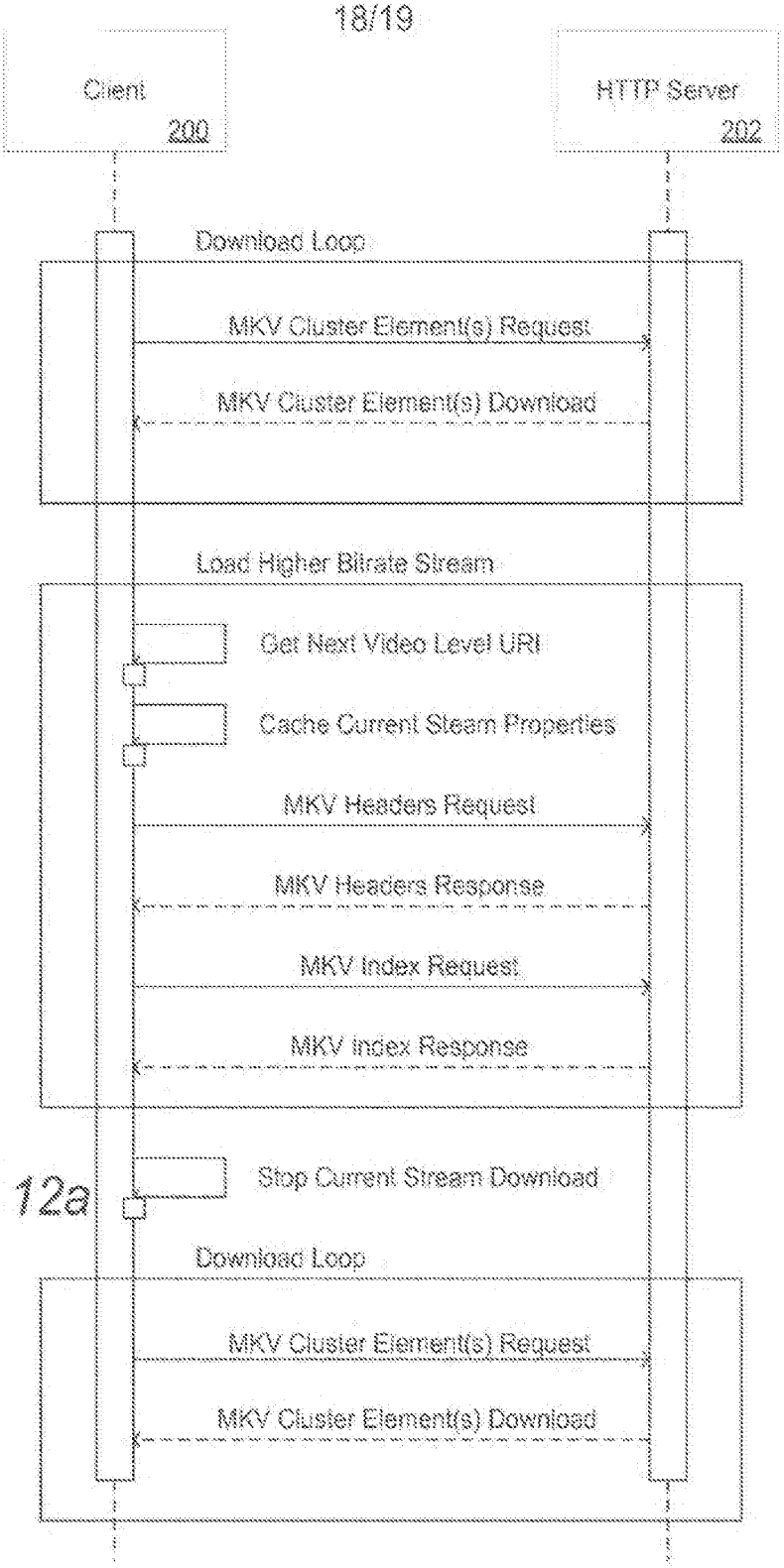


FIG. 12a

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1129
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

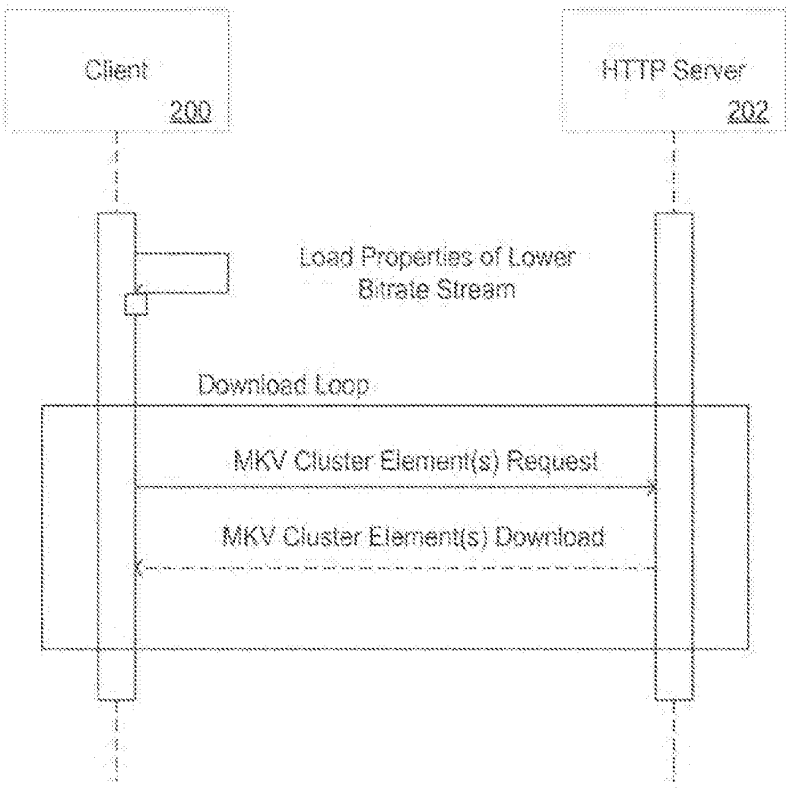


FIG. 12b

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1130
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 March 2013 (07.03.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/032518 A3

(51) International Patent Classification:
H04L 9/18 (2006.01)

(21) International Application Number:
PCT/US2011/068276

(22) International Filing Date:
31 December 2011 (31.12.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/530,305 1 September 2011 (01.09.2011) US
13/340,623 29 December 2011 (29.12.2011) US
13/341,265 30 December 2011 (30.12.2011) US

(71) Applicant *(for all designated States except US)*: **DIVX, LLC** [US/US]; 2830 De La Cruz Boulevard, Santa Clara, CA 95050 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **KIEFER, Michael, George** [US/US]; 7007 E. Gold Dust Ave., Apt. 1053, Scottsdale, AZ 85253 (US). **GRAB, Eric, William** [US/US]; 5387 Channing Street, San Diego, CA 92117 (US). **BRANESS, Jason** [US/US]; 15885 Concord Ridge Terrace, San Diego, CA 92127 (US).

(74) Agent: **BAILEY, David, J.**; Kauth, Pomeroy, Peck & Bailey LLP, 2400 E. Katella, Suite 1050, Anaheim, CA 92806 (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, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, 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, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

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))*

(88) Date of publication of the international search report:
6 September 2013

(54) Title: SYSTEMS AND METHODS FOR PROTECTING ALTERNATIVE STREAMS IN ADAPTIVE BITRATE STREAMING SYSTEMS

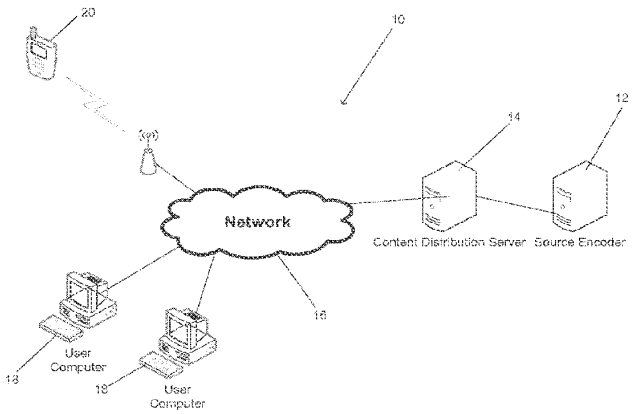


FIG. 1A

(57) Abstract: Systems and methods for performing adaptive bitrate streaming using alternative streams of protected content in accordance with embodiments of the invention are described. One embodiment includes a processor, and non-volatile storage containing an encoding application. In addition, the encoding application configures the processor to: receive source content; obtain common cryptographic information; encode the source content as a plurality of streams including a plurality of alternative streams of content; and protect the plurality of alternative streams of content using the common cryptographic information.

WO 2013/032518 A3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2011/068276

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - H04L 9/18 (2013.01)
USPC - 380/255
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)
IPC(8) - H04L 9/00, 9/08, 9/14, 9/18, (2013.01)
USPC - 380/1, 45, 255, 269, 277, 281

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
CPC- H04L 9/00, 9/08, 9/14, 9/18, (2013.01)

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X -- Y	US 2009/0290706 A1 (AMINI et al) 26 November 2009 (26.11.2009) entire document	1, 2, 14, 15, 27, 28 --- 3-13, 16-26, 29-105
Y	WO 2011/103364 A1 (THORWIRTH) 25 August 2011 (25.08.2011) entire document	4-13, 17-26, 29-105
Y	US 2009/0328228 A1 (SCHNELL) 31 December 2009 (31.12.2009) entire document	3, 10-13, 16, 23-26, 29-66, 68, 70-83, 85, 87-102, 104
Y	US 2009/0132721 A1 (SOROUSHIAN et al) 21 May 2009 (21.05.2009) entire document	9-13, 22-26, 34, 35, 41-48, 54, 55, 59-66, 68, 75-83, 85, 94-102, 104

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"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
19 June 2013	08 JUL 2013
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)

Electronic Acknowledgement Receipt

EFS ID:	16903337
Application Number:	13340623
International Application Number:	
Confirmation Number:	1094
Title of Invention:	Systems and Methods for Playing Back Alternative Streams of Protected Content Protected Using Common Cryptographic Information
First Named Inventor/Applicant Name:	Michael George Kiefer
Customer Number:	71897
Filer:	William P. Wilbar/Katrina Lee
Filer Authorized By:	William P. Wilbar
Attorney Docket Number:	D1:02359A
Receipt Date:	19-SEP-2013
Filing Date:	29-DEC-2011
Time Stamp:	17:54:13
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	02359aidsxtml.pdf	102679 6c10dba8d87d06024949181a9fe7e3dad4d3e354	no	2

Warnings:	
Information:	

2	Information Disclosure Statement (IDS) Form (SB08)	02359aids1449.pdf	95731 462225ead226a8980d656d607315097727 78e2f3	no	2
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Non Patent Literature	02359asearchreport.pdf	3027703 b37d8f97a7bb89e8b2a3425ed8f8d54e4cc 81627	no	24
Warnings:					
Information:					
4	Foreign Reference	wo2011103364r.pdf	1983397 589cf663f3365bc98323aa65e1da611cbbb 2635a	no	30
Warnings:					
Information:					
5	Foreign Reference	wo2013032518.pdf	4882229 5ed766127e984c5d366c715025e5e4f5fffd 9b29	no	86
Warnings:					
Information:					
6	Foreign Reference	wo2013032518a3.pdf	2485175 51329007fbc2b2b7b8cbb35318dad502d5 dffa57	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	12576914		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being electronically filed with the United States Patent and Trademark Office on September 19, 2013 at or before 11:59 p.m. Pacific Time under the Rules of 37 C.F.R. 1.8.

/Katrina Lee/
Katrina Lee

Appl No.	: 13/340,623	Confirmation No. 1094
Applicant	: Michael George Kiefer, et al.	
Filed	: December 29, 2011	
Title	: Systems and Methods for Playing Back Alternative Streams of Protected Content Protected Using Common Cryptographic Information	
TC/A.U.	: 2434	
Examiner	: Abiy Getachew	
Docket No.	: D1:02359A	
Customer No.	: 71897	

INFORMATION DISCLOSURE STATEMENT § 1.97(b)

MAIL STOP AMENDMENT
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

2400 E. Katella, Suite 1050
Anaheim, CA 92806
September 19, 2013

Commissioner

In compliance with the duty of disclosure under 37 C.F.R. §§ 1.56, 1.97 and 1.98, and in accordance with the provisions in the MPEP §§ 609 and 707.05(b), enclosed is FORM PTO/SB/08A/B with a listing of references that are known to applicant. A copy of the reference listed under "Non-Patent Literature Documents" is enclosed.

It is respectfully requested that these references be considered in the examination of this application and identified on the list of references cited on the patent issuing on this application. Applicant also requests that an initialed copy of said FORM PTO/SB/08A/B be entered in the application file, and returned to the Applicant with the next official communication from the Office in accordance with MPEP § 609.

It is believed that there are no fees due in connection with this filing. If there are any fees due in connection with this filing, the Commissioner is authorized to charge Deposit Account 50-4407. Please show our docket number with any charge to the Deposit Account.

Respectfully submitted,

KPPB LLP

/William Wilbar/
William Wilbar
Registration No. 43,265
949.852.0000

WPW/kl

Enclosure(s)

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1136
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/340,623	12/29/2011	Michael George Kiefer	D1:02359A

CONFIRMATION NO. 1094

71897
KAUTH , POMEROY , PECK & BAILEY ,LLP
2400 EAST KATELLA AVENUE
SUITE 1050
ANAHEIM, CA 92806

PUBLICATION NOTICE

OC000000059718125

Title: Systems and Methods for Playing Back Alternative Streams of Protected Content Protected Using Common Cryptographic Information

Publication No.US-2013-0061045-A1
Publication Date:03/07/2013

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 13/340,623

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	380
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	620
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	250
TOTAL CLAIMS (37 CFR 1.16(i))	39 minus 20 =	* 19			OR	x 60 =	1140
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*				x 250 =	0.00
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	2390

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/340,623	12/29/2011	2431	2520	D1:02359A	39	3

CONFIRMATION NO. 1094

UPDATED FILING RECEIPT

71897
KAUTH , POMEROY , PECK & BAILEY ,LLP
2400 EAST KATELLA AVENUE
SUITE 1050
ANAHEIM, CA 92806

OC000000053374548

Date Mailed: 04/03/2012

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Michael George Kiefer, Scottsdale, AZ;
Eric William Grab, San Diego, CA;
Jason Braness, San Diego, CA;

Assignment For Published Patent Application

DIVX, LLC, Santa Clara, CA

Power of Attorney: The patent practitioners associated with Customer Number 71897

Domestic Priority data as claimed by applicant

This appln claims benefit of 61/530,305 09/01/2011

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)

If Required, Foreign Filing License Granted: 01/13/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/340,623**

Projected Publication Date: 03/07/2013

Non-Publication Request: No

Early Publication Request: No

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1139
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Title

Systems and Methods for Playing Back Alternative Streams of Protected Content Protected Using Common Cryptographic Information

Preliminary Class

713

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where

the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage, facilitate, and accelerate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being electronically filed with the United States Patent and Trademark Office on March 20, 2012 at or before 11:59 p.m. Pacific Time under the Rules of 37 C.F.R. 1.8.

/ Trudi Thompson /
Trudi Thompson

Applicant	: Michael George Kiefer	Confirmation No. 1094
Application No.	: 13/340623	
Filed	: December 29, 2012	
Title	: SYSTEMS AND METHODS FOR PLAYING BACK ALTERNATIVE STREAMS OF PROTECTED CONTENT PROTECTED USING COMMON CRYPTOGRAPHIC INFORMATION	
Grp./Div.	: 2431	
Examiner	: Unassigned	
Docket No.	: D1:02359A	
Customer No.	: 71897	

LETTER IN RESPONSE TO NOTICE TO FILE MISSING PARTS

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

2400 E. Katella, Suite 1050
Anaheim, CA 92806
March 20, 2012

Commissioner:

In response to the Notice to File Missing Parts dated January 18, 2012, enclosed are:

1. Declaration and Power of Attorney; and
2. Petition for Extension of Time

The $130 surcharge, basic filing fee of $380, examination fee of $250, search fee of $620 and $1140 additional claim fees (total $2520) will be paid via credit card.

The Commissioner is authorized to charge any fee under 37 CFR 1.16 and 1.17 which may be required during the **entire pendency** of the application to Deposit Account No. 50-4407. Please show our docket number with any transaction to the Deposit Account.

Respectfully submitted,

KAUTH, POMEROY, PECK & BAILEY LLP

By /David J. Bailey/
David J. Bailey
Registration No. 59,632
949.852.0000

DJB/t
Enclosures
24785

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
PETITION FOR EXTENSION OF TIME

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being electronically filed with the United States Patent and Trademark Office on March 20, 2012 at or before 11:59 p.m. Pacific Time under the Rules of 37 C.F.R. 1.8.

/ Trudi Thompson /
Trudi Thompson

Applicant	:	Michael George Kiefer	Confirmation No. 1094
Application No.	:	13/340623	
Filed	:	December 29, 2012	
Title	:	SYSTEMS AND METHODS FOR PLAYING BACK ALTERNATIVE STREAMS OF PROTECTED CONTENT PROTECTED USING COMMON CRYPTOGRAPHIC INFORMATION	
Grp./Div.	:	2431	
Examiner	:	Unassigned	
Docket No.	:	D1:02359A	
Customer No.	:	71897	

PETITION FOR EXTENSION OF TIME

Mail Stop MISSING PARTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

2400 E. Katella, Suite 1050
Anaheim, CA 92806
March 20, 2012

Commissioner:

Applicant petitions the Commissioner to extend the time for response to the Notice of Missing Parts dated January 18, 2012 for one month from March 18, 2012 to April 18, 2012.

The$150 extension of time fee required by 37 CFR § 1.17 will be paid via credit card. The Commissioner is hereby authorized to charge any fees under 37 CFR 1.16 and 1.17 which may be required during the **entire pendency** of the application to Deposit Account No. 50-4407. Please show our docket number with any charge or credit to our Deposit Account.

Respectfully submitted,

KAUTH, POMEROY, PECK & BAILEY LLP

By /David J. Bailey/
David J. Bailey
Reg. No. 59,632
949.852.0000

DJB/t
24843

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION PATENT

Docket No. : D1:02359A

As a below named inventor, I hereby declare that:

My residence, mailing address and citizenship are as stated below next to my name.
I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled SYSTEMS AND METHODS FOR PLAYING BACK ALTERNATIVE STREAMS OF PROTECTED CONTENT PROTECTED USING COMMON CRYPTOGRAPHIC INFORMATION, the specification of which is attached hereto unless the following is checked:

__X____ was filed on December 29, 2011 as United States Application Number or PCT International Application Number 13/340623 and was amended on ___ (if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR § 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT International filing date of the continuation-in-part application.

I hereby claim foreign priority benefits under 35 U.S.C. § 119(a)-(d) or § 365(b) of the foreign application(s) for patent or inventor's certificate, or § 365(a) of any PCT International application which designated at least one country other than the United States of America, listed below and have also identified below, any foreign application for patent or inventor's certificate, or any PCT International application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)

Application Number	Country	Filing Date (day/month/year)	Priority Claimed

I hereby claim the benefit under 35 U.S.C. § 119(e) of any United States provisional application(s) listed below.

Application Number	Filing Date
61/530305	September 1, 2011

I hereby claim the benefit under 35 U.S.C. § 120 of any United States application(s), or any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR § 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application.

Application Number	Filing Date	Patented/Pending/Abandoned

DECLARATION AND POWER OF ATTORNEY
FOR PATENT APPLICATION

Docket No.: D1:02359A

POWER OF ATTORNEY: I hereby appoint the practitioners associated with the law firm of Knuth, Pomeroy, Peck & Bailey LLP,

CUSTOMER NUMBER 71897

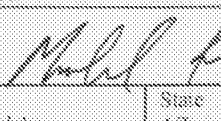
to prosecute this application and any U.S. continuation or divisional application based on it, and to prosecute any international application under the Patent Cooperation Treaty based on it, and to transact all business in the U.S. Patent and Trademark Office connected with either of them in accordance with instructions from the assignee of the entire interest in this application; or from the first or sole inventor named below in the event the application is not assigned; or from ___ in the event the power granted herein is for an application filed on behalf of a foreign attorney or agent.

The authority under this Power of Attorney of each person associated with the law firm of Knuth, Pomeroy, Peck & Bailey LLP, Customer Number 71897, shall automatically terminate and be revoked upon such person ceasing to be a member or associate of or of counsel to that law firm.

DIRECT ALL CORRESPONDENCE TO: CUSTOMER NUMBER 71897

DIRECT TELEPHONE CALLS TO: David J. Bailey, 949.852.0000
KNUTH, POMEROY, PECK & BAILEY LLP
2400 E. Katella, Suite 1050
Anaheim, CA 92806

I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

NAME OF FIRST INVENTOR			
Michael George Kuefer			
Inventor's Signature 			Date 2-24-2012
Residence: City Scottsdale	State AZ	Country US	Citizenship US
Mailing Address:	7007 E. Gold Dust Ave., Apt. 1053, Scottsdale, AZ 85253		

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1145
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

DECLARATION AND POWER OF ATTORNEY
FOR PATENT APPLICATION

Docket No.: D11023S9A

NAME OF SECOND INVENTOR			
Eric William Grab			
Inventor's Signature			Date Feb 24, 2012
Residence: City San Diego	State CA	Country US	Citizenship US
Mailing Address:	5387 Channing Street, San Diego, CA 92117		

NAME OF THIRD INVENTOR			
BRANESS, Jason			
Inventor's Signature			Date 2/24/2012
Residence: City San Diego	State CA	Country US	Citizenship US
Mailing Address:	15885 Concord Ridge Terrace, San Diego, CA 92127		

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1146
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION — PATENT

Docket No. : DI02359A

As a below named inventor, I hereby declare that:

My residence, mailing address and citizenship are as stated below next to my name.
I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled SYSTEMS AND METHODS FOR PLAYING BACK ALTERNATIVE STREAMS OF PROTECTED CONTENT PROTECTED USING COMMON CRYPTOGRAPHIC INFORMATION, the specification of which is attached hereto unless the following is checked:

__X____ was filed on December 29, 2011 as United States Application Number or PCT International Application Number 13/340623 and was amended on ___ (if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR § 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT International filing date of the continuation-in-part application.

I hereby claim foreign priority benefits under 35 U.S.C. § 119(a)-(d) or § 363(b) of the foreign application(s) for patent or inventor's certificate, or § 365(a) of any PCT International application which designated at least one country other than the United States of America, listed below and have also identified below, any foreign application for patent or inventor's certificate, or any PCT International application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)

Application Number	Country	Filing Date (day/month/year)	Priority Claimed

I hereby claim the benefit under 35 U.S.C. § 119(e) of any United States provisional application(s) listed below.

Application Number	Filing Date
61/530305	September 1, 2011

I hereby claim the benefit under 35 U.S.C. § 120 of any United States application(s), or any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR § 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application.

Application Number	Filing Date	Patented/Pending/Abandoned

DECLARATION AND POWER OF ATTORNEY
FOR PATENT APPLICATION

Docket No.: D1:02359A

POWER OF ATTORNEY: I hereby appoint the practitioners associated with the law firm of Knuth, Pomeroy, Peck & Bailey LLP,

CUSTOMER NUMBER 71897

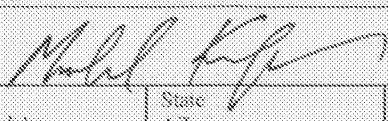
to prosecute this application and any U.S. continuation or divisional application based on it, and to prosecute any international application under the Patent Cooperation Treaty based on it, and to transact all business in the U.S. Patent and Trademark Office connected with either of them in accordance with instructions from the assignee of the entire interest in this application; or from the first or sole inventor named below in the event the application is not assigned; or from ___ in the event the power granted herein is for an application filed on behalf of a foreign attorney or agent.

The authority under this Power of Attorney of each person associated with the law firm of Knuth, Pomeroy, Peck & Bailey LLP, Customer Number 71897, shall automatically terminate and be revoked upon such person ceasing to be a member or associate of or of counsel to that law firm.

DIRECT ALL CORRESPONDENCE TO: CUSTOMER NUMBER 71897

DIRECT TELEPHONE CALLS TO: David J. Bailey, 949.852.0000
KNUTH, POMEROY, PECK & BAILEY LLP
2400 E. Katella, Suite 1050
Anaheim, CA 92806

I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

NAME OF FIRST INVENTOR			
Michael George Kiefer			
Inventor's Signature 			Date 2-24-2012
Residence: City Scottsdale	State AZ	Country US	Citizenship US
Mailing Address:	7007 E. Gold Dust Ave., Apt. 1053, Scottsdale, AZ 85253		

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1148
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

DECLARATION AND POWER OF ATTORNEY
FOR PATENT APPLICATION

Docket No.: D11023S9A

NAME OF SECOND INVENTOR			
Eric William Grab			
Inventor's Signature			Date Feb 24, 2012
City Residence: San Diego	State CA	Country US	Citizenship US
Mailing Address:	5387 Channing Street, San Diego, CA 92117		

NAME OF THIRD INVENTOR			
BRANESS, Jason			
Inventor's Signature			Date 2/24/2012
City Residence: San Diego	State CA	Country US	Citizenship US
Mailing Address:	15885 Concord Ridge Terrace, San Diego, CA 92127		

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1149
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Electronic Patent Application Fee Transmittal

Application Number:	13340623
Filing Date:	29-Dec-2011
Title of Invention:	Systems and Methods for Playing Back Alternative Streams of Protected Content Protected Using Common Cryptographic Information
First Named Inventor/Applicant Name:	Michael George Kiefer
Filer:	David J. Bailey/Trudi Thompson
Attorney Docket Number:	D1:02359A

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility application filing	1011	1	380	380
Utility Search Fee	1111	1	620	620
Utility Examination Fee	1311	1	250	250
Pages:				
Claims:				
Claims in excess of 20	1202	19	60	1140
Miscellaneous-Filing:				
Late filing fee for oath or declaration	1051	1	130	130

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 1 month with $0 paid	1251	1	150	150
Miscellaneous:				
		Total in USD ($)		**2670**

Electronic Acknowledgement Receipt

EFS ID:	12345629
Application Number:	13340623
International Application Number:	
Confirmation Number:	1094
Title of Invention:	Systems and Methods for Playing Back Alternative Streams of Protected Content Protected Using Common Cryptographic Information
First Named Inventor/Applicant Name:	Michael George Kiefer
Customer Number:	71897
Filer:	David J. Bailey/Trudi Thompson
Filer Authorized By:	David J. Bailey
Attorney Docket Number:	D1:02359A
Receipt Date:	20-MAR-2012
Filing Date:	29-DEC-2011
Time Stamp:	19:03:57
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$2670
RAM confirmation Number	6078
Deposit Account	504407
Authorized User	BAILEY,DAVID

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)	
Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)	
Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Applicant Response to Pre-Exam Formalities Notice	02359amissingpartsxmtl.pdf	12808 5f9d8e96e50c0f02b799f34c5ae3df875ae620db	no	1
Warnings:					
Information:					
2	Extension of Time	02359aextensionoftime.pdf	24624 2ce6ab815eead605611b361b6e08de9213b35295	no	1
Warnings:					
Information:					
3	Power of Attorney	02359apower.pdf	2316519 3c3d66e95986885460ec1e3d056f356481ebb1c6	no	3
Warnings:					
Information:					
4	Oath or Declaration filed	02359aoath.pdf	2317243 3f405675f2175a6e86f4ab523d5c955ef9d72d4e	no	3
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	40165 c07bb32451adbd1777010aa73ce59fe0dcf50683	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	4711359		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/340,623	12/29/2011	Michael George Kiefer	D1:02359A

CONFIRMATION NO. 1094

71897
KAUTH , POMEROY , PECK & BAILEY ,LLP
2400 EAST KATELLA AVENUE
SUITE 1050
ANAHEIM, CA 92806

FORMALITIES LETTER

OC000000052000076

Date Mailed: 01/18/2012

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The statutory basic filing fee is missing.
  *Applicant must submit $**380** to complete the basic filing fee for a non-small entity. If appropriate, applicant may make a written assertion of entitlement to small entity status and pay the small entity filing fee (37 CFR 1.27).*
- The oath or declaration is missing.
  A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.
  Note: If a petition under 37 CFR 1.47 is being filed, an oath or declaration in compliance with 37 CFR 1.63 signed by all available joint inventors, or if no inventor is available by a party with sufficient proprietary interest, is required.

The applicant needs to satisfy supplemental fees problems indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- Additional claim fees of $**1140** as a non-small entity, including any required multiple dependent claim fee, are required. Applicant must submit the additional claim fees or cancel the additional claims for which fees are due.
- A surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.16(f) of $**130** for a non-small entity, must be submitted.

SUMMARY OF FEES DUE:

Total fee(s) required within **TWO MONTHS** from the date of this Notice is $**2520** for a non-small entity
- $**380** Statutory basic filing fee.
- $**130** Surcharge.
- The application search fee has not been paid. Applicant must submit $**620** to complete the search fee.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1155
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

- The application examination fee has not been paid. Applicant must submit $**250** to complete the examination fee for a non-small entity.
- Total additional claim fee(s) for this application is $**1140**
  - $**1140** for **19** total claims over 20.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web.
https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

/smunpanthovong/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1156
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/340,623	12/29/2011	2431	0.00	D1:02359A	39	3

CONFIRMATION NO. 1094

71897
KAUTH , POMEROY , PECK & BAILEY ,LLP
2400 EAST KATELLA AVENUE
SUITE 1050
ANAHEIM, CA 92806

FILING RECEIPT

OC000000052000075

Date Mailed: 01/18/2012

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Michael George Kiefer, Scottsdale, AZ;
Eric William Grab, San Diego, CA;
Jason Braness, San Diego, CA;

Assignment For Published Patent Application

DIVX, LLC, Santa Clara, CA

Power of Attorney: None

Domestic Priority data as claimed by applicant

This appln claims benefit of 61/530,305 09/01/2011

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)

If Required, Foreign Filing License Granted: 01/13/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/340,623**

Projected Publication Date: To Be Determined - pending completion of Missing Parts

Non-Publication Request: No

Early Publication Request: No

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1157
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Title

Systems and Methods for Playing Back Alternative Streams of Protected Content Protected Using Common Cryptographic Information

Preliminary Class

713

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where

the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage, facilitate, and accelerate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 13/340,623

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	380
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	620
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	250
TOTAL CLAIMS (37 CFR 1.16(i))	39 minus 20 =	* 19			OR	x 60 =	1140
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*				x 250 =	0.00
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	2390

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

PTO/SB/14 (11-08)
Approved for use through 09/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	D1:02359A
	Application Number	
Title of Invention	Systems and Methods for Playing Back Alternative Streams of Protected Content Protected Using Common Cryptographic Information	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Applicant Information:

Applicant 1

Applicant Authority	◉ Inventor	◯ Legal Representative under 35 U.S.C. 117	◯ Party of Interest under 35 U.S.C. 118

Prefix	Given Name	Middle Name	Family Name	Suffix
	Michael	George	Kiefer	

Residence Information (Select One)	◉ US Residency	◯ Non US Residency	◯ Active US Military Service

City	Scottsdale	State/Province	AZ	Country of Residence	US

Citizenship under 37 CFR 1.41(b)	US

Mailing Address of Applicant:

Address 1	7007 E. Gold Dust Ave.
Address 2	APT. 1053

City	Scottsdale	State/Province	AZ
Postal Code	85253	Country	US

Applicant 2

Applicant Authority	◉ Inventor	◯ Legal Representative under 35 U.S.C. 117	◯ Party of Interest under 35 U.S.C. 118

Prefix	Given Name	Middle Name	Family Name	Suffix
	Eric	William	Grab	

Residence Information (Select One)	◉ US Residency	◯ Non US Residency	◯ Active US Military Service

City	San Diego	State/Province	CA	Country of Residence	US

Citizenship under 37 CFR 1.41(b)	US

Mailing Address of Applicant:

Address 1	5387 Channing Street
Address 2	

City	San Diego	State/Province	CA
Postal Code	92117	Country	US

Applicant 3

Applicant Authority	◉ Inventor	◯ Legal Representative under 35 U.S.C. 117	◯ Party of Interest under 35 U.S.C. 118

Prefix	Given Name	Middle Name	Family Name	Suffix
	Jason		Braness	

Residence Information (Select One)	◉ US Residency	◯ Non US Residency	◯ Active US Military Service

City	San Diego	State/Province	CA	Country of Residence	US

PTO/SB/14 (11-08)
Approved for use through 09/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	D1:02359A
	Application Number	
Title of Invention	Systems and Methods for Playing Back Alternative Streams of Protected Content Protected Using Common Cryptographic Information	

Citizenship under 37 CFR 1.41(b)	US		
Mailing Address of Applicant:			
Address 1	15885 Concord Ridge Terrace		
Address 2			
City	San Diego	**State/Province**	CA
Postal Code	92127	**Country**	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	71897		
Email Address	pto@kppb.com	Add Email	Remove Email

Application Information:

Title of the Invention	Systems and Methods for Playing Back Alternative Streams of Protected Content Protected Using Common Cryptographic Information		
Attorney Docket Number	D1:02359A	**Small Entity Status Claimed**	☐
Application Type	Nonprovisional		
Subject Matter			
Suggested Class (if any)		**Sub Class (if any)**	
Suggested Technology Center (if any)			
Total Number of Drawing Sheets (if any)	19	**Suggested Figure for Publication (if any)**	1

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Enter either Customer Number or complete the Representative Name section below. If both sections are completed the Customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)

PTO/SB/14 (11-08)
Approved for use through 09/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	D1:02359A
	Application Number	
Title of Invention	Systems and Methods for Playing Back Alternative Streams of Protected Content Protected Using Common Cryptographic Information	

Customer Number	71897

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.

Prior Application Status			Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	non provisional of	61/530305	2011-09-01

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.

Foreign Priority Information:

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).

Remove

Application Number	Country	Parent Filing Date (YYYY-MM-DD)	Priority Claimed
			◉ Yes ○ No

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button.

Assignee Information:

Providing this information in the application data sheet does not substitute for compliance with any requirement of part 3 of Title 37 of the CFR to have an assignment recorded in the Office.

Assignee 1

If the Assignee is an Organization check here. ☒

Organization Name	DIVX, LLC		
Mailing Address Information:			
Address 1	2830 De La Cruz Boulevard		
Address 2			
City	Santa Clara	**State/Province**	CA
Country	US	Postal Code	95050
Phone Number		Fax Number	
Email Address			

Additional Assignee Data may be generated within this form by selecting the **Add** button.

Signature:

A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature.

PTO/SB/14 (11-08)
Approved for use through 09/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	D1:02359A
	Application Number	
Title of Invention	Systems and Methods for Playing Back Alternative Streams of Protected Content Protected Using Common Cryptographic Information	

Signature	/David J. Bailey/			Date (YYYY-MM-DD)	2011-12-29
First Name	David	Last Name	Bailey	Registration Number	59632

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

SYSTEMS AND METHODS FOR PLAYING BACK ALTERNATIVE STREAMS OF PROTECTED CONTENT PROTECTED USING COMMON CRYPTOGRAPHIC INFORMATION

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to U.S. Provisional Application Serial No. 61/530,305 filed September 1, 2011, entitled "Multi-Asset Protected Content Multimedia Delivery System" the entirety of which is incorporated herein by reference.

FIELD OF THE INVENTION

[0002] The present invention generally relates to adaptive streaming and more specifically to adaptive bitrate streaming of encoded media contained within Matroska container files using Hypertext Transfer Protocol.

BACKGROUND

[0003] The term streaming media describes the playback of media on a playback device, where the media is stored on a server and continuously sent to the playback device over a network during playback. Typically, the playback device stores a sufficient quantity of media in a buffer at any given time during playback to prevent disruption of playback due to the playback device completing playback of all the buffered media prior to receipt of the next portion of media. In many instances, content is divided into multiple streams. For example, content can be divided into audio, video, and subtitle streams and some streams can be encoded as alternative streams that are suitable for different network connection bandwidths or comply with specific geographic restrictions and/or other restrictions.

[0004] Adaptive bit rate streaming or adaptive streaming involves detecting the present streaming conditions (e.g. the user's network bandwidth and CPU capacity) in real time and adjusting the quality of the streamed media accordingly by selecting between different streams encoded for use at different network connection data rates.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1165
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Typically, the source media is encoded at multiple bitrates and the playback device or client switches between streaming the different encodings depending on available resources.

[0005] Adaptive streaming solutions typically utilize either Hypertext Transfer Protocol (HTTP), published by the Internet Engineering Task Force and the World Wide Web Consortium as RFC 2616 to stream media between a server and a playback device. HTTP is a stateless protocol that enables a playback device to request a byte range within a file. HTTP is described as stateless, because the server is not required to record information concerning the state of the playback device requesting information or the byte ranges requested by the playback device in order to respond to requests received from the playback device.

[0006] In adaptive streaming systems, the source media is typically stored on a media server as a top level index file pointing to a number of alternate streams that contain the actual video and audio data. Each stream is typically stored in one or more container files. Different adaptive streaming solutions typically utilize different index and media containers. The Synchronized Multimedia Integration Language (SMIL) developed by the World Wide Web Consortium is utilized to create indexes in several adaptive streaming solutions including IIS Smooth Streaming developed by Microsoft Corporation of Redmond, Washington, and Flash Dynamic Streaming developed by Adobe Systems Incorporated of San Jose, California. HTTP Adaptive Bitrate Streaming developed by Apple Computer Incorporated of Cupertino, California implements index files using an extended M3U playlist file (.M3U8), which is a text file containing a list of URIs that typically identify a media container file. The most commonly used media container formats are the MP4 container format specified in MPEG-4 Part 14 (i.e. ISO/IEC 14496-14) and the MPEG transport stream (TS) container specified in MPEG-2 Part 1 (i.e. ISO/IEC Standard 13818-1). The MP4 container format is utilized in IIS

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1166
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Smooth Streaming and Flash Dynamic Streaming. The TS container is used in HTTP Adaptive Bitrate Streaming.

[0007] The Matroska container is a media container developed as an open standard project by the Matroska non-profit organization of Aussonne, France. The Matroska container is based upon Extensible Binary Meta Language (EBML), which is a binary derivative of the Extensible Markup Language (XML). Decoding of the Matroska container is supported by many consumer electronics (CE) devices. The DivX Plus file format developed by DivX, LLC of San Diego, California utilizes an extension of the Matroska container format (i.e. is based upon the Matroska container format, but includes elements that are not specified within the Matroska format).

[0008] The term Digital Rights Management (DRM) is utilized to describe access control technologies that are used to control access to and/or copying of digital content. DRM systems typically involve the use of cryptographic information to control access to or protect a piece of content. Content protection is typically achieved using cryptographic information such as (but not limited to) one or more encryption keys to encrypt some or all of the content. An important component of most DRM systems is a mechanism for securely providing cryptographic information to authorized playback devices for use in accessing protected content. The protected content cannot be accessed without the cryptographic data and ideally the cryptographic data is bound to specific playback devices and cannot be readily used by unauthorized playback devices or is securely provided to the playback devices (often on a session basis).

SUMMARY OF THE INVENTION

[0009] Systems and methods in accordance with embodiments of the invention perform adaptive bitrate streaming using alternative streams of protected content. One embodiment of the invention includes a processor, and memory containing a client application. In addition, the client application configures the processor to: request a top

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1167
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

level index file identifying a plurality of alternative streams of protected content, where each of the alternative streams of protected content are encrypted using common cryptographic information; obtain the common cryptographic information; request portions of content from at least the plurality of alternative streams of protected content; access the protected content using the common cryptographic information; and playback the content.

[0010] In a further embodiment, the alternative streams of protected content are alternative streams of protected video, each of the alternative streams of protected video includes DRM information indicating portions of frames of video that are encrypted and identifying at least a portion of the common cryptographic information used to access the encrypted portions of the frames of video, and the client application configures the processor to: obtain a protected frame of video from one of the alternative streams of protected video; obtain DRM information indicating a portion of the protected frame of video that is encrypted; identify at least a portion of the common cryptographic information that is used to access the encrypted portion of the protected frame using the DRM information; decrypt the encrypted portion of the protected frame of video using the identified portion of the common cryptographic information; and decode the frame of video.

[0011] In another embodiment, each of the alternative streams of protected content is contained within a separate container file, and the top level index file identifies a container file containing each of the alternative streams.

[0012] In still further embodiment, the container files containing each of the alternative streams of protected content includes at least one header including the common cryptographic information and information that describes the encoding of the stream of protected content, and the top level index file identifies the location of the at least one header within each container file.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1168
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

[0013] In still another embodiment, the common cryptographic information is a set of encryption keys.

[0014] In a yet further embodiment, the common set of encryption keys is encrypted; and the client application configures the processor to securely receive cryptographic information used to unencrypt the common set of encryption keys.

[0015] In yet another embodiment, the client application configures the processor to obtain the common cryptographic information by requesting at least one header of a container file identified in the top level index file.

[0016] In a further embodiment again, each container file containing one of the alternative streams of protected content further includes an index, and the client application configures the processor to request a portion of content from one of the container files by configuring the processor to: request at least a portion of an index from the container file; identify the portion of the container file containing a specific portion of content using the index; and request the identified portion of the container file.

[0017] In another embodiment again, the container files are Matroska container files.

[0018] In a further additional embodiment, the common cryptographic information is stored in a common DRM Header element contained within a Tracks element within each of the Matroska container files containing the alternative streams of protected content.

[0019] In another additional embodiment, the common cryptographic information is a set of encryption keys; and the set of encryption keys is encrypted and stored within the DRM Header element.

[0020] In a still yet further embodiment, the client application configures the processor to: obtain cryptographic information that can be used to unencrypt the set of encryption keys stored within the DRM Header element; and unencrypt the set of

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1169
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

encryption keys stored within the DRM Header element using the obtained cryptographic information.

[0021] In still yet another embodiment, the client application configures the processor to obtain the DRM Header element by requesting a Tracks element from one of the Matroska container files identified in the top level index file.

[0022] In a still further embodiment again, each Mastroska container file containing an alternative stream of protected content further includes an index contained within a Cues element, and the client application configures the processor to request a portion of content from one of the Matroska container files by configuring the processor to: request at least a portion of a Cues element from a Matroska container file containing one of the alternative streams of protected content; identify a portion of the Matroska container file containing a specific portion of content using at least one CueTrackPosition element within the Cues element; and request the portion of the Matroska container file identified by the at least one CueTrackPosition element.

[0023] In still another embodiment again, the index includes a plurality of CueTrackPosition elements that identify the location of a plurality of Cluster elements within the Matroska container file.

[0024] In a still further additional embodiment, each Cluster element contains a plurality of BlockGroup elements including encoded portions of content, a CueTrack Position element indexes each Cluster element, and each CueTrackPosition element includes the size of the Cluster element that it indexes.

[0025] In still another additional embodiment, the alternative streams of protected content are alternative streams of protected video, each of the Matroska container files containing an alternative stream of protected video includes a DRMInfo element in a BlockGroup element containing a protected frame of video, where the DRMInfo element indicates at least a portion of the protected frames of video that is encrypted and identifies at least a portion of the common cryptographic information used to access the

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1170
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

at least one encrypted portion of the protected frame of video, and the client application configures the processor to access video frames in a stream of protected video using the common cryptographic information by configuring the processor to: obtain a BlockGroup containing a protected frame of video; parse the BlockGroup element to obtain a DRMInfo element indicating at least a portion of the protected frame of video that is encrypted using an encryption key from the set of encryption keys; decrypt the at least one encrypted portion of the protected frame of video using the identified encryption key; and decode the frame of video.

[0026] An embodiment of the method of the invention includes requesting a top level index file identifying a plurality of alternative streams of protected content using a playback device, where each of the alternative streams of protected content are encrypted using common cryptographic information, obtaining the common cryptographic information using the playback device, requesting portions of content from at least the plurality of alternative streams of protected content using the playback device, accessing the protected content using the playback device and the common cryptographic information, and playing back the content using the playback device.

[0027] In a further embodiment of the method of the invention, the alternative streams of protected content are alternative streams of protected video, each of the alternative streams of protected video includes DRM information indicating portions of frames of video that are encrypted and identifying at least a portion of the common cryptographic information used to access the encrypted portions of the frames of video, and the method further includes obtaining a protected frame of video from one of the alternative streams of protected video using the playback device, obtaining DRM information indicating a portion of the protected frame of video that is encrypted using the playback device, identify at least a portion of the common cryptographic information that is used to access the encrypted portion of the protected frame using the playback device and the DRM information, decrypting the encrypted portion of the protected

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1171
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

frame of video using the playback device and the identified portion of the common cryptographic information, and decoding the frame of video using the playback device.

[0028] In another embodiment of the method of the invention, each of the alternative streams of protected content is contained within a separate container file, and the top level index file identifies a container file containing each of the alternative streams.

[0029] In a still further embodiment of the method of the invention, the container files containing each of the alternative streams of protected content include at least one header including the common cryptographic information and information that describes the encoding of the stream of protected content, and the top level index file identifies the location of the at least one header within each container file.

[0030] In still another embodiment of the method of the invention, the common cryptographic information is a set of encryption keys.

[0031] In a yet further embodiment of the method of the invention, the set of encryption keys is encrypted so that it is accessible using cryptographic information obtained by the playback device, and the method further comprising obtaining cryptographic information using the playback device.

[0032] In yet another embodiment of the method of the invention, the set of encryption keys is encrypted using at least one encryption key, and the playback device securely obtains the at least one encryption key.

[0033] In a further embodiment again of the method of the invention, the at least one encryption key is encrypted using at least one encryption key included in the cryptographic information bound to the playback device.

[0034] Another embodiment again of the method of the invention also includes obtaining the common cryptographic information by requesting at least one header of a container file identified in the top level index file using the playback device.

[0035] In a further additional embodiment of the method of the invention, each container file containing one of the alternative streams of protected content further

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1172
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

includes an index, and the method further includes: requesting at least a portion of an index from the container file using the playback device; identify the portion of the container file containing a specific portion of content using the playback device and the index; and requesting the identified portion of the container file using the playback device.

[0036] In another additional embodiment of the method of the invention, the container files are Matroska container files.

[0037] In a still yet further embodiment of the method of the invention, the common cryptographic information is stored in a common DRM Header element contained within a Tracks element within each of the Matroska container files containing the alternative streams of protected content.

[0038] In still yet another embodiment of the method of the invention, the common cryptographic information is a set of encryption keys, and the set of encryption keys is encrypted and stored within the DRM Header element.

[0039] In a still further embodiment again of the method of the invention, the set of encryption keys is encrypted so that it is accessible using cryptographic information obtained by the playback device, and the method further comprising obtaining cryptographic information using the playback device.

[0040] Still another embodiment again of the method of the invention also includes obtaining the DRM Header element by requesting a Tracks element from one of the Matroska container files identified in the top level index file.

[0041] In a still further additional embodiment of the method of the invention, each Mastroska container file containing an alternative stream of protected content further includes an index contained within a Cues element, andthe method further includes: requesting at least a portion of a Cues element from a Matroska container file containing one of the alternative streams of protected content using the playback device; identifying a portion of the Matroska container file containing a specific portion

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1173
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

of content using the playback device and at least one CueTrackPosition element within the Cues element; and requesting the portion of the Matroska container file identified by the at least one CueTrackPosition element.

[0042] In still another additional embodiment of the method of the invention, the index includes a plurality of CueTrackPosition elements that identify the location of a plurality of Cluster elements within the Matroska container file.

[0043] In a yet further embodiment again of the method of the invention, each Cluster element contains a plurality of BlockGroup elements including encoded portions of content, a CueTrack Position element indexes each Cluster element, and each CueTrackPosition element includes the size of the Cluster element that it indexes.

[0044] In yet another embodiment again of the method of the invention, the alternative streams of protected content are alternative streams of protected video, each of the Matroska container files containing an alternative stream of protected video includes a DRMInfo element in a BlockGroup element containing a protected frame of video, where the DRMInfo element indicates at least a portion of the protected frames of video that is encrypted and identifies at least a portion of the common cryptographic information used to access the at least one encrypted portion of the protected frame of video, and the method further includes: obtaining a BlockGroup containing a protected frame of video using the playback device; parsing the BlockGroup element to obtain a DRMInfo element indicating at least a portion of the protected frame of video that is encrypted using the playback device and an encryption key from the set of encryption keys; decrypting the at least one encrypted portion of the protected frame of video using the playback device and the identified encryption key; and decoding the frame of video using the playback device.

[0045] Another further embodiment includes a machine readable medium containing processor instructions, where execution of the instructions by a processor causes the processor to perform a process including request a top level index file

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1174
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

identifying a plurality of alternative streams of protected content, where each of the alternative streams of protected content are encrypted using common cryptographic information, obtaining the common cryptographic information, requesting portions of content from at least the plurality of alternative streams of protected content, accessing the protected content using the common cryptographic information, and playing back the content.

[0046] In still another further embodiment, the alternative streams of protected content are alternative streams of protected video, each of the alternative streams of protected video includes DRM information indicating portions of frames of video that are encrypted and identifying at least a portion of the common cryptographic information used to access the encrypted portions of the frames of video, and execution of the instructions by a processor also causes the processor to perform a process including: obtaining a protected frame of video from one of the alternative streams of protected video; obtaining DRM information indicating a portion of the protected frame of video that is encrypted; identify at least a portion of the common cryptographic information that is used to access the encrypted portion of the protected frame using the DRM information; decrypting the encrypted portion of the protected frame of video using and the identified portion of the common cryptographic information; and decoding the frame of video.

[0047] In yet another further embodiment, the machine readable medium is non-volatile memory.

BRIEF DESCRIPTION OF THE DRAWINGS

[0048] FIG. 1A is a network diagram of an adaptive bitrate streaming system in accordance with an embodiment of the invention.

[0049] FIG. 1B is a block diagram illustrating a source encoder in accordance with an embodiment of the invention.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1175
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

[0050] FIG. 1C is a block diagram illustrating a content distribution server in accordance with an embodiment of the invention.

[0051] FIG. 1D is a block diagram illustrating a playback device in accordance with an embodiment of the invention.

[0052] FIG. 2 conceptually illustrates a top level index file and Matroska container files generated by the encoding of source media in accordance with embodiments of the invention.

[0053] FIG. 3 conceptually illustrates a specialized Matroska container file incorporating a TracksData Payload containing cryptographic information in accordance with an embodiment of the invention.

[0054] FIGS. 4a – 4c conceptually illustrate the insertion of different types of protected media into the Clusters element of a Matroska container file subject to various constraints that facilitate adaptive bitrate streaming in accordance with embodiments of the invention.

[0055] FIG. 4d conceptually illustrates the multiplexing of different types of protected media into the Clusters element of a Matroska container file subject to various constraints that facilitate adaptive bitrate streaming in accordance with an embodiment of the invention.

[0056] FIG. 4e conceptually illustrates the inclusion of a protected trick play track into the Clusters element of a Matroska container file subject to various constraints that facilitate adaptive bitrate streaming in accordance with an embodiment of the invention.

[0057] FIG. 5 conceptually illustrates a modified Cues element of a specialized Matroska container file, where the Cues element includes information enabling the retrieval of Cluster elements using HTTP byte range requests in accordance with an embodiment of the invention.

[0058] FIG. 5a conceptually illustrates a modified Cues element of a specialized Matroska container file in accordance with an embodiment of the invention, where the

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1176
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Cues element is similar to the Cues element shown in FIG. 5 with the exception that attributes that are not utilized during adaptive bitrate streaming are removed.

[0059] FIG. 6 conceptually illustrates the indexing of Cluster elements within a specialized Matroska container file utilizing modified CuePoint elements within the container file in accordance with embodiments of the invention.

[0060] FIG. 7 conceptually illustrates the use of a hierarchical index to index CuePoint elements within a Matroska container file in accordance with embodiments of the invention.

[0061] FIG. 8 is a flow chart illustrating a process for encoding and protecting source media for adaptive bitrate streaming in accordance with an embodiment of the invention.

[0062] FIG. 9 is a flow chart illustrating a process for encoding and encrypting frames of source video in accordance with an embodiment of the invention.

[0063] FIG. 10 conceptually illustrates a DRM header element that can be included in a Matroska container file in accordance with an embodiment of the invention.

[0064] FIG. 11 conceptually illustrates communication between a playback device and an HTTP server associated with the commencement of streaming of encoded media contained within Matroska container files indexed by a top level index file in accordance with an embodiment of the invention.

[0065] FIGS. 12a and 12b conceptually illustrate communication between a playback device and an HTTP server associated with switching between streams in response to the streaming conditions experienced by the playback device prior to the decision to switch streams in accordance with embodiments of the invention.

DETAILED DISCLOSURE OF THE INVENTION

[0066] Turning now to the drawings, systems and methods for performing adaptive bitrate streaming using alternative streams of protected content in accordance with

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1177
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

embodiments of the invention are illustrated. In a number of embodiments, source media is encoded as a number of alternative streams and the alternative streams are protected using a common set of cryptographic information. In many embodiments, the alternative streams are video streams and each stream is protected by encrypting at least a portion of a plurality of video frames within the stream using the common set of cryptographic information. In several embodiments, the common set of cryptographic information is a set of frame keys. In order to protect a video frame, a frame key can be selected from the set of frame keys and used to encrypt at least a portion of the encoded frame and DRM information can be provided with the protected frame indicating the frame key utilized to perform the encryption and the location of the encrypted portion within the frame. By encrypting each of the alternative streams using the same set of cryptographic information, a playback device can switch between streams without the need to maintain or acquire multiple sets of cryptographic information in memory or to reinitialize the decryption engine of the playback device with a different set of cryptographic information.

[0067] In many embodiments, each of the alternative streams is stored in a separate container file referenced by a top level index file. In several embodiments, the common cryptographic information is embedded in each of the container files so that a playback device has access to the cryptographic information irrespective of which alternative is initially select to commence playback of the media. The common cryptographic information can be stored on a content distribution system and associated with a title identifier or title ID that uniquely identifies the source content used to create the alternative streams. When a new alternative stream is generated, a source encoder can utilize the title ID to request the common cryptographic information from the content distribution system and the common cryptographic information can be utilized to encrypt the new alternative stream and embedded in a container file created to contain the new encrypted alternative stream.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1178
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

[0068] In several embodiments, each stream associated with a piece of source content and/or title ID is stored in a Matroska (MKV) container file. In many embodiments, the Matroska container file is a specialized Matroska container file in that the manner in which the media in each stream is encoded and stored within the container is constrained to improve streaming performance. In several embodiments, the Matroska container file is further specialized in that additional DRM elements (i.e. elements that are not specified as part of the Matroska container format) can be included within the file to facilitate the distribution of protected media during adaptive bitrate streaming. In a number of embodiments, common cryptographic information is included within a DRM header element in each of the Matroska container files and references to the common cryptographic information are made using DRMInfo elements within a BlockGroup element corresponding to a specific frame of encrypted video. In other embodiments, any of a variety of mechanisms can be utilized to store DRM information within a Matroska container in accordance with embodiments of the invention. In several embodiments, each stream (i.e. audio, video, or subtitle) is stored within a separate Matroska container file. In other embodiments, an encoded video stream is multiplexed with one or more encoded audio, and/or subtitle streams in each Matroska container file.

[0069] A top level index file containing an index to the streams contained within each of the container files is also generated to enable adaptive bitrate streaming of the encoded media. In many embodiments, the top level index file is a Synchronized Multimedia Integration Language (SMIL) file containing URIs for each of the Matroska container files. In other embodiments, any of a variety of file formats can be utilized in the generation of the top level index file.

[0070] The performance of an adaptive bitstrate streaming system in accordance with embodiments of the invention can be significantly enhanced by encoding each portion of the source video at each bit rate in such a way that the portion of video is

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1179
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

encoded in each stream as a single (or at least one) closed group of pictures (GOP) starting with an Instantaneous Decoder Refresh (IDR) frame. The GOP for each stream can then be stored as a Cluster element within the Matroska container file for the stream. In this way, the playback device can switch between streams at the completion of the playback of a Cluster and, irrespective of the stream from which a Cluster is obtained the first frame in the Cluster will be an IDR frame and can be decoded without reference to any encoded media other than the encoded media contained within the Cluster element. In many embodiments, the sections of the source video that are encoded as GOPs are all the same duration. In a number of embodiments each two second sequence of the source video is encoded as a GOP.

[0071] Adaptive streaming of source media encoded in the manner outlined above can be coordinated by a playback device in accordance with embodiments of the invention. The playback device obtains information concerning each of the available streams from the top level index file and selects one or more streams to utilize in the playback of the media. The playback device can then obtain header information from the Matroska container files containing the one or more bitstreams or streams, and the headers provide information concerning the decoding of the streams including a DRM header, which contains the cryptographic information utilized to protect the stream. The playback device can also request index information that indexes the encoded media stored within the relevant Matroska container files. The index information can be stored within the Matroska container files or separately from the Matroska container files in the top level index or in separate index files. The index information enables the playback device to request byte ranges corresponding to Cluster elements within the Matroska container file containing specific portions of encoded media via HTTP from the server. As the playback device receives the Cluster elements from the HTTP server, the playback device can evaluate current streaming conditions to determine whether to increase or decrease the bitrate of the streamed media. In the event that the playback

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1180
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

device determines that a change in bitrate is necessary, the playback device can obtain header information and index information for the container file(s) containing the desired stream(s) (assuming the playback device has not already obtained this information). The playback device need not perform the computationally intensive process of accessing the encrypted cryptographic information in the header of the new stream, because each of the alternative streams uses common cryptographic information. The index information can then be used to identify the byte range of the Cluster element containing the next portion of the source media encoded at the desired bit rate and the identified Cluster element can be retrieved from the server via HTTP. The next portion of the source media that is requested is typically identified based upon the Cluster elements already requested by the playback device and the Cluster elements buffered by the playback device. The next portion of source media requested from the alternative stream is requested to minimize the likelihood that the buffer of the playback device will underflow (i.e. run out media to playback) prior to receipt of the Cluster element containing the next portion of source media by the playback device. In this way, the playback device can achieve adaptive bitrate streaming by retrieving sequential Cluster elements from the various streams as appropriate to the streaming conditions using the top level index and index information describing the Cluster elements within each of the Matroska container files.

[0072] In a number of embodiments, variation in the bitrate between different streams can be achieved by modifying the encoding parameters for each stream including but not limited to the bitrate, frame rate, resolution and sample aspect ratio. The encoding and protection of source video using common cryptographic information for use in adaptive bitrate streaming and the playback of alternative streams of protected content via adaptive bitrate streaming in accordance with embodiments of the invention is discussed further below.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1181
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

ADAPTIVE STREAMING SYSTEM ARCHITECTURE

[0073] An adaptive bitrate streaming system in accordance with an embodiment of the invention is illustrated in FIG. 1. The adaptive streaming system 10 includes a source encoder 12 configured to encode source media as a number of alternative streams and to protect the encoded streams using common cryptographic information. Alternative streams are streams that encode the same media content in different ways. In several embodiments, the source encoder 12 ingests source content and obtains a title ID and common cryptographic information from a content distribution server 14 that the content distribution server assigns to the source content. The source encoder encodes the alternative streams and protects the streams using the common cryptographic information received from the content distribution server. In many instances, alternative streams encode media content (such as but not limited to video) at different maximum bitrates. In a number of embodiments, the alternative streams are encoded with different resolutions, sample aspect ratios and/or frame rates. When the streams are written to file(s), the common cryptographic information is also written to the file(s). The content distribution server 14 can receive request to access the alternative streams of content (i.e. the title) via the Internet from a playback device such as (but not limited to) a user computer 18 or a mobile phone 20 and can commence streaming content. In several embodiments, the common cryptographic information is protected by encrypting at least a portion of the common cryptographic information using at least one encryption key. The playback device can securely obtain the cryptographic key using a process such as (but not limited to) Hypertext Transfer Protocol Secure or HTTPS. Other processes for securely obtaining cryptographic information to obtain access to encrypted common cryptographic information in accordance with embodiments of the invention are discussed below.

[0074] In many embodiments, a playback device commences playback by requesting a top level index file from the content distribution server. The source encoder 12, the

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1182
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

content distribution server 14, or another server can generate the top level index to the file(s) containing the streams, at least a plurality of which are alternative streams, at the time the request is made or at the time the streams are generated by the source encoder. The playback device can then use HTTP or another appropriate stateless protocol to request portions of the top level index file and the file(s) containing the protected streams via a network 16 such as the Internet.

[0075] In many embodiments, the top level index file is a SMIL file and the media is stored in Matroska container files. As is discussed further below, the media can be stored within the Matroska container file in a way that facilitates the protection of the content using common cryptographic information. In many embodiments, the Matroska container files are specialized Matroska container files that include enhancements (i.e. elements that do not form part of the Matroska file format specification) that facilitate retrieval and decryption using common cryptographic information of specific portions of media during adaptive bitrate streaming.

[0076] Although a specific content distribution system configured to support adaptive bitrate streaming is illustrated in FIG. 1A, any of a variety of content distribution system architectures can be utilized to implement an adaptive bitrate streaming system in accordance with embodiments of the invention. Source encoders, content distribution server systems, and playback devices in accordance with embodiments of the invention are discussed further below.

SOURCE ENCODERS

[0077] In many embodiments, a source encoder can be implemented using a server. In other embodiments, the source encoder can be any processing device including a processor and sufficient resources to perform the transcoding and encryption of source media (including but not limited to video, audio, and/or subtitles). A source encoder in accordance with an embodiment of the invention is illustrated in FIG. 1B. The source

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1183
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

encoder 12 is implemented on a computing platform including a processor 12a, volatile memory 12b and non-volatile storage 12c. An encoder application 12d is stored in non-volatile storage 12c. The encoder application includes the machine readable instructions that configure the processor to encode source content 12e as a plurality of streams. In a number of embodiments, the encoder application also configures the source encoder to obtain common cryptographic information 12g that can be utilized to protect alternative streams generated using the source content 12e. In many embodiments, the source encoder obtains the common cryptographic information and a title ID from a content distribution system. In other embodiments, the source encoder generates a title ID and/or cryptographic data and provides the generated information to a content distribution system.

[0078] Although a specific source encoder in accordance with embodiments of the invention is illustrated in FIG. 1B, any of a variety of computing platforms can be utilized to implement a source encoder that is configured to encode at least one stream of source content as a plurality of alternative streams and to protect each of the alternative streams using common cryptographic information in accordance with embodiments of the invention.

CONTENT DISTRIBUTION SERVERS

[0079] Content distribution servers in accordance with embodiments of the invention can be responsible for storing protected streams of content for streaming to playback devices using adaptive bitrate streaming processes. Content distribution servers can also store common cryptographic information utilized to protect the alternative streams of protected content. In several embodiments, the common cryptographic information is identified utilizing a title ID associated with the common cryptographic information and a set of streams that form part of a specific title or piece of content. A content distribution server in accordance with an embodiment of the invention is illustrated in

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1184
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

FIG. 1C. The content distribution server is implemented using a computing platform including a processor 14a, volatile memory 14b, and non-volatile storage 14c. In the illustrated embodiment, a plurality of container files 14d are stored on the content distribution server. Playback devices can stream content from the content distribution server utilizing adaptive bitrate streaming processes in accordance with embodiments of the invention. To facilitate the creation of new streams with respect to a specific piece of content, the content distribution server also stores title IDs 14e for specific pieces of content and common cryptographic information 14f associated with each title ID. A source encoder can request common cryptographic information to protect a new stream related to a specific piece of content, by providing a request to the content distribution server that identifies the specific piece of content using the title ID assigned to it.

[0080] Although a specific content distribution server is illustrated in FIG. 1C, any of a variety of computational platform including (but not limited to) platforms in which container files and common cryptographic information are stored on separate servers can be utilized in content distribution systems in accordance with embodiments of the invention.

PLAYBACK DEVICES

[0081] Referring back to FIG. 1A, the illustrated playback devices include personal computers 18 and mobile phones 20. In other embodiments, playback devices can include consumer electronics devices such as DVD players, Blu-ray players, televisions, set top boxes, video game consoles, tablets, and other devices that are capable of playing back protected media stored on a content distribution server using adaptive bitrate streaming. A playback device in accordance with an embodiment of the invention is illustrated in FIG. 1D. The playback device is implemented on a processing platform 20 including a processor 20a, volatile memory 20b, and non-volatile memory

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1185
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

(or other non-volatile storage) 20c. The non-volatile memory 20c contains a client application 20d, which includes machine readable instructions that can be utilized to configure the processor to register with a content distribution system to obtain cryptographic data 20e bound to the playback device. The playback device can then use the bound cryptographic data 20e to request adaptive bitrate streaming of protected content. As is discussed further below, the alternative streams of protected content utilized to perform adaptive bitrate streaming are protected using common cryptographic information. Once the client application 20d has obtained the common cryptographic information, which can be a time consuming and/or computationally intensive process, the playback device can use the same cryptographic information to access content in any of the alternative streams of protected content within a single instance of a title.

[0082] Although a specific architecture for a playback device is shown in FIG. 1D any of a variety of architectures can be utilized that enable playback devices to request portions of the top level index file and the container files in accordance with embodiments of the invention.

FILE STRUCTURE

[0083] Files generated by a source encoder and/or stored on an HTTP server for streaming to playback devices in accordance with embodiments of the invention are illustrated in FIG. 2. The files utilized in the adaptive bitrate streaming of the source media include a top level index 30 and a plurality of container files 32 that each contain at least one stream. The top level index file describes the content of each of the container files. As is discussed further below, the top level index file can take a variety of forms including an SMIL file and the container files can take a variety of forms including a specialized Matroska container file.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1186
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

[0084] In many embodiments, each Matroska container file contains a single protected stream. For example, the stream could be one of a number of alternate video streams protected using common cryptographic information, an audio stream, one of a number of alternate audio streams, a subtitle stream, one of a number of alternate subtitle streams, a trick play stream, or one of a number of alternate trick play streams protected using common cryptographic information. In several embodiments, the Matroska container file includes multiple multiplexed streams. For example, the Matroska container could include a video stream, and one or more audio streams, one or more subtitle streams, and/or one or more trick play streams. As is discussed further below, in many embodiments the Matroska container files are specialized files. The encoding of the media and the manner in which the media is stored within Cluster elements within the Matroska container file can be subject to constraints designed to enhance the performance of an adaptive bitrate streaming system. In a number of embodiments, common cryptographic information is included within a DRM header element in each of the Matroska container files and references to the common cryptographic information are made using DRMInfo elements included within BlockGroup elements of protected (not all frames need be protected to protect the stream). In addition, the Matroska container file can include index elements that facilitate the location and downloading of Cluster elements from the various Matroska container files during the adaptive streaming of the media. Top level index files and Matroska container files that can be used in adaptive bitrate streaming systems in accordance with embodiments of the invention are discussed below.

TOP LEVEL INDEX FILES

[0085] Playback devices in accordance with many embodiments of the invention utilize a top level index file to identify the container files that contain the streams available to the playback device for use in adaptive bitrate streaming. In many

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1187
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

embodiments, the top level index files can include references to container files that each include an alternative stream of encoded media. The playback device can utilize the information in the top level index file to retrieve encoded media from each of the container files according to the streaming conditions experienced by the playback device.

[0086] In several embodiments, the top level index file provides information enabling the playback device to retrieve information concerning the encoding of the media in each of the container files and an index to encoded media within each of the container files. In a number of embodiments, each container file includes information concerning the encoded media contained within the container file and an index to the encoded media within the container file and the top level index file indicates the portions of each container file containing this information. Therefore, a playback device can retrieve the top level index file and use the top level index file to request the portions of one or more of the container files that include information concerning the encoded media contained within the container file and an index to the encoded media within the container file. A variety of top level index files that can be utilized in adaptive bitrate streaming systems in accordance with embodiments of the invention are discussed further below.

[0087] In a number of embodiments, the top level index file utilized in the adaptive bitrate streaming of media is a SMIL file, which is an XML file that includes a list of URIs describing each of the streams and the container files that contain the streams. The URI can include information such as the "system-bitrate" of the stream contained within the stream and information concerning the location of specific pieces of data within the container file. The top level index SMIL file can be generated when the source media is encoded for playback via adaptive bitrate streaming. Alternatively, the top level index SMIL file can be generated when a playback device requests the commencement of playback of the encoded media. When the playback device receives the top level index SMIL file, the playback device can parse the SMIL file to identify the

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1188
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

available streams. The playback device can then select the streams to utilize to playback the content and can use the SMIL file to identify the portions of the container file to download to obtain information concerning the encoding of a specific stream and/or to obtain an index to the encoded media within the container file.

[0088] Although top level index SMIL files are described above, any of a variety of top level index file formats can be utilized to create top level index files as appropriate to a specific application in accordance with an embodiment of the invention. The use of top level index files to enable playback of encoded media using adaptive bitrate streaming in accordance with embodiments of the invention is discussed further below.

STORING PROTECTED MEDIA IN MKV FILES FOR ADAPTIVE BITRATE STREAMING

[0089] A Matroska container file used to store encoded video in accordance with an embodiment of the invention is illustrated in FIG. 3. The container file 32 is an Extensible Binary Markup Language (EBML) file that is an extension of the Matroska container file format. The specialized Matroska container file 32 includes a standard EBML element 34, and a standard Segment element 36 that includes a standard Seek Head element 40, a standard Segment Information element 42, and a standard Tracks element 44 including a tracks data payload that is a non-standard EBML element containing cryptographic information utilized to access the protected stream(s) contained within the Matroska container file. In many embodiments, the cryptographic data takes the form of a DRMHeaders element (discussed below) that includes a set of keys utilized to access encrypted portions of the stream contained within the Matroska container file. In many embodiments, the set of keys is encrypted in such a way that a playback device can only access the set of keys in the clear using a specific piece or set of cryptographic information.

[0090] The Segment element 36 also includes a standard Clusters element 46. As is described below, the manner in which encoded media is inserted within individual

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1189
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Cluster elements 48 within the Clusters element 46 is constrained to improve the playback of the media in an adaptive streaming system. In many embodiments, the constraints imposed upon the encoded video are consistent with the specification of the Matroska container file format and involve encoding the video so that each cluster includes at least one closed GOP commencing with an IDR frame. In addition to the above elements, the Segment element 36 can optionally include a modified version of the standard Cues element. As is discussed further below, the Cues element includes specialized CuePoint elements (i.e. non-standard CuePoint elements) that facilitate the retrieval of the media contained within specific Cluster elements via HTTP. The Segment element 36 can optionally include a non-standard Hierarchical Index element 54. The Hierarchical Index element is an extension to the Matroska file format proposed by DivX, LLC of San Diego, California. The Hierarchical Index element is described in U.S. Patent Application Serial No. 12/272,631, the disclosure of which is incorporated by reference above in its entirety.

[0091] The constraints imposed upon the encoding of media and the formatting of the encoded media within the Clusters element of a Matroska container file for adaptive bitrate streaming of protected streams and the additional DRM and index information inserted within the container file in accordance with embodiments of the invention are discussed further below.

ENCODING MEDIA FOR INSERTION IN CLUSTER ELEMENTS

[0092] An adaptive bitrate streaming system provides a playback device with the option of selecting between different protected streams of encoded media during playback according to the streaming conditions experienced by the playback device. In many embodiments, switching between protected streams is facilitated by separately pre-encoding discrete portions of the source media in accordance with the encoding parameters of each stream and then including each separately encoded portion in its

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1190
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

own Cluster element within the stream's container file. Furthermore, the media contained within each Cluster is encoded so that the media is capable of playback without reference to media contained in any other Cluster within the stream. In this way, each stream includes a Cluster element corresponding to the same discrete portion of the source media and, at any time, the playback device can select the Cluster element from the stream that is most appropriate to the streaming conditions experienced by the playback device and can commence playback of the media contained within the Cluster element. Accordingly, the playback device can select clusters from different streams as the streaming conditions experienced by the playback device change over time. In several embodiments, the Cluster elements are further constrained so that each Cluster element contains a portion of encoded media from the source media having the same duration. In a number of embodiments, each Cluster element includes two seconds of encoded media. The specific constraints applied to the media encoded within each Cluster element depending upon the type of media (i.e. video, audio, or subtitles) are discussed below.

[0093] A Clusters element of a Matroska container file containing a video stream in accordance with an embodiment of the invention is illustrated in FIG. 4a. The Clusters element 46 includes a plurality of Cluster elements 48 that each contains a discrete portion of encoded video. In the illustrated embodiment, each Cluster element 48 includes two seconds of encoded video. In other embodiments, the Cluster elements include encoded video having a greater or lesser duration than two seconds. In several embodiments, the encoded video sequences in the Cluster elements have different durations.

[0094] Each Cluster element 48 includes a Timecode element 60 indicating the start time of the encoded video within the Cluster element and a plurality of BlockGroup elements. As noted above, the encoded video stored within the Cluster is constrained so that the encoded video can be played back without reference to the encoded video

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1191
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

contained within any of the other Cluster elements in the container file. In many embodiments, encoding the video contained within the Cluster element as a GOP in which the first frame is an IDR frame enforces the constraint. In the illustrated embodiment, the first BlockGroup element 62 contains an IDR frame. Therefore, the first BlockGroup element 62 does not include a ReferenceBlock element. The first BlockGroup element 62 includes a Block element 64, which specifies the Timecode attribute of the frame encoded within the Block element 64 relative to the Timecode of the Cluster element 48 and a DRMInfo element 65 that identifies a portion of the frame that is encrypted and the cryptographic information that can be utilized to access the encrypted portion of the frame. In a number of embodiments, only a small portion of the video frame is encrypted and the DRMInfo includes a reference to the start of an encrypted block of data and the size of the encrypted block of data. As is discussed further below, the common cryptographic information utilized to protect alternative streams of video content is a set of frame keys in many embodiments of the invention and the DRMInfo element can also include an index to a specific frame key in the set of frame keys that can be utilized to access the encrypted block of data in the clear. In other embodiments, any of a variety of information appropriate to identifying encrypted data within a video frame and decrypting the encrypted data can be stored within a DRMInfo element.

[0095] Subsequent BlockGroup elements 66 are not restricted in the types of frames that they can contain (other than that they cannot reference frames that are not contained within the Cluster element). Therefore, subsequent BlockGroup elements 66 can include ReferenceBlock elements 68 referencing other BlockGroup element(s) utilized in the decoding of the frame contained within the BlockGroup or can contain IDR frames and are similar to the first BlockGroup element 62. In addition, subsequent BlockGroup elements 66 can also include DRMInfo elements to describe the manner in which the frame of video contained within the BlockGroup element is protected. As

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1192
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

noted above, the manner in which encoded video is inserted within the Cluster elements of the Matroska file conforms with the specification of the Matroska file format.

[0096] The insertion of encoded audio and subtitle information within a Clusters element 46 of a Matroska container file in accordance with embodiments of the invention is illustrated in FIGS. 4b and 4c. In the illustrated embodiments, the encoded media is inserted within the Cluster elements 48 subject to the same constraints applied to the encoded video discussed above with respect to FIG. 4a. In addition, the duration of the encoded audio and subtitle information within each Cluster element corresponds to the duration of the encoded video in the corresponding Cluster element of the Matroska container file containing the encoded video. In other embodiments, the Cluster elements within the container files containing the audio and/or subtitle streams need not correspond with the start time and duration of the Cluster elements in the container files containing the alternative video streams. In many embodiments, audio, and/or subtitle tracks are protected and information identifying the protected portions of the stream can be included in an element in a manner similar to that described above with respect to protected video streams.

MULIPLEXING STREAMS IN A SINGLE MKV CONTAINER FILE

[0097] The Clusters elements shown in FIGS. 4a – 4c assume that a single stream is contained within each Matroska container file. In several embodiments, media from multiple streams is multiplexed within a single Matroska container file. In this way, a single container file can contain a video stream multiplexed with one or more corresponding audio streams, and/or one or more corresponding subtitle streams. Storing the streams in this way can result in duplication of the audio and subtitle streams across multiple alternative video streams. However, the seek time to retrieve encoded media from a video stream and an associated audio, and/or subtitle stream can be reduced due to the adjacent storage of the data on the server. The Clusters

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1193
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

element 46 of a Matroska container file containing multiplexed video, audio and subtitle data in accordance with an embodiment of the invention is illustrated in FIG. 4d. In the illustrated embodiment, each Cluster element 48 includes additional BlockGroup elements for each of the multiplexed streams. The first Cluster element includes a first BlockGroup element 62v for encoded video that includes a Block element 64v containing an encoded video frame and indicating the Timecode attribute of the frame relative to the start time of the Cluster element (i.e. the Timecode attribute 60). A second BlockGroup element 62a includes a Block element 64a including an encoded audio sequence and indicating the timecode of the encoded audio relative to the start time of the Cluster element, and a third BlockGroup element 62s including a Block element 64s containing an encoded subtitle and indicating the timecode of the encoded subtitle relative to the start time of the Cluster element. In the illustrated embodiment, only the video stream is protected. Therefore, the BlockGroup elements 62v containing the video stream include DRMInfo elements 65v to identify the portions of the frames within the video stream that are encrypted. In other embodiments, the audio, and/or subtitle streams can also be protected. Although not shown in the illustrated embodiment, each Cluster element 48 likely would include additional BlockGroup elements containing additional encoded video, audio or subtitles. Despite the multiplexing of the encoded video, audio, and/or subtitle streams, the same constraints concerning the encoded media apply.

INCORPORATING TRICK PLAY STREAMS IN MKV CONTAINER FILES FOR USE IN ADAPTIVE BITRATE STREAMING SYSTEMS

[0098] The incorporation of trick play tracks within Matroska container files is proposed by DivX, LLC in U.S. Patent Application No. 12/260,404 entitled "Application Enhancement Tracks", filed October 29, 2008, the disclosure of which is hereby incorporated by reference in its entirety. Trick play tracks similar to the trick play

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1194
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

tracks described in U.S. Patent Application No. 12/260,404 can be used to provide a trick play stream in an adaptive bitrate streaming system in accordance with an embodiment of the invention to provide smooth visual search through source content encoded for adaptive bitrate streaming. A separate trick play stream can be encoded that appears to be an accelerated visual search through the source media when played back, when in reality the trick play stream is simply a separate stream encoding the source media at a lower frame rate. In several embodiments, a trick play stream is generated in the manner outlined in U.S. Patent Application No. 12/260,404 and inserting the trick play stream into a Matroska container file subject to the constraints mentioned above with respect to insertion of a video stream into a Matroksa container file. In many embodiments, the trick play stream is also subject to the further constraint that every frame in the GOP of each Cluster element in the trick play stream is encoded as an IDR frame. As with the other video streams, each Cluster element contains a GOP corresponding to the same two seconds of source media as the corresponding Cluster elements in the other streams. There are simply fewer frames in the GOPs of the trick play stream and each frame has a longer duration. In this way, transitions to and from a trick play stream can be treated in the same way as transitions between any of the other encoded streams are treated within an adaptive bitrate streaming system in accordance with embodiments of the invention. In embodiments where the trick play stream(s) are protected, the same common cryptographic information utilized to encrypt the primary video stream(s) is utilized to protect the trick play stream(s). Playback of the frames contained within the trick play stream to achieve accelerated visual search typically involves the playback device manipulating the timecodes assigned to the frames of encoded video prior to providing the frames to the playback device's decoder to achieve a desired increase in rate of accelerated search (e.g. x2, x4, x6, etc.).

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1195
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

[0099] A Clusters element containing encoded media from a trick play stream is shown in FIG. 4e. In the illustrated embodiment, the encoded trick play stream is inserted within the Cluster elements 48 subject to the same constraints applied to the encoded video discussed above with respect to FIG. 4a including the constraint that frames are protected using the common cryptographic information. However, each BlockGroup element contains an IDR. In other embodiments, the Cluster elements within the container files containing the trick play streams need not correspond with the start time and duration of the Cluster elements in the container files containing the alternative video streams.

[00100] In many embodiments, source content can be encoded to provide a single trick play stream or multiple trick play streams for use by the adaptive bit rate streaming system. When a single trick play stream is provided, the trick play stream is typically encoded at a low bitrate. When multiple alternative trick play streams are provided, adaptive streaming can also be performed with respect to the trick play streams. In several embodiments, multiple trick play streams are provided to support different rates of accelerated visual search through the encoded media.

INCORPORATING INDEXING INFORMATION WITHIN MKV CONTAINER FILES

[00101] The specification for the Matroska container file format provides for an optional Cues element that is used to index Block elements within the container file. A modified Cues element that can be incorporated into a Matroska container file in accordance with an embodiment of the invention to facilitate the requesting of clusters by a playback device using HTTP is illustrated in FIG. 5. The Cues element 52 is similar to a standard Cues element 52 in that it includes a plurality of standard CuePoint elements 70 that each include a standard CueTime attribute 72. Each CuePoint element includes a CueTrackPositions element 74 containing the standard CueTrack 76 and CueClusterPosition 78 attributes. In many embodiments, the CuePoint element is

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1196
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

mainly configured to identify a specific Cluster element as opposed to a specific Block element within a Cluster element. Although, in several applications the ability to seek to specific Block elements within a Cluster element is required and additional index information is included in the Cues element.

[00102] The use of a modified Cues element to index encoded media within a Clusters element of a Matroska file in accordance with an embodiment of the invention is illustrated in FIG. 6. A CuePoint element is generated to correspond to each Cluster element within the Matroska container file. The CueTime attribute 72 of the CuePoint element 70 corresponds to the Timecode attribute 60 of the corresponding Cluster element 48. In addition, the CuePoint element contains a CueTrackPositions element 74 having a CueClusterPosition attribute 78 that points to the start of the corresponding Cluster element 48. The CueTrackPositions element 74 can also include a CueBlockNumber attribute, which is typically used to indicate the Block element containing the first IDR frame within the Cluster element 48.

[00103] As can readily be appreciated the Cues element 52 forms an index to each of the Cluster elements 48 within the Matroska container file. Furthermore, the CueTrackPosition elements provide information that can be used by a playback device to request the byte range of a specific Cluster element 48 via HTTP or another suitable protocol from a remote server. The Cues element of a conventional Matroska file does not directly provide a playback device with information concerning the number of bytes to request from the start of the Cluster element in order to obtain all of the encoded video contained within the Cluster element. The size of a Cluster element is, therefore, inferred by using the CueClusterPosition attribute of the CueTrackPositions element that indexes the first byte of the next Cluster element. Alternatively, additional CueTrackPosition elements could be added that index the last byte of the Cluster element (in addition to the CueTrackPositions elements that index the first byte of the Cluster element), and/or a non-standard CueClusterSize attribute that specifies the size

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1197
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

of the Cluster element pointed to by the CueClusterPosition attribute is included in each CueTrackPosition element to assist with the retrieval of specific Cluster elements within a Matroska container file via HTTP byte range requests or a similar protocol.

[00104] The modification of the Cues element in the manner outlined above significantly simplifies the retrieval of Cluster elements from a Matroska container file via HTTP or a similar protocol during adaptive bitrate streaming. In addition, by only indexing the first frame in each Cluster the size of the index is significantly reduced. Given that the index is typically downloaded prior to playback, the reduced size of the Cues element (i.e. index) means that playback can commence more rapidly. Using the CueClusterPosition elements, a playback device can request a specific Cluster element from the stream most suited to the streaming conditions experienced by the playback device by simply referencing the index of the relevant Matroska container file using the Timecode attribute for the desired Cluster element.

[00105] A number of the attributes within the Cues element are not utilized during adaptive bitrate streaming. Therefore, the Cues element can be further modified by removing the unutilized attributes to reduce the overall size of the index for each Matroska container file. A modified Cues element that can be utilized in a Matroska container file that includes a single encoded stream, where portions of the encoded stream having the same duration are contained in each Cluster element within the Matroska file in accordance with an embodiment of the invention is illustrated in FIG. 5a. The Cues element 52' shown in FIG. 5a is similar to the Cues element 52 shown in FIG. 5 with the exception that the CuePoint elements 70' do not include a CueTime attribute (see 72 in FIG. 5) and/or the CueTrackPositions elements 74' do not include a CueTrack attribute (76 in FIG. 5). When the portions of encoded media in each Cluster element in the Matroska container file have the same duration, the CueTime attribute is not necessary. When the Matroska contain file includes a single encoded stream, the CueTrack attribute is not necessary. In other embodiments, the Cues element and/or

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1198
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

other elements of the Matroska container file can be modified to remove elements and/or attributes that are not necessary for the adaptive bitrate streaming of the encoded stream contained within the Matroska container file, given the manner in which the stream is encoded and inserted in the Matroska container file.

[00106] Although various modifications to the Cues element to include information concerning the size of each of the Cluster elements within a Matroska container file and to eliminate unnecessary attributes are described above, many embodiments of the invention utilize a conventional Matroska container. In several embodiments, the playback device simply determines the size of Cluster elements on the fly using information obtained from a conventional Cues element, and/or relies upon a separate index file containing information concerning the size and/or location of the Cluster elements within the MKV container file. In several embodiments, the additional index information is stored in the top level index file. In a number of embodiments, the additional index information is stored in separate files that are identified in the top level index file. When index information utilized to retrieve Cluster elements from a Matroska container file is stored separately from the container file, the Matroska container file is still typically constrained to encode media for inclusion in the Cluster elements in the manner outlined above. In addition, wherever the index information is located, the index information will typically index each Cluster element and include (but not be limited to) information concerning at least the starting location and, in many instances, the size of each Cluster element.

INCORPORATING HIERARCHICAL INDEXES INTO MKV CONTAINERS

[00107] Retrieval of media using HTTP during adaptive streaming can be improved by adding additional index information to the Matroska container files used to contain each of the encoded streams. In a number of embodiments, the index is a reduced index in that the index only points to the IDRs at the start of each cluster. In many

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1199
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

embodiments, the index of the Matroska container file includes additional non-standard attributes (i.e. attributes that do not form part of the Matroska container file format specification) that specify the size of each of the clusters so that a playback device can retrieve a Cluster element from the Matroska container file via HTTP using a byte range request. In several embodiments, the Matroska container file includes a hierarchical index using a HierarchicalIndex element similar to the hierarchical indexes disclosed in U.S. Patent Application Serial No. 12/272,631 entitled "Hierarchical and Reduced Index Structures for Multimedia Files" to Soroushian et al. filed November 17, 2008 to increase the speed with which a playback device can seek to a specific Cluster element containing encoded media within the container file. The disclosure of U.S. Patent Application Serial No. 12/272,631 is herby incorporated by reference in its entirety.

[00108] A hierarchical index included in a Matroska container file using a HierarchicalIndex element in accordance with an embodiment of the invention is illustrated in FIG. 7. The HierarchicalIndex element 54 includes a plurality of HierarchicalIndexPointer elements 80 that each point to a CuePoint element 70 within the Cues element 52. In this way, the hierarchical index can be utilized to rapidly locate specific Cluster elements within a Matroska file using the Timecode attribute of the Cluster element. Furthermore, the entire index (i.e. the entire Cues element) need not be downloaded in order to locate a specific Cluster element. The playback device can simply download the hierarchical index and download the specific CuePoint elements that enable the location of a desired Cluster element within the Matroska container file.

[00109] In several embodiments, the HierarchicalIndex element is generated so that the HierarchicalIndexPointer elements point to CuePoint elements indexing Cluster elements that are a predetermined time period apart. For example, the HierarchicalIndexPointer elements can point to CuePoint elements indexing Cluster elements that are spaced 30 seconds apart. In other implementations, any of a variety of implementations can be utilized to determine the interval between the CuePoint

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1200
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

elements referenced by the higher layers of the hierarchical index. In addition, although a two layer hierarchical index is illustrated in FIG. 7, hierarchical indexes including three or more layers can also be incorporated within Matroska container files generated for use in adaptive bitrate streaming systems in accordance with embodiments of the invention.

[00110] As noted above, index information can be stored in a separate file to the Matroska container file in accordance with embodiments of the invention. In embodiments where the index information is stored separately, the index can be hierarchical to prevent the need to download the entire index for a container file prior to playback and to facilitate seeking within the index.

ENCODING AND PROTECTING SOURCE MEDIA FOR ADAPTIVE BITRATE STREAMING

[00111] A process for encoding source media as a top level index file and a plurality of Matroska container files for use in an adaptive bitrate streaming system in accordance with an embodiment of the invention is illustrated in FIG. 8. The encoding process 100 commences by writing headers for each of the MKV files that will contain the streams of content generated using the source content. In the illustrated embodiment, the source content includes a stream of video that is encoded as a plurality of protected streams. The frames of the source video are encoded (104) using the encoding parameters associated with each of the alternative streams and portions of the encoded frames can be encrypted using a frame key selected from a set of frame keys. When the encoding and encryption of the streams is complete, an index is inserted (106) into each Matroska container file containing an alternative stream of protected video. The common set of frame keys is also encrypted (108) and the process writes (110) a DRM header including the encrypted set of frame keys to each container file. DRM headers and processes for restricting access to cryptographic information stored within the DRM header of a

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1201
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Matroska container file in accordance with embodiments of the invention are discussed further below.

[00112] A process for encoding and protecting frames of video to create a plurality of alternative streams of protected video in accordance with embodiments of the invention is illustrated in FIG. 9. The process 120 includes selecting (122) a first portion of the source media and encoding (123) the source media using the encoding parameters for each alternative stream. Assuming that the resulting frame is to be encrypted, a frame key can be selected (124) from a common set of frame keys and utilized to encrypt at least a portion of the frame of video. A DRMInfo element can then be written (125) to a BlockGroup element. The DRMInfo element identifies the portion of the frame that is encrypted and the frame key that can be utilized by a playback device to access the encrypted portion of the frame. The encoded and/or encrypted frame can then be written (126) to the BlockGroup element. When the entire source video stream is determined (127) as being encoded and protected, then the process is complete.

[00113] Each portion of source video that is encoded (123) can be encoded as a single GOP commencing with an IDR frame. In many embodiments, encoding parameters used to create the alternative GOPs vary based upon bitrate, frame rate, encoding parameters and resolution. In this way, the portion of media is encoded as a set of interchangeable alternatives and a playback device can select the alternative most appropriate to the streaming conditions experienced by the playback device. When different resolutions are supported, the encoding of the streams is constrained so that each stream has the same display aspect ratio. A constant display aspect ratio can be achieved across different resolution streams by varying the sample aspect ratio with the resolution of the stream. In many instances, reducing resolution can result in higher quality video compared with higher resolution video encoded at the same bit rate.

[00114] Although specific processes involving the encoding and protection of a source video stream as a set of alternative streams are illustrated in FIGS. 8 and 9, any of a

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1202
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

variety of processes can be utilized to protect audio, video, and/or subtitle streams using common cryptographic information in accordance with embodiments of the invention. Following the encoding of the source media to create Matroska container files containing each of the protected streams, which can include trick play streams, the Matroska container files can be uploaded to a content distribution server for adaptive bitrate streaming to playback devices. The adaptive bitrate streaming of protected media encoded in accordance with embodiments of the invention using HTTP requests is discussed further below.

DRM HEADERS

[00115] Common cryptographic information utilized in protecting alternative streams can be inserted into container files containing each of the alternative streams. When the container files are Matroska container files, the common cryptographic information can be inserted into the container file as a DRMHeader element. A DRMHeader element configured to contain a set of keys in accordance with an embodiment of the invention is illustrated in FIG. 10. The DRM Header element 130 includes a plurality of pieces of information 132 including a frame keys record 134 that can be utilized to contain a set of frame keys or frame key table common to each of a plurality of alternative streams.

[00116] If the frame key record 134 is communicated in the clear, then any playback device can access the protected streams. Therefore, the frame keys record 134 is typically encrypted using one or more encryption keys. The encryption key(s) used to encrypt the frame key record 134 can be securely provided to an individual playback device using any of a variety of techniques appropriate to a specific application. In the context of streaming systems that also support the downloading of content.

[00117] Although a specific format for storing common cryptographic information in a Matroska container file is illustrated in FIG. 10, any format can be utilized to store

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1203
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

common cryptographic information in a Matroska container file and/or any other container file appropriate to a specific application in accordance with an embodiment of the invention. Adaptive bitrate streaming of protected content in accordance with embodiments of the invention is discussed further below.

ADAPTIVE BITRATE STREAMING FROM MKV CONTAINER FILES USING HTTP

[00118] When source media is encoded so that there are alternative streams of protected media contained in separate Matroska container files for at least one of video, audio, and subtitle content, adaptive streaming of the media contained within the Matroska container files can be achieved using HTTP requests or a similar stateless data transfer protocol. In many embodiments, a playback device requests a top level index file from a content distribution server and uses the index information to identify the streams that are available to the playback device and the cryptographic information required to access any protected streams. The playback device can then retrieve the indexes for one or more of the Matroska files and can use the indexes to request media from one or more of the protected streams contained within the Matroska container files using HTTP requests or using a similar stateless protocol. As noted above, many embodiment of the invention implement the indexes for each of the Matroska container files using a modified Cues element. In several embodiments, the index is a hierarchical index and is also includes a HierarchicalIndex element contained within the Matroska container file. In a number of embodiments, however, the encoded media for each stream is contained within a standard Matroska container file and separate index file(s) can also be provided for each of the container files.

[00119] Based upon the streaming conditions experienced by the playback device, the playback device can select media from alternative protected streams encoded at different bitrates. When the media from each of the streams is protected using common cryptographic information and inserted into the Matroska container files in the

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1204
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

manner outlined above, transitions between streams can occur upon the completion of playback of media within a Cluster element without the need to retrieve additional cryptographic information. As noted above, the size of the Cluster elements (i.e the duration of the encoded media within the Cluster elements) is typically chosen so that the playback device is able to respond quickly enough to changing streaming conditions and to instructions from the user that involve utilization of a trick play track. The smaller the Cluster elements (i.e. the smaller the duration of the encoded media within each Cluster element) the higher the overhead associated with requesting each Cluster element. Therefore, a tradeoff exists between the responsiveness of the playback device to changes in streaming conditions and the effective data rate of the adaptive streaming system for a given set of streaming conditions (i.e. the portion of the available bandwidth actually utilized to transmit encoded media). In many embodiments, the size of the Cluster elements is chosen so that each Cluster element contains two seconds of encoded media. In other embodiments, the duration of the encoded media can be greater or less than two seconds and/or the duration of the encoded media can vary from Cluster element to Cluster element.

[00120] Communication between a playback device or client and an HTTP server during the playback of media encoded in separate streams contained within Matroska container files indexed by a top level index file in accordance with an embodiment of the invention is illustrated in FIG. 11. In the illustrated embodiment, the playback device 200 commences playback by requesting the top level index file from the server 202 using an HTTP request or a similar protocol for retrieving data. The server 202 provides the bytes corresponding to the request. The playback device 200 then parses the top level index file to identify the URIs of each of the Matroska container files containing the streams of encoded media derived from a specific piece of source media. The playback device can then request the byte ranges corresponding to headers of one or more of the Matroska container files via HTTP or a similar protocol, where the byte ranges are

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1205
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

determined using the information contained in the URI for the relevant Matroska container files (see discussion above). The server returns the following information in response to a request for the byte range containing the headers of a Matroska container file:

```
ELEM("EBML")
  ELEM("SEEKHEAD")
  ELEM("SEGMENTINFO")
  ELEM("TRACKS")
```

[00121] The EBML element is typically processed by the playback device to ensure that the file version is supported. The SeekHead element is parsed to find the location of the Matroska index elements and the SegmentInfo element contains two key elements utilized in playback: TimecodeScale and Duration. The TimecodeScale specifies the timecode scale for all timecodes within the Segment of the Matroska container file and the Duration specifies the duration of the Segment based upon the TimecodeScale. The Tracks element contains the information used by the playback device to decode the encoded media contained within the Clusters element of the Matroska file including the common cryptographic information, which can take a variety of forms including but not limited to a DRMHeader element. As noted above, adaptive bitrate streaming systems in accordance with embodiments of the invention can support different streams encoded using different encoding parameters including but not limited to frame rate, and resolution. Therefore, the playback device can use the information contained within the Matroska container file's headers to configure the decoder every time a transition is made between encoded streams. Due to the fact that alternative protected streams utilize the same cryptographic information, the engine utilized to decrypt the content on the client 200 (i.e. the software process used to

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1206
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

decrypt encrypted portions of frames of video) does not require reconfiguration using different cryptographic information with each stream switch.

[00122] In many embodiments, the playback device does not retrieve the headers for all of the Matroska container files indexed in the top level index file. Instead, the playback device determines the stream(s) that will be utilized to initially commence playback and requests the headers from the corresponding Matroska container files. Depending upon the structure of the URIs contained within the top level index file, the playback device can either use information from the URIs or information from the headers of the Matroska container files to request byte ranges from the server that contain at least a portion of the index from relevant Matroska container files. The byte ranges can correspond to the entire index or can correspond to the top level of a hierarchical index and a portion of a lower level index (i.e. a HierarchicalIndex element and one or more CuePoint elements). The server provides the relevant byte ranges containing the index information to the playback device, and the playback device can use the index information to request the byte ranges of Cluster elements containing encoded media using this information. When the Cluster elements are received, the playback device can extract encoded media from the BlockGroup elements within the Cluster element, and can decode and playback the media within the BlockGroup elements in accordance with their associated Timecode attributes. Prior to decoding the encoded media, the playback device can check for the presence of a DRMInfo element within each BlockGroup of a video stream to identify whether the encoded media is protected. The playback device can use the information within the DRMInfo element to decrypt encrypted portions of the video prior to decoding.

[00123] In the illustrated embodiment, the playback device 200 requests sufficient index information from the HTTP server prior to the commencement of playback that the playback device can stream the entirety of each of the selected streams using the index information. In other embodiments, the playback device continuously retrieves

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1207
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

index information as media is played back. In several embodiments, all of the index information for the lowest bitrate steam is requested prior to playback so that the index information for the lowest bitrate stream is available to the playback device in the event that streaming conditions deteriorate rapidly during playback.

SWITCHING BETWEEN STREAMS

[00124] The communications illustrated in FIG. 11 assume that the playback device continues to request media from the same streams (i.e. Matroska container files) throughout playback of the media. In reality, the streaming conditions experienced by the playback device are likely to change during the playback of the streaming media and the playback device can request media from alternative streams (i.e. different Matroska container files) to provide the best picture quality for the streaming conditions experienced by the playback device. In addition, the playback device may switch streams in order to perform a trick play function that utilizes a trick play track stream.

[00125] Communication between a playback device and a server when a playback device switches to a new stream in accordance with embodiments of the invention are illustrated in FIG. 12a. The communications illustrated in FIG. 12a assume that the index information for the new stream has not been previously requested by the playback device and that downloading of Cluster elements from the old stream proceeds while information is obtained concerning the Matroska container file containing the new stream. When the playback device 200 detects a change in streaming conditions, determines that a higher bitrate stream can be utilized at the present streaming conditions, or receives a trick play instruction from a user, the playback device can use the top level index file to identify the URI for a more appropriate alternative stream to at least one of the video, audio, or subtitle streams from which the playback device is currently requesting encoded media. The playback device can save the information concerning the current stream(s) and can request the byte ranges of the headers for the

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1208
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Matroska container file(s) containing the new stream(s) using the parameters of the corresponding URIs. Caching the information in this way can be beneficial when the playback device attempts to adapt the bitrate of the stream downward. When the playback device experiences a reduction in available bandwidth, the playback device ideally will quickly switch to a lower bitrate stream. Due to the reduced bandwidth experienced by the playback device, the playback device is unlikely to have additional bandwidth to request header and index information. Ideally, the playback device utilizes all available bandwidth to download already requested higher rate Cluster elements and uses locally cached index information to start requesting Cluster elements from Matroska container file(s) containing lower bitrate stream(s). When a hierarchical index is used, the playback device typically will download additional index information. However, the amount of index information that is downloaded is significantly reduced as the headers of the Matroska container file are already cached on the playback device and the playback device only needs a portion of the index in order commence requesting Cluster elements from the Matroska container file(s) containing the new stream(s).

[00126] Byte ranges for index information for the Matroska container file(s) containing the new stream(s) can be requested from the HTTP server 202 in a manner similar to that outlined above with respect to FIG. 11. At which point, the playback device can stop downloading of cluster elements from the previous streams and can commence requesting the byte ranges of the appropriate Cluster elements from the Matroska container file(s) containing the new stream(s) from the HTTP server, using the index information from the Matroska container file(s) to identify the Cluster element(s) containing the encoded media following the encoded media in the last Cluster element retrieved by the playback device. As noted above, the encoding of the alternative streams so that corresponding Cluster elements within alternative streams (i.e. Cluster elements containing the same portion of the source media encoded in accordance with

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1209
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

different encoding parameters) start with the same Timecode element and an IDR frame facilitates the smooth transition from one stream to another. In addition, the use of common cryptographic information further facilitates smooth switching between alternative streams.

[00127] When the Matroska file includes a hierarchical index, the process for switching between streams can involve downloading less than the entire index of the new streams. The index information can be downloaded by requesting the byte range for the hierarchical index and then using the Timecode attribute of media played back by the playback device 200 to identify the location of CuePoint elements within the Matroska container file(s) containing the new stream(s) that reference Cluster elements containing sequential encoded media and requesting the byte ranges of the CuePoint elements from the HTTP server 202. After the HTTP server has provided the byte ranges including the CuePoint elements, the playback device can use the information within the CuePoint elements to request byte ranges containing desired Cluster elements from the HTTP server. At which point, playback of the encoded media contained within the Cluster elements proceeds in the manner discussed above.

[00128] When the playback device caches the header and the entire index for each stream that has be utilized in the playback of the media, the process of switching back to a previously used stream can be simplified. The playback device already has the header and index information for the Matroska file containing the previously utilized stream and the playback device can simply use this information to start requesting Cluster elements from the Matroska container file of the previously utilized stream via HTTP. Communication between a playback device and an HTTP server when switching back to a stream(s) for which the playback device has cached header and index information in accordance with an embodiment of the invention is illustrated in FIG. 12b. The process illustrated in FIG. 12b is ideally performed when adapting bitrate downwards, because a reduction in available resources can be exacerbated by a need to

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1210
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

download index information in addition to media. The likelihood of interruption to playback is reduced by increasing the speed with which the playback device can switch between streams and reducing the amount of overhead data downloaded to achieve the switch. When a hierarchical index is utilized, the playback device requests the appropriate portion of the index from the Matroska container file(s) containing the lower bitrate stream(s) prior to requesting Cluster elements from the Matroska container file.

[00129] Although the present invention has been described in certain specific aspects, many additional modifications and variations would be apparent to those skilled in the art. It is therefore to be understood that the present invention may be practiced otherwise than specifically described, including various changes in the implementation such as utilizing encoders and decoders that support features beyond those specified within a particular standard with which they comply, without departing from the scope and spirit of the present invention. Thus, embodiments of the present invention should be considered in all respects as illustrative and not restrictive.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1211
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

WHAT IS CLAIMED:

1. A playback device, comprising:

a processor;

memory containing a client application;

wherein the client application configures the processor to:

request a top level index file identifying a plurality of alternative streams of protected content, where each of the alternative streams of protected content are encrypted using common cryptographic information;

obtain the common cryptographic information;

request portions of content from at least the plurality of alternative streams of protected content;

access the protected content using the common cryptographic information; and

playback the content.

2. The playback device of claim 1, wherein:

the alternative streams of protected content are alternative streams of protected video;

each of the alternative streams of protected video includes DRM information indicating portions of frames of video that are encrypted and identifying at least a portion of the common cryptographic information used to access the encrypted portions of the frames of video; and

the client application configures the processor to:

obtain a protected frame of video from one of the alternative streams of protected video;

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1212
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

obtain DRM information indicating a portion of the protected frame of video that is encrypted;

identify at least a portion of the common cryptographic information that is used to access the encrypted portion of the protected frame using the DRM information;

decrypt the encrypted portion of the protected frame of video using the identified portion of the common cryptographic information; and

decode the frame of video.

3. The playback device of claim 1, wherein:

each of the alternative streams of protected content is contained within a separate container file; and

the top level index file identifies a container file containing each of the alternative streams.

4. The playback device of claim 3, wherein:

the container files containing each of the alternative streams of protected content comprise at least one header including the common cryptographic information and information that describes the encoding of the stream of protected content; and

the top level index file identifies the location of the at least one header within each container file.

5. The playback device of claim 4, wherein the common cryptographic information is a set of encryption keys.

6. The playback device of claim 5, wherein:

the common set of encryption keys is encrypted; and

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1213
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

the client application configures the processor to securely receive cryptographic information used to unencrypt the common set of encryption keys.

7. The playback device of claim 4, wherein the client application configures the processor to obtain the common cryptographic information by requesting at least one header of a container file identified in the top level index file.

8. The playback device of claim 7, wherein:

each container file containing one of the alternative streams of protected content further comprises an index; and

the client application configures the processor to request a portion of content from one of the container files by configuring the processor to:

request at least a portion of an index from the container file;

identify the portion of the container file containing a specific portion of content using the index; and

request the identified portion of the container file.

9. The playback device of claim 4, wherein the container files are Matroska container files.

10. The playback device of claim 9, wherein the common cryptographic information is stored in a common DRM Header element contained within a Tracks element within each of the Matroska container files containing the alternative streams of protected content.

11. The playback device of claim 10, wherein:

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1214
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

the common cryptographic information is a set of encryption keys; and

the set of encryption keys is encrypted and stored within the DRM Header element.

12. The playback device of claim 11, wherein the client application configures the processor to:

obtain cryptographic information that can be used to unencrypt the set of encryption keys stored within the DRM Header element; and

unencrypt the set of encryption keys stored within the DRM Header element using the obtained cryptographic information.

13. The playback device of claim 10, wherein the client application configures the processor to obtain the DRM Header element by requesting a Tracks element from one of the Matroska container files identified in the top level index file.

14. The playback device of claim 13, wherein:

each Mastroska container file containing an alternative stream of protected content further comprises an index contained within a Cues element; and

the client application configures the processor to request a portion of content from one of the Matroska container files by configuring the processor to:

request at least a portion of a Cues element from a Matroska container file containing one of the alternative streams of protected content;

identify a portion of the Matroska container file containing a specific portion of content using at least one CueTrackPosition element within the Cues element; and

request the portion of the Matroska container file identified by the at least one CueTrackPosition element.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1215
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

15. The playback device of claim 14, wherein the index comprises a plurality of CueTrackPosition elements that identify the location of a plurality of Cluster elements within the Matroska container file.

16. The playback device of claim 15, wherein:

each Cluster element contains a plurality of BlockGroup elements including encoded portions of content;

a CueTrack Position element indexes each Cluster element; and

each CueTrackPosition element includes the size of the Cluster element that it indexes.

17. The playback device of claim 14, wherein

the alternative streams of protected content are alternative streams of protected video;

each of the Matroska container files containing an alternative stream of protected video includes a DRMInfo element in a BlockGroup element containing a protected frame of video, where the DRMInfo element indicates at least a portion of the protected frames of video that is encrypted and identifies at least a portion of the common cryptographic information used to access the at least one encrypted portion of the protected frame of video; and

the client application configures the processor to access video frames in a stream of protected video using the common cryptographic information by configuring the processor to:

obtain a BlockGroup containing a protected frame of video;

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1216
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

parse the BlockGroup element to obtain a DRMInfo element indicating at least a portion of the protected frame of video that is encrypted using an encryption key from the set of encryption keys;

decrypt the at least one encrypted portion of the protected frame of video using the identified encryption key; and

decode the frame of video.

18. A method of performing adaptive bitrate streaming using a plurality of alternative streams of protected content, where each of the streams of protected content is protected using common cryptographic information, the method comprising:

requesting a top level index file identifying a plurality of alternative streams of protected content using a playback device, where each of the alternative streams of protected content are encrypted using common cryptographic information;

obtaining the common cryptographic information using the playback device;

requesting portions of content from at least the plurality of alternative streams of protected content using the playback device;

accessing the protected content using the playback device and the common cryptographic information; and

playing back the content using the playback device.

19. The method of claim 18, wherein:

the alternative streams of protected content are alternative streams of protected video;

each of the alternative streams of protected video includes DRM information indicating portions of frames of video that are encrypted and identifying at

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1217
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

least a portion of the common cryptographic information used to access the encrypted portions of the frames of video; and

the method further comprises:

obtaining a protected frame of video from one of the alternative streams of protected video using the playback device;

obtaining DRM information indicating a portion of the protected frame of video that is encrypted using the playback device;

identify at least a portion of the common cryptographic information that is used to access the encrypted portion of the protected frame using the playback device and the DRM information;

decrypting the encrypted portion of the protected frame of video using the playback device and the identified portion of the common cryptographic information; and

decoding the frame of video using the playback device.

20. The method of claim 18, wherein:

each of the alternative streams of protected content is contained within a separate container file; and

the top level index file identifies a container file containing each of the alternative streams.

21. The method of claim 20, wherein:

the container files containing each of the alternative streams of protected content comprise at least one header including the common cryptographic information and information that describes the encoding of the stream of protected content; and

the top level index file identifies the location of the at least one header within each container file.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1218
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

22. The method of claim 21, wherein the common cryptographic information is a set of encryption keys.

23. The method of claim 22, wherein:

the set of encryption keys is encrypted so that it is accessible using cryptographic information obtained by the playback device; and

the method further comprising obtaining cryptographic information using the playback device.

24. The method of claim 23, wherein

the set of encryption keys is encrypted using at least one encryption key; and

the playback device securely obtains the at least one encryption key.

25. The method of claim 24, wherein the at least one encryption key is encrypted using at least one encryption key included in the cryptographic information bound to the playback device.

26. The method of claim 23, further comprising obtaining the common cryptographic information by requesting at least one header of a container file identified in the top level index file using the playback device.

27. The method of claim 26, wherein:

each container file containing one of the alternative streams of protected content further comprises an index; and

the method further comprising:

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1219
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

requesting at least a portion of an index from the container file using the playback device;

identify the portion of the container file containing a specific portion of content using the playback device and the index; and

requesting the identified portion of the container file using the playback device.

28. The method of claim 21, wherein the container files are Matroska container files.

29. The method of claim 28, wherein the common cryptographic information is stored in a common DRM Header element contained within a Tracks element within each of the Matroska container files containing the alternative streams of protected content.

30. The method of claim 29, wherein:

the common cryptographic information is a set of encryption keys; and

the set of encryption keys is encrypted and stored within the DRM Header element.

31. The method of claim 30, wherein:

the set of encryption keys is encrypted so that it is accessible using cryptographic information obtained by the playback device; and

the method further comprising obtaining cryptographic information using the playback device.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1220
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

32. The method of claim 30, further comprising obtaining the DRM Header element by requesting a Tracks element from one of the Matroska container files identified in the top level index file.

33. The method of claim 32, wherein:

each Mastroska container file containing an alternative stream of protected content further comprises an index contained within a Cues element; and

the method further comprises:

requesting at least a portion of a Cues element from a Matroska container file containing one of the alternative streams of protected content using the playback device;

identifying a portion of the Matroska container file containing a specific portion of content using the playback device and at least one CueTrackPosition element within the Cues element; and

requesting the portion of the Matroska container file identified by the at least one CueTrackPosition element.

34. The method of claim 33, wherein the index comprises a plurality of CueTrackPosition elements that identify the location of a plurality of Cluster elements within the Matroska container file.

35. The method of claim 34, wherein:

each Cluster element contains a plurality of BlockGroup elements including encoded portions of content;

a CueTrack Position element indexes each Cluster element; and

each CueTrackPosition element includes the size of the Cluster element that it indexes.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1221
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

36. The method of claim 33, wherein

the alternative streams of protected content are alternative streams of protected video;

each of the Matroska container files containing an alternative stream of protected video includes a DRMInfo element in a BlockGroup element containing a protected frame of video, where the DRMInfo element indicates at least a portion of the protected frames of video that is encrypted and identifies at least a portion of the common cryptographic information used to access the at least one encrypted portion of the protected frame of video; and

the method further comprising:

obtaining a BlockGroup containing a protected frame of video using the playback device;

parsing the BlockGroup element to obtain a DRMInfo element indicating at least a portion of the protected frame of video that is encrypted using the playback device and an encryption key from the set of encryption keys;

decrypting the at least one encrypted portion of the protected frame of video using the playback device and the identified encryption key; and

decoding the frame of video using the playback device.

37. A machine readable medium containing processor instructions, where execution of the instructions by a processor causes the processor to perform a process comprising:

request a top level index file identifying a plurality of alternative streams of protected content, where each of the alternative streams of protected content are encrypted using common cryptographic information;

obtaining the common cryptographic information;

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1222
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

requesting portions of content from at least the plurality of alternative streams of protected content;

accessing the protected content using the common cryptographic information; and

playing back the content.

38. The machine readable medium of claim 37, wherein:

the alternative streams of protected content are alternative streams of protected video;

each of the alternative streams of protected video includes DRM information indicating portions of frames of video that are encrypted and identifying at least a portion of the common cryptographic information used to access the encrypted portions of the frames of video; and

execution of the instructions by a processor also causes the processor to perform a process comprising:

obtaining a protected frame of video from one of the alternative streams of protected video;

obtaining DRM information indicating a portion of the protected frame of video that is encrypted;

identify at least a portion of the common cryptographic information that is used to access the encrypted portion of the protected frame using the DRM information;

decrypting the encrypted portion of the protected frame of video using and the identified portion of the common cryptographic information; and

decoding the frame of video.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1223
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

39. The machine readable medium of claim 37, wherein the machine readable medium is non-volatile memory.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1224
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

D1:02359A

Systems and Methods For Playing Back Alternative Streams of Protected Content Protected Using Common Cryptographic Information

Abstract

Systems and methods for performing adaptive bitrate streaming using alternative streams of protected content in accordance with embodiments of the invention are described. One embodiment of the invention includes a processor, and memory containing a client application. In addition, the client application configures the processor to: request a top level index file identifying a plurality of alternative streams of protected content, where each of the alternative streams of protected content are encrypted using common cryptographic information; obtain the common cryptographic information; request portions of content from at least the plurality of alternative streams of protected content; access the protected content using the common cryptographic information; and playback the content.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 1225
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

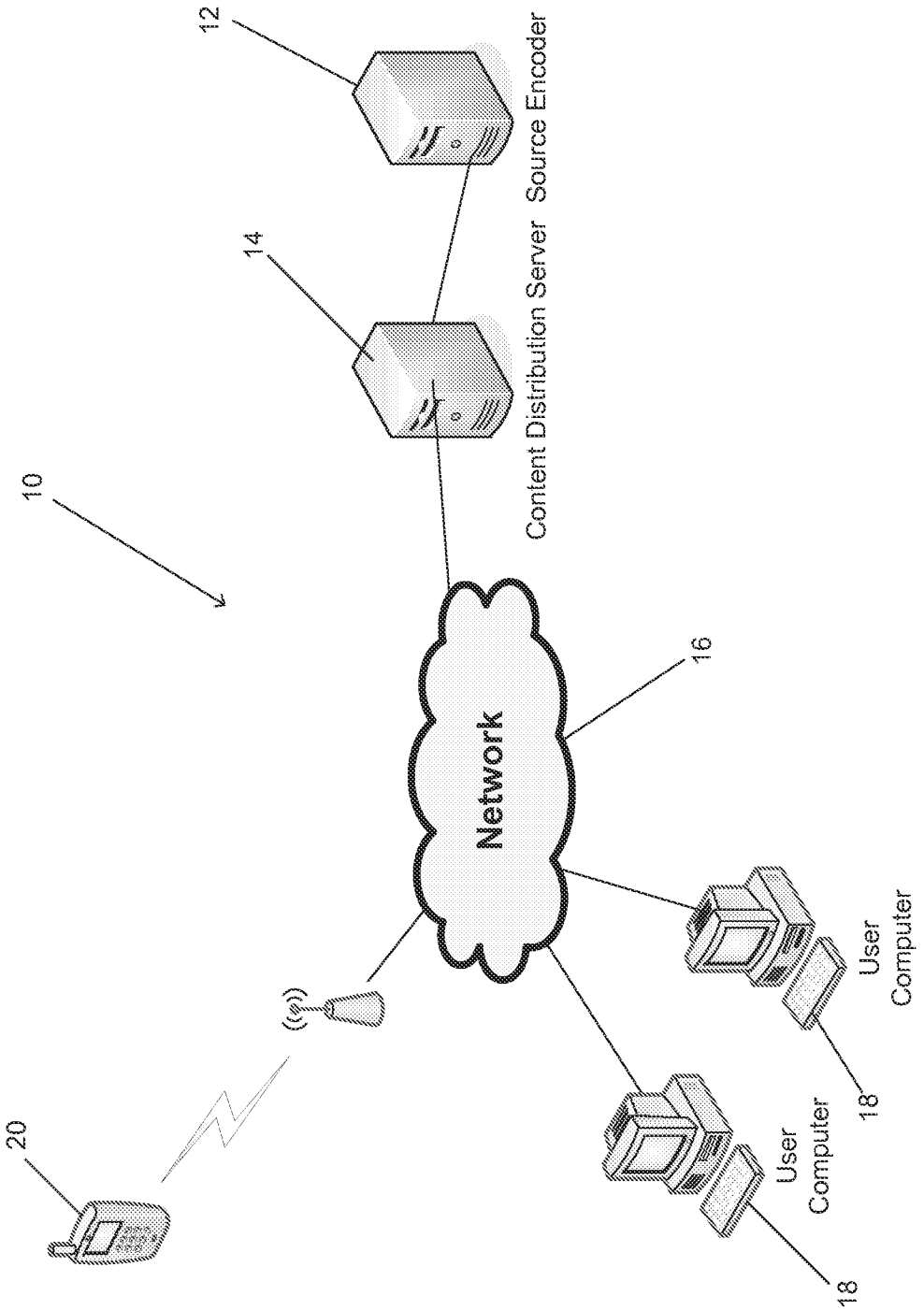

12
Content Distribution Server Source Encoder
14
10
Network
16
User Computer
18
User Computer
18
20

FIG. 1A

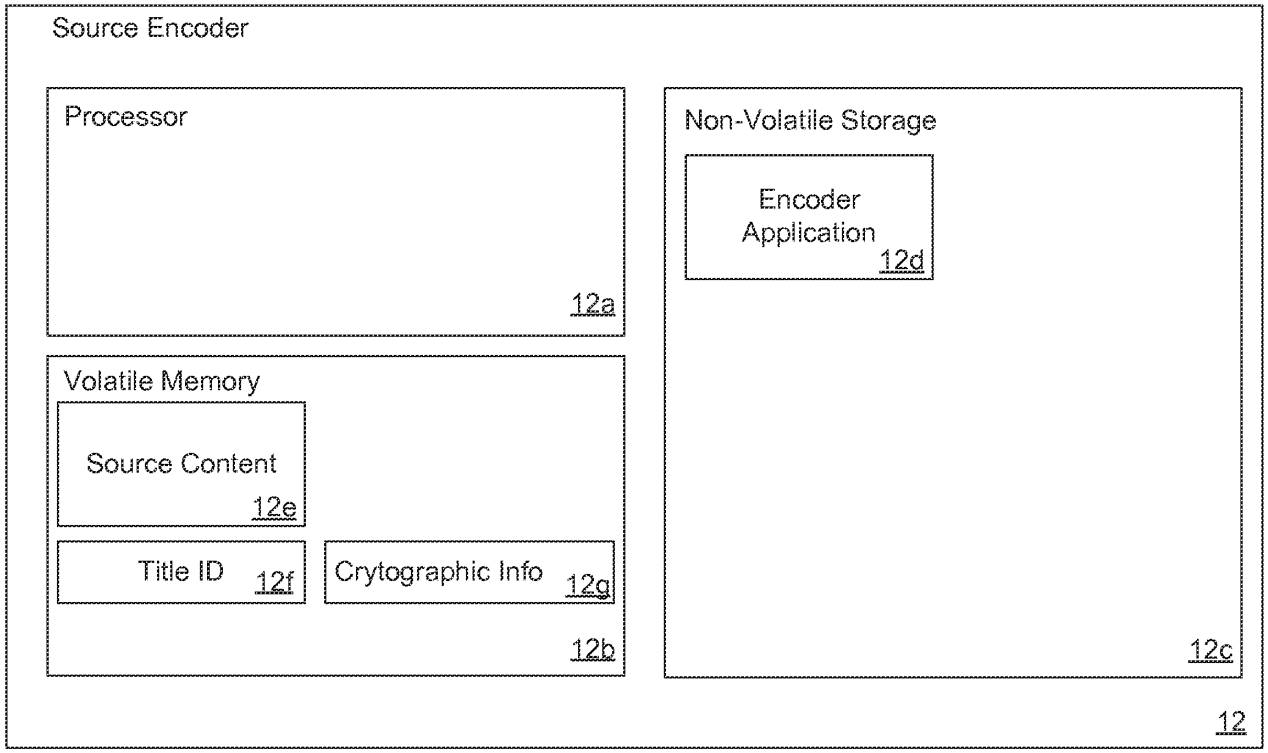

Source Encoder
Processor
12a
Volatile Memory
Source Content
12e
Title ID
12f
Crytographic Info
12g
12b
Non-Volatile Storage
Encoder Application
12d
12c
12

FIG. 1B

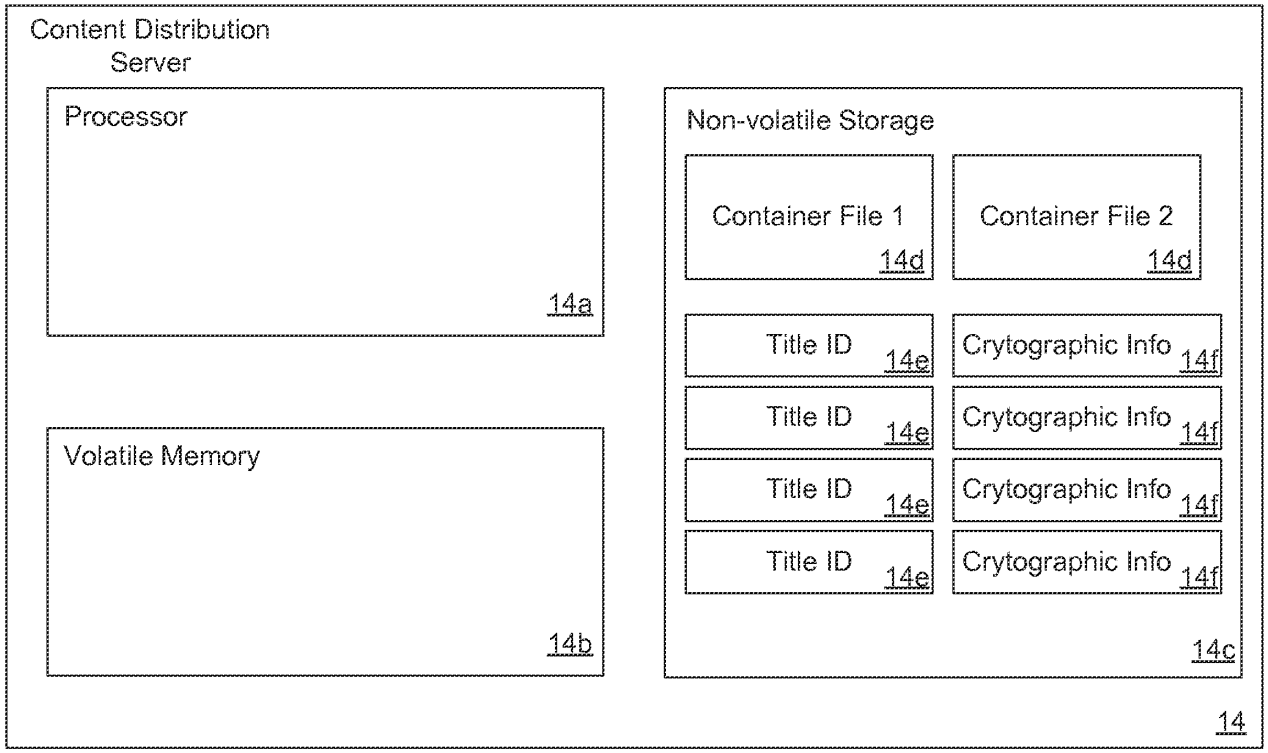

Content Distribution
Server
Processor
14a
Volatile Memory
14b
Non-volatile Storage
Container File 1
14d
Container File 2
14d
Title ID
14e
Crytographic Info
14f
Title ID
14e
Crytographic Info
14f
Title ID
14e
Crytographic Info
14f
Title ID
14e
Crytographic Info
14f
14c
14

FIG. 1C

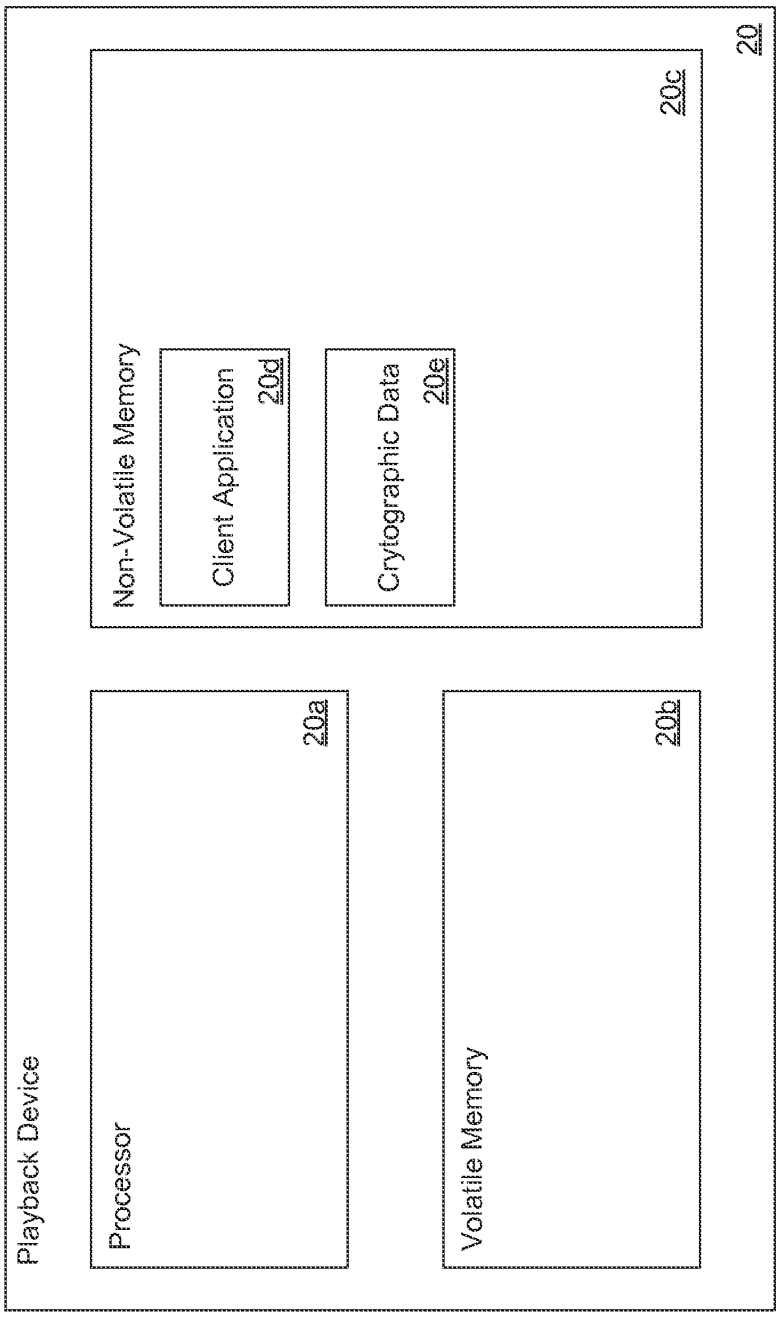

Playback Device
20
Processor
20a
Volatile Memory
20b
Non-Volatile Memory
20c
Client Application
20d
Crytographic Data
20e

FIG. 1D

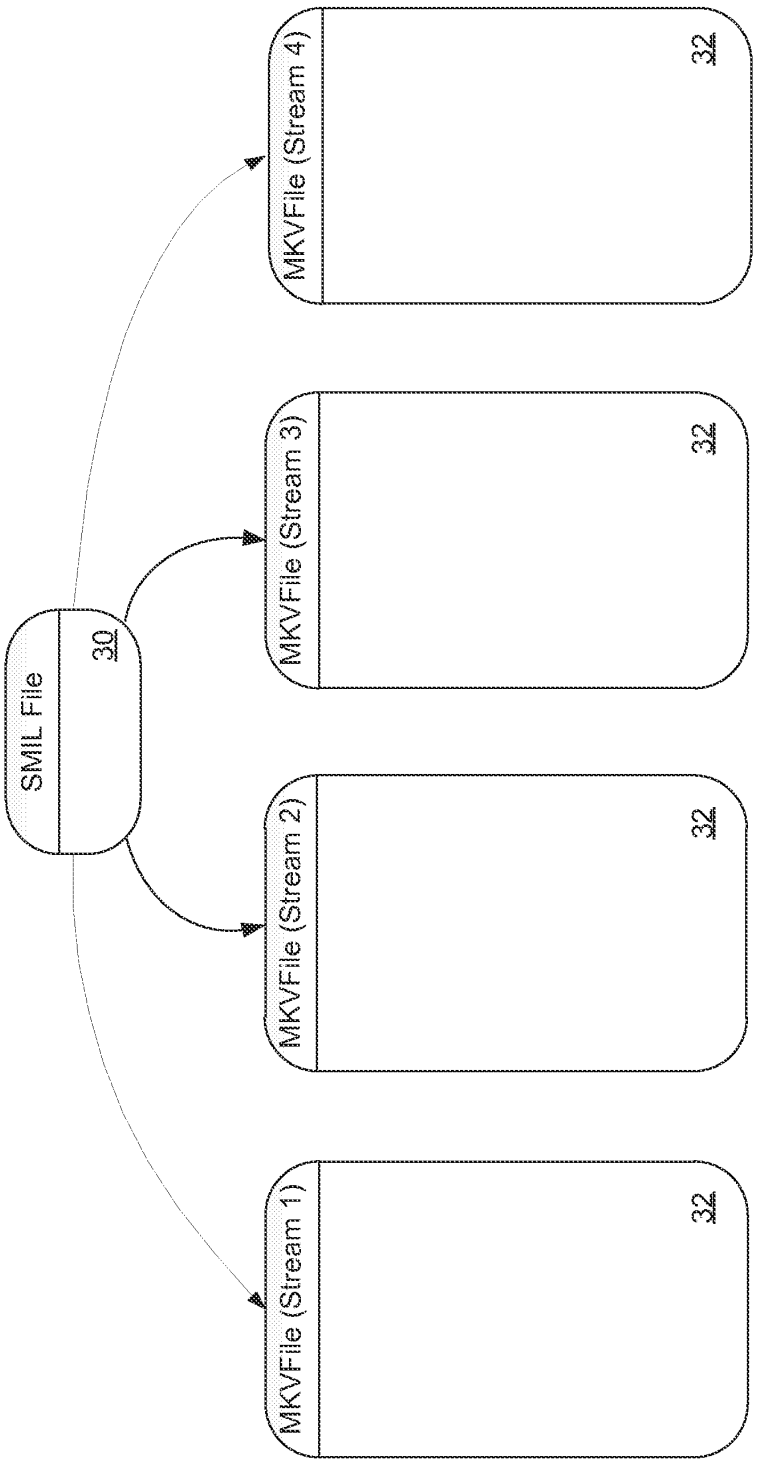

SMIL File
30
MKVFile (Stream 1)
32
MKVFile (Stream 2)
32
MKVFile (Stream 3)
32
MKVFile (Stream 4)
32

FIG. 2

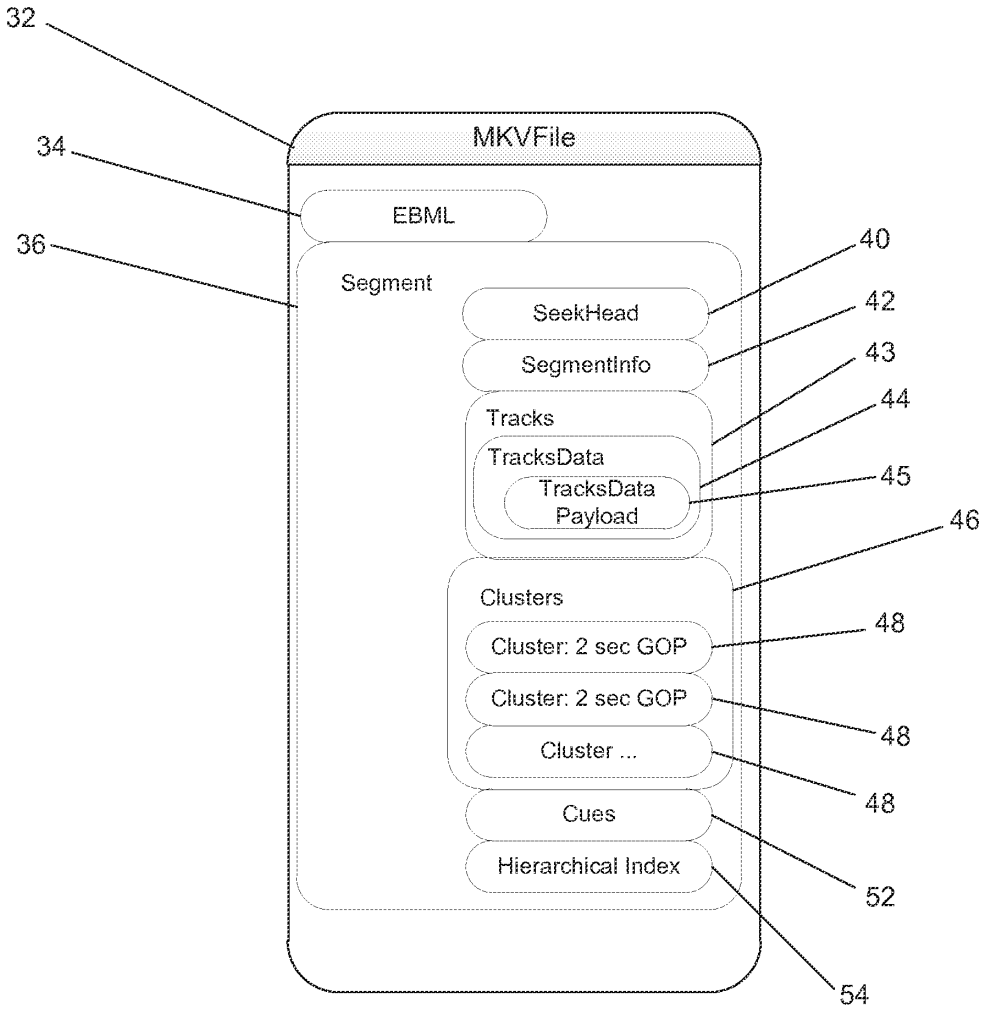

32
MKVFile
34
EBML
36
Segment
40
SeekHead
42
SegmentInfo
43
Tracks
44
TracksData
45
TracksData Payload
46
Clusters
48
Cluster: 2 sec GOP
Cluster: 2 sec GOP
48
Cluster ...
48
Cues
52
Hierarchical Index
54

FIG. 3

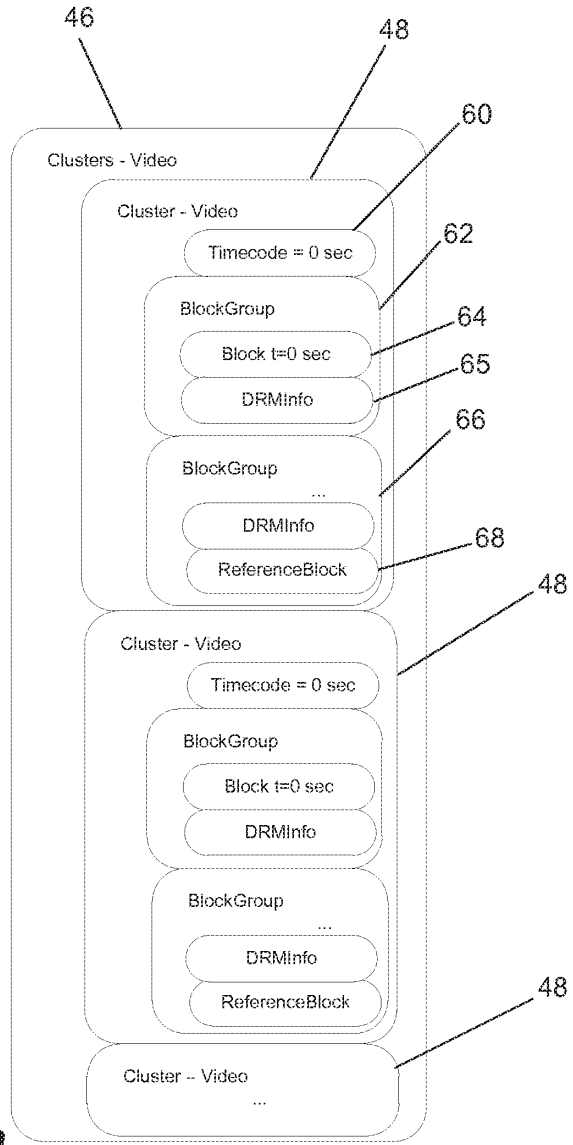

46
48
60
Clusters - Video
Cluster - Video
Timecode = 0 sec
62
BlockGroup
64
Block t=0 sec
65
DRMInfo
66
BlockGroup
...
DRMInfo
68
ReferenceBlock
48
Cluster - Video
Timecode = 0 sec
BlockGroup
Block t=0 sec
DRMInfo
BlockGroup
...
DRMInfo
ReferenceBlock
48
Cluster – Video
...

FIG. 4a

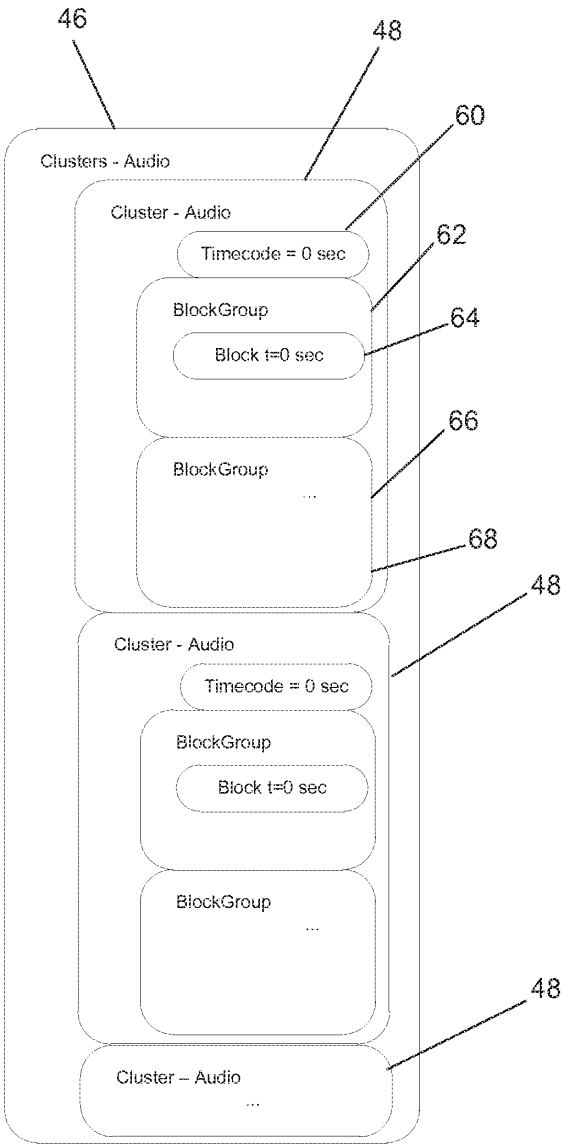

46
48
60
Clusters - Audio
Cluster - Audio
Timecode = 0 sec
62
BlockGroup
64
Block t=0 sec
66
BlockGroup
...
68
48
Cluster - Audio
Timecode = 0 sec
BlockGroup
Block t=0 sec
BlockGroup
...
48
Cluster – Audio
...

FIG. 4b

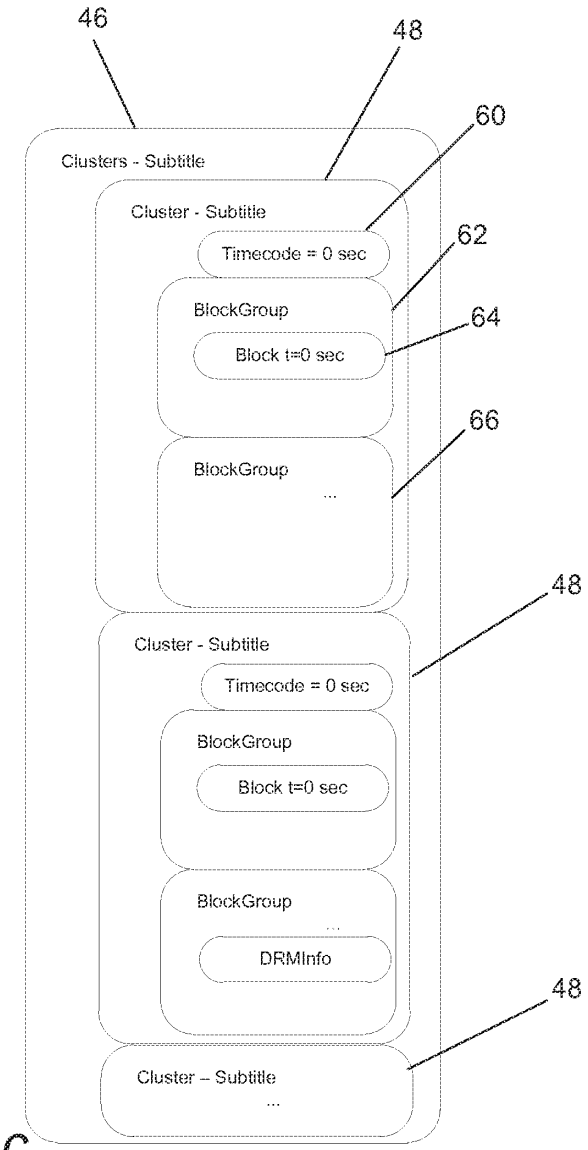


FIG. 4c

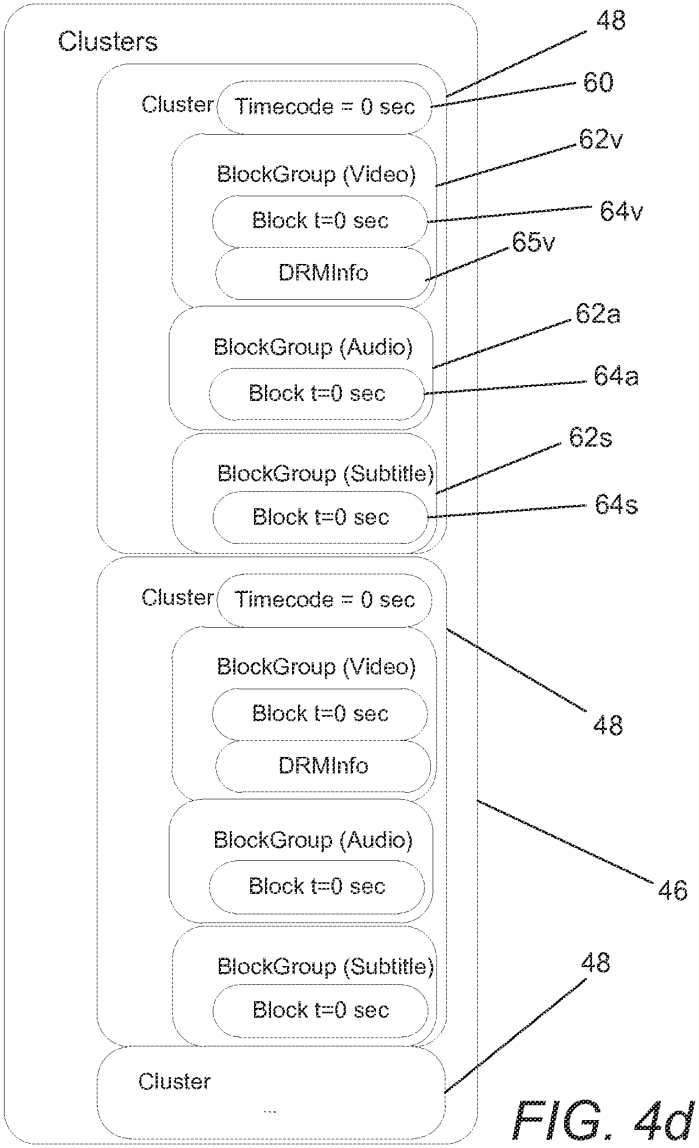


FIG. 4d

Atty Docket: D1:02359A
Title: Systems and Methods for Playing Back Alternative Streams of Protected Content Protected Using Common Cryptographic Information
Sheet 8/19

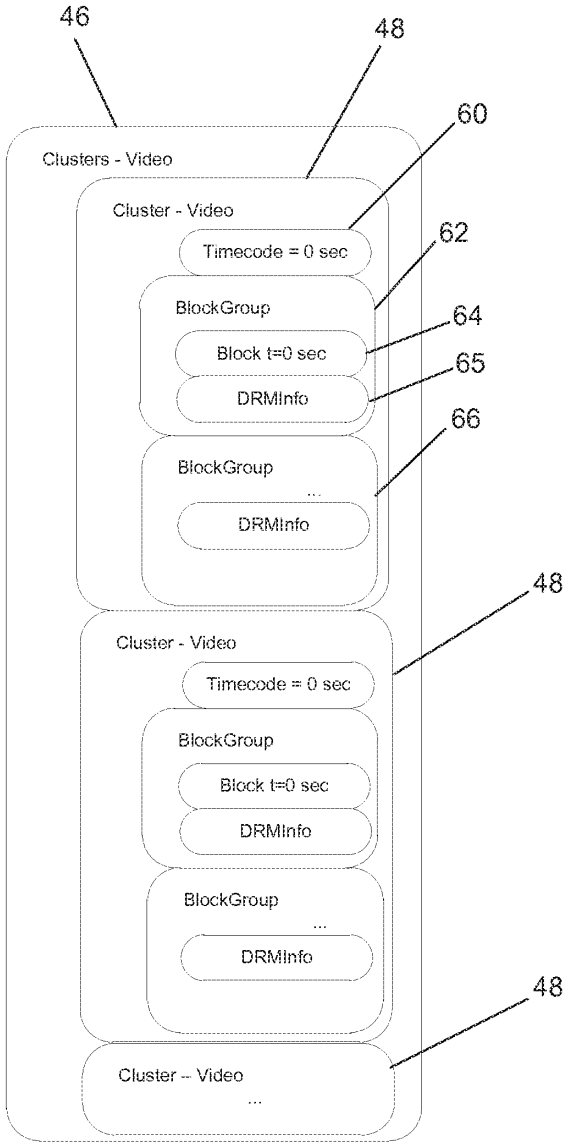

46
48
60
Clusters - Video
Cluster - Video
Timecode = 0 sec
62
BlockGroup
64
Block t=0 sec
65
DRMInfo
66
BlockGroup
...
DRMInfo
48
Cluster - Video
Timecode = 0 sec
BlockGroup
Block t=0 sec
DRMInfo
BlockGroup
...
DRMInfo
48
Cluster -- Video
...

FIG. 4e

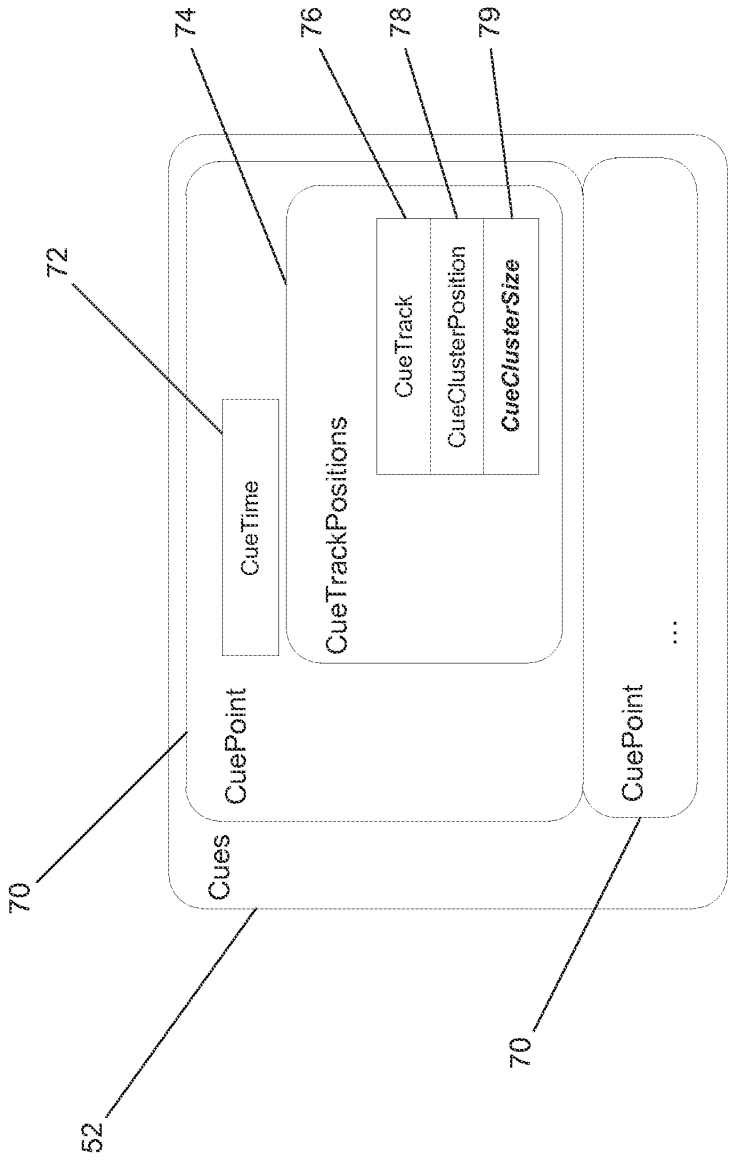

74
76
78
79
72
CueTime
CueTrackPositions
CueTrack
CueClusterPosition
CueClusterSize
CuePoint
CuePoint
...
Cues
70
70
52

FIG. 5

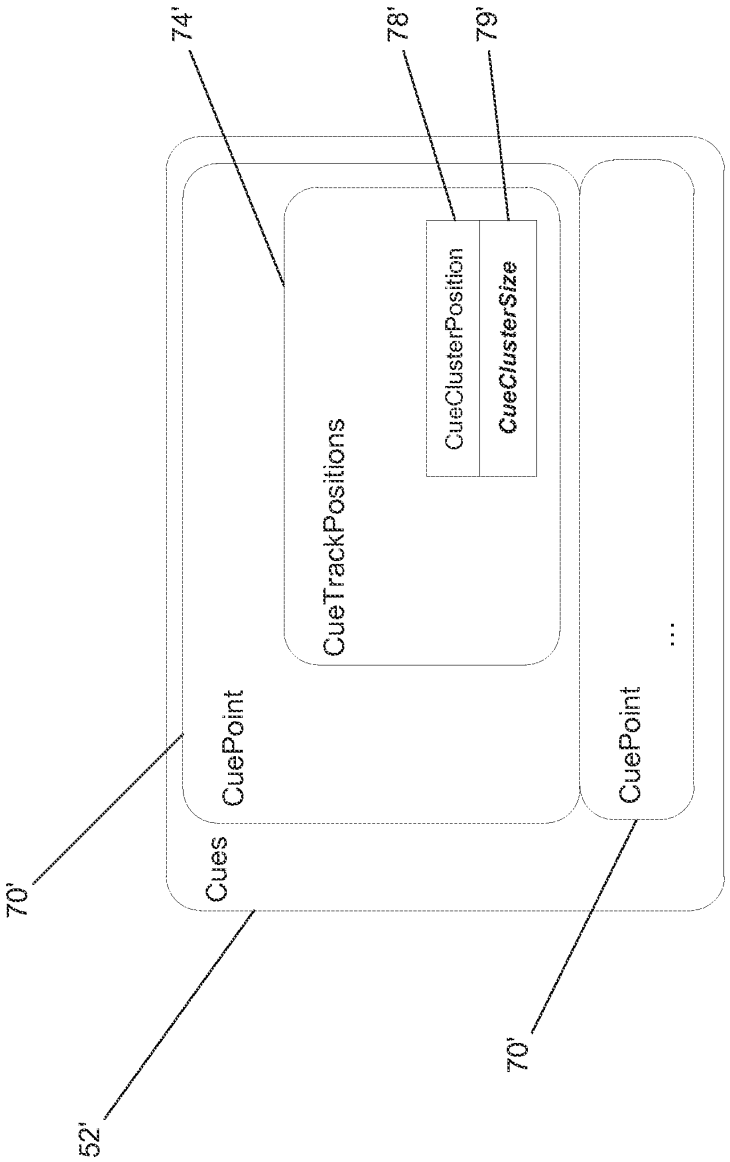

74'
78'
79'
CueClusterPosition
CueClusterSize
CueTrackPositions
CuePoint
...
CuePoint
Cues
70'
52'
70'

FIG. 5a

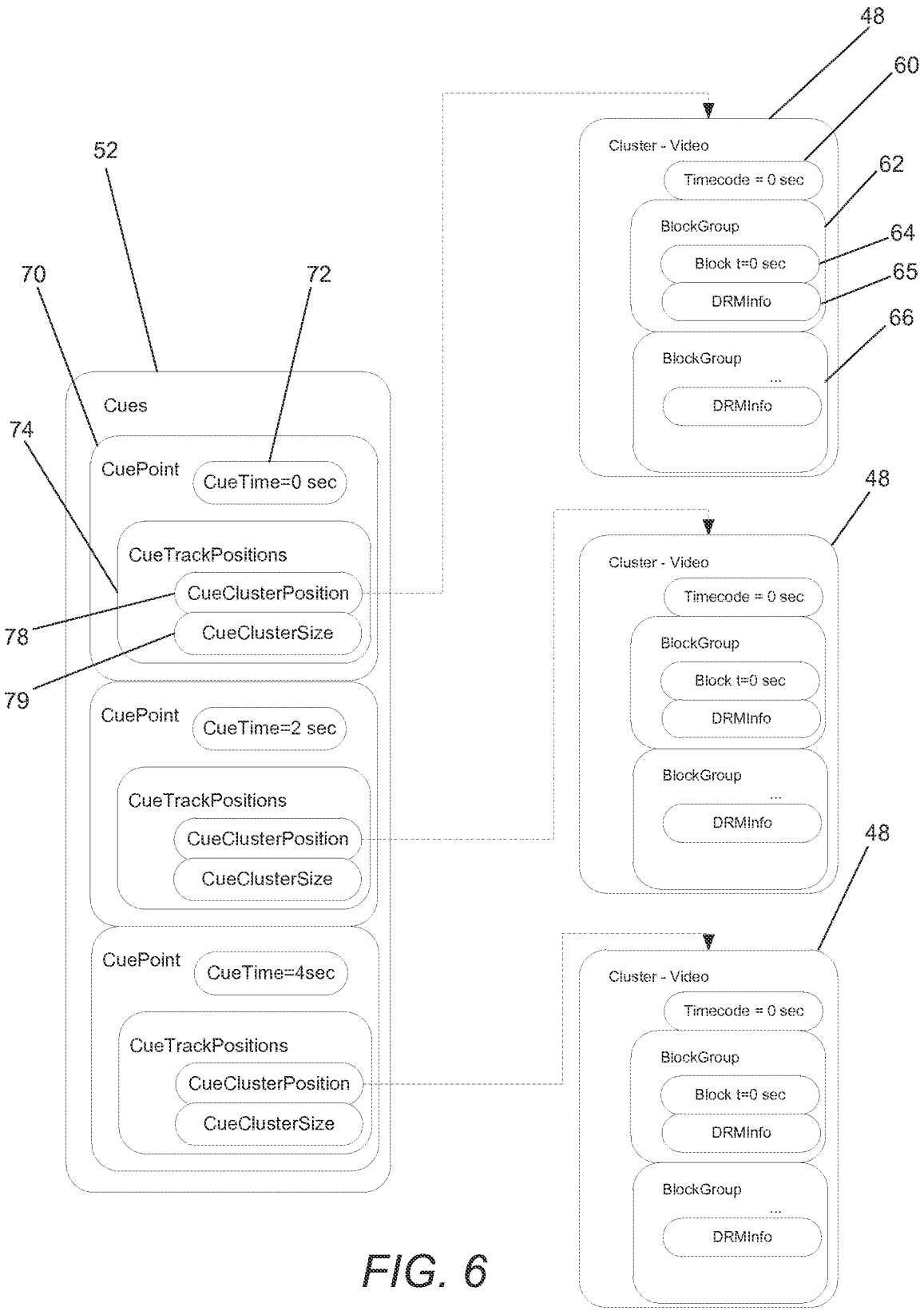

48
60
52
Cluster - Video
Timecode = 0 sec
62
BlockGroup
64
Block t=0 sec
65
DRMInfo
66
BlockGroup
...
DRMInfo
70
72
Cues
74
CuePoint
CueTime=0 sec
CueTrackPositions
CueClusterPosition
CueClusterSize
78
79
CuePoint
CueTime=2 sec
CueTrackPositions
CueClusterPosition
CueClusterSize
CuePoint
CueTime=4sec
CueTrackPositions
CueClusterPosition
CueClusterSize
48
Cluster - Video
Timecode = 0 sec
BlockGroup
Block t=0 sec
DRMInfo
BlockGroup
...
DRMInfo
48
Cluster - Video
Timecode = 0 sec
BlockGroup
Block t=0 sec
DRMInfo
BlockGroup
...
DRMInfo

FIG. 6

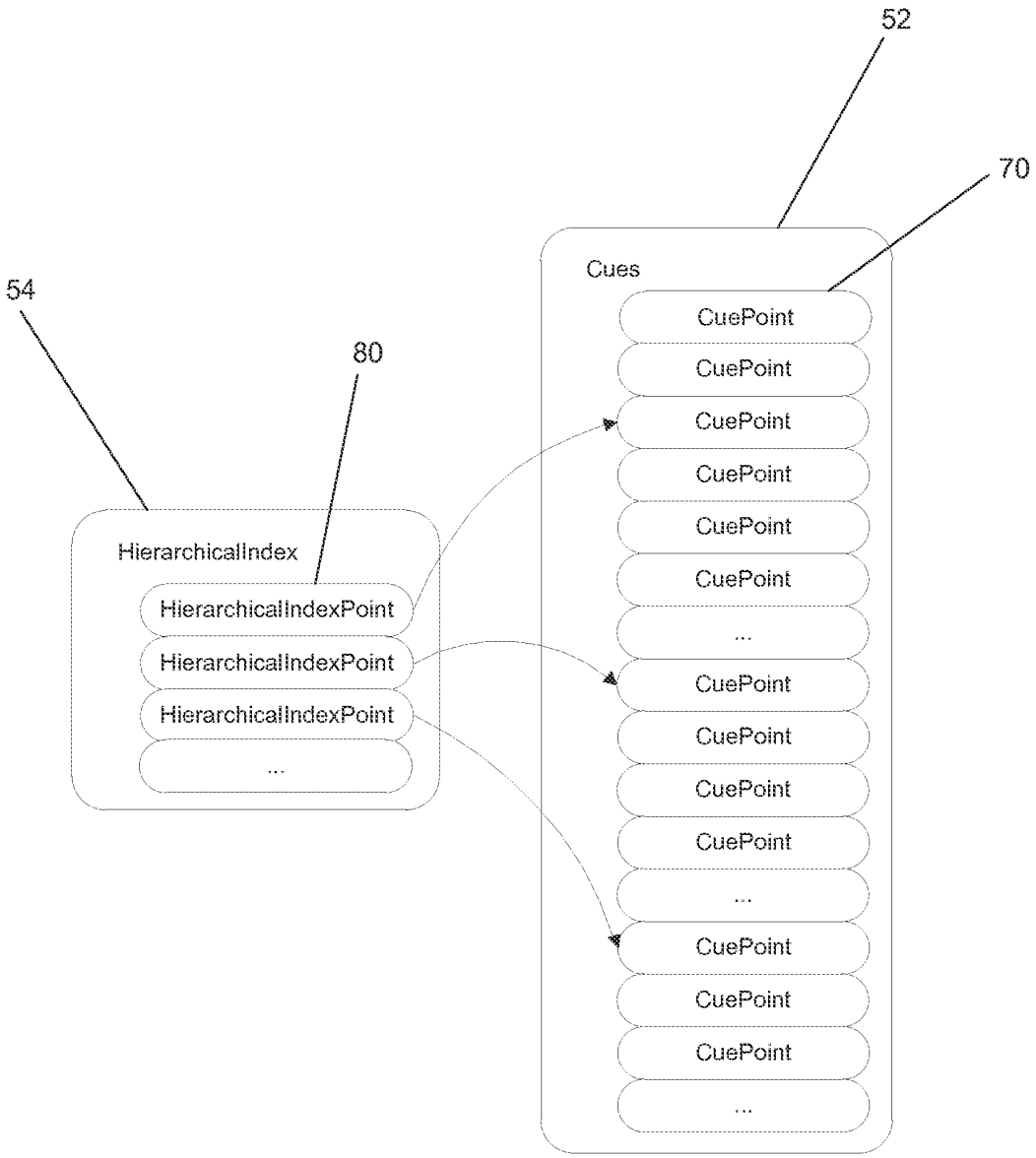

52
70
54
80
Cues
CuePoint
CuePoint
CuePoint
CuePoint
CuePoint
CuePoint
...
CuePoint
CuePoint
CuePoint
CuePoint
...
CuePoint
CuePoint
CuePoint
...
HierarchicalIndex
HierarchicalIndexPoint
HierarchicalIndexPoint
HierarchicalIndexPoint
...

FIG. 7

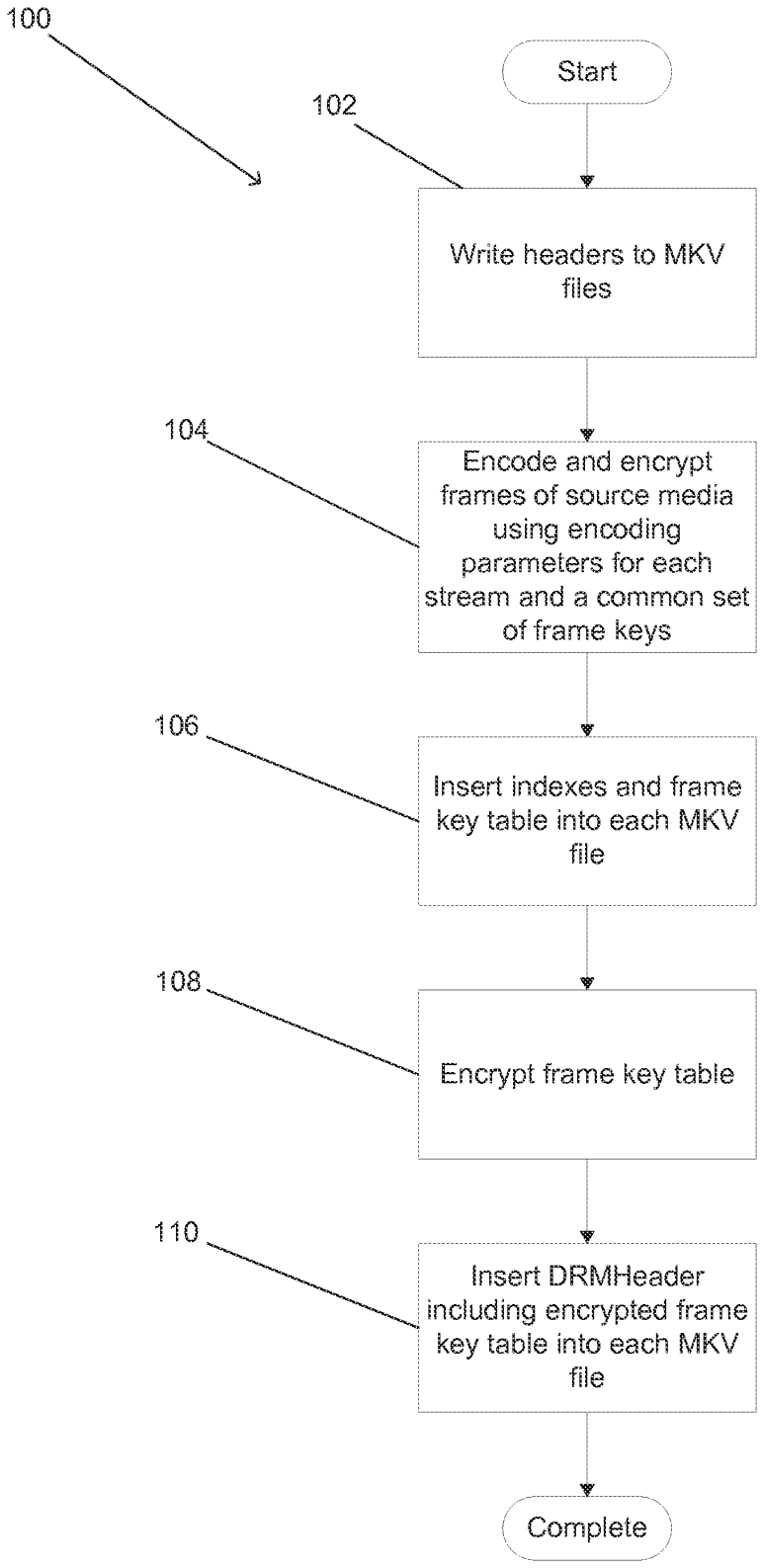

100
Start
102
Write headers to MKV files
104
Encode and encrypt frames of source media using encoding parameters for each stream and a common set of frame keys
106
Insert indexes and frame key table into each MKV file
108
Encrypt frame key table
110
Insert DRMHeader including encrypted frame key table into each MKV file
Complete

FIG. 8

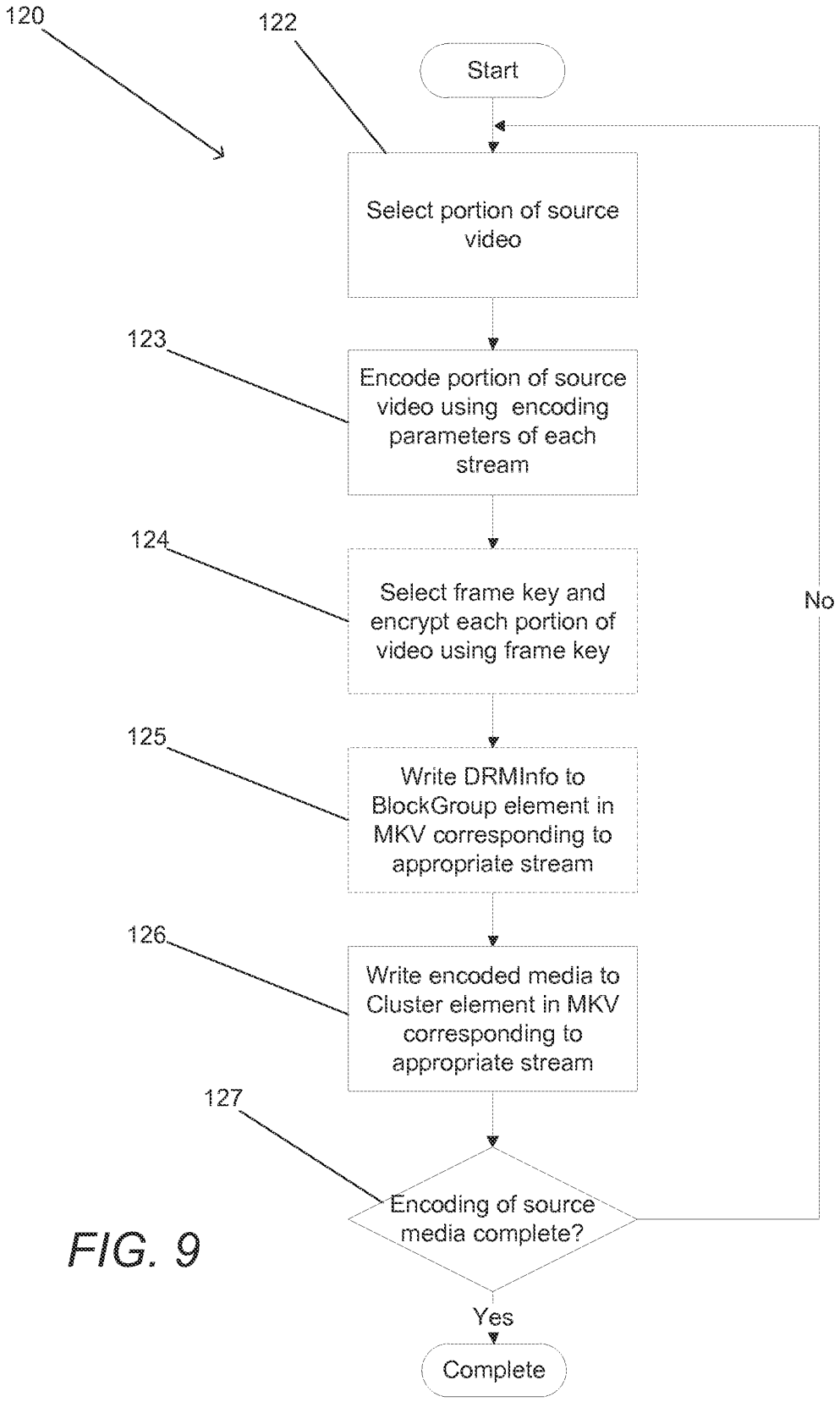

120
122
Start
Select portion of source video
123
Encode portion of source video using encoding parameters of each stream
124
Select frame key and encrypt each portion of video using frame key
125
Write DRMInfo to BlockGroup element in MKV corresponding to appropriate stream
126
Write encoded media to Cluster element in MKV corresponding to appropriate stream
127
Encoding of source media complete?
No
Yes
Complete

FIG. 9

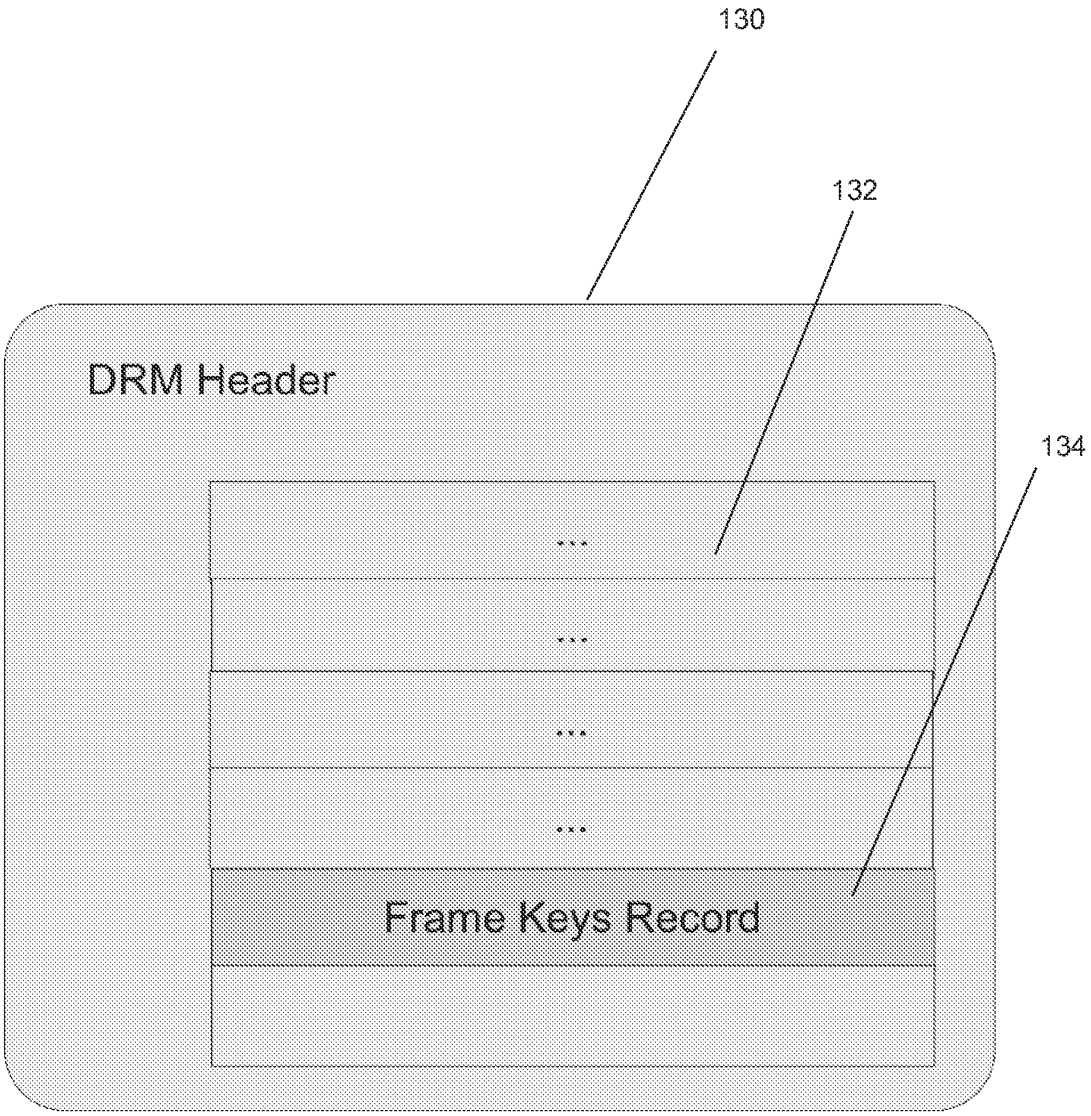


FIG. 10

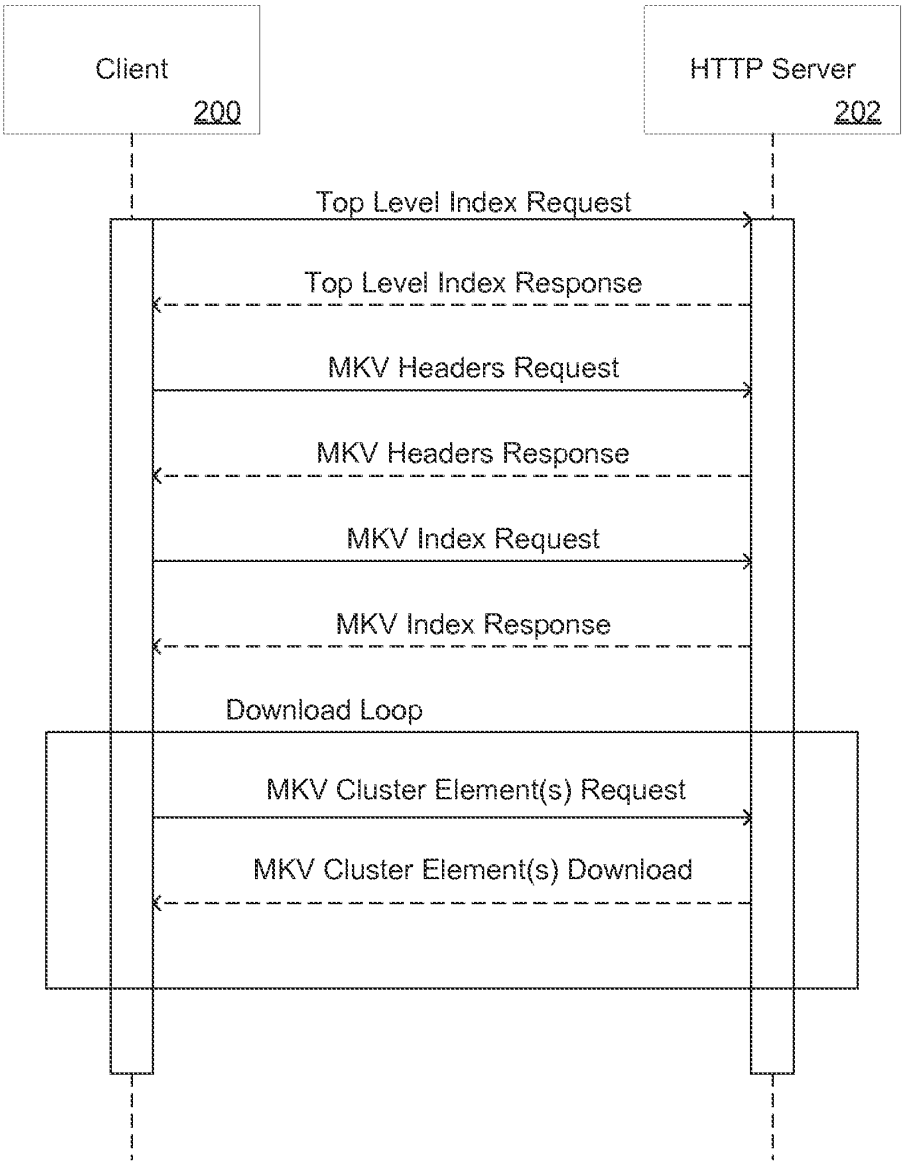

Client
200
HTTP Server
202
Top Level Index Request
Top Level Index Response
MKV Headers Request
MKV Headers Response
MKV Index Request
MKV Index Response
Download Loop
MKV Cluster Element(s) Request
MKV Cluster Element(s) Download

FIG. 11

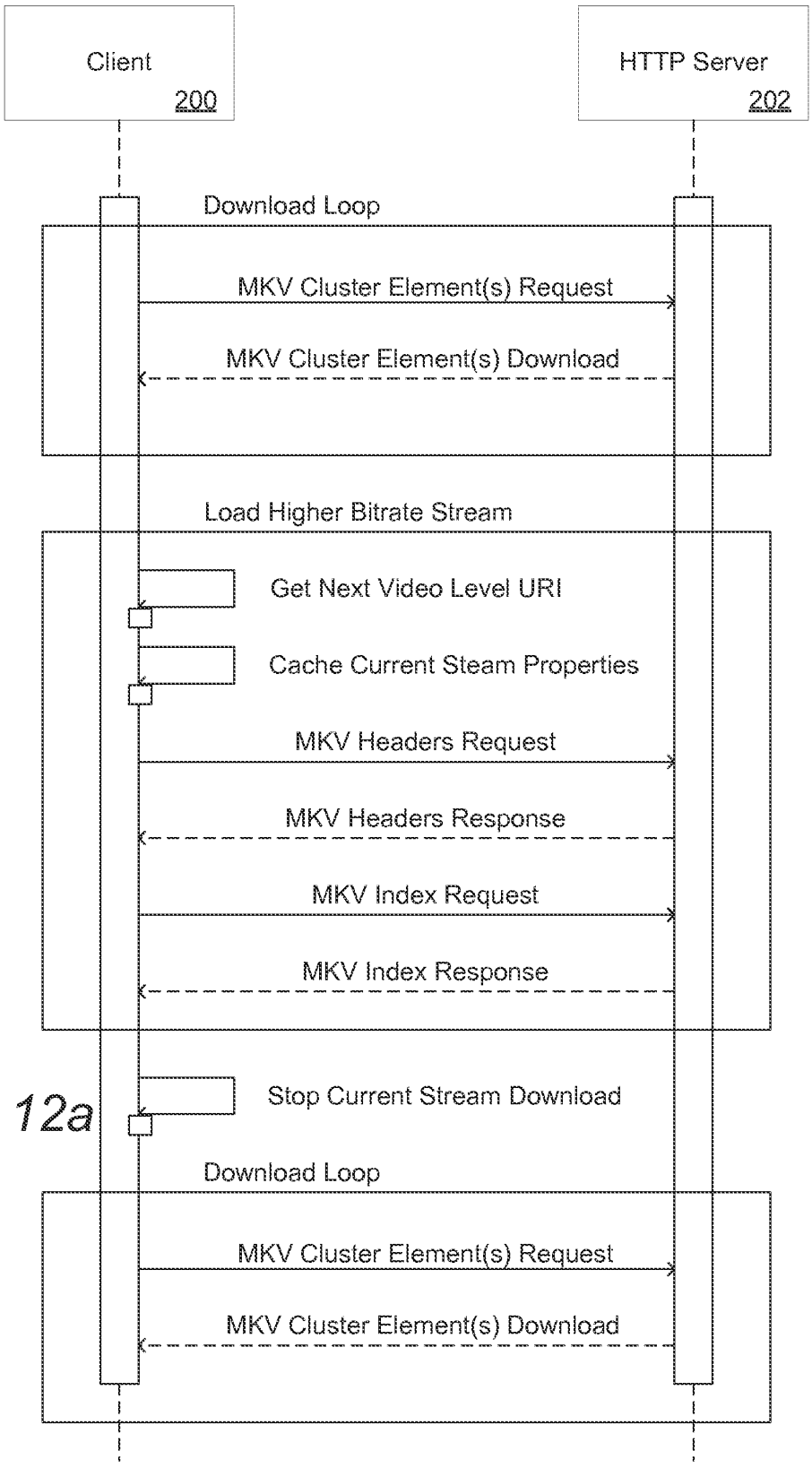

Client
200
HTTP Server
202
Download Loop
MKV Cluster Element(s) Request
MKV Cluster Element(s) Download
Load Higher Bitrate Stream
Get Next Video Level URI
Cache Current Steam Properties
MKV Headers Request
MKV Headers Response
MKV Index Request
MKV Index Response
Stop Current Stream Download
Download Loop
MKV Cluster Element(s) Request
MKV Cluster Element(s) Download

FIG. 12a

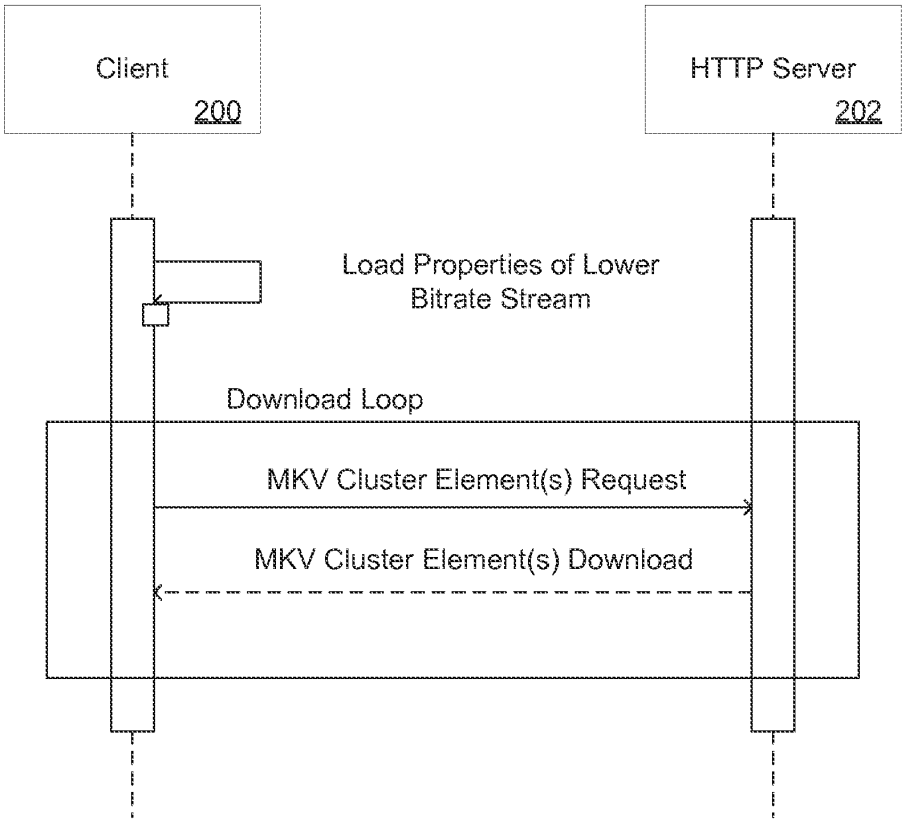

Client
200
HTTP Server
202
Load Properties of Lower
Bitrate Stream
Download Loop
MKV Cluster Element(s) Request
MKV Cluster Element(s) Download

FIG. 12b

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	Systems and Methods for Playing Back Alternative Streams of Protected Content Protected Using Common Cryptographic Information
First Named Inventor/Applicant Name:	Michael George Kiefer
Filer:	David J. Bailey/Trudi Thompson
Attorney Docket Number:	D1:02359A

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility application filing	1011	1	380	380
Utility Search Fee	1111	1	620	620
Utility Examination Fee	1311	1	250	250
Pages:				
Claims:				
Claims in excess of 20	1202	19	60	1140
Miscellaneous-Filing:				
Late filing fee for oath or declaration	1051	1	130	130

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**2520**

Electronic Acknowledgement Receipt

EFS ID:	11733147
Application Number:	13340623
International Application Number:	
Confirmation Number:	1094
Title of Invention:	Systems and Methods for Playing Back Alternative Streams of Protected Content Protected Using Common Cryptographic Information
First Named Inventor/Applicant Name:	Michael George Kiefer
Customer Number:	71897
Filer:	David J. Bailey/Trudi Thompson
Filer Authorized By:	David J. Bailey
Attorney Docket Number:	D1:02359A
Receipt Date:	29-DEC-2011
Filing Date:	
Time Stamp:	22:09:09
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	02359adatasheet.pdf	80307 0f7e7adba57e4f553064fa58b3e8944f323f73b3	no	4

Warnings:	
Information:	

This is not an USPTO supplied ADS fillable form					
2		02359AUSapplication.pdf	151993 01da69c0036a2ce457038be1715b175318f693d0	yes	61

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Specification	1	47
	Claims	48	60
	Abstract	61	61

Warnings:					
Information:					
3	Drawings-only black and white line drawings	02359AUSdrawings.pdf	231459 3265e38aac8ab427992c02524e47721492e39136	no	19
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	37956 29410a521a322ac183fb92fe49ba4c65e6b14a0d	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	501715		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

SCORE Placeholder Sheet for IFW Content

Application Number: 13340623 Document Date: 12/29/2011

The presence of this form in the IFW record indicates that the following document type was received in electronic format on the date identified above. This content is stored in the SCORE database.

- Drawings – Other than Black and White Line Drawings

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded in PALM, and no paper documents or physical media exist. The TIFF images in the IFW record were created from the original documents that are stored in SCORE.

To access the documents in the SCORE database, refer to instructions developed by SIRA.

At the time of document entry (noted above):

- Examiners may access SCORE content via the eDAN interface.
- Other USPTO employees can bookmark the current SCORE URL (http://es/ScoreAccessWeb/).
- External customers may access SCORE content via the Public and Private PAIR interfaces.

Form Revision Date: February 8, 2006