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.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/340,623	12/09/2014	8909922	D1:02359A	1094

71897 7590 11/19/2014

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

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 183 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

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

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 and facilitate 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.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0001
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
KPPB LLP
2400 EAST KATELLA AVENUE
SUITE 1050
ANAHEIM, CA 92806

POA ACCEPTANCE LETTER

OC000000071815221

Date Mailed: 11/13/2014

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 11/10/2014.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/tcouch/

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 0002
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF TRANSMISSION

I hereby certify that the enclosed Fee(s) Transmittal is being electronically filed with the United States Patent and Trademark Office on November 10, 2014 at or before 11:59 p.m. Pacific Time under the Rules of 37 CFR § 1.8.

/Katrina Lee/
Katrina Lee

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

71897 7590 10/03/2014

KPPB LLP
2400 E. Katella Ave., Suite 1050
Anaheim, CA 92806

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

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

TITLE OF INVENTION:

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

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	undiscounted	$960	$0	$0	$960	January 5, 2015

EXAMINER	ART UNIT	CLASS-SUBCLASS
Abiy Getachew	2434	713-160000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 KPPB LLP
2
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: Sonic IP, Inc.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): San Diego, California

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

☒ Issue Fee

☐ Publication Fee (No small entity discount permitted)

☐ Advance Order - # of Copies .....

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

☐ A check is enclosed.

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

☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number 504407 (enclose an extra copy of this form).

PTOL-85 (Rev. 02/11)

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0004
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

5. **Change in Entity Status** (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29	NOTE: Absent a valid certification of Micro Entity Status (see form PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
☐ Applicant asserting small entity status. See 37 CFR 1.27	NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
☐ Applicant changing to regular undiscounted fee status.	NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature /Jason D. Wolfe/ Date 11/10/2014

Typed or printed name Jason D. Wolfe Registration No. 71,327

This collection of information is required by 37 CFR 1.311. 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, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

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.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0005
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:	Jason Daniel Wolfe/Katrina Lee
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:				
Utility Appl Issue Fee	1501	1	960	960
Publ. Fee- Early, Voluntary, or Normal	1504	1	0	0

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**960**

Electronic Acknowledgement Receipt

EFS ID:	20656438
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:	10-NOV-2014
Filing Date:	29-DEC-2011
Time Stamp:	20:57:40
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$960
RAM confirmation Number	7216
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	Transmittal Letter	02359apoaxtml.pdf	98781 e79562b98d07d5a513f542cd38038d8efed1f60a	no	1
Warnings:					
Information:					
2	Assignee showing of ownership per 37 CFR 3.73.	02359aassigneestatement.pdf	78002 8bb299cf097874c631671e46751c3b3110e75d08	no	2
Warnings:					
Information:					
3	Power of Attorney	02359apoa.pdf	1425943 8d0b108d5f8de40102b338d8ab4ae75a421965c7	no	1
Warnings:					
Information:					
4	Issue Fee Payment (PTO-85B)	02359aissuefeextml.pdf	1983532 1646df3dad7b9b32b20c03d5a5045a14bb46919d	no	3
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	32340 6655100f33228065b9967f7369ac4d2cf91329d4	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	3618598		

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 November 10, 2014 at or before 11:59 p.m. Pacific Time under the Rules of 37 C.F.R. 1.8.

/Katrina Lee/
Katrina Lee

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

TRANSMITTAL OF POWER OF ATTORNEY

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

2400 E. Katella Ave., Suite 1050
Anaheim, CA 92806
November 10, 2014

Commissioner:

Enclosed is the Power of Attorney for the Assignee of record in the above-referenced patent application.

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,

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

JDW/kl
Enclosures

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. 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.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: Sonic IP, Inc.

Application No./Patent No.: 13/340,623 Filed/Issue Date: December 29, 2011

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

Sonic IP, Inc., a corporation

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☑ The assignee of the entire right, title, and interest.

2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):

   ☐ The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.

   ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (*e.g.*, bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

A. ☐ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

B. ☑ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: Michael George Kiefer; Eric William Grab; Jason Braness To: DivX, LLC

   The document was recorded in the United States Patent and Trademark Office at
   Reel 027897, Frame 0620, or for which a copy thereof is attached.

2. From: DivX, LLC To: Sonic IP, Inc.

   The document was recorded in the United States Patent and Trademark Office at
   Reel 031713, Frame 0032, or for which a copy thereof is attached.

This collection of information is required by 37 CFR 3.73(b). 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 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.

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. 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.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☑ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Jason D. Wolfe/	11/10/2014
Signature	Date
Jason D. Wolfe	71,327
Printed or Typed Name	Title or Registration Number

PTO/SB/80 (11-08)
Approved for use through 11/30/2011. OMB 0651-0035
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.

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(b).

I hereby appoint:

☑ Practitioners associated with the Customer Number: 71897

OR

☐ Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

as attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(b).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(b) to:

☑ The address associated with Customer Number: 71897

OR

☐ Firm or Individual Name			
Address			
City		State	Zip
Country			
Telephone		Email	

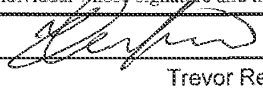
Assignee Name and Address:

Sonic IP, Inc.
4780 Eastgate Mall
San Diego, CA 92121

A copy of this form, together with a statement under 37 CFR 3.73(b) (Form PTO/SB/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(b) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature		Date
Name	Trevor Renfield	Telephone
Title	Treasurer, Sonic IP, Inc.	

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. 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 3 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.

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

71897 7590 10/03/2014

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

EXAMINER
GETACHEW, ABIY

ART UNIT	PAPER NUMBER
2434	

DATE MAILED: 10/03/2014

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

TITLE OF INVENTION: SYSTEMS AND METHODS FOR PLAYING BACK ALTERNATIVE STREAMS OF PROTECTED CONTENT PROTECTED USING COMMON CRYPTOGRAPHIC INFORMATION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$960	$0	$0	$960	01/05/2015

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0015
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

71897 7590 10/03/2014

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

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

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

TITLE OF INVENTION: SYSTEMS AND METHODS FOR PLAYING BACK ALTERNATIVE STREAMS OF PROTECTED CONTENT PROTECTED USING COMMON CRYPTOGRAPHIC INFORMATION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$960	$0	$0	$960	01/05/2015

EXAMINER	ART UNIT	CLASS-SUBCLASS
GETACHEW, ABIY	2434	713-160000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:

❑ Issue Fee

❑ Publication Fee (No small entity discount permitted)

❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

❑ A check is enclosed.

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

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

❑ Applicant asserting small entity status. See 37 CFR 1.27

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

❑ Applicant changing to regular undiscounted fee status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0016
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 10/03/2014

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

EXAMINER	
GETACHEW, ABIY	
ART UNIT	PAPER NUMBER
2434	

DATE MAILED: 10/03/2014

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0017
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. 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, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. 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.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	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--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *09/08/2014*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
2. ☐ 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.
3. ☒ The allowed claim(s) is/are *1,2,4-6,8-10,12-19,21-23,25-29 and 32-38*. As a result of the allowed claim(s), 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 .
4. ☐ 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)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 09/08/2014 and 09/08/2014
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☐ Examiner's Amendment/Comment
6. ☐ Examiner's Statement of Reasons for Allowance
7. ☒ Other *Examiner's Statement*.

/ABIY GETACHEW/ Examiner, Art Unit 2434	/TESHOME HAILU/ Primary Examiner, Art Unit 2434

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0019
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.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after allowance or after an Office action under *Ex Parte Quayle*, 25 USPQ 74, 453 O.G. 213 (Comm'r Pat. 1935). Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, prosecution in this application has been reopened pursuant to 37 CFR 1.114. Applicant's submission filed on 09/08/2014 has been entered.

Allowable Subject Matter

3. Claims 1-2, 4-6, 8-10, 12-19, 21-23, 25-29 and 32-38 are allowed. The information disclosure statements (IDS) submitted 09/08/2014 has been considered. The submission is in compliance with the provisions of 37 CFR 1.97. Form PTO-1449 is signed and attached hereto. The claims recited in claims 1-2, 4-6, 8-10, 12-19, 21-23, 25-29 and 32-38 are reviewed over the references submitted with the IDS. In light of the review; update search and consideration, the claim limitations recited in claims 1-2, 4-6, 8-10, 12-19, 21-23, 25-29 and 32-38 are still found to be distinct and allowable. In view of this

understanding claims 1-2, 4-6, 8-10, 12-19, 21-23, 25-29 and 32-38 are found to be novel and allowed. As the result no further reason for allowance is needed as the record is clear.

4. According to MPEP 1302.14 (I): "In most cases, the examiner's actions and the applicant's replies make evident the reasons for allowance, satisfying the "record as a whole" proviso of the rule. This is particularly true when applicant fully complies with 37 CFR 1.111 (b) and (c) and 37 CFR 1.133(b). Thus, where the examiner's actions clearly point out the reasons for rejection and the applicant's reply explicitly presents reasons why claims are patentable over the reference, the reasons for allowance are in all probability evident from the record and no statement should be necessary."

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.

/ABIY GETACHEW/
Examiner, Art Unit 2434

A.G.
September 18, 2014

/TESHOME HAILU/
Primary Examiner, Art Unit 2434

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	09/25/2014							
1	1	✓	=							
2	2	✓	=							
	3	✓	-							
3	4	✓	=							
4	5	✓	=							
5	6	✓	=							
	7	✓	-							
6	8	✓	=							
7	9	✓	=							
8	10	✓	=							
	11	✓	-							
9	12	✓	=							
10	13	✓	=							
11	14	✓	=							
12	15	✓	=							
14	16	✓	=							
13	17	✓	=							
15	18	✓	=							
16	19	✓	=							
	20	✓	-							
17	21	✓	=							
27	22	✓	=							
28	23	✓	=							
	24	✓	-							
29	25	✓	=							
18	26	✓	=							
19	27	✓	=							
20	28	✓	=							
21	29	✓	=							
	30	✓	-							
	31	✓	-							
22	32	✓	=							
23	33	✓	=							
24	34	✓	=							
25	35	✓	=							
26	36	✓	=							

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0023
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	09/25/2014							
30	37	✓	=							
31	38	✓	=							
	39	✓	-							

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0024
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

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

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0025
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

						11:02
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;	OR	OFF	2013/10/09 11:48

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0026
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			EPO; JPO; DERWENT; IBM_TDB			
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; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 11:55
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;	OR	OFF	2013/10/09 12:41

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0027
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
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; FPRS; EPO; JPO; DERWENT; IBM_TDB	WITH	OFF	2013/10/09 13:02
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

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0028
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

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;	WITH	OFF	2013/10/09 14:08

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0029
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			DERWENT; IBM_TDB			
S56	4	(index or indexing or indexed) near20 (streams with content) near20 (content with cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	WITH	OFF	2013/10/09 14:08
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

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0030
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

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 or indexed) near20 (cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 15:18
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;	OR	OFF	2013/10/09 15:21

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0031
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			DERWENT; IBM_TDB			
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; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 17:50
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;	OR	OFF	2013/10/09 17:51

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0032
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
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;	OR	OFF	2013/10/09

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0033
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			17:57
S92	9	(Request) with (index) near20 (plurality with streams)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/09 18:01
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;	OR	OFF	2013/10/09 18:04

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0034
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			IBM_TDB			
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 same DRM)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 10:19
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;	OR	OFF	2013/10/10 10:23

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0035
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			EPO; JPO; DERWENT; IBM_TDB			
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; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 14:16
S119	10	(DRM with Header same Tracks)	US-PGPUB; USPAT;	OR	OFF	2013/10/10 14:16

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0036
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
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

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0037
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

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 (protected)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 14:55
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;	OR	OFF	2013/10/10 14:58

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0038
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			DERWENT; IBM_TDB			
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; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/10/10 15:49
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;	OR	OFF	2013/10/10 15:51

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0039
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
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	US-PGPUB;	OR	OFF	2013/10/16

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0040
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

		(alternative with streams) same (protected crypto$5)	USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			15:16
S155	1	(13/340623).APP.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 12:47
S156	6105	("Digital Rights Management" or DRM)	USPAT	OR	OFF	2013/11/05 12:51
S158	3456	("Digital Rights Management" or DRM) same (DRM with (encryption or decryption or code))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 12:54
S159	2	("Digital Rights Management" or DRM) same (DRM with (encryption or decryption or code)) and (Matroska with container with files) with (Hypertext with Transfer)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 12:56
S160	4	(("20090132721") or ("20130061045")).PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 12:58
S162	4	("Digital Rights Management" or DRM) same (DRM with (encryption or decryption or code)) and ("top level index file")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 13:02
S163	35	("top level index file")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 13:06
S164	3	("Digital Rights Management" or DRM) near20 ("top level index file")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 13:09
S165	10	("Digital Rights Management" or DRM) and ("top level index file")	US-PGPUB; USPAT; USOCR; FPRS;	OR	OFF	2013/11/05 13:24

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0041
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			EPO; JPO; DERWENT; IBM_TDB			
S166	5	(("20040039916") or ("20100138903")).PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 13:29
S167	35	("top level index file")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 13:48
S168	9	("top level index file").clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 13:52
S169	2	("20060245727").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 13:55
S170	2	("20090132599").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 14:05
S171	6	("2009/0132599").URPN.	USPAT	OR	OFF	2013/11/05 14:17
S172	27	processor and memory and ("top level index file")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 14:19
S173	20	processor and memory and ("top level index file")and (alternative with streams)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 14:19
S175	16	S173 and (client with application)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 14:20

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0042
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

S176	6	(("20130046902") or ("8386621") or ("20090293116")).PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 14:24
S177	203241	(streams witrh protected with content with encrypted with common with cryptographic)	USPAT	OR	OFF	2013/11/05 16:21
S178	484775	(streams witrh protected with content with encrypted with common with cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 16:21
S179	2	(streams with protected with content with encrypted with common with cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 16:21
S180	40	(content with encrypted with common with cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 16:23
S181	2	(streams) near20 (content with encrypted with common with cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 16:24
S182	2	(playback) near20 (content with encrypted with common with cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 16:24
S183	1015	(content with encrypted with cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 16:24
S184	2	(streams with protected with content with encrypted with cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 16:24
S185	20	(streams same content with encrypted with common with cryptographic)	US-PGPUB; USPAT; USOCR;	OR	OFF	2013/11/05 16:25

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0043
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S186	2	(plurality with streams same content with encrypted with common with cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 16:25
S187	2	(streams same content with encrypted with common with cryptographic) and (access with protected with content)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 16:26
S188	20	(streams same content with encrypted with common with cryptographic) and (access with content)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 16:26
S189	6	S188 and (protected with content)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 16:27
S190	2	S188 and (alternative with streams)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 16:33
S191	2	(streams same content with encrypted with common with cryptographic) and (access with content) and (alternative with streams)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 16:34
S192	2	(content with encrypted with common with cryptographic) and (alternative with streams)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 16:34
S193	5972	(alternative with streams)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 16:34
S194	2	(alternative with streams) near20 (content with	US-PGPUB;	OR	OFF	2013/11/05

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0044
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

		encrypted with cryptographic)	USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			16:35
S195	2	(alternative with streams) near20 (encrypted with cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 16:35
S196	2	(alternative with streams) near20 (content with encrypted)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 16:35
S197	2	(alternative with streams) near20 (encrypted with cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 16:35
S198	23	(alternative with streams) near20 (encrypted)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 16:36
S199	3	(alternative with streams) near20 (encrypted) same common	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 16:36
S200	2	(alternative with streams) near20 (encrypted) same (cryptographic with information)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 16:37
S201	1907	(encrypted) near20 (cryptographic with information)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 16:38
S202	2	S201 and (alternative with streams) near20 (encrypted)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	OFF	2013/11/05 16:38

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0045
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			IBM_TDB			
S203	516	(encrypt$3 with common with cryptographic with key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 16:39
S204	1	(alternative with streams) near20 (encrypt$3 with common with cryptographic with key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 16:39
S205	1	(streams) near20 (encrypt$3 with common with cryptographic with key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 16:39
S206	176	(streams data content) near20 (encrypt$3 with common with cryptographic with key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 16:41
S207	11	(streams data content) near20 (encrypt$3 with common with cryptographic with key) and (playback with content)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 16:41
S208	5	(streams data content) near20 (encrypt$3 with common with cryptographic with key) and (playback with content) and (index with file)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 16:42
S209	6	(streams data content) near20 (encrypt$3 with common with cryptographic with key) and (playback with content).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 16:47
S210	29	(streams data content) near20 (encrypt$3 with common with cryptographic with key).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 16:48
S211	2	("20040193876").PN.	US-PGPUB; USPAT; USOCR; FPRS;	OR	OFF	2013/11/05 16:51

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0046
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			EPO; JPO; DERWENT; IBM_TDB			
S212	2	("20020078353").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 16:58
S213	1	("Digital Rights Management" or DRM) near20 (encrypt$3 with common with cryptographic with key).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 17:01
S214	1	(DRM) near20 (encrypt$3 with common with cryptographic with key).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 17:01
S215	3	("Digital Rights Management" or DRM) and (encrypt$3 with common with cryptographic with key).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 17:02
S216	1	("Digital Rights Management" or DRM) near20 (encrypt$3 with common with cryptographic with key).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 17:03
S217	1	(DRM) near20 (encrypt$3 with common with cryptographic with key).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 17:03
S218	2	(DRM) near20 (encrypt$3 with common with cryptographic).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/05 17:03
S219	1120	(hierarchical with index with structure)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/06 15:13
S220	3	(hierarchical with index with structure) and Soroushian	US-PGPUB; USPAT;	OR	OFF	2013/11/06 15:13

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0047
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S221	4	(hierarchical with index with structure) and (top with level with index with file)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/06 15:18
S224	2	(hierarchical with index with structure) and (top with level with index with file) and (content)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/06 15:25
S227	2	(hierarchical with index with structure) same (top with level with index with file)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/06 15:26
S230	13	(streams) same (top with level with index with file)near20 (content)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/06 15:47
S231	12	(streams) same (top with level with index with file)near20 (playback with content)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/06 15:47
S232	3	(streams) same (top with level with index with file)near20 (playback with content).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/06 15:49
S233	2	("7295752").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/06 15:51
S234	1	(10/067550).APP.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/06 15:53

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0048
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

S235	2	("20020150243").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/06 15:57
S236	14	(top with level with index with file)near20 (playback with content)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/06 16:01
S237	2	("20080301734").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/06 16:09
S238	2	("20070074254").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/06 16:13
S239	35	("top level index file")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/06 16:17
S240	9	("top level index file") and (encrypted same cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/06 16:18
S241	1	(level with index) near20 (encrypted same cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/06 16:19
S242	1	(level with index) near20 (common with cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/06 16:20
S243	45	(level with index) near20 (encrypted)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	OFF	2013/11/06 16:21

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0049
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			DERWENT; IBM_TDB			
S244	1	(top with level with index) near20 (encrypted)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/06 16:22
S245	72	(top with level with index) and (encrypted)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/06 16:23
S246	41	(top with level with index) and (encrypted same using)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/06 16:23
S247	19	(top with level with index) and (encrypted same using with key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/06 16:25
S248	1	(top with level with index) near20 (encrypted same encrypted)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/06 16:48
S249	45	(level with index) near20 (encrypted same encrypted)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/06 16:48
S250	6063	(alternative with streams)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/06 16:51
S251	2	(alternative with streams) near20 (encrypted with using with common with cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/06 16:52
S252	2	(alternative with streams) near20 (encrypted with common with cryptographic)	US-PGPUB; USPAT; USOCR;	OR	OFF	2013/11/06 16:52

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0050
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S253	2	(alternative with streams) near20 (encrypt$5 with common with cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/06 16:52
S254	3	(alternative with streams) near20 (encrypt$5 with cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/06 16:53
S255	23	(alternative with streams) near20 (encrypted with encrypt$5)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/06 16:53
S256	117	(("top level index file") or (top with level with index with file))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/06 16:54
S257	2	S255 and S256	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/06 16:55
S258	8	(alternative with streams) near20 (encrypted with using with encrypt$5)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/06 16:55
S259	2	("20080046369").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 09:51
S261	117	(top with level with index with file)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 10:30
S265	3	((top high) with (level layer) with (file$1 document$1	US-PGPUB;	OR	OFF	2013/11/07

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0051
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

		stream content)) near20 (Symmetric common secret) near3 (key)	USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			10:39
S266	1	((top) with (level) with (stream content)) near20 (Symmetric common secret) near3 (key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 10:44
S269	35	(top with level) near20 (Symmetric common secret) near3 (key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 10:46
S270	1	S269 and (protected with content)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 10:46
S273	32	((top high) with (index file)) near20 (Symmetric common secret) near3 (key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 10:48
S274	1	((top high) with (level) with (index)) near20 (Symmetric common secret) near3 (key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 10:49
S277	2	((top) with (level) with (index)) same (Symmetric common secret) near3 (key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 10:51
S278	8154	((encrypted with using) with (Symmetric common secret) near3 (key))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 10:52
S279	11092	((encrypted with using) with (Symmetric common secret))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	OFF	2013/11/07 10:52

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0052
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			IBM_TDB			
S280	1	((top with level with index with file) near20 (Symmetric common secret))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 10:55
S285	15	((top with index) near20 (Symmetric))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 10:56
S286	3	"380"/$.ccls. and (top with level with index with file)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 10:57
S287	2	"380"/$.ccls. and ((top high) with (level layer) with (file$1 document$1 stream content)) near20 (Symmetric common secret) near3 (key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 10:58
S290	742	streams near20 ((top high) with (level layer) with (file$1 document$1 stream content))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 11:40
S291	7	streams near20 ((top high) with (level layer) with (file$1 document$1 stream content)) near20 (Symmetric common secret)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 11:41
S292	1	streams near20 ((top) with (level layer) with (file$1)) near20 (Symmetric common secret)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 11:43
S294	17	streams and ((top) with (level layer) with (file$1)) near20 (Symmetric secret)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 11:43
S295	1	streams and ((top) with (level layer) with (file$1)) near20 (Symmetric encryp$3)	US-PGPUB; USPAT; USOCR; FPRS;	OR	OFF	2013/11/07 12:19

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0053
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			EPO; JPO; DERWENT; IBM_TDB			
S296	11	(streams frame packet stream bitstream) and ((top) with (level layer) with (file$1)) near20 (Symmetric encrypt$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 12:22
S297	3	(top with level with index with file) and (streams frame packet stream bitstream) near20 (Symmetric encrypt$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 12:24
S298	49	(top with index with file) and (streams frame packet stream bitstream) near20 (Symmetric encrypt$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 12:24
S299	1	(top with index with file) near20 ((common with cryptographic) and (playback with content))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 12:33
S300	1	(top with index with file) near20 ((Symmetric encrypt$3) and (playback with content))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 12:34
S301	1	(top with index with file) near20 ((Symmetric encrypt$3) and (content))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 12:35
S302	2	(top with index with file) near20 (Symmetric encrypt$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 12:35
S303	452	(common with cryptographic with information)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 12:37
S304	5	(top with level with index with file) and S303	US-PGPUB; USPAT;	OR	OFF	2013/11/07 12:37

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0054
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S305	5	(top with level with index) and S303	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 12:37
S306	16	(top with level with file) and S303	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 12:38
S308	4	(top with file) near20 (encrypted with using with key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 12:41
S309	1	(11/611188).APP.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 12:43
S310	91230	(content with encrypt$3 with using encrypt$3)	USPAT	OR	OFF	2013/11/07 12:59
S312	1	(top with level with index with file) near20 (content with encrypt$3 with using encrypt$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 13:01
S313	22	(top with level with index with file) and (content with encrypt$3 with using encrypt$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 13:01
S314	7	(top with level with index with file) and (content with encrypt$3 with using encrypt$3) and (plurality with streams)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 13:02
S315	14	(top with level with index with file) and (content with encrypt$3 with using encrypt$3) and (streams)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	OFF	2013/11/07 13:02

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0055
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			DERWENT; IBM_TDB			
S316	22	(top with level with index with file) and (content with encrypt$3 with using encrypt$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 13:18
S317	22	(top with level with index with file) and (encrypt$3 with using encrypt$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 13:22
S318	600	((top high) with (level layer) with (file$1 document$1 stream content)) near20 (Symmetric common secret)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 13:23
S319	210	S318 and (encrypt$3 with using encrypt$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 13:24
S320	1	S319 and (top with index with file)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 13:24
S321	1	S319 and (top with index)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 13:24
S322	32	S319 and (index with file)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 13:24
S323	20	S319 and (index with file) and streams	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 13:25
S324	2	DRM and ((encryption decrption) with (content)) and (matroska with content)	US-PGPUB; USPAT; USOCR;	OR	OFF	2013/11/07 13:29

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0056
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S325	2	("20090158318").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 13:41
S326	254	(distribute with common with key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 13:46
S329	3	(index with file) and (distribute with common with key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 13:47
S330	2	("20090290706").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/07 15:27
S331	2	("20090328228").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/08 13:21
S332	8	(("20090132721") or ("20090290706") or ("20090328228") or ("20130061040")).PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/08 13:55
S333	77792	(plurality same streams)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/08 14:10
S334	41	(plurality same streams) same (protected with content)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/08 14:11
S335	8	(plurality same streams) near10 (protected with	US-PGPUB;	OR	OFF	2013/11/08

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0057
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

		content)	USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			14:11
S336	1	(index with file) near10 (plurality same streams) near10 (protected with content)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/08 14:12
S337	31	(plurality same streams) and (top with level with index with file)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/08 14:15
S338	117	(top with level with index with file)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/08 14:22
S340	1	(top with level with index with file) near20 (common crypto$6)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/08 14:23
S345	14	(top with level with index with file) near20 (playback with content)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/08 14:25
S346	1	(top with level with index with file) near20 encrypt$4 same (playback with content)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/08 14:26
S348	1	(top with level with index with file) near20 encrypt$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/08 14:27
S349	4	(top with level with index with file) near20 (playback with content).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	OFF	2013/11/08 14:28

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0058
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			IBM_TDB			
S350	117	(encrypt$ with stream$ with (common "same" identical$5) with (encrypt$ with Stream$ with (common "same" identical$5) with key)"ti.key").clm. (encrypt$ with stream$ with (common "same" identical$5) with key).ab.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/08 16:18
S351	110	S350 and @ad<"20110901"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/08 16:19
S353	30	S351 and ("713"/$ "726"/$380/$).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/08 16:21
S354	7	S353 and ((access$ play$ play$1back playback) with (Common "same" identical$5) with Key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/08 16:22
S356	2	("20070067646").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/11 12:10
S357	2	("20130046902").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/11 12:22
S358	22	(multimedia with digital with data with transmission with procedure)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/11 13:06
S359	12733	((access$ play$ play$1back playback) with (Common "same" identical$5) with Key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/11 13:30
S360	1	(top with level with index with file) near20 encrypt$4 same (playback)	US-PGPUB; USPAT; USOCR; FPRS;	OR	OFF	2013/11/11 14:32

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0059
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			EPO; JPO; DERWENT; IBM_TDB			
S361	2	("20080172341").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/12 10:12
S362	2	("20130046902").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/12 11:43
S363	87	(stream$4 same bitrate with stream$3 with encoded with media)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/12 11:51
S364	11	(stream$4 same bitrate with stream$3 with encoded with media) same (Matroska same container ame files same Hypertext with Transfer with Protocol)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/12 11:52
S365	10	(stream$4 same bitrate with stream$3 with encoded with media) near20 (Matroska)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/12 11:53
S366	87	(stream$4 same bitrate with stream$3 with encoded with media)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/12 11:53
S367	4127	(stream$3 with encoded with media)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/12 11:53
S368	12	(stream$3 with encoded with media) near20 (Matroska)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/12 11:53
S369	42	(stream$3) near20 (Matroska)	US-PGPUB; USPAT;	OR	OFF	2013/11/12 11:55

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0060
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S370	9	S369 and processor and (memory with client with application)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/12 11:56
S371	2	("6005621").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/12 12:00
S372	1	(stream$3 with encoded with media with Matroska)	USPAT	OR	OFF	2013/11/12 14:28
S373	0	(stream$3 with encoded with media near20 Matroska)	USPAT	OR	OFF	2013/11/12 14:29
S374	1	(stream$3 with encoded with media same Matroska)	USPAT	OR	OFF	2013/11/12 14:30
S375	3	(stream$3 with encoded same Matroska)	USPAT	OR	OFF	2013/11/12 14:30
S377	11	("top level index file" near20 Matroska)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/12 14:32
S378	2	("20070140647").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/12 14:35
S379	159	Matroska	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/12 15:52
S380	143	Matroska and (plurality adj$3 streams)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/12 15:52
S381	0	Matroska and (plurality adj$3 streams) near20 (common with crypt$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	OFF	2013/11/12 15:53

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0061
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			DERWENT; IBM_TDB			
S382	2	Matroska and (plurality adj$3 streams) near20 (encrypt$3 with use$3 same cryptographic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/12 15:54
S383	6	Matroska and (plurality adj$3 streams) near20 (encrypt$3 with use$3 same encrypt$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/12 15:55
S384	6	Matroska and (streams) near20 (encrypt$3 with use$3 same encrypt$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/12 16:07
S385	2	("20100107260").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/12 16:53
S386	2	("20110135090").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/12 17:10
S387	2	("20040081333").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/12 17:21
S388	2	("20090290706").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/14 16:27
S389	1	(13/258981).APP.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/14 16:33
S390	2	("20110283361").PN.	US-PGPUB; USPAT; USOCR;	OR	OFF	2013/11/15 14:33

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0062
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S391	2	("2009290706").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/16 11:31
S392	2	("20090290706").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/16 11:31
S393	2	("20070067646").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/16 11:50
S394	1	(13/340623).APP.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/16 14:10
S395	4	("2011103364").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/16 14:51
S396	1	(13/579020).APP.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/16 14:51
S397	2	("20090328228").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/16 14:52
S398	2	("20090132721").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/16 14:53
S399	0	("20090328228and(protect$4withframewithvideo)").PN.	US-PGPUB;	OR	OFF	2013/11/17

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0063
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			10:38
S400	0	"20090328228" and(protect$4 with frame with video)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/17 10:40
S401	3	"20090328228" and (protect$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/17 10:41
S403	36482	(protect$4)same (encrypted)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/17 10:48
S405	2	("20090328228").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/17 10:48
S412	10	("digital rights management" or "DRM") near20 (protect$4 with frame with video)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/17 11:08
S413	2	("digital rights management" or "DRM") near20 (protect$4 with frame with video) same (video same encrypted)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/17 11:11
S414	9	("digital rights management" or "DRM") near20 (protect$4 with frame with video) and (video same encrypted)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/17 11:13
S415	4	("2011103364").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	OFF	2013/11/17 12:45

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0064
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			IBM_TDB			
S418	4	("2011103364").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/17 14:39
S419	1	(13/579020).APP.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/17 14:39
S420	2	("20110103364").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/17 15:19
S429	4	("2011103364").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/17 15:27
S430	1	WO-2011103364-$.did.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/17 15:28
S431	1	WO-2011103364-$.did.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/17 15:30
S432	2	("20090132721").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/17 16:42
S433	4	("2011103364").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/11/17 17:08
S434	0	("20111003364").PN.	US-PGPUB; USPAT; USOCR; FPRS;	OR	OFF	2013/11/17 17:08

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0065
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			EPO; JPO; DERWENT; IBM_TDB			
S435	2034	((access$ play$ play$1back playback) with (common "same" identical$5) with key).ab.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/11 10:41
S436	12060	((access$ play$ play$1back playback) with (common "same" identical$5) with key) and @ad<"20110901"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/11 10:43
S440	396	(("20010046299" | "20020051494" | "20020110193" | "20030001964" | "20030002578" | "20030035488" | "20030035545" | "20030035546" | "20030093799" | "20030152370" | "20030163824" | "20030174844" | "20030185542" | "20030231863" | "20030231867" | "20030233464" | "20030236836" | "20030236907" | "20040081333" | "20040105549" | "20040136698" | "20040255115" | "20050038826" | "20050071280" | "20050193070" | "20050193322" | "20050204289" | "20050207578" | "20050273695" | "20060036549" | "20060052095" | "20060064605" | "20060129909" | "20060245727" | "20070031110" | "20070086528" | "20070140647" | "20070154165" | "20070168541" | "20070168542" | "20070180125" | "20070192810" | "20070192818" | "20070195744" | "20070239839" | "20070292107" | "20080120389" | "20080137736" | "20080256105" | "20080263354" | "20080310454" | "20080310496" | "20090031220" | "20090048852" | "20090055546" | "20090132599" | "20090169181" | "20090201988" | "20090307258" | "20090307267" | "20090313544" | "20100040351" | "20100074324" | "20100095121" | "20110047209" | "20110066673" | "20110080940" | "20110126191" | "20110150100" | "20110153785" | "20110197237" | "20110225315" | "20110239078" | "20110246659" | "20110302319" | "20110314176" | "20120023251" | "20120093214" | "20120170642" | "20120170906" | "20120254455" | "20130046902" | "20130166765" | "20130166906" | "20130311094" | "20140101722" | "20140189065" | "20140201382" | "5361332" | "5404436" | "5502766" | "5509070" | "5754648" | "5805700" | "5892900" | "5999812" | "6031622" | "6155840" | "6175921" | "6195388" | "6282653" | "6289450" | "6449719" | "6466671" | "6510513" | "6658056" | "6807306" | "6810389" | "6859496" | "6956901" | "6965993" | "0604469" | "7007170" | "7043473" | "7151832" | "7151833" | "7165175" | "7185363" | "7242772" | "7328345" | "7349886" | "7356143" | "7376831" | "7406174" | "7472280" | "7478325" | "7484103" | "7526450" | "7594271" | "7640435" | "7817608" | "7991156" | "8023562" | "8046453" | "8054880" | "8201264" | "8225061" | "8233768" | "8249168" | "8261356" | "8270473" | "8270819" | "8289338" | "8291460" | "8311115" | "8321556" | "8386621" | "8412841" | "8456380" | "8472792" | "8515265" | "8781122") or (".PN")).PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/11 14:45

S441	0	(("20090132721" | "20090290706" | "20090328228" | "20130061040").PN.").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/11 15:05
S442	10	(("20090132721" | "20090290706" | "20090328228" | "20130061040") or (".PN.")).PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/11 15:05
S443	4	(("5715403") or ("6141754")).PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/11 15:23
S444	0	(("20010046299" | "20020051494" | "20020110193" | "20030001964" | "20030002578" | "20030035488" | "20030035545" | "20030035546" | "20030093799" | "20030152370" | "20030163824" | "20030174844" | "20030185542" | "20030231863" | "20030231867" | "20030233464" | "20030236836" | "20030236907" | "20040081333" | "20040105549" | "20040136698" | "20040255115" | "20050038826" | "20050071280" | "20050193070" | "20050193322" | "20050204289" | "20050207578" | "20050273695" | "20060036549" | "20060052095" | "20060064605" | "20060129909" | "20060245727" | "20070031110" | "20070086528" | "20070140647" | "20070154165" | "20070168541" | "20070168542" | "20070180125" | "20070192810" | "20070192818" | "20070195744" | "20070239839" | "20070292107" | "20080120389" | "20080137736" | "20080256105" | "20080263354" | "20080310454" | "20080310496" | "20090031220" | "20090048852" | "20090055546" | "20090132599" | "20090169181" | "20090201988" | "20090307258" | "20090307267" | "20090313544" | "20100040351" | "20100074324" | "20100095121" | "20110047209" | "20110066673" | "20110080940" | "20110126191" | "20110150100" | "20110153785" | "20110197237" | "20110225315" | "20110239078" | "20110246659" | "20110302319" | "20110314176" | "20120023251" | "20120093214" | "20120170642" | "20120170906" | "20120254455" | "20130046902" | "20130166765" | "20130166906" | "20130311094" | "20140101722" | "20140189065" | "20140201382" | "5361332" | "5404436" | "5502766" | "5509070" | "5754648" | "5805700" | "5892900" | "5999812" | "6031622" | "6155840" | "6175921" | "6195388" | "6282653" | "6289450" | "6449719" | "6466671" | "6510513" | "6658056" | "6807306" | "6810389" | "6859496" | "6956901" | "6965993" | "0604469" | "7007170" | "7043473" | "7151832" | "7151833" | "7165175" | "7185363" | "7242772" | "7328345" | "7349886" | "7356143" | "7376831" | "7406174" | "7472280" | "7478325" | "7484103" | "7526450" | "7594271" | "7640435" | "7817608" | "7991156" | "8023562" | "8046453" | "8054880" | "8201264" | "8225061" | "8233768" | "8249168" |	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/11 15:25

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0067
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

		"8261356" | "8270473" | "8270819" | "8289338" | "8291460" | "8311115" | "8321556" | "8386621" | "8412841" | "8456380" | "8472792" | "8515265" | "8781122")").PN.				
S445	396	("20010046299" | "20020051494" | "20020110193" | "20030001964" | "20030002578" | "20030035488" | "20030035545" | "20030035546" | "20030093799" | "20030152370" | "20030163824" | "20030174844" | "20030185542" | "20030231863" | "20030231867" | "20030233464" | "20030236836" | "20030236907" | "20040081333" | "20040105549" | "20040136698" | "20040255115" | "20050038826" | "20050071280" | "20050193070" | "20050193322" | "20050204289" | "20050207578" | "20050273695" | "20060036549" | "20060052095" | "20060064605" | "20060129909" | "20060245727" | "20070031110" | "20070086528" | "20070140647" | "20070154165" | "20070168541" | "20070168542" | "20070180125" | "20070192810" | "20070192818" | "20070195744" | "20070239839" | "20070292107" | "20080120389" | "20080137736" | "20080256105" | "20080263354" | "20080310454" | "20080310496" | "20090031220" | "20090048852" | "20090055546" | "20090132599" | "20090169181" | "20090201988" | "20090307258" | "20090307267" | "20090313544" | "20100040351" | "20100074324" | "20100095121" | "20110047209" | "20110066673" | "20110080940" | "20110126191" | "20110150100" | "20110153785" | "20110197237" | "20110225315" | "20110239078" | "20110246659" | "20110302319" | "20110314176" | "20120023251" | "20120093214" | "20120170642" | "20120170906" | "20120254455" | "20130046902" | "20130166765" | "20130166906" | "20130311094" | "20140101722" | "20140189065" | "20140201382" | "5361332" | "5404436" | "5502766" | "5509070" | "5754648" | "5805700" | "5892900" | "5999812" | "6031622" | "6155840" | "6175921" | "6195388" | "6282653" | "6289450" | "6449719" | "6466671" | "6510513" | "6658056" | "6807306" | "6810389" | "6859496" | "6956901" | "6965993" | "0604469" | "7007170" | "7043473" | "7151832" | "7151833" | "7165175" | "7185363" | "7242772" | "7328345" | "7349886" | "7356143" | "7376831" | "7406174" | "7472280" | "7478325" | "7484103" | "7526450" | "7594271" | "7640435" | "7817608" | "7991156" | "8023562" | "8046453" | "8054880" | "8201264" | "8225061" | "8233768" | "8249168" | "8261356" | "8270473" | "8270819" | "8289338" | "8291460" | "8311115" | "8321556" | "8386621" | "8412841" | "8456380" | "8472792" | "8515265" | "8781122").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/11 15:25
S446	396	("20010046299" | "20020051494" | "20020110193" | "20030001964" | "20030002578" | "20030035488" | "20030035545" | "20030035546" | "20030093799" | "20030152370" | "20030163824" | "20030174844" | "20030185542" | "20030231863" | "20030231867" | "20030233464" | "20030236836" | "20030236907" | "20040081333" | "20040105549" | "20040136698" | "20040255115" | "20050038826" | "20050071280" | "20050193070" | "20050193322" | "20050204289" | "20050207578" | "20050273695" | "20060036549" | "20060052095" | "20060064605" | "20060129909" | "20060245727" | "20070031110" | "20070086528" | "20070140647" | "20070154165" | "20070168541" | "20070168542" | "20070180125" | "20070192810" |	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/11 19:20

		"20070192818" | "20070195744" | "20070239839" | "20070292107" | "20080120389" | "20080137736" | "20080256105" | "20080263354" | "20080310454" | "20080310496" | "20090031220" | "20090048852" | "20090055546" | "20090132599" | "20090169181" | "20090201988" | "20090307258" | "20090307267" | "20090313544" | "20100040351" | "20100074324" | "20100095121" | "20110047209" | "20110066673" | "20110080940" | "20110126191" | "20110150100" | "20110153785" | "20110197237" | "20110225315" | "20110239078" | "20110246659" | "20110302319" | "20110314176" | "20120023251" | "20120093214" | "20120170642" | "20120170906" | "20120254455" | "20130046902" | "20130166765" | "20130166906" | "20130311094" | "20140101722" | "20140189065" | "20140201382" | "5361332" | "5404436" | "5502766" | "5509070" | "5754648" | "5805700" | "5892900" | "5999812" | "6031622" | "6155840" | "6175921" | "6195388" | "6282653" | "6289450" | "6449719" | "6466671" | "6510513" | "6658056" | "6807306" | "6810389" | "6859496" | "6956901" | "6965993" | "0604469" | "7007170" | "7043473" | "7151832" | "7151833" | "7165175" | "7185363" | "7242772" | "7328345" | "7349886" | "7356143" | "7376831" | "7406174" | "7472280" | "7478325" | "7484103" | "7526450" | "7594271" | "7640435" | "7817608" | "7991156" | "8023562" | "8046453" | "8054880" | "8201264" | "8225061" | "8233768" | "8249168" | "8261356" | "8270473" | "8270819" | "8289338" | "8291460" | "8311115" | "8321556" | "8386621" | "8412841" | "8456380" | "8472792" | "8515265" | "8781122").PN.				
S447	4	("5715403" | "6141754").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/11 19:25
S448	2	("20090290706").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/22 10:01
S450	2	("20090328228").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/22 10:03
S451	3	("20090132721").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/22 10:04
S452	2	("20090158318").PN.	US-PGPUB; USPAT;	OR	OFF	2014/09/22 10:06

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0069
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

			USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S453	3	("20060101269").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/22 10:08
S454	2	("20070283448").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/22 10:09
S455	2	("20090290706").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/22 10:23
S456	2	("20090328228").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/22 10:24
S457	8	("2008013272").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/22 10:24
S458	2	("20080132721").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/22 10:24
S459	3	("20090132721").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/22 10:25
S460	0	("WO-2011103364-$.did.").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/22 10:41

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0070
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

S461	3	("20130054972").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/22 10:43
S465	2	WO-2011103364-$.did.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/22 10:45
S466	2	("20090158318").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/22 10:46
S467	2	("20060191289").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/22 10:47
S468	3	("20060101269").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/22 10:47
S469	396	("20010046299" | "20020051494" | "20020110193" | "20030001964" | "20030002578" | "20030035488" | "20030035545" | "20030035546" | "20030093799" | "20030152370" | "20030163824" | "20030174844" | "20030185542" | "20030231863" | "20030231867" | "20030233464" | "20030236836" | "20030236907" | "20040081333" | "20040105549" | "20040136698" | "20040255115" | "20050038826" | "20050071280" | "20050193070" | "20050193322" | "20050204289" | "20050207578" | "20050273695" | "20060036549" | "20060052095" | "20060064605" | "20060129909" | "20060245727" | "20070031110" | "20070086528" | "20070140647" | "20070154165" | "20070168541" | "20070168542" | "20070180125" | "20070192810" | "20070192818" | "20070195744" | "20070239839" | "20070292107" | "20080120389" | "20080137736" | "20080256105" | "20080263354" | "20080310454" | "20080310496" | "20090031220" | "20090048852" | "20090055546" | "20090132599" | "20090169181" | "20090201988" | "20090307258" | "20090307267" | "20090313544" | "20100040351" | "20100074324" | "20100095121" | "20110047209" | "20110066673" | "20110080940" | "20110126191" | "20110150100" | "20110153785" | "20110197237" | "20110225315" | "20110239078" | "20110246659" | "20110302319" | "20110314176" | "20120023251" | "20120093214" | "20120170642" | "20120170906" | "20120254455" |	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/22 13:26

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0071
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

		"20130046902" | "20130166765" | "20130166906" | "20130311094" | "20140101722" | "20140189065" | "20140201382" | "5361332" | "5404436" | "5502766" | "5509070" | "5754648" | "5805700" | "5892900" | "5999812" | "6031622" | "6155840" | "6175921" | "6195388" | "6282653" | "6289450" | "6449719" | "6466671" | "6510513" | "6658056" | "6807306" | "6810389" | "6859496" | "6956901" | "6965993" | "0604469" | "7007170" | "7043473" | "7151832" | "7151833" | "7165175" | "7185363" | "7242772" | "7328345" | "7349886" | "7356143" | "7376831" | "7406174" | "7472280" | "7478325" | "7484103" | "7526450" | "7594271" | "7640435" | "7817608" | "7991156" | "8023562" | "8046453" | "8054880" | "8201264" | "8225061" | "8233768" | "8249168" | "8261356" | "8270473" | "8270819" | "8289338" | "8291460" | "8311115" | "8321556" | "8386621" | "8412841" | "8456380" | "8472792" | "8515265" | "8781122").PN.				
S470	4	("5715403" | "6141754").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/22 13:32
S471	396	("20010046299" | "20020051494" | "20020110193" | "20030001964" | "20030002578" | "20030035488" | "20030035545" | "20030035546" | "20030093799" | "20030152370" | "20030163824" | "20030174844" | "20030185542" | "20030231863" | "20030231867" | "20030233464" | "20030236836" | "20030236907" | "20040081333" | "20040105549" | "20040136698" | "20040255115" | "20050038826" | "20050071280" | "20050193070" | "20050193322" | "20050204289" | "20050207578" | "20050273695" | "20060036549" | "20060052095" | "20060064605" | "20060129909" | "20060245727" | "20070031110" | "20070086528" | "20070140647" | "20070154165" | "20070168541" | "20070168542" | "20070180125" | "20070192810" | "20070192818" | "20070195744" | "20070239839" | "20070292107" | "20080120389" | "20080137736" | "20080256105" | "20080263354" | "20080310454" | "20080310496" | "20090031220" | "20090048852" | "20090055546" | "20090132599" | "20090169181" | "20090201988" | "20090307258" | "20090307267" | "20090313544" | "20100040351" | "20100074324" | "20100095121" | "20110047209" | "20110066673" | "20110080940" | "20110126191" | "20110150100" | "20110153785" | "20110197237" | "20110225315" | "20110239078" | "20110246659" | "20110302319" | "20110314176" | "20120023251" | "20120093214" | "20120170642" | "20120170906" | "20120254455" | "20130046902" | "20130166765" | "20130166906" | "20130311094" | "20140101722" | "20140189065" | "20140201382" | "5361332" | "5404436" | "5502766" | "5509070" | "5754648" | "5805700" | "5892900" | "5999812" | "6031622" | "6155840" | "6175921" | "6195388" | "6282653" | "6289450" | "6449719" | "6466671" | "6510513" | "6658056" | "6807306" | "6810389" | "6859496" | "6956901" | "6965993" | "0604469" | "7007170" | "7043473" | "7151832" | "7151833" | "7165175" | "7185363" | "7242772" | "7328345" | "7349886" | "7356143" | "7376831" |	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/22 13:33

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0072
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

		"7406174" | "7472280" | "7478325" | "7484103" | "7526450" | "7594271" | "7640435" | "7817608" | "7991156" | "8023562" | "8046453" | "8054880" | "8201264" | "8225061" | "8233768" | "8249168" | "8261356" | "8270473" | "8270819" | "8289338" | "8291460" | "8311115" | "8321556" | "8386621" | "8412841" | "8456380" | "8472792" | "8515265" | "8781122").PN.				

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S477	6	713/160.ccls. and ((((access$3 play$4 play$1back playback) with (Common "same" identical$5) with Key) and((access$4 play$3 play$1back playback) with (common "same" identical$5) with key) and ((access$ play$1back playback) with (common "same" identical$5) with key).ab.)).clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/09/22 14:03
S483	1	((((access$3 play$4 play$1back playback) with (Common "same" identical$5) with Key) and((access$4 play$3 play$1back playback) with (common "same" identical$5) with key) and ((access$ play$1back playback) with (common "same" identical$5) with key)))and (bitrate with stream$4).clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/09/22 14:08
S484	1	713/160.ccls. and ((((access$3 play$4 play$1back playback) with (Common "same" identical$5) with Key) and((access$4 play$3 play$1back playback) with (common "same" identical$5) with key) and ((access$ play$1back playback) with (common "same" identical$5) with key)))and (bitrate with stream$4).clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/09/22 14:08

9/22/2014 2:13:48 PM
C:\Users\agetachew\Documents\EAST\Workspaces\13340623.wsp

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0073
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

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

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./		ANONYMOUS, "Method for the encoding of a compressed video sequence derived from the same video sequence compressed at a different bit rate without loss of data", ip.com, ip.com number: IPCOM000008165D, May 22, 2012, pp. 1-9.	
/A.G./		AUTHOR UNKNOWN, "Entropy and Source Coding (Compression)", TCOM 570, 1999-9, pp. 1-22,	
		~~AUTHOR UNKNOWN, "MPEG-4 Video Encoder: Based on International Standard ISO/IEC 14496-2", Patni Computer Systems, Ltd., Publication date unknown, 15 pgs.~~	
/A.G./		AUTHOR UNKNOWN, "Tunneling QuickTime RTSP and RTP over HTTP", Published by Apple Computer, Inc.: 1999 (month unknown), 6 pages. 1999	
/A.G./		BLASIAK, PH.D., DAREK, Video Transrating and Transcoding: Overview of Video Transrating and Transcoding Technologies", Ingenient Technologies, TI Developer Conference, August 6-8, 2002, 22 pgs.	
/A.G./		DEUTSCHER, "IIS Transform Manager Beta - Using the MP4 to Smooth Task", Retrieved from: https://web.archive.org/web/20130328111303/http://blog.johndeutscher.com/category/smooth-streaming, Blog post of April 17, 2010, 14 pgs.	
/A.G./		GANNES, "The Lowdown on Apple's HTTP Adaptive Bitrate Streaming", GigaOM, June 10, 2009, 12 pgs.	
		~~GHOSH, "Enhancing Silverlight Video Experiences with Contextual Data", Retrieved from: http://msdn.microsoft.com/en-us/magazine/ee336025.aspx, 15 pgs.~~	
		~~INLET TECHNOLOGIES, "Adaptive Delivery to iDevices", 2 pages.~~	
		~~INLET TECHNOLOGIES, "Adaptive delivery to iPhone 3.0", 2 pgs.~~	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.G./

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

		~~INLET TECHNOLOGIES, "HTTP versus RTMP", 3 pages.~~	
/A.G./		INLET TECHNOLOGIES, "The World's First Live Smooth Streaming Event: The French Open", 2 pages. 2009	
/A.G./		KIM, KYUHEON, "MPEG-2 ES/PES/TS/PSI", Kyung-Hee University, October 4, 2010, 66 pages.	
		~~KURZKE ET AL., "Get Your Content Onto Google TV", Google, Retrieved from: http://commondatastorage.googleapis.com/io2012/presentations/live%20to%20website/1300.pdf, 58 pgs.~~	
		~~LANG, "Expression Encoder, Best Practices for live smooth streaming broadcasting", Microsoft Corporation, 20 pgs.~~	
		~~LEVKOV, "Mobile Encoding Guidelines for Android Powered Devices", Adobe Systems Inc., Addendum B, source and date unknown, 42 pgs.~~	
		~~MSDN, "Adaptive streaming, Expression Studio 2.0", 2 pgs.~~	
/A.G./		NELSON, "Smooth Streaming Deployment Guide", Microsoft Expression Encoder, August 2010, 66 pgs.	
/A.G./		NELSON, MARK, "Arithmetic Coding + Statistical Modeling = Data Compression: Part 1 - Arithmetic Coding", Doctor Dobb's Journal, February 1991, printed from http://www.dogma.net/markn/articles/arith/part1.htm; printed July 2, 2003, 12 pgs.	
/A.G./		Noé, ALEXANDER, "Matroska File Format (under construction !)", June 24, 2007, XP002617671, Retrieved from: http://web.archive.org/web/20070821155146/www.matroska.org/technical/specs/matroska.pdf, Retrieved on January 19, 2011, 1-51.	
/A.G./		OZER, "The 2012 Encoding and Transcoding Buyers' Guide", Streamingmedia.com, Retrieved from: http://www.streamingmedia.com/Articles/Editorial/Featured-Articles/The-2012-Encoding-and-Transcoding-Buyers-Guide-84210.aspx, 2012, 8 pgs.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.G./

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

/A.G./		PANTOS, "HTTP Live Streaming, draft-pantos-http-live-streaming-10", IETF Tools, October 15, 2012, Retrieved from: http://tools.ietf.org/html/draft-pantos-http-live-streaming-10, 37 pgs.	
		PANTOS, R., "HTTP Live Streaming: draft-pantos-http-live-streaming-06", Published by the Internet Engineering Task Force (IETF), March 31, 2011, 24 pages.	
		PHAMDO, NAM, "Theory of Data Compression", printed from http://www.data-compression.com/theoroy.html on October 10, 2003, 12 pgs.	
		RGB NETWORKS, "Comparing Adaptive HTTP Streaming Technologies", November 2011, Retrieved from: http://btreport.net/wp-content/uploads/2012/02/RGB-Adaptive-HTTP-Streaming-Comparison-1211-01.pdf, 20 pgs.	
		SCHULZRINNE, H et al., "Real Time Streaming Protocol 2.0 (RTSP): draft-ietfmmusic-rfc2326bis-27", MMUSIC Working Group of the Internet Engineering Task Force (IETF), March 9, 2011, 296 pages.	
		SIGLIN, "HTTP Streaming: What You Need to Know", streamingmedia.com, 2010, 16 pages.	
		SIGLIN, "Unifying Global Video Strategies, MP4 File Fragmentation for Broadcast, Mobile and Web Delivery", Nov. 16, 2011, 16 pgs.	
		WU, FENG et al., "Next Generation Mobile Multimedia Communications: Media Codec and Media Transport Perspectives", In China Communications, October 2006, pp. 30-44.	
		ZAMBELLI, ALEX, "IIS Smooth Streaming Technical Overview", Microsoft Corporation, March 2009.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.G./

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/ (09/18/2014)	Date Considered	09/18/2014

*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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.G./

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.
Search has been updated.	05/29/2014	A.G.
Inventourship search has been updated.	05/29/2014	A.G
Search has been updated.	09/08/2014	A.G.
Consulted with Samsom Lemma.	09/08/2014	A.G.

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
713	160	05/29/2014	A.G.
	713/160.ccls. and ((((access$ play$ play$1back playback) with (Common "same" identical$5) with Key) and((access$ play$ play$1back playback) with (common "same" identical$5) with key) and ((access$ play$1back playback) with (common "same" identical$5) with key).ab.)).clm.	05/29/2014	A.G.

/ABIY GETACHEW/ Examiner.Art Unit 2434	

INTERFERENCE SEARCH			
US Class/ CPC Symbol	**US Subclass / CPC Group**	**Date**	**Examiner**
	processor and (memory with client with application) and ((((access$ play$ play$1back playback) with (Common "same" identical$5) with Key) and((access$ play$ play$1back playback) with (common "same" identical$5) with key) and ((access$ play$1back playback) with (common "same" identical$5) with key).ab.)).clm.	05/29/2014	A.G.

/ABIY GETACHEW/ Examiner.Art Unit 2434	

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

CPC						
Symbol					**Type**	**Version**
H04L		9	/	0819	F	2013-01-01
H04L		2209	/	603	A	2013-01-01
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			

CPC Combination Sets							
Symbol					**Type**	**Set**	**Ranking**	**Version**
			/					
			/					

/ABIY GETACHEW/ Examiner.Art Unit 2434	09/18/2014	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	31	
/TESHOME HAILU/ Primary Examiner.Art Unit 2434	09/26/2014	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	12a

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

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION										
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED					
713	160	H	0	4	L	29 / 06 (2006.01)						

CROSS REFERENCE(S)					
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				

/ABIY GETACHEW/ Examiner.Art Unit 2434	09/18/2014	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	31	
/TESHOME HAILU/ Primary Examiner.Art Unit 2434	09/26/2014	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	12a

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0081
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

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

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

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	13	17	23	33										
2	2	15	18	24	34										
	3	16	19	25	35										
3	4		20	26	36										
4	5	17	21	30	37										
5	6	27	22	31	38										
	7	28	23		39										
6	8		24												
7	9	29	25												
8	10	18	26												
	11	19	27												
9	12	20	28												
10	13	21	29												
11	14		30												
12	15		31												
14	16	22	32												

/ABIY GETACHEW/ Examiner.Art Unit 2434	09/18/2014	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	31	
/TESHOME HAILU/ Primary Examiner.Art Unit 2434	09/26/2014	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	12a

U.S. Patent and Trademark Office

Part of Paper No. 20140911

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	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
/A.G./		5361332	A	1994-11-01	Yoshida, Masayuki et al.	
		5404436	A	1995-04-04	Hamilton, Robert H.	
		5502766	A	1996-03-26	Boebert, William et al.	
		5509070	A	1996-04-16	Schull, Jonathan	
		5754648	A	1998- 05-19	Ryan, John et al	
		5805700	A	1998-09-08	Nardone, Joseph et al.	
		5892900	A	1999-04-06	Ginter, Karl et al.	
		5999812	A	1999-12-07	Himsworth, Winston E.	
		6031622	A	2000-02-29	Ristow, Allan et al.	
		6044469	A	2000-03-28	Horstmann, Cay S.	
		6155840	A	2000-12-05	Sallette, Alfred V.	
		6175921	B1	2001-01-16	Rosen, Sholom	
		6195388	B1	2001-02-27	Choi, Jae G., et al.	
		6282653	B1	2001-08-28	Berstis, Viktors et al.	
		6289450	B1	2001-09-11	Pensak, David A., et al.	
		6449719	B1	2002-09-10	Baker, Brian	
		6466671	B1	2002-10-15	Maillard, Michel et al.	
		6510513	B1	2003-01-21	Danieli, Damon V.	
		6658056	B1	2003-12-02	Duruöz, Cem I., et al.	
		6807306	B1	2004-10-19	Girgensohn, Andreas et al.	
		6810389	B1	2004-10-26	Meyer, Marc A.	
		6859496	B1	2005-02-22	Boroczky, Lilla et al.	
		6956901	B2	2005-10-18	Boroczky, Lilla et al.	
		6965993	B2	2005-11-15	Baker, Brian	
		7007170	B2	2006-02-28	Morten, Glenn	
		7043473	B1	2006- 05-09	Rassool, Reza et al.	
		7150045	B2	2006-12-12	Koelle, Katharina et al.	
		7151832	B1	2006-12-19	Fetkovich, John et al.	
		7151833	B2	2006-12-19	Candelore, Brant et al.	
		7165175	B1	2007-01-16	Kollmyer, Brad et al.	
		7185363	B1	2007-02-27	Narin, Attila et al.	
		7242772	B1	2007-07-10	Tehranchi, Babak	
		7328345	B2	2008-02-05	Morten, Glenn et al	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.G./

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	02359A

/A.G./		7349886	B2	2008-03-25	Morten, Glenn et al.	
		7356143	B2	2008-04-08	Morten, Glenn	
		7376831	B2	2008- 05-20	Kollmyer, Brad et al.	
		7406174	B2	2008-07-29	Palmer, Tomas	
		7472280	B2	2008-12-30	Giobbi, John J.	
		7478325	B2	2009-01-13	Foehr, Oliver H.	
		7484103	B2	2009-01-27	Woo, Je-Hak et al.	
		7526450	B2	2009-04-28	Hughes, David A., et al.	
		7594271	B2	2009-09-22	Zhuk, Oscar et al.	
		7640435	B2	2009-12-29	Morten, Glenn	
		7817608	B2	2010-10-19	Rassool, Reza et al.	
		7991156	B1	2011-08-02	Miller, Eric	
		8023562	B2	2011-09-20	Zheludkov, Alexander et al.	
		8046453	B2	2011-10-25	Olaiya, Oladipupo	
		8054880	B2	2011-11-08	Yu, Guoyao et al.	
		8201264	B2	2012-06-12	Grab, Eric et al.	
		8225061	B2	2012-07-17	Greenebaum, Kenneth	
		8233768	B2	2012-07-31	Soroushian, K et al.	
		8249168	B2	2012-08-21	Graves, Hans W.	
		8261356	B2	2012-09-04	Choi, Bum S., et al.	
		8270473	B2	2012-09-18	Chen, William et al.	
		8270819	B2	2012-09-18	Vannier, Eric	
		8289338	B2	2012-10-16	Priyadarshi, Shaiwal et al.	
		8291460	B1	2012-10-16	Peacock, Gavin	
		8311115	B2	2012-11-13	Gu, Chuang et al.	
		8321556	B1	2012-11-27	Chatterjee, Manjirnath et al.	
		8386621	B2	2013-02-26	Park, Anthony N.	
		8412841	B1	2013-04-02	Swaminathan, Viswanathan et al.	
		8456380	B2	2013-06-04	Pagan, William G.	
		8472792	B2	2013-06-25	Butt, Abou U.	
		8515265	B2	2013-08-20	Kwon, O-hoon et al.	
		8781122		2014-07-15	Chan, Francis Y., et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.G./

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	02359A

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./		20010046299	A1	2001-11-29	Wasilewski, Anthony J., et al.	
		20020051494	A1	2002- 05-02	Yamaguchi, Noboru et al.	
		20020110193	A1	2002-08-15	Yoo, Kook Yeol et al.	
		20030002578	A1	2003-01-02	Tsukagoshi, Ikuo et al.	
		20030001964	A1	2003-01-02	Masukura et al.	
		20030035545	A1	2003-02-20	Jiang, S.	
		20030035546	A1	2003-02-20	Jiang, S. S., et al.	
		20030035488	A1	2003-02-20	Barrau	
		20030093799	A1	2003- 05-15	Kauffman et al.	
		20030152370	A1	2003-08-14	Otomo, Hitoshi et al.	
		20030163824	A1	2003-08-28	Gordon, Donald F., et al.	
		20030174844	A1	2003-09-18	Candelore, Brant L.	
		20030185542	A1	2003-10-02	McVeigh et al.	
		20030231863	A1	2003-12-18	Eerenberg, O. et al.	
		20030231867	A1	2003-12-18	Gates, M. et al.	
		20030233464	A1	2003-12-18	Walpole, Jonathan et al.	
		20030236836	A1	2003-12-25	Borthwick, Ernest M.	
		20030236907	A1	2003-12-25	Stewart, James C., et al.	
		20040081333	A1	2004-04-29	Grab, E. W., et al.	
		20040105549	A1	2004-06-03	Suzuki, K et al.	
		20040136698	A1	2004-07-15	Mock, Wayne E.	
		20040139335	A1	2004-07-15	Diamand, Joseph et al.	
		20040158878	A1	2004-08-12	Ratnakar, Viresh et al.	
		20040255115	A1	2004-12-16	DeMello, Marco A., et al.	
		20050038826	A1	2005-02-17	Bae, Dae-gyu et al.	
		20050071280	A1	2005-03-31	Irwin, Scott A.	
		20050114896	A1	2005- 05-26	Hug, Joshua D.	
		20050193322	A1	2005-09-01	Lamkin, Allan B., et al.	
		20050193070	A1	2005-09-01	Brown, Michael W., et al.	
		20050204289	A1	2005-09-15	Mohammed, Sohail B., et al.	
		20050207578	A1	2005-09-22	Matsuyama, Shinako et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.G./

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	02359A

/A.G./		20050207442	A1	2005-09-22	Zoest et al.	
		20050273695	A1	2005-12-08	Schnurr, Jeffrey R.	
		20050275656	A1	2005-12-15	Corbin, Toby et al.	
		20060036549	A1	2006-02-16	Wu, Bo	
		20060052095	A1	2006-03-09	Vazvan, Behruz	
		20060053080	A1	2006-03-09	Edmonson et al.	
		20060064605	A1	2006-03-23	Giobbi, John J.	
		20060078301	A1	2006-04-13	Ikeda, Wataru et al.	
		20060129909	A1	2006-06-15	BUTT, ABOU U., et al.	
		20060173887	A1	2006-08-03	Breitfeld, Volkmar et al.	
		20060245727	A1	2006-11-02	Nakano, Hiroshi et al.	
		20060259588	A1	2006-11-16	Lerman, David R., et al.	
		20060263056	A1	2006-11-23	Lin, Shu et al.	
		20070031110	A1	2007-02-08	Rijckaert, Albert M.	
		20070047901	A1	2007-03-01	Ando, Hideo et al.	
		20070083617	A1	2007-04-12	Chakrabarti, A et al.	
		20070086528	A1	2007-04-19	Mauchly, J. W., et al.	
		20070136817	A1	2007-06-14	Nguyen, Binh	
		20070140647	A1	2007-06-21	Kusunoki, Yoshiaki et al.	
		20070154165	A1	2007-07-05	Hemmeryckx-Deleersnijder, Bert K., et al.	
		20070168541	A1	2007-07-19	Gupta, Manish et al.	
		20070168542	A1	2007-07-19	Gupta, Manish et al.	
		20070180125	A1	2007-08-02	Knowles, Michael et al.	
		20070192810	A1	2007-08-16	Pritchett, Thaddeus C., et al.	
		20070239839	A1	2007-10-11	Buday, Michael E., et al.	
		20070255940	A1	2007-11-01	Ueno, T.	
		20070292107	A1	2007-12-20	Yahata, Hiroshi et al.	
		20080120389	A1	2008- 05-22	Bassali, Harpal S., et al.	
		20080126248	A1	2008- 05-29	Lee, Seung-Jae et al.	
		20080137736	A1	2008-06-12	Richardson, John W., et al.	
		20080192818	A1	2008-08-14	DiPietro, Donald V., et al.	
		20080195744	A1	2008-08-14	Bowra, Todd et al.	
		20080256105	A1	2008-10-16	Nogawa, Hiroshi et al.	
		20080263354	A1	2008-10-23	Beuque, Jean-Bernard G.	
		20080279535	A1	2008-11-13	Haque, Shaheedur R., et al.	
		20080310454	A1	2008-12-18	Bellwood, Thomas A., et al.	
		20080310496	A1	2008-12-18	Fang, Nicholas J.	
		20090031220	A1	2009-01-29	Tranchant, Julien et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.G./

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	02359A

/A.G./		20090048852	A1	2009-02-19	Burns, Gregory et al.	
		20090055546	A1	2009-02-26	Jung, Edward K., et al.	
		20090060452	A1	2009-03-05	Chaudhri, Imran A.	
		20090066839	A1	2009-03-12	Jung, Kil-Soo et al.	
		20090097644	A1	2009-04-16	Harukl, K.	
		20090132599	A1	2009- 05-21	Soroushian, K. et al.	
		20090132824	A1	2009- 05-21	Terada, Masayuki et al.	
		20090150557	A1	2009-06-11	Wormley, Nicholas et al.	
		20090169181	A1	2009-07-02	Priyadarshi, S. et al.	
		20090201988	A1	2009-08-13	Gazier, Michael et al.	
		20090226148	A1	2009-09-10	Nesvadba, Jan A., et al.	
		20090293116	A1	2009-11-26	DeMello, Marco A.	
		20090303241	A1	2009-12-10	Priyadarshi, S et al.	
		20090307258	A1	2009-12-10	Priyadarshi, S et al.	
		20090307267	A1	2009-12-10	Chen, Danny Y., et al.	
		20090313544	A1	2009-12-17	Wood, Policarpo et al.	
		20090313564	A1	2009-12-17	Rottler, Benjamin A., et al.	
		20090328124	A1	2009-12-31	Khouzam, Gilles et al.	
		20100040351	A1	2010-02-18	Toma, Tadamasa et al.	
		20100074324	A1	2010-03-25	Qian, Zhebin et al.	
		20100083322	A1	2010-04-01	Rouse, Alan	
		20100095121	A1	2010-04-15	Shetty, Pritham et al.	
		20100111192	A1	2010- 05-06	Graves, Hans W.	
		20100158109	A1	2010-06-24	Dahlby, Joshua et al.	
		20100186092	A1	2010-07-22	Takechi, Hideaki et al.	
		20100189183	A1	2010-07-29	Gu, Chuang et al.	
		20100228795	A1	2010-09-09	Hahn, Judah G.	
		20100235472	A1	2010-09-16	Sood, Vishal et al.	
		20110047209	A1	2011-02-24	Lindholm, Fredrik et al.	
		20110066673	A1	2011-03-17	Outlaw, B	
		20110080940	A1	2011-04-07	Bocharov, John A.	
		20110082924	A1	2011-04-07	Gopalakrishnan, Kumar	
		20110126191	A1	2011- 05-26	Hughes, Richard et al.	
		20110142415	A1	2011-06-16	Rhyu, Sung-Ryeul	
		20110145726	A1	2011-06-16	Wei, Eugene C., et al.	
		20110149753	A1	2011-06-23	Bapst, Mark et al.	
		20110150100	A1	2011-06-23	Abadir, Essam E.	
		20110153785	A1	2011-06-23	Minborg, Per-Åke et al.	
		20110197237	A1	2011-08-11	Turner, Steven E.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.G./

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	02359A

/A.G./		20110225315	A1	2011-09-15	Wexler, Yosef et al.	
		20110225417	A1	2011-09-15	Maharajh, Kavi et al.	
		20110239078	A1	2011-09-29	Luby, Michael G., et al.	
		20110246657	A1	2011-10-06	Glow, Andy	
		20110246659	A1	2011-10-06	Bouazizi, Imed	
		20110268178	A1	2011-11-03	Park, Anthony N.	
		20110302319	A1	2011-12-08	Ha, Ho-jin et al.	
		20110305273	A1	2011-12-15	He, Yaming et al.	
		20110314176	A1	2011-12-22	Frojdh, Per et al.	
		20120023251	A1	2012-01-26	Pyle, Harry et al.	
		20120093214	A1	2012-04-19	URBACH, Julian M.	
		20120170642	A1	2012-07-05	Braness, J et al.	
		20120170643	A1	2012-07-05	Soroushian, K et al.	
		20120170906	A1	2012-07-05	Soroushian, K et al.	
		20120170915	A1	2012-07-05	Braness, J et al.	
		20120173751	A1	2012-07-05	Braness, J et al.	
		20120179834	A1	2012-07-12	Van Der, S A., et al.	
		20120254455	A1	2012-10-04	Adimatyam, Venkata S., et al.	
		20120278496	A1	2012-11-01	Hsu, James K.	
		20120307883	A1	2012-12-06	Graves, Hans W.	
		20120311094	A1	2012-12-06	Biderman, David et al.	
		20130019107		2013-01-17	Grab, E et al.	
		20130044821	A1	2013-02-21	Braness, Jason et al.	
		20130046902	A1	2013-02-21	Villegas Nuñez, Alvaro et al.	
		20130166765	A1	2013-06-27	Kaufman, Matthew	
		20130166906	A1	2013-06-27	Swaminathan, Viswanathan et al.	
		20140101722	A1	2014-04-10	Moore, Jonathan	
		20140189065	A1	2014-07-03	Schaar, Auke V., et al.	
		20140201382	A1	2014-07-17	Shivadas, Abhishek et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.G./

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	02359A

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./		813167	EP	A2	1997-12-17	Ristow, Allan W., et al.		
		936812	EP	A1	1999-08-18	Maillard, Michael et al.		
		0165762	WO	A2	2001-09-07	Platt, David et al.		
		02/37210	WO	A2	2002- 05-10	Lightning Source, Inc.		
		02/054196	WO	A2	2002-07-11	Thomson Licensing S.A.		
		2004102571	WO	A1	2004-11-25	Rijckaert, Albert		
		2005080204	JP	A	2005-03-24	Watanabe, Junya		
		2006524007	JP	A	2006-10-19	モーテン，グレン・エイ et al.		
		2008010275	WO	A1	2008-01-24	Hatano, Kouji et al.		
		2009065137	WO	A1	2009- 05-22	Soroushian, K. et al.		
		2010060106	WO	A1	2010- 05-27	Kohli, J et al.		
		2010122447	WO	A1	2010-10-28	Foo, Teck et al.		
		2011068668	WO	A1	2011-06-09	Chan, F et al.		
		2012094181	WO	A2	2012-07-12	Soroushian, K et al.		
		2012/094189	WO	A1	2012-07-12	Braness, J et al.		
		2012094171	WO	A1	2012-07-12	Braness, Jason et al.		

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.G./

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	02359A

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./		"Information Technology-Coding of Audio Visual Objects- Part 2: Visual" International Standard, ISO/IEC 14496-2, Third Edition, Jun. 1, 2004, pp. 1-724.	
		Cloakware Corporation, "Protecting Digital Content Using Cloakware Code Transformation Technology", Version 1.2, May 2002, pgs 1-10.	
		European Search Report for Application 11855103.5, search completed June 26, 2014, 9 pgs.	
		European Search Report for Application 11855237.1, search completed June 25, 2014, 9 pgs.	
		Federal Computer Week, "Tool Speeds Info to Vehicles", July 25, 1999, 5 pages.	
		HTTP Live Streaming Overview, Networking & Internet, Apple, Inc., April 1, 2011, 38 pages.	
		International Preliminary Report on Patentability for International Application No. PCT/US2011/068276, International Filing Date December 31, 2011, Issue Date March 4, 2014, 23 pgs.	
		International Search Report and Written Opinion for International Application No. PCT/US2010/56733, International Filing Date November 15, 2010, Search Completed January 3, 2011, Mailed January 14, 2011, 9 pgs.	
		International Search Report and Written Opinion for International Application PCT/US2011/066927, International Filing Date December 22, 2011, Report Completed April 3, 2012, Mailed April 20, 2012, 14 pgs.	
		International Search Report and Written Opinion for International Application PCT/US2011/067167, International Filing Date December 23, 2011, Report Completed June 19, 2012, Mailed July 2, 2012, 11 pgs.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.G./

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	02359A

/A.G./		International Search Report for International Application No. PCT/US2005/025845 filed July 21, 2005, report completed February 5, 2007 and mailed May 10, 2007, 3 pgs.	
/A.G./		International Search Report for International Application No. PCT/US2007/063950 filed March 14, 2007, report completed February 19, 2008; report mailed March 19, 2008, 3 pgs.	
/A.G./		ITS International, "Fleet System Opts for Mobile Server", August 26, 1999, 1 page.	
/A.G./		Microsoft, Microsoft Media Platform: Player Framework, "Silverlight Media Framework v1.1", 2 pages. Jan. 7, 2010	
		~~Microsoft, Microsoft Media Platform: Player Framework, "Microsoft Media Platform: Player Framework v2.5 (formerly Silverlight Media Framework)", 2 pages.~~	
		~~The Official Microsoft IIS Site, Smooth Streaming Client, 4 pages.~~	
/A.G./		Written Opinion for International Application No. PT/US2005/025845 filed July 21, 2005, report completed February 5, 2007 and mailed May 10, 2007, 5 pgs.	
/A.G./		Written Opinion for International Application No. PCT/US2007/063950 filed March 14, 2007, report completed March 1, 2008; report mailed March 19, 2008, 5 pgs.	
/A.G./		"Adaptive Streaming Comparison", January 28, 2010, 5 pgs.	
/A.G./		"Best Practices for Multi-Device Transcoding", Kaltura Open Source Video, 13 pgs. 11/27/2013	
/A.G./		"Informationweek: Front End: Daily Dose, Internet on Wheels", July 20. 1999, 3 pgs.	
		~~"Netflix turns on subtitles for PC, Mac streaming", 3 pgs.~~	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.G./

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	02359A

/A.G./		Supplementary European Search Report for Application No. EP 10834935, International Filing Date November 15, 2010, Search Completed May 27, 2014, 9 pgs.	
/A.G./		"Supported Media Formats", Supported Media Formats, Android Developers, November 27, 2013, 3 pgs.	
		~~"Thread: SSME (Smooth Streaming Medial Element) config.xml review (Smooth Streaming Client configuration file)", 3 pgs.~~	
/A.G./		"Transcoding Best Practices", From movideo, November 27, 2013, 5 pgs.	
		~~"Using HTTP Live Streaming", iOS Developer Library, Retrieved from: http://developer.apple.com/library/ios/#documentation/networkinginternet/conceptual/streamingmediaguide/UsingHTTPLiveStreaming/UsingHTTPLiveStreaming.html#//apple_ref/doc/uid/TP40008332-CH102-SW1, 10 pgs.~~	
/A.G./		AKHSHABI ET AL., "An Experimental Evaluation of Rate-Adaptation Algorithms in Adaptive Streaming over HTTP", MMSys'11, February 24-25, 2011, 12 pgs.	

EXAMINER SIGNATURE

Examiner Signature	/Abiy Getachew/ (09/18/2014)	Date Considered	09/18/2014

*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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.G./

PTO/SB/30EFS (07-09)
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.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	13/340,623	Filing Date	2011-12-29	Docket Number (if applicable)	D1-02359A	Art Unit	2434
First Named Inventor	Michael George Kiefer			Examiner Name	Abiy Getachew		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

- ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
- ☐ Other _____

☒ Enclosed

- ☐ Amendment/Reply
- ☒ Information Disclosure Statement (IDS)
- ☐ Affidavit(s)/ Declaration(s)
- ☐ Other _____

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____
(Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

☒ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 504407

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature

☐ Applicant Signature

PTO/SB/30EFS (07-09)
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.

Signature of Registered U.S. Patent Practitioner			
Signature	/Jason D. Wolfe/	Date (YYYY-MM-DD)	2014-09-08
Name	Jason D. Wolfe	Registration Number	71327

This collection of information is required by 37 CFR 1.114. 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 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.

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

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 8, 2014 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 8, 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 "Foreign Patent Documents" and "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.

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/kl

Enclosure(s)

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0096
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

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	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
		5361332	A	1994-11-01	Yoshida, Masayuki et al.	
		5404436	A	1995-04-04	Hamilton, Robert H.	
		5502766	A	1996-03-26	Boebert, William et al.	
		5509070	A	1996-04-16	Schull, Jonathan	
		5754648	A	1998- 05-19	Ryan, John et al	
		5805700	A	1998-09-08	Nardone, Joseph et al.	
		5892900	A	1999-04-06	Ginter, Karl et al.	
		5999812	A	1999-12-07	Himsworth, Winston E.	
		6031622	A	2000-02-29	Ristow, Allan et al.	
		6044469	A	2000-03-28	Horstmann, Cay S.	
		6155840	A	2000-12-05	Sallette, Alfred V.	
		6175921	B1	2001-01-16	Rosen, Sholom	
		6195388	B1	2001-02-27	Choi, Jae G., et al.	
		6282653	B1	2001-08-28	Berstis, Viktors et al.	
		6289450	B1	2001-09-11	Pensak, David A., et al.	
		6449719	B1	2002-09-10	Baker, Brian	
		6466671	B1	2002-10-15	Maillard, Michel et al.	
		6510513	B1	2003-01-21	Danieli, Damon V.	
		6658056	B1	2003-12-02	Duruöz, Cem I., et al.	
		6807306	B1	2004-10-19	Girgensohn, Andreas et al.	
		6810389	B1	2004-10-26	Meyer, Marc A.	
		6859496	B1	2005-02-22	Boroczky, Lilla et al.	
		6956901	B2	2005-10-18	Boroczky, Lilla et al.	
		6965993	B2	2005-11-15	Baker, Brian	
		7007170	B2	2006-02-28	Morten, Glenn	
		7043473	B1	2006- 05-09	Rassool, Reza et al.	
		7150045	B2	2006-12-12	Koelle, Katharina et al.	
		7151832	B1	2006-12-19	Fetkovich, John et al.	
		7151833	B2	2006-12-19	Candelore, Brant et al.	
		7165175	B1	2007-01-16	Kollmyer, Brad et al.	
		7185363	B1	2007-02-27	Narin, Attila et al.	
		7242772	B1	2007-07-10	Tehranchi, Babak	
		7328345	B2	2008-02-05	Morten, Glenn et al	

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	02359A

		7349886	B2	2008-03-25	Morten, Glenn et al.	
		7356143	B2	2008-04-08	Morten, Glenn	
		7376831	B2	2008- 05-20	Kollmyer, Brad et al.	
		7406174	B2	2008-07-29	Palmer, Tomas	
		7472280	B2	2008-12-30	Giobbi, John J.	
		7478325	B2	2009-01-13	Foehr, Oliver H.	
		7484103	B2	2009-01-27	Woo, Je-Hak et al.	
		7526450	B2	2009-04-28	Hughes, David A., et al.	
		7594271	B2	2009-09-22	Zhuk, Oscar et al.	
		7640435	B2	2009-12-29	Morten, Glenn	
		7817608	B2	2010-10-19	Rassool, Reza et al.	
		7991156	B1	2011-08-02	Miller, Eric	
		8023562	B2	2011-09-20	Zheludkov, Alexander et al.	
		8046453	B2	2011-10-25	Olaiya, Oladipupo	
		8054880	B2	2011-11-08	Yu, Guoyao et al.	
		8201264	B2	2012-06-12	Grab, Eric et al.	
		8225061	B2	2012-07-17	Greenebaum, Kenneth	
		8233768	B2	2012-07-31	Soroushian, K et al.	
		8249168	B2	2012-08-21	Graves, Hans W.	
		8261356	B2	2012-09-04	Choi, Bum S., et al.	
		8270473	B2	2012-09-18	Chen, William et al.	
		8270819	B2	2012-09-18	Vannier, Eric	
		8289338	B2	2012-10-16	Priyadarshi, Shaiwal et al.	
		8291460	B1	2012-10-16	Peacock, Gavin	
		8311115	B2	2012-11-13	Gu, Chuang et al.	
		8321556	B1	2012-11-27	Chatterjee, Manjirnath et al.	
		8386621	B2	2013-02-26	Park, Anthony N.	
		8412841	B1	2013-04-02	Swaminathan, Viswanathan et al.	
		8456380	B2	2013-06-04	Pagan, William G.	
		8472792	B2	2013-06-25	Butt, Abou U.	
		8515265	B2	2013-08-20	Kwon, O-hoon et al.	
		8781122		2014-07-15	Chan, Francis Y., et al.	

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	02359A

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
		20010046299	A1	2001-11-29	Wasilewski, Anthony J., et al.	
		20020051494	A1	2002- 05-02	Yamaguchi, Noboru et al.	
		20020110193	A1	2002-08-15	Yoo, Kook Yeol et al.	
		20030002578	A1	2003-01-02	Tsukagoshi, Ikuo et al.	
		20030001964	A1	2003-01-02	Masukura et al.	
		20030035545	A1	2003-02-20	Jiang, S.	
		20030035546	A1	2003-02-20	Jiang, S. S., et al.	
		20030035488	A1	2003-02-20	Barrau	
		20030093799	A1	2003- 05-15	Kauffman et al.	
		20030152370	A1	2003-08-14	Otomo, Hitoshi et al.	
		20030163824	A1	2003-08-28	Gordon, Donald F., et al.	
		20030174844	A1	2003-09-18	Candelore, Brant L.	
		20030185542	A1	2003-10-02	McVeigh et al.	
		20030231863	A1	2003-12-18	Eerenberg, O. et al.	
		20030231867	A1	2003-12-18	Gates, M. et al.	
		20030233464	A1	2003-12-18	Walpole, Jonathan et al.	
		20030236836	A1	2003-12-25	Borthwick, Ernest M.	
		20030236907	A1	2003-12-25	Stewart, James C., et al.	
		20040081333	A1	2004-04-29	Grab, E. W., et al.	
		20040105549	A1	2004-06-03	Suzuki, K et al.	
		20040136698	A1	2004-07-15	Mock, Wayne E.	
		20040139335	A1	2004-07-15	Diamand, Joseph et al.	
		20040158878	A1	2004-08-12	Ratnakar, Viresh et al.	
		20040255115	A1	2004-12-16	DeMello, Marco A., et al.	
		20050038826	A1	2005-02-17	Bae, Dae-gyu et al.	
		20050071280	A1	2005-03-31	Irwin, Scott A.	
		20050114896	A1	2005- 05-26	Hug, Joshua D.	
		20050193322	A1	2005-09-01	Lamkin, Allan B., et al.	
		20050193070	A1	2005-09-01	Brown, Michael W., et al.	
		20050204289	A1	2005-09-15	Mohammed, Sohail B., et al.	
		20050207578	A1	2005-09-22	Matsuyama, Shinako et al.	

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	02359A

		20050207442	A1	2005-09-22	Zoest et al.	
		20050273695	A1	2005-12-08	Schnurr, Jeffrey R.	
		20050275656	A1	2005-12-15	Corbin, Toby et al.	
		20060036549	A1	2006-02-16	Wu, Bo	
		20060052095	A1	2006-03-09	Vazvan, Behruz	
		20060053080	A1	2006-03-09	Edmonson et al.	
		20060064605	A1	2006-03-23	Giobbi, John J.	
		20060078301	A1	2006-04-13	Ikeda, Wataru et al.	
		20060129909	A1	2006-06-15	BUTT, ABOU U., et al.	
		20060173887	A1	2006-08-03	Breitfeld, Volkmar et al.	
		20060245727	A1	2006-11-02	Nakano, Hiroshi et al.	
		20060259588	A1	2006-11-16	Lerman, David R., et al.	
		20060263056	A1	2006-11-23	Lin, Shu et al.	
		20070031110	A1	2007-02-08	Rijckaert, Albert M.	
		20070047901	A1	2007-03-01	Ando, Hideo et al.	
		20070083617	A1	2007-04-12	Chakrabarti, A et al.	
		20070086528	A1	2007-04-19	Mauchly, J. W., et al.	
		20070136817	A1	2007-06-14	Nguyen, Binh	
		20070140647	A1	2007-06-21	Kusunoki, Yoshiaki et al.	
		20070154165	A1	2007-07-05	Hemmeryckx-Deleersnijder, Bert K., et al.	
		20070168541	A1	2007-07-19	Gupta, Manish et al.	
		20070168542	A1	2007-07-19	Gupta, Manish et al.	
		20070180125	A1	2007-08-02	Knowles, Michael et al.	
		20070192810	A1	2007-08-16	Pritchett, Thaddeus C., et al.	
		20070239839	A1	2007-10-11	Buday, Michael E., et al.	
		20070255940	A1	2007-11-01	Ueno, T.	
		20070292107	A1	2007-12-20	Yahata, Hiroshi et al.	
		20080120389	A1	2008- 05-22	Bassali, Harpal S., et al.	
		20080126248	A1	2008- 05-29	Lee, Seung-Jae et al.	
		20080137736	A1	2008-06-12	Richardson, John W., et al.	
		20080192818	A1	2008-08-14	DiPietro, Donald V., et al.	
		20080195744	A1	2008-08-14	Bowra, Todd et al.	
		20080256105	A1	2008-10-16	Nogawa, Hiroshi et al.	
		20080263354	A1	2008-10-23	Beuque, Jean-Bernard G.	
		20080279535	A1	2008-11-13	Haque, Shaheedur R., et al.	
		20080310454	A1	2008-12-18	Bellwood, Thomas A., et al.	
		20080310496	A1	2008-12-18	Fang, Nicholas J.	
		20090031220	A1	2009-01-29	Tranchant, Julien et al.	

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	02359A

		20090048852	A1	2009-02-19	Burns, Gregory et al.	
		20090055546	A1	2009-02-26	Jung, Edward K., et al.	
		20090060452	A1	2009-03-05	Chaudhri, Imran A.	
		20090066839	A1	2009-03-12	Jung, Kil-Soo et al.	
		20090097644	A1	2009-04-16	Harukl, K.	
		20090132599	A1	2009- 05-21	Soroushian, K. et al.	
		20090132824	A1	2009- 05-21	Terada, Masayuki et al.	
		20090150557	A1	2009-06-11	Wormley, Nicholas et al.	
		20090169181	A1	2009-07-02	Priyadarshi, S. et al.	
		20090201988	A1	2009-08-13	Gazier, Michael et al.	
		20090226148	A1	2009-09-10	Nesvadba, Jan A., et al.	
		20090293116	A1	2009-11-26	DeMello, Marco A.	
		20090303241	A1	2009-12-10	Priyadarshi, S et al.	
		20090307258	A1	2009-12-10	Priyadarshi, S et al.	
		20090307267	A1	2009-12-10	Chen, Danny Y., et al.	
		20090313544	A1	2009-12-17	Wood, Policarpo et al.	
		20090313564	A1	2009-12-17	Rottler, Benjamin A., et al.	
		20090328124	A1	2009-12-31	Khouzam, Gilles et al.	
		20100040351	A1	2010-02-18	Toma, Tadamasa et al.	
		20100074324	A1	2010-03-25	Qian, Zhebin et al.	
		20100083322	A1	2010-04-01	Rouse, Alan	
		20100095121	A1	2010-04-15	Shetty, Pritham et al.	
		20100111192	A1	2010- 05-06	Graves, Hans W.	
		20100158109	A1	2010-06-24	Dahlby, Joshua et al.	
		20100186092	A1	2010-07-22	Takechi, Hideaki et al.	
		20100189183	A1	2010-07-29	Gu, Chuang et al.	
		20100228795	A1	2010-09-09	Hahn, Judah G.	
		20100235472	A1	2010-09-16	Sood, Vishal et al.	
		20110047209	A1	2011-02-24	Lindholm, Fredrik et al.	
		20110066673	A1	2011-03-17	Outlaw, B	
		20110080940	A1	2011-04-07	Bocharov, John A.	
		20110082924	A1	2011-04-07	Gopalakrishnan, Kumar	
		20110126191	A1	2011- 05-26	Hughes, Richard et al.	
		20110142415	A1	2011-06-16	Rhyu, Sung-Ryeul	
		20110145726	A1	2011-06-16	Wei, Eugene C., et al.	
		20110149753	A1	2011-06-23	Bapst, Mark et al.	
		20110150100	A1	2011-06-23	Abadir, Essam E.	
		20110153785	A1	2011-06-23	Minborg, Per-Åke et al.	
		20110197237	A1	2011-08-11	Turner, Steven E.	

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	02359A

		20110225315	A1	2011-09-15	Wexler, Yosef et al.	
		20110225417	A1	2011-09-15	Maharajh, Kavi et al.	
		20110239078	A1	2011-09-29	Luby, Michael G., et al.	
		20110246657	A1	2011-10-06	Glow, Andy	
		20110246659	A1	2011-10-06	Bouazizi, Imed	
		20110268178	A1	2011-11-03	Park, Anthony N.	
		20110302319	A1	2011-12-08	Ha, Ho-jin et al.	
		20110305273	A1	2011-12-15	He, Yaming et al.	
		20110314176	A1	2011-12-22	Frojdh, Per et al.	
		20120023251	A1	2012-01-26	Pyle, Harry et al.	
		20120093214	A1	2012-04-19	URBACH, Julian M.	
		20120170642	A1	2012-07-05	Braness, J et al.	
		20120170643	A1	2012-07-05	Soroushian, K et al.	
		20120170906	A1	2012-07-05	Soroushian, K et al.	
		20120170915	A1	2012-07-05	Braness, J et al.	
		20120173751	A1	2012-07-05	Braness, J et al.	
		20120179834	A1	2012-07-12	Van Der, S A., et al.	
		20120254455	A1	2012-10-04	Adimatyam, Venkata S., et al.	
		20120278496	A1	2012-11-01	Hsu, James K.	
		20120307883	A1	2012-12-06	Graves, Hans W.	
		20120311094	A1	2012-12-06	Biderman, David et al.	
		20130019107		2013-01-17	Grab, E et al.	
		20130044821	A1	2013-02-21	Braness, Jason et al.	
		20130046902	A1	2013-02-21	Villegas Nuñez, Alvaro et al.	
		20130166765	A1	2013-06-27	Kaufman, Matthew	
		20130166906	A1	2013-06-27	Swaminathan, Viswanathan et al.	
		20140101722	A1	2014-04-10	Moore, Jonathan	
		20140189065	A1	2014-07-03	Schaar, Auke V., et al.	
		20140201382	A1	2014-07-17	Shivadas, Abhishek et al.	

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	02359A

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]
		813167	EP	A2	1997-12-17	Ristow, Allan W., et al.		
		936812	EP	A1	1999-08-18	Maillard, Michael et al.		
		0165762	WO	A2	2001-09-07	Platt, David et al.		
		02/37210	WO	A2	2002- 05-10	Lightning Source, Inc.		
		02/054196	WO	A2	2002-07-11	Thomson Licensing S.A.		
		2004102571	WO	A1	2004-11-25	Rijckaert, Albert		
		2005080204	JP	A	2005-03-24	Watanabe, Junya		
		2006524007	JP	A	2006-10-19	モーテン，グレン・エイ et al.		
		2008010275	WO	A1	2008-01-24	Hatano, Kouji et al.		
		2009065137	WO	A1	2009- 05-22	Soroushian, K. et al.		
		2010060106	WO	A1	2010- 05-27	Kohli, J et al.		
		2010122447	WO	A1	2010-10-28	Foo, Teck et al.		
		2011068668	WO	A1	2011-06-09	Chan, F et al.		
		2012094181	WO	A2	2012-07-12	Soroushian, K et al.		
		2012/094189	WO	A1	2012-07-12	Braness, J et al.		
		2012094171	WO	A1	2012-07-12	Braness, Jason et al.		

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	02359A

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
		"Information Technology-Coding of Audio Visual Objects- Part 2: Visual" International Standard, ISO/IEC 14496-2, Third Edition, Jun. 1, 2004, pp. 1-724.	
		Cloakware Corporation, "Protecting Digital Content Using Cloakware Code Transformation Technology", Version 1.2, May 2002, pgs 1-10.	
		European Search Report for Application 11855103.5, search completed June 26, 2014, 9 pgs.	
		European Search Report for Application 11855237.1, search completed June 25, 2014, 9 pgs.	
		Federal Computer Week, "Tool Speeds Info to Vehicles", July 25, 1999, 5 pages.	
		HTTP Live Streaming Overview, Networking & Internet, Apple, Inc., April 1, 2011, 38 pages.	
		International Preliminary Report on Patentability for International Application No. PCT/US2011/068276, International Filing Date December 31, 2011, Issue Date March 4, 2014, 23 pgs.	
		International Search Report and Written Opinion for International Application No. PCT/US2010/56733, International Filing Date November 15, 2010, Search Completed January 3, 2011, Mailed January 14, 2011, 9 pgs.	
		International Search Report and Written Opinion for International Application PCT/US2011/066927, International Filing Date December 22, 2011, Report Completed April 3, 2012, Mailed April 20, 2012, 14 pgs.	
		International Search Report and Written Opinion for International Application PCT/US2011/067167, International Filing Date December 23, 2011, Report Completed June 19, 2012, Mailed July 2, 2012, 11 pgs.	

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	02359A

		International Search Report for International Application No. PCT/US2005/025845 filed July 21, 2005, report completed February 5, 2007 and mailed May 10, 2007, 3 pgs.	
		International Search Report for International Application No. PCT/US2007/063950 filed March 14, 2007, report completed February 19, 2008; report mailed March 19, 2008, 3 pgs.	
		ITS International, "Fleet System Opts for Mobile Server", August 26, 1999, 1 page.	
		Microsoft, Microsoft Media Platform: Player Framework, "Silverlight Media Framework v1.1", 2 pages.	
		Microsoft, Microsoft Media Platform: Player Framework, "Microsoft Media Platform: Player Framework v2.5 (formerly Silverlight Media Framework)", 2 pages.	
		The Official Microsoft IIS Site, Smooth Streaming Client, 4 pages.	
		Written Opinion for International Application No. PT/US2005/025845 filed July 21, 2005, report completed February 5, 2007 and mailed May 10, 2007, 5 pgs.	
		Written Opinion for International Application No. PCT/US2007/063950 filed March 14, 2007, report completed March 1, 2008; report mailed March 19, 2008, 5 pgs.	
		"Adaptive Streaming Comparison", January 28, 2010, 5 pgs.	
		"Best Practices for Multi-Device Transcoding", Kaltura Open Source Video, 13 pgs.	
		"Informationweek: Front End: Daily Dose, Internet on Wheels", July 20. 1999, 3 pgs.	
		"Netflix turns on subtitles for PC, Mac streaming", 3 pgs.	

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	02359A

		Supplementary European Search Report for Application No. EP 10834935, International Filing Date November 15, 2010, Search Completed May 27, 2014, 9 pgs.	
		"Supported Media Formats", Supported Media Formats, Android Developers, November 27, 2013, 3 pgs.	
		"Thread: SSME (Smooth Streaming Medial Element) config.xml review (Smooth Streaming Client configuration file)", 3 pgs.	
		"Transcoding Best Practices", From movideo, November 27, 2013, 5 pgs.	
		"Using HTTP Live Streaming", iOS Developer Library, Retrieved from: http://developer.apple.com/library/ios/#documentation/networkinginternet/conceptual/streamingmediaguide/UsingHTTPLiveStreaming/UsingHTTPLiveStreaming.html#//apple_ref/doc/uid/TP40008332-CH102-SW1, 10 pgs.	
		AKHSHABI ET AL., "An Experimental Evaluation of Rate-Adaptation Algorithms in Adaptive Streaming over HTTP", MMSys'11, February 24-25, 2011, 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.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

(Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44*bis*)

Applicant's or agent's file reference D1:02359AB.PCT	**FOR FURTHER ACTION**	See item 4 below
International application No. PCT/US2011/068276	International filing date *(day/month/year)* 31 December 2011 (31.12.2011)	Priority date *(day/month/year)* 01 September 2011 (01.09.2011)
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237		
Applicant SONIC IP, INC.		

1. This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 *bis*.1(a).

2. This REPORT consists of a total of 23 sheets, including this cover sheet.

   In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.

3. This report contains indications relating to the following items:

☒	Box No. I	Basis of the report
☐	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 Article 35(2) 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

4. The International Bureau will communicate this report to designated Offices in accordance with Rules 44*bis*.3(c) and 93*bis*.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44*bis* .2).

	Date of issuance of this report 04 March 2014 (04.03.2014)
The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 338 82 70	Authorized officer Philippe Bécamel e-mail: pt03.pct@wipo.int

Form PCT/IB/373 (January 2004)

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 D1:02359AB.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:

- [X] 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
- [X] 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/US2011/068276

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:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2011/068276

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]).

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 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, 49-53, 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 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 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 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).

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 36, 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).

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).

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 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).

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 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 0058); 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).

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 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).

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 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 0057]; the chunks are protected using different watermark payloads, para 0052). 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 0057).

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).

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 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 i=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).

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 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, 41-48, 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).

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 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, 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 i=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, 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).

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).

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 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 156 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; 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 i=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 0056). 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 i=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 0056). 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).

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 i=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).

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 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 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 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).

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 0053). 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 89, 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)

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).

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 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 0058). 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 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 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 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). 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 i=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 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. 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).
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).

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 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, 0054). 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 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 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.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference D1:01940.PCT	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US 10/56733	International filing date *(day/month/year)* 15 November 2010 (15.11.2010)	(Earliest) Priority Date *(day/month/year)* 04 December 2009 (04.12.2009)
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. 2
      ☒ 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/US 10/56733

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - H04N 7/167 (2010.01)
USPC - 380/217
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 - 380/217

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC - 380/210; 380/239; 705/51 (keyword limited; terms below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Dialog; Google
Transmit, sent, deliver, transport, distrib, media, multimedia, video, content, encrypt, decrypt, crypt, encipher, decipher, scramble, process, algorithm, data, stream, bitstream, container, wrapper, file, digital, rights, management, DRM, header, user, metadata, data, heu

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 2004/0081333 A1 (GRAB et al.) 29 April 2004 (29.04.2004), Para [0033], [0037]-[0042], [0047]-[0048], [0050], [0052], [0055]-[0056]	1-9 and 13-21 --- 10-12 and 22-25
Y	US 2003/0035546 A1 (JIANG et al.) 20 February 2003 (20.02.2003), Para [0021]	10-12 and 22-25
A	US 2003/0035545 A1 (JIANG) 20 February 2003 (20.02.2003)	10, 22, 25
A	US 2004/0105549 A1 (SUZUKI et al.) 03 June 2004 (03.06.2004)	1-25
A	US 2007/0255940 A1 (UENO) 01 November 2007 (01.11.2007)	1-25
A	US 2009/0097644 A1 (HARUKI) 16 April 2009 (16.04.2009)	1-25

☐ 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
03 January 2011 (03.01.2011)	14 JAN 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)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To: DAVID J. BAILEY
KAUTH, POMEROY, PECK & BAILEY LLP
2875 MICHELLE DRIVE, SUITE 110
IRVINE, CA 92606

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	14 JAN 2011

Applicant's or agent's file reference	FOR FURTHER ACTION
D1:01940.PCT	See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US 10/56733	15 November 2010 (15.11.2010)	04 December 2009 (04.12.2009)

International Patent Classification (IPC) or both national classification and IPC
IPC(8) - H04N 7/167 (2010.01)
USPC - 380/217

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.

3. For further details, see notes to 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	03 January 2011 (03.01.2011)	Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/237 (cover sheet) (July 2009)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 10/56733

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 0133
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 10/56733

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	10-12 and 22-25	YES
	Claims	1-9 and 13-21	NO
Inventive step (IS)	Claims	None	YES
	Claims	1-25	NO
Industrial applicability (IA)	Claims	1-25	YES
	Claims	None	NO

2. Citations and explanations:

Claims 1-9 and 13-21 lack novelty under PCT Article 33(2) as being anticipated by US 2004/0081333 A1 to Grab et al. (hereinafter 'Grab').

As per claim 1, Grab discloses a method of playing back encrypted video on a playback device, where at least partially encrypted video data (Para [0033] -- selected portions of a stream) is contained within a container file (Para [0033] -- header data; Para [0040] -- tagged, synchronized frame decryption stream) and can be used to create an elementary bitstream using cryptographic information (Para [0033] -- encrypted material), which can be used to decrypt the at least partially encrypted video data (Para [0040]), the method comprising: obtaining the cryptographic information (Para [0040] -- encryption key); extracting the at least partially encrypted video data from the container file to create an elementary bitstream (Para [0038] -- marked frames; Para [0042]); enciphering the cryptographic information (Para [0047]); inserting the cryptographic information in the elementary bitstream (Para [0042], [0047]); providing the elementary bitstream to a video decoder (Para [0048]); extracting the cryptographic information from the elementary bitstream at the video decoder (Para [0048] -- parsing frames); deciphering the cryptographic information (Para [0048] -- decryption routine); decrypting the elementary bitstream with the cryptographic information (Para [0048] -- decrypting with appropriate decryption key); and decoding the elementary bitstream for rendering on a display device using the video decoder (Para [0048], [0052]).

As per claim 13, Grab further discloses a system for playback of encrypted video, where at least partially encrypted video data (Para [0033] -- selected portions of a stream) is contained within a container file (Para [0033] -- header data; Para [0040] -- tagged, synchronized frame decryption stream) and can be used to create an elementary bitstream using cryptographic information (Para [0033] -- encrypted material), which can be used to decrypt the at least partially encrypted video data (Para [0040]), comprising: a demultiplexer configured to extract the at least partially encrypted video data from the container file to create an elementary bitstream (Para [0038] -- marked frames; Para [0042]); and a video decoder configured to decrypt the elementary bitstream using the cryptographic information (Para [0048] -- decrypting with appropriate decryption key) and decode the elementary bitstream for rendering on a display device (Para [0048], [0052]); wherein the demultiplexer is configured to encipher the cryptographic information (Para [0047]) and insert the enciphered cryptographic information in the elementary bitstream (Para [0042], [0047]); and wherein the decoder is configured to extract enciphered cryptographic information from an elementary bitstream (Para [0048] -- parsing frames) and to decipher the cryptographic information (Para [0048] -- decryption routine).

As per claims 2 and 14, Grab further discloses wherein the cryptographic information is obtained from the container file (Para [0040] -- encryption key from synchronized frame decryption stream).

As per claims 3 and 15, Grab further discloses wherein the cryptographic information comprises: key information (Para [0040]); and information concerning at least a portion of the at least partially encrypted video data that is encrypted using the key information (Para [0038], [0040] -- encryption on/off status).

As per claims 4 and 16, Grab further discloses wherein the information concerning at least a portion of the at least partially encrypted video data is a reference to a block of encrypted data within an encoded frame of video that is encrypted using the key information (Para [0040] -- size of data field).

As per claims 5 and 17, Grab further discloses wherein the cryptographic information inserted in the elementary bitstream is delimited by an identifier (Para [0040] -- encryption on/off status); and the cryptographic information is inserted before the at least partially encrypted video data encrypted using the key information (Para [0050] -- frame decryption information).

As per claims 6 and 18, Grab further discloses wherein the cryptographic information is extracted using the identifier (Para [0048] -- parsing frames).

As per claims 7 and 19, Grab further discloses wherein the decrypting process is performed by using the key information to identify the encrypted portion of video data and decrypting the encrypted video data using the key information (Para [0048]).

As per claims 8 and 20, Grab further discloses wherein cryptographic information inserted in different locations within the elementary bitstream includes different key information (Para [0041] -- new key for new partially encrypted video data).

As per claims 9 and 21, Grab further discloses wherein the at least partially encrypted video data comprises: frames of encoded video (Para [0039]); wherein at least a portion of a plurality of the encoded frames is encrypted (Para [0039]).

-- Please See Supplemental Sheet --

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0134
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 10/56733

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:
Box V.2 Citations and Explanations

Claims 10-12 and 22-25 lack an inventive step under PCT Article 33(3) as being obvious over Grab in view of US 2003/0035546 A1 to Jiang et al. (hereinafter 'Jiang').

As per claims 10 and 22, Grab does not disclose wherein the enciphering process and the deciphering process are synchronized such that a delay in excess of a predetermined time between enciphering and deciphering results in the cryptographic information being unrecoverable. However, Jiang does disclose wherein the enciphering process and the deciphering process are synchronized such that a delay in excess of a predetermined time between enciphering and deciphering results in the cryptographic information being unrecoverable (Para [0021]). It would have been obvious to one of ordinary skill in the art to have modified Grab so as to include synchronized processes, as taught by Jiang, since such would help protect the encrypted bitstream by recognizing if any additional processes were being performed on the bitstream, thereby extending the delay above the predetermined time, and stopping access to the deciphering process.

As per claims 11 and 23, Grab does disclose wherein the enciphering process enciphers data by using a sequence of scrambling processes to scramble data (Para [0033], [0037], [0055] -- signal processing techniques).

As per claims 12 and 24, Grab does disclose wherein the deciphering process deciphers data by performing the inverse sequence of scrambling processes to the sequence used to scramble the data (Para [0056]).

As per claim 25, Grab further discloses method of playing back encrypted video on a playback device, where at least partially encrypted video data (Para [0033] -- selected portions of a stream) is contained within a container file (Para [0033] -- header data; Para [0040] -- tagged, synchronized frame decryption stream) and can be used to create an elementary bitstream using cryptographic information (Para [0033] -- encrypted material), which can be used to decrypt the at least partially encrypted video data (Para [0040]), the method comprising: obtaining the cryptographic information (Para [0040] -- encryption key), wherein the cryptographic information is obtained from the container file (Para [0040] -- encryption key from synchronized frame decryption stream); wherein the at least partially encrypted video data comprises: frames of encoded video (Para [0039]); and wherein at least a portion of a plurality of the encoded frames is encrypted (Para [0039]); wherein the cryptographic information comprises: key information (Para [0040]); and information concerning at least a portion of the least partially encrypted video data that is encrypted using the key information (Para [0038], [0040] -- encryption on/off status); wherein the information concerning at least a portion of the at least partially encrypted video data is a reference to a block of encrypted data within an encoded frame of video that is encrypted using the key information (Para [0040] -- size of data field); and wherein cryptographic information inserted in different locations within the elementary bitstream includes different key information (Para [0041] -- new key for new partially encrypted video data); extracting the at least partially encrypted video data from the container file to create an elementary bitstream (Para [0038] -- marked frames; Para [0042]), wherein the cryptographic information inserted in the elementary bitstream is delimited by an identifier (Para [0040] -- encryption on/off status); and wherein the cryptographic information is inserted before the at least partially encrypted video data encrypted using the key information (Para [0050] -- frame decryption information); enciphering the cryptographic information (Para [0047]); inserting the cryptographic information in the elementary bitstream (Para [0042], [0047]), wherein the cryptographic information is extracted using the identifier (Para [0048] -- parsing frames); providing the elementary bitstream to a video decoder (Para [0048]); extracting the cryptographic information from the elementary bitstream at the video decoder (Para [0048] -- parsing frames); deciphering the cryptographic information (Para [0048] -- decryption routine), wherein the enciphering process enciphers data by using a sequence of scrambling processes to scramble data (Para [0033], [0037], [0055] -- signal processing techniques); and wherein the deciphering process deciphers data by performing the inverse sequence of scrambling processes in the sequence used to unscramble data (Para [0056]); decrypting the elementary bitstream with the cryptographic information (Para [0048] -- decrypting with appropriate decryption key), wherein the decrypting process is performed by using the key information to identify the encrypted portion of video data and decrypting the encrypted video data using the key information (Para [0048]); and decoding the elementary bitstream for rendering on a display device using the video decoder (Para [0048], [0052]). Grab does not disclose wherein the enciphering process and the deciphering process are synchronized such that a delay in excess of a predetermined time between enciphering and deciphering results in the cryptographic information being unrecoverable. However, Jiang does disclose wherein the enciphering process and the deciphering process are synchronized such that a delay in excess of a predetermined time between enciphering and deciphering results in the cryptographic information being unrecoverable (Para [0021]). It would have been obvious to one of ordinary skill in the art to have modified the method of Grab so as to include synchronized processes, as taught by Jiang, since such would help protect the encrypted bitstream by recognizing if any additional processes were being performed on the bitstream, thereby extending the delay above the predetermined time, and stopping access to the deciphering process.

Claims 1-25 have industrial applicability as defined by PCT Article 33(4), because the subject matter can be made or used in industry.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0135
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

SEARCH HISTORY

Application Number	PCT/US 10/56733
Search Conducted By	ANK
Search Approved By	PJN

US/IPC Classifications Searched	USPC - 380/217
Date Conducted	03 January 2011 (03.01.2011)

Documentation Searched	USPC - 380/210; 380/239; 705/51 (keyword limited; terms below)
Search Terms Used	Transmit, sent, deliver, transport, distrib, media, multimedia, video, content, encrypt, decrypt, crypt, encipher, decipher, scramble, process, algorithm, data, stream, bitstream, container, wrapper, file, digital, rights, management, DRM, header, user, metadata, data, heuristic, rule, playing, back, delay
Date Conducted	03 January 2011 (03.01.2011)

Electronic Database Searched	Dialog
Files Searched	2 - INSPEC; 6 - NTIS (National Technical Information Service); 63 - Transportation Research Information Services (TRIS); 65 - Inside Conferences; 118 - ICONDA - International Construction Database; 144 - PASCAL; 440 - Current Contents Search; 344 - Chinese Patent Abstracts in English; 348 - European Patents Fulltext; 349 - WIPO/PCT Patents Fulltext; 371 - French Patents; 652 - US Patents Fulltext (1971 – 1975); 654 - US Patents Fulltext (1976 – present)
Date Conducted	03 January 2011 (03.01.2011)

Search Logic:

```
S1      203  CL=380-217
S2     3208  CL=(380-210 OR 380-239 OR 705-51)
S3     3357  S1 OR S2
S4     1998  S3 AND (TRANSMIT? OR SEND??? OR DELIVER? OR TRANSPORT? OR
                 DISTRIB?)(N5)(MEDIA OR MULTIMEDIA OR VIDEO OR CONTENT)
```

SEARCH HISTORY

S5	1693	S4 AND (ENCRYPT? OR DECRYPT? OR CRYPT?)
S6	84	S5 AND (ENCIPHER? OR DECIPHER? OR SCRAMBLE)(N3)(PROCESS? OR ALGORITHM)
S7	24	S6 AND (MEDIA OR MULTIMEDIA OR VIDEO)(N5)(DATA(N3)STREAM OR BITSTREAM)
S8	32	S5 AND (CONTAINER OR WRAPPER)(N3)FILE
S9	325	S5 AND (DIGITAL(N3)RIGHTS(N3)MANAGEMENT OR DRM)
S10	158	S9 AND (HEADER OR USER OR METADATA)(N3)DATA
S11	44	S10 AND (HEURISTIC OR RULE)
S12	482686	(TRANSMIT? OR SEND??? OR DELIVER? OR TRANSPORT? OR DISTRIB?)(N5)(MEDIA OR MULTIMEDIA OR VIDEO OR CONTENT)
S13	40351	(MEDIA OR MULTIMEDIA OR VIDEO)(N5)(DATA(N3)STREAM OR BITSTREAM)
S14	5808	(ENCIPHER? OR DECIPHER? OR SCRAMBLE)(N3)(PROCESS? OR ALGORITHM)
S15	1777	S14 AND (TRANSMIT? OR SEND??? OR DELIVER? OR TRANSPORT? OR DISTRIB?)(N5)(MEDIA OR MULTIMEDIA OR VIDEO OR CONTENT)
S16	1145	S15 AND (ENCRYPT? OR DECRYPT? OR CRYPT?)
S17	225	S16 AND (MEDIA OR MULTIMEDIA OR VIDEO)(N5)(DATA(N3)STREAM OR BITSTREAM)
S18	218	S17 AND (ENCOD? OR DECOD?)
S19	14	S18 AND (DIGITAL(N3)RIGHTS(N3)MANAGEMENT OR DRM)

Electronic Database Searched	Google
Files Searched	Google Patents
Date Conducted	03 January 2011 (03.01.2011)

Search Logic:

Patents 401 - 464 on playing back encrypted video
Patents 1 - 74 on playing back encrypted video deciphering synchronized
Patents 1 - 13 on enciphering sync delay
Patents 101 - 174 on encrypted video enciphering
Patents 1 - 84 on encrypting video DRM container

Electronic Database Searched	Google
Files Searched	Google Scholar
Date Conducted	03 January 2011 (03.01.2011)

Search Logic:

playing back encrypted video
Results 1 - 10 of about 35,800

SEARCH HISTORY

playing back encrypted video deciphering synchronized
Results **1** - **10** of about **6,340**
enciphering sync delay
Results **1** - **10** of about **154**
encrypted video enciphering
Results **1** - **10** of about **1,410**
encrypting video DRM container
Results **1** - **10** of about **954**

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 01974AB.PCT	FOR FURTHER ACTION	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US 11/66927	International filing date *(day/month/year)* 22 December 2011 (22.12.2011)	(Earliest) Priority Date *(day/month/year)* 05 January 2011 (05.01.2011)
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 35 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:

ADAPTIVE BITRATE STREAMING OF MEDIA STORED IN MATROSKA CONTAINER FILES USING HYPERTEXT TRANSFER PROTOCOL

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. 1

   ☒ 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.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 11/66927

Box No. IV Text of the abstract (Continuation of item 5 of the first sheet)

Systems and methods for adaptive bitrate streaming of media stored in Matroska container files utilizing Hypertext Transfer Protocol (HTTP) are disclosed. In one embodiment, a processor requests portions of files from a remote server and retrieves top level index data that identifies EBML container files and describes a maximum bitrate of the alternative streams contained within the EBML container files. The top level index data is parsed to obtain information identifying the EBML container files, requests a portion of at least one of the EBML container files that contains the at least one element that specifies the encoding parameters of the stream contained within the EBML container file, and requests portions of a first EBML container file that includes elements that contain portions of encoded video, where the selection is based upon the measured streaming conditions and the description of the bitrate of the alternative stream contained within the top level data.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 11/66927

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F 15/16 (2012.01)
USPC - 709/231
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: 709/231

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 709/231 | 709/203 | 375/240.28 | 375/E07.011 | 375/E07.154 (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: streaming, video, adaptive, server, network, bit, rate, container, frame, block, parse, http, encode, elements, level, layer, cluster, chunk, matroska, xml, ebml.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2010/0189183 A1 (Gu et al.) 29 July 2010 (29.07.2010), entire document, especially abstract; para [0004], [0006], [0008], [0020], [0022], [0024], [0026], [0042], [0046], [0047], [0068].	1-66
Y	US 2007/0168541 A1 (Gupta et al.) 19 July 2007 (19.07.2007), entire document, especially abstract; para [0003], [0004], [0022], [0023], [0028], [0040], [0047], [0055], [0068], [0080], [0083].	1-66
A	US 2007/0083617 A1 (Chakrabarti et al.) 12 April 2007 (12.04.2007), entire document, especially abstract; para [0007], [0010], [0012], [0014], [0024], [0030], [0061], [0078], [0102].	1-66

☐ 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
03 April 2012 (03.04.2012)	20 APR 2012
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)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

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

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	20 APR 2012
Applicant's or agent's file reference 01974AB.PCT	FOR FURTHER ACTION See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US 11/66927	22 December 2011 (22.12.2011)	05 January 2011 (05.01.2011)

International Patent Classification (IPC) or both national classification and IPC
IPC(8) - G06F 15/16 (2012.01)
USPC - 709/231

Applicant DIVX, LLC

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

- [X] 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
- [X] 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	03 April 2012 (03.04.2012)	Lee W. Young 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/US 11/66927

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:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 11/66927

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	1-66	YES
	Claims	None	NO
Inventive step (IS)	Claims	None	YES
	Claims	1-66	NO
Industrial applicability (IA)	Claims	1-66	YES
	Claims	None	NO

2. Citations and explanations:

Claims 1-66 lack an inventive step under PCT Article 33(3) as being obvious over US 2010/0189183 A1 to Gu et al. (hereinafter Gu) in view of US 2007/0168541 A1 to Gupta et al. (hereinafter Gupta).

Regarding claim 1, Gu teaches a playback device configured to perform adaptive bitrate streaming (a multiple bit rate video encoder encodes a plurality of video streams for multiple bit rate video streaming with an objective of providing a more consistent video quality, para [0008]) using a plurality of alternative streams of encoded video packaged within extensible binary markup language (EBML) container files (utilizes the motion information to perform inter-frame coding of the predicted frames of the video content. The encoding can be performed according to a known video encoding standard, such as Windows Media Video format, SMPTE 421-M format, MPEG-x format (e.g., MPEG-1, MPEG-2, or MPEG-4), H.26x times, format (e.g., H.261, H.262, H.263, or H.264), or other format, para [0026]), where each of the plurality of alternative streams is the same source video encoded using different encoding parameters in such a way that each portion of encoded video packed into an element of an EBML container file (source video content is encoded into alternative bit streams at different coding rates and typically stored in the same media file at the server. This then allows the content to be streamed in segments or chunks at varying levels of quality corresponding to different coding rates according to the changing network conditions, para [0004]) commences with an intra frame starting a closed Group of Pictures (GOP) and each of the EBML container files includes at least one element that specifies the encoding parameters of the stream contained within the EBML container file (Video streams at intermediate bit rates are encoded at progressively decreasing variable bit rates (subject to decreasing peak and average bit rate constraints), para [0008]), the playback device comprising: a processor configured, via a client application, to request portions of files from a remote server (a server 110 (e.g., a server computer system such as a standard HTTP server) provides multimedia content to a client 120 (e.g., a client computer system, such as a laptop or desktop computer, or another type of computing device, such as a PDA or mobile phone) via a network, para [0020]); wherein the client application further configures the processor to: retrieve top level index data that identifies a plurality of EBML container files and describes at least a maximum bitrate of the alternative streams contained within the EBML container files (top MBR video stream (generally having highest overall bit rate), the video encoder 200 encodes the video stream with a varying bit rate constrained to fall under a specified peak bit rate while satisfying a specified average bit rate. For the bottom MBR stream (generally having the lowest bit rate of the set), the video encoder uses a constant chunk rate approach. In the context of the multiple bit rate video streaming system, the term chunk refers to a group of pictures (GOP) into which the video stream are segmented, para [0042]); request a portion of at least one of the EBML container files that contains the at least one element that specifies the encoding parameters of the stream contained within the EBML container file (divides video of a multimedia program into multiple streaming segments, and contains a number of compressed bit streams representing the video segments at various bit rates, para [0020]); retrieve an index that references each element containing portions of encoded video within at least one of the EBML container files (the indexed file for multi bit rate streaming can be used by standard HTTP servers to serve multimedia content at multiple bit rates with bit rate selection (rate control) being performed client-side (e.g., exclusively client-side). Clients can perform rate control by first obtaining index information from the server describing the various bit rates available for streaming segments of a program, para [0022]); utilize the index to request portions of a first EBML container file that includes elements that contain portions of encoded video (divided into temporal chunks called streaming segments (self-contained units). The server stores each streaming segment at one or more bit rates (e.g., each streaming segment--bit rate combination is a separate streaming segment encoding). Each streaming segment includes one or more available bit rate encodings for a specific track, para [0024]); receive and buffer the requested elements (Based on the index information, and possibly other information (e.g., network bandwidth, buffer information, etc.), the client can decide which bit rate streaming segments to download from the server to provide a desired user experience, para [0022]); decode the encoded video contained within the buffered elements utilizing the encoding parameters (the video streams at the multiple bit rates can all be decoded and scaled to this same final display resolution in order to achieve a glitch free video presentation, para [0006]). Gu does not expressly teach parse the top level index data to obtain information identifying the plurality of EBML container files; measure current streaming conditions; and select another of the EBML container files from which to retrieve elements containing portions of encoded video for decoding, where the selection is based upon the measured streaming conditions and the description of the bitrate of the alternative stream contained within the top level data. However Gupta, in an analogous art, teaches parse the top level index data to obtain information identifying the plurality of EBML container files (enumerating and assigning each frame a timestamp, parsing the media file headers and footers, and computing format-specific "chunk" boundary points based on the indexable file portions, or chunks. The media content is stored in a source file data storage 125, and data about the media content is stored out-of-band from the media content in a content index, para [0022]); measure current streaming conditions (the server 110 can measure the time between client reads of successive 64 kB chunks of content. This is a reasonable measurement of client 105 throughput because the standard internet networking architecture (routers, switches, etc.) have very small

---continued in supplemental box---

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 11/66927

Supplemental Box

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

Continuation of:
Box No. V.2. Citations and explanations.

Claim 1 (continued): buffers, and thus, the rate at which the client is reading can be estimated in this way. The amount of network buffering may also be able to be determined by keeping statistics and probing each client's destination network or sub-net. Other factors that affect client networking speed (such as the required retransmission of TCP/IP network packets) can be known, measured, and accounted for as well, to give a more accurate estimation of client read speed, para [0080]); and select another of the EBML container files from which to retrieve elements containing portions of encoded video for decoding, where the selection is based upon the measured streaming conditions and the description of the bitrate of the alternative stream contained within the top level data (Once the sending rate is adjusted 1060, the server 110 returns to selecting 1020 the next portion of content, modifying 1030 the content if necessary, and writing 1040 the portion to output. Following the writing 1040 step, the server 110 next determines 1070 whether more instructions apply to the requested media content. If the request includes more instructions, steps 1020-1040 repeat according to the next instruction. Once all instructions are processed and the altered media shot is formed from the selected frames, the server 110 serves 1080 any remaining portion of the combined media shot to the client , para [0083]). It would have been obvious to one skilled in the art to combine the teachings of Gu with those of Gupta in order to more efficiently adapt to multiple streaming bit rates in the video playback system of Gu (see Gupta para [0003]-[0004]).

Regarding claim 2, Gu further teaches wherein: each of the EBML container files comprises a plurality of Cluster elements, where each Cluster element contains a portion of encoded video (term chunk refers to a group of pictures (GOP) into which the video stream are segmented, and define the level of granularity at which the video streaming system may switch playing individual segments between video streams. The constant chunk rate approach enables the video streaming system to guarantee predictability of streaming, para [0042]); and the portion of encoded video in each of the Cluster elements commences with an intra frame and includes at least one closed group of pictures (video encoder then performs intra-frame coding of reference frames of the video content, and utilizes the motion information to perform inter-frame coding of the predicted frames of the video content, para [0026]).

Regarding claim 3, Gu further teaches wherein the portions of encoded video in each of the Cluster elements have the same duration (constant chunk rate approach enables the video streaming system to guarantee predictability of streaming, in that when the lowest bit rate or quality video stream is streamed, the client will receive the chunk amount of pictures at the constant rate so as to maintain minimum quality continuous playing of the video, para [0042]).

Regarding claim 4, Gupta further teaches wherein the portions of encoded video in each of the Cluster elements have a 2 second duration (request also includes a time range for each shot, specified as the starting time (e.g., in seconds into the content) and length (e.g., in seconds). For example, for shot 1, the starting time is 10 seconds (begin=10) and the length is 8 seconds (len=8). The request also includes an edit list that refers to a list of instructions for interleaving the four streams from shots 1-4, such that the new piece of content includes the video of each of shots 1-3 and the audio of shot, para [0058]).

Regarding claim 5, Gu further teaches wherein each Cluster element contains a time code and each encoded frame of the portion of encoded video contained within the Cluster element is contained within a separate BlockGroup element (Between marked boundaries of a video sequence (sequence mark-in and sequence mark-out positions), the MBR encoding process 300 further determines a total number of group of pictures segments in which to divide the video sequence within user-specified constraints (such as a specified average GOP length and maximum allowed GOP length within a scene) and sets boundaries of each group of pictures, para [0046]).

Regarding claim 6, Gu further teaches wherein the first BlockGroup element in the Cluster element contains the intra frame (MBR engine controls the video encoder to produce an encoding of the video stream to meet the constant chunk rate constraint, which helps guarantee client side predictability for playing the streamed video. In intermediate video streams, the MBR engine causes the video encoder to encode the source video with encoding parameters to produce the video stream a variable bit rate falling within maximal peak and average bit rate constraints for the respective intermediate stream, para [0047]).

Regarding claim 7, Gupta further teaches wherein the first BlockGroup element contains a Block element, which specifies the time code attribute of the intra frame relative to the time code of the Cluster element (enumerating and assigning each frame a timestamp, parsing the media file headers and footers, and computing format-specific "chunk" boundary points based on the indexable file portions, or chunks, para [0022]).

Regarding claim 8, Gu further teaches wherein each of the alternative streams of encoded video is encoded at a different maximum bitrate (source video content is encoded into alternative bit streams at different coding rates and typically stored in the same media file at the server. This then allows the content to be streamed in segments or chunks at varying levels of quality corresponding to different coding rates according to the changing network conditions, para [0004]).

Regarding claim 9, Gupta further teaches wherein at least two of the alternative streams of encoded video are encoded at the same display aspect ratio, but with different resolutions using different sample aspect ratios (an identifier for the video encoding format and resolution. In this example, the row identifier includes multiple columns to specify the content index 130 data as discussed herein. Alternatively, all data for all chunks of a media file is stored in a single database row, using one or more columns, para [0028]).

Regarding claim 10, Gupta further teaches wherein the at least one element in each of the EBML container files that specifies the encoding parameters of the stream contained within the EBML container file specifies the frame height, frame width and sample aspect ratio of the video stream contained within the EBML container file (an identifier for the video encoding format and resolution. In this example, the row identifier includes multiple columns to specify the content index 130 data as discussed herein. Alternatively, all data for all chunks of a media file is stored in a single database row, using one or more columns, para [0028]).

---continued in supplemental box---

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 11/66927

Supplemental Box

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

Continuation of:
Box No. V 2. Citations and explanations.

Regarding claim 11, Gupta further teaches wherein the client application configures the processor to set the frame height, frame width, and sample aspect ratio prior to commencing the decoding of encoded video contained within buffered elements from one of the EBML container files (an identifier for the video encoding format and resolution. In this example, the row identifier includes multiple columns to specify the content index 130 data as discussed herein. Alternatively, all data for all chunks of a media file is stored in a single database row, using one or more columns, para [0028]).

Regarding claim 12, Gu further teaches wherein at least two of the alternative streams of encoded video are encoded at different frame rates (source video content is encoded into alternative bit streams at different coding rates and typically stored in the same media file at the server. This then allows the content to be streamed in segments or chunks at varying levels of quality corresponding to different coding rates according to the changing network conditions, para [0004]).

Regarding claim 13, Gupta further teaches wherein the at least one element in each of the EBML container files that specifies the encoding parameters of the stream contained within the EBML container file specifies the frame rate of the video stream contained within the EBML container file (in addition, the server 110 stores the relevant header and footer information, such as video resolution and frame rate, byte range of the portion of the file that is being composed, and other file format specific information, para [0040]).

Regarding claim 14, Gupta further teaches wherein the client application configures the processor to set the frame rate prior to commencing the decoding of encoded video contained within buffered elements from one of the EBML container files (in addition, the server 110 stores the relevant header and footer information, such as video resolution and frame rate, byte range of the portion of the file that is being composed, and other file format specific information, para [0040]).

Regarding claim 15, Gu further teaches wherein the client application configures the playback device to request portions of files from remote servers via Hypertext Transfer Protocol (HTTP) byte range requests (the indexed file for multi bit rate streaming can be used by standard HTTP servers to serve multimedia content at multiple bit rates with bit rate selection (rate control) being performed client-side (e.g., exclusively client-side). Clients can perform rate control by first obtaining index information from the server describing the various bit rates available for streaming segments of a program, para [0022]).

Regarding claim 16, Gupta further teaches wherein the top level index data is SMIL data and the information that identifies the plurality of EBML container files is a plurality of Universal Resource Indicators that identify the location of each of the EBML container files (instructions are converted into a request from the client for the edited content, for example in the form of a URL as described in conjunction with FIGS. 4A-C, which is sent to the server, para [0068]).

Regarding claim 17, Gu further teaches wherein the SMIL data specifies the maximum bitrate of the encoded stream contained within the EBML container file identified by each of the URLs (source video content is encoded into alternative bit streams at different coding rates and typically stored in the same media file at the server. This then allows the content to be streamed in segments or chunks at varying levels of quality corresponding to different coding rates according to the changing network conditions, para [0004]).

Regarding claim 18, Gupta further teaches wherein: the index that references each of the elements containing portions of the encoded stream within the EBML container file is located within at least one element of the EBML container file (an identifier for the video encoding format and resolution. In this example, the row identifier includes multiple columns to specify the content index 130 data as discussed herein. Alternatively, all data for all chunks of a media file is stored in a single database row, using one or more columns, para [0028]); the SMIL file specifies the portions of the EBML container file that contain the elements that contain the encoding parameters (an identifier for the video encoding format and resolution. In this example, the row identifier includes multiple columns to specify the content index 130 data as discussed herein. Alternatively, all data for all chunks of a media file is stored in a single database row, using one or more columns, para [0028]); the client application further configures the processor to: parse the SMIL file to identify the portions of the EBML container file that contain the elements that contain the encoding parameters; and request the portions of the EBML container file that contain the elements that contain the encoding parameters (enumerating and assigning each frame a timestamp, parsing the media file headers and footers, and computing format-specific "chunk" boundary points based on the indexable file portions, or chunks. The media content is stored in a source file data storage 125, and data about the media content is stored out-of-band from the media content in a content index, para [0022]).

Regarding claim 19, Gupta further teaches wherein: each EBML container file includes at least one element containing an index that references each element containing portions of encoded video within the EBML container file; and the client application configures the processor to retrieve the index that references each element containing portions of encoded video within an EBML container file by requesting the portion of the EBML container file that includes the at least one element containing the index (enumerating and assigning each frame a timestamp, parsing the media file headers and footers, and computing format-specific "chunk" boundary points based on the indexable file portions, or chunks. The media content is stored in a source file data storage 125, and data about the media content is stored out-of-band from the media content in a content index, para [0022]).

Regarding claim 20, Gupta further teaches wherein the index is located within a Cues element within the EBML container file (computing format-specific "chunk" boundary points based on the indexable file portions, or chunks. The media content is stored in a source file data storage 125, and data about the media content is stored out-of-band from the media content in a content index 130, which can be queried using a content identifier, para [0022]).

---continued in supplemental box---

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 11/66927

Supplemental Box

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

Continuation of:
Box No. V.2. Citations and explanations.

Regarding claim 21, Gupta further teaches wherein the Cues element includes a plurality of CuePoint elements that include a time attribute and point to the location of each element containing a portion of encoded video within the EBML file (enumerating and assigning each frame a timestamp, parsing the media file headers and footers, and computing format-specific "chunk" boundary points based on the indexable file portions, or chunks. The media content is stored in a source file data storage 125, and data about the media content is stored out-of-band from the media content in a content index, para [0022]).

Regarding claim 22, Gupta further teaches wherein the client application configures the processor to: search for the location of an element containing a specific portion of encoded video within the EBML file using the time attributes of the CuePoint elements within the index; and request a portion of the EBML file including at least the element identified using the CuePoint elements (computing format-specific "chunk" boundary points based on the indexable file portions, or chunks. The media content is stored in a source file data storage 125, and data about the media content is stored out-of-band from the media content in a content index 130, which can be queried using a content identifier, para [0022]).

Regarding claim 23, Gupta further teaches wherein the encoding parameters utilized to decode the encoded video include at least one encoding parameter selected from the group consisting of frame rate, frame height, frame width, sample aspect ratio, maximum bitrate, and minimum buffer size (an identifier for the video encoding format and resolution. In this example, the row identifier includes multiple columns to specify the content index 130 data as discussed herein. Alternatively, all data for all chunks of a media file is stored in a single database row, using one or more columns, para [0028]).

Regarding claim 24, Gupta further teaches wherein the client application configures the processor to measure the current streaming conditions by measuring the time taken to receive requested elements from the time at which the elements were requested (enumerating and assigning each frame a timestamp, parsing the media file headers and footers, and computing format-specific "chunk" boundary points based on the indexable file portions, or chunks. The media content is stored in a source file data storage 125, and data about the media content is stored out-of-band from the media content in a content index, para [0022]).

Regarding claim 25, Gu further teaches wherein: the client application configures the processor to initially request a portion of a first EBML container file containing at least one element that specifies the encoding parameters of the stream contained within the first EBML container file (a server 110 (e.g., a server computer system such as a standard HTTP server) provides multimedia content to a client 120 (e.g., a client computer system, such as a laptop or desktop computer, or another type of computing device, such as a PDA or mobile phone) via a network, para [0020]); and the client application further configures the processor to request a portion of a second EBML container file containing at least one element that specifies the encoding parameters of the stream contained within the second EBML container file, when the client application selects to retrieve elements containing portions of encoded video for decoding from the second EBML container file based upon the measured streaming conditions and the description of the bitrate of the alternative stream contained within the top level index (divides video of a multimedia program into multiple streaming segments, and contains a number of compressed bit streams representing the video segments at various bit rates, para [0020]).

Regarding claim 26, Gu further teaches wherein the playback device is further configured to perform adaptive bitrate streaming using an EBML container file that contains a trick play track (Each streaming segment includes one or more available bit rate encodings for a specific track (e.g., a specific audio track, such as an English audio track, or a specific video track) of a program. Clients then determine which bit rate, from the available bit rates (e.g., from the available streaming segment encodings), to download for each streaming segment. For example, a client may obtain a first streaming segment, for a video track, encoded at 250 Kb/sec (kilo-bits per second) (from one or more available streaming segment encodings for the first streaming segment), para [0024]).

Regarding claim 27, Gu further teaches wherein the client application configures the processor to select the EBML container file containing the trick play track as the EBML container file from which to retrieve elements containing portions of encoded video in response to a user instruction (Each streaming segment includes one or more available bit rate encodings for a specific track (e.g., a specific audio track, such as an English audio track, or a specific video track) of a program. Clients then determine which bit rate, from the available bit rates (e.g., from the available streaming segment encodings), to download for each streaming segment. For example, a client may obtain a first streaming segment, for a video track, encoded at 250 Kb/sec (kilo-bits per second) (from one or more available streaming segment encodings for the first streaming segment), para [0024]).

Regarding claim 28, Gu further teaches wherein the playback device is further configured to perform adaptive streaming using at least one EBML container file containing a track of encoded audio (a multiple bit rate video encoder encodes a plurality of video streams for multiple bit rate video streaming with an objective of providing a more consistent video quality, para [0008]).

Regarding claim 29, Gu further teaches wherein the client application configures the processor to retrieve and decode encoded audio from one of the at least one EBML container files containing an audio track and to synchronize the decoded audio with the decoded video (Each streaming segment includes one or more available bit rate encodings for a specific track (e.g., a specific audio track, such as an English audio track, or a specific video track) of a program. Clients then determine which bit rate, from the available bit rates (e.g., from the available streaming segment encodings), to download for each streaming segment. For example, a client may obtain a first streaming segment, for a video track, encoded at 250 Kb/sec (kilo-bits per second) (from one or more available streaming segment encodings for the first streaming segment), para [0024]).

---continued in supplemental box---

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 11/66927

Supplemental Box

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

Continuation of:
Box No. V.2. Citations and explanations.

Regarding claim 30, Gu further teaches wherein each of the EBML container files includes elements containing at least one track of encoded audio multiplexed with the encoded video (Each streaming segment includes one or more available bit rate encodings for a specific track (e.g., a specific audio track, such as an English audio track, or a specific video track) of a program. Clients then determine which bit rate, from the available bit rates (e.g., from the available streaming segment encodings), to download for each streaming segment. For example, a client may obtain a first streaming segment, for a video track, encoded at 250 Kb/sec (kilo-bits per second) (from one or more available streaming segment encodings for the first streaming segment), para [0024]).

Regarding claim 31, Gu further teaches wherein the client application is configured to: retrieve portions of the EBML file containing elements that include portions of one of the tracks of encoded audio (Each streaming segment includes one or more available bit rate encodings for a specific track (e.g., a specific audio track, such as an English audio track, or a specific video track) of a program. Clients then determine which bit rate, from the available bit rates (e.g., from the available streaming segment encodings), to download for each streaming segment. For example, a client may obtain a first streaming segment, for a video track, encoded at 250 Kb/sec (kilo-bits per second) (from one or more available streaming segment encodings for the first streaming segment), para [0024]); decode the retrieved encoded audio; and synchronize the decoded audio and the decoded video (For audio, the input device(s) 650 may be a sound card or similar device that accepts audio input in analog or digital form, or a CD-ROM reader that provides audio samples to the computing environment, para [0068]).

Regarding claim 32, Gu further teaches wherein the playback device is further configured to perform adaptive streaming using at least one EBML container file containing a subtitle track (a multiple bit rate video encoder encodes a plurality of video streams for multiple bit rate video streaming with an objective of providing a more consistent video quality, para [0008]).

Regarding claim 33, Gupta further teaches wherein the client application configures the processor to: subtitle track; retrieve subtitles from one of the at least one EBML container files containing a synchronize the subtitle with the decoded video (This process ensures that the total duration of video and audio content is identical in each stream. Another example of data interleaving is mixing a text or metadata stream, e.g., closed captioning or promotional data, with an existing audio and/or video stream, para [0047]); and overlay the subtitle over the decoded video (may include other data associated with the video content such as program guide information, metadata, and closed captioning text, para [0023]).

Regarding claim 34, Gupta further teaches wherein each of the EBML container files includes elements containing at least one subtitle track multiplexed with the encoded video (This process ensures that the total duration of video and audio content is identical in each stream. Another example of data interleaving is mixing a text or metadata stream, e.g., closed captioning or promotional data, with an existing audio and/or video stream, para [0047]).

Regarding claim 35, Gupta further teaches wherein the client application is configured to: retrieve portions of the EBML file containing elements that include portions of one of the subtitle tracks (This process ensures that the total duration of video and audio content is identical in each stream. Another example of data interleaving is mixing a text or metadata stream, e.g., closed captioning or promotional data, with an existing audio and/or video stream, para [0047]); synchronize the subtitles with the decoded video; and overlay the subtitles on the decoded video (may include other data associated with the video content such as program guide information, metadata, and closed captioning text, para [0023]).

Regarding claim 36, Gu teaches a method of performing adaptive bitrate streaming of media on a playback device (a multiple bit rate video encoder encodes a plurality of video streams for multiple bit rate video streaming with an objective of providing a more consistent video quality, para [0008]) using a plurality of alternative streams of encoded video packaged within extensible binary markup language (EBML) container files (utilizes the motion information to perform inter-frame coding of the predicted frames of the video content. The encoding can be performed according to a known video encoding standard, such as Windows Media Video format, SMPTE 421-M format, MPEG-x format (e.g., MPEG-1, MPEG-2, or MPEG-4), H.26.times. format (e.g., H.261, H.262, H.263, or H.264), or other format, para [0026]), where each of the alternative streams of video is the same source video encoded using different encoding parameters in such a way that each portion of encoded video packed into an element of an EBML container file (source video content is encoded into alternative bit streams at different coding rates and typically stored in the same media file at the server. This then allows the content to be streamed in segments or chunks at varying levels of quality corresponding to different coding rates according to the changing network conditions, para [0004]) commences with an intra frame starting a closed Group of Pictures (GOP) and each of the EBML container files includes at least one element that specifies the encoding parameters of the stream contained within the EBML container file (Video streams at intermediate bit rates are encoded at progressively decreasing variable bit rates (subject to decreasing peak and average bit rate constraints), para [0008]), the method comprising: retrieving top level index data that identifies each of the plurality of EBML container files and describes at least the maximum bitrate of each of the alternative streams contained within the EBML container files (generally having highest overall bit rate), the video encoder 200 encodes the video stream with a varying bit rate constrained to fall under a specified peak bit rate while satisfying a specified average bit rate. For the bottom MBR stream (generally having the lowest bit rate of the set), the video encoder uses a constant chunk rate approach. In the context of the multiple bit rate video streaming system, the term chunk refers to a group of pictures (GOP) into which the video stream are segmented, para [0042]); requesting a portion of at least one of the EBML container files that contains the at least one element that specifies the encoding parameters of the stream contained within the EBML container file (divides video of a multimedia program into multiple streaming segments, and contains a number of compressed bit streams representing the video segments at various bit rates, para [0020]); retrieving an index that references each element containing portions of encoded video within at least one of the EBML container files (the indexed file for multi bit rate streaming can be used by standard HTTP servers to serve multimedia content at multiple bit rates with bit rate selection (rate control) being performed client-side (e.g , exclusively client-side). Clients can perform rate control by first obtaining index information from the server describing the various bit rates available for streaming segments of a program, para [0022]); utilizing the index to request portions of a first EBML container file that includes elements that contain portions of encoded video (divided into temporal chunks called streaming segments (self-contained units). The server stores each

---continued in supplemental box---

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 11/66927

Supplemental Box

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

Continuation of:
Box No. V.2. Citations and explanations.

Claim 36 (continued): streaming segment at one or more bit rates (e.g., each streaming segment--bit rate combination is a separate streaming segment encoding). Each streaming segment includes one or more available bit rate encodings for a specific track, para [0024]); receiving and buffering the requested elements (Based on the index information, and possibly other information (e.g., network bandwidth, buffer information, etc.), the client can decide which bit rate streaming segments to download from the server to provide a desired user experience, para [0022]); decoding the encoded video contained within the buffered elements utilizing the encoding parameters (the video streams at the multiple bit rates can all be decoded and scaled to this same final display resolution in order to achieve a glitch free video presentation, para [0006]). Gu does not expressly teach parsing the top level index data to obtain information identifying the plurality of EBML container files; measuring current streaming conditions; and selecting another of the EBML container files from which to retrieve elements containing portions of encoded video for decoding, where the selection is based upon the measured streaming conditions and the description of the bitrate of the alternative stream contained within the top level index data. However Gupta, in an analogous art, teaches parsing the top level index data to obtain information identifying the plurality of EBML container files (enumerating and assigning each frame a timestamp, parsing the media file headers and footers, and computing format-specific "chunk" boundary points based on the indexable file portions, or chunks. The media content is stored in a source file data storage 125, and data about the media content is stored out-of-band from the media content in a content index, para [0022]); measuring current streaming conditions (the server 110 can measure the time between client reads of successive 64 kB chunks of content. This is a reasonable measurement of client 105 throughput because the standard internet networking architecture (routers, switches, etc.) have very small buffers, and thus, the rate at which the client is reading can be estimated in this way. The amount of network buffering may also be able to be determined by keeping statistics and probing each client's destination network or sub-net. Other factors that affect client networking speed (such as the required retransmission of TCP/IP network packets) can be known, measured, and accounted for as well, to give a more accurate estimation of client read speed, para [0080]); and selecting another of the EBML container files from which to retrieve elements containing portions of encoded video for decoding, where the selection is based upon the measured streaming conditions and the description of the bitrate of the alternative stream contained within the top level index data (Once the sending rate is adjusted 1060, the server 110 returns to selecting 1020 the next portion of content, modifying 1030 the content if necessary, and writing 1040 the portion to output. Following the writing 1040 step, the server 110 next determines 1070 whether more instructions apply to the requested media content. If the request includes more instructions, steps 1020-1040 repeat according to the next instruction. Once all instructions are processed and the altered media shot is formed from the selected frames, the server 110 serves 1080 any remaining portion of the combined media shot to the client , para [0083]). It would have been obvious to one skilled in the art to combine the teachings of Gu with those of Gupta in order to more efficiently adapt to multiple streaming bit rates in the video playback system of Gu (see Gupta para [0003]-[0004]).

Regarding claim 37, Gu teaches a source encoder configured to encode source video (a multiple bit rate video encoder encodes a plurality of video streams for multiple bit rate video streaming with an objective of providing a more consistent video quality, para [0008]) as a plurality of alternative video streams packed in container files , where the container files are extensible binary markup language (EBML) files, the source encoder comprising:a processor configured via a source encoding application to ingest at least one multimedia file containing a source video (utilizes the motion information to perform inter-frame coding of the predicted frames of the video content. The encoding can be performed according to a known video encoding standard, such as Windows Media Video format, SMPTE 421-M format, MPEG-x format (e.g., MPEG-1, MPEG-2, or MPEG-4), H.26 times. format (e.g., H.261, H.262, H.263, or H.264), or other format, para [0026]); wherein the source encoding application further configures the processor to: select a portion of the source video (source video content is encoded into alternative bit streams at different coding rates and typically stored in the same media file at the server. This then allows the content to be streamed in segments or chunks at varying levels of quality corresponding to different coding rates according to the changing network conditions, para [0004]); transcode the selected portion of the source video into a plurality of alternative portions of encoded video, where each alternative portion is encoded using a different set of encoding parameters and commences with an intra frame starting a closed Group of Pictures (GOP) (Video streams at intermediate bit rates are encoded at progressively decreasing variable bit rates (subject to decreasing peak and average bit rate constraints), para [0006]); write each of the alternative portions of encoded video to an element of a different EBML container file, where each element is located within an EBML container file that also includes another element that indicates the encoding parameters used to encode the alternative portion of encoded video (a server 110 (e.g., a server computer system such as a standard HTTP server) provides multimedia content to a client 120 (e.g., a client computer system, such as a laptop or desktop computer, or another type of computing device, such as a PDA or mobile phone) via a network, para [0020]). Gu does not expressly teach add an entry to at least one index that identifies the location of the element containing one of the alternative portions of encoded video within each of the EBML container files. However Gupta, in an analogous art, teaches add an entry to at least one index that identifies the location of the element containing one of the alternative portions of encoded video within each of the EBML container files (enumerating and assigning each frame a timestamp, parsing the media file headers and footers, and computing format-specific "chunk" boundary points based on the indexable file portions, or chunks. The media content is stored in a source file data storage 125, and data about the media content is stored out-of-band from the media content in a content index, para [0022]). It would have been obvious to one skilled in the art to combine the teachings of Gu with those of Gupta in order to more efficiently adapt to multiple streaming bit rates in the video playback system of Gu (see Gupta para [0003]-[0004]).

Regarding claim 38, Gu further teaches wherein transcoding a selected portion of the source video further comprises transcoding the selected portion into at least one closed group of pictures (term chunk refers to a group of pictures (GOP) into which the video stream are segmented, and define the level of granularity at which the video streaming system may switch playing individual segments between video streams. The constant chunk rate approach enables the video streaming system to guarantee predictability of streaming, para [0042]).

---continued in supplemental box---

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No. PCT/US 11/66927

Supplemental Box

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

Continuation of:
Box No. V.2. Citations and explanations

Claim 38 (continued): and the portion of encoded video in each of the Cluster elements commences with an intra frame and includes at least one closed group of pictures (video encoder then performs intra-frame coding of reference frames of the video content, and utilizes the motion information to perform inter-frame coding of the predicted frames of the video content, para [0026]).

Regarding claim 39, Gu further teaches wherein the portion of source video is selected based upon the duration of the selected portion of source video (constant chunk rate approach enables the video streaming system to guarantee predictability of streaming, in that when the lowest bit rate or quality video stream is streamed, the client will receive the chunk amount of pictures at the constant rate so as to maintain minimum quality continuous playing of the video, para [0042]).

Regarding claim 40, Gupta further teaches wherein the source encoding application configures the processor to select a portion of the source video having a duration of two seconds (request also includes a time range for each shot, specified as the starting time (e.g., in seconds into the content) and length (e.g., in seconds). For example, for shot 1, the starting time is 10 seconds (begin=10) and the length is 8 seconds (len=8). The request also includes an edit list that refers to a list of instructions for interleaving the four streams from shots 1-4, such that the new piece of content includes the video of each of shots 1-3 and the audio of shot, para [0055]).

Regarding claim 41, Gu further teaches wherein each of the alternative portions of encoded video is encoded with a different maximum bitrate (MBR engine controls the video encoder to produce an encoding of the video stream to meet the constant chunk rate constraint, which helps guarantee client side predictability for playing the streamed video. In intermediate video streams, the MBR engine causes the video encoder to encode the source video with encoding parameters to produce the video stream a variable bit rate falling within maximal peak and average bit rate constraints for the respective intermediate stream, para [0047]).

Regarding claim 42, Gupta further teaches wherein at least two of the alternative portions of encoded video are encoded with different resolutions (an identifier for the video encoding format and resolution. In this example, the row identifier includes multiple columns to specify the content index 130 data as discussed herein. Alternatively, all data for all chunks of a media file is stored in a single database row, using one or more columns, para [0028]).

Regarding claim 43, Gupta further teaches wherein at least two of the alternative portions of encoded video are encoded with different frame rates (an identifier for the video encoding format and resolution. In this example, the row identifier includes multiple columns to specify the content index 130 data as discussed herein. Alternatively, all data for all chunks of a media file is stored in a single database row, using one or more columns, para [0028]).

Regarding claim 44, Gupta further teaches wherein the element of the EBML container file to which each alternative portion of encoded video is written is a Cluster element containing a time code and the portion of encoded video is contained within BlockGroup elements within the Cluster element (In addition, the server 110 stores the relevant header and footer information, such as video resolution and frame rate, byte range of the portion of the file that is being composed, and other file format specific information, para [0040]).

Regarding claim 45, Gu further teaches wherein each encoded frame of the alternative portion of encoded video contained within the Cluster element is contained within a separate BlockGroup element (Between marked boundaries of a video sequence (sequence mark-in and sequence mark-out positions), the MBR encoding process 300 further determines a total number of group of pictures segments in which to divide the video sequence within user-specified constraints (such as a specified average GOP length and maximum allowed GOP length within a scene) and sets boundaries of each group of pictures, para [0046]).

Regarding claim 46, Gu further teaches wherein the first BlockGroup element in the Cluster element contains the IDR frame (MBR engine controls the video encoder to produce an encoding of the video stream to meet the constant chunk rate constraint, which helps guarantee client side predictability for playing the streamed video. In intermediate video streams, the MBR engine causes the video encoder to encode the source video with encoding parameters to produce the video stream a variable bit rate falling within maximal peak and average bit rate constraints for the respective intermediate stream, para [0047]).

Regarding claim 47, Gupta further teaches wherein the first BlockGroup element contains a Block element, which specifies the time code attribute of the IDR frame relative to the time code of the Cluster element (enumerating and assigning each frame a timestamp, parsing the media file headers and footers, and computing format-specific "chunk" boundary points based on the indexable file portions, or chunks, para [0022]).

Regarding claim 48, Gupta further teaches wherein each element to which each of the alternative portions of encoded video is written is assigned the same time code (enumerating and assigning each frame a timestamp, parsing the media file headers and footers, and computing format-specific "chunk" boundary points based on the indexable file portions, or chunks, para [0022]).

Regarding claim 49, Gupta further teaches wherein the source encoding application further configures the processor to create an index for each of the EBML container files (an identifier for the video encoding format and resolution. In this example, the row identifier includes multiple columns to specify the content index 130 data as discussed herein. Alternatively, all data for all chunks of a media file is stored in a single database row, using one or more columns, para [0028]).

Regarding claim 50, Gupta further teaches wherein the source encoding application further configures the processor to add the location of the element containing one of the alternative portions of encoded video within each of the EBML container files to the index for the EBML container file (an identifier for the video encoding format and resolution. In this example, the row identifier includes multiple columns to specify the content index 130 data as discussed herein. Alternatively, all data for all chunks of a media file is stored in a single database row, using one or more columns, para [0028]).

---continued in supplemental box---

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 11/66927

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:
Box No. V.2. Citations and explanations.

Regarding claim 51, Gupta further teaches wherein the source encoding application further configures the processor to pack the index for each EBML container file into the EBML container file (an identifier for the video encoding format and resolution. In this example, the row identifier includes multiple columns to specify the content index 130 data as discussed herein. Alternatively, all data for all chunks of a media file is stored in a single database row, using one or more columns, para [0028])

Regarding claim 52, Gupta further teaches wherein each index comprises a Cues element (computing format-specific "chunk" boundary points based on the indexable file portions, or chunks. The media content is stored in a source file data storage 125, and data about the media content is stored out-of-band from the media content in a content index 130, which can be queried using a content identifier, para [0022]).

Regarding claim 53, Gupta further teaches wherein each Cues element includes a CuePoint element that points to the location of the element containing one of the alternative portions of encoded video within the EBML file (enumerating and assigning each frame a timestamp, parsing the media file headers and footers, and computing format-specific "chunk" boundary points based on the indexable file portions, or chunks. The media content is stored in a source file data storage 125, and data about the media content is stored out-of-band from the media content in a content index, para [0022]).

Regarding claim 54, Gupta further teaches wherein the source encoding application further configures the processor to create a top level index file that identifies each of the EBML container files (an identifier for the video encoding format and resolution. In this example, the row identifier includes multiple columns to specify the content index 130 data as discussed herein. Alternatively, all data for all chunks of a media file is stored in a single database row, using one or more columns, para [0028]).

Regarding claim 55, Gu further teaches wherein the ingested multimedia file also includes source audio (Each streaming segment includes one or more available bit rate encodings for a specific track (e.g., a specific audio track, such as an English audio track, or a specific video track) of a program. Clients then determine which bit rate, from the available bit rates (e.g., from the available streaming segment encodings), to download for each streaming segment. For example, a client may obtain a first streaming segment, for a video track, encoded at 250 Kb/sec (kilo-bits per second) (from one or more available streaming segment encodings for the first streaming segment), para [0024]).

Regarding claim 56, Gu further teaches wherein the source encoding application configures the processor to multiplex the audio into each of the EBML container files (Each streaming segment includes one or more available bit rate encodings for a specific track (e.g., a specific audio track, such as an English audio track, or a specific video track) of a program. Clients then determine which bit rate, from the available bit rates (e.g., from the available streaming segment encodings), to download for each streaming segment. For example, a client may obtain a first streaming segment, for a video track, encoded at 250 Kb/sec (kilo-bits per second) (from one or more available streaming segment encodings for the first streaming segment), para [0024]).

Regarding claim 57, Gu further teaches wherein the source encoding application configures the processor to write the audio to a separate EBML container file (Each streaming segment includes one or more available bit rate encodings for a specific track (e.g., a specific audio track, such as an English audio track, or a specific video track) of a program. Clients then determine which bit rate, from the available bit rates (e.g., from the available streaming segment encodings), to download for each streaming segment. For example, a client may obtain a first streaming segment, for a video track, encoded at 250 Kb/sec (kilo-bits per second) (from one or more available streaming segment encodings for the first streaming segment), para [0024]).

Regarding claim 58, Gu further teaches wherein the source encoding application further configures the processor to transcode at least one of the at least one audio tracks (Video streams at intermediate bit rates are encoded at progressively decreasing variable bit rates (subject to decreasing peak and average bit rate constraints), para [0008]).

Regarding claim 59, Gupta further teaches wherein the ingested multimedia file further comprises subtitles (This process ensures that the total duration of video and audio content is identical in each stream. Another example of data interleaving is mixing a text or metadata stream, e.g., closed captioning or promotional data, with an existing audio and/or video stream, para [0047]).

Regarding claim 60, Gupta further teaches wherein the source encoding application configures the processor to multiplex the subtitles into each of the EBML container files (This process ensures that the total duration of video and audio content is identical in each stream. Another example of data interleaving is mixing a text or metadata stream, e.g., closed captioning or promotional data, with an existing audio and/or video stream, para [0047]).

Regarding claim 61, Gupta further teaches wherein the source encoding application configures the processor to write the subtitles to a separate EBML container file (This process ensures that the total duration of video and audio content is identical in each stream. Another example of data interleaving is mixing a text or metadata stream, e.g., closed captioning or promotional data, with an existing audio and/or video stream, para [0047]).

Regarding claim 62, Gu further teaches wherein the source encoding application further configures the processor to transcode the source video to create a lower frame rate trick play track and to write the trick play track to a separate EBML container file (Each streaming segment includes one or more available bit rate encodings for a specific track (e.g., a specific audio track, such as an English audio track, or a specific video track) of a program. Clients then determine which bit rate, from the available bit rates (e.g., from the available streaming segment encodings), to download for each streaming segment. For example, a client may obtain a first streaming segment, for a video track, encoded at 250 Kb/sec (kilo-bits per second) (from one or more available streaming segment encodings for the first streaming segment), para [0024]).

---continued in supplemental box---

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No. PCT/US 11/66927

Supplemental Box

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

Continuation of:
Box No. V.2. Citations and explanations.

Regarding claim 63, Gu further teaches wherein the trick play track is also lower resolution than the source video (Each streaming segment includes one or more available bit rate encodings for a specific track (e.g., a specific audio track, such as an English audio track, or a specific video track) of a program. Clients then determine which bit rate, from the available bit rates (e.g., from the available streaming segment encodings), to download for each streaming segment. For example, a client may obtain a first streaming segment, for a video track, encoded at 250 Kb/sec (kilo-bits per second) (from one or more available streaming segment encodings for the first streaming segment), para [0024]).

Regarding claim 64, Gu further teaches wherein the source encoding application further configures the processor to write the element containing a set of encoding parameters in each of the EBML container files (Each streaming segment includes one or more available bit rate encodings for a specific track (e.g., a specific audio track, such as an English audio track, or a specific video track) of a program. Clients then determine which bit rate, from the available bit rates (e.g., from the available streaming segment encodings), to download for each streaming segment. For example, a client may obtain a first streaming segment, for a video track, encoded at 250 Kb/sec (kilo-bits per second) (from one or more available streaming segment encodings for the first streaming segment), para [0024]).

Regarding claim 65, Gupta further teaches wherein the set of encoding parameters includes at least one parameter selected from the group consisting of frame rate, frame height, frame width, sample aspect ratio, maximum bitrate, and minimum buffer size (an identifier for the video encoding format and resolution. In this example, the row identifier includes multiple columns to specify the content index 130 data as discussed herein. Alternatively, all data for all chunks of a media file is stored in a single database row, using one or more columns, para [0028]).

Regarding claim 66, Gu teaches a method of encoding source video as a plurality of alternative streams packed in extensible binary markup language (EBML) files using a source encoder (utilizes the motion information to perform inter-frame coding of the predicted frames of the video content. The encoding can be performed according to a known video encoding standard, such as Windows Media Video format, SMPTE 421-M format, MPEG-x format (e.g., MPEG-1, MPEG-2, or MPEG-4), H.26.times. format (e.g., H.261, H.262, H.263, or H.264), or other format, para [0026]), the method comprising: repeatedly selecting a portion of the source video using the source encoder (source video content is encoded into alternative bit streams at different coding rates and typically stored in the same media file at the server. This then allows the content to be streamed in segments or chunks at varying levels of quality corresponding to different coding rates according to the changing network conditions, para [0004]); transcoding the selected portion of the source video into a plurality of alternative portions of encoded video using the source encoder, where each alternative portion is encoded using a different set of encoding parameters and commences with an intra frame starting a closed Group of Pictures (GOP) (Video streams at intermediate bit rates are encoded at progressively decreasing variable bit rates (subject to decreasing peak and average bit rate constraints), para [0008]); writing each of the alternative portions of encoded video to an element of a different EBML container file using the source encoder, where each element is located within an EBML container file that also includes another element containing a set of encoding parameters corresponding to the encoding parameters used to encode the portion of video (a server 110 (e.g., a server computer system such as a standard HTTP server) provides multimedia content to a client 120 (e.g., a client computer system, such as a laptop or desktop computer, or another type of computing device, such as a PDA or mobile phone) via a network, para [0020]). Gu does not expressly teach adding an entry to at least one index that identifies the location of the element containing one of the alternative portions of encoded video within each of the EBML container files. However Gupta, in an analogous art, teaches adding an entry to at least one index that identifies the location of the element containing one of the alternative portions of encoded video within each of the EBML container files (enumerating and assigning each frame a timestamp, parsing the media file headers and footers, and computing format-specific "chunk" boundary points based on the indexable file portions, or chunks. The media content is stored in a source file data storage 125, and data about the media content is stored out-of-band from the media content in a content index, para [0022]). It would have been obvious to one skilled in the art to combine the teachings of Gu with those of Gupta in order to more efficiently adapt to multiple streaming bit rates in the video playback system of Gu (see Gupta para [0003]-[0004]).

Claims 1-66 have industrial applicability as defined by PCT Article 33(4) because the subject matter can be made or used in industry.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference G2353AB.PCT	FOR FURTHER ACTION	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US2011/067167	International filing date *(day/month/year)* 23 December 2011	(Earliest) Priority Date *(day/month/year)* 05 January 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 4 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. 1

   ☒ 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/US2011/067167

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

See Extra Sheet.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:
1-28

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0154
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2011/067167

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06T 11/00 (2012.01)
USPC - 345/471
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) - G06T 11/00; H04N 5/228, 5/262, 7/00 (2012.01)
USPC - 345/467, 471; 348/222.1, 239, 468

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2009/0303241 A1 (PRIYADARSHI et al) 10 December 2009 (10.12.2009) entire document	1-25
Y	WO 2010/060106 A1 (KOHLI et al) 27 May 2010 (27.05.2010) entire document	1-25
Y	US 2009/0132599 A1 (SOROUSHIAN et al) 21 May 2009 (21.05.2009) entire document	18-23
A	US 2009/0307258 A1 (PRIYADARSHI et al) 10 December 2009 (10.12.2009) entire document	1-25

☐ 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 2012	02 JUL 2012

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

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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2011/067187

Continuation of Box III

This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1. In order for all inventions to be examined, the appropriate additional examination fees must be paid.

Group I, claims 1-25, drawn to a method of playing back encoded media and a playback device, comprising requesting and buffering portions of video from at least one of alternative streams using a playback device; requesting information indicative of a font utilized by a font-rendering engine to render text from a selected subtitle stream, device; downloading at least one font file when the font is not present on the playback requesting and buffering at least a portion of the selected subtitle stream; decoding the buffered portions of video using a decoder on the playback device; rendering the portions of the subtitle stream corresponding to the buffered portion of video using a font-rendering engine configured by the at least one downloaded font file; and performing synchronized playback of the decoded video and rendered subtitles using the playback device.

Group II, claims 26-43, drawn to method of encoding source media and a source encoder, comprising: selecting a portion of the source media using a source encoder; transcoding the selected portion of the source media into a plurality of alternative portions of encoded video using the source encoder, where each alternative portion is encoded using a different set of encoding parameters and commences with an intra frame at the start of a closed group of pictures (GOP); writing each of the alternative portions of encoded video to a separate container file using the source encoder; writing a subtitle stream segment from each subtitle track corresponding to the selected portion of the source media to a separate container file using the source encoder; and associating a font file with at least one of the container files containing subtitle stream segments.

The inventions listed as Groups I-II do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons: the special technical feature of the Group I invention: requesting and buffering portions of video from at least one of alternative streams using a playback device; requesting information indicative of a font utilized by a font-rendering engine to render text from a selected subtitle stream; device, downloading at least one font file when the font is not present on the playback requesting and buffering at least a portion of the selected subtitle stream; decoding the buffered portions of video using a decoder on the playback device; rendering the portions of the subtitle stream corresponding to the buffered portion of video using a font-rendering engine configured by the at least one downloaded font file; and performing synchronized playback of the decoded video and rendered subtitles using the playback device as claimed therein is not present in the invention of Group II. The special technical feature of the Group II invention: selecting a portion of the source media using a source encoder; transcoding the selected portion of the source media into a plurality of alternative portions of encoded video using the source encoder, where each alternative portion is encoded using a different set of encoding parameters and commences with an intra frame at the start of a closed group of pictures (GOP); writing each of the alternative portions of encoded video to a separate container file using the source encoder; writing a subtitle stream segment from each subtitle track corresponding to the selected portion of the source media to a separate container file using the source encoder; and associating a font file with at least one of the container files containing subtitle stream segments as claimed therein is not present in the invention of Groups I.

Groups I and II lack unity of invention because even though the inventions of these groups require the technical feature of encoding media including at least one subtitle track, where the media is encoded as a plurality of alternative video streams and at least one subtitle stream, using a source encoder, this technical feature is not a special technical feature as it does not make a contribution over the prior art in view of US 2009/0307258 A1 (PRIYARDARSHI et al) 10 December 2009 (10.12.2009) paragraphs [0021], [0048], [0067], [0069], claim 20.

Since none of the special technical features of the Group I or II inventions are found in more than one of the inventions, unity of invention is lacking.

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

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

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

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	02 JUL 2012
Applicant's or agent's file reference 02353AB.PCT	FOR FURTHER ACTION See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2011/067167	23 December 2011	05 January 2011

International Patent Classification (IPC) or both national classification and IPC
IPC(8) - G06T 11/00 (2012.01)
USPC - 345/471

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 2012	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/US2011/067167

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:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2011/057187

Box No. IV Lack of unity of invention

1. ☒ In response to the invitation (Form PCT/ISA/206) to pay additional fees the applicant has, within the applicable time limit:

☐ paid additional fees

☐ paid additional fees under protest and, where applicable, the protest fee

☐ paid additional fees under protest but the applicable protest fee was not paid

☒ not paid additional fees

2. ☐ This Authority found that the requirement of unity of invention is not complied with and chose not to invite the applicant to pay additional fees.

3. This Authority considers that the requirement of unity of invention in accordance with Rule 13.1, 13.2 and 13.3 is

☐ complied with

☒ not complied with for the following reasons:

This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1. In order for all inventions to be examined, the appropriate additional examination fees must be paid.

Group I, claims 1-25, drawn to a method of playing back encoded media and a playback device, comprising requesting and buffering portions of video from at least one of alternative streams using a playback device; requesting information indicative of a font utilized by a font-rendering engine to render text from a selected subtitle stream; device; downloading at least one font file when the font is not present on the playback requesting and buffering at least a portion of the selected subtitle stream; decoding the buffered portions of video using a decoder on the playback device; rendering the portions of the subtitle stream corresponding to the buffered portion of video using a font-rendering engine configured by the at least one downloaded font file; and performing synchronized playback of the decoded video and rendered subtitles using the playback device.

Group II, claims 26-43, drawn to method of encoding source media and a source encoder, comprising: selecting a portion of the source media using a source encoder; transcoding the selected portion of the source media into a plurality of alternative portions of encoded video using the source encoder, where each alternative portion is encoded using a different set of encoding parameters and commences with an intra frame at the start of a closed group of pictures (GOP); writing each of the alternative portions of encoded video to a separate container file using the source encoder; writing a subtitle stream segment from each subtitle track corresponding to the selected portion of the source media to a separate container file using the source encoder; and associating a font file with at least one of the container files containing subtitle stream segments.

The inventions listed as Groups I-II do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons: the special technical feature of the Group I invention: requesting and buffering portions of video from at least one of alternative streams using a playback device; requesting information indicative of a font utilized by a font-rendering engine to render text from a selected subtitle stream; device; downloading at least one font file when the font is not present on the playback requesting and buffering at least a portion of the selected subtitle stream; decoding the buffered portions of video using a decoder on the playback device, rendering the portions of the subtitle stream corresponding to the buffered portion of video using a font-rendering engine configured by the at least one downloaded font file; and performing synchronized playback of the decoded video and rendered subtitles using the playback device as claimed therein is not present in the invention of Group II. The special technical feature of the Group II invention: selecting a portion of the source media using a source encoder; transcoding the selected portion of the source media into a plurality of alternative portions of encoded video using the source encoder, where each alternative portion is encoded using a different set of encoding parameters and commences with an intra frame at the start of a closed group of pictures (GOP); writing each of the alternative portions of encoded video to a separate container file using the source encoder; writing a subtitle stream segment from each subtitle track corresponding to the selected portion of the source media to a separate container file using the source encoder; and associating a font file with at least one of the container files containing subtitle stream segments as claimed therein is not present in the invention of Groups I.

Groups I and II lack unity of invention because even though the inventions of these groups require the technical feature of encoding media including at least one subtitle track, where the media is encoded as a plurality of alternative video streams and at least one subtitle stream, using a source encoder, this technical feature is not a special technical feature as it does not make a contribution over the prior art in view of US 2009/0307258 A1 (PRIYARDARSHI et al) 10 December 2009 (10.12.2009) paragraphs [0021], [0048], [0067], [0069], claim 20.

Since none of the special technical features of the Group I or II inventions are found in more than one of the inventions, unity of invention is lacking.

4. Consequently, this opinion has been established in respect of the following parts of the international application:

☐ all parts

☒ the parts relating to claims Nos. 1-25

Form PCT/ISA/237 (Box No. IV) (July 2011)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2011/067167

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

1. Statement

Novelty (N)	Claims	1-25	YES
	Claims	None	NO
Inventive step (IS)	Claims	None	YES
	Claims	1-25	NO
Industrial applicability (IA)	Claims	1-25	YES
	Claims	None	NO

2. Citations and explanations:

Claims 1-17 and 24-25 lack an inventive step under PCT Article 33(3) as being obvious over Priyadarshi et al. (US 2009/0303241 A1; hereinafter Priyadarshi) in view of Kohli et al. (WO 2010/060106 A1; hereinafter Kohli).

Regarding claim 1, Priyadarshi discloses a method of playing back encoded media (Fig. 1 and Paragraphs [0005], [0027] and [0030]; the invention is to a playback system that displays multimedia files with rendered font and text subtitles that match the video file. The multimedia presentation is analyzed by an encoder/decoder to determine the unique character for each movie/video), where the media is encoded as a stream and at least one subtitle stream (Fig. 6, Paragraphs [0027], [0030] and [0036]; the stream of data includes encoded movie stream data and subtitle information that corresponds to the movie data. With the subtitle information being several font files (31, 32, 33) that correspond to the over time stream of video data), the method comprising: requesting and buffering portions of video from at least one stream using a playback device (Fig. 4 and Paragraph [0031]; video textual elements are sent to a character buffer for playback processing); requesting information indicative of a font utilized by a font-rendering engine to render text from a selected subtitle stream (Fig. 6 and Paragraphs [0021], [0026]-[0027] and [0036]; font files are used by a rendering module (font-rendering engine) to render the text or characters displayed with the movie stream); downloading at least one font file when the font is not present on the playback device (Paragraphs [0020], [0035] and [0038]; the necessary font files can be downloaded as an attachment); requesting and buffering at least a portion of the selected subtitle stream (Fig. 4 and Paragraph [0031]; video textual elements are sent to a character buffer for playback processing); decoding the buffered portions of video using a decoder on the playback device (Paragraphs [0030]-[0031] and [0033]; the buffered portions can be sent to a decoder for decoding of the text, audio and video portions); rendering the portions of the subtitle stream corresponding to the buffered portion of video using a font-rendering engine configured by the at least one downloaded font file (Fig. 6 and Paragraphs [0021], [0026]-[0027] and [0036]; font files are used by a rendering module (font-rendering engine) to render the text or characters displayed with the movie stream), and performing synchronized playback of the decoded video and rendered subtitles using the playback device (Fig. 6 and Paragraph [0036]; using start and end time code values the font files (31, 32, 33) are associated (synchronized) with their corresponding decoded video presentation timeline segments). Priyadarshi does not disclose wherein the streams are a plurality of alternative streams. However in disclosing a system of streaming media content (Abstract), Kohli teaches wherein the streams are a plurality of alternative streams (Figs. 1 and 5 and Paragraphs [0027], [0030] and [0162]; multiple media flow directors (alternative streams) can be used to deliver and stream media content to a user device). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to include wherein the streams are a plurality of alternative streams in the invention of Priyadarshi as taught by Kohli, so the multiple media flow directors can be used to efficiently deliver the media content to a user (Kohli; Paragraph [0162]).

Regarding claim 2, Priyadarshi discloses the method of claim 1, but Priyadarshi does not disclose measuring the current streaming conditions by measuring the time taken to receive requested portions of a stream from the time at which the portions were requested. Kohli teaches measuring the current streaming conditions by measuring the time taken to receive requested portions of a stream from the time at which the portions were requested (Paragraph [0160]; the system measures the delays from streaming to displaying the video and sets the buffer at a setting that covers for these delays). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to include measuring the current streaming conditions by measuring the time taken to receive requested portions of a stream from the time at which the portions were requested in the invention of Priyadarshi as taught by Kohli, so the delays can be covered (Kohli; Paragraph [0160]).

Regarding claim 3, Priyadarshi discloses the method of claim 2, but Priyadarshi does not disclose wherein requesting and buffering portions of video from at least one of the alternative streams using a playback device further comprises requesting and buffering portions of video from at least one of the alternative streams based upon the bitrates of the alternative streams and the measured streaming conditions using a playback device. Kohli teaches wherein requesting and buffering portions of video from at least one of the alternative streams using a playback device further comprises requesting and buffering portions of video from at least one of the alternative streams based upon the bitrates of the alternative streams and the measured streaming conditions using a playback device (Paragraphs [0142], [0159]-[0160]; the requested stream can be video from a server at a particular bit rate that suits the clients needs. The requested streams are then buffered to overcome delays as previously disclosed). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to include wherein requesting and buffering portions of video from at least one of the alternative streams using a playback device further comprises requesting and buffering portions of video from at least one of the alternative streams based upon the bitrates of the alternative streams and the measured streaming conditions using a playback device in the invention of Priyadarshi as taught by Kohli, so the delays can be covered and a set bit rate file can be sent to the client (Kohli; Paragraphs [0159]-[0160]).

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0160
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2011/067167

Supplemental Box

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

Regarding claim 4, Priyadarshi discloses the method of claim 1, wherein the selected subtitle stream is stored within a container file that includes the font file as an attachment to the container file (Paragraphs [0021] and [0038], the font files for the subtitles are electronic data files containing a set of representations for displaying characters or symbols where the containers can include an attachment link).

Regarding claim 5, Priyadarshi discloses the method of claim 4, wherein the container file in which the selected subtitle stream is stored includes a separate element containing metadata describing the attached font file (Paragraph [0038] and Claim 11; the font file can include metadata tags in the file such as the description, start time and end time for each attachment).

Regarding claim 6, Priyadarshi discloses the method of claim 5, further comprising determining whether the font file is present on the playback device without downloading the font file by requesting the metadata describing the attached font file from the container file using the playback device (Fig. 6 and Paragraph [0038]; using the description in each multimedia container the system can determine if an attachment font link is/file is necessary for each time period in a movie).

Regarding claim 7, Priyadarshi discloses the method of claim 5, wherein the metadata describing the attached font file includes a description of the font file and the location of the font file within the container file (Fig. 6 and Paragraph [0038]; using the description in each multimedia container the system can determine if an attachment font link is/file is necessary for each time period in a movie).

Regarding claim 8, Priyadarshi discloses the method of claim 1, but Priyadarshi does not disclose wherein the font file is compressed and the method further ~~comprises~~ decompressing the downloaded font file using the playback device. Kohli teaches wherein the font file is compressed and the method further comprises decompressing the downloaded font file using the playback device (Paragraph [0080]; the video information can include compressed and/uncompressed video data and video attributes (font files)). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to include wherein the font file is compressed and the method further comprises decompressing the downloaded font file using the playback device in the invention of Priyadarshi as taught by Kohli, so space can be conserved (Kohli, Paragraphs [0080]).

Regarding claim 9, Priyadarshi discloses the method of claim 1, but Priyadarshi does not disclose wherein the selected subtitle stream is selected by the playback device in response to a user instruction. However turning on subtitles on a movie is a known practice in the art and would simply be a matter of inventor design choice. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to include wherein the selected subtitle stream is selected by the playback device in response to a user instruction in the invention of Priyadarshi so users can see corresponding text to videos if necessary or desired.

Regarding claim 10, Priyadarshi discloses the method of claim 1, but Priyadarshi does not disclose displaying a user interface indicative of the estimated time to download the at least one font file using the playback device. However displaying download information such as estimated download time in a media related system is a known practice in the art and the specifics would simply be a matter of inventor design choice. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to include displaying a user interface indicative of the estimated time to download the at least one font file using the playback device in the invention of Priyadarshi so users can see how long till their media file is done downloading and plan their time accordingly.

Regarding claim 11, Priyadarshi discloses the method of claim 1, wherein the subtitle stream is encoded as Unicode text (Paragraph [0005]; the fonts/subtitles can be encoded using Unicode encoding).

Regarding claim 12, Priyadarshi discloses the method of claim 1, wherein requesting and buffering at least a portion of the selected subtitle stream comprises downloading and buffering the entire subtitle stream prior to the commencement of playback (Paragraph [0031]; all textual elements (subtitles) can be extracted, buffered and then decoded for playback)

Regarding claim 13, Priyadarshi discloses the method of claim 1, wherein requesting and buffering at least a portion of the selected subtitle stream comprises requesting and buffering segments of the subtitle stream with timing corresponding to the timing of the portions of video requested by the playback device (Fig. 6 and Paragraphs [0033] and [0036]; the font file portions can be segmented to smaller sized segments that correspond to time segments within the overall movie timeline as shown in figure 6).

Regarding claim 14, Priyadarshi discloses the method of claim 13, wherein the font used to render the subtitle track is contained within a plurality of font files and at least one of the plurality of font files corresponds to a segment of the subtitle stream (Fig. 6 and Paragraphs [0033] and [0036], the font file portions can be segmented to smaller sized segments that correspond to time segments within the overall movie timeline as shown in figure 6), the method further comprising downloading the font file corresponding to a segment of the subtitle stream when the playback device requests the segment of the subtitle stream (Paragraphs [0036] and [0038]; font files corresponding to a particular time can be attached/downloaded as necessary to display subtitles during that time period).

Regarding claim 15, Priyadarshi discloses the method of claim 14, wherein the font used to render the subtitle track is active according to an associated start timecode and end timecode, and the start and end timecodes are independent of the subtitle segment times (Paragraph [0036]; the fonts rendered for each time periods can be downloaded based on font attachment file start and end times).

Regarding claim 16, Priyadarshi discloses the method of claim 15, wherein start and end timecodes for a plurality of font segments overlap, and lead to multiple font segments being utilized for rendering subtitles at a given time (Paragraphs [0036] and [0036]; the video can have multiple font files which are associated with the overall timeline with all the files being attached to the movie based on a corresponding start and end time of the font attachment file).

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2011/067167

Supplemental Box

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

Continuation of:

Regarding claim 17, Priyadarshi discloses the method of claim 1, wherein the streams and the subtitle stream are stored in separate container files (Paragraphs [0036] and [0038]; the video can have multiple font container files which are associated with the overall timeline with all the files being attached to the movie based on a corresponding start and end time of the font attachment file). Priyadarshi does not disclose wherein requesting portions of a stream further comprising requesting portions of files from remote servers via Hypertext Transfer Protocol (HTTP) byte range requests using the playback device. Kohli teaches wherein requesting portions of a stream further comprising requesting portions of files from remote servers via Hypertext Transfer Protocol (HTTP) byte range requests using the playback device (Paragraphs [0114]-[0115]; the server can be a HTTP server and the client can request content by byte ranges). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to include wherein requesting portions of a stream further comprising requesting portions of files from remote servers via Hypertext Transfer Protocol (HTTP) byte range requests using the playback device in the invention of Priyadarshi as taught by Kohli, so the managing device can server the appropriate content to the user (Kohli; Paragraphs [0114]-[0115]).

Regarding claim 24, Priyadarshi discloses the method of claim 1, but Priyadarshi does not disclose retrieving a top level index file using the playback device that identifies the alternative streams and identifies at least one subtitle stream. Kohli teaches retrieving a top level index file using the playback device that identifies the alternative streams and identifies at least one subtitle stream (Paragraph [0041]; the video file format information (which include the subtitle information as previously disclosed) can be stored in a server side index table (top level index file) that can be used to quickly be used to find the associated frame for each new bit rate video stream). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to include retrieving a top level index file using the playback device that identifies the alternative streams and identifies at least one subtitle stream in the invention of Priyadarshi as taught by Kohli, so the index can be used to quickly find the associated frame for each new bit rate video stream (Kohli; Paragraph [0041]).

Regarding claim 25, Priyadarshi discloses a playback device configured to playback encoded media (Fig. 1 and Paragraphs [0006], [0027] and [0030]; the invention is to a playback system that displays multimedia files with rendered font and text subtitles that match the video file. The multimedia presentation is analyzed by an encoder/decoder to determine the unique character for each movie/video), where the media is encoded as a stream and at least one subtitle stream (Fig. 6, Paragraphs [0027], [0030] and [0036]; the stream of data includes encoded movie stream data and subtitle information that corresponds to the movie data. With the subtitle information being several font files (31, 32, 33) that correspond to the over time stream of video data), the playback device comprising: a processor configured to request portions of files (Paragraph [0010]; the system includes a processor that is configured to extract/request text data from a multimedia file having audio and video data) wherein the processor is configured to: request and buffer portions of video from at least one of the streams (Fig. 4 and Paragraph [0031]; video textual elements are sent to a character buffer for playback processing); request information indicative of a font utilized by a font-rendering engine to render text from a selected subtitle stream (Fig. 6 and Paragraphs [0021], [0026]-[0027] and [0038]; font files are used by a rendering module (font-rendering engine) to render the text or characters displayed with the movie stream); download at least one font file when the font is not present on the playback device (Paragraphs [0020], [0035] and [0038]; the necessary font files can be downloaded as an attachment); request and buffer at least a portion of the selected subtitle stream (Fig. 4 and Paragraph [0031]; video textual elements are sent to a character buffer for playback processing); decode the buffered portions of video (Paragraphs [0030]-[0031] and [0033]; the buffered portions can be sent to a decoder for decoding of the text, audio and video portions); render the portions of the subtitle stream corresponding to the buffered portion of video using a font-rendering engine configured by the at least one downloaded font file (Fig. 6 and Paragraphs [0021], [0026]-[0027] and [0038]; font files are used by a rendering module (font-rendering engine) to render the text or characters displayed with the movie stream); and perform synchronized playback of the decoded video and rendered subtitles (Fig. 6 and Paragraph [0038]; using start and end time code values the font files (31, 32, 33 - subtitles) are associated (synchronized) with their corresponding decoded video presentation timeline segments). Priyadarshi does not disclose wherein the streams are a plurality of alternative streams; wherein the processor is configured by a client application; wherein the requested portions are from a remote server. However in disclosing a system of streaming media content (Abstract), Kohli teaches wherein the streams are a plurality of alternative streams (Figs. 1 and 5 and Paragraphs [0027], [0030] and [0162]; multiple media flow directors (alternative streams) can be used to deliver and stream media content to a user device), wherein the processor is configured by a client application (Paragraph [0166]; the system can have an input device that receives and sends client commands (client application) to the processor); wherein the requested portions are from a remote server (Paragraphs [0151] and [0173]; the requested code information can be received from a remote server (630)). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to include wherein the streams are a plurality of alternative streams; wherein the processor is configured by a client application; wherein the requested portions are from a remote server in the invention of Priyadarshi as taught by Kohli, so the multiple media flow directors can be used to efficiently deliver the media content to a user (Kohli; Paragraph [0162]).

Claims 18-23 lack an inventive step under PCT Article 33(3) as being obvious over Priyadarshi et al. (US 2009/0303241 A1; hereinafter Priyadarshi) in view of Kohli et al. (WO 2010/060106 A1; hereinafter Kohli) in further view of Soroushian et al. (US 2009/0132599 A1; hereinafter Soroushian).

Regarding claim 18, Priyadarshi discloses the method of claim 1, but Priyadarshi does not disclose wherein the alternative streams and the subtitle stream are stored in separate Extensible Binary Markup Language (EBML) container files. However in disclosing a playback and distribution system (Abstract), Soroushian teaches wherein the alternative streams and the subtitle stream are stored in separate Extensible Binary Markup Language (EBML) container files (Fig. 9 and Paragraph [0042]; media files (which would include the subtitles) are stored in extensible Binary Meta Language (EBML) elements (containers)). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to include wherein the alternative streams and the subtitle stream are stored in separate Extensible Binary Markup Language (EBML) container files in the invention of Priyadarshi as taught by Soroushian, so the media file can be easily indexed (Soroushian; Paragraph [0042]).

Form PCT/ISA/237 (Supplemental Box) (July 2011)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2011/067167

Supplemental Box

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

Regarding claim 19, Priyadarshi discloses the method of claim 18, wherein each of the container files comprises a plurality of Cluster elements, where each Cluster element contains a portion of encoded media (Fig. 6 and Paragraphs [0033] and [0036]; the font file portions can be segmented in smaller sized segments (clusters) that correspond to time segments within the overall movie timeline as shown in figure 6). But Priyadarshi does not disclose wherein the container files are EBML container files. However in disclosing a playback and distribution system (Abstract), Soroushian teaches wherein the container files are EBML container files. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to include wherein the container files are EBML container files in the invention of Priyadarshi as taught by Soroushian, so the media file can be easily indexed (Soroushian; Paragraph [0042]).

Regarding claim 20, Priyadarshi discloses the method of claim 19, wherein the portions of encoded media in each of the Cluster elements have the same duration (Paragraph [0037]; the font files can all be of an approximate equal size and duration).

Regarding claim 21, Priyadarshi discloses the method of claim 20, but Priyadarshi does not disclose wherein the portions of encoded media in each of the Cluster elements have a 2 second duration. However setting a segment to a particular duration is disclosed by Priyadarshi as disclosed in claim 20 and specifically setting the duration to 2 seconds would simply be a matter of inventor design choice. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to include wherein the portions of encoded media in each of the Cluster elements have a 2 second duration in the invention of Priyadarshi, so the font files can all span an approximately equal amount of time within a movie (Priyadarshi; Paragraph [0037]).

Regarding claim 22, Priyadarshi discloses the method of claim 18, wherein the container file containing the selected subtitle stream includes at least one font file as an attachment to the container file (Paragraphs [0021] and [0036]; the font files for the subtitles are electronic data files containing a set of representations for displaying characters or symbols where the containers can include an attachment link). But Priyadarshi does not disclose wherein the container files are EBML container files. However in disclosing a playback and distribution system (Abstract), Soroushian teaches wherein the container files are EBML container files. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to include wherein the container files are EBML container files in the invention of Priyadarshi as taught by Soroushian, so the media file can be easily indexed (Soroushian; Paragraph [0042]).

Regarding claim 23, Priyadarshi discloses the method of claim 22, but Priyadarshi does not disclose wherein the at least one font file attached to the container file are compressed. Kohli teaches wherein the at least one font file attached to the container file are compressed (Paragraph [0080]; the video information can include compressed and/uncompressed video data and video attributes (font files)). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to include wherein the at least one font file attached to the container file are compressed in the invention of Priyadarshi as taught by Kohli, so space can be conserved (Kohli; Paragraphs [0080]).

Claims 1-25 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.

Form PCT/ISA/237 (Supplemental Box) (July 2011)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 53684P/DS79	FOR FURTHER ACTION	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US05/25845	International filing date (*day/month/year*) 21 July 2005 (21.07.2005)	(Earliest) Priority Date (*day/month/year*) 21 July 2004 (21.07.2004)
Applicant DIVXNETWORKS, INC.		

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 3 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. ☐ 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(b), 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. 4
      ☒ 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) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US05/25845

Box IV TEXT OF THE ABSTRACT (Continuation of Item 5 of the first sheet)

A media player (105) manages and controls rights to playback of media content (403) by the media player, which stores, during a registration (401) process in which the media player need not be connected to an external computing system, information (402) used by the media player to control playback. A minimal amount of the media player's memory is used to store the information used to control playback.

PAGE 6/12 * RCVD AT 5/24/2007 1:36:25 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/2 * DNIS:2738300 * CSID:19494768640 * DURATION (mm-ss):02-38

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US05/25845

A. CLASSIFICATION OF SUBJECT MATTER
IPC: G06F 12/14(2006.01);G06F 17/30(2006.01);H04L 9/00(2006.01)
H04N 7/16(2006.01)

USPC: 705/59;726/26
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)
U.S. : 705/59; 726/26

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,509,070 (SCHULL) 16 April 1996 (16.04.1996), column 8, line 31 to column 9, line 53; column 10, lines 26-58; column 14 line 56 to column 15, line 35).	1-24

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

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

"E" earlier application or patent 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
05 February 2007 (05.02.2007)	10 MAY 2007
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 Matthew Heneghan Telephone No. (571)272-2100 DEBORAH A. THOMAS PARALEGAL SPECIALIST

Form PCT/ISA/210 (second sheet) (April 2005)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 59264P/D579	**FOR FURTHER ACTION** see Form PCT/ISA/220 as well as, where applicable, item 5 below.	
International application No. PCT/US07/63950	International filing date (*day/month/year*) 14 March 2007 (14.03.2007)	(Earliest) Priority Date (*day/month/year*) 14 March 2006 (14.03.2006)
Applicant DIVX, INC.		

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 3 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(b), 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. 1
      ☒ 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.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0167
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US07/63950

Box IV TEXT OF THE ABSTRACT (Continuation of Item 5 of the first sheet)

NEW ABSTRACT
Federated systems for issuing playback certifications granting access to technically protected content are described. One embodiment of the system includes a registration server 26 connected to a network 14, a content server 12 connected to the network 14 and to a trusted system 24, a first device including a non-volatile memory that is connected to thenetwork and a second device inlcuding a non-volatile memory that is conected to the network 12. In addition, the registration server 26 is configured to provide the first device with a first set of activation information in a first format, the first device is configured to store the first set of activation information in non-voatile memory, the registration server 26 is configured to provide the second device is configured to store the second set of activation information in non-volatile memory.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0168
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US07/63950

A. CLASSIFICATION OF SUBJECT MATTER
IPC: **H04L 9/00**(2006.01)

USPC: 380/200,201;713/156;705/57,59
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)
U.S. : 380/200,201;713/156;705/57,59

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2005/0071200 (IRWIN et al.) 31 March 2005 (31.03.05), Entire Document.	1-29
Y	US 2006/0036549 (WU) 16 March 2006 (16.02.2006), Entire Document, especially [0092].	1-29

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

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

"E" earlier application or patent 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
19 February 2008 (19.02.2008)

Date of mailing of the international search report
19 MAR 2008

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
/Tongoc Tran/

Telephone No. (571)272-3843

Form PCT/ISA/210 (second sheet) (April 2007)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/63950

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. type of material

☐ a sequence listing

☐ table(s) related to the sequence listing

b. format of material

☐ on paper

☐ in electronic form

c. time of filing/furnishing

☐ contained in the international application as filed.

☐ filed together with the international application in electronic form.

☐ furnished 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 and/or table(s) relating thereto 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 0170
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/63950

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 NONE	YES
	Claims 1-29	NO
Inventive step (IS)	Claims NONE	YES
	Claims 1-29	NO
Industrial applicability (IA)	Claims 1-29	YES
	Claims NONE	NO

2. Citations and explanations:

Please See Continuation Sheet

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0171
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/63950

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 NONE	YES
	Claims 1-29	NO
Inventive step (IS)	Claims NONE	YES
	Claims 1-29	NO
Industrial applicability (IA)	Claims 1-29	YES
	Claims NONE	NO

2. Citations and explanations:

Please See Continuation Sheet

Form PCT/ISA/237 (Box No. V) (April 2007)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/63950

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

V. 2. Citations and Explanations:

Claims 1-29 lack inventive step under PCT Article 33(3) as being obvious over Irwin et al. (U.S. Patent Application Publication No. 2005/007280 A1, hereinafter Irwin) in view of Wu (U.S. Patent Application Publication No. 2006/0036549).

Claims 1-3, 11, 13, 15-19 and 21-27 lack an inventive step under PCT Article 33(3) as being obvious over Irwin (U.S. Patent Application Publication No. 2005/007280 A1)
With respect to claim 1, Irwin discloses a content distributed network, a registration server, a content server, a device, a registration process and a process for issuing playback certifications, comprising:
A registration server connected to a network (e.g. Fig. 1, License Server, [0032], [0089], register client, establish communication link, [0177], package rights documents with decryption keys, process encryption key [0032] ;
A content server connected to the network and to a trusted system (e.g. repository of content [0085], client device interaction, process client request [0085], implementing encryption technology [0100], [0135];
A first device including a non-volatile memory that is connected to the network (e.g. Fig. 1, client device);
A second device including a non-volatile memory that is connected to the network; and
Wherein the registration server is configured to provide the first device with a first set of activation information in a first format (e.g. Fig. 1, license service and client device);
Wherein the registration server is configured to store the first set of activation information in non-volatile memory.
Wherein the registration server is configured to provide the second device with a second set of activation information in a second format; and
Wherein the second device is configured to store the second set of activation information in non-volatile memory (e.g. Fig. 1, DRM controller,license store, unique PKI certificate [0144].
Irwin does not explicitly disclose the content server provide playback certifications containing at least one encrypted copy of the encryption keys used to encrypt the stored content and transmit the certication via the network interface. However, Irwin discloses encrypted content and encryption information is communicated with the client device (e.g. rights documents are packaged with appropriate decryption key [0032]). Furthermore, Wu discloses a content key is encrypted with specific device key (e.g. Wu, [0092]). It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the playback certificate containing encrypted keys provided by the content server with Wu's teaching of encrypting content key with device key to ensure the integrity of the content key used to decrypt the content.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0173
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/63950

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

With respect to claims 4 and 8, Irwin and Wu disclose the content distribution network of claim 2, wherein:
The first set of activation information is protected by a base encryption key and includes a user encryption key;
the playback certification includes information encrypted using the user encryption key (Wu, e.g. [0092]). Furthermore, encryption key generated with random number is common in encryption schemes. It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the teaching Irwin and Wu's utilization of content protection with base key and user key (or device key) with random number to improve the security of the digital content.

With respect to claim 5, Irwin and Wu disclose the content distribution system of claim 4, wherein the information encrypted using the base encryption key and the user encryption key enables playback of the technically protected content (Wu, e.g. [0092]).

With respect to claim 6, Irwin and Wu discloses the content distribution system of claim 4, wherein:
Wherein the second set of activation information includes the same base encryption key and a different user encryption key (Wu, e.g. [0092]).

With respect to claim 7, Irwin and Wu disclose the content distribution system of claim 4, wherein the second set of activation information includes a different base encryption key and a different user encryption key (Wu, e.g. [0092]).

With respect to claim 9, Irwin and Wu discloses the distribution system of claim 4, wherein:
The registration server is configure to revoke the user encryption key (Irwin, e.g. [0137]).

With respect to claim 10, Irwin and Wu discloses the content distribution system of claim 4, wherein the registration server is configure to revoke the user encryption key (Irwin, e.g. [0137]).

With respect to claim 12, Irwin and Wu disclose the registration server of claim 11, wherein the activation information includes a base encryption key and a user encryption key (Wu, e.g. [0092]).

With respect to claim 14, Irwin and Wu disclose the registration server of claim 11, wherein:
The processor is configured to generate multiple base encryption keys and multiple user encryption keys;
The activation information includes the multiple base encryption keys and a single user encryption key and information concerning an active base encryption key; The processor is configured to store the multiple base encryption keys and the multiple user encryption keys in the storage device; and the processor is configured to store information indicative of the active base encryption key and the user encryption key included in the activation information in the storage device (Wu, e.g. [0092]).

With respect to claim 20, Irwin and Wu disclose the device of claim 19, wherein the activation information includes a base encryption key and a user encryption key (Wu, e.g. [0092]).

With respect to claim 28, a process for issuing playback certifications, comprising:
Receiving a content key from content provider; Receiving playback parameters from a content provider;
Locating a user key and a base key associated with a device; Encrypting the playback parameters using the base key; Encrypting the content key using the user key; and Providing a playback certification including the encrypted playback parameters and the encrypted content key (Wu, e.g. [0092]).

With respect to claim 29, the process of claim 28, further comprising:
Locating multiple user keys and multiple base keys associated with a device; forming a playback parameters table, where each entry in the table includes the playback parameters encrypted using a different base key; forming a content key table, where each entry in the table includes a copy of the content key encrypted usig a different user key (Wu, e.g. [0092]).

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0174
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
WESLEY W. MONROE
CHRISTIE, PARKER & HALE, LLP
P.O. BOX 7068
PASADENA, CA 91109-7068

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	10 MAY 2007
Applicant's or agent's file reference 53684P/D579	FOR FURTHER ACTION See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US05/25845	21 July 2005 (21.07.2005)	21 July 2004 (21.07.2004)

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

IPC: **G06F 12/14**(2006.01);**G06F 17/30**(2006.01);**H04L 9/00**(2006.01) H04N 7/16(2006.01)
USPC: 705/59;726/26

Applicant

DIVXNETWORKS, INC.

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.

3. For further details, see notes to 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	05 February 2007 (05.02.2007)	Matthew Heneghan DEBORAH A. THOMAS PARALEGAL SPECIALIST Telephone No. (571)272-2100

Form PCT/ISA/237 (cover sheet) (April 2005)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US05/25845

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. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

a. type of material

☐ a sequence listing

☐ table(s) related to the sequence listing

b. format of material

☐ on paper

☐ in electronic form

c. time of filing/furnishing

☐ contained in the international application as filed.

☐ filed together with the international application in electronic form.

☐ furnished subsequently to this Authority for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto 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.

4. Additional comments:

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0176
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US05/25845

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 NONE	YES
	Claims 1-24	NO
Inventive step (IS)	Claims NONE	YES
	Claims 1-24	NO
Industrial applicability (IA)	Claims 1-24	YES
	Claims NONE	NO

2. Citations and explanations:

Claims 1-24 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. The invention may be in the area of protected copyrighted media from unauthorized usage.

Claims 1-24 lack novelty under PCT Article 33(2) as being anticipated by US 5509070 (SCHULL).
As per claims 1-5 and 17, Schull discloses a distribution system wherein registration information including a guard (a password) is provided for producing configuration information; received back is the password, keys, and key ID for key lookup and a check against the password for key retrieval (see column 8, line 31 to column 9, line 53; column 10, lines 26-58).
As per claim 6-16 and18-24, Schull discloses a key lookup according to the ID for media retrieval (see column 14, line 56 to column 15, line 35).

Claims 1-24 lack an inventive step under PCT Article 33(3) as being obvious over US 5509070 (SCHULL) for the reasons stated regarding the lack of novelty.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0177
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US05/25845

Box No. VII Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

Form PCT/ISA/237 (Box No. VII) (April 2005)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US05/25845

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the questions whether the claims are fully supported by the description, are made:

In the preamble of claim 1, "randomly-generated" should read as "randomly generating"

Form PCT/ISA/237 (Box No. VIII) (April 2005)

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 813 167 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
17.12.1997 Bulletin 1997/51

(51) Int. Cl.[6]: **G06T 9/00**

(21) Application number: **97201489.8**

(22) Date of filing: **14.05.1997**

(84) Designated Contracting States:
BE DE FR GB

(30) Priority: **16.05.1996 US 17169**

(71) Applicant: **Bayer Corporation**
Pittsburgh, PA 15219-2502 (US)

(72) Inventors:
- **Ristow, Allan W.**
  Salem, New Hampshire 03079 (US)
- **Kaasila, Sampo J.**
  Plaistow, New Hampshire 03865 (US)

(74) Representative:
Ramon, Charles Lucien
Agfa-Gevaert N.V.
Dienst Intellectuele Eigendom 3800
Septestraat 27
2640 Mortsel (BE)

(54) Method and apparatus for font compression and decompression

(57) A method and apparatus for compressing and decompressing font files using a two step compression/decompression technique. The font data comprising a collection of tables and a directory of these tables are converted into an intermediate compressed format. The intermediate compressed data is then further compressed to produce corresponding compressed data sets which can be merged subsequently into a single output file. Decompression of the data sets or of the single output file produces a font file that is functionally equivalent to the original font file. The method and apparatus have particular application to TrueType fonts.

EP 0 813 167 A2

Printed by Xerox (UK) Business Services
2.15.3/3.4

Description

1. Field of Invention

The present invention relates to font compression and decompression and has particular application to TrueType fonts.

2. Description of Related Art

The Data Compression Book, (2nd Edition, by Mark Nelson & Jean-Louis Gailly, ISBN 1-55851-434-1;

[ZIV77] ZIV]. Lempel A, "A Universal Algorithm For Sequential Data Compression", IEEE Transactions on Information Theory, Vol. 23, No. 3, pp. 337-343.

BRIEF SUMMARY OF THE INVENTION

A two step compression/decompression process is employed on font files to reduce file size while maintaining character quality. The font data comprising a collection of tables and a directory of these tables are converted into an intermediate compressed format. The intermediate compressed data is then further compressed to produce corresponding compressed data sets. These further compressed data sets can be merged into a single output file. Decompression of the data sets or the single output file produces a font file that is functionally equivalent to the original font file.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

Figure 1 is a top level block diagram showing the compression and decompression process and the associated data files;

Figure 2 is a more detailed block diagram of the compressors and associated data files for a TrueType font consisting of a collection of tables and a directory of these tables;

Figure 3 illustrates in block form an individual TrueType character, individual compression modules and the resulting intermediate compressed TrueType font; and,

Figure 4 is a block diagram illustrating the application of the present invention to a network or communications channel configuration.

DESCRIPTION OF THE PREFERRED EMBODIMENT

Turning now to the drawings, Figure 1 is a top level block diagram showing the compression arid decompression process and the associated data files. An exemplar TrueType font file D1 is input to a compression mechanism C1 which produces a compressed data font file D2 representative of the TrueType font file D1.

The compressed file is typically transmitted either electronically over a digital network or via a storage medium like diskettes. A decompressor C2 takes as input the compressed data file D2 and produces a TrueType font file D3. The file D3 is not necessarily identical to the file D1. The two files are, however, functionally equivalent in that they behave identically as TrueType fonts. The differences between the D1 and D3 will be explained below in connection with the more detailed levels.

Figure 2 is a more detailed view of the compressor and associated data files. The TrueType font D1 consists of a collection of tables and a directory of these tables. The TrueType font format which is abbreviated hereinafter as "TTF" is defined in "TrueType 1.0 Font Files Technical Specification", Revision 1.66, August 1995,. Microsoft Corporation, incorporated herein by reference. The font directory together with all of the tables are first converted by compressors C10 through C17 into an intermediate form called compressed TrueType font, or "CTF" format. The CTF data is identified as D10, D11, and D12.

The 3 data sets are:

D11 "data":	all the data from the initial push bursts for each glyph
D12 "code":	all the TrueType instructions for all the glyphs minus the initial push burst sequence concatenated together.
D10 "rest":	Everything else goes here.

The three sections D10, D11 and D12 of the CTF data are then further compressed in a second step using three compressors C17, C18, and C19 which can be the same or different generic compressors.

Preferably, C17, C18 and C19 are three instances of LZCOMP, a loss-less data compressor which produces three compressed data sets D13, D14, and D15. These three data sets are then preferably merged by compressor C20 into a single output file D2 for packaging convenience.

The fact that the data is separated into three sets, all with different statistical distributions, results in a smaller total size since LZCOMP compresses each set independently of the other, and therefore, LZCOMP can adapt to the particular distinctly different statistical data distribution for each different data set. This technique results in a more compact final result when the CTF format is further compressed by LZCOMP.

The TTF to CTF translation can eliminate glyphs that are not needed. This is called character subsetting. The actual glyph outlines and instructions in the 'glyf' table are deleted and replaced with a null glyph. For the hmtx and hdmx tables the values for the deleted glyphs are set to zero. This results in a smaller final file size.

TTF to CTF file translation techniques

The goal for the TTF_Converter class is to create a more compact file without losing any information. Another goal is that the output should be suitable for compression by traditional compression methods (e.g.,

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0181
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

LZCOMP). This basically means that data mostly needs to be byte aligned, unless there is a huge win in going to the bit-level.

The table directory and the tables loca, cvt, hdmx, VDMX, hmtx, and glyf are compressed by compressors C10 through C15. All of the other tables in the TrueType font file are passed through C16 which simply copies the tables into D10. The hdmx and VDMX tables are kept bit aligned while the other tables remain byte aligned.

The Table Directory

The font table directory has the same format in both the CTF and TTF files.

Loca Table

The TrueType 'loca' table contains information regarding the specific location of each glyph in the 'glyf' table, and implicitly also the length of each glyph in the 'glyf' table. The glyphs are accessed in sequence. The length of each glyph is already implicitly defined by the data for that glyph. Since the glyphs are stored in sequence in the 'glyf' table starting at offset zero, there is no need to store the 'loca' table in the CTF format. When the information is translated back to the TTF format, the 'loca' table is recreated from the available information, which is sufficient for this task. The elimination of the 'loca' table results in a more compact CTF format. However, many compression benefits can be achieved even if the $loca_F$ table is retained and compressed as shown by the dashed line in Figure 2.

Cvt Table

The contents of the cvt table in a TrueType font consists of a sequence of signed 16 bit 2's complement integers. The CTF format stores the values relative to the previous value modulo 2 raised to 16. The first value is stored relative to zero. Sometimes numerically close values are stored next to each other in the Cvt, and this technique will cause them to be stored as numerically small relative values instead. In this situation, the relative values are stored with the following technique: Each value is encoded in 1 to 3 bytes, so that most values can be stored as one, or two bytes instead of 2. In this encoded format, each byte is treated as an unsigned byte in the range 0..255 inclusive. If the byte is in the range 248..255 inclusive, then this byte is called b1, and then another byte is read as b2. The value in this case is defined as equal to 238 * (b1-247) + b2. Thus, one can encode values in the range 238..2159 inclusive in two bytes. If the byte is in the range 239..247 inclusive, then it is called byte b1, and then another byte is read as b2. The value in this case is defined as equal to -(238 * (b1-239) + b2) . Thus, one can encode values in the range -0 to -2159 inclusive in two bytes. If the byte is equal to 238, 2 more bytes are read and the value is treated as a signed 2 byte quantity, based on the last two read bytes. The value is equal to this quantity. Thus, one can encode large values in 3 bytes. However, if the byte is less than 238, the value equal to the byte is set without reading any more bytes thereby encoding 0.237 inclusive in one byte. This technique results in a more compact CTF format since the typical statistical distribution of the data values allows storage of a majority of the values as single or double bytes.

Hdmx Table

The 'hdmx' table in TrueType contain the device advance widths of the glyphs for a range of sizes. TrueType instructions can change the device advance width in a non-linear manner and therefore they are stored in the TrueType file so that the client of the TrueType rasterizer can quickly obtain access to the widths of characters without actually rendering them.

In translating to CTF format, the most likely device advance width is predicted. The most likely value is the device independent advance width linearly scaled to the particular device resolutions, and size, and then rounded to the closest integer. This prediction is always very close to the truth. Therefore, one can treat the difference between the actual device advance width and the prediction as the surprise. This method only stores the surprise value which is typically equal to zero or very small with the "Magnitude dependent variable size encoding" described below. When the TTF file is reconstructed from the CTF file, the prediction is simply made and then the surprise is added to the prediction to get the actual true value. This technique results in a more compact CTF format.

"Magnitude dependent variable size encoding" of a value is used in the encoding of the 'hdmx' and 'VDMX' table.

A value of 0 is encoded as a 0 bit.
A value of +1 is encoded as the 100 bits.
A value of -1 is encoded as the 101 bits.
A value of +2 is encoded as the 1100 bits.
A value of -2 is encoded as the 1101 bits.
A value of +3 is encoded as the 11100 bits.
A value of -3 is encoded as the 11101 bits.
etc . . .

The absolute of the value is equal to the number of 1's preceding the '0'. Then if the value is greater than zero there is one additional sign bit, where '0' represents '+' and '1' represents '-' . This means that one obtains a variable bit length encoding of values, where the number of bits used grows with the magnitude of the value. This encoding can be used advantageously for storing very small values.

VDMX Table

The 'VDMX' table contains the maximum font wide

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0182
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

maximum and minimum y value for a range of sizes and aspect ratios. Similarly to the 'hdmx' table, the values are predicted and then only the surprise is encoded which is equal to the error in the prediction with the "Magnitude dependent variable size encoding" described above. The following technique is used to predict the 3 values (ppem (size), ymax, ymin) The predicted ppem is simply the previous ppem + one. The predicted ymax is equal to size * yMaxMultiplier rounded to the closest pixel. The predicted ymin is equal to size * yMinMultiplier rounded to the closest pixel. The yMaxMultiplier and yMinMultiplier are simply computed as the average of the exact multipliers for each instance during the TTF to CTF file translation. These two average values are then stored in the file, so that the actual ymax and ymin values can be predicted with the previously mentioned formula.

Glyf Table

The 'glyf' table contains the individual scalable characters in the font. These characters are stored within the table sequentially and are indexed by entries in the 'loca' table. Module C15 compresses the 'glyf' table into CTF format producing data files D11 and D12. Within C15, each character in the 'glyf' table is compressed as shown in Figure 3.

Figure 3 depicts an individual TrueType character D20, the individual compression modules C30 through C34 and resulting compressed character data in CTF format D21 and D22. These two data blocks are stored sequentially, character by character, within D11 and D12. Composite characters are stored in native TrueType format, however, non-composite glyphs are stored more compactly.

Number of Contours

The number of contours is a 16 bit integer that is stored as a signed 2 byte quantity.

Bounding Box

Each glyph in the 'glyf' table contains the bounding box for that character. It is stored as 4*2 bytes of data. The bounding box is a direct function of the coordinate data for each glyph. Since the coordinate data for each glyph is stored, this directly specifies the bounding box and there is no need to explicitly store the bounding box. In the CTF file format, the bounding box is not stored for regular glyphs. The bounding box is simply recomputed during translation back to the TTF format. This technique results in a more compact CTF format. 255UShort format encoding is effective for small positive values. Each value is encoded in 1 to 3 bytes, so that most small positive values can be stored as one byte instead of 2. In this encoded format each byte is treated as an unsigned byte in the range 0..255 inclusive. If the byte is equal to 253, 2 more bytes are read and the value is treated as a signed 2 byte quantity, bases on the last two read bytes. The value is equal to this quantity. Thus large values are encoded in 3 bytes. If the byte is equal to 255, then this byte is called b1, and then another byte is read as b2. The value in this case is defined as (253 + b2). Thus values in the range 253 to 505 inclusive are encoded in two bytes.

If the byte is equal to 254, it is called byte b1, and then another byte is read as b2. The value in this case is defined as (2*253 + b2). Thus values in the range 506 to 758 inclusive are encoded in two bytes.

However, if the byte is less than 253 it is interpreted as the magnitude of the value. Thus values in the range 0 to 252 inclusive are encoded in one byte. This technique results in a more compact CTF format, since it is used where the typical statistical distribution of the data values permits storage of a majority of the values as single bytes, instead of double bytes as in the TrueType format.

Contour End Points

Instead of storing the actual endpoint numbers as TrueType does, only the difference between the current endpoint and the previous endpoint is stored. The „previous end point" for contour zero is set to zero by definition. During translation back to TTF from the CTF format, the endpoint value for each contour is simply set equal to the cumulative sum of the stored values in the contours so far. This technique results in sequence of small positive numbers. Each value is encoded in 1 to 3 bytes, so that most values can be stored as one byte instead of 2, with the "255UShort format encoding" mentioned above. This technique results in a more compact CTF format, since the typical statistical distribution of the data values allows storage of a majority of the values as single bytes, instead of double bytes as in the TrueType format. If the first contour has two points, the process is started by storing a one.

Instructions

TrueType contains four instructions for pushing data onto the stack. These four instructions occupy 18 opcodes out of at most 256 possibilities in byte encoded TrueType instruction language. Glyph programs for TrueType glyphs typically start with a burst of various PUSH instructions aimed at setting up the initial stack for the TrueType instructions belonging to that glyph. The fact that this PUSH burst sequence is typical and only 18 out of 256 codes are used leaves room for improvement. Storage is used for how many values are pushed and the actual values independent of the TrueType opcodes used to push them onto the stack. These values are collectively known as „an initial state of the stack". During translation back to TrueType new TrueType instructions for pushing the values onto the initial stack are simply generated. This technique results in a more compact CTF format.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0183
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

The storage of the initial push data for the stack is as follows. "255UShort format encoding" is used to encode the number of values pushed onto the initial stack as well as the number of remaining instruction bytes after the pushes. Each data value is in the range -32768 and 32767 inclusive. Most of these values are small positive numbers. Each value is encoded in 1 to 3 bytes (or less) , so that most values can be stored in two or less bytes instead of 2 bytes. In this encoded format, each byte is treated as an unsigned byte in the range 0..255 inclusive. If the byte is equal to 251, then it is treated as a Hop3Code command. This command causes a read of only one value, according to this specified technique, but without further Hop3 or Hop4 commands. The command then sets 3 values. The first value is set equal to the value 2 indices back into the stream and is called value A. Then the next value is set equal to the value read with this technique, and then the third value is set equal to A again. Hop3Code does the following transformation going from TTF to CTF and then back to TTF:

A,X1,A,X2,A -> A,X1,Hop3Code,X2 ->A,X1,A,X2,A

If the byte is equal to 252, it is treated as a Hop4Code command. This command reads only two values, according to this specified technique, but without further Hop3 or Hop4 commands. The command then sets 5 values. The first value is set equal to the value 2 indices back into the stream and is called value A. Then the next value is set equal to the first value read with this technique, and then the third value is set equal to A again. The fourth value is set equal to the 2nd value read with this technique. Finally the fifth value is set equal to A again. Hop4Code does the following transformation going from TTF to CTF and then back to TTF:

A,X1,A,X2,A,X3,A -> A,X1,Hop4Code,X2,X3 ->A,X1,A,X2,A,X3,A

When encoding the data one first determines if any values can be encoded with the Hop3 or Hop4 commands, thereafter all remaining values are encoded in the 255Short format.

In the 255Short format, values in the range 0..249 inclusive are encoded as the value itself expressed as one byte.

Values in the range 250..499 inclusive are encoded as a byte with value 255 followed by a second byte containing the value minus 250.

Values in the range 500..749 inclusive are encoded as a byte with value 254 followed by a second byte containing the value minus 500.

Values in the range -1..-249 inclusive are encoded as a byte with value 250 followed by a second byte containing the absolute of the value.

Values greater than 749 and values less than -249 are encoded as a byte with value 253 followed by two bytes containing the value directly.

Thus values in the range 0..249 inclusive are encoded with one byte while values in the following inclusive ranges -1..-249, 250..499, 500..749 are encoded with two bytes. Everything else is encoded with 3 bytes.

This technique results in a more compact CTF format since the typical statistical distribution of the data values allow storage of a majority of the values as single or double bytes, or even less when the Hop3Code or Hop4Code commands are used.

Character Outline

A more compact format for storing the outlines in the 'glyf' table is utilized. The TrueType format stores the coordinate data in a sub-optimal format, leaving room for optimization, so that in the CTF format the coordinates are stored using less bits per {dx, dy, on/off-curve} triplet. Each triplet is stored with a variable length encoding which consumes 2 to 5 bytes per triplet. One bit of the first byte is used to indicate whether the point is an "on" or "off"-curve point. Thus there are 128 remaining combinations for the first byte. All 128 remaining combinations have a precisely defined meaning. They specify the following seven properties:

(a) total number of bytes used for this triplet. (2-5)
(b) Number of additional bits beyond the first byte used for describing the dx value.
(c) Number of additional bits beyond the first byte used for describing the dy value.
(d) An additional amount to add to the dx value described by data beyond the first byte.
(e) An additional amount to add to the dy value described by data beyond the first byte.
(f) The sign of the dx value. (This has no meaning if the value of dx is zero, which is specified by 0 xbits) .
(g) The sign of the dy value. (This has no meaning if the value of dy is zero, which is specified by 0 ybits) .

Each of the 128 combinations has a unique combination of these 7 properties. The properties are assigned so that with the typical statistical distribution of data found in TrueType files the resulting data size in the CTF format is much reduced compared to the less efficient native TrueType format. The data is still left byte aligned so that LZCOMP in the 2nd stage can further compress the data. This technique results in a more compact CTF format.

LZCOMP

The LZCOMP compression algorithm is a variation on the LZ77 theme.

An excellent starting point for data compression information is the 2nd edition of [Nelson95] "The Data Compression Book" by Mark Nelson. ISBN 1-55851-434-1.

An unmodified LZ77 algorithm encodes the data to be compressed into tokens. Each token consists of:

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0184
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

(1) An offset to the start of the string to be copied.
(2) The length of the string
(3) The first character in the Look-Ahead buffer that follows the string. [Ziv77] Ziv J., "A universal Algorithm for Sequential Data Compression", IEEE Transactions on Information Theory, Vol. 23, No 3, pp 337-343, incorporated herein by reference.

LZCOMP differs from LZ77 as follows:

(1) LZ77 always transmits a triplet (0,0,c) for a character not matched. Instead literals (characters not matched) and copy items (string matches) can be outputted in any sequence and order.
(2) Some predefined constant data is concatenated in front of the history buffer, so that there is a possibility that copy items may be used even at the beginning of the data. This idea is mentioned in Nelson95.
(3) Adaptive Huffman encoding is employed to further enhance the compression. Three separate Adaptive Huffman trees are employed with the trees encoding everything, including the offset amount, string length, and copy commands.
(4) 3 single byte copy commands are used. (This is helpful but not necessarily in the general case)
(5) The distance to the tail of the string is encoded but not the head as in LZ77. This way one can reach a greater distance.
(6) LZ77 only provides a small window into the previously seen text. LZCOMP can address all of the previously seen text.
(7) LZ77 limits the length of the phrase that can be matched. LZCOMP has no such limit on the phrase length.
(8) A variable minimum copy length is used. If the offset is greater or equal to 512 bytes the minimum phrase length is 3 bytes, otherwise it is 2 bytes.
(9) The compression code communicates with the entropy based encoders so that it knows the exact cost of various decisions. With this information it makes an optimal choice. This item(10) is highly related to item 11. This communication enables one to make a better choice than a normal "greedy" algorithm would.
(10) LZ77 is greedy; LZCOMP is a little better, because all of the following are considered:

(a) the "best" copy item for the current position.
(b) using a literal instead of the "best" copy item.
(c) cutting back the length of the "best" copy item by one byte.
(d) If the length of the copy item is just two, then a combination of a copy item and literal item is also considered.

(11) The encoding scheme is so compact that one can advantageously have copy lengths as short as two bytes in the general case.

LZCOMP Decompression

The LZCOMP decompression steps follow. Everything is stored as a sequence of symbols. The symbols are encoded with a plain Adaptive Huffman encoding tree (AHUFF #1). (For an explanation of Adaptive Huffman see [Nelson95].) The sequence of symbols is read one at a time until the input data is exhausted.

(1) If the symbol value is less than 256 then it is interpreted as literal byte and the value is copied directly into the output stream.
(2) If the symbol is equal to DUP2 then it is interpreted as a single byte copy item from 2 bytes backwards. If the symbol is equal to DUP4 then it is interpreted as a single byte copy item from 4 bytes backwards. If the symbol is equal to DUP6 then it is interpreted as a single byte copy item from 6 bytes backwards.
(3) However if the symbol is greater than 255 and it is not equal to DUP2, DUP4 or DUP6 then it is interpreted as a copy command. This first copy command value encodes the number of distance symbols used for this copy item. The number of distance symbols used is equal to (symbol value - 256) / 8 + 1.

Additionally, this first copy command value encodes the first range for the length. The first range for the length is (symbol value - 256) % 8. This is a 3 bit quantity. The length is first initialized to zero, then shift in the 2 least significant bits from the 3 bit quantity. The most significant of the 3 bits is treated as a stop bit. If it is set then the process is finished.

However, there is continued reading of symbols through a separate Adaptive Huffman tree (AHUFF #2). These new symbols all have a value between 0 and 7. Now one keeps shifting in the 2 lowest bits, including the 2 lowest bits in the symbol that has the stop bit set. Then when done, the minimum length (+= 2) is added to the length. Next a sequence of symbols is read in through a third Adaptive Huffman tree (AHUFF #3). This sequence encodes the offset value. One already knows how many symbols to read in since this was encoded in the initial symbol. This means one does not have to rely on stop-bits. Each symbol is 3 bits wide, and one simply reads the right number of them and concatenates them all together. Now add 1 to this concatenated value and the resulting value forms the offset. Additionally, once the offset has been decoded and if it is greater than or equal to the maximum 2 byte copy offset (512), then one is added to the length since the minimum copy length jumps from 2 to 3 bytes at the 512 byte boundary.

LZCOMP Compression

The compressor simply sits in a loop and for each

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0185
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

byte or string decides exactly which one of the 3 possible actions to take:

(1) Literal byte.
(2) Single byte copy command. If it is possible to use a single byte copy command the code always gives preference to this option over the literal byte option. This is advantageous for the kind of data present in the CTF format.
(3) A copy item. When the code decides to use a copy item it also decides on an optimal length & offset for the copy item.

The decision is based on minimum cost of representing the data.

(a) When exploring the copy item possibility the code first finds the best possible copy item for the current position. The best possible copy item is the item that produces the maximum gain. The gain is defined as the literalCost - copyCost. The literalCost is the total cost of representing the string as a sequence of literal items. The copyCost is the cost of representing the string as a copy item. The code queries the adaptive Huffman trees for the actual representation cost when computing this gain, which is called gain1.
(b) Next, if the previous gain1 is greater than zero then the code explores the gain that would result if it sent the current byte as a literal byte, and then did the best possible copy item on the next byte. This gain is called gain2. If gain2 is greater than gain1 then the current byte will be sent as a literal item. This is different from normal $_{T}$greedy^{L} behavior in an LZ77 based compressor. Also note that the next byte will undergo the same evaluation, so that it is possible that more than one byte will be sent in sequence as literals, even though one could have used copy items.
(c) However, if after paragraph (b) one is still considering a copy item AND the length from the gain1 computation is greater than 3 the code explores the effects of cutting back the length in the gain1 computation by one byte. The costPerByteA is the representation cost per byte for the two consecutive copy items if the normal decision resulting in gain1 is taken. The costPerByteB is the representation cost per byte for the two consecutive copy items if one cuts back the length of the first copy item by one byte. If costPerByteB is less than costPerByteA then the length of the copy item is cut back by one byte.
(d) Finally, if the code is still contemplating a copy item decision and the length of the best copy item is two bytes and one would be able to use a single byte copy from 2 bytes back combined with a single literal item, then this cost is computed. If this cost is lower, then a normal copy item is not produced. The code does check for both a single byte copy, followed by a literal item, and a literal item followed by a single byte copy.

Figure 4 illustrates in block diagram form a network embodiment with compression and decompression processing occurring at separate locations 36 and 38, respectively, that are connected by a communication channel 40 such as the Internet. It will be appreciated that communication channel 40 can be wired, wireless or a combination thereof.

The compression location or station 36 contains a processor 42 with associated RAM 44 and data storage 46. Station 36 can represent a web server connected to a plurality of local and/or remote devices. Fonts can be displayed on font display 48 and hard copy produced at a local printer 50. Compressed font data can be sent to one or more of the plurality of local and/or remote devices at corresponding local and/or remote locations. If desired, decompression can be performed at location 36 as well as compression or compressed data can be storted on the data storage 46 for subsequentt delivery to another location or locations.

The compressed representation of the TrueType font file is transmitted over communication channel 40 to decompression location 38. It should be noted that the compressed representation can be sent as part of a document so that the original design, layout and typography can be duplicated at location 38 after decompression. Similar remote station components 42A, 44A, 46A, 48A and 50A correspond to the processor, RAM, data storage, font display and printer at location 36. Decompression station 38 can have its own printer 52 and the decompression facility can be provided in this printer or in any other remote device connected to station 36. Furthermore, the compressed representation of the original TrueType font file can be stored in the printer itself.

Having described in detail a preferred embodiment of our invention, it will now be apparent those in the art that numerous modifications can be made without departing from the invention as defined in the following claims.

Claims

1. A method for font compression comprising the steps of:

   compressing at least a portion of a font file to produce a plurality of intermediate compressed data sets; and,
   further compressing said plurality of intermediate compressed data sets to produce a corresponding plurality of compressed output data sets.

2. The method of claim 1 further comprising the step of merging said plurality of compressed output data sets to produce a single compressed output font file.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0186
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

3. The method of claim 1 wherein said plurality of intermediate compressed data sets constitutes three data sets.

4. The method of claim 1 wherein at least some of said plurality of intermediate compressed data sets have a format optimized for subsequent further compression.

5. The method of claim 1 further comprising the step of transmitting the plurality of compressed output data sets over a communications channel.

6. The method of claim 1 further comprising the step of storing the plurality of compressed output data sets on a machine readable medium.

7. The method of claim 2 further comprising the step of transmitting the compressed output font file over a communications channel.

8. The method of claim 2 further comprising the step of storing the compressed output file on a machine readable medium.

9. A method for producing a compressed representation of a TrueType font file, said method comprising the steps of:

compressing at least a portion of the TrueType font file to produce an intermediate compressed font file; and,
further compressing the intermediate compressed font file to produce a compressed representation of the TrueType font file.

10. The method of claim 9 further comprising the step of transmitting the compressed representation of the TrueType font file over a communications channel.

11. The method of claim 9 further comprising the step of storing the compressed representation of the TrueType font file on a machine readable medium.

12. A method for producing a compressed representation of a TrueType font file, said method comprising the steps of:

compressing at least a portion of the TrueType font file to produce an intermediate compressed font file having a format that is optimized for subsequent compression; and,
further compressing the intermediate compressed font file to produce a compressed representation of the TrueType font file.

13. A method for producing a compressed TrueType font file comprising the steps of:

compressing at least a portion of a TrueType font file to produce a plurality of intermediate compressed data sets; and,
further compressing said plurality of intermediate compressed data sets to produce a corresponding plurality of compressed output data sets that collectively represent the TrueType font file.

14. The method of claim 13 further comprising the step of merging the plurality of compressed output data sets to produce a compressed representation of the TrueType font file.

15. A method for producing a compressed representation of a TrueType font file having a font table directory, and tables loca, cvt, hdmx, VDMX, and glyf, said method comprising the steps of:

compressing the font table directory and tables cvt, hdmx, VDMX, hmtx and glyf to produce an intermediate compressed font file; updating the font table directory; and,
further compressing said intermediate compressed font file to produce a compressed representation of the TrueType font file.

16. A method for producing a compressed representation of a TrueType font file having a font table directory, and tables loca, cvt, hdmx, VDMX, and glyf, said method comprising the steps of:

compressing the tables cvt, hdmx, VDMX, hmtx and glyf to produce an intermediate compressed font file;
updating the font table directory; and,
further compressing said intermediate compressed font file to produce a compressed representation of the TrueType font file.

17. A method for producing a compressed representation of a TrueType font file having a font table directory, and tables loca, cvt, hdmx, VDMX, and glyf, said method comprising the steps of:

compressing the tables loca, cvt, hdmx, VDMX, hmtx and glyf to produce an intermediate compressed font file;
updating the font table directory; and,
further compressing said intermediate compressed font file to produce a compressed representation of the TrueType font file.

18. A method for producing a compressed representation of a TrueType font file having a font table directory, and tables loca, cvt, hdmx, VDMX, and glyf, said method comprising the steps of:

compressing the font table directory, tables

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0187
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

loca, cvt, hdmx, VDMX, hmtx and glyf to produce an intermediate compressed font file;
updating the font table directory; and,
further compressing said intermediate compressed font file to produce a compressed representation of the TrueType font file.

19. The method of claim 18 further comprising the step of maintaining byte alignment of all tables except the hdmx and VDMX tables during compression to said intermediate compressed font file.

20. A method for producing a compressed representation of a TrueType font file having a font table directory, and tables loca, cvt, hdmx, VDMX, hmtx and glyf, said method comprising the steps of:

compressing at least tables cvt, hdmx, VDMX and glyf outline data to produce a first intermediate compressed data set;
compressing the glyf table to produce a second intermediate compressed data set representing glyf data and a third intermediate compressed data set representing glyf code;
updating the font table directory; and,
further compressing said three intermediate data sets to produce corresponding three compressed output data sets that collectively represent the TrueType font file.

21. The method of claim 20 further comprising the step of maintaining byte alignment of all tables except the hdmx and VDMX tables during compression to said first intermediate compressed data set.

22. The method of claim 20 further comprising the step of maintaining byte alignment of at least some of the tables other than the hdmx and VDMX tables during compression to said first intermediate compressed data set.

23. A method for font decompression comprising the steps of:

decompressing a plurality of compressed output data sets to produce a corresponding plurality of intermediate compressed data sets; and,
decompressing said plurality of intermediate compressed data sets to produce at least a portion of a decompressed output font file.

24. The method of claim 23 further comprising the step of rendering at least a portion of said decompressed output font file.

25. The method of claim 23 wherein said at least a portion of said decompressed output font file is rendered on a display device.

26. The method of claim 23 wherein said at least a portion of said decompressed output font file is rendered on a printer.

27. The method of claim 23 further comprising the step of storing the plurality of compressed output data sets for subsequent decompression.

28. A method for font decompression comprising the steps of:

decompressing a compressed output font file comprising a plurality of compressed output data sets to produce a corresponding plurality of intermediate compressed data sets; and,
decompressing said plurality of intermediate compressed data sets to produce at least a portion of a decompressed output font file.

29. The method of claim 28 further comprising the step of rendering at least a portion of said decompressed output font file.

30. The method of claim 28 wherein said at least a portion of said decompressed output font file is rendered on a display device.

31. The method of claim 28 wherein said at least a portion of said decompressed output font file is rendered on a printer.

32. The method of claim 28 further comprising the step of storing the compressed output font file for subsequent decompression.

33. A method for decompressing a compressed representation of a TrueType font file comprising three merged compressed data sets with the first data set containing an updated table directory and twice compressed tables cvt, hdmx and VDMX and with the second and third data sets containing twice compressed glyf data and glyf code, respectively, said method comprising the steps of:

splitting the merged three data sets into individual compressed first, second and third data sets;
decompressing said individual compressed first, second and third data sets to produce intermediate compressed first, second and third data sets;
further decompressing said intermediate compressed first set to produce a TrueType table directory, tables cvt, hdmx and VDMX and glyf outlines;
further decompressing said intermediate compressed second and third data sets to produce a glyf table; and,
rebuilding a TrueType loca table with said table

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0188
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

directory and tables representing a TrueType font file that is functionally equivalent to the TrueType font file before compression.

34. A method for producing a functional equivalent of a TrueType font file from a compressed representation thereof, said method comprising the step of:

decompressing at least a portion of said compressed representation of the TrueType font file to produce a decompressed output font file having bit map identity with the TrueType font file at all character sizes, but not binary file identity therewith.

35. A method for producing a functional equivalent of a TrueType font file from a compressed representation thereof, said method comprising the step of:

decompressing at least a portion of said compressed representation of the TrueType font file to produce a decompressed output font file having bit map identity with the TrueType font file at preselected character sizes, but not binary file identity therewith.

36. The method of claim 35 further comprising the step during decompression of generating new TrueType instructions for pushing initial state of the stack values onto the initial stack.

37. A method for producing a compressed representation of a TrueType font file at one location and for decompressing at least a portion of the compressed representation at another location, said method comprising the steps of:

compressing at least a portion of the TrueType font file to produce an intermediate compressed font file and further compressing the intermediate compressed font file to produce a compressed representation of the TrueType font file at said one location;
transmitting the compressed representation of the TrueType font file over a communications channel to another location; and,
decompressing at said another location at least a portion of said compressed representation of the TrueType font file to produce a decompressed output font file having functional equivalency with said TrueType font file.

38. The method of claim 37 further comprising the step of rendering at least a portion of said decompressed output font file.

39. The method of claim 37 further comprising the step of rendering at least a portion of said decompressed output font file on a display device.

40. The method of claim 37 further comprising the step of rendering at least a portion of said decompressed output font file on a printer.

41. The method of claim 37 further comprising the step of storing said compressed representation of the TrueType font file at said another location for subsequent decompression of at least a portion thereof.

42. The method of claim 41 wherein said compressed representation of the TrueType font file is stored in a printer at said another location.

43. A method for producing a compressed representation of a TrueType font file at a first location and for decompressing at least a portion of the compressed representation at another location, said method comprising the steps of:

compressing at least a portion of the TrueType font file to produce an intermediate compressed font file and further compressing the intermediate compressed font file to produce a compressed representation of the TrueType font file at said one location;
transmitting the compressed representation of the TrueType font file over a communications channel to a second location;
storing said compressed representation of the TrueType font file at said second location; and,
decompressing at said another location at least a portion of said stored compressed representation of the TrueType font file to produce a decompressed output font file having functional equivalency with said TrueType font file.

44. An apparatus for compressing a TrueType font file comprising:

a first compressor that compresses at least a portion of the TrueType font file, said first compressor producing a plurality of intermediate compressed data sets; and,
a second compressor that compresses said plurality of intermediate compressed data sets, said second compressor producing a corresponding plurality of compressed output data sets.

45. The apparatus of claim 44 further comprising a data storage that stores the compressed output data sets.

46. An apparatus for decompressing a compressed representation of a TrueType font file comprising:

a file splitter that splits the compressed representation of a TrueType font file into a plurality of compressed data sets;

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0189
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

a corresponding plurality of decompressors that decompress the plurality of compressed data sets into a corresponding plurality of intermediate compressed data sets; and,

another corresponding plurality of decompressors that decompress the plurality of intermediate compressed data sets to produce a functional equivalent of the uncompressed TrueType font file.

47. A printer comprising:

a character image renderer;
a data storage; and,
a compressed representation of a TrueType font file stored in said data storage, said compressed representation comprising a plurality of compressed output data sets.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0190
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

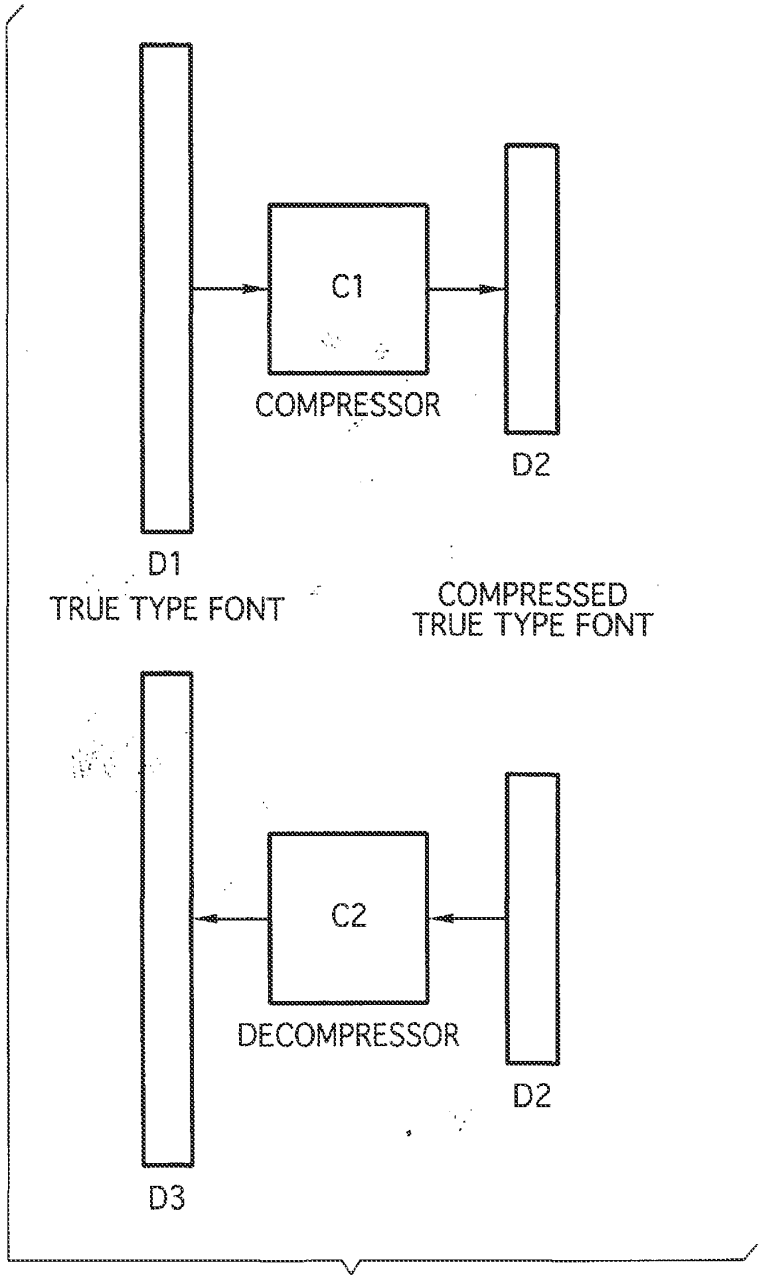


FIG. 1

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0191
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

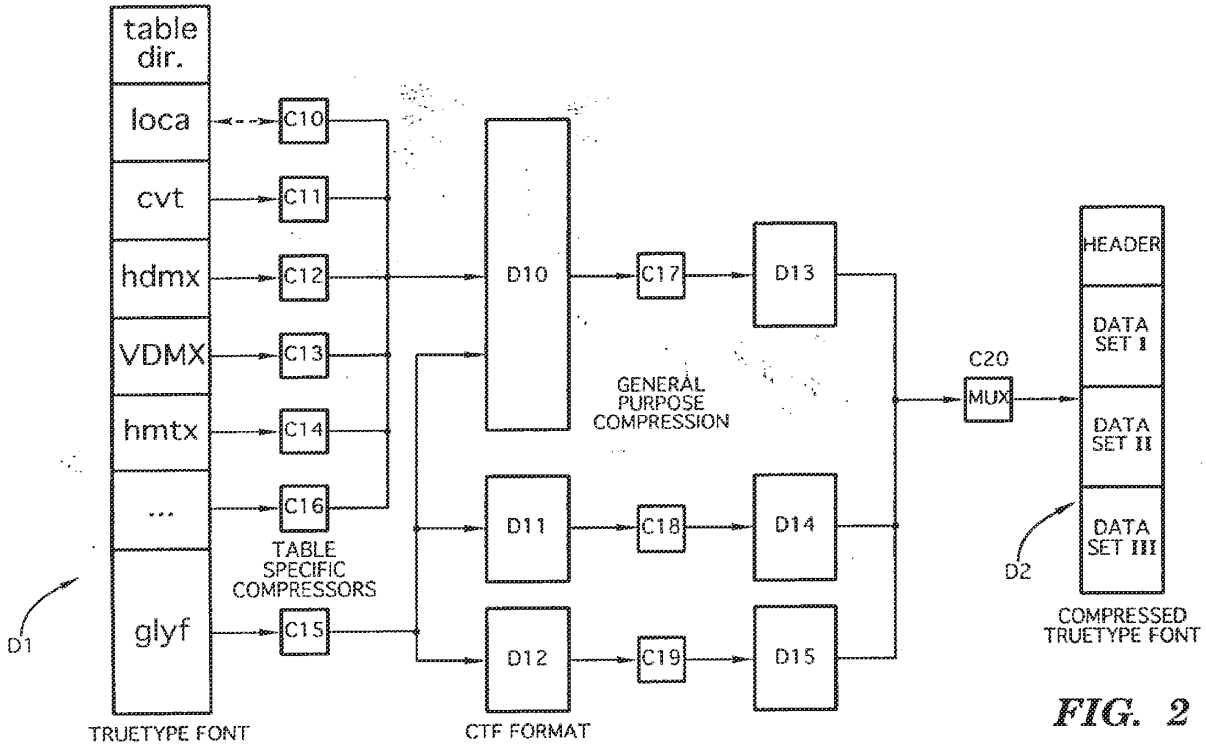

table dir.
loca
cvt
hdmx
VDMX
hmtx
...
glyf
TRUETYPE FONT
D1
C10
C11
C12
C13
C14
C16
TABLE SPECIFIC COMPRESSORS
C15
D10
D11
D12
CTF FORMAT
C17
C18
C19
GENERAL PURPOSE COMPRESSION
D13
D14
D15
C20
MUX
D2
HEADER
DATA SET I
DATA SET II
DATA SET III
COMPRESSED TRUETYPE FONT

FIG. 2

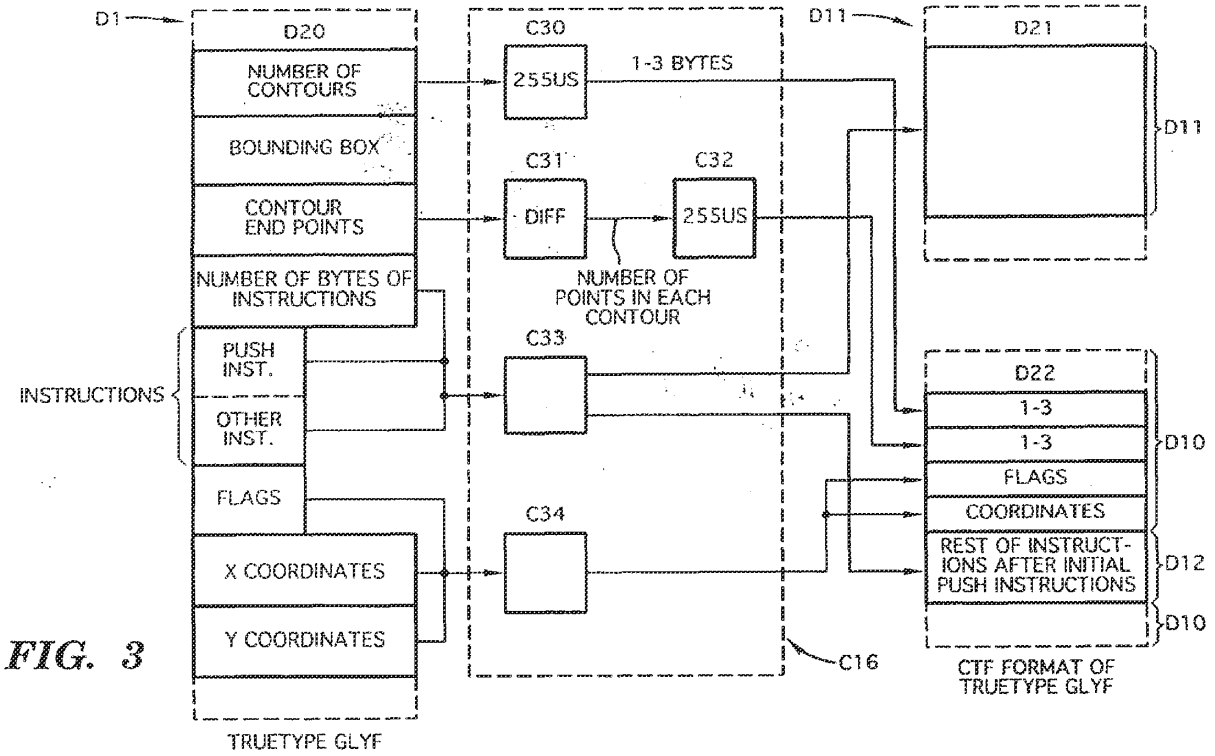


FIG. 3

EP 0 813 167 A2

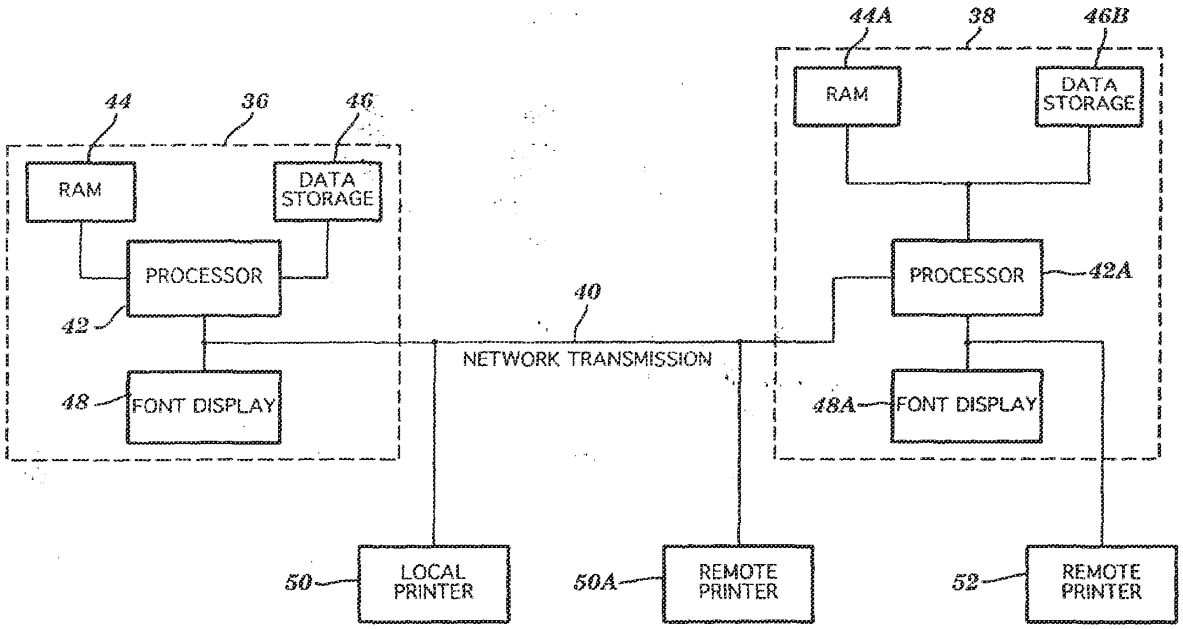

44A
38
46B
RAM
DATA STORAGE
44
36
46
RAM
DATA STORAGE
PROCESSOR
42A
40
42
NETWORK TRANSMISSION
48
FONT DISPLAY
48A
FONT DISPLAY
50
LOCAL PRINTER
50A
REMOTE PRINTER
52
REMOTE PRINTER

FIG. 4

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 936 812 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
18.08.1999 Bulletin 1999/33

(51) Int. Cl.[6]: **H04N 5/913**

(21) Application number: **98401513.1**

(22) Date of filing: **18.06.1998**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **13.02.1998 EP 98400344**

(71) Applicant:
CANAL+ Société Anonyme
75711 Paris Cedex 15 (FR)

(72) Inventors:
- **Maillard, Michael**
  28130 Maintenon (FR)
- **Benardeau, Christian**
  77600 Bussy Saint Georges (FR)

(74) Representative:
Cozens, Paul Dennis et al
Mathys & Squire
100 Grays Inn Road
London WC1X 8AL (GB)

(54) Method and apparatus for recording of encrypted digital data

(57) A method of recording transmitted digital data in which transmitted digital information CW 96 is encrypted 97 using a recording encryption key E(NE) 98 and the resulting encrypted ECM message 99 stored on recording support medium. An equivalent of the recording encryption key E(NE) 100 is further encrypted by a recording transport key RT(A) 102 to form an EMM message 103 stored on the support medium together with the encrypted ECM message 99.

Fig.10.

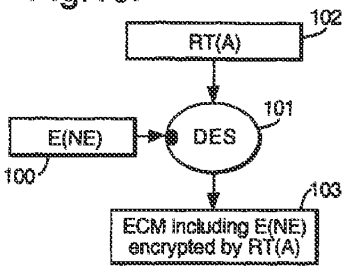
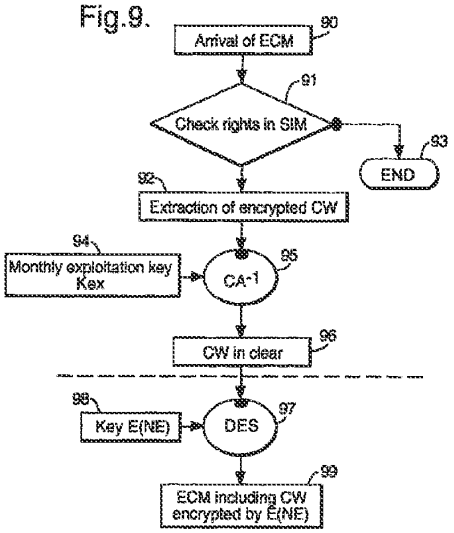


Fig.9.



EP 0 936 812 A1

Printed by Xerox (UK) Business Services
2.16.7/3.6

Description

[0001] The present invention relates to a method and apparatus for recording scrambled digital data, for example television broadcasts.

[0002] Transmission of encrypted data is well-known in the field of pay TV systems, where scrambled audio-visual information is broadcast typically by satellite to a number of subscribers, each subscriber possessing a decoder or integrated receiver/decoder (IRD) capable of descrambling the transmitted program for subsequent viewing.

[0003] In a typical system, scrambled digital data is transmitted together with a control word for descrambling of the digital data, the control word itself being encrypted by an exploitation key and transmitted in encrypted form. A decoder receives the scrambled digital data and encrypted control word which uses an equivalent of the exploitation key to decrypt the encrypted control word and thereafter descramble the transmitted data. A paid-up subscriber will receive periodically the exploitation key necessary to decrypt the encrypted control word so as to permit viewing of a particular program.

[0004] With the advent of digital technology, the quality of the transmitted data has increased many times over. A particular problem associated with digital quality data lies in its ease of reproduction. Where a descrambled program is passed via an analogue link (e.g. the ((Peritel)) link) for viewing and recording by a standard VCR the quality remains no greater than that associated with a standard analogue cassette recording. The risk that such a recording may be used as a master tape to make pirate copies is thus no greater than with a standard shop bought analogue cassette.

[0005] By way of contrast, any descrambled digital data passed by a direct digital link to one of the new generation of digital recording devices (for example, a DVHS recorder) will be of the same quality as the originally transmitted program and may thus be reproduced any number of times without any degradation of image or sound quality. There is therefore a considerable risk that the descrambled data will be used as a master recording to make pirate copies.

[0006] French Patent Application 95 03859 shows one of overcoming this problem, by means of a system in which descrambled digital data is never allowed to be recorded on the digital recording medium. Instead, the decoder described in this application forwards the data for recordal on the support medium in its scrambled form. The control word necessary to descramble the data is re-encrypted by means of another key and stored on the recording support with the scrambled data. This new key is known only to the receiver/decoder and replaces the exploitation key needed to obtain the control word for viewing of the program.

[0007] The advantage of such a system is that the data is never stored in a ((clear))form and cannot be viewed without possession of the new key, stored in the decoder. The system also possesses the advantage that, since the exploitation key changes on a monthly basis, the use of a key chosen by the decoder to re-encrypt the control word registered on the digital tape means that the decoder will still be able to decrypt the control word recorded on the tape even after the end of a subscription month.

[0008] The disadvantage of the system proposed in this previous patent application is that the recording can only be viewed in conjunction with that particular decoder. If that decoder breaks down, or is replaced, the recording can no longer be replayed. Equally, it is not possible to play the recording directly in a digital recorder without connecting the decoder in the system.

[0009] It is an object of the present invention in its broadest and specific aspects to overcome some or all of the problems associated with this known solution.

[0010] According to the present invention, there is provided a method of recording transmitted digital data in which transmitted digital information is encrypted by a recording encryption key and stored by a recording means on a recording support medium and characterised in that an equivalent of the recording encryption key is encrypted by a recording transport key and stored on the support medium together with the encrypted information.

[0011] The advantage of this method lies in the fact that the specific encryption key used to encrypt the information is itself permanently recorded with the associated encrypted information. In order to facilitate future access, and as will be described below, one or more safeguard copies of the recording transport key may be stored at another location than in the recorder.

[0012] In one embodiment, the information encrypted by the recording encryption key comprises control word information usable to descramble a scrambled data transmission also recorded on the support medium. Other embodiments are conceivable, for example, in which the encrypted information corresponds simply to transmitted data that will be ultimately read or displayed, e.g. the audiovisual information itself rather than a control word used to descramble it.

[0013] In one embodiment, the recording encryption key and/or recording transport key are stored on a portable security module associated with the recording means. This may comprise, for example, any convenient microprocessor and/or memory card device, such as a PCMCIA card, a smart card, a SIM card etc. In alternative realisations, the keys may be stored in a security module permanently embodied in the recording means.

[0014] In one embodiment, the transmitted information is encrypted prior to transmission and received by a decoder means before being communicated to the recording means. The decoder may be physically separate or combined with the recording means. As will be

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0196
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

explained in further detail below, the transmitted information may be in some cases processed and/or reencrypted by the decoder before being communicated to the recording means.

[0015] The decoder means may itself be associated with a portable security module used to store transmission access control keys used to decrypt the transmitted encrypted information. In some embodiments, this may be distinct from the portable security module associated with the recording means. However, in the case of an integrated decoder/recorder, for example, the same security module may be used to hold all keys.

[0016] In one embodiment, the recording encryption key and/or recording transport key function in accordance with a first encryption algorithm and the transmission access control keys function in accordance with a second encryption algorithm.

[0017] For example, the recording encryption and transport keys may use the symmetric DES algorithm, whilst the transmission keys function in accordance with a customised algorithm, unique to the broadcast access control system. This enables the system manager to retain control over the algorithm chosen for the transmission keys whilst allowing a generic algorithm to be used for the keys relating to a recording.

[0018] In one embodiment, the recording transport key is generated at a central recording authorisation unit and a copy of this key communicated to the recording means. In the event of loss or destruction of the key support associated with the recording means a backup copy or at least the means to generate the the transport key will at all times be present at the central recording authorisation unit.

[0019] For security reasons, the recording transport key is preferably encrypted by a further encryption key prior to being communicated to the recording means. This further encryption key may be based, for example, on an encryption key common to all recorder security modules diversified by the serial number of the security module, such that only that security module can read the message.

[0020] In the case where the system comprises a receiver/decoder physically separate from the recording means it may be desirable for the recording means to possess the same access rights as the receiver/decoder, for example to permit the receiver/decoder to simply forward the data stream "as is" to the recorder for processing.

[0021] Accordingly, in one embodiment, a central access control system communicates transmission access control keys to a portable security module associated with the recording means. These may comprise, for example, a double of the keys normally held by the portable security module associated with the decoder and which are used to descramble transmissions.

[0022] In this embodiment, the recording means directly descrambles transmitted information using the transmission access keys prior to re-encryption of the information by the recording encryption key and storage on the support medium.

[0023] In a similar manner as with the communication of the transport key, the central access control system preferably encrypts the broadcast access control keys by a further encryption key prior to their communication to the recording means. This further encryption key may equally comprise an audience key common to all security modules diversified by the serial number of the recording means.

[0024] In order to enable the central access control system to correctly identify the broadcast access keys that need to be forwarded to the recording means, the recording means preferably sends a request to the central access control system including information identifying the broadcast access keys needed, the request being authentified by the recording means using a key unique to the recording means. This may correspond, for example, to the key used to encrypt communications from the central access control system to the recording means.

[0025] In the above realisations of the invention, a number of diverse embodiments have been described, in particular in which a central recording authorisation unit generates and maintains a copy of the recording transport keys and in which a central access control system sends a duplicate set of transmission access control keys to the recording means. Alternative embodiments are possible.

[0026] For example, in one embodiment comprising a decoder means and associated security module and a recording means and associated security module, a copy of the recording transport key is stored in the security module associated with the decoder means. In this way, a backup key for decrypting a recording will always be available even in the event of destruction or loss of the recorder security module.

[0027] The recording transport key may be generated, for example, by the recording means security module and communicated to the decoder means security module or vice versa. For security reasons, the recording transport key is preferably encrypted before communication to the decoder security module and decrypted by a key unique to the security module receiving the recording transport key.

[0028] This unique key and its equivalent may be embedded in the respective security modules at the moment of their creation. However, alternatively, the decoder security module and recording security module carry out a mutual authorisation process, the unique decryption key being passed to the other security module from the encrypting security module depending on the results of the mutual authorisation.

[0029] In one embodiment, the mutual authorisation step is carried out using, inter alia, an audience key known to both security modules diversified by the serial number of each module.

[0030] In a further development of this double security

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0197
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

module embodiment, the decoder means security module possesses transmission access control keys to decrypt the transmitted information in an encrypted form and a session key re-encrypt the information prior to communication to the recording means security module, the recording means security module possessing an equivalent of the session key to decrypt the information prior to encryption by the recording transport key.

[0031] This session key may be generated by the decoder means security module or recording means security module and communicated to the other module in encrypted form using an encryption key uniquely decryptable by the other security module.

[0032] The present invention extends to a recording means for use in the above method, a decoder means and a portable security module for use in each.

[0033] The terms "scrambled" and "encrypted" and "control word" and "key" have been used at various parts in the text for the purpose of clarity of language. However, it will be understood that no fundamental distinction is to be made between "scrambled data" and "encrypted data" or between a "control word" and a "key". Similarly, the term "equivalent key" is used to refer to a key adapted to decrypt data encrypted by a first mentioned key, or vice versa. Unless obligatory in view of the context or unless otherwise specified, no general distinction is made between keys associated with symmetric algorithms and those associated with public/private algorithms.

[0034] The term "receiver/decoder" or "decoder" used herein may connote a receiver for receiving either encoded or non-encoded signals, for example, television and/or radio signals, which may be broadcast or transmitted by some other means. The term may also connote a decoder for decoding received signals. Embodiments of such receiver/decoders may include a decoder integral with the receiver for decoding the received signals, for example, in a "set-top box", such a decoder functioning in combination with a physically separate receiver, or such a decoder including additional functions, such as a web browser or a video recorder or a television.

[0035] As used herein, the term "digital transmission system" includes any transmission system for transmitting or broadcasting for example primarily audiovisual or multimedia digital data. Whilst the present invention is particularly applicable to a broadcast digital television system, the invention may also be applicable to a fixed telecommunications network for multimedia internet applications, to a closed circuit television, and so on.

[0036] As used herein, the term "digital television system" includes for example any satellite, terrestrial, cable and other system.

[0037] There will now be described, by way of example only, a number of embodiments of the invention, with reference to the following figures, in which:

Figure 1 shows the overall architecture of a digital TV system according to this embodiment;

Figure 2 shows the architecture of the conditional access system of Figure 1;

Figure 3 shows the encryption levels in the conditional access system;

Figure 4 shows the layout of a decoder and digital recording device according to this embodiment;

Figure 5 shows in schematic form the organisation of zones within the memory cards associated with the decoder and recorder of Figure 4;

Figures 6 and 7 show the steps in the preparation of messages for communication between the decoder card and a centralised server in this first embodiment;

Figure 8 shows the cryptology architecture of the decoder card in generating a recording encryption key according to this first embodiment;

Figures 9 and 10 show the preparation of ECM and EMM messages for recordal on the digital recording support according to this first embodiment;

Figure 11 shows the decryption steps associated with the replay of a recording in this first embodiment;

Figure 12 shows in schematic form the organisation of zones within the memory cards of the decoder and recording device according to a second embodiment of the invention;

Figures 13 and 14 show the initial mutual authorisation steps and transfer of data between the decoder memory card and the recorder memory card according to this second embodiment;

Figure 15 shows the creation and communication of a session key to be used by both memory cards during recording of a programme in this second embodiment;

Figure 16 shows the operation of the recorder card to generate a recording encryption key in this second embodiment;

Figure 17 shows the treatment of transmission ECMs by the decoder card in order to communicate the control word CW in encrypted form to the recorder card in this second embodiment;

Figures 18 and 19 show the preparation of ECM and EMM messages for recordal on the digital

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0198
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

recording support according to this second embodiment; and

Figure 20 shows communication between a decoder card and a recorder card.

[0038] An overview of a digital television broadcast and reception system 1 is shown in Figure 1. The invention includes a mostly conventional digital television system 2 which uses the MPEG-2 compression system to transmit compressed digital signals. In more detail, MPEG-2 compressor 3 in a broadcast centre receives a digital signal stream (for example a stream of audio or video signals). The compressor 3 is connected to a multiplexer and scrambler 4 by linkage 5. The multiplexer 4 receives a plurality of further input signals, assembles one or more transport streams and transmits compressed digital signals to a transmitter 6 of the broadcast centre via linkage 7, which can of course take a wide variety of forms including telecom links.

[0039] The transmitter 6 transmits electromagnetic signals via uplink 8 towards a satellite transponder 9, where they are electronically processed and broadcast via a notional downlink 10 to earth receiver 11, conventionally in the form of a dish owned or rented by the end user. The signals received by receiver 11 are transmitted to an integrated receiver/decoder 12 owned or rented by the end user and connected to the end user's television set 13. The receiver/decoder 12 decodes the compressed MPEG-2 signal into a television signal for the television set 13.

[0040] A conditional access system 20 is connected to the multiplexer 4 and the receiver/decoder 12, and is located partly in the broadcast centre and partly in the decoder. It enables the end user to access digital television broadcasts from one or more broadcast suppliers. A smartcard, capable of decrypting messages relating to commercial offers (that is, one or several television programmes sold by the broadcast supplier), can be inserted into the receiver/decoder 12. Using the decoder 12 and smartcard, the end user may purchase events in either a subscription mode or a pay-per-view mode.

[0041] An interactive system 17, also connected to the multiplexer 4 and the receiver/decoder 12 and again located partly in the broadcast centre and partly in the decoder, may be provided to enable the end user to interact with various applications via a modemmed back channel 16.

[0042] The conditional access system 20 will now be described in more detail. With reference to Figure 2, in overview the conditional access system 20 includes a Subscriber Authorization System (SAS) 21. The SAS 21 is connected to one or more Subscriber Management Systems (SMS) 22, one SMS for each broadcast supplier, by a respective TCP-IP linkage 23 (although other types of linkage could alternatively be used). Alternatively, one SMS could be shared between two broadcast suppliers, or one supplier could use two SMSs, and soon.

[0043] First encrypting units in the form of ciphering units 24 utilising "mother' smartcards 25 are connected to the SAS by linkage 26. Second encrypting units again in the form of ciphering units 27 utilising mother smartcards 28 are connected to the multiplexer 4 by linkage 29. The receiver/decoder 12 receives a portable security module, for example in the form of "daughter" smartcard 30. It is connected directly to the SAS 21 by Communications Servers 31 via the modemmed back channel 16. The SAS sends, amongst other things, subscription rights to the daughter smartcard on request.

[0044] The smartcards contain the secrets of one or more commercial operators. The "mother" smartcard encrypts different kinds of messages and the "daughter" smartcards decrypt the messages, if they have the rights to do so.

[0045] The first and second ciphering units 24 and 27 comprise a rack, an electronic VME card with software stored on an EEPROM, up to 20 electronic cards and one smartcard 25 and 28 respectively, for each electronic card, one card 28 for encrypting the ECMs and one card 25 for encrypting the EMMs.

[0046] The operation of the conditional access system 20 of the digital television system will now be described in more detail with reference to the various components of the television system 2 and the conditional access system 20.

Multiplexer and Scrambler

[0047] With reference to Figures 1 and 2, in the broadcast centre, the digital audio or video signal is first compressed (or bit rate reduced), using the MPEG-2 compressor 3. This compressed signal is then transmitted to the multiplexer and scrambler 4 via the linkage 5 in order to be multiplexed with other data, such as other compressed data.

[0048] The scrambler generates a control word used in the scrambling process and included in the MPEG-2 stream in the multiplexer. The control word is generated internally and enables the end user's integrated receiver/decoder 12 to descramble the programme.

[0049] Access criteria, indicating how the programme is commercialised, are also added to the MPEG-2 stream. The programme may be commercialised in either one of a number of "subscription" modes and/or one of a number of "Pay Per View" (PPV) modes or events. In the subscription mode, the end user subscribes to one or more commercial offers, or "bouquets", thus getting the rights to watch every channel inside those bouquets. In the preferred embodiment, up to 960 commercial offers may be selected from a bouquet of channels.

[0050] In the Pay Per View mode, the end user is provided with the capability to purchase events as he wishes. This can be achieved by either pre-booking the

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0199
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

event in advance ("pre-book mode"), or by purchasing the event as soon as it is broadcast ("impulse mode"). In the preferred embodiment, all users are subscribers, whether or not they watch in subscription or PPV mode, but of course PPV viewers need not necessarily be subscribers.

Entitlement Control Messages

[0051] Both the control word and the access criteria are used to build an Entitlement Control Message (ECM). This is a message sent in relation with a scrambled program; the message contains a control word (which allows for the descrambling of the program) and the access criteria of the broadcast program. The access criteria and control word are transmitted to the second encrypting unit 27 via the linkage 29. In this unit, an ECM is generated, encrypted and transmitted on to the multiplexer and scrambler 4. During a broadcast transmission, the control word typically changes every few seconds, and so ECMs are also periodically transmitted to enable the changing control word to be descrambled. For redundancy purposes, each ECM typically includes two control words; the present control word and the next control word.

[0052] Each service broadcast by a broadcast supplier in a data stream comprises a number of distinct components; for example a television programme includes a video component, an audio component, a sub-title component and so on. Each of these components of a service is individually scrambled and encrypted for subsequent broadcast to the transponder 9. In respect of each scrambled component of the service, a separate ECM is required. Alternatively, a single ECM may be required for all of the scrambled components of a service. Multiple ECMs are also generated in the case where multiple conditional access systems control access to the same transmitted program.

Entitlement Management Messages (EMMs)

[0053] The EMM is a message dedicated to an individual end user (subscriber), or a group of end users. Each group may contain a given number of end users. This organisation as a group aims at optimising the bandwidth; that is, access to one group can permit the reaching of a great number of end users.

[0054] Various specific types of EMM can be used. Individual EMMs are dedicated to individual subscribers, and are typically used in the provision of Pay Per View services; these contain the group identifier and the position of the subscriber in that group.

[0055] Group subscription EMMs are dedicated to groups of, say, 256 individual users, and are typically used in the administration of some subscription services. This EMM has a group identifier and a subscribers' group bitmap.

[0056] Audience EMMs are dedicated to entire audiences, and might for example be used by a particular operator to provide certain free services. An "audience" is the totality of subscribers having smartcards which bear the same conditional access system identifier (CA ID). Finally, a "unique" EMM is addressed to the unique identifier of the smartcard.

[0057] EMMs may be generated by the various operators to control access to rights associated with the programs transmitted by the operators as outlined above. EMMs may also be generated by the conditional access system manager to configure aspects of the conditional access system in general.

Programme Transmission

[0058] The multiplexer 4 receives electrical signals comprising encrypted EMMs from the SAS 21, encrypted ECMs from the second encrypting unit 27 and compressed programmes from the compressor 3. The multiplexer 4 scrambles the programmes and sends the scrambled programmes, the encrypted EMMs and the encrypted ECMs to a transmitter 6 of the broadcast centre via the linkage 7. The transmitter 6 transmits electromagnetic signals towards the satellite transponder 9 via uplink 8.

Programme Reception

[0059] The satellite transponder 9 receives and processes the electromagnetic signals transmitted by the transmitter 6 and transmits the signals on to the earth receiver 11, conventionally in the form of a dish owned or rented by the end user, via downlink 10. The signals received by receiver 11 are transmitted to the integrated receiver/decoder 12 owned or rented by the end user and connected to the end user's television set 13. The receiver/decoder 12 demultiplexes the signals to obtain scrambled programmes with encrypted EMMs and encrypted ECMs.

[0060] If the programme is not scrambled, that is, no ECM has been transmitted with the MPEG-2 stream, the receiver/decoder 12 decompresses the data and transforms the signal into a video signal for transmission to television set 13.

[0061] If the programme is scrambled, the receiver/decoder 12 extracts the corresponding ECM from the MPEG-2 stream and passes the ECM to the "daughter" smartcard 30 of the end user. This slots into a housing in the receiver/decoder 12. The daughter smartcard 30 controls whether the end user has the right to decrypt the ECM and to access the programme. If not, a negative status is passed to the receiver/decoder 12 to indicate that the programme cannot be descrambled. If the end user does have the rights, the ECM is decrypted and the control word extracted. The decoder 12 can then descramble the programme using this control word. The MPEG-2 stream is decompressed and translated into a video sig-

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0200
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

nal for onward transmission to television set 13.

Subscriber Management System (SMS)

[0062] A Subscriber Management System (SMS) 22 includes a database 32 which manages, amongst others, all of the end user files, commercial offers, subscriptions, PPV details, and data regarding end user consumption and authorization. The SMS may be physically remote from the SAS.

[0063] Each SMS 22 transmits messages to the SAS 21 via respective linkage 23 which imply modifications to or creations of Entitlement Management Messages (EMMs) to be transmitted to end users.

[0064] The SMS 22 also transmits messages to the SAS 21 which imply no modifications or creations of EMMs but imply only a change in an end user's state (relating to the authorization granted to the end user when ordering products or to the amount that the end user will be charged).

[0065] The SAS 21 sends messages (typically requesting information such as call-back information or billing information) to the SMS 22, so that it will be apparent that communication between the two is two-way.

Subscriber Authorization System (SAS)

[0066] The messages generated by the SMS 22 are passed via linkage 23 to the Subscriber Authorization System (SAS) 21, which in turn generates messages acknowledging receipt of the messages generated by the SMS 21 and passes these acknowledgements to the SMS 22.

[0067] In overview the SAS comprises a Subscription Chain area to give rights for subscription mode and to renew the rights automatically each month, a Pay Per View Chain area to give rights for PPV events, and an EMM Injector for passing EMMs created by the Subscription and PPV chain areas to the multiplexer and scrambler 4, and hence to feed the MPEG stream with EMMs. If other rights are to be granted, such as Pay Per File (PPF) rights in the case of downloading computer software to a user's Personal Computer, other similar areas are also provided.

[0068] One function of the SAS 21 is to manage the access rights to television programmes, available as commercial offers in subscription mode or sold as PPV events according to different modes of commercialisation (pre-book mode, impulse mode). The SAS 21, according to those rights and to information received from the SMS 22, generates EMMs for the subscriber.

[0069] The EMMs are passed to the Ciphering Unit (CU) 24 for ciphering with respect to the management and exploitation keys. The CU completes the signature on the EMM and passes the EMM back to a Message Generator (MG) in the SAS 21, where a header is added. The EMMs are passed to a Message Emitter (ME) as complete EMMs. The Message Generator determines the broadcast start and stop time and the rate of emission of the EMMs, and passes these as appropriate directions along with the EMMs to the Message Emitter. The MG only generates a given EMM once; it is the ME which performs cyclic transmission of the EMMs.

[0070] On generation of an EMM, the MG assigns a unique identifier to the EMM. When the MG passes the EMM to the ME, it also passes the EMM ID. This enables identification of a particular EMM at both the MG and the ME.

[0071] In systems such as simulcrypt which are adapted to handle multiple conditional access systems e.g. associated with multiple operators, EMM streams associated with each conditional access system are generated separately and multiplexed together by the multiplexer 4 prior to transmission.

Encryption Levels of the System

[0072] Referring now to Figure 3, a simplified outline of the encryption levels in the broadcast system will now be described. The stages of encryption associated with the broadcast of the digital data are shown at 41, the transmission channel (eg a satellite link as described above) at 42 and the stages of decryption at the receiver at 43.

[0073] The digital data N is scrambled by a control word CW before being transmitted to a multiplexer Mp for subsequent transmission. As will be seen from the lower part of Figure 3, the transmitted data includes an ECM comprising, inter alia, the control word CW as encrypted by an encrypter Ch1 controlled by a first encryption key Kex. At the receiver/decoder, the signal passes by a demultiplexer DMp and descrambler D before being passed to a television 2022 for viewing. A decryption unit DCh1 also possessing the key Kex decrypts the ECM in the demultiplexed signal to obtain the control word CW subsequently used to descramble the signal.

[0074] For security reasons, the control word CW embedded in the encrypted ECM changes on average every 10 seconds or so. In contrast, the first encryption key Kex used by the receiver to decode the ECM is changed every month or so by means of an operator EMM. The encryption key Kex is encrypted by a second unit ChP using a personalised group key K1(GN). If the subscriber is one of those chosen to receive an updated key Kex, a decryption unit DChP in the decoder will decrypt the message using its group key K1(GN) to obtain that month's key Kex.

[0075] The decryption units DChp and DCh1 and the associated keys are held on a smart card provided to the subscriber and inserted in a smart card reader in the decoder. The keys may be generated, for example, according to any generally used symmetric key algorithm or in accordance with a customised symmetric key

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0201
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

algorithm.

[0076] As will be described, different keys may be associated with different operators or broadcasters as well as with the conditional access system supplier. In the above description, a group key K1(GN) is held by the smart card associated with the decoder and used to decrypt EMM messages. In practice, different operators will have different subscriber unique keys K1 (Op1, GN), K1 (Op2, GN) etc. Each group key is generated by an operator and diversified by a value associated with the group to which the subscriber belongs. Different memory zones in the smart card hold the keys for different operators. Each operator may also have a unique key associated solely with the smart card in question and an audience key for all subscribers to the services provided by that operator (see above).

[0077] In addition, a set of keys may also be held by the manager of the conditional access system. In particular, a given smart card may include a user specific key K0 (NS) and an audience key K1 (C), common to all smart cards. Whilst the operator keys are generally used to decode EMM messages associated with broadcast rights, the conditional access manager keys may be used to decrypt EMM messages associated with changes to conditional access system in general, as will be described below.

[0078] The above description of the system shown in Figure 3 relates to the implementation of access control in a broadcast system in which transmissions are descrambled by a decoder and displayed immediately. Referring to Figure 4, the elements of an access control system for recordal and repaying of scrambled transmission will now be described.

[0079] As before, a decoder 12 receives scrambled broadcast transmissions via a receiver 11. The decoder includes a portable security module 30, which may conveniently take the form of a smart card, but which may comprise any other suitable memory or microprocessor device. The decoder 12 includes a modem channel 16, for example, for communicating with servers handling conditional access information and is also adapted to pass descrambled audiovisual display information, e.g. via a Peritel link 53, to a television 13. The system additionally includes a digital recorder 50, such as a DVHS or DVD recorder, adapted to communicate with the decoder, for example, via an IEEE 1394 bus 51. The recorder 50 receives a digital support (not shown) on which information is recorded.

[0080] The recorder 50 is further adapted to function with a portable security module 52 containing, inter alia, the keys used to control access to the replaying of a recording. The portable security module may comprise any portable memory and/or microprocessor device as is conventionally known, such as a smart card, a PCMCIA card, a microprocessor key etc. In the present case, the portable security module 52 has been designated as a SIM card, known from the field of portable telephones.

[0081] The digital recorder 50 includes a direct link 54 to the display 13. In alternative realisations, digital audiovisual information may be passed from the recorder 50 to the decoder 12 prior to display. Equally, whilst the elements of decoder 12, recorder 50 and display 13 have been indicated separately, it is conceivable that some or all of these elements may be merged, for example, to provide a combined decoder/television set or combined decoder/recorder etc.

[0082] Similarly, whilst the invention will be discussed in relation to the recording of audiovisual broadcast information, it may also conveniently be applied, for example, to broadcast audio information subsequently recorded on a DAT or minidisc recorder or even a broadcast software application recorded on the hard disc of a computer.

[0083] A first and second embodiment of the invention will now be described with reference to Figures 5 to 11 and 12 to 19, respectively. In the first embodiment a central server is used to handle the generation and safeguard of the keys permitting access to a recording. Furthermore, in this embodiment, the real time decryption and descrambling of a broadcast is carried out by the SIM card of the recorder prior to recordal. In the second embodiment, the decoder smart card manages the safeguard of recording access keys and also plays a part in the real time decryption and decoding of broadcast transmissions.

First Embodiment

[0084] Referring to Figure 5, the structure of the memory zones in the smart card 30 and SIM card 52 associated with the decoder and recorder, respectively, will now be described.

[0085] As shown, the decoder smart card 30 includes a number of keys adapted to function with a symmetric encryption/decryption algorithm associated with the conditional access system. In the present example, a custom algorithm "CA" is used for operations generally associated with access to the broadcast transmission. This is to distinguish from the operations carried out by the SIM card 52 using the DES algorithm and which are generally associated with the recordal and playback of information on the digital support (see below).

[0086] The first set of keys, associated with the conditional access system manager indicated in the zone 55, are implanted in the smart card at the moment of personalisation. These keys include a key K0 diversified by a number NS unique to that card. The system manager zone 55 may also include other keys, such as an audience key K1 (not shown) diversified by a constant C and common to all smart cards handled by the conditional access system manager.

[0087] A second zone 56 contains the keys associated with one or more broadcast operators. These keys may be implanted at the moment of personalisation of the card 30 by the conditional access system manager but

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0202
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

are more usually created by means of a special transmitted EMM message at the start up of a decoder.

[0088] As mentioned above, the operator keys may typically include a K0' diversified by a number NS unique to that card, a group key K1' diversified by a group number GN and an audience key K2' diversified by a constant Z and common to all subscriber card addressed by that operator.

[0089] Finally, the smart card includes the value of the unique number NS of that card, implanted at the moment of personalisation and held in the zone 57 of the smart card memory.

[0090] As is shown, the SIM card 52 associated with the digital recorder includes two sections 58, 59 associated with keys and operations carried out using the CA and DES algorithms, respectively. The section 59 associated with operations using the CA algorithm includes a first system manager zone 60 and an operator zone 61. The keys in the system manager zone are implanted in the card at the moment of personalisation by the conditional access system manager and include a key K0 diversified by the serial number NSIM of the SIM card as well as a communications transport key T also diversified by the serial number NSIM of the card. Both keys are unique to the SIM card in question.

[0091] The SIM card further includes an operator zone 61 adapted to store keys associated with one or more operators. In the present Figure 5, the SIM card is shown as it is at the moment of its creation and personalisation by the conditional access system manager and before insertion in a recorder. For this reason, both the operator zone 61 and the DES zone 58 are shown as blank, i.e. without any stored keys.

[0092] Finally, the SIM card includes a zone 63 adapted to hold the unique SIM card serial number NSIM.

[0093] As mentioned above, in this embodiment, the recorder SIM card 52 is adapted to handle the real time decryption and descrambling of broadcast data autonomously and independent of the smart card 30 associated with the decoder. In order to carry out these operations, it is necessary for the recorder SIM card 52 to possess a double of the keys usually held in the system manager and operator zones 55, 56 of the decoder smart card (see Figure 5). As will be described, once the necessary keys are installed in the recorder SIM card 52, the decoder 12 will thereafter pass the broadcast transmission stream "as is" to the digital recorder 50 and card 52.

[0094] In this embodiment, the generation of duplicate broadcast related keys is managed by the central conditional access system 21, the digital recorder 50 acting to transmit a request to the appropriate server, e.g. via the modem link provided by the decoder 12. Alternatively, it may be envisaged that the recorder itself will be equipped with a modem to carry out this request. In this embodiment, the central conditional access system serves to regulate both transmission access control keys and, as will be described recording access control keys

[0095] In order to enable the central conditional access system server to generate a double of the keys associated with the decoder smart card it is necessary that the request message from the recorder SIM card includes an identification of the identity of the decoder smart card (e.g. the smart card serial number NS) as well as providing secured confirmation of its own identity.

[0096] As a first step therefore, the decoder smart card 30 communicates its serial number NS and a list of operators Op1, Op2 etc. to the SIM card 52. For reasons of security, this communication may itself be encrypted by a simple transport encryption algorithm applied to all communications between the decoder 12 and recorder 50. To avoid unnecessary complexity in the Figures, the keys associated with this encryption are not shown. The decider card serial number NS is then stored in the system manager zone of the SIM card.

[0097] The recorder SIM card 52 then sets up a communication with the conditional access system 21 and requests the unique number NMERE of the conditional access system 21 at the conditional access server (see Figure 2). Using the information thus obtained, the recorder SIM card 52 generates a message using the CA algorithm, as shown in Fig. 6.

[0098] In the convention adopted in the accompanying drawings, the symmetric algorithm to be used in a given cryptographic step (CA or DES) is identified within an oval. The data to be encrypted and/or the data serving as a diversifier is identified as arriving via a blacked out input to the oval. See the encryption of the smart card number and operator list at 70 in Figure 6. Decryption steps are distinguished using an inverse power sign, for example CA^{-1} or DES^{-1}.

[0099] As a first step in Figure 6, the smart card number NS and operator list are encrypted by the key K0 (NSIM) as shown at 70 to generate a message 71 comprising the SIM card serial number NSIM and the encrypted data. At a second step 72, the encrypted data is again re-encrypted by the key T (NSIM, NMERE), created by diversifying the key T (NSIM) by a unique value NMERE associated with the conditional access system. As will be understood, the steps 70, 71 may be carried out in the inverse order. The message 73 and signature thus formed are then sent to the conditional access server 21, ciphering unit 24 and mother card 25.

[0100] The conditional access system 21 decrypts the message as shown in Figure 7. The system possesses the original key K0 shown at 76. Diversifying the key K0 with the NSIM value contained in the message, as shown at 77, generates the key K0 (NSIM). The key K0 (NSIM) is first used to validate the signature at 78. In the event that the signature is not valid, the analysis of the message ends, as shown at 81.

[0101] In addition to the key K0, the system also possesses the transport key T or at least the key T

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0203
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

(NMERE) representing the value of this key T diversified by unique conditional access system number NMERE. Diversifying T (NMERE) by the value NSIM contained in the message enables the system to generate the key T (NSIM, NMERE). For the sake of simplicity, the steps in the preparation of this key have not been shown in Figure 7.

[0102] Equipped with keys K0 (NSIM) and T (NSIM, NMERE), the system manager can then decrypt the message at 79 to obtain the decoder smart card serial number NS and the list of operators associated with the subscriber in question. The system manager then further verifies that the list of operators does indeed match the smart card serial number and thereafter assembles in an EMM message the duplicate key values that will be needed by the recorder SIM card to decrypt a transmission, including a duplicate of the smart card system manager key K0 (NS) as well as the various operator keys K0' (Op1, NS), K1' (Op1, GN) etc.

[0103] The access system also prepares a recording transport key RT (A) which will be subsequently used by the SIM card in controlling access during the recording and playback of a digital recording, as will be discussed in more detail below. In accordance with the choice of algorithm preferred for dealing with the recording, this key will be prepared from a DES key RT diversified by a random number A. The key RT is always present in the mother card and a copy of the value A is maintained for safeguard purposes in a database associated with the system operator. In this way, the value RT (A) may be regenerated at any moment.

[0104] The smart card duplicate keys K0 (NS), K0' (Op1, NS), Kex etc. and the recording transport key RT (A) are then formatted into an EMM message sent to the recorder SIM card. For security reasons, this message is encrypted by the key K0 (NSIM) to ensure that only the correct SIM card can obtain this information.

[0105] For any subsequent change or update, for example, in relation to the operator keys or other access rights, the SIM card (as a copy of the smart card) will receive all EMM/ECM messages needed to decrypt broadcast transmissions.

[0106] Referring to Figure 8, the state of the recorder SIM card 52 immediately prior to the recordal of a broadcast transmission will now be described. As shown, the digital recorder card 59 now includes complete system manager and operator zones 60, 61 as well as a stored value the DES recording transport key RT (A) shown at 85. In addition, the card generates a recording encryption key E (NE) shown at 86 and obtained by diversifying at 87 a DES key E shown at 88 by a random value NE shown at 89. In this case, the key E(NE) is used as a type of session key and may be changed between recordings. The pair of keys E (NE) and RT (A) will subsequently be used in all encryption and decryption of the digital recording.

[0107] Referring to Figure 9, the steps in the treatment by the recorder of an ECM message associated with a broadcast transmission will now be described. After the arrival of an ECM message at 90, the card verifies at 91 that it has the rights to read this particular transmission, for example, that it is a transmission from one of the operators in its list of operators. If so, the encrypted control word CW is extracted from the ECM at the step 92. If not, the processing stops at step 93. Using that month's exploitation key Kex for the operator in question shown at 94, the card decodes at 95 the encrypted value to obtain the control word CW in clear, as shown at 96.

[0108] The recorder card then re-encrypts at 97 the control word CW using the DES key E (NE) shown at 98 and prepares an ECM including the newly encrypted control word for insertion in the data stream to replace the previous ECM. The scrambled transmission together with the sequence of new ECM messages are then recorded on the support in the digital recorder.

[0109] Simultaneously and as shown at step 101 in Figure 10, the SIM recorder card encrypts the value E (NE) shown at 100 using the recording transport key RT (A) shown at 102, so as to generate a special EMM type message 103. This EMM message is then recorded on the digital recording support at the start or header of the recording. As will be understood from the foregoing description, other than the safeguard copy held at the conditional access system database, the key RT (A) is unique to the recorder card and this EMM message may not be decrypted by cards other than the recorder card that generated the message.

[0110] Referring to Figure 11, the steps in the decryption and descrambling of a recording will now be described. Firstly, the EMM message 111 at the head of the recording is decrypted at 110 using the recording transport key 112 stored in the SIM card. Assuming the EMM message was originally created using the same recording transport key the result of the decryption step 110 will be the recording encryption key E (NE) at 116.

[0111] As the recording is played, ECMs 113 are picked out from the data stream and decrypted at step 114 using the recording encryption key E (NE) to obtain at step 115 the control word CW used to scramble that part of the data stream associated with the ECM. This control word CW is then fed together with the scrambled audiovisual data to a descrambling unit, either in the recorder SIM card or in the recorder itself, and a descrambled audiovisual output obtained for subsequent display via the television display or the like.

[0112] As will be understood, the presence of a safeguard means for preparing a copy of the transport key RT (A) at the mother card 25 of the central access control system means that, in the event of loss or destruction of the recorder SIM card 25, it will be possible to reconstruct a new recorder card to allow playback of previously made recordings.

[0113] The above embodiment is particularised by the fact that the recording transport key RT (A) is generated and safeguarded at a central server and also by the fact

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0204
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

that the recorder SIM card contains a duplicate of the necessary operator keys to independently decrypt and descramble a real time transmission. The second embodiment, described below in Figures 12 to 19 does not suffer from these constraints, but describes a realisation in which the decoder smart card plays a more important role.

Second Embodiment

[0114] Referring to Figure 12, the structure of the conditional access zones in the decoder smart card 30 and recorder SIM card 52 in such a system are shown. As before, both cards include zones reserved for operations using the CA algorithm and storage of key data, in particular system manager zones 55, 60 and operator zones 56, 61.

[0115] In the present embodiment, the system manager zone 55 of the decoder card 30 includes, in addition to the key K0 (NS), an audience key K1 (C) common to all cards personalised and managed by the system manager and formed by the diversification of a CA key by a constant value C. This key K1 (C) is also present in the system management zone 60 of the recorder card 52.

[0116] The other significant change in comparison with the zone structure of the previous embodiment is that the smart card 30 is additionally provided with the DES algorithm and includes a DES operating zone 120.

[0117] In order to enable the decoder smart card and recorder SIM card to work together and, in particular, to enable the eventual generation of a recording transport key TR, it is necessary for a mutual authentification of both cards to be carried out.

[0118] As shown in Figure 13, as a first step 121 the recorder SIM card 52 requests a random number from the decoder smart card 30 which returns the number A1 at 122. This number is then used to diversify the audience key K1 (C) at step 123 to generate the key K1 (C, A1) shown at step 124. The SIM card then generates a second random number A2 shown at 125, which is in turn encrypted by the key K1 (C, A1) at 126. Before communication to the smart card, this message is again encrypted and signed at 128 by a second key K1 (C, NSIM) shown at 127 and formed by diversifying the audience key K1 (C) by the value NSIM. The message 129 thus formed is sent as a request for serial number NS and associated individual key K0(NS) to the decoder smart card 30.

[0119] Referring to Figure 14, on arrival at the decoder smart card 30, the communicated value NSIM is used by the smart card to generate the key K1 (C, NSIM). The value of A2 is then decrypted at 130 using this key and the key K1 (C, A1) obtained by the smart card using the random number A1 that it had previously generated and stored in its memory.

[0120] This random number value A2 obtained at 131 is then used to diversify the audience key K1 (C) to obtain the key K1 (C, A2) shown at 132. The key K1 (C, A2) then encrypts the smart card unique serial number NS and system key K0 (NS) at 133 to create the message 134.

[0121] As before, this message is then re-encrypted at 135 using the key K1 (C, NSIM) shown at 136 and the message returned to the recorder SIM card 52 as shown at 137.

[0122] The recorder SIM card generates the keys K1 (C, A2) and K1 (C, NSIM) shown at 138 by diversifying the key K1 (C) by the NSIM serial number and the previously generated and memorised random number A2. These keys are used to decrypt at 139 the messages so as to obtain the unique serial number NS and unique system manager key K0 (NS) of the smart card, this information thereafter being recorded in the memory of the recorder SIM card at 140.

[0123] Unlike the previous embodiment, in which doubles of all system manager and operator keys were taken to ensure independent operation of the recorder SIM card, the double key K0 (NS) and the smart card serial number NS are used to set up a session key for recording and to enable secure communication between the cards during a recording session, notably to enable secure communication of a recording transport key.

[0124] In this embodiment, the initial decryption of the CW is handled by the smart card using the operator keys and monthly exploitation keys that it possesses. Whilst it is conceivable that the control word CW could be passed directly to the SIM card during the creation of a recording it is desirable for security reasons to use a session key to transport the control word CW for this purpose.

[0125] Figure 15 shows one way of creating such a key. As shown, the recorder SIM card picks a random key K3 shown at 141 and diversifies this key at 142 with the SIM card serial number NSIM shown at 143. The key K3 may be taken from any one of a number of such keys stored for this purpose in the system manager zone. The CA session key K3 (NSIM) thus created at 144 is then encrypted at 145 using the previously obtained smart card system manager key K0 (NS) shown at 146. The message 147 thus generated is thereafter transmitted to the decoder smart card 55 which uses its key K0 (NS) to decrypt the message at 148 and store the session key K3 (NSIM) in the memory of the card at step 149.

[0126] Referring to Figure 16, the state of the recorder SIM card prior to a recording operation will now be described. The system manager zone 60 includes the smart card key K0 (NS) and the session key K3 (NSIM) as well as the normally present system keys K0 (NSIM) etc. (not shown). In addition, the card creates a DES recording encryption key from a DES key E shown at 150 by diversifying this key at 151 by a random value NE shown at 152. As before, the resulting recording encryption key E (NE) will be used in the re-encryption

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0205
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

of the control words associated with a program. Similarly, a recording transport key RT (A) shown at 153 is generated to be used to encrypt the recording encryption key E (NE) also recorded on the digital support medium.

[0127] Unlike the previous embodiment, in which the recording transport key was generated at the access control server, the key RT (A) is generated by the recorder SIM card itself using a DES key diversified by a random number A. In order to safeguard a copy of this key a copy is communicated to the decoder smart card. For obvious security reasons, this copy is communicated in encrypted form, for example, as encrypted by the smart card key K0 (NS) currently stored in the SIM card memory.

[0128] Referring to Figure 20, upon first insertion in the decoder the recorder SIM card 52 first sends a request 190 to the smart card to see if a value of RT(A) has already been generated. An evaluation is carried out by the decoder smart card at 191.

[0129] If the answer is negative, the recorder SIM card 52 generates a random DES key RT at 192, which value is diversified at 193 by a random value A shown at 194 to generate the key RT(A) shown at 195. This key value RT(A) is then encrypted at 196 using the custom algorithm and the key K0(NS) shown at 197 and the resulting message 198 then sent to the decoder smart card 30 for decryption and safeguard of the key RT(A).

[0130] If the determination at 191 is positive, then the previously stored value of RT(A) is sent back at 199 to the recorder SIM card 52.

[0131] Referring to Figure 17, the operations of the decoder smart card 30 during recording of a scrambled transmission will now be described. As mentioned above, in this embodiment, the decoder smart card handles the initial decryption steps using the operator keys before communicating the value of the control word CW to the recorder SIM card 52.

[0132] As shown, the decoder smart card 30 receives an ECM 160 for processing in the operator zone 56. Firstly, the smart card 30 checks that it has the rights to access this program. Assuming that this is the case, the encrypted code word CW is extracted from the ECM at 162 and decrypted at 163 using the appropriate exploitation key Kex shown at 164. Otherwise, the process ends as shown at 165.

[0133] As mentioned above, the clear value of the control word CW shown at 166 cannot be directly communicated to the recorder SIM card. Accordingly, the control word CW is encrypted at 167 using the session key K3 (NSIM) shown at 168 and the resulting value 169 communicated to the recorder card SIM for the next steps in the process.

[0134] Referring to Figure 18, the control word encrypted by the session key is received by the recorder SIM card 52 which carries out a decryption process at 170 using the equivalent of the session key K3 (NSIM) previously stored in memory shown at 171. The clear value of the control word CW at 172 is then passed to the DES zone of the card for encryption at 173 using the recording encryption key E (NE) shown at 174. The resulting encrypted value is then encapsulated in an ECM and inserted in the data stream for recordal with the still scrambled data on the recording support.

[0135] At the same time and in a similar manner to the first embodiment, the recording encryption key value shown at 180 in Figure 19 is encrypted at 181 using the recording transport key RT(A) shown at 182. The resulting encrypted value 183 is encapsulated in an EMM for recordal in the header of the digital recording.

[0136] During replay of the recording, and as described before in relation to Figure 11, the EMM at the start of a recording containing the recording encryption key E (NE) is decrypted by the recorder SIM card using the recording transport key RT (A). The recording encryption key E (NE) is then used to decrypt each ECM so as to obtain the control word CW associated with that particular section of the scrambled recording. The recording is then descrambled and played.

[0137] As will be understood, the presence of a safeguard copy of the recording transport key RT (A) stored in the decoder smart card means that, in the event of loss or breakdown of the recorder SIM card, a replacement recorder card may be generated. Unlike the previous embodiment, however, it is not necessary to use a centralised server to maintain this duplicate copy.

[0138] As will be understood, alternative embodiments may be envisaged. For example, in the above embodiments the encryption recording key E (NE) is generated using a key and a random number. However, in alternative embodiments the key E (NE) may be generated from a key diversified by the serial number of the recording device itself (i.e. not the recorder SIM card) to link a given recording to both the recorder SIM card and the recording device.

[0139] Similarly, certain elements of the first embodiment such as a centralised transport key store and an autonomously operating recorder are independent from each other and may be used in the second embodiment, and vice versa.

Claims

1. A method of recording transmitted digital data in which transmitted digital information is encrypted by a recording encryption key (E(NE)) and stored by a recording means (50) on a recording support medium and characterised in that an equivalent of the recording encryption key (E(NE)) is encrypted by a recording transport key (RT(A)) and stored on the support medium together with the encrypted information.

2. A method as claimed in claim 1 in which the information encrypted by the recording encryption key (E(NE)) comprises control word information (CW)

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0206
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

usable to descramble a scrambled data transmission also recorded on the support medium.

3. A method as claimed in claim 1 or 2 in which the recording encryption key (E(NE)) and/or recording transport key (RT(A)) are stored on a portable security module (52) associated with the recording means (50).

4. A method as claimed in any preceding claim in which the transmitted information is encrypted prior to transmission and received by a decoder means (12) before being communicated to the recording means (50).

5. A method as claimed in claim 4 in which the decoder (50) is associated with a portable security module (30) used to store transmission access control keys (K0(NS), K0'(Op1,NS) etc.) used to decrypt the transmitted encrypted information.

6. A method as claimed in claim 5 in which the recording encryption key (E(NE)) and/or recording transport key (RT(A)) function in accordance with a first encryption algorithm (DES) and the transmission access control keys (K0(NS), K0'(Op1,NS)etc.) function in accordance with a second encryption algorithm (CA).

7. A method as claimed in any preceding claim in which the recording transport key (RT(A)) is generated at a central recording authorisation unit (21,24,25) and a copy of this key communicated to the recording means (50).

8. A method as claimed in claim 7 in which the recording transport key (RT(A)) is preferably encrypted by a further encryption key (K0(NSIM)) prior to being communicated to the recording means (50).

9. A method as claimed in any preceding claim in which a central access control system (21,24,25) communicates transmission access control keys (K0(NS), K0'(Op1,NS) etc.) to the recording means (50).

10. A method as claimed in claim 9 in which the transmission access control keys (K0(NS), K0'(Op1,NS) etc.) are communicated to a portable security module (52) associated with the recording means (50).

11. A method as claimed in claim 9 or 10 in which the recording means (50) directly descrambles transmitted information using the transmission access keys (K0(NS), K0'(Op1,NS) etc.) prior to re-encryption of the information by the recording encryption key (E(NE)) and storage on the support medium.

12. A method as claimed in any of claims 9, 10 or 11 in which the central access control system (21, 24, 25) preferably encrypts the broadcast access control keys (K0(NS), K0'(Op1,NS) etc.) by a further encryption key (K0(NSIM)) prior to their communication to the recording means (50).

13. A method as claimed in any of claims 9 to 12 in which the recording means (50) sends a request to the central access control system including information identifying the broadcast access keys needed (K0(NS), K0'(Op1,NS) etc.), the request being authentified by the recording means (50) using a key (K0(NSIM)) unique to that recording means.

14. A method as claimed in claim 1 using a decoder means (12) and associated security module (30) and a recording means (50) and associated security module (52) and in which a copy of the recording transport key (RT(A)) is stored in the security' module (30) associated with the decoder means (12).

15. A method as claimed in claim 14 in which the recording transport key (RT(A)) is generated by the recording security module (52) or decoder security module (30) and communicated to the other security module.

16. A method as claimed in claim 15 in which the recording transport key (RT(A)) is preferably encrypted before communication to the other security module and decrypted by a key unique (K0(NS)) to that other security module.

17. A method as claimed in claim 16 in which the decoder security module (30) and recording security module (52) carry out a mutual authorisation process, the unique decryption key (K0(NS)) being passed to the other security module from the encrypting security module depending on the results of the mutual authorisation.

18. A method as claimed in claim 17 in which the mutual authorisation step is carried out using, inter alia, an audience key K1(C) known to both security modules (30,52) diversified by the serial number (NS, NSIM) of each module.

19. A method as claimed in any of claims 14 to 18 in which the decoder security module (30) possesses transmission access control keys (K0(NS), K0'(Op1,NS) etc.) to decrypt the transmitted information in an encrypted form and a session key (K3(NSIM)) re-encrypt the information prior to communication to the recording security module (52), the recording security module (52) possessing an

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0207
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

equivalent of the session key (K3(NSIM)) to decrypt the information prior to encryption by the recording transport key (RT(A)).

20. A method as claimed in claim 19 in which the session key (K3(NSIM)) is generated by the decoder security module or recording means security module (52) and communicated to the other module in encrypted form using an encryption key (K0(NS)) uniquely decryptable by the other security module.

21. A recording means (50) adapted for use in a method as claimed in any preceding claim comprising a security module (52) for encrypting transmitted digital information by a recording encryption key (E(NE)) for storage on a recording support medium and characterised in that the security module (52) is further adapted to encrypt the recording encryption key (E(NE)) by a recording transport key (RT(A)) for storage on the support medium.

22. A portable security module (52) adapted for use in the recording means of claim 21 and characterised in comprising a recording encryption key (E(NE)) for encryption of transmitted digital information for subsequent recordal and a recording transport key (RT(A)) for encryption of the recording encryption key for subsequent recordal.

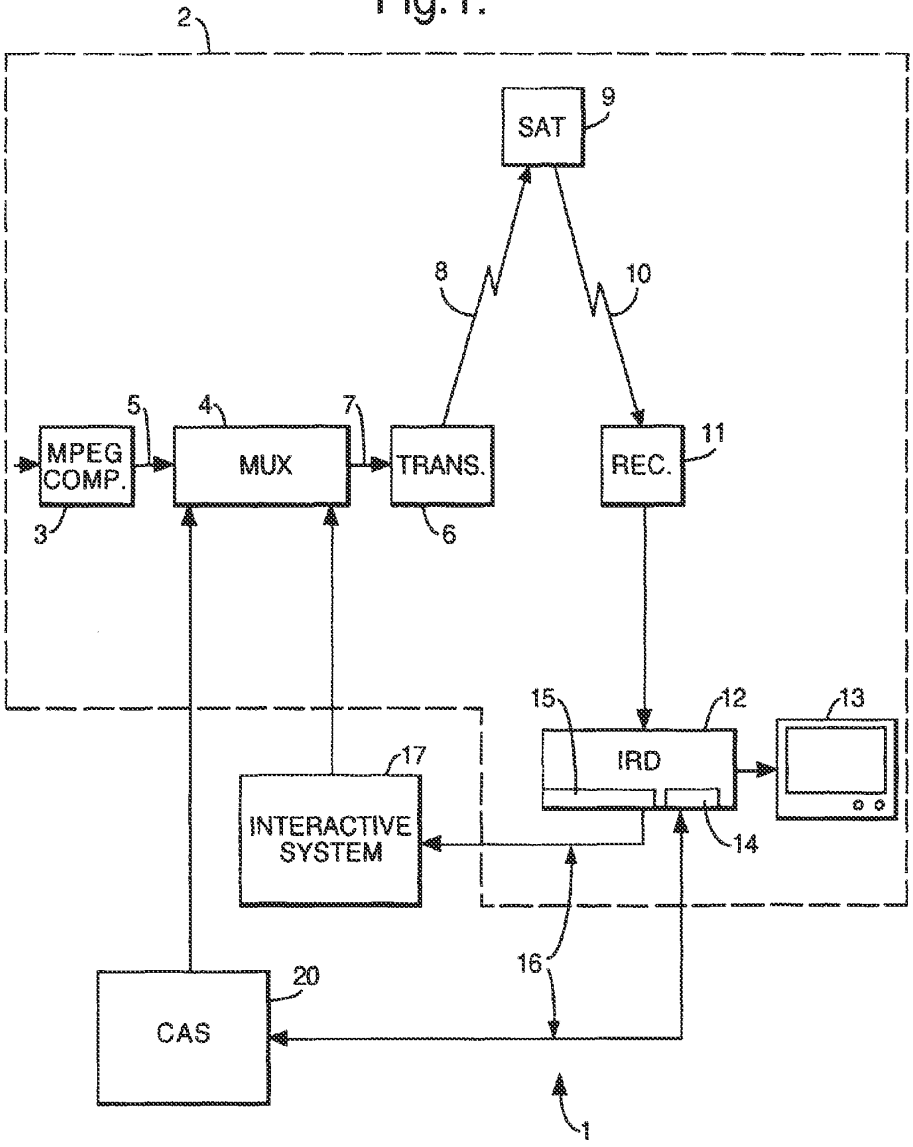
23. A decoder means (20) adapted for use in a method as claimed in any of claims 14 to 20 including a security module (30) adapted to store a copy of the recording transport key (RT(A)).

24. A decoder means (20) as claimed in claim 23 including a security module (30) adapted to descramble transmitted information using one or more transmission access keys (K0(NS), K0'(Op,NS) etc.) prior to reencryption by a session key (K3(NSIM)) for subsequent communication to a recording means.

25. A portable security module (30) adapted for use in the decoder means (20) of claim 23 or 24 and comprising at least a copy of the recording transport key (RT(A)).

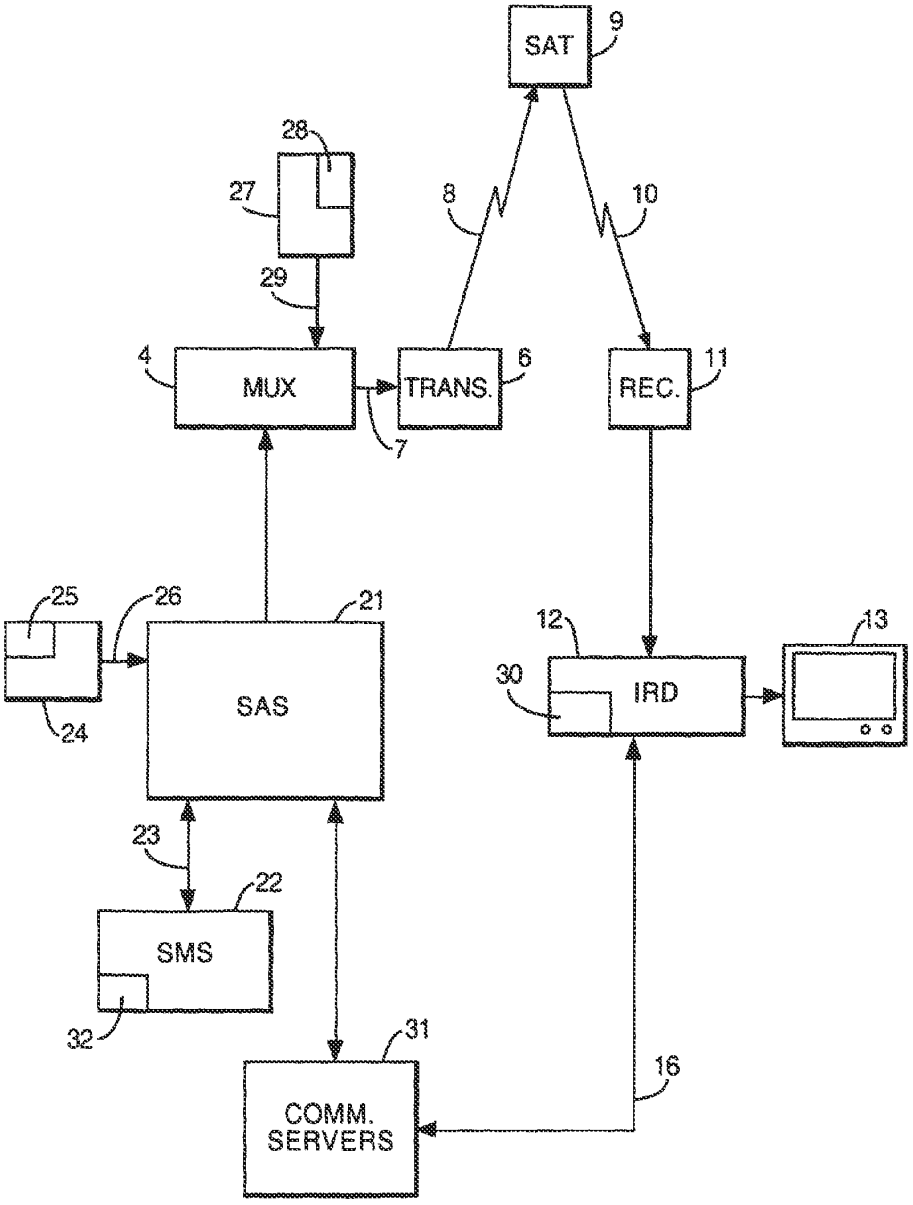
Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0208
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Fig.1.



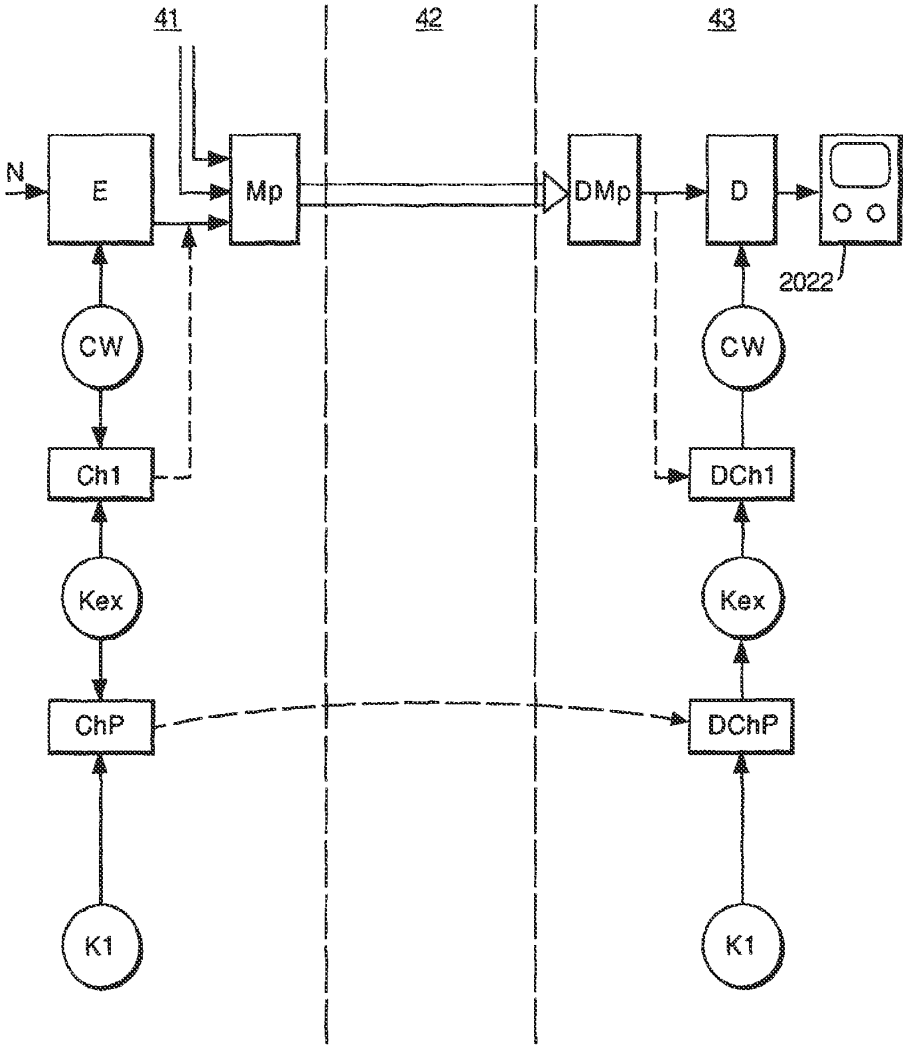
Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0209
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

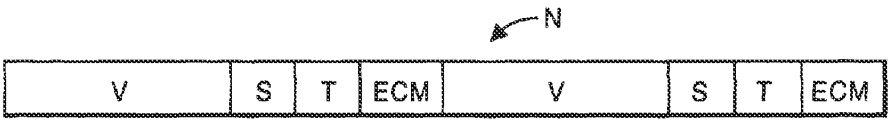
Fig.2.



Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0210
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

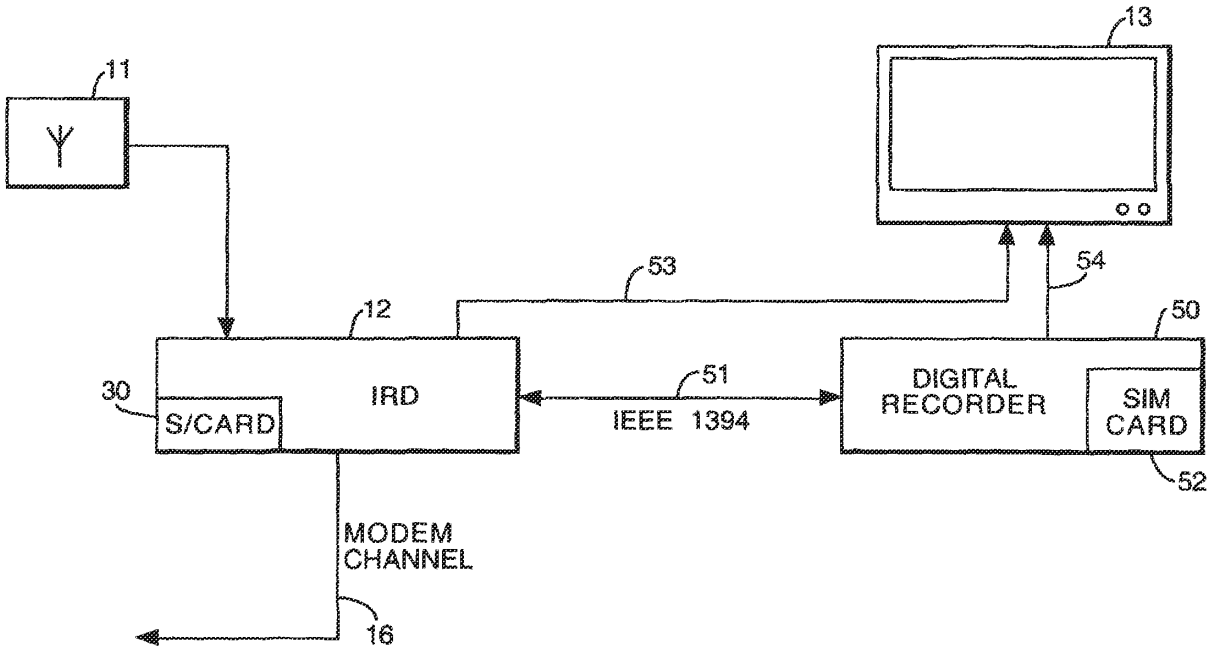
Fig.3.





Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0211
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Fig.4.



EP 0 936 812 A1

Fig.5.

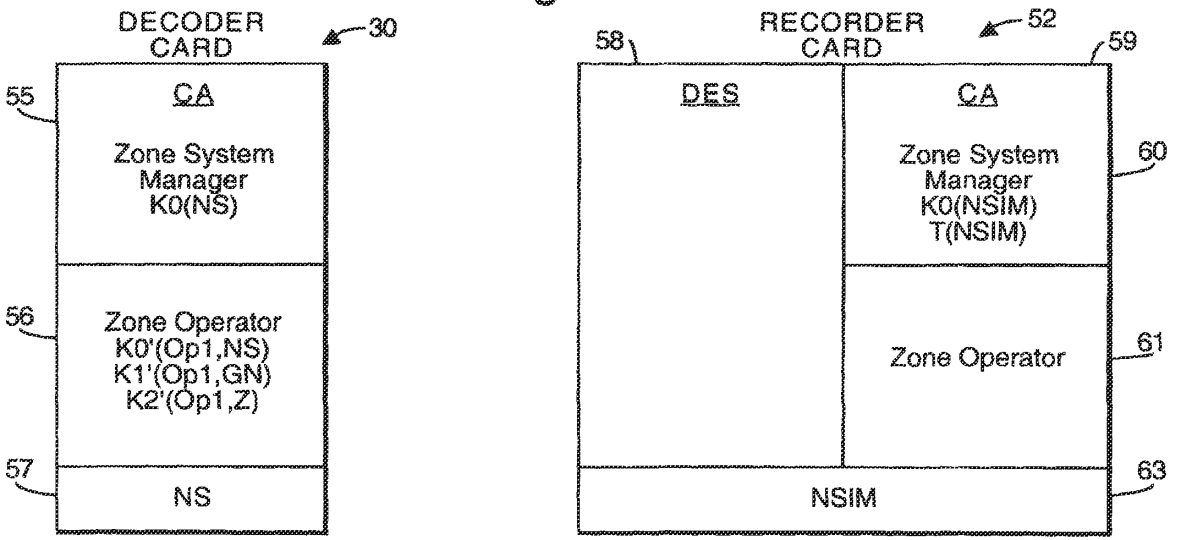

DECODER CARD
30
55
CA
Zone System Manager K0(NS)
56
Zone Operator K0'(Op1,NS) K1'(Op1,GN) K2'(Op1,Z)
57
NS
RECORDER CARD
52
58
59
DES
CA
Zone System Manager K0(NSIM) T(NSIM)
60
Zone Operator
61
NSIM
63

Fig.6.

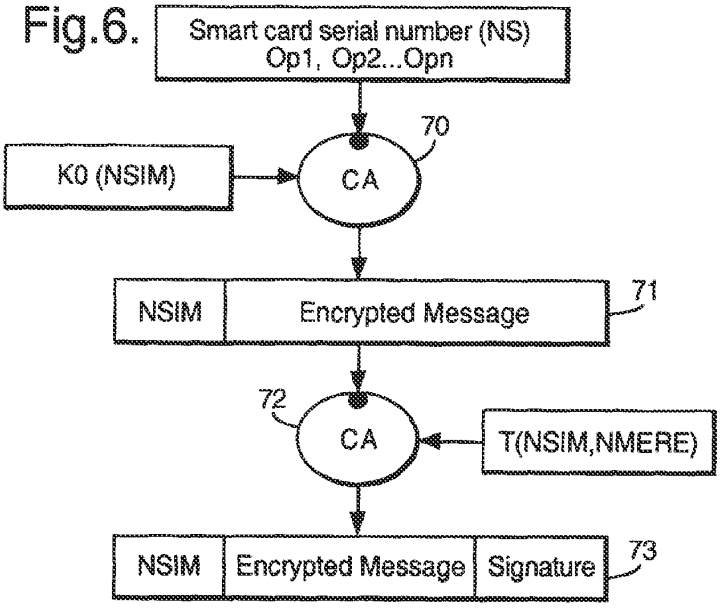
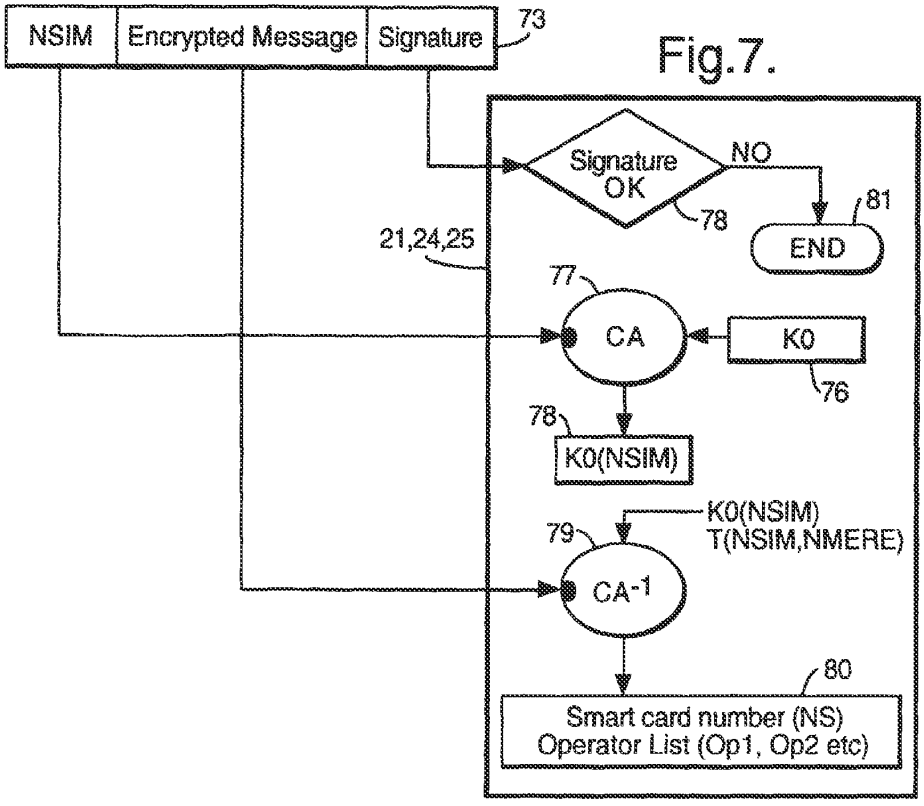


Fig.7.



Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0214
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Fig.8.

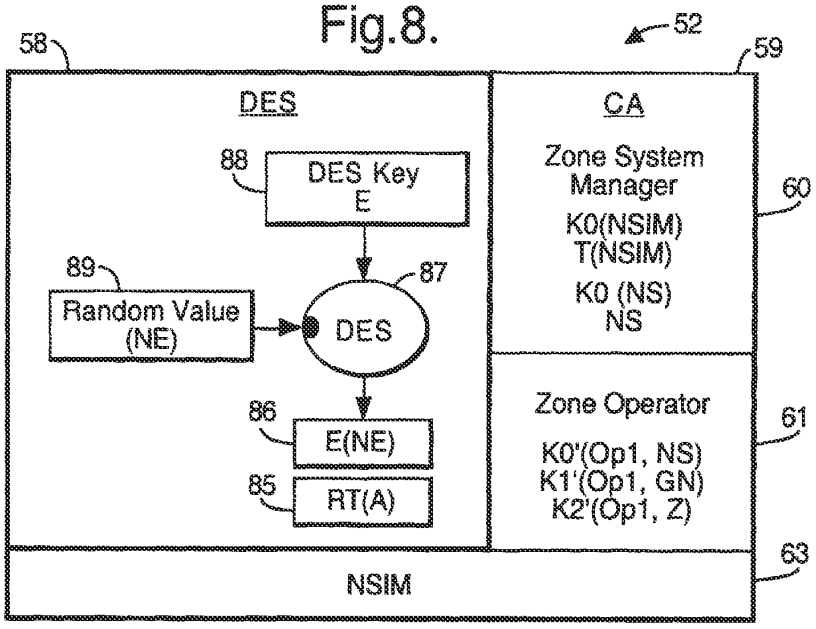
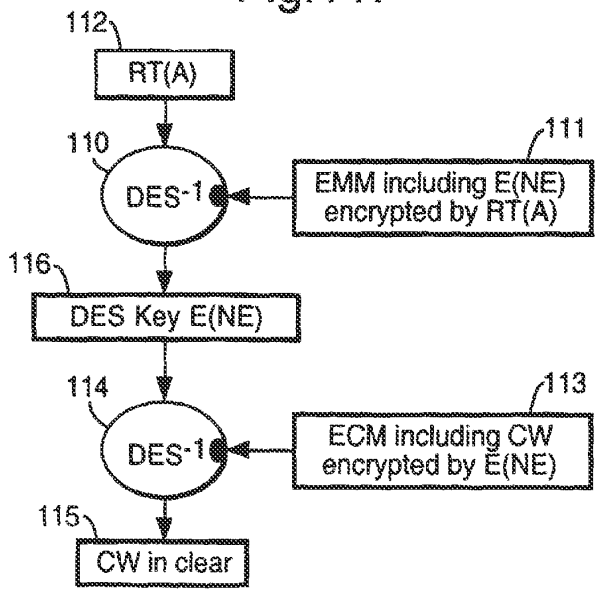


Fig.11.



Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0215
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Fig.9.

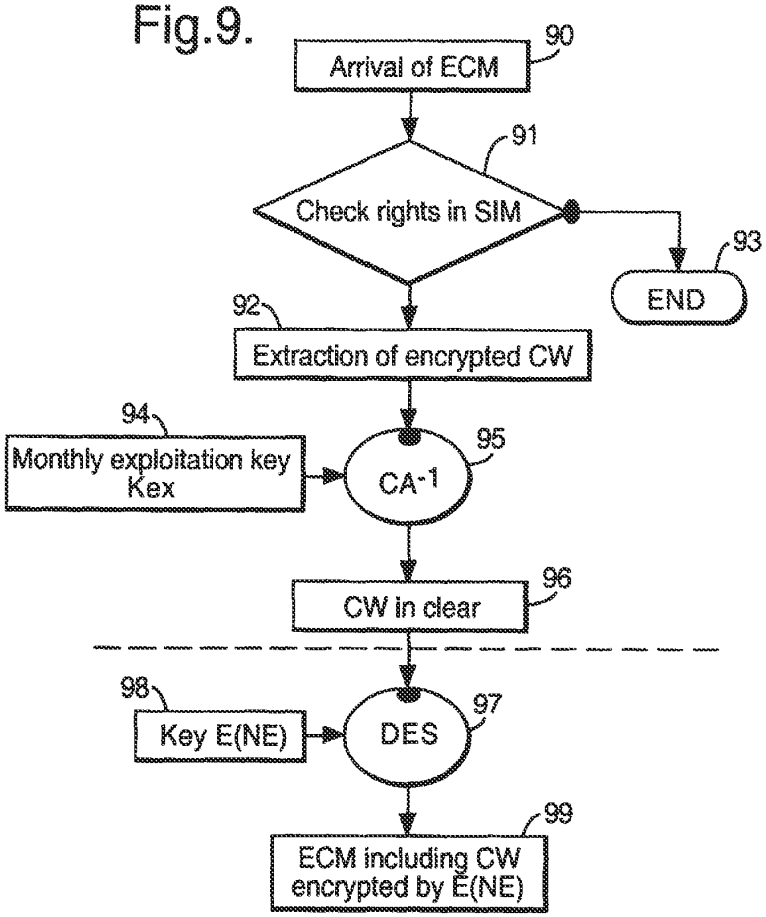
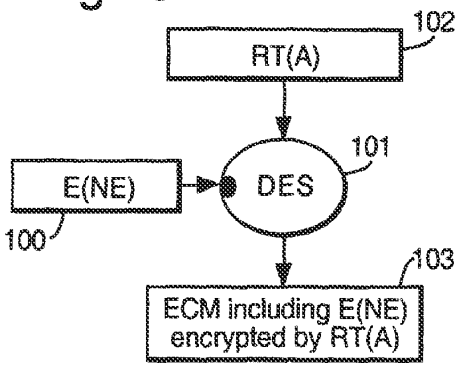
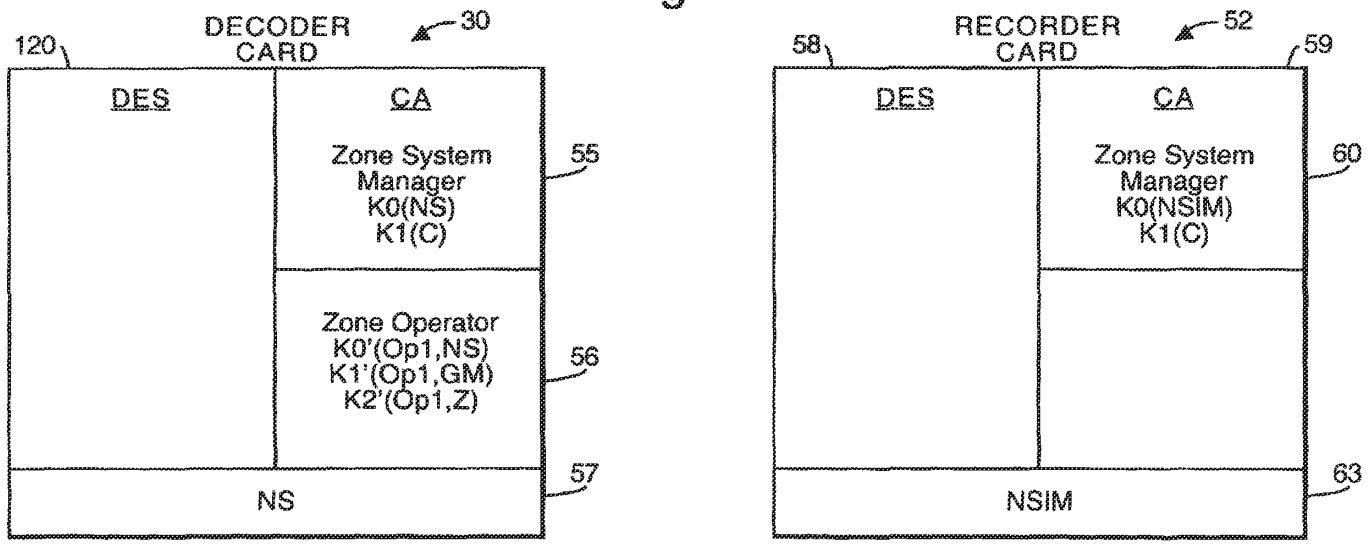


Fig.10.



Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0216
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Fig.12.



EP 0 936 812 A1

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0217
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Fig.13.

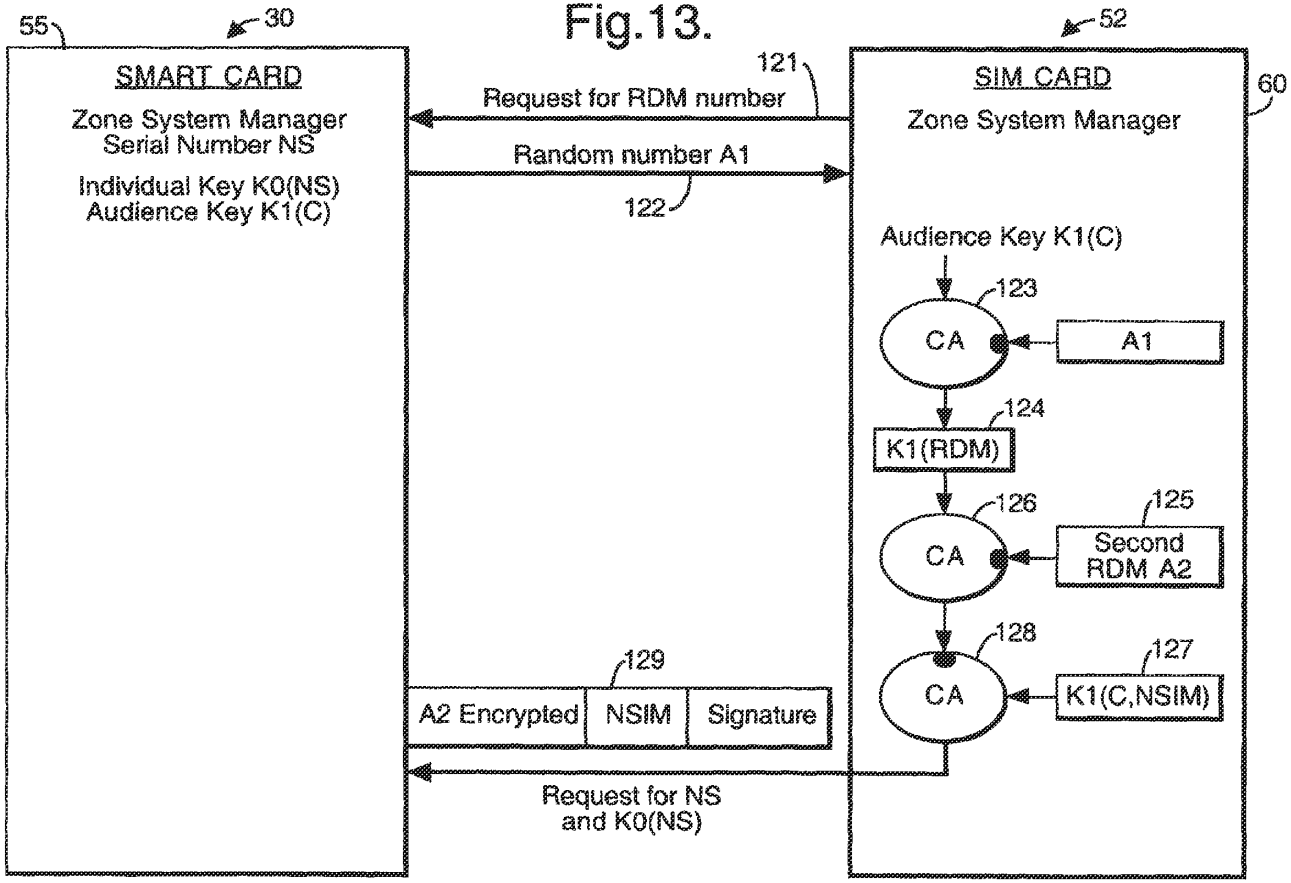
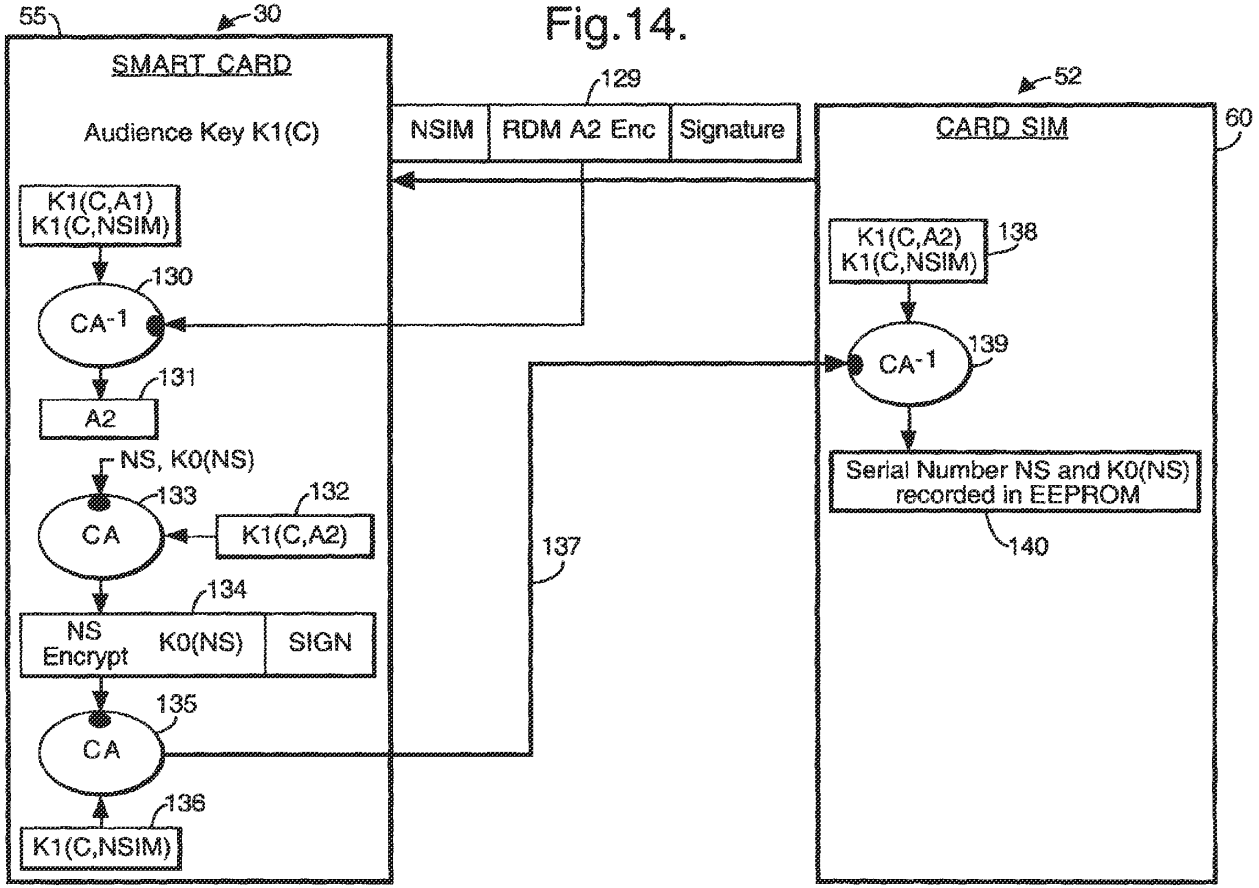

55
30
SMART CARD
Zone System Manager
Serial Number NS
Individual Key K0(NS)
Audience Key K1(C)
121
Request for RDM number
Random number A1
122
52
SIM CARD
Zone System Manager
60
Audience Key K1(C)
123
CA
A1
124
K1(RDM)
126
125
CA
Second
RDM A2
128
127
CA
K1(C,NSIM)
129
A2 Encrypted
NSIM
Signature
Request for NS
and K0(NS)

Fig.14.



EP 0 936 812 A1

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0219
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Fig.15.

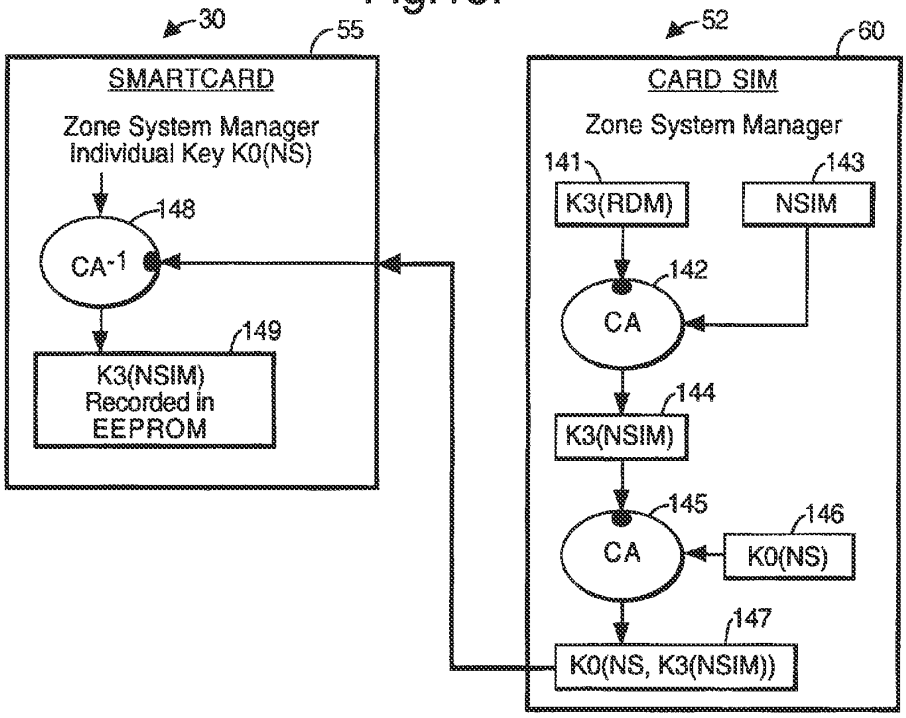
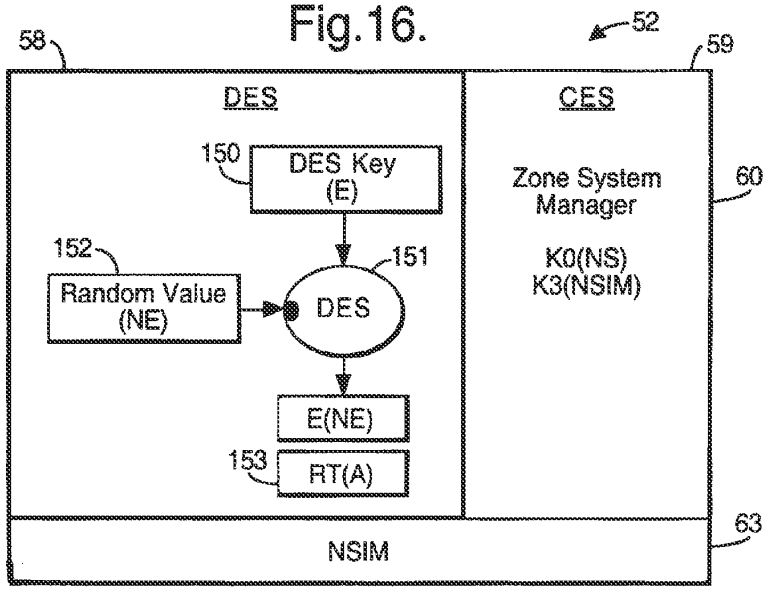
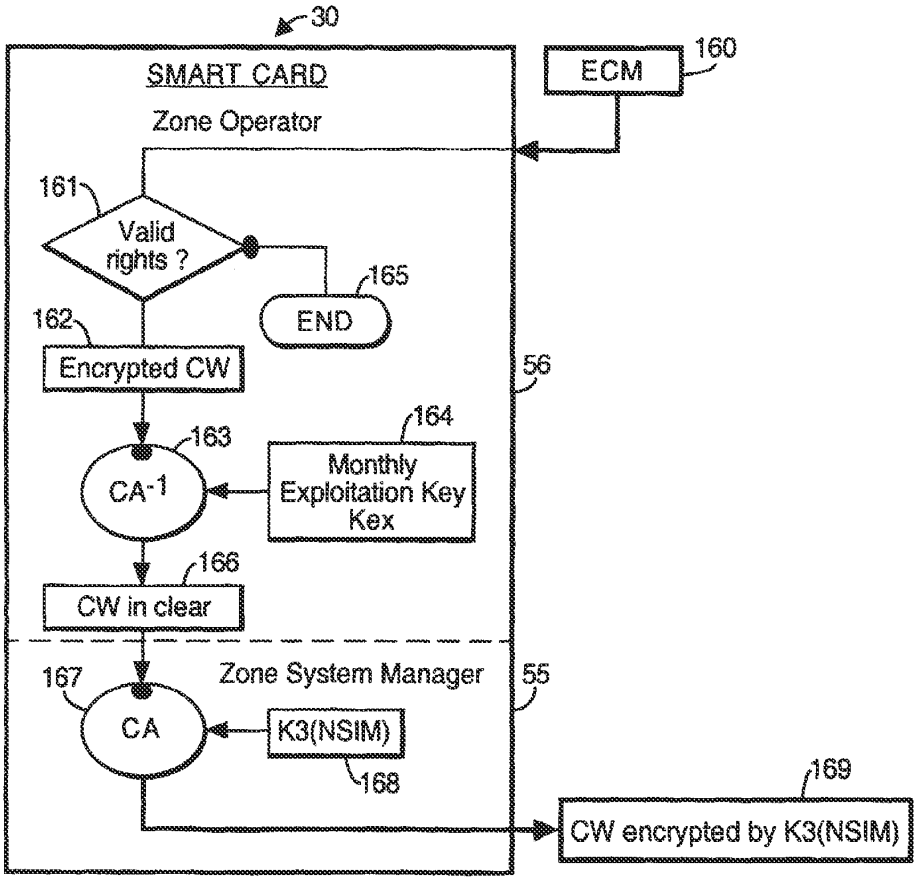


Fig.16.



Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0220
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Fig.17.



Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0221
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Fig.18.

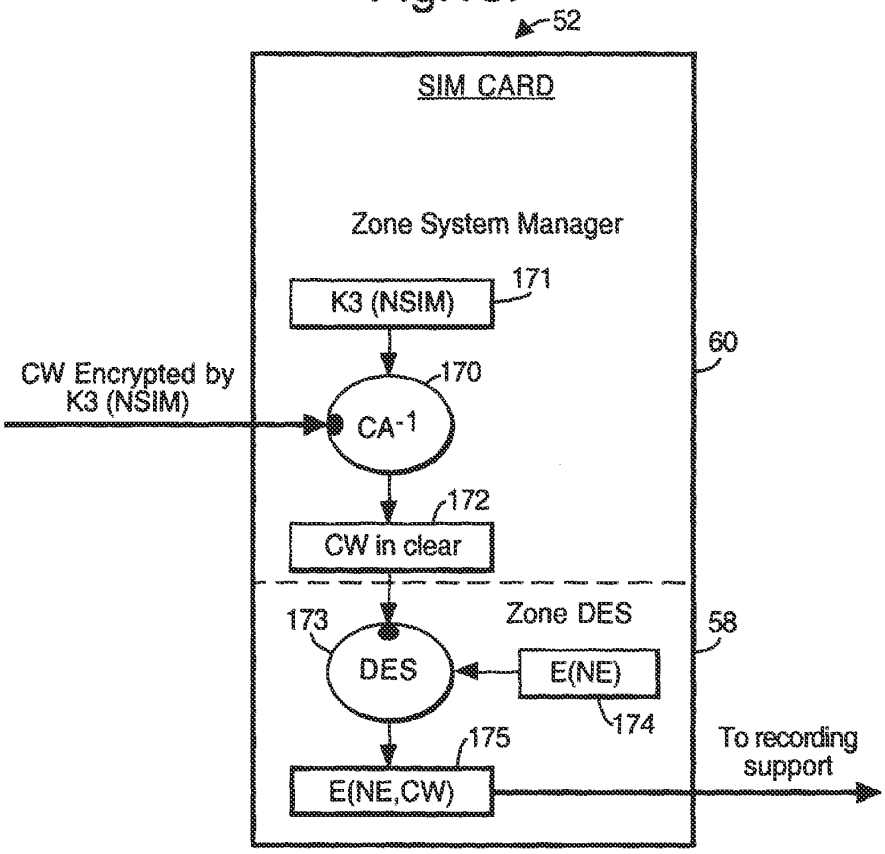
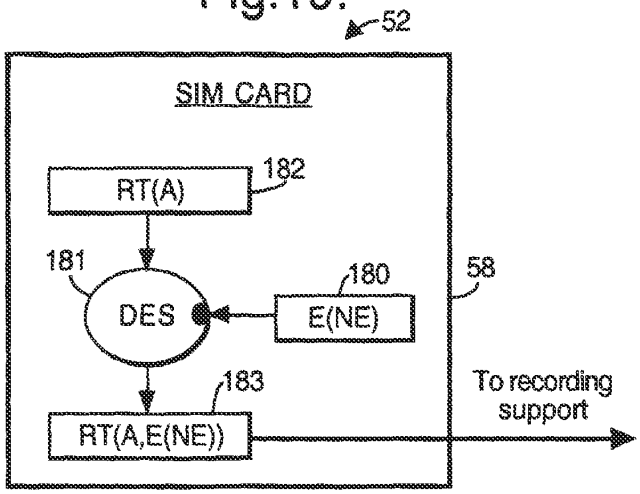
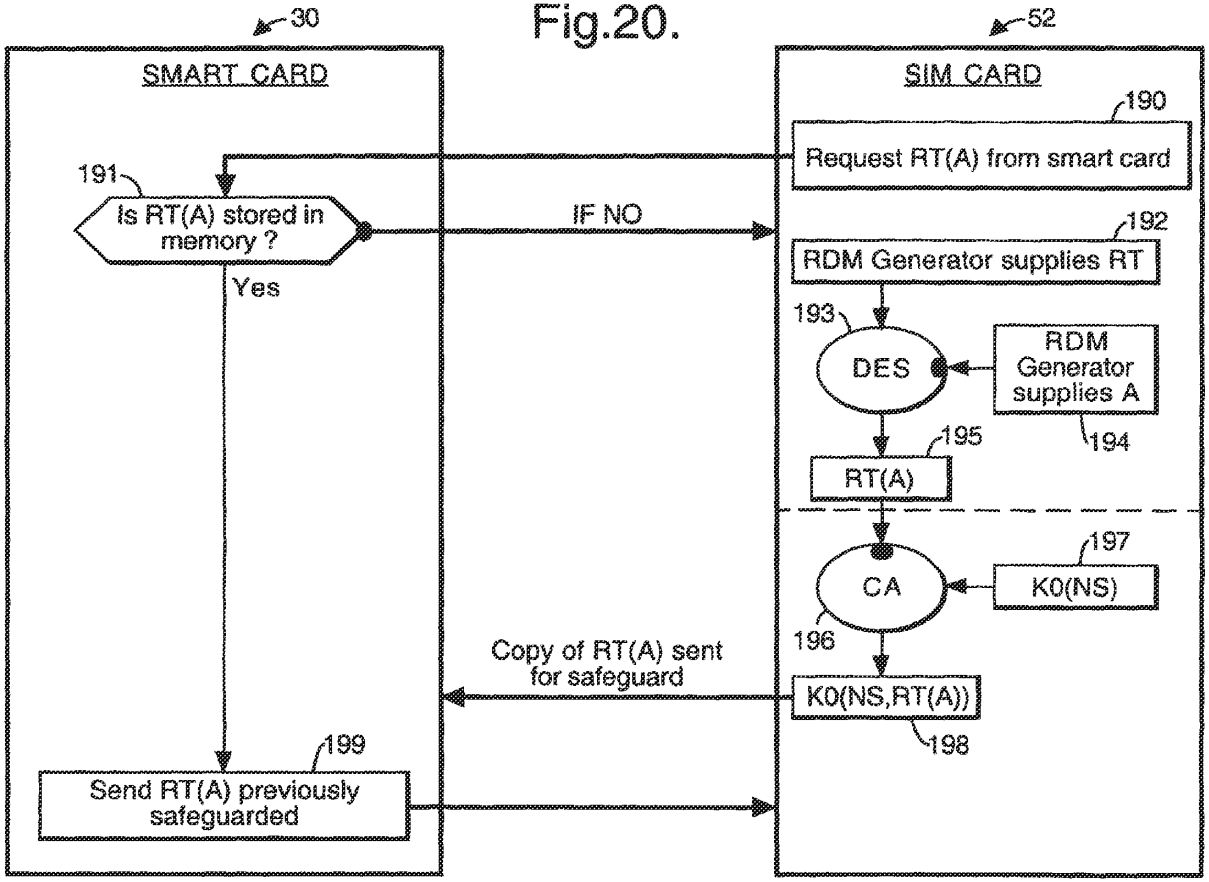


Fig.19.



Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0222
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Fig.20.


30
SMART CARD
52
SIM CARD
190
Request RT(A) from smart card
191
Is RT(A) stored in memory ?
IF NO
192
RDM Generator supplies RT
Yes
193
DES
RDM Generator supplies A
194
195
RT(A)
197
CA
K0(NS)
196
Copy of RT(A) sent for safeguard
K0(NS,RT(A))
198
199
Send RT(A) previously safeguarded

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 98 40 1513

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
D,A	FR 2 732 537 A (CANAL+ SOCIETE ANONYME) 4 October 1996 * the whole document *	1	H04N5/913
A	EP 0 714 204 A (LG ELECTRONICS INC) 29 May 1996 * the whole document *	1	
A	EP 0 763 936 A (LG ELECTRONICS INC) 19 March 1997 * the whole document *	1	

TECHNICAL FIELDS SEARCHED (Int.Cl.6)

H04N

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	7 May 1999	Verleye, J

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0224
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 98 40 1513

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

07-05-1999

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR 2732537 A	04-10-1996	NONE	
EP 714204 A	29-05-1996	CN 1137723 A	11-12-1996
		JP 8242438 A	17-09-1996
		US 5757909 A	26-05-1998
EP 763936 A	19-03-1997	CN 1150738 A	28-05-1997
		JP 9093561 A	04-04-1997
		US 5799081 A	25-08-1998

EPO FORM P0459

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0225
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 September 2001 (07.09.2001)

PCT

(10) International Publication Number
WO 01/65762 A2

(51) International Patent Classification[7]: H04L 9/00

(21) International Application Number: PCT/US01/06911

(22) International Filing Date: 2 March 2001 (02.03.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/186,551 2 March 2000 (02.03.2000) US

(71) Applicant *(for all designated States except US)*: **TIVO, INC.** [US/US]; 2160 Gold Street, P.O. Box 2160, Aviso, CA 95002-2160 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **PLATT, David, C.** [US/US]; 323 Aldean Avenue, Mountain View, CA 94043 (US). **GOODMAN, Andrew** [US/US]; 2171 Avy Avenue, Menlo Park, CA 94025 (US). **ZENCHELSKY, Daniel** [US/US]; 497 San Benito Avenue, Los Gatos, CA 95030 (US).

(74) Agents: **GLENN, Michael** et al.; Glenn Patent Group, Suite L, 3475 Edison Way, Menlo Park, CA 94025 (US).

(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

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

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

WO 01/65762 A2

(54) Title: CONDITIONAL ACCESS SYSTEM AND METHOD FOR PREVENTION OF REPLAY ATTACKS

(57) Abstract: In a conditional access system, a headend transmits content to one or more receivers in encrypted transport streams. The system provides a multi-layer security architecture, rendering the system resistant to key replay attacks; if one layer is circumvented, subsequent layers remain intact. A first layer prevents unencrypted keys from being recorded by shielding the unencrypted keys from users and encrypting the path from the receiver's conditional access module to the transport decryption module; a second layer prevents a key recorded on one receiver from being played back to the transport decryption module on a second receiver; a third layer prevents a user from decrypting transport streams without the encryption module by encrypting the stream a second time prior to being passed through any user-accessible memory or processor. Events tables are transmitted with the transport stream, either unencrypted for immediate use or encrypted, to prevent unauthorized use.

CONDITIONAL ACCESS SYSTEM AND METHOD FOR PREVENTION OF REPLAY ATTACKS

BACKGROUND OF THE INVENTION

TECHNICAL FIELD

The invention relates to security in conditional access systems. More particularly the invention relates to a conditional access system that includes a multi-layer cryptographic security architecture for prevention of replay attacks.

TECHNICAL BACKGROUND

In conditional access systems, such as cable television networks, audio, video, data and other forms of content in electronic form may be broadcast as digital transport streams. The transport stream originates at the system headend and is transmitted to and received by receiver units that display or make use of the transport stream. In order to prevent unauthorized use or viewing of the transport stream, the stream may be encrypted. In such systems, the receiver is capable of decrypting the transport stream prior to viewing or using it.

Typically, the algorithm used to encrypt the transport stream is controlled by an encryption key. When decrypting the transport stream at the receiver end, the receiver must have the key. As a security measure, the key is periodically changed. Because the key is changed on a regular basis, there can be multiple keys required to decrypt the transport stream. The keys are then encrypted and broadcast within the transport stream.

Generally, within the receiver unit of a conditional access system, a Transport Reception Module (TRM) is operative to receive the transport stream transmitted from the headend. Furthermore, a Conditional Access Module (CAM) decides whether or not to decrypt the stream, based on services purchased by the user. If the CAM allows the user to view or otherwise use the transport stream, it decrypts the keys and provides them to the Transport Decryption Module (TDM) for use in decrypting the transport stream. Thus, the TDM is operative to decrypt the transport stream, using the

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0227
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

decrypted keys supplied by the CAM. Following decryption, the decrypted stream is displayed to the user on a display module.

Often, encrypted transport streams are recorded by the receiver and stored for future use. Furthermore, current conditional access systems are subject to replay attacks, particularly key replay attacks, in which unencrypted decryption information is intercepted and recorded as it is being passed to a TDM. Subsequently, the recorded decryption information may then be used at a later time to gain unauthorized access to the encrypted transport streams. For example, User A and User B both record a transport stream containing a particular audio/video stream, such as a movie. User A purchases the service; therefore the CAM in A's receiver will provide keys to use in decrypting the transport stream. User A can record the keys provided by the CAM as they are being passed to the TDM, and send them to User B. Thus, User B is able to decrypt the stream using the keys provided by A, viewing or using the stream without purchasing it.

A. Wasilewski, H. Pinder, G. Akins, M. Palgon, *Conditional access system*, U.S. Patent No. 6,157,719 (December 5, 2000) and R. Banker, G. Akins, *Preventing replay attacks on digital information distributed by network service providers*, U.S. Patent No 6,005,938 (December 21,1999) provide techniques for preventing replay attacks on digital information distributed by network services. At the beginning of a subscription period for a service, a network service provider sends entitlement messages to the subscriber that provide the subscriber with a session key and authorization information, specifying a service and a period of time. When an encrypted service instance is distributed, it is accompanied by entitled control messages. The subscriber equipment that decrypts the service instance does so only if the time specifier in the entitlement control message specifies a time period specified by the authorization information. While the disclosed technique certainly complicates replay attacks by introducing a time element absent in conventional methods, it does not prevent them. In particular, it does not prevent recording and replaying of generated control words or instance keys.

S. Ooi, *Decryptor*, U.S. Patent No. 5,790,666 (August 4, 1998) describes a decryptor within a receiver unit of a conditional access system that includes a descrambler for descrambling signals scrambled at the headend using a pseudo-random noise generator. At the receiver, a pseudo-random noise generator is induced to change its state, through the provision of a scramble key, so that it generates pseudo-random noise signals that descramble the scrambled signal. The encrypted scramble key is transmitted from the headend and decrypted at the receiver after a cascade of conditions is satisfied. The decryptor, as described, provides a robust, multi-layer security apparatus for a conditional access system. Nevertheless, it suffers a vulnerability to

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0228
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

replay attacks common to many conditional access systems. The scramble key, when it has been decrypted, may be intercepted and recorded as it is passed to the descrambler. Subsequently, the recorded key may be replayed, either on the same receiver, or different receivers, creating the possibility of pirating and unauthorized use of the signal.

Accordingly, there exists a need for a way of preventing replay attacks in conditional access systems. It would be desirable to provide protection in multiple layers, so that if one layer is compromised, the other layers remain intact.

SUMMARY OF THE INVENTION

In a conditional access system, a headend transmits content to one or more receivers as encrypted transport streams. The system includes a multi-layer security architecture that renders the system highly resistant to key replay attacks at the receiver. Thus, if one layer is circumvented, the other layers remain intact. A first layer prevents unencrypted keys from being recorded by shielding the unencrypted keys from users and encrypting the path from the receiver's conditional access module (CAM) to the transport decryption module (TDM); a second layer prevents a key recorded on one receiver from being played back to the transport decryption module on a second receiver; and a third layer prevents a user from decrypting transport streams without the encryption module by encrypting the stream a second time prior to being passed through any user-accessible memory or processor.

The multi-layer security architecture is achieved by means of a series of cryptographic procedures between the headend and the various components of the receiver. First is a procedure for pairing the transport components with the CAM in which a random secret generated at the headend is encrypted and transmitted to the transport reception module (TRM), the TDM and the CAM. Each of the three components decrypts the secret and stores it for future use. Second is a transport stream recording procedure that requires a local key, specific to the receiver, generated by the CAM. Third is a procedure for decrypting and replaying the transport stream, also requiring the local key.

An event table for an MPEG stream is constructed in advance of the user purchasing rights to use the stream. In one embodiment, the event table is transmitted unencrypted, along with the corresponding stream, so that the receiver may access the

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0229
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

table without decrypting the stream. In an alternative embodiment, the event table is encrypted to prevent unauthorized use.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 provides a block diagram of a conditional access system that is resistant to replay attacks, according to the invention.

DETAILED DESCRIPTION

The invention provides a conditional access system that is resistant to playback attacks. The invention is also embodied as a cryptographic method for rendering a conditional access system resistant to replay attacks, particularly key replay attacks.

Referring now to Figure 1, shown is a conditional access system that includes a headend 11 and a receiver 12. In actual fact, the system includes a plurality of substantially identical receivers, but the invention is described herein in terms of one receiver. The receiver includes a transport reception module (TRM) 15 for receiving a transport stream 14 from the headend, and saving it to storage component 17. As Figure 1 shows, the transport stream 14 is encrypted by an encryptor 20 prior to transmission. Further, the receiver includes a transport decryption module (TDM) 16 that retrieves the transport stream from storage components 17 and decrypts it when access rights to the steam have been purchased by an end user. Additionally, the receiver includes a conditional access module (CAM) 18 that is operative to decide whether or not to decrypt the stream, based on the serves that the user has purchased. If the CAM allows the user to view or use the transport stream, it decrypts the key required to decrypt the transport stream and provides them to the TDM. The conditional access system 10 incorporates a multi-layer security architecture that prevents key replay attacks at the receiver 12. The novel security architecture relies on conventional encryption technology, applied in a new and unique way. The multi-layer security architecture, based on public key encryption is implemented in a series of cryptographic procedures, described in greater detail below.

By providing multiple layers of security, if one security layer is circumvented, the other layers remain intact, thus providing a much higher degree of protection against replay attacks than is conventionally possible.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0230
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

A first security layer is provided to prevent keys from being recorded from the CAM 18. This is accomplished by never exposing unencrypted keys to the end user or any user programmable processor within the system, or storing them within any user-accessible memory within the system. Furthermore, the communication path between the CAM and the TDM is encrypted.

If, for some reason, the first layer were to fail, and the user were to gain access to the keys, a second layer prevents the keys from being played back to a TDM on another receiver by ensuring that the TDM will not accept the key without it being transformed in a way that is unique to a particular receiver. Thus, a local key is required that is derived from the decryption key provided by the headend. In the current invention, the CAM provides the functionality required to generate local keys. It should be noted that the degree of security provided by this layer is in direct proportion to the degree of difficulty a cracker would encounter in transforming one receiver's key into a key required by a second receiver.

A third layer of security prevents a user from intercepting the transport stream and decrypting it without the TDM. This is accomplished by never exposing the transport stream to the user. Before passing the stream through any user-programmable processor or user-accessible memory, the transport stream must be encrypted a second time. The security of the doubly-encrypted stream is further enhanced by providing an encryption mechanism that produces an encrypted stream that is particular to the receiver, rendering it useless on another receiver.

IMPLEMENTATION

The multi-layer security architecture is implemented as a series of cryptographic procedures, described in detail in Tables 1 – 3, below.

As shown in Figure 1,

The headend 11 has:

- a Global Secret Key: GSK;
- a Headend Private Key;
- receiver's Transport Public Key; and
- Receiver's CAM Public Key.

The TRM 15 has:

- Transport Private Key; and
- Headend Public Key.

Likewise, the TDM 16 also has:

- Transport Private Key; and

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0231
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

- Headend Public Key

The CAM 18 has:

- CAM Private Key;
- Headend Public Key;
- Global Secret Key; and
- CAM Secret Key.

Table 1: CAM to TRM/TDM Pairing Procedure

1. Headend generates random secret: S
2. Headend cryptographically signs S using Headend Public Key: HPK(S).
3. Headend encrypts S,HPK(S) using Transport Public Key: TPK(S,HPK(S)).
4. Headend encrypts S,HPK(S) using CAM Public Key: CPK(S,HPK(S)).
5. Headend transmits (TPK(S,HPK(S)) and CPK(S,HPK(S)) to TRM.
6. TRM decrypts TPK(S,HPK(S)) using Transport Private Key; S,HPK(S).
7. TRM verifies signature of HPK(S) using Headend Public Key. If signature is invalid, processing stops here.
8. TRM stores shared secret, S, for later use.
9. TRM passes TPK(S,HPK(S)) to TDM.
10. TDM decrypts TPK(S,HPK(S)) using Transport Private Key; S,HPK(S).
11. TDM verifies signature of HPK(S) using Headend Public Key. If signature is invalid, processing stops here.
12. TDM store shared secret, S, for future use.
13. TRM passes CPK(S,HPK(S)) to CAM.
14. CAM decrypts CPK(S,HPK(S)) using CAM Private Key: S,HPK(S).
15. CAM verifies signature of HPK(S) using Headend Public Key. If signature is invalid, processing stops here.
16. CAM stores shared secret, S, for future use.

Thus, as described in Table 1, above, a random secret is generated by the headend. As Figure 1 shows, the random secret is generated at the headend 11 by a pseudo-random number generator 19. However, other equally suitable methods of generating the secret will be apparent to those skilled in the art. The general direction of the encrypted signal is shown by arrow 13. Thus, encrypted decryption keys, encrypted, signed secrets, and the encrypted transport stream itself traverse this same path from the headend to the receiver. The encrypted keys and secrets may be provided at the same time as the transport stream, either embedded in the stream, or as a separate stream, or they may be provided separately from the transport stream. Upon being received from the headend, the TRM, the TDM and the CAM all receive the encrypted secret. They decrypt the secret, verify the signature and store the secret for future use. As described below, the shared secret is necessary for the generation and utilization of the local key, which is required for recording and decrypting the transport stream.

Table 2: Transport Stream Recording Procedure

1. Headend generates an encryption Key: K.
2. Headend encrypts key using Global Secret Key: GSK(K).
3. Headend transmits GSK(K) to TRM.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0232
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

4. Headend encrypts transport stream using K: K(TS).
5. TRM sends GSK(K) to CAM.
6. CAM generates Local Key by encrypting GSK(K) using CAM Secret Key: LK=CSK(GSK(K)).
7. CAM encrypts LK using shared secret, S: S(LK).
8. CAM sends S(LK) to TRM.
9. TRM decrypts S(LK) using shared secret, S: LK.
10. Headend transmits K(TS) to TRM.
11. TRM further encrypts K(TS) using LK: LK(K(TS)).
12. TRM stores GSK(K) and LK(K(TS)) on a storage medium.

As Table 2 describes, the encrypted decryption key is transmitted from the headend. The CAM transforms the decryption key using the CAM secret key, and the shared secret, S, both unique to that particular receiver, rendering the decryption key useless on any other receiver. The local secret is transmitted to the TRM from the CAM. Prior to being stored, in storage component 17, the encrypted transport stream is encrypted a second time, using the local key, effectively rendering the transport stream inaccessible. It should be mentioned that the storage component may consist of a memory or a mass storage device. The mass storage device may be a fixed drive such as a disk drive, or it may be a removable storage medium, such as a DVD.

Table 3: Transport Stream Playback Procedure

1. TDM retrieves GSK(K) and LK(K(TS)) from storage medium.
2. TDM sends GSK(K) to CAM
3. CAM generates Local Key by encrypting GSK(K) using CAM Secret Key: LK=CSK(GSK(K)).
4. CAM decrypts GSK(K) using GSK: K.
5. CAM encrypts K, LK using shared secret, S: S(K,LK).
6. CAM sends S(K,LK) to Transport.
7. TDM decrypts S(K,LK) using shared secret, S:K,LK.
8. TDM decrypts LK(K(TS)) using LK: K(TS).
9. TDM decrypts K(TS) using K: TS.
10. TDM sends Transport Stream, TS, to display module

As Table 3 describes, the TDM retrieves the doubly encrypted transport stream from the storage component 17, along with the decryption key. The decryption key is transmitted to the CAM, whereupon it is transformed into a local key, using shared secret, S and the CAM secret key. Prior to display, the transport stream must be decrypted twice. The first time using the local key, and the second time using the decryption key provided by the headend. Thus, in the form it is retrieved from the storage component, the transport stream is useless, except on that particular receiver.

The invention is applicable in any type of subscription-based or conditional access network environment, in which a network service provider distributes digital information to users of the network. Typically, the network will be a publicly-accessible

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0233
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

telecommunications network such as a cable television network or the Internet. Furthermore, the network connection may be wired or wireless. Depending on the network and the nature of the content provided, the receiver may constitute a set-top box or a personal computer. The nature of the content is highly-variable; the invention is equally applicable to television programming, movies, pay-per-view sports events, digital music, digitized images, information products in digital format or software. Other network environments, hardware platforms and areas of application consistent with the spirit and scope of the invention will be apparent to those skilled in the art.

* * * * *

MPEG is an industry standard for compressing, multiplexing, and transmitting digital video and audio. An MPEG stream is composed of a sequence of data bytes. These bytes can be logically grouped together to form a single element within an MPEG stream. For example, a single element within an MPEG stream might represent a single frame of video within a movie.

The MPEG standard defines byte sequences that indicate the start of an element within an MPEG stream; such byte sequences are commonly referred to as "start codes." Some common examples of MPEG start codes are:

- Video Packetized Elementary Stream Header;
- Video Group of Pictures Header;
- Video I Frame Header;
- Video P Frame Header;
- Video B Frame Header;
- Video Slice Header; and
- Audio Packetized Elementary Stream Header.

It is often useful or necessary to build an Event Table that indicates the location of start codes within an MPEG stream. This table is composed of a list of offsets into the MPEG stream. The offsets listed in the table correspond to location in the MPEG stream that contain start codes.

The Event table may contain additional information, as well. For example, it is often useful to describe what type of start code is located at each offset. Using the Event Table allows a playback device to quickly locate a particular element within an MPEG stream. For example, one method of quickly scanning through video (fast forward) is to play only a subset of the video frames contained within the stream. The Event Table can be used to quickly locate those frames that need to be displayed.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0234
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

One application where it is useful to build such a table is on a device designed to receive, store and play back MPEG stream transmissions. Since MPEG streams are often encrypted before transmission to prevent unauthorized use, it is desirable to store the MPEG stream at the receiver in its encrypted from prior to purchase, in order to prevent unauthorized use. Typically, the stream is not decrypted until the rights to use or view the stream are purchased. Conventionally, the event table cannot be built until the MPEG stream is decrypted. Building the event table can be a time consuming process. Accordingly, this can impose a significant time delay between the time that the rights to use the stream are purchased and the time that the Event Table is created and available for use.

In order to make the Event Table available immediately, an embodiment of the invention is provided in which the Event Table is created prior to transmission of the stream. A first alternative is to transmit the Event Table along with the associated MPEG stream, so that the receiver has access to the Event Table without decrypting the MPEG stream. A second alternative is to encrypt the Event Table itself prior to transmission, to protect it from unauthorized use.

Although the invention has been described herein with reference to certain preferred embodiments, one skilled in the art will readily appreciate that other applications may be substituted without departing from the spirit and scope of the present invention. Accordingly, the invention should only be limited by the Claims included below.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0235
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

CLAIMS

What is claimed is:

1. A cryptographic method for rendering a conditional access system resistant to playback attacks, said system comprising a headend and at least one receiver connected to said headend, said method comprising the steps of:

providing at least a global secret key (GSK), headend public (HPK) and private keys, receiver transport public (TPK) and private keys; receiver conditional access module (CAM) public (CPK) and private keys and a CAM secret key (CSK);

pairing transport reception and decryption components of the receiver with said CAM such that a Transport Reception Module (TRM), a Transport Decryption Module TDM) and said CAM all share a secret;

generating a Local Key (LK);

recording an encrypted transport stream transmitted from said headend, wherein the transport stream is further encrypted at said receiver, using LK, so that a doubly-encrypted transport stream is stored on a storage medium on said receiver; and

playing back said transport stream, wherein said transport stream is decrypted by said TDM, using LK.

2. The method of Claim 1, wherein said step of pairing transport reception and decryption components of the receiver with said CAM comprises the steps of:

generating a random secret (S) by said headend;

signing S by said headend using HPK (HPK(S));

encrypting S, HPK(S) by said headend using TPK (TPK(S, HPK(S));

encrypting S, HPK(S) by said headend using CPK (CPK(S, HPK(S));

transmitting TPK(S, HPK(S) and CPK(S, HPK(S) to TRM by said headend;

decrypting TPK(S, HPK(S) by TRM using said Transport private key;

verifying said signature (HPK(S) by TRM using HPK, wherein processing stops if said signature is invalid;

storing S for future use by TRM;

passing TPK(S, HPK(S) to TDM by TRM;

decrypting TPK(S, HPK(S) by TDM using said Transport private key;

verifying said signature (HPK(S) by TDM using HPK, wherein processing stops if said signature is invalid;

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0236
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

storing S for future use by TDM;
passing CPK(S, HPK(S) to CAM by TRM;
decrypting CPK(S, HPK(S) by CAM using said CAM private key;
verifying said signature (HPK(S) by CAM using HPK, wherein processing stops if said signature is invalid; and
storing S for future use by CAM;
wherein S is shared by TRM, TDM and CAM.

3. The method of Claim 2, wherein said step of recording an encrypted transport stream transmitted from said headend comprises the steps of:
generating an encryption key, K by said headend;
encrypting K using GSK (GSK(K));
transmitting GSK(K) to TRM;
encrypting a transport stream (TS) by said headend using K (K(TS));
sending GSK(K) to CAM by TRM;
generating LK, wherein generating LK comprises:
encrypting GSK(K) by CAM using CSK (LK=CSK(GSK(L)));
encrypting LK by CAM using S (S(LK));
sending S(LK) to TRM;
decrypting S(LK) by TRM using S
transmitting K(TS) to TRM by said headend;
further encrypting K(TS) using LK (LK(K(TS)); and
storing LK(K(TS) on said storage medium;
wherein said transport stream is doubly encrypted.

4. The method of Claim 3, wherein said step of playing back said transport stream comprises the steps of:
retrieving GSK(K) and LK(K(TS) by TDM;
sending GSK(K) to CAM by TDM;
generating LK by CAM;
decrypting GSK(K) by CAM suing GSK;
encrypting K, LK by CAM using S (S(K,LK));
sending S(K,LK) to TDM by CAM;
decrypting S(K, LK) by TDM using S;
decrypting LK(K(TS) by TDM using LK;
decrypting K(TS) by TDM using K; and
sending said decrypted transport stream TS to a display module for one of display and use by a user.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0237
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

5. The method of Claim 4, wherein multiple layers of security are provided so that if one layer is a circumvented, subsequent layers remain intact.

6. The method of Claim 5, wherein a first layer comprises preventing said user from accessing unencrypted keys by avoiding exposing said unencrypted keys to user accessible and user programmable resources within said receiver.

7. The method of Claim 6, wherein said first layer further comprises encrypting a communication path between said CAM and said TDM.

8. The method of Claim 5, wherein a second layer comprises preventing keys from being played back into said TDM by requiring that keys be first transformed in a manner particular to a receiver.

9. The method of Claim 8, wherein said transformation comprises encrypting said keys by said CAM using LK.

10. The method of Claim 5, wherein a third layer comprises preventing said user from accessing said transport stream.

11. The method of Claim 10, wherein preventing said user from accessing said transport stream comprises doubly encrypting said transport stream prior to storage.

12. The method of Claim 11, wherein a corresponding Event Table is built for said transport stream prior to transmission.

13. The method of Claim 12, wherein said Event Table is transmitted along with said transport stream so that said Event Table is available for immediate use by said receiver.

14. The method of Claim 12, wherein said Event Table is encrypted prior to transmission to prevent unauthorized use.

15. A conditional access system rendered resistant to playback attacks, wherein multiple layers of security are provided so that if one layer is circumvented, subsequent layers remain intact, said system comprising:

a headend, wherein said headend sources a digital transport stream;

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0238
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

at least one receiver connected to said headend for receiving said transport stream, said receiver including a Transport Reception Module (TRM), a Transport Decryption Module (TDM) and a Conditional Access Module (CAM);

a global secret key (GSK);

headend public (HPK) and private keys;

receiver transport public (TPK) and private keys; and

receiver conditional access module (CAM) public (CPK) and private keys and a CAM secret key (CSK), wherein said keys are operative in a plurality of cryptographic procedures.

16. The system of Claim 15, wherein a first layer comprises preventing a user from accessing unencrypted keys by avoiding exposing said unencrypted keys to user accessible and user programmable resources within said receiver.

17. The system of Claim 16, wherein said first layer further comprises encrypting a communication path between said CAM and said TDM.

18. The system of Claim 16, wherein a second layer comprises preventing keys from being played back into said TDM by requiring that keys be first transformed in a manner particular to a receiver.

19. The system of Claim 18, wherein said transformation comprises encrypting said keys by said CAM using a local key (LK) generated by said CAM.

20. The system of Claim 19, wherein a third layer comprises preventing said user from accessing said transport stream.

21. The system of Claim 20, wherein preventing said user from accessing said transport stream comprises doubly encrypting said transport stream prior to storing said transport stream locally.

22. The system of Claim 21, wherein transport reception and decryption components of the receiver are paired with said CAM such that said TRM, said TDM and said CAM all share a secret, and wherein said pairing is accomplished by:

generating a random secret (S) by said headend;

signing S by said headend using HPK (HPK(S));

encrypting S, HPK(S) by said headend using TPK (TPK(S, HPK(S));

encrypting S, HPK(S) by said headend using CPK (CPK(S, HPK(S));

transmitting TPK(S, HPK(S) and CPK(S, HPK(S) to TRM by said headend;

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0239
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

decrypting TPK(S, HPK(S) by TRM using said Transport private key;

verifying said signature (HPK(S) by TRM using HPK, wherein processing stops if said signature is invalid;

storing S for future use by TRM;

passing TPK(S, HPK(S) to TDM by TRM;

decrypting TPK(S, HPK(S) by TDM using said Transport private key;

verifying said signature (HPK(S) by TDM using HPK, wherein processing stops if said signature is invalid;

storing S for future use by TDM;

passing CPK(S, HPK(S) to CAM by TRM;

decrypting CPK(S, HPK(S) by CAM using said CAM private key;

verifying said signature (HPK(S) by CAM using HPK, wherein processing stops if said signature is invalid; and

storing S for future use by CAM;

wherein S is shared by TRM, TDM and CAM.

23. The system of Claim 22, wherein an encrypted transport stream transmitted from said headend is recorded, wherein the transport stream is further encrypted at said receiver, using LK, so that a doubly-encrypted transport stream is stored on a storage medium on said receiver;

wherein recording said stream comprises:

generating an encryption key, K by said headend;

encrypting K using GSK (GSK(K));

transmitting GSK(K) to TRM;

encrypting a transport stream (TS) by said headend using K (K(TS));

sending GSK(K) to CAM by TRM;

generating LK, wherein generating LK comprises:

encrypting GSK(K) by CAM using CSK (LK=CSK(GSK(L)));

encrypting LK by CAM using S (S(LK));

sending S(LK) to TRM;

decrypting S(LK) by TRM using S

transmitting K(TS) to TRM by said headend;

further encrypting K(TS) using LK (LK(K(TS)); and

storing LK(K(TS) on said storage medium;

wherein said transport stream is doubly encrypted.

playing back said transport stream, wherein said transport stream is decrypted by said TDM, using LK.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0240
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

24. The system of Claim 23, wherein said transport stream is decrypted by said TDM, using LK and played back by:

retrieving GSK(K) and LK(K(TS) by TDM;

sending GSK(K) to CAM by TDM;

generating LK by CAM;

decrypting GSK(K) by CAM suing GSK;

encrypting K, LK by CAM using S (S(K,LK));

sending S(K,LK) to TDM by CAM;

decrypting S(K, LK) by TDM using S;

decrypting LK(K(TS) by TDM using LK;

decrypting K(TS) by TDM using K; and

sending said decrypted transport stream TS to a display module for one of display and use by said user.

25. The system of Claim 15, further comprising a corresponding event table for said transport stream, wherein said event table is built prior to transmission.

26. The system of Claim 25, wherein said Event Table is transmitted along with said transport stream so that said Event Table is available for immediate use by said receiver.

27. The system of Claim 25, wherein said Event Table is encrypted prior to transmission to prevent unauthorized use.

28. A method of providing an event table for a corresponding MPEG transport stream, wherein said transport stream is transmitted from a headend to at least one receiver, said method comprising;

building said event table prior to transmission of said stream.

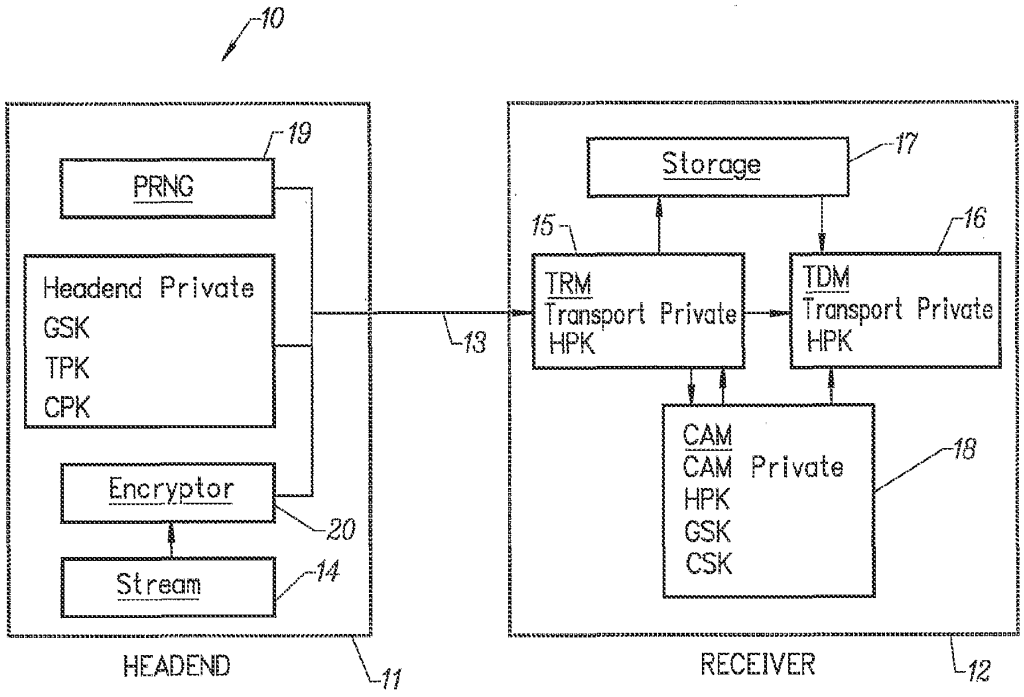
29 The method of Claim 28, further comprising the step of:

transmitting said event table along with said transport stream so that said event table is available for immediate use by said receiver.

30. The method of Claim 29, further comprising the step of:

encrypting said event table prior to transmission so that unauthorized use of said event table is prevented.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0241
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)



Legend

CAM	Conditional Access Module
TRM	Transport Reception Module
TDM	Transport Decryption Module
GSK	Global Secret Key
TPK	Transport Public Key
CPK	CAM Public Key
HPK	Headend Public Key
CSK	CAM Secret Key

FIG. 1

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0242
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
10 May 2002 (10.05.2002)

PCT

(10) International Publication Number
WO 02/37210 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number: PCT/US01/30602

(22) International Filing Date:
28 September 2001 (28.09.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/243,259 25 October 2000 (25.10.2000) US
09/906,428 16 July 2001 (16.07.2001) US

(71) Applicant: **LIGHTNING SOURCE, INC.** [US/US]; One Ingram Boulevard, La Vergne, TN 37086 (US).

(72) Inventors: **CLARK, George, Phillip**; 19211 Pristine Place, Lutz, FL 33549 (US). **CRAWFORD, Jeffrey, Walter**; 7 Valewood Run, Penfield, NY 14526 (US). **MARINO, Edward, John**; 215 Burlington Place, Nashville, TN 37215 (US). **BREWSTER, Laurance, Holmes**; 9242 Brushboro Drive, Brentwood, TN 37027 (US).

(74) Agents: **PHAM, Chinh, H.** et al.; Patent Group, Foley, Hoag & Eliot LLP, One Post Office Square, Boston, MA 02109-2170 (US).

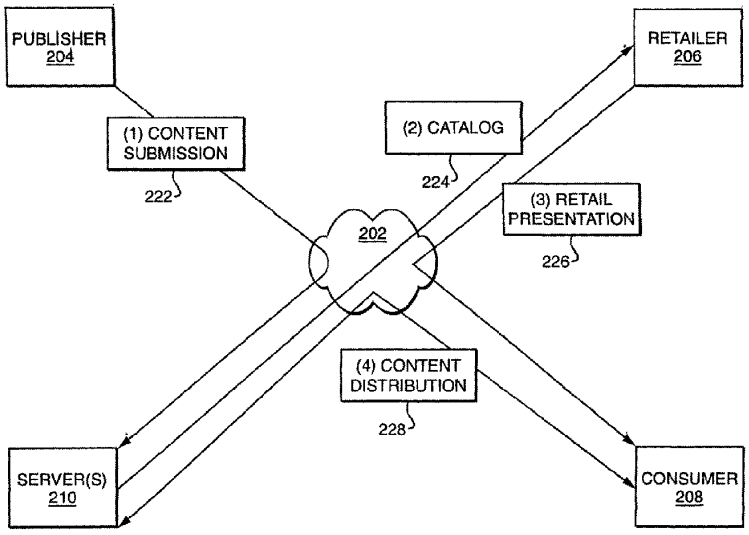
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (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*

[Continued on next page]

(54) Title: PROCESSING CONTENT FOR ELECTRONIC DISTRIBUTION USING A DIGITAL RIGHTS MANAGEMENT SYSTEM



(57) Abstract: In general, in one aspect, the disclosure describes a method of processing content for distribution over a computer network. The method includes receiving submitted electronic content, accessing identification of at least one of a set of more than one electronic book digital rights management (DRM) systems, and automatically generating an electronic book from the received electronic content for distribution in accordance with the identified electronic book digital rights management systems(s).

WO 02/37210 A2

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

PROCESSING CONTENT FOR ELECTRONIC DISTRIBUTION USING A DIGITAL RIGHTS MANAGEMENT SYSTEM

Background

Much like an ordinary printed book, electronic books ("eBooks") can be used to present text and pictures to readers. Instead of ink and paper, however, an electronic book is a collection of digital data that software, known as an electronic book reader, can interpret and present on a display. A variety of devices run electronic book reader software such as personal computers, handheld personal digital assistants (PDAs), cellular phones with displays, and so forth.

Electronic books can offer a variety of features not traditionally associated with print books. For example, instead of text and pictures, an electronic book may also store data used to present sound such as music and speech. Further, instead of still pictures, an electronic book can also present animated images. Additionally, by transmitting eBook data over a computer network, eBooks can be delivered to remote locations almost instantaneously.

Unfortunately, in many ways, copying data is easier than photocopying pages of a book. To protect the rights of those trying to sell or otherwise limit access to electronic books from pirating, companies have developed a wide variety of digital rights management (DRM) systems. For example, Microsoft currently offers a "Digital Asset Server" that guards against unauthorized user access to Microsoft Reader eBooks. Similarly, Adobe offers a number of different DRM solutions such as Adobe Content Server.

DRM solutions differ significantly in their approaches to the task of controlling access to eBooks. For the purposes of illustration, however, FIGs. 1 and 2 depict a typical DRM scheme. As shown in FIG. 1, a client 104, such as a PDA or personal computer, can send a message 108 to a server 100 over a network 102 such as the Internet. The message 108 requests access to an eBook and includes credentials of the requestor such as the identity of the device 104 and/or reader software making the request. The server 100 uses the credentials to scramble (i.e., encrypt) the data of the requested eBook. As shown in FIG. 2, the server 100 then sends the scrambled data 106 to the requesting client 104. Using its own credentials, the client 104 reader can unscramble (i.e., decrypt) and present

the eBook to a user. If a device other than the client 104 receives the eBook data, it should lack the proper credentials needed to perform the unscrambling.

Summary

In general, in one aspect, the disclosure describes a method of processing content for distribution over a computer network. The method includes receiving submitted electronic content, accessing identification of at least one of a set of more than one electronic book digital rights management (DRM) systems, and automatically generating an electronic book from the received electronic content for distribution in accordance with the identified electronic book digital rights management system(s).

Embodiments may include one or more of the following features. The electronic content may be received over a network. The method may also include receiving metadata for the electronic content such as an author, a subject, a publisher, and/or a summary; hard copy printing information such as a number of pages, a cover size, and/or a type of binding; and distribution information such as the identification of the DRM(s), street date, and/or authorized retailers. The DRMs may be digital rights management systems offered by non-affiliated vendors. The method may also include transmitting user interface instructions (e.g., markup language instructions) to the network client that enables a submitter to identify electronic content.

In general, in another aspect, the disclosure describes a computer program product, disposed on a computer readable medium, for processing content for distribution over a computer network. The program includes instructions for causing a processor to receive electronic content, access identification of at least one of a set of more than one electronic book DRM systems, and automatically generate an electronic book from the received electronic content for distribution in accordance with the identified electronic book DRM system(s).

In general, in another aspect, the disclosure describes a server that includes at least one network connection, at least one processor, and at least one computer readable medium storing instructions for processing by the processor. The computer readable medium stores instructions corresponding to a set of more than one electronic book digital rights management systems. The medium also stores instructions for receiving electronic content over the at least one network connection, receiving metadata corresponding to the

electronic content over the network connection that identifies of at least one of the set of more than one electronic book digital rights management systems, and automatically generating an electronic book from the received electronic content corresponding to the identified electronic book DRM system.

Brief Description of the Drawings

FIGs. 1-2 are diagrams illustrating an example of an electronic book digital rights management system.

FIG. 3 is a diagram illustrating different features a server can provide to publishers, retailers, and consumers.

FIG. 4 is a diagram illustrating content submission over a network.

FIGs. 5-11 are screenshots of a user interface presented to a publisher.

FIG. 12 is a flow-chart of a process for automatically processing received content.

FIG. 13 is a diagram illustrating catalog distribution to a retailer.

FIG. 14 is a diagram illustrating catalog generation.

FIG. 15 is a flow-chart of a process for generating a catalog.

FIGs. 16-18 are diagrams illustrating fulfillment of a request for an electronic book.

FIG. 19 is a flow-chart of a process for fulfilling a request for an electronic book.

Detailed Description

I. Introduction

FIG. 3 shows a server 210 that can provide a variety of features that can ease tasks involved in electronic and printed book distribution. To illustrate some of these features, FIG. 3 shows a sample sequence that begins with submission 222 of a title from a publisher 204 and ends with the title's distribution 228 to a consumer 208.

As shown in FIG. 3, a publisher client 204 can submit content 222 for a title to the server 210 over a network 202 such as the Internet. Such content can include data specifying text, graphics, and even multimedia such as music or video.

The publisher client 204 can also submit information about the content known as "metadata". The metadata can include identifier information such as the ISBN, UPC, or DOI of the work; pricing information for one or more markets in which the work may be sold; bibliographic information such as the author and title of the work; distribution

information such as identification of territories where selling the work is authorized, retailers authorized to sell the work, and/or identification of one or more digital rights management systems for protecting the work when distributed electronically; and/or manufacturing information, such as a printing and/or binding specifications, for use in the preparation of hard copies of the work.

The server 210 can automatically prepare the content for distribution. For example, for electronic distribution, the server 210 can automatically format eBook information for distribution of the title in accordance with one or more selected digital rights management systems. For hard copy manufacturing and distribution, the server 210 can automatically prepare the content for printing, for example, by extracting a cover page for color printing and generating bit-map images of book pages.

In addition to the behind-the-scenes work of preparing content for distribution, the server 210 may also provide information to retailers 206, such as Amazon.com and BarnesandNoble.com, to help display and sell titles. For example, the server 210 may use collected metadata to generate a customized catalog file 224 of content authorized for sale by a retailer 206. The catalog file 224 can include author names, a summary, and/or selected images (e.g., book cover thumbnails). A retailer 206 can use the catalog file 224 to automatically update its web-site's offerings. For example, Amazon.com can automatically generate web-pages for newly available titles identified in the catalog file 224.

The server 210 can also insulate retailer 206 from the technical details of title distribution across multiple digital rights management systems. For example, after a consumer 208 selects an eBook from the retailer's 206 web-site 226, the server 210 can distribute 228 the title to a consumer 208 in accordance with a digital rights management system selected for the content. This frees the retailer 206 from the burden of setting-up, integrating, and maintaining a host of different digital rights management systems that different eBook formats may require. Similarly, for a hard copy, the server 210 can offer a "print-on-demand" service that produces a hard copy of a title for delivery to a consumer or retailer.

Though FIG. 3 depicts a single publisher 204, retailer 206, and consumer 208, the server 210 can support a very large number of each of these entities. Further, while the server 210 may constitute a single computer, the server 210 may instead represent a logical collection of devices.

While the description above highlights a few features offered by the server 210, the server 210 can also offer a wide array of other services such as providing reports (e.g. usage reports, title demand reports, retailer invoices, and publisher compensation) to retailers 206 and publishers 204. A server 210 may offer all of the features described above or only support a limited subset of these services. These and other features are described in greater detail below.

II. Content Submission

FIG. 4 illustrates a scheme that enables a publisher 204 to securely transmit content 230 over a network 202 to a server 210 for subsequent electronic distribution and/or hard copy printing. As shown, in addition to content 230, the server 210 can also receive metadata 232 corresponding to the content. Such metadata can include bibliographic information about the content, "print-on-demand" information used to generate a hard copy of the content, and/or distribution information such as identification of retailers authorized to sell the content and/or identification of one or more electronic book digital rights management (DRM) systems. For security, the server 210 and publisher client 204 can communicate over a secure network connection, such as HTTPS (HyperText Transfer Protocol Secure), that encrypts/decrypts information communicated by the publisher's client 204 and the server 210.

The server 210 can use the received content 230 and metadata 232 to automatically generate distribution versions of the content. For example, for electronic distribution, the server 210 can automatically prepare a version of the content for distribution in accordance with the identified DRM scheme(s). Similarly, for hard copy printing, the server 210 can automatically generate a version of the content, for example, by preparing an image of each page to be printed.

As shown in FIG. 4, the server 210 includes a content management 214 system that stores and processes the received content 230 and metadata 232. The server 210 also includes a fulfillment system 220 that features instructions for different digital rights management systems. For example, the fulfillment system 220 may support DRMs from non-affiliated vendors. For instance, the system 220 may feature Microsoft Reader Digital Asset Server and Adobe Content Server Digital Rights Management System.

As shown, the server 210 may also include web server instructions 212 that make these features available to a publisher 204 via an Internet web-site. In technical terms, the web server instructions 212 handle HTTP (HyperText Transfer Protocol) messages exchanged with network clients (e.g., web browsers). These messages can include, for example, instructions for presenting a user interface that transmits information collected from a remote user back to the server 210. Such user interface instructions may be encoded in a variety of ways such as SGML (Structured Generalized Markup Language) instructions (e.g., HTML (HyperText Markup Language) and XML (eXtensible Markup Language)) or instructions that include conditional statements (e.g., "IF" statements) such as an applet.

FIGs. 5-11 illustrate samples of user interface screens the server 210 may provide to a publisher to collect content and metadata. These sample screens depict stages of a sample process of content submission that includes selecting one or more distribution options, providing information for the selected options, monitoring the processing status of submitted content, and proofing a distribution version of the content. The following sequence may be preceded, for example, by user interface screens that enable a publisher to set up an account. For instance, a publisher may provide banking or credit information for billing and/or compensation.

As shown in FIG. 5, after establishment of an account, content submission can permit user selection of hard copy "print-on-demand" preparation 262 and/or eBook distribution 264 of the content. As shown, a publisher selecting eBook distribution 264 may also select one or more DRM schemes for eBook distribution (e.g., "MS Reader Format" 266 or "Adobe eBook Format" 268).

As shown in FIG. 6, a user interface screen may collect some metadata applicable to both eBooks and "print-on-demand" titles. For example, as shown, the user interface can collect a title 271, a publisher reference number 272 such as an ISBN (International Standard Book Number), a language 273, a list of contributors 270, and a summary annotation 277. The user interface may also collect a publication date 274 and/or a "street date" (the date the publication may first be offered for sale) 276 that represents a date in the future before which the publisher does not want distribution to occur.

As shown, the user interface also enables a publisher to select a method of delivering content 278 to the server. For example, a publisher can select file upload over the Internet, physical delivery of a computer readable medium (e.g., a CD-ROM or floppy),

or a hard copy for scanning or other conversion into electronic form. The publisher can similarly specify 279 a mechanism for uploading a book cover image.

Other screens may collect other information from a publisher. For example, other screens may collect an edition number or description, an indication of whether the edition is an abridged edition, whether the content is "large print", a series ID and/or number, one or more subject matter categories, an audience age range or reading level, and one or more identification codes (e.g., a Library of Congress card number, a Dewey Decimal Classification No., a UPC [Universal Product Code] code, and so forth).

As shown in FIG. 7, a publisher can also specify both list prices and wholesale discounts. The server can use this information to automatically initiate transactions to compensate the publisher for each sale. The publisher may also specify territorial rights. For example, a publisher may not wish, or be permitted, to sell or transmit content beyond particular geographic bounds.

The information collected from a publisher may differ depending on the distribution methods selected. For example, FIG. 8 shows additional information collected for eBook distribution. As shown, the user interface can enable a publisher to select different DRM options 284, 286 supported by selected DRM systems. For example, Adobe Reader options 286 can give a publisher control over consumer printing and copying based on a maximum number of days or copies.

The user interface shown in FIG. 8 also enables a publisher to rate 280 the complexity of the content. For instance, a novel with plain text may be less complex to convert to an eBook than a multi-column, graphic-intensive textbook. The rating scheme may be based on a number of criteria such as the number of columns of text, number of images or tables per page, number of hyperlinks per page, whether the content includes a table of contents, footnotes, and so forth. For example, a rating scheme may be defined as follows:

	Description	Example
Type 1	Single column text Limited line art, line charts, tables, and B&W images (no more than 1 per 15 pages) Table of Contents hyperlinking	Novels
Type 2	Single column text Column based images, line art, line charts and tables (no more than 1 per 4 pages) Content hyperlinking (up to 1 per page)	Novels
Type 3	Single column text Column based images, line art, line charts and tables (no more than .6 per page) Intensive content hyperlinking (up to 3 links per page) Extensive and complex tables Indexes, bibliography, or footnotes	Technical , academic, and reference books
Type 4	Multicolumn text Heavy, repetitive formatting Heavy images, large image orientation Limited hyperlinking (less than 1 per page) Images, text or tables across spreads	Cooking , arts & crafts, coffee table books
Type 5	Flowing layouts with minimal repetitive formatting Highly illustrative Intensive content hyperlinking Media enhancement	Instructional children and young adult books

Based on the rating, the server may determine a fee for processing the content. Additionally, the server can use the rating to determine whether a requested format may be a poor selection. For example, Adobe PDF format provides a fixed page layout regardless of display device and may not be appropriate for material having many columns.

As shown in FIG. 9, information collected for content selected for "print-on-demand" may differ from that collected for eBook distribution. For example, as shown, the user interface may collect user input specifying a type of binding 288 and/or the text 290 to print on the book spine.

Again, after receiving the metadata entered by the publisher and the content, the server can automatically prepare the content for distribution in the publisher selected

format(s). After doing so, the server may generate one or more "proofing" copies of the distribution version(s) of the content. For example, the server may prepare and transmit an eBook to the publisher or, in the case of "print-on-demand" content, the server may prepare an Adobe PDF (Portable Document Format) file featuring images of the pages as they would be printed. In either case, as shown in FIG. 10, a publisher can accept 292 or reject 294 the proofing copy by interaction with the user interface. Accepted proofs will be made available for distribution.

As shown in FIG. 11, a publisher can monitor progress of their submitted titles throughout the content submission process. For example, the user interface shown indicates the status of each submitted title. Such statuses include "awaiting material", "pre-flighting", and "proofing". Additionally, selecting a title hyperlink can cause display of more detailed information about the title, such as its corresponding metadata.

FIG. 12 shows a process 240 for automatic handling of content submission. As shown, the process 240 may begin with receipt 241 of content and its corresponding metadata. The process 240 can handle a wide variety of content formats such as Adobe Acrobat PDF, PostScript, QuarkXpress, PageMaker, InDesign, Word, and tagged text formats such as HTML. Many of these content formats do not include conditional statements.

As shown, the process 240 may validate 243 received metadata. For example, the process 240 may ensure that no metadata specifies a wholesale discount over %50. The process 240 may also validate an ISBN number, for example, by verifying the number's check digit. A wide number of other metadata validations may take place such as a request of payment authorization from a publisher's credit source.

After receipt 241 of the content and metadata, the process 240 automatically checks ("pre-flights") the content for numerous issues which might prevent accurate automatic preparation of a title. For example, the process 240 may verify receipt of all image files and required fonts. Should an error be encountered, the server can automatically notify the publisher and await resubmission.

Assuming the metadata validation 243 and pre-flighting proceeded without significant error, the process 240 can continue converting the received content to selected distribution format(s), for example, by reflowing and repaginating text, replacing images, and so forth.

If the selected distribution format(s) include hard copy distribution 245, the process 240 can automatically perform a number of tasks that prepare the content for printing. For example, for text submissions, the process 240 can parse the content to construct 247 a table of contents. The process 240 can also perform a wide variety of other tasks such as analyzing the structure of text to indent the first paragraph of a new chapter more than other paragraphs. Similarly, the process 240 may alter text, for example, by compressing three consecutive periods into a single ellipses character or using an elongated dash instead of using a simple "-" character. The process 240 may also perform other tasks, such as extracting a cover image from the content.

As shown, the process 240 can calculate 249 a spine width for a manufactured book based on page thickness and the number of pages. The process 240 can also determine a spine image for the binding, for example, by creating an image of the title in a font that fits the spine width.

After automatically generating information for printing the content, the process 240 can generate 250 a proof copy, for example, by e-mailing images of the pages to be printed or by sending a hard copy of the title for publisher review. After review, the process 240 can send 251 the generated information for the title to a manufacturing engine that can control printing of the title on demand, for example, by printing a color cover, printing a book block, and binding the printed cover and book block.

A different sequence may occur if the selected distribution format(s) include electronic book distribution 253. For example, the process 240 may process the content to generate 255 one or more Open eBook (OEB) files. For instance, the process 240 may include extraction of a cover page from submitted content and/or lossy compression of submitted images to reduce the size of any distribution files.

Based on these OEB files, the process 240 may generate 257 DRM specific files. Generation of DRM specific files may include DRM specific conversions. For example, for an Adobe eBook generation may include construction of an Adobe style hyperlinked table of contents, a copyright page updated to include eBook ISBN, and logical page numbers that permit eBook pages to match a title page numbering sequence. For a Microsoft eBook, generation may include construction of a Microsoft style floating hyperlinked table of contents, a copyright page updated to include eBook ISBN, and conversion of non-supported book layouts (e.g., marginal notes, floating art, cross spread

images or boxes, conversion of footnotes to endnote, placement of footnote as display text, and placement of images or graphics close to, but not preceding, the callout). Additional advanced features may also be available at the option of the publisher. These can include linked index entries, removal of blank pages, cross-referencing, contextual links, listings of figures and tables, and links from text reference of a figure to the figure or a footnote text reference to an endnote. After proofing 259, the completed DRM specific file is posted 261 to a DRM Engine (described below) for subsequent distribution.

As shown, after generation of a title in the selected distribution format(s), the process 240 may store 260 the title's metadata in a database of metadata corresponding to different titles. As described below, this stored metadata can be used to construct a catalog of titles for a retailer.

III. Catalogs

Retailers often play an important role in publication sales, for example, by handling the tasks of promoting publications. For instance, Amazon.com promotes most of its available publications with a web-page providing a cover image, summary, and reader reviews. Some retailers provide libraries of over one million titles making the maintenance of their offerings a potentially time consuming task.

As shown in FIG. 13, a server 210 can include catalog generation and distribution instructions 218 that can generate a "catalog" 300 of titles a retailer is authorized and desires to sell. The catalog 300 can list titles available to a retailer and can include some or all of the metadata submitted with a title. Additionally, the catalog generation instructions 218 can customize the format of the catalog 300 for a particular retailer 206, for example, to work with software the retailer may use to manage title information. For instance, the retailer 206 may feature software that automatically processes a received catalog 300 to create new web-page information for new titles or amend web-page information for pre-existing ones.

FIG. 14 illustrates an example of catalog 300 generation. As shown, a process 308 selects catalog 300 data from stored metadata records 310. The metadata records 310 correspond to submitted titles and can include information identifying one or more authorized retailers and/or one or more unauthorized dealers. The process 308 can use the information to select metadata records of titles a particular retailer is authorized to handle.

For example, metadata records 302 and 306 designate "Amazon" as an authorized retailer for eBooks of John Grisham's "The Firm" 302 and "The Chamber" 306. Thus, the catalog 300 generated by the process 308 can include records for these titles, for example, as a result of an SQL (Structured Query Language) query for records listing "Amazon" as an authorized retailer.

While the metadata records shown specify individual retailers, a publisher may identify a group of retailers by attributes or a grouping code (e.g., "E-Commerce Vendors"). Additionally, a default set of retailers may apply to metadata records that do not specify a particular set of retailers.

Since different retailers may use different software and/or data formats to process title records, the process 308 can customize the catalog 300 file generated for a particular retailer by using customized formatting information 312. Such formatting information 312 can specify the metadata to include in the catalog 300 and the arrangement and encoding of included metadata. For example, as shown, the catalog 310 features a semi-colon delimited record for each title. That is, a semi-colon separates different fields of the record. Alternatively, catalog 300 records can be encoded in a markup language for easy incorporation into a retailer's web-pages. For example, a record of "<TITLE>The Firm</TITLE><AUTHOR>Grisham</AUTHOR>" includes <TITLE> and <AUTHOR> markup tags that identify the information included in the record.

In addition to text and other data, a retailer may also prefer to receive an image of a book cover for display by their web-pages. Such images may be included as data within a catalog, for example, as JPEG (Joint Picture Experts Group) or GIF (Graphics Interchange Format) image data. Alternatively, each title may have corresponding images stored at a FTP (File Transfer Protocol) site in accordance with a naming convention such as title_xpixelsize_x_ypixelsize.format (e.g., TheFirm_600_ x_400.jpeg).

FIG. 15 illustrates an example of a process 330 that the catalog generation instructions 218 may implement. As shown, the process 330 selects 332 metadata records of titles for inclusion in a retailer's catalog. The selection 332 can feature both "authorization filters" that restrict retailers to titles they are authorized to sell and "retailer defined filters" that prevent retailers from catalog inclusion of works they are not interested in selling or promoting.

The authorization filters can test for a variety of conditions that may prevent inclusion of a work in a retailer's catalog. For example, the filters may eliminate a work from a catalog if the retailer is outside the territory in which the work is authorized to be sold. Similarly, the filters may eliminate a title from inclusion in a catalog if the title has not yet been priced for sale or if the work has not yet been proofed by the publisher.

The "retailer defined filters" enable a retailer to specify characteristics of works that the retailer does not want to sell or promote. For instance, "Bob's Sci-Fi eBook Store" may only be interested in publications categorized as science or science fiction. Thus, in this example, the process 330 may check to limit titles included in a Bob's catalog to only include titles in these categories. Similarly, a retailer, for example, may request only those titles approved by some organization.

As described above, information for titles selected for inclusion in the catalog may be formatted 334 according to retailer preference. After completing the selection 332 and formatting 334, the catalog may be transmitted 336 to the retailer. Transmission may occur, for example, via e-mail or a sequence of HTTP messages. Transmission may alternatively occur by storing the catalog in an FTP (File Transfer Protocol) directory accessible by the retailer. This latter option enables the retailer to control when and how often the catalog information is received.

The process 330 shown in FIG. 15 may be programmed to automatically repeat at a designated interval. For example, a retailer may request automatic generation of a catalog on a daily or weekly basis. For retailers receiving more than one catalog at different times, the process 330 may generate "delta" catalog files that only include changes from a preceding catalog. For example, the catalog may only include new titles authorized for sale by a retailer or new/changed information about titles in a previous catalog or catalogs.

IV. Fulfillment

A server 210 may provide a web-site that enables consumers and/or publishers to request electronic books or "print-on-demand" hard copies of a title. However, as described above, retailers often handle the task of presenting titles to consumers for purchase. For example, Amazon.com allows consumers to search lists and descriptions of different available eBooks. In the case of eBooks, fulfilling purchase requests can add the burden of

DRM system maintenance and support to a retailers responsibilities. FIGs. 16-18 illustrate a system that can remove the burden of handling these fulfillment duties from a retailer.

As shown in FIG. 16, a consumer 208 can interact with a retailer 206 over a network 202 through mechanisms selected by the retailer 206 such web-pages, email, and so forth. After a consumer 208 requests 322 an eBook title, for example, by selecting a title from a web-page 320, a fulfillment process 220 provided by a remote server 210 handles distribution of the eBook to the consumer. The server 210 may be the same server 210 providing other features described herein.

As shown in FIG. 17, the retailer 206 transmits fulfillment information 324, such as a URL (Universal Resource Locator) link, to the consumer 208 for each purchased eBook. For example, the retailer 206 may include the URL in an e-mail message sent to the consumer 208 or may include the URL in a dynamically constructed web-page that lists items requested by a consumer 208.

When activated, the link directs a secure message 326 to the server 210. The message 326 encodes identification of the title ordered and identification of the retailer. For example, a consumer may receive a URL having the following format:

https://server.com?parameters=retailerID&itemID

where "https" identifies a secure connection between the consumer 208 and server 210, "server.com" identifies the location of the server 210 in the network, and retailerID and item ID identify the retailer and ordered item SKU (Store Keeping Unit, the product identifying number used by the server 210), respectively. The URL parameters may be encrypted, for example, using Triple DES. Additionally, the URL may feature additional parameters such as a time stamp and/or the results of a hashing of the other parameters to thwart pirate attempts to construct a valid URL. The URL may also include a tracking number assigned by the retailer to the transaction for retailer tracking purposes. As the server 210 may insulate the retailer 206 from DRM tasks, the URL need not include identification of any particular DRM system.

As shown in FIG. 17, when the consumer selects the URL link, the consumer's 208 client no longer needs to interact with the retailer 206, but is instead interacting with the server 210. However, this may be completely transparent to a consumer 208. That is, the

consumer 208 may only perceive interaction with the retailer 206. To enhance this effect, the server 210 may provide user interfaces customized for a particular retailer. For example, a server 210 may provide status and error message web-pages that prominently feature the retailer's logo, stylesheet, or other information for each retailer using the server 210

As shown in FIG. 18, after receiving the eBook request, the server 210 handles distribution 332 of the eBook to the consumer in accordance with the digital rights management system associated with the title. After distribution 332, the server 212 can transmit confirmation 333 to the Retailer 206 describing both successful delivery of the content or, in the event of a failure, what the reason for failure.

As shown, the server 210 supports multiple DRM systems. While each DRM system may operate differently, many share a similar sequence. In a typical scenario, DRM distribution of a title begins when a DRM system attempts to connect to the consumer's 208 reader software. If the reader software is not installed, the system can guide the consumer through a download/installation process. The DRM system then requests credentials (e.g. computer ID, reader software ID) and uses these credentials to "lock" a copy of the ordered title for that consumer. Such locking may occur by encrypting a copy of the title or providing an encrypted voucher needed by the reader software to open a generically encrypted copy of the title. A "locked" copy of the title is then sent to the consumer 208. The consumer's 208 device then automatically launches the reader software associated with the DRM scheme used and loads and presents the title. While the process described above may seem complex, the entire process happens in real-time and, typically, does not take more time than loading a standard web page.

The scheme described above can offer a number of potential benefits. Again, by server 210 handling fulfillment, retailers need not be aware that DRMs are even being used. Additionally, while FIGs. 16-18 illustrate distribution of a title for a single retailer 206, the server 210 can support many different retailers and their consumers simultaneously. Thus, addition of a new DRM system at the server 210 can expand the number and variety of product distribution capabilities of many retailers.

The server 210 may implement DRM handling by bundling instructions for different DRM systems into a DRM Processing Engine. The server 210 may include many different DRM Processing Engines operating in parallel. This technique can permit load balancing

between the DRM Processing Engines and provide scalability as the number of fulfillment operations increases. Additionally, new DRM Processing Engines can be added or removed at any time without impacting system availability.

FIG. 19 illustrates a title fulfillment process 350. As shown, the process 350 receives a request for a title 352. The process 350 may then verify security information (e.g., a hash value) received with the request. This may trigger transmission of a confirmation message (e.g., an HTTP message) to the retailer. This provides retailers with virtually real-time confirmation of consumer use of an the order link supplied by the retailer 206. These confirmation messages may be queued for retransmission when a retailer's 206 web-site is down. The confirmation message may include identification of the ordered title and/or a order number, among other information.

As shown in FIG. 19, the process 350 may determine 354 whether to distribute the electronic book to the network client in accordance with one or more business rules applied 354 independent of DRM operation. For example, a business rule may verify that the retailer identified in the request is authorized to sell the title. A different business rule may deny access to a title before a street date specified by the publisher. Yet another business rule may verify that the consumer is not downloading the book to different devices or exceeding a maximum number of downloads. As new requirements emerge, business rules may be created and/or updated. The business rules may be encoded, for example, as boolean expressions or in a programming language such as C and/or SQL (Structured Query Language). If a business rule indicates distribution should not occur 358, the process 350 can transmit 360 corresponding error messages and/or customized screens to the retailer and/or consumer.

After business rule application, the process 350 may determine 362 a DRM system selected for the title. For example, server instructions may use the received retailer ID and the title ID of the request to perform a table lookup of DRM systems associated with the title by the retailer. Thereafter, the title can be distributed 364 in accordance with the determined DRM. As specified by a DRM or business rule, successful downloading of titles may be noted to prevent the consumer from re-downloading the same eBook using the original URL link. Failed downloads may not be recorded to enable a consumer to attempt to re-download in the event of a bad Internet connection.

As shown, the process 350 may log 366 information describing a transaction, for example, by logging information used in billing, determining publisher compensation, business rule audits, determining DRM usage fees, and so forth.

Again, throughout the process 350 illustrated in FIG. 19, retailers and/or consumers may receive status and error messages regarding the progress of their request. Examples of events that can cause notification include the occurrence of unknown errors, completion of a successful download, a determination that a title was not found or available, a determination that the consumer did not order the title from an authorized retailer, a determination that the download attempt exceeded a limit, the occurrence of communication errors, a determination that reader software was not installed or activated, and a determination that the received consumer credentials were incorrect. While the server may offer a predefined set of status and error message web pages, these messages may be customize in real-time to each retailer's specifications. Alternatively, events can trigger a re-direct to a web-page provided by the retailer's web-server.

Again, the process 350 may provide retailers with status information such as confirmation of an order. For example, a server may transmit a confirmation message to a retailer that encrypts the order tracking number, time stamp, and other information.

V. Implementations

The techniques described herein are not limited to any particular hardware or software configuration; they may find applicability in any computing or processing environment. The techniques may be implemented in hardware or software, or a combination of the two. Preferably, the techniques are implemented in computer programs executing on programmable computers that each include a processor, a storage medium readable by the processor (including volatile and non-volatile memory and/or storage elements), at least one input device, and one or more output devices.

Each program is preferably implemented in high level procedural or object oriented programming language to communicate with a computer system. However, the programs can be implemented in assembly or machine language, if desired. In any case the language may be compiled or interpreted language.

Each such computer program is preferably stored on a storage medium or device (e.g., CD-ROM, hard disk, or magnetic disk) that is readable by a general or special

purpose programmable computer for configuring and operating the computer when the storage medium or device is read by the computer to perform the procedures described herein. The system may also be considered to be implemented as a computer-readable storage medium, configured with a computer program, where the storage medium so configured causes a computer to operate in a specific and predefined manner.

Other embodiments are within the scope of the following claims.

What is claimed is:

1. A method of processing content for distribution over a computer network, the method comprising:

receiving electronic content submitted by a submitter;

accessing identification of at least one of a set of more than one electronic book digital rights management systems; and

automatically generating an electronic book from the received electronic content for distribution in accordance with the identified electronic book digital rights management system(s).

2. The method of claim 1, wherein receiving the electronic content comprises receiving the electronic content over a network from a network client operated by the submitter.

3. The method of claim 2, further comprising transmitting user interface instructions to the network client, the user interface instructions providing a user interface that enables the submitter to identify electronic content to submit.

4. The method of claim 3,

wherein the user interface instructions comprise markup language instructions; and

wherein transmitting the user interface instructions to the network client comprise transmitting the user interface instructions in response to an HTTP (HyperText Transfer Protocol) message.

5. The method of claim 1, wherein the set of more than one electronic book digital rights management systems comprise digital rights management systems offered by non-affiliated vendors.

6. The method of claim 1, wherein automatically generating an electronic book comprises lossy compression of graphic images included in the electronic content.

7. The method of claim 1, further comprising receiving metadata corresponding to the electronic content.

8. The method of claim 7, wherein the metadata comprises at least one of the following: an author, a subject, a publisher, and a summary.

9. The method of claim 7, wherein the metadata comprises hard copy printing information.

10. The method of claim 9, wherein the hard copy printing information comprises at least one of the following: a number of pages, a cover size, and a type of binding.

11. The method of claim 9, further comprising hard copy printing of the electronic content.

12. The method of claim 11, wherein the hard copy printing comprises:

printing a color cover;

printing a book block; and

binding the printed cover and book block.

13. The method of claim 7, wherein the metadata comprises distribution information.

14. The method of claim 13, wherein the distribution information includes the identification of the at least one electronic book digital rights management system.

15. The method of claim 13, wherein the distribution information comprises a street date.

16. The method of claim 13, wherein the distribution information comprises identification of at least one authorized retailer.

17. The method of claim 16, further comprising storing the metadata with metadata associated with other received electronic content.

18. The method of claim 17, further comprising selecting metadata from the stored metadata, the selected metadata corresponding to electronic content authorized for a retailer.

19. The method of claim 18, further comprising storing at least a portion of the selected metadata for transmission to the retailer over the network.

20. The method of claim 19,

further comprising receiving formatting information from a retailer; and

wherein storing at least a portion of the selected metadata comprises storing in accordance with the received formatting information.

21. A computer program product, disposed on a computer readable medium, for processing content for distribution over a computer network, the program including instructions for causing a processor to:

receive electronic content submitted by a submitter;

access identification of at least one of a set of more than one electronic book digital rights management systems; and

automatically generate an electronic book from the received electronic content for distribution in accordance with the identified electronic book digital rights management system(s).

22. The computer program of claim 21, wherein the instructions that cause the processor to receive the electronic content comprise instructions that cause the processor to receive the electronic content over a network from a network client operated by the submitter.

23. The computer program of claim 22, further comprising instructions that cause the processor to transmit user interface instructions to the network client, the user interface instructions providing a user interface that enables the submitter to identify electronic content to submit.

24. The computer program of claim 21, wherein the instructions that cause the processor to automatically generate an electronic book comprise instructions that cause the processor to perform lossy compression of graphic images included in the electronic content.

25. The computer program of claim 21, further comprising instructions for causing the processor to receive metadata corresponding to the electronic content.

26. The computer program of claim 25, wherein the metadata comprises hard copy printing information.

27. The computer program of claim 26, wherein the hard copy printing information comprises at least one of the following: a number of pages, a cover size, and a type of binding.

28. The computer program of claim 27, further comprising instructions for causing the processor to initiate hard copy printing of the electronic content.

29. The computer program of claim 25, wherein the metadata comprises distribution information.

30. The computer program of claim 29, wherein the distribution information comprises identification of at least one authorized retailer.

31. The computer program of claim 30, further comprising instructions that cause the processor to store the metadata with metadata associated with other received electronic content.

32. The computer program of claim 31, further comprising instructions that cause the processor to select metadata from the stored metadata, the selected metadata corresponding to electronic content authorized for a retailer.

33. The computer program of claim 32, further comprising instructions that cause the processor to store at least a portion of the selected metadata for transmission to the retailer over the network.

34. A server, comprising:

(1) at least one network connection;

(2) at least one processor; and

(3) at least one computer readable medium storing instructions for processing by the processor, the computer readable medium storing:

(a) instructions corresponding to a set of more than one electronic book digital rights management systems; and

(b) instructions for:

(i) receiving electronic content from a submitter over the at least one network connection;

(ii) receiving metadata corresponding to the electronic content over the at least one network connection, the metadata including identification of at least one of the set of more than one electronic book digital rights management systems; and

(iii) automatically generating an electronic book from the received electronic content corresponding to the identified electronic book digital rights management system.

35. The server of claim 34,

wherein the metadata comprises identification of at least one authorized retailer; and

further comprising instructions for:

(iv) storing the metadata with metadata associated with other received electronic content;

(v) selecting metadata corresponding to electronic content authorized for a retailer; and

(vi) storing at least a portion of the selected metadata for transmission to the retailer over the network.

36. The server of claim 34, wherein the instructions for (i) receiving electronic content from a submitter comprise web-server instructions for handling HTTP (HyperText Transfer Protocol) messages.

37. A method of distributing electronic books over a computer network, the method comprising:

transmitting user interface instructions to a publisher's network client in response to an HTTP (HyperText Transfer Protocol) request received from the client, the user interface instructions providing a web-page form that enables the publisher to identify electronic content and corresponding metadata, the metadata including designation of at least one electronic book digital rights management system from at least two supported digital rights management schemes from different unaffiliated vendors, the metadata also including hard printing information;

receiving the identified electronic content and metadata from the network client;

automatically generating an electronic book from the received electronic content corresponding to the identified electronic book digital rights management system;

storing the metadata with metadata associated with other received electronic content;

selecting metadata from the stored metadata, the selected metadata corresponding to electronic content authorized for a retailer;

storing at least a portion of the selected metadata for transmission to the retailer over the network in accordance with formatting information received from the retailer;

receiving a request for the electronic book from a network client in response to a user's selection of the corresponding electronic content from a user interface provided by the retailer, the request including an electronic book identifier and a retailer identifier, the request being a URL (Universal Resource Locator) that encodes the electronic book identifier and the retailer identifier as one or more URL parameters;

determining whether to distribute the electronic book to the network client by applying one or more business rules to the request; and

distributing the electronic book to the network client in accordance with the electronic book's electronic book digital rights management system.

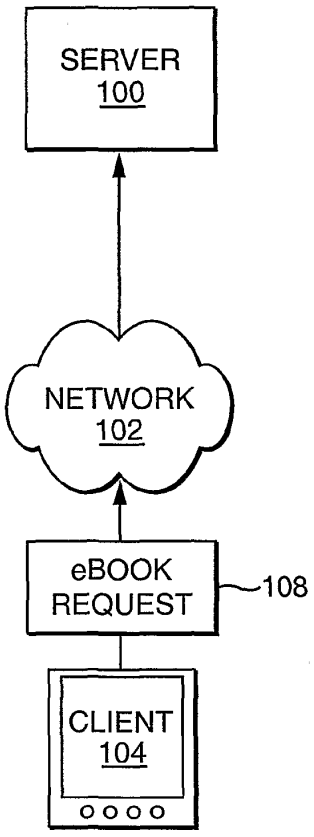


FIG. 1
(PRIOR ART)

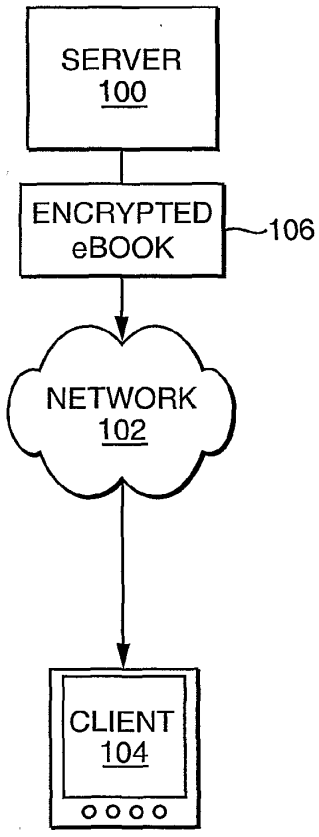


FIG. 2
(PRIOR ART)

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0270
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

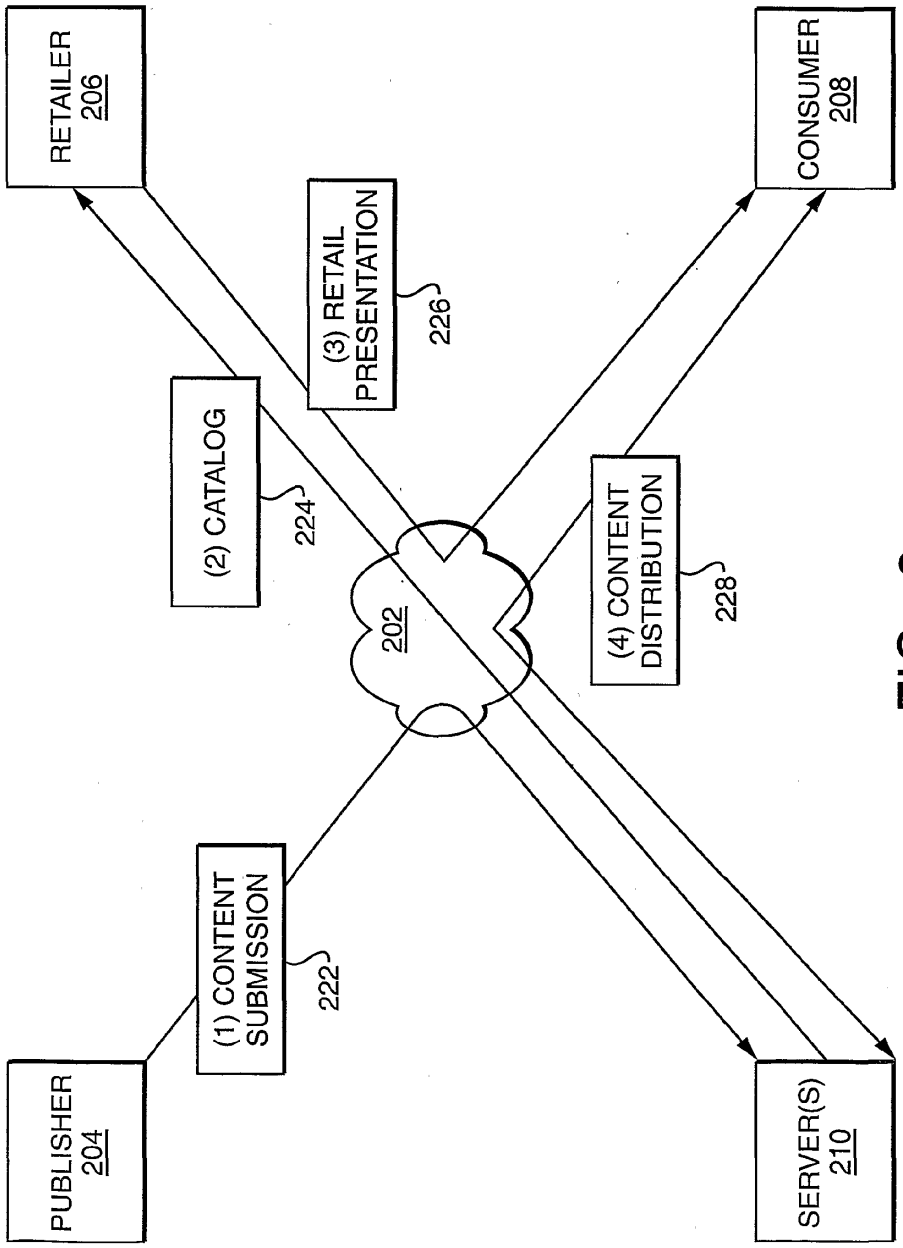


FIG. 3

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0271
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

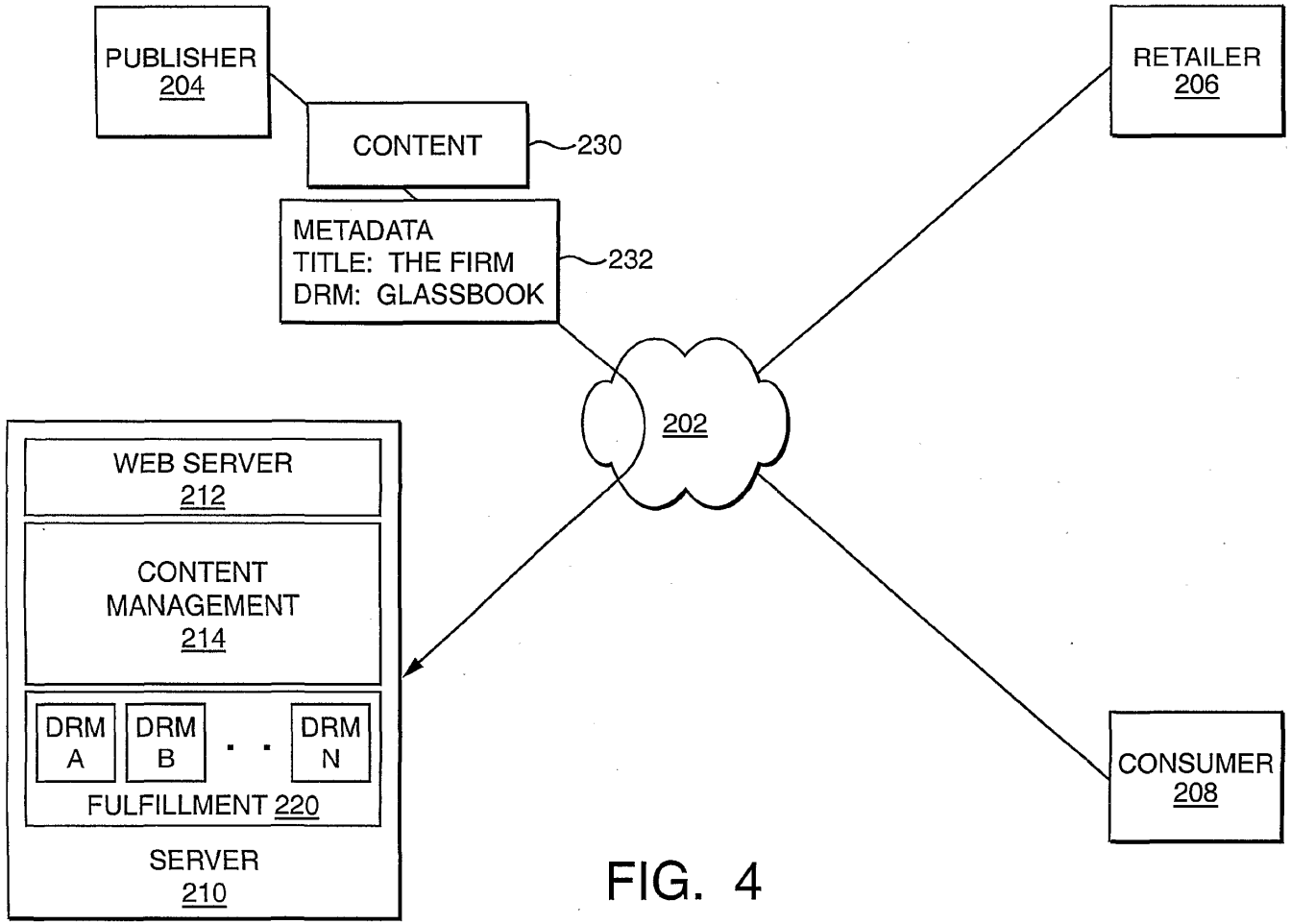


FIG. 4

SUBSTITUTE SHEET (RULE 26)

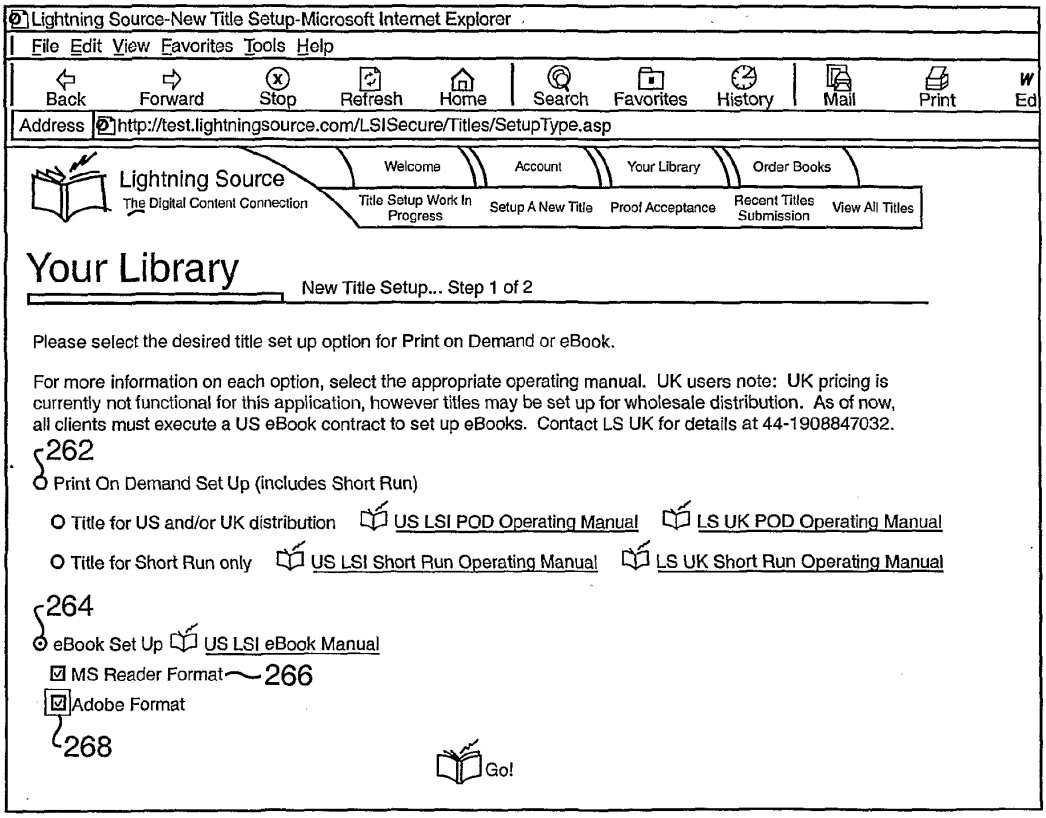


FIG. 5

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0273
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

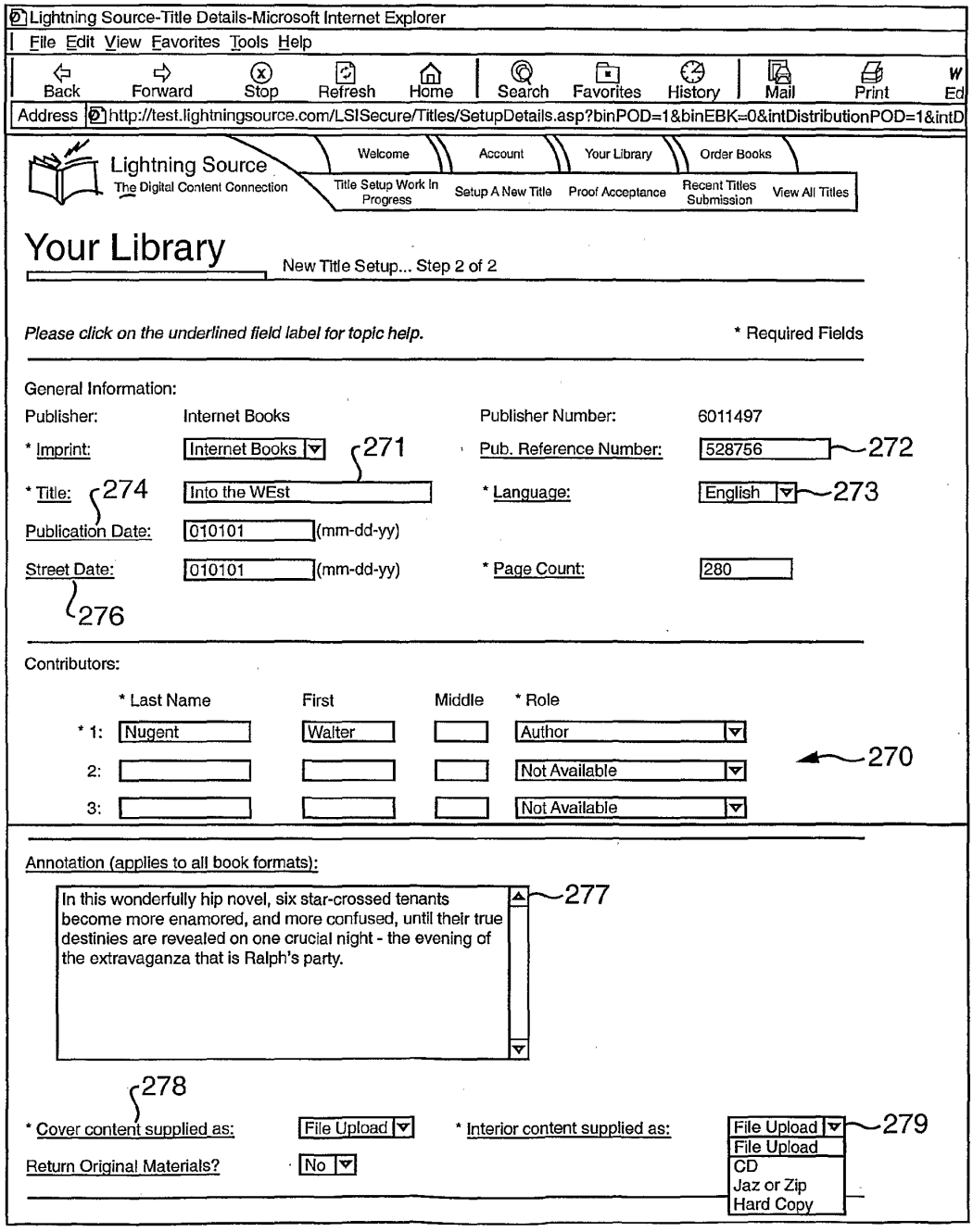


FIG. 6

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0274
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

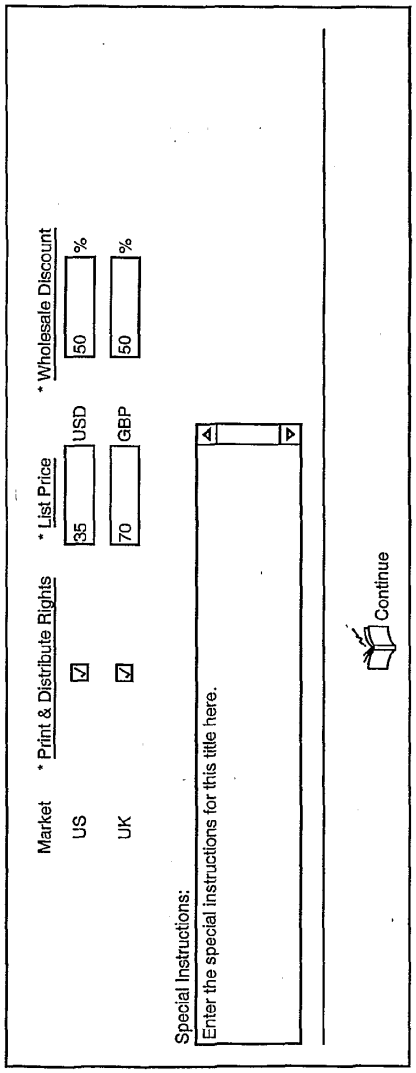


FIG. 7

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0275
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

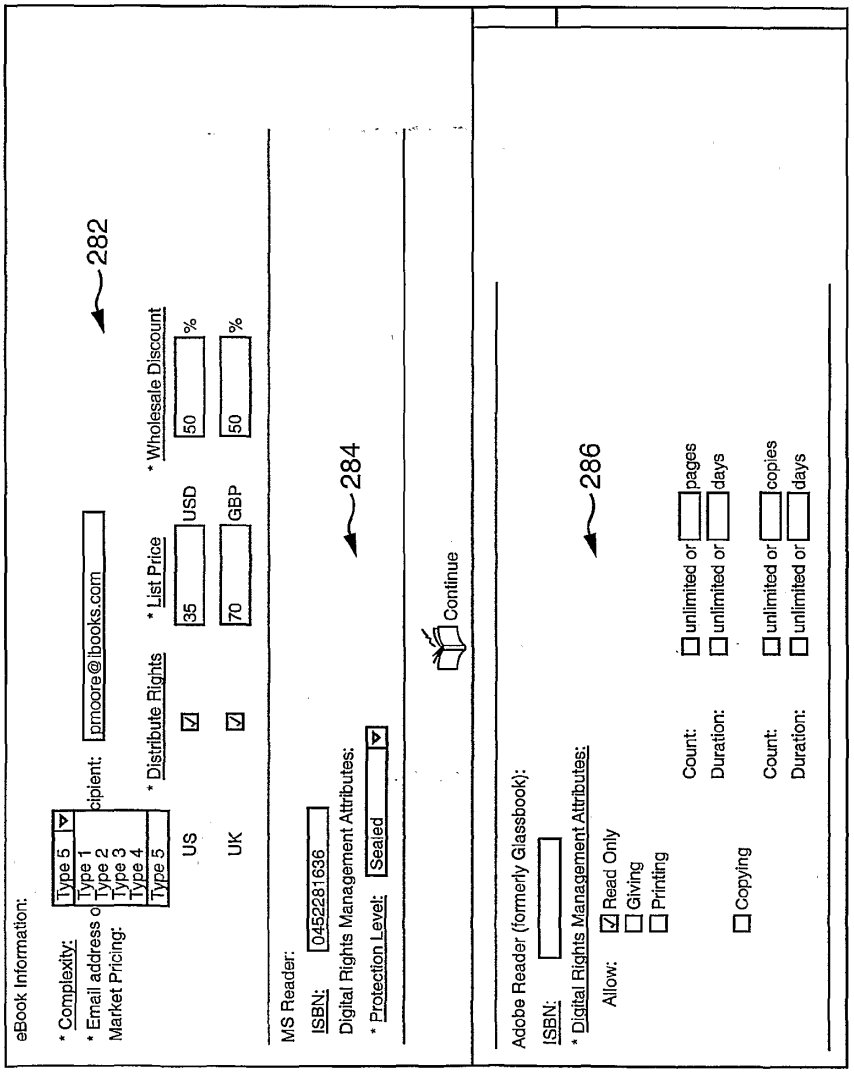


FIG. 8

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0276
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

SUBSTITUTE SHEET (RULE 26)

FIG. 9

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0277
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

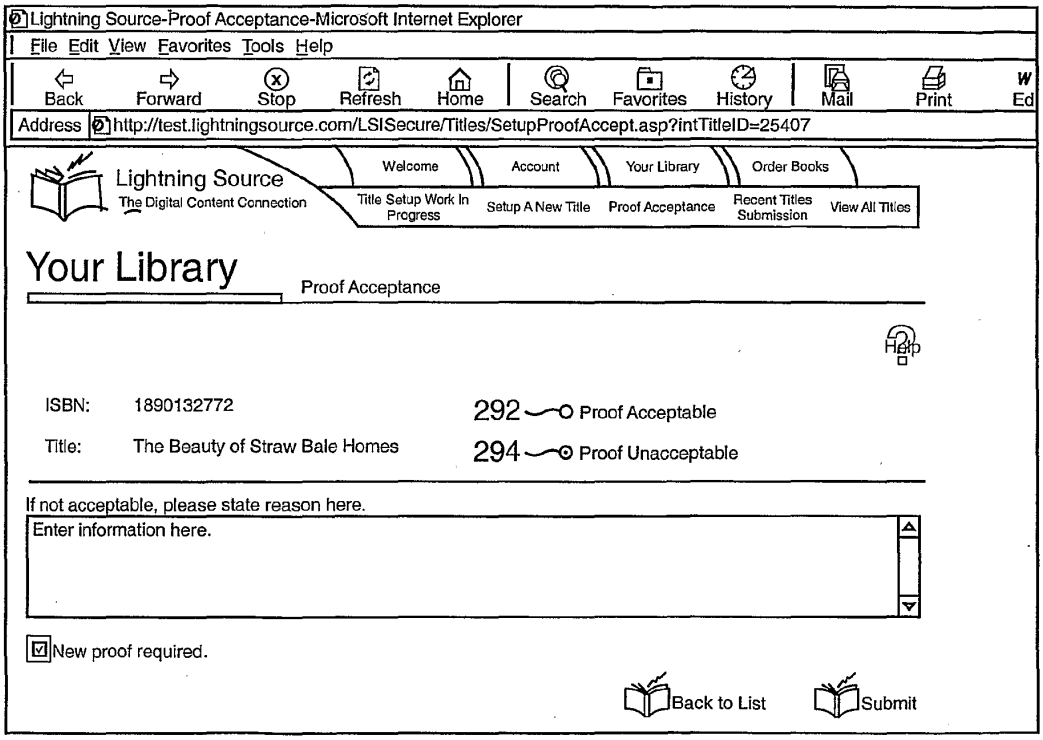


FIG. 10

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0278
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

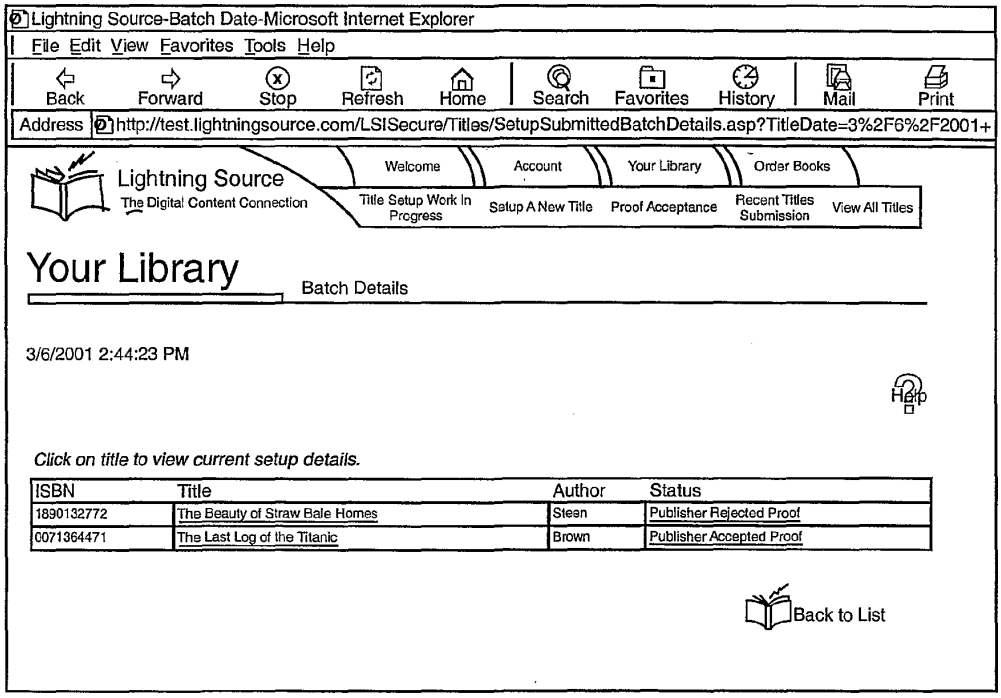


FIG. 11

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0279
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

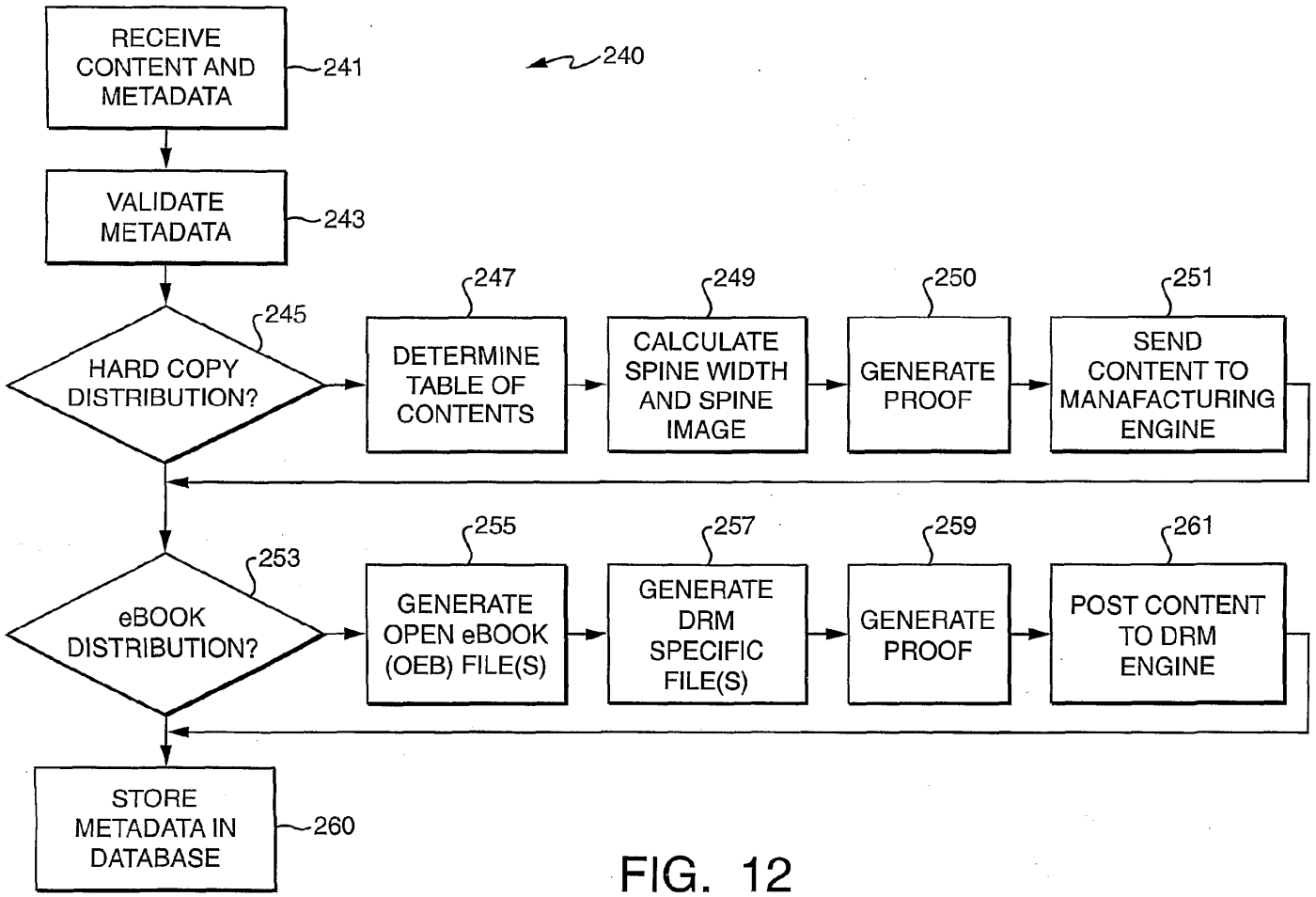


FIG. 12

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0280
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

FIG. 13

SUBSTITUTE SHEET (RULE 26)

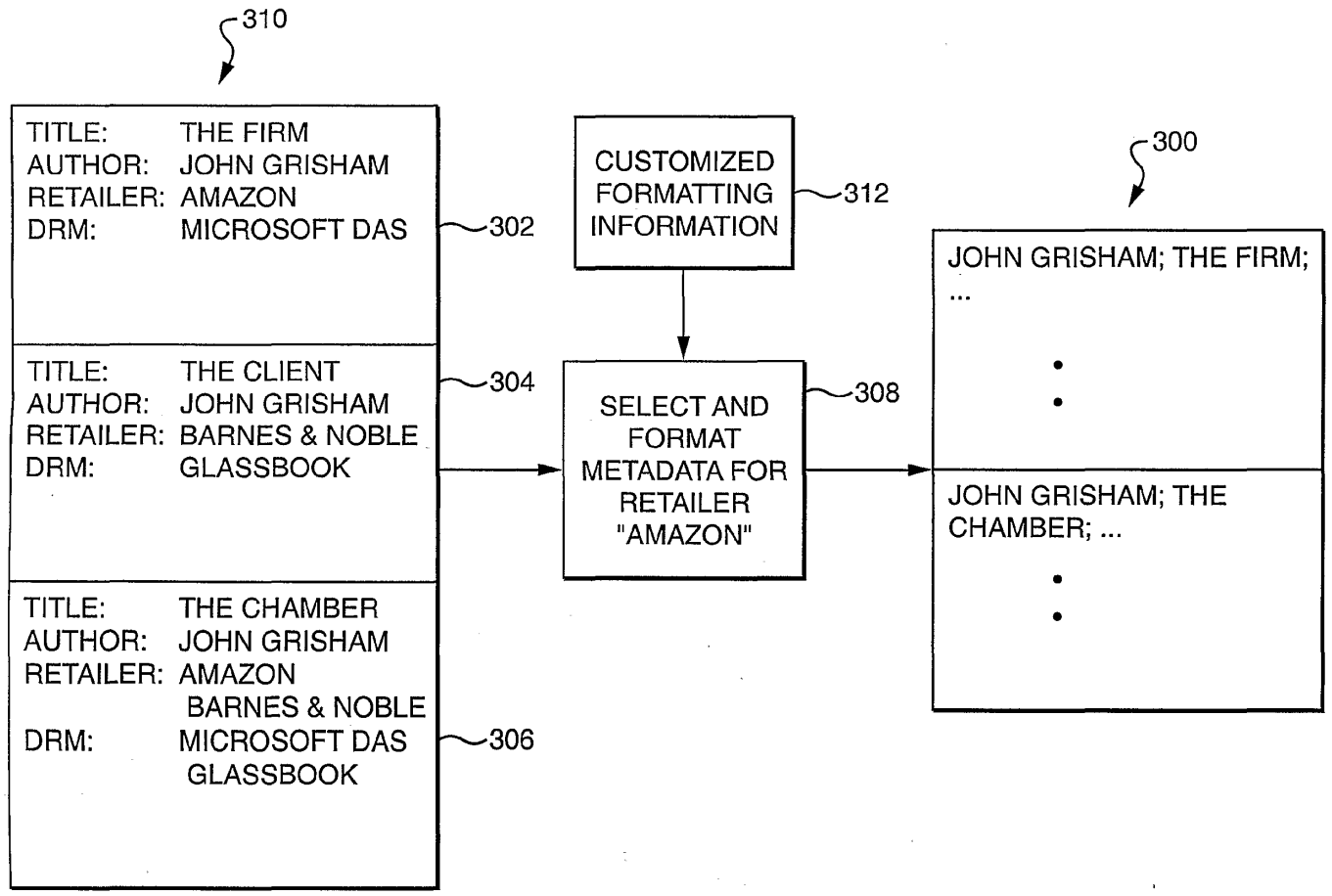


FIG. 14

SUBSTITUTE SHEET (RULE 26)

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0282
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

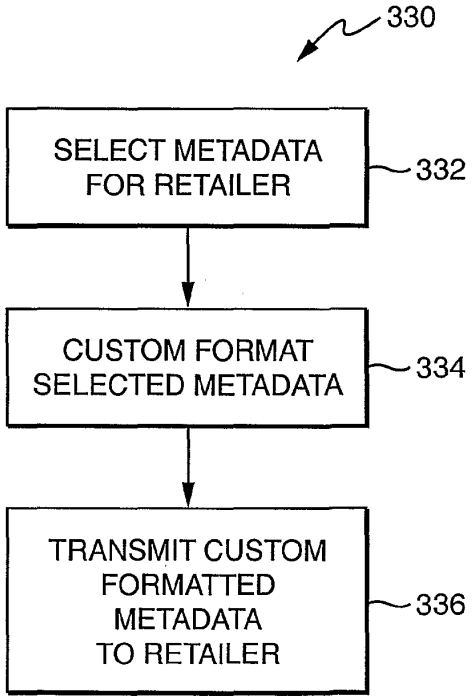


FIG. 15

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0283
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

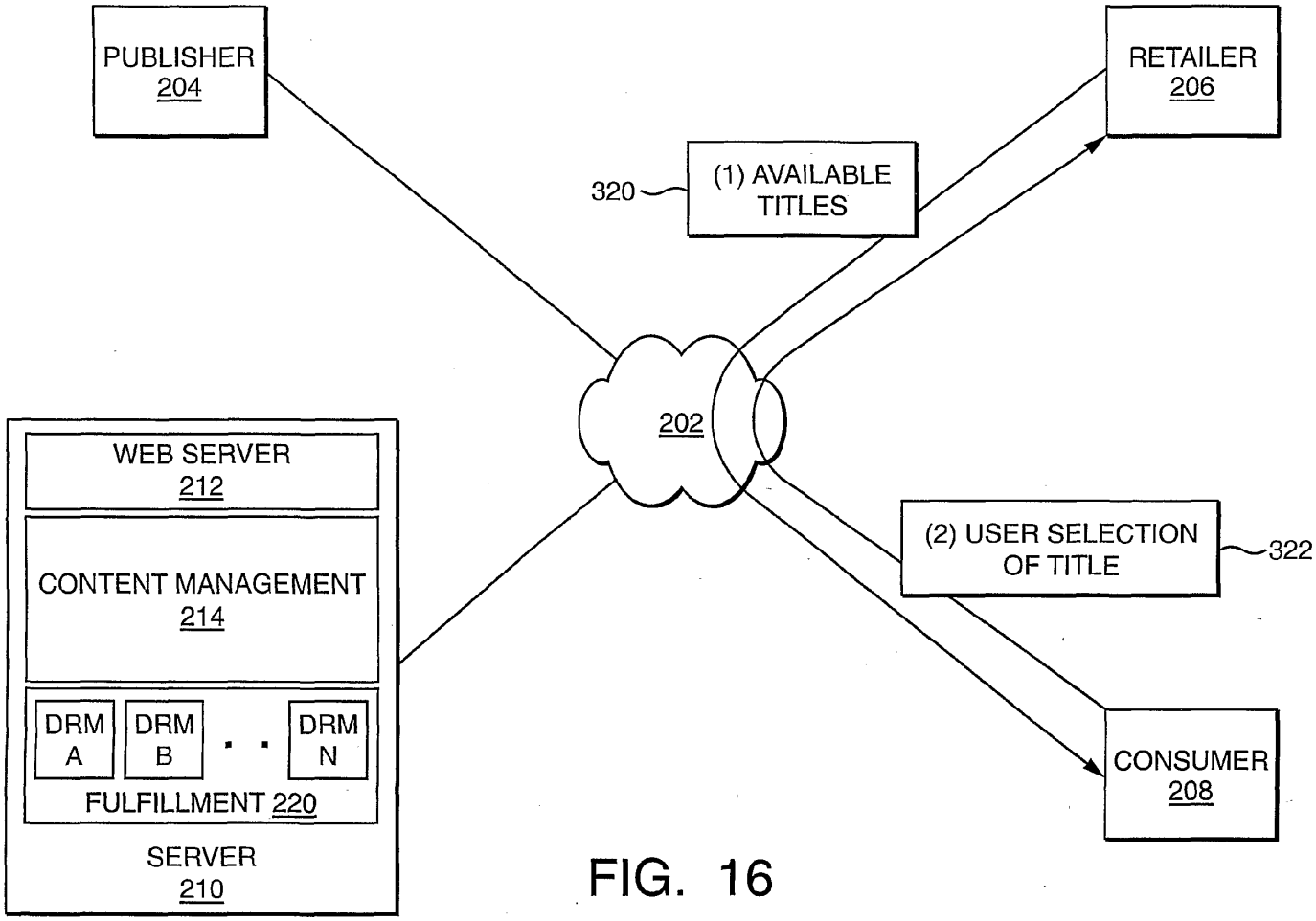


FIG. 16

SUBSTITUTE SHEET (RULE 26)

FIG. 17

SUBSTITUTE SHEET (RULE 26)

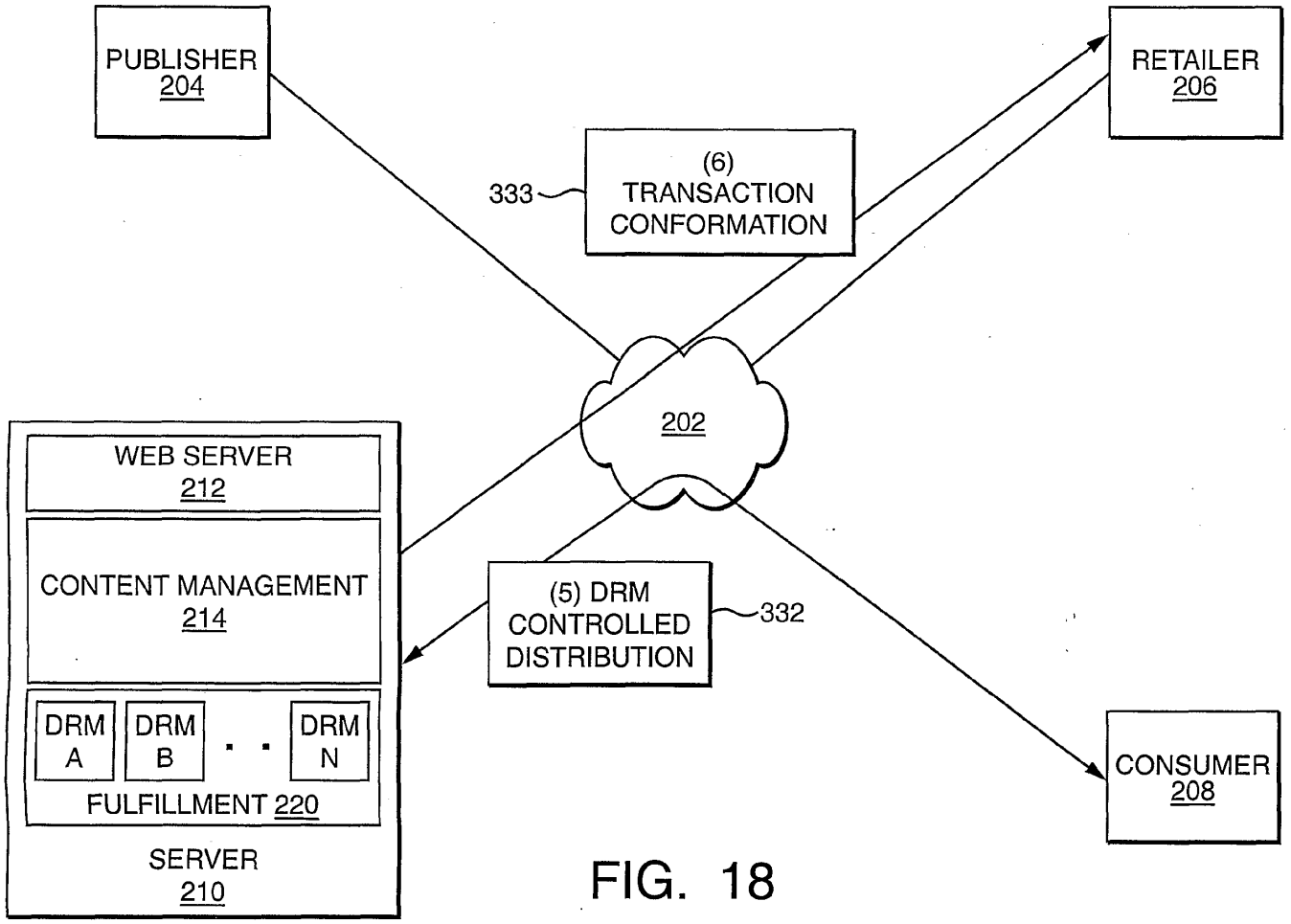


FIG. 18

SUBSTITUTE SHEET (RULE 26)

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0286
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

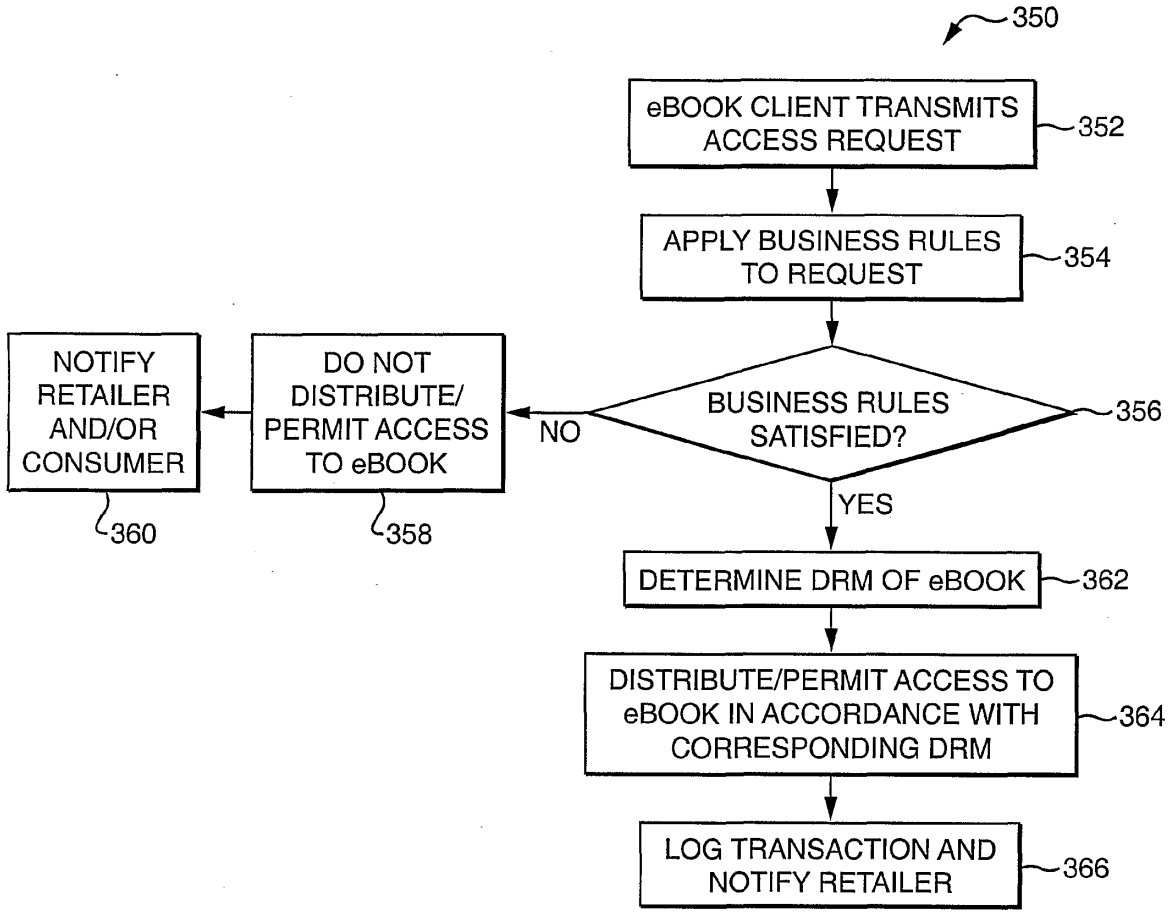


FIG. 19

SUBSTITUTE SHEET (RULE 26)

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0287
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
11 July 2002 (11.07.2002)

PCT

(10) International Publication Number
WO 02/054196 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/EP01/15107

(22) International Filing Date:
20 December 2001 (20.12.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
00403721.4 29 December 2000 (29.12.2000) EP

(71) Applicant *(for all designated States except US)*: **THOMSON LICENSING S.A.** [FR/FR]; 46 Quai Alphonse Le Gallo, F-92100 Boulogne-Billancourt (FR).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **DURAND, Alain** [FR/FR]; 79, rue de Dinan, F-35000 Rennes (FR). **LAURENT, Christophe** [FR/FR]; 3 rue des Fraîches, F-35630 Vignoc (FR). **LETELLIER, Philippe** [FR/FR]; 4, rue des Melliers, F-35760 St Grégoire (FR).

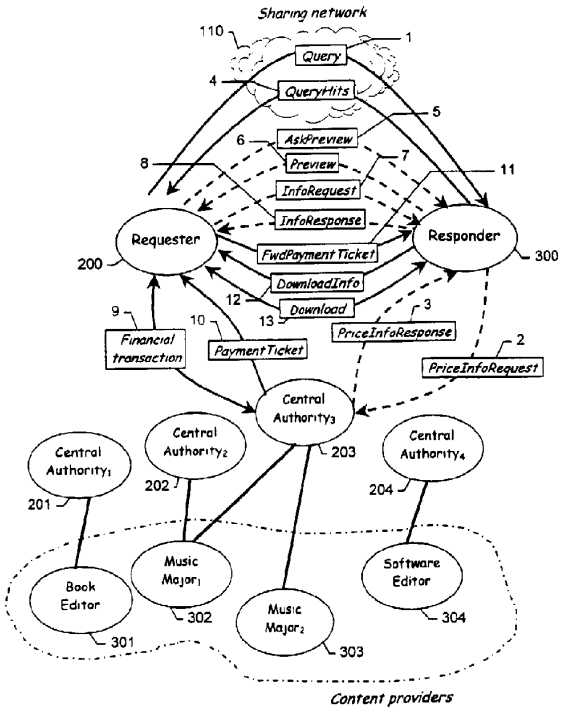
(74) Agent: **BERTHIER, Karine**; Thomson multimedia, 46 Quai Alphonse Le Gallo, F-92648 Boulogne cedex (FR).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR THE SECURE DISTRIBUTION OF DIGITAL CONTENT IN A SHARING NETWORK



(57) Abstract: The system for distributing a digital content, created by a content provider (301 - 304), to a requester (200) through a sharing network (110), comprises a central authority (201 - 204) working on behalf of the content provider and a responder (300), registered with the central authority. When the responder (300) receives a request (1) for a content corresponding to a file stored on his/her computer, content purchase information data (4) are sent to the requester. The requester then buys the content to the central authority and receives a proof of buying (11). In response to the sending of this proof of buying to the responder, the requester receives the file corresponding to the requested content. The responder then receives a compensation from the central authority for his/her participation in the distribution of the content.

WO 02/054196 A2

Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

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

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

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

Published:

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

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

System and method for the secure distribution of digital content in a sharing network

Field of the invention

The invention relates to a system and a method for distributing digital content through a sharing network.

Background art

With the increasing use of the Internet, distributed sharing networks in which users propose digital contents for sharing are becoming more and more popular. Examples of such systems are the NAPSTER browser and communication system (provided by Napster Inc.) allowing users to exchange MP3 files (audio files compressed using the MP3 compression format – "MP3" standing for "*Moving Picture Experts Group phase 1, audio layer 3*") or the GNUTELLA distributed information sharing system (provided by Wego.com, Inc.).

One problem encountered with these systems is that the contents are usually distributed for free by some users to others. The distribution protocols behind these systems do not take into account the right management of copyrighted contents and rely only on the goodwill of users. This results in a high piracy level and in important losses for copyrighted content providers who are left outside these sharing networks and do not receive any income for the distribution of the contents they have created.

In document US-A-6 029 141 there is disclosed an Internet-based software system and method enabling entities called "associates" to market products (e.g. books) that are sold from a merchant Internet site, in return for a commission. However, this system and method does not contain any security feature and may be subject to attacks from hackers (for example to receive commission instead of the "real" associate).

It is therefore an object of the present invention to provide a distributed sharing system in which copyrighted contents are protected against free distribution. Another object of the invention is to propose a secure protocol enabling secure commercial distribution of contents through sharing networks.

Summary of the invention

The invention relates to a system for distributing a digital content to a requester through a sharing network, characterized in that it comprises a central authority ; a responder, registered with said central authority, having means for distributing a data file corresponding to said content to the requester in exchange of a proof of buying received from said requester. The central authority comprises : means

CONFIRMATION COPY
Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0290
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

for establishing a financial transaction with said requester for the payment by the requester of the content proposed by said responder and for delivering the proof of buying to said requester; and a responder compensation means for providing said responder with a compensation in exchange of the buying of a content by a requester.

The invention also relates to a method for distributing a digital content through a sharing network using the above mentioned system and comprising the steps consisting for a responder in:

a) in response to a request for a digital content received from a requester through said sharing network, sending content purchase information data to said requester ; said content purchase information data including a responder identifier generated by a central authority and data identifying said central authority ;

b) receiving from said requester a proof of buying of said digital content, said proof of buying being delivered by said central authority ;

c) providing said requester with a data file corresponding to said digital content ; and

d) receiving from said central authority a compensation for the distribution of said digital content.

The invention further relates to a method for distributing a digital content through a sharing network using the above mentioned system and comprising the steps consisting for a requester in:

i) sending through said sharing network a first message to request a digital content ;

j) receiving content purchase information data from a responder having a data file corresponding to said content ; said content purchase information data including data identifying a central authority ;

k) in response to a financial transaction with said central authority, receiving a proof of buying of said digital content ;

l) sending said proof of buying to said responder ; and

m) receiving a data file corresponding to said digital content.

Brief description of the drawings

The various features and advantages of the present invention and its preferred embodiments will now be described with reference to the accompanying drawings which are intended to illustrate and not to limit the scope of the present invention and in which:

Fig. 1 illustrates the principle of an information sharing system.

Fig. 2a to 2c illustrate an example of a sharing network architecture.

CONFIRMATION COPY

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0291
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Fig. 3 illustrate the preferred protocol for distributing digital content through a sharing network according to the invention.

Description of the preferred embodiments

The present invention is independent of the underlying information sharing system but some mechanisms used by these systems need to be understood before presenting the detailed description of the invention.

Fig. 1 illustrates an abstract model of an information sharing system 100 in which hosts 101 – 106 are interconnected through a sharing network 110. A host designates both a computer and a specific software which is running on this computer to generate and to handle messages necessary to implement the sharing network. Some users logged on these hosts can propose files containing digital contents for sharing with other users. These files include music files, video files, image files, computer program files, etc.

Once a user, for example logged on $Host_1$ 101, sends a request 120 for a specific digital content on the sharing network 110, all users who are connected to the sharing network and who own files corresponding to this request can respond by sending responses 130. These users are called responders whereas the user who has sent the request is a requester.

Upon receipt of the responses, the requester can choose the files he is interested in and download these files by establishing a peer-to-peer connection between the host on which he is logged on and the host on which the responder is logged on.

Each user connected to the sharing network can be a requester and a responder.

On Fig. 2a to 2c, an example of a sharing network architecture corresponding to the information sharing system of Fig. 1 is presented. In this network, $Host_1$ 101 is connected to $Host_2$ 102 and $Host_6$ 106; $Host_2$ 102 being itself connected to $Host_3$ 103, $Host_4$ 104 and $Host_5$ 105. Each participating host of the system acts both as a client (a program sending a request and waiting for a response) and as a server (a program which respond to a request).

Each host 101 – 106 in the network can send a message to its neighbors in the network. Then, each host which receives a message forwards this message to its neighbors, resulting in a propagation of the message in the network until the message has expired or all the hosts of the network have received the message.

Fig. 2a illustrates such a routing system. In this example, a message M is first sent by $Host_1$ 101 to its peers $Host_2$ 102 and $Host_6$ 106. Then $Host_2$ 102 forwards

CONFIRMATION COPY
Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0292
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

this message M to its peers 103 – 105. At this moment, all the hosts of the network have received message M.

Fig. 2b and 2c illustrate a request/response mechanism. In Fig. 2b, $Host_1$ 101 submit a request RQ to its peers 102 and 106.The request RQ is forwarded until all the hosts of the network have received it (or until the request has expired). In this example, we suppose that $Host_4$ 104 and $Host_6$ 106 are able to give a response RS to the request RQ. In Fig. 2c, these hosts 104 and 106 send the response RS which is routed in the reverse direction of RQ to $Host_1$ 101. If the request RQ corresponds to a request by a user logged on $Host_1$ for a specific digital content, then the user can choose on which host 104 or 106 which have sent a response RS he will download the file containing the digital content.

We will now present in more details the commercial distributed sharing system of the invention and the secure protocol for distributing digital content in this system.

This system comprises classical actors of a sharing system:

- requesters, who represent users requesting file(s) containing digital content on the sharing network; and

- responders, who represent users who propose files for sharing and who have locally on their computer files requested by requesters.

Of course, as stated above, a same user may act as a requester and as a responder.

Contrary to known sharing systems of the prior art, in the system of the invention, requesters pay for the content they want to receive and responders receive money each time they propose a content to a requester who later buys it.

A new type of actor is therefore added in the sharing system of the invention: the central authorities. These entities are third parties who are responsible for selling contents on behalf of content providers. More specifically, they are responsible for collecting payments from requesters for contents which are sold on the network. They are also responsible for redistributing money both to the responder who distributed the content and to the content provider who created it.

Each central authority works on behalf of one or, preferably, several content providers such as music majors, book editors, software editors, etc. and is responsible for the selling of contents produced by these particular content providers. It is also possible for one content provider to work with several central authorities to sell its contents on the sharing network.

The purchase act is performed between the central authority and a requester who has found an interesting content proposed by a responder on the sharing network.

CONFIRMATION COPY
Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0293
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

The responder will receive later a compensation for having participated to the distribution of the content.

However, before being able to distribute contents on the sharing network and to receive money from a central authority working on behalf of content providers, all potential responder must be registered with this central authority. If a responder wants to distribute contents (copyrighted files) created by several content providers which do not use the same central authority, the responder must be registered with all the central authorities involved before being able to propose the contents for sharing.

The registration process may be performed in several ways: for example, via e-mail (electronic mail) or via a registration zone on the central authority's Web site. At the end of the registration process, a unique responder identifier is attributed to the responder by the central authority and this responder identifier is sent to the responder and is stored in a database of the central authority.

Once a responder is registered with a central authority, he is authorized to propose on the sharing network contents created by content providers for which the central authority works on behalf of.

Fig. 3 illustrates the actors involved in the secure protocol of the invention for distributing contents on a sharing network and the messages exchanged during this protocol.

Four different content providers have been represented on Fig. 3: a book editor 301, two music majors : Music $Major_1$ 302 and Music $Major_2$ 303 and a software editor 304.

Four central authorities are also represented on Fig. 3. Central $Authority_1$ 201 is working on behalf of the book editor 301. Central $Authority_2$ 202 is working on behalf of the music major 302 while Central $authority_3$ works for both music majors 302 and 303 and Central $Authority_4$ works for the software editor 304. These links between content providers and central authorities are represented on Fig. 3 by continuous lines.

It should be noted that the number of content providers and the number of central authorities are not linked and that each content provider may work with several central authorities. In the same way, each central authority may work on behalf of several content providers.

In fact the term "central authority" used in the following of the description designates both the entity itself (which may be for example a merchant) and a computer or server of this entity on which a particular software is running to implement the protocol which will be described bellow.

A requester 200 and a responder 300 are also represented on Fig. 3. We suppose that, before sending the first message to search for a specific content, the requester 200 and the responder 300 are both connected to the sharing network 110. The

CONFIRMATION COPY
Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0294
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

connection mechanism is out of the scope of the present invention and uses the underlying sharing protocol.

The terms "requester" and "responder" as used bellow both designate on the one hand a computer and a software running on this computer forming a host of the sharing network, and on the other hand a natural person who is using this computer either for looking for a digital content on the sharing network (requester), or for proposing his/her files containing digital contents for sharing (responder). Of course, as previously stated, a same natural person and host may be sometimes a requester and sometimes a responder.

Fig. 3 illustrates more particularly the messages exchanged by the actors described above during a search and a purchase of a digital content on the sharing network 110.

In the following description of the protocol for distributing digital content, we suppose that all files (containing protected digital contents) requested by the requester have been produced by Central Authority$_3$ 203 with which the responder is registered. Of course, the responder may distribute files created by several central authorities. In that case, the responder must be registered with all these central authorities and must have a way to retrieve the right central authority according to the requested file.

A possible implementation to create a file containing a protected digital content in a responder's computer will be described bellow.

If we take the example of audio contents, we suppose that the responder has bought a CD (acronym of "Compact Disc") containing several songs, this CD being produced by Music Major$_2$ 303. If the responder wants to share these songs with potential requesters (and to receive compensation for that), he/she will first insert the CD in the CD or DVD (acronym of "Digital Versatile Disc") player of his/her computer. Through the user interface of the sharing network software running on his/her computer, the requester will choose which songs he/she wants to propose for sharing. Then, the central authority working on behalf of Music Major$_2$ 303 (here Central Authority$_3$ 203) will be contacted by the responder for example by entering the URL (acronym of "Uniform Resource Locator" which defines a unique address fully specifying the location of a file or other resource on the Internet) of Central Authority$_3$ 203's Web site (indicated for example in the booklet accompanying the CD) on his/her Web browser.

If the responder has already been registered with Central Authority$_3$ 203, then he/she will indicate the songs he/she wants to distribute on the sharing network and will receive from Central Authority$_3$ 203 the corresponding files (containing the songs

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0295
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

in a compressed format for example) comprising an identifier of Central Authority$_3$ 203 and other information such as the price of the song.

If the responder is not registered with Central Authority$_3$ 203, he/she will first have to register with this central authority as explained above before receiving the files corresponding to the songs he/she wants to propose for sharing.

Then, the sharing network software running on the requester's computer will store the files received from Central Authority$_3$ 203 on a particular place of the computer's storage medium.

Referring back to Fig. 3, when a requester 200 sends a query to the sharing network 110 (message *Query* sent at step 1), he/she receives responses when some users connected to the network have files satisfying the requester's query.

In Fig. 3, we suppose that responder 300 has locally a file (or some files) that satisfies the query sent at step 1 by the requester 200. If the file (i.e. the digital content) is available for free, then the classical protocol of the prior art is used. Otherwise, if the file (i.e. the content) is copyright-protected, the responder has locally an information about the price of the file. This price information has been previously delivered by the central authority (here Central Authority$_3$ 203) working on behalf of the content provider which has produced the requested content (here Music Major$_2$ 303).

However, this price information has an expiration date allowing the central authority to change the price of the file over the time. If the price information stored by the responder (or more precisely stored in the storage medium of the responder's computer) has expired, then the responder requests to Central Authority$_3$ 203 a new price information for the particular file requested by the requester 200 by sending a *PriceInfoRequest* message 2.

This *PriceInfoRequest* message 2 which is optional (it is not sent if the price information of the file stored by the responder has not expired) is illustrated in Fig. 3 with a dotted-line arrow as will be illustrated all optional messages which can be sent in the protocol of the invention.

When the central authority 203 receives a *PriceInfoRequest* message 2, it responds by a *PriceInfoResponse* message 3 containing the new price information for the requested file. This message has an expiration date. It should be noted in addition that, preferably, the price information returned by the central authority depends on the identity of the responder. Indeed, some responders can actively participate to the distribution of copyright-protected files and thus can have agreements with central authorities to sell files at lower prices and/or have more interested price margins.

When the responder has a non-expired price information of the file containing a digital content requested in the *Query* message 1, it sends a *QueryHits*

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0296
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

message 4 containing information that the requester needs to make his choice and to buy the file. This information includes the file name, the file size, the quality of the file (e.g. a recording mode in case of audio files, version for a software file, etc.), the price, the name of the central authority (or URL) where the file can be bought, the payment protocol accepted by the central authority, the responder identifier (generated by the central authority and given to the responder at the end of the registration process described above).

In a preferred implementation, the sharing network software is running permanently on the responder's computer when the responder is connected to the sharing network 110 and the messages *QueryHits* 4 and/or *PriceInfoRequest* 2 are generated automatically by this software without any intervention of the responder (as natural person).

A requester may receive several *QueryHits* messages from different responders connected to the sharing network. Upon receipt of these responses to his/her query, the requester can make his/her choice. For example, the requester can choose the best price, make a tradeoff between the price and the quality or choose a preferred central authority with which he/she has preferential agreements, etc.

While messages *Query* 1 and *Queryhits* 4 are routed between the requester 200 and the responder 300 through the sharing network 110 (using a routing mechanism which depends on the underlying sharing system), once the requester has chosen one responder, it switches to a point-to-point communication with the responder. A point-to-point communication (also known as "peer-to-peer" communication) consists in exchanging messages between two identified hosts of the sharing network contrary to the mechanism explained with reference to Fig. 2a to 2c.

All other messages, described bellow, exchanged between the requester and the responder, are point-to-point messages.

Furthermore, the requester may optionally ask for a preview of the file by sending a *AskPreview* message 5 to the responder. This feature is particularly interesting in the case of a copyright-protected file: it can be a short time of music in the case of music file, or a demonstration version in the case of a software, or a short clip in the case of video file, etc.

If the requester 200 asked for a preview, the responder 300 responds by a *Preview* message 6 and sends the requester a preview of the requested file.

If the requester 200 decides to buy many files containing copyright-protected content (for example if the query consists in searching all the songs of one singer, then several files may correspond to this query), he can optionally ask for a preferential price by sending an *InfoRequest* message 7 to the responder 300. Upon receipt of this message, the responder 300 requests preferential prices on behalf of the

CONFIRMATION COPY
Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0297
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

requester 200 by sending a *PriceInfoRequest* message 2 to the central authority 203 and receives a *PriceInfoResponse* message 3 from the central authority 203.

Then, the responder sends to the requester the preferential prices in the *InfoResponse* message 8. If preferential prices have not been accepted by the central authority, this message is empty.

In a preferred embodiment, messages *PriceInfoRequest* 2 and *InfoResponse* 8 are generated automatically by the software running on the requester without any "human" intervention.

If the requester 200 is satisfied with the conditions obtained from the responder 300, he/she is able to make the purchase of the requested file(s) by using the information contained in the *QueryHits* 4, and optionally *InfoReponse* 8, messages. Preferably, the purchase act uses the World Wide Web to get the existing payment infrastructure. The requester 200 contacts the central authority 203 (using the central authority URL contained in the *QueryHits* message 4) and performs a secure Financial transaction 9 with the central authority. During this transaction, the requester sends some data contained in the *QueryHits* message (such as responder identifier). The result of this transaction 9 is the payment of the central authority 203 for the copyright-protected file(s).

The central authority will later be able to pay, on the one hand the content provider and, on the other hand the responder 300 for his/her participation in the distribution of the file(s). Payment of the responder may be made by crediting an account of the responder opened by the central authority during the registration process.

At the end of the financial transaction 9, the central authority 203 delivers a payment ticket (sent in *PaymentTicket* message 10) to the requester 200 that proves the requester has paid for the file(s). This payment ticket is forwarded to the responder 300 which has distributed the bought file(s) in a message *FwdPaymentTicket* 11. Upon receipt of this message 11, the responder 300 verifies the validity of the payment ticket and, if the verification succeeds, the responder responds by sending to the requester all information needed to download the requested file(s) in a *DownloadInfo* message 12. Then, the requester 200 begins the *Download* operation 13 of the bought file(s).

Given the sensitivity of some data contained in the messages exchanged in the above described protocol, it is necessary to protect these messages against any possible attack during their transmission.

We will now describe in further details the security needs of the system for distributing digital content according to the invention and how they are fulfilled in the preferred embodiment of the invention.

CONFIRMATION COPY
Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0298
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

The following notations and acronyms will be used throughout this description :

"," denotes the concatenation operator;

"{M}+" denotes the repetition of message M n times with n>0;

"PBSK" denotes a signature verification public key;

"PRSK" denotes a signature private key;

"SK" denotes a symmetric key;

"MK" denotes a master symmetric key;

"DK" denotes a derived symmetric key;

"SSK" denotes a symmetric session key;

"E_{SK} (M)" denotes the symmetric encryption of message M using the symmetric key SK;

"S_{PRSK}^{A} (M)" denotes the signature of message M using A's signature private key PRSK;

"H (M)" denotes the hash value of message M using hash function H.

Preferably, the following cryptographic algorithms will be used to implement the system and method of the invention :

- "AES" (acronym of "*Advanced Encryption Standard*") will be used for symmetric encryption. More details about the AES standard can be found in the Internet publication "NIST, "*Adanced Encryption Standard Development Effort*", at http://csrc.nist.gov/encryption/aes" and in "DAEMEN J. and RIJMEN V., *"The Rijndael Block Cipher"*, AES Proposal, at http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf".

- "RSA" (acronym of "*Rivest Shamir Adelman*" the names of the creators of this algorithm) with "SHA-1" as hash function will be used as signature algorithm. This algorithm will be used in accordance with the standard PKCS#1 v2.1 described in the following Internet publication: "RSA LABORATORIES, "*PKCS #1 v2.1: RSA Cryptography Standard*", September 1999 (draft status), http://www.rsalabs.com/pkcs/pkcs-1".

- "SHA-1" will be used as hash function *H* (information about SHA-1 function can be found in "*NIST, SIPS PUB 180-1, "Secure Hash Standards", Avril 1995*").

In the preferred implementation of the invention, the size of the cryptographic keys is the following:

- 1024 bits for signature keys;

- 128 bits for symmetric keys.

CONFIRMATION COPY
Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0299
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

At first, the system should guarantee to requesters:

a) *Anonymity*: the responder should not know the identity of the requester. He/she should not be able to link several purchases, i.e. to know whether two different purchases are from the same requester or not.

To ensure this anonymity, in a preferred implementation, the identity of the requester is hidden behind its IP address (IP being the acronym of "Internet Protocol"). As in most of cases, this address is dynamically attributed at each Internet connection; therefore the responder is not able to link two different requests.

b) *Security of Payment*: the responder should be sure that his/her payment is secure.

This is ensured by the payment protocol itself used in the financial transaction 9 whatever it is, for example SET (acronym of "*Secure Electronic Transaction*", information about which can be found in "Loeb L., "*Secure Electronic Transactions: Introduction and Technical Reference*", Artech House Publishers, 1998") or SSL (acronym of "*Secure Socket Layer*", a well-known payment protocol used on the Internet) or a micropayment protocol.

c) *Proof of buying*: the responder should be sure that the proof of buying he/she gets (i.e. the payment ticket received in message 10) from the central authority is valid and will always allow him/her to get the file he/she bought. Nobody else than him/her may use that proof of buying. In addition, the responder should have the ability to verify that proof which should also be checkable by the responder.

In a preferred embodiment, the proof of buying, i.e. the payment ticket, is signed by the central authority (using a signature private key $PRSK_{CA}$ as further explained bellow) before being transmitted to the requester to prove its validity. This signed payment ticket preferably includes information on the bought content and the identity of the responder (i.e. the responder identifier which has been received by the requester in the *QueryHits* message 4).

In addition, in order not to be used by a hacker who may intercept the *PaymentTicket* message 10, the latter (in fact the signed payment ticket) is further encrypted by the central authority before being transmitted to the requester. It is encrypted using a key K_{PAY} that has already been used (or generated) in the payment protocol used during the financial transaction 9 and which is shared by the requester and the central authority. For example SET and SSL protocols define such keys.

Moreover, in order to secure the transmission of the payment ticket between the requester and the responder in the *FwdPaymentTicket* message 11, a symmetric session key SSK is used to create an encrypted channel between the requester and the responder for the transmission of the *FwdPaymentTicket* message 11. The way this key

CONFIRMATION COPY
Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0300
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

SSK is generated by the central authority and shared by both the requester and the responder will be further detailed bellow.

The system should further guarantee to responders:

a) *Privacy*: nobody else than the relevant responder may obtain information (prices, reductions... which may be different for each responder) on commercial agreements made with a central authority.

To ensure this privacy, in a preferred implementation the *PriceInfoResponse* message 3 is encrypted by the central authority before its transmission to the responder in such a way that only the right responder is able to decrypt it. Preferably, it is encrypted using a symmetric encryption key DK_{PR} which is generated by the central authority during the responder's registration process and which is derived from a master key MK_{PR} (only known by the central authority) and from the responder identifier. This key DK_{PR}, which is different for each responder, is sent by the central authority to the responder at the end of the registration process together with the responder identifier. If a responder tries to know the price conditions of one concurrent, he will receive them encrypted and will not be able to decrypt them.

b) *Rightness of pricing*: the responder should be sure that the price information received from a central authority in the *PriceInfoResponse* message 3 is valid and will thus be further accepted by this authority.

In a preferred embodiment, the price information is signed by the central authority (using the signature private key $PRSK_{CA}$) before being transmitted to the responder in the *PriceInfoResponse* message 3. Preferably, the signed price information contains some information on the file proposed for sharing, the price, the time limit of the price validity, the responder identifier, some information about the quality of the file, the modes of payment accepted by the central authority and the central authority URL.

c) *Assurance of payment*: nobody else than the relevant responder should obtain payment from a central authority.

This is ensured in the preferred implementation by the presentation of the proof of buying (i.e. payment ticket) to the responder (in the *FwdPaymentTicket* message 11), since the responder identifier is included in that proof which is generated by the central authority.

d) *Confidentiality*: the download information transmitted to the requester in the *DownloadInfo* message 12 and the content to be downloaded during *Download* operation 13 are to be kept confidential during their transmission to the requester.

CONFIRMATION COPY
Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0301
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

This is ensured in the preferred embodiment by the presence of an encrypted channel between the responder and the requester, this encrypted channel being created thanks to a symmetric session key SSK as it will be further described bellow.

e) *Restriction to the purchase*: it should be ensured that the requester may get nothing from the responder but the content he bought.

In a preferred implementation, the responder's computer has a permanent directory where all the contents (i.e. all the files received from central authorities when the responder has acquired the right to distribute the contents on the sharing network) are available in an encrypted form (each content being encrypted with its proper key $K_{content}$). Then, the responder transmits the decryption key $K_{content}$ of the bought content (via the encrypted channel) to the requester in the *DownloadInfo* message 12 and the content itself is transmitted in its encrypted form (using key $K_{content}$) to the requester in the *Download* operation 13. Integrity of the content may be obtained by including in the encrypted content transmitted the hash value of the content.

An alternative solution would be for the responder to dynamically create a directory in which the bought files are placed. This directory would be destroyed after the *Download* operation 13 occurs. The content will have to be encrypted on the fly by the responder to be sent, through the encrypted channel, to the requester.

Finally, the system should ensure to central authorities the validity of payment (i.e. the fact that the payment they receive is valid). This is ensured by the payment protocol used in the *Financial transaction* 9.

In order to implement the preferred embodiments that have been described to ensure security in the protocol of the invention, several cryptographic keys need to be generated and shared by the actors of the system as it will be described bellow.

At first each central authority has a signature private key $PRSK_{CA}$ which is used to certify the prices and the payments. The associated signature verification public key $PBSK_{CA}$ will need to be certified. In a preferred solution, we propose to use cross-certification between the different central authorities which avoids building a heavy Public Key Infrastructure. The requester will then have to trust at least one central authority.

Moreover, each central authority has also two master symmetric keys MK_{PR} (to protect the transmission of the price information in the *PriceInfoResponse* message 3) and MK_{EC} (to build an encrypted channel between the responder and the requester). Central authorities will distribute to each responder at its registration, in addition to its responder identifier, two derived keys :

$DK_{PR} = E_{MK_{PR}}$ (*responder identifier*); and

CONFIRMATION COPY
Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0302
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

$DK_{EC} = E_{MK_{EC}}(responder\ identifier)$.

As for the responders, they need to get at their registration the two derived keys DK_{PR} and DK_{EC}. They also have to create a symmetric key $K_{content}$ for each content they will distribute through the sharing network. Each content will be stored in a specific directory of the responder in the following form:

$E_{K_{content}}(content, H(content))$.

Regarding requesters, they do not need any dedicated key beforehand. However, they will use a key K_{PAY} that is used and / or built in the payment protocol used in the financial transaction 9. This key K_{PAY} is used to encrypt the payment ticket transmitted between the central authority and the requester in message *PaymentTicket* 10.

Finally, one symmetric session key SSK is created at each purchase of a content. This key SSK will be used to create an encrypted channel between the requester and the responder. The key SSK is created by the central authority after the financial transaction 9 (during when the responder identifier has been transmitted to it). The central authority first generates a random value R. Then, it calculates $SSK=E_{DK_{EC}}(R)$. The key DK_{EC} is reconstructed by the central authority from the master key MK_{EC} and the responder identifier:

$DK_{EC} = E_{MK_{EC}}(responder\ identifier)$.

The session key SSK is transmitted, together with the random value R, to the requester in the *PaymentTicket* message 10 (encrypted with key K_{PAY}). Then, the requester sends the random value R to the responder which is able to calculate $SSK= E_{DK_{EC}}(R)$ with its key DK_{EC}. Finally, both the requester and the responder share the same session key SSK and can therefore built an encrypted channel.

In the following part of the description, we will propose a more detailed description of the internal content of the messages 1-13 exchanged in the protocol illustrated in Fig. 3. This description is of course a possible implementation and should not be understood as limiting the scope of the invention.

1. *Query* message 1:

This message is sent by a requester to search for specific file(s) in the sharing network 110. For this purpose, the requester types a search criterion describing the requested file(s). For example, a "*britneyspears*.mp3*" search criterion may indicate that the requester is looking for all shared MP3 files for which the artist is "Britney Spears".

The detailed message format is presented in Table 1 bellow:

CONFIRMATION COPY
Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0303
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Fields of message	Description of the fields
Query message data	{*Minimum speed, Search criteria*}
Minimum speed (2 bytes)	Minimum speed (in KB/second) of hosts that should respond to this message with a *QueryHit* message.
Search Criteria (variable length)	Null-terminated search string.

Table 1

2. *PriceInfoRequest* message 2:

This message is sent by a responder to a central authority to request purchase information (price, payment schemes accepted by the central authority, etc.) for copyrighted files proposed by the responder for sharing. In practice, the responder has locally purchase information for all of his copyrighted-shared files. However, this information has an expiration date and must therefore be refreshed on a regular basis.

This message can be sent at different times during the procedure:

- at first, it can be sent by the responder before he proposes copyrighted files for sharing. In that case, the responder uses this message to have an initial purchase information;

- secondly, it can be sent after the responder has received an *InfoRequest* message 7 from the requester. The *InfoRequest* message 7 is used by a requester to have preferential prices in some situations (for example when the requester decides to buy many files);

- it can also be sent each time a responder detects that some local purchase information has expired.

This *PriceInfoRequest* message 2 also contains information about the responder identity. Indeed, the responder can negotiate in an out of band way with central authorities his price margins and/or preferential prices proposed to the requesters. Therefore, the presence of the responder identity in this message allows the central authority to propose the right prices according to the responder.

The detailed message format is presented in Table 2 bellow:

Fields of message	Description of the fields
***PriceInfoRequest* message data**	{***ResponderID, ReqPurchaseNumber,*** {***ReqPurchaseInfo***}+}
ResponderID (32 bytes)	Responder identifier generated by the central authority during the responder registration.
ReqPriceNumber (1 byte)	Number of requested purchase information.
ReqPurchaseInfo	{***FileIndex, FileSize, FileName, Quality***}

CONFIRMATION COPY
Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0304
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

FileIndex (4 bytes)	Unique identifier representing the file for which the responder requests price information.
FileSize (4 bytes)	Size (in bytes) of the file indexed by *FileIndex*.
FileName (variable length)	Double-null terminated string representing the name of the local file indexed by *FileIndex*.
Quality (variable length)	Double-null terminated string representing a quality measure of the file indexed by *FileIndex*.

Table 2

It should be noted that :

- the *ReqPurchaseInfo* field appears *ReqPurchaseNumber* times in the *PriceInfoRequest* message 2 (one for each file for which the responder needs purchase information);

- the set (*FileIndex, FileSize, FileName, Quality*) must uniquely identify a same file at the responder side and at the central authority side. This ensures that the central authority is able to give the right price to the responder. For this purpose, *FileIndex* can use a mechanism similar to ISBN for books numbering ("ISBN" is the acronym of "*International Standard Book Number*").

3. *PriceInfoResponse* message 3:

This message is sent by the central authority to the responder and contains purchase information requested by the responder in the *PriceInfoRequest* message 2. This purchase information includes all information needed by a requester to choose a file to download once he has sent a query and he has received responses from responders. All proposed purchase information has an expiration date and once this information is received by the responder, it must be stored by the responder until this date.

As previously stated, this message should be confidential. The data it contains are therefore encrypted with the symmetric key DK_{PR} before being sent to the responder.

The detailed message format is presented in Table 3 bellow:

Fields of message	Description of the fields
***PriceInfoResponse* message data**	***{EncryptedPriceInfoResponse}***
EncryptedPriceInfoResponse	$E_{DK_{PR}}$(***PurchaseInfoNumber,{SignedPurchaseInfo}+***)
PurchaseInfoNumber (1 byte)	Number of purchase information contained in the message.
SignedPurchaseInfo	S^{CA}_{PRSK} (***PurchaseInfo***)

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0305
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

PurchaseInfo	{*FileIndex*, *FileSize*, *FileName*, *Quality*, *Price*, *PriceValidity*, *MerchantName*, *PaymentMode*, *CA_URL*, *ResponderID*}
FileIndex (4 bytes)	Unique file identifier. This field is extracted from the *PriceInfoRequest* message 2.
FileSize (4 bytes)	Size (in bytes) of the file indexed by *FileIndex*. This field is extracted from the *PriceInfoRequest* message 2.
FileName (variable length)	Double-null terminated string representing the name of the local file indexed by *FileIndex*. This field is extracted from the *PriceInfoRequest* message 2.
Quality (variable length)	Double-null terminated string representing a quality measure of the file indexed by *FileIndex*. This field is extracted from the *PriceInfoRequest* message 2.
Price (variable length)	Double-null terminated string indicating the price of the file indexed by *FileIndex*. This field is formed by three sub-fields separated each other by null character: "*Currency*", "*Amount*", "*AmtExp10*". *Currency* specifies the three-digit ISO 4217 currency code. *Amount* represents the amount of payment. *AmtExp10* represents an exponent base 10 such that amount*($10^{amtExp10}$) shall be the value in the minor unit of the currency specified in ISO 4217.
PriceValidity (variable length)	Double-null terminated string indicating the time during which the proposed price is valid for the file indexed by *FileIndex*. After this time, the responder will have to request new purchase information.
MerchantName (variable length)	Double-null terminated string representing a human readable name of the central authority responsible for the selling of the file indexed by *FileIndex*.
PaymentMode (variable length)	Double-null terminated string representing the payment schemes acceptable by the central authority for the purchase of the corresponding file. The schemes are separated from each other's by a null character.
CA_URL (variable length)	Double-null terminated string indicating the URL of the central authority that will sell the file indexed by *FileIndex* to requesters. A payment server accepting the payment protocols indicated in the *PaymentMode* field must run at this URL.
ResponderID (variable length)	Unique identifier generated by the central authority during the registration of the responder that emitted the *PriceInfoRequest* message 2. This field is extracted from the *PriceInfoRequest* message.

Table 3

4. *QueryHits* message 4:

This message is sent by a responder in response to a *Query* message 1 received from a requester. If a responder has locally files that correspond to the

CONFIRMATION COPY
Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0306
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

requester's query, the responder responds by a *QueryHits* message 4. This message should contain all data needed by the requester to make his/her choice.

This choice can be made on several bases:

- the price: the requester should know the price of copyrighted files;
- the price/quality tradeoff: the requester should know the quality for the proposed files. Therefore, a quality measure has to be proposed by the commercial distributed sharing system;
- the accepted payment systems: the requester should know if he is able to pay the requested files with the proposed payment schemes;
- the merchant name (i.e. central authority name): the requester may have preferential relationships with some merchants.

All these data have been originally generated by the central authority, which is responsible for the selling of the corresponding files. Therefore, most part of this message is extracted from the *PriceInfoResponse* message 2.

Moreover, this message proposes an optional field representing the personal responder's Web site URL allowing the requester to get personal information on the responder. This field can be useful in the case where the requester detects that the responder has many interesting files. By giving his/her Web site address, the responder provides the requester with a way to access value-added services such as complete file catalogue, e-mail service, chat, etc.

The detailed message format is presented in Table 4 bellow:

Fields of message	Description of the fields
***QueryHits* message data**	***{HitNumber, PortNumber, IPAddress, Speed, [ResponderURL], {SignedPurchaseInfo}+}***
HitNumber (1 byte)	Number of shared files proposed by the responder that satisfy the requester's query.
PortNumber (2 bytes)	Transport-layer port number that the requester must use if he decides to use this responder as the file seller.
IP Address (4 bytes)	Responder's IP address that the requester must use if he decides to use this responder as the file seller.
Speed (4 bytes)	Speed (in KB/second) of the responder.
ResponderURL (variable length)	Double-null terminated string that indicates the address of the responder's personal Web site. This field is optional and can be used by the requester to find responder's personal information and other value-added services (chat, e-mail, etc.).
SignedPurchaseInfo	This field contains all information about the files proposed by the responder for sharing and that satisfy the requester's query. This field has been generated and signed by the central authority to build the *PriceInfoResponse* message 3 and is extracted from this message.

CONFIRMATION COPY
Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0307
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Table 4

It should be noted that:

- the *SignedPurchaseInfo* field appears *HitNumber* times in the *QueryHits* message 4 (one for each file satisfying the requester's request);

- the prices given by the responder in this message are imposed by the central authority working for the content providers which have produced the corresponding contents. These prices are known by the responder thanks to the *PriceInfoRequest/PriceInfoResponse* messages pair.

5. *AskPreview* message 5:

This optional message is sent by the requester to ask for a preview of a specific file. This message is sent once the requester has received a *QueryHits* message 4. By choosing a specific file in the list of responders' propositions, the requester can receive a preview of the file by sending this message.

It should be noted that this message is a point-to-point message and thus does not traverse the sharing network 110. For this purpose, it uses the *IPAddress* and *PortNumber* fields received from the responder in the *QueryHits* message 4.

The detailed message format is presented in Table 5 bellow:

Fields of message	Description of the fields
***AskPreview* message data**	***{FileIndex, FileSize, FileName, Quality}***
FileIndex (4 bytes)	Unique file identifier. This field is extracted from the *QueryHits* message 4.
FileSize (4 bytes)	Size (in bytes) of the file indexed by *FileIndex*. This field is extracted from the *QueryHits* message 4.
FileName (variable length)	Double-null terminated string representing the name of the local file indexed by *FileIndex*. This field is extracted from the *QueryHits* message 4.
Quality (variable length)	Double-null terminated string representing a quality measure of the file indexed by *FileIndex*. This field is extracted from the *QueryHist* message 4.

Table 5

6. *Preview* message 6:

This message is used by the responder to send a preview requested by the requester in the *AskPreview* message 5. The sent preview is not interpreted by the requester's client software but locally stored for being later played by the adequate player.

The detailed message format is presented in Table 6 bellow:

CONFIRMATION COPY
Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0308
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Fields of message	Description of the fields
***Preview* message data**	***{FileIndex, FileSize, FileName, BitStream}***
FileIndex (4 bytes)	Unique file identifier. This field is extracted from the *AskPreview* message 5.
FileSize (4 bytes)	Size (in bytes) of the file indexed by *FileIndex*. This field is extracted from the *AskPreview* message 5.
FileName (variable length)	Double-null terminated string representing the name of the local file indexed by *FileIndex*. This field is extracted from the *AskPreview* message 5.
BitStream (variable length)	BitStream representing the preview requested by the requester in the *AskPreview* message 5.

Table 6

7. *InfoRequest* message 7:

This message is optional and is used by the requester to receive preferential prices for a set of files chosen from a previously received *QueryHits* message 4. This message is typically used when a requester wants to buy many files that can justify such preferential prices. Upon receipt of this message, the responder will send a new *PriceInfoRequest* message 2 to the central authority in order to get fresh price information.

Contrary to *Query* and *QueryHits* messages 1 and 2, this message is directly sent, through a point-to-point connection, to the responder by using the *IPAddress* and *PortNumber* fields contained in the *QueryHits* message 4. Therefore, this message is not routed through the sharing network 110.

The detailed message format is presented in Table 7 bellow:

Fields of message	Description of the fields
***InfoRequest* message data**	***{ReqInfoNumber, {ReqFileInfo}+}***
ReqInfoNumber (1 byte)	Number of shared files proposed by the responder and for which the requester wants to get purchase information.
ReqFileInfo	***{FileIndex, FileSize, FileName, Quality}***
FileIndex (4 bytes)	File index used to uniquely identify the file for which the requester asks purchase information. This field is extracted from the *QueryHits* message 4.
FileSize (4 bytes)	Size (in bytes) of the file indexed by *FileIndex* and for which the requester asks purchase information. This field is extracted from the *QueryHits* message 4.

CONFIRMATION COPY
Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0309
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

FileName (variable length)	Double-null terminated string representing the name of the local file indexed by *FileIndex* and for which the requester asks purchase information. This field is extracted from the *QueryHits* message 4.
Quality (variable length)	Double-null terminated string representing a quality measure of the file indexed by *FileIndex* and for which the requester asks purchase information. This field is extracted from the *QueryHits* message 4.

Table 7

It should be noted that the *ReqFileInfo* field appears *ReqInfoNumber* times in the *InfoRequest* message 7 (one for each file for which the requester needs purchase information).

8. *InfoResponse* message 8:

This message contains all purchase information requested by the requester in the *InfoRequest* message 7. Moreover, this message proposes an optional field representing the personal responder's Web site URL allowing the requester to get personal information on the responder. This field can be useful in the case where the requester detects that the responder has many interesting files. By giving his Web site address, the responder provides the requester with a way to access value-added services such as complete file catalogue, e-mail service, chat, etc.

As the *InfoRequest* message 7, this message does not traverse the sharing network 110 but is directly sent to the requester.

The detailed message format is presented in Table 8 bellow:

Fields of message	Description of the fields
***InfoResponse* message data**	***{[ResponderURL], PurchaseInfoNumber, {SignedPurchaseInfo}+}***
ResponderURL (variable length)	If present, this field indicates the responder's Web site address at which the requester can fin value-added services.
PurchaseInfoNumber (1 byte)	Number of purchase information contained in this message.
SignedPurchaseInfo	This field is the same as the one generated in the *PriceInfoResponse* message 3 and contains all price information requested by the requester

Table 8

It should be noted that:

- the *SignedPurchaseInfo* field appears *PurchaseInfoNumber* times in the *InfoResponse* message 8 (one for each file for which the requester needs purchase information);

CONFIRMATION COPY
Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0310
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

- theoretically (in the best case), the *PurchaseInfoNumber* field has the same value as the *ReqInfoNumber* field of the *InfoRequest* message 7. However, in some malfunction cases (central authority shutdown, database crashing, etc.), the responder may be unable to send purchase information about some files. In this case, we have *PurchaseInfoNumber< ReqInfoNumber*;

- upon receipt of this message 8, the requester should verify that the received information matches the one he requested. If the verification fails, an adapted behavior should be taken by the requester. A reasonable behavior would consist to skip all purchase information that do not match.

9. Financial transaction 9:

This section does not cover a special message but a suite of messages resulting in the payment of the central authority by the requester for the requested files. The payment phase is out of the scope of the invention and can be implemented by any payment protocol (e.g. SET, SSL, micropayment, etc.) supported by the central authority (i.e. those which have been sent in the *QueryHits* and *InfoResponse* messages 4 and 8).

However, the payment phase should be preceded by a negotiation phase in which the requester presents an order form and the payment scheme he/she chooses among the list of accepted payment protocols. This information is extracted from the *InfoResponse* or *QueryHits* messages previously received by the requester.

Table 9 bellow presents the *Negotiation* message sent by the requester to the central authority:

Fields of message	Description of the fields
***Negotiation* message data**	***{FileNumber, ChosenPaymentMode, {SignedPurchaseInfo}+}***
FileNumber (1 byte)	Number of files that the user wants to buy to this central authority.
ChosenPaymentMode (variable length)	Double-null terminated string representing the payment scheme chosen by the requester to pay the corresponding file. This field must belong to the *PaymentMode* sub-field of the *SignedPurchaseInfo* field of the *QueryHits* message 4.
SignedPurchaseInfo (variable length)	Data set representing a file that the requester wants to buy. This set is retrieved from the *QueryHits* message 4 or the *InfoResponse* message 8 and has been originally generated and signed by the central authority contacted by the requester for the purchase.

Table 9

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0311
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

It should be noted that:

- the *SignedPurchaseInfo* field appears *FileNumber* times in the *Negotiation* message (one for each file that the requester wants to buy);

- Before launching the financial transaction, the central authority verifies the validity of the presented price information and the responder identifier contained in the *SignedPurchaseInfo* field. If the verification fails, the transaction is cancelled.

10. *PaymentTicket* message 10:

This message is delivered by the central authority to the requester once the financial transaction is completed.

The detailed message format is presented in Table 10 bellow:

Fields of message	Description of the fields
***PaymentTicket* message data**	***{EncryptedPaymentTicket}***
EncryptedPaymentTicket	$E_{K_{PAY}}$ ***(SignedPaymentTicket, Challenge, SSK)***
SignedPaymentTicket	S^{CA}_{PRSK} ***(ResponderID, TransactionNumber, {TransactionInfo}+)***
ResponderID (32 bytes)	Responder identifier used by the central authority during the purchase of the corresponding files.
TransactionNumber (1 byte)	Number of files that the requester has paid.
TransactionInfo	***{FileIndex, FileSize, FileName, Quality}***
FileIndex (4 bytes)	Unique file identifier representing the corresponding file paid by the requester.
FileSize (4 bytes)	Size (in bytes) of the file indexed by *FileIndex*.
FileName (variable length)	Double-null terminated string representing the name of the local file indexed by *FileIndex*.
Quality (variable length)	Double-null terminated string representing a quality measure of the file indexed by *FileIndex*.
Challenge (16 bytes)	Random value generated by the central authority to derive the session key *SSK*.
SSK (16 bytes)	Session key to be shared between the requester and the responder: $SSK = E_{DK_{EC}}$ *(Challenge)*.

Table 10

It should be noted that the *TransactionInfo* field appears *TransactionNumber* times in the *PaymentTicket* message 10 (one for each file that the requester paid).

11. *FwdPaymentTicket* message 11:

CONFIRMATION COPY
Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0312
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

This message is sent by the requester to the responder to prove that he/she has bought some copyright-protected files. This message contains about the same data than the *PaymentTicket* message 10.

The detailed message format is presented in Table 11 bellow:

Fields of message	Description of the fields
***FwdPaymentTicket* message data**	***{EncryptedFwdPaymentTicket}***
EncryptedFwdPaymentTicket	E_{SSK} (***SignedPaymentTicket*), *Challenge***
SignedPaymentTicket (variable length)	*SignedPaymentTicket* field that was generated by the central authority as a proof of buying and which is extracted from the *PaymentTicket* message 10.
Challenge (16 bytes)	*Challenge* generated by the central authority and which is extracted from the *PaymentTicket* message 10. It will be used by the responder to calculate the session key SSK.

Table 11

12. *DownloadInfo* message 12:

This message is sent by the responder to the requester once he received the *FwdPaymentTicket* message 11 proving that the requester paid some files. In this message, the responder gives the URL at which the requester can ask the download of the bought files. For facility purpose, we propose to use the HTTP protocol for the download phase. Therefore, an HTTP server should run at the URL contained in the *DownloadInfo* message 12.

Moreover, in order to secure the download phase against eavesdropping, the downloaded files will be encrypted. The *DownloadInfo* message 12 therefore also contains the decryption key that will be used by the requester to retrieve the original bought files.

In addition, this feature prevents the requester to download files other than those he bought.

The detailed message format is presented in Table 12 bellow:

Fields of message	Description of the fields
***DownloadInfo* message data**	***{EncryptedDownloadInfo}***
EncryptedDownloadInfo	E_{SSK} (***{FileDownloadInfo}*+, *DownloadURL*)**
FileDownloadInfo	***{FileName, ContentKey}***
FileName (variable length)	Null-terminated string representing the name of the file to be downloaded.
ContentKey (16 bytes)	Decryption key of the relevant file ($K_{content}$)

CONFIRMATION COPY
Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0313
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

DownloadURL (variable length)	Null-terminated string representing the URL at which the requester can download the bought files.

Table 12

It should be noted that upon receipt of this message, the requester should verify that the number of received downloaded information correspond to the number of bought files.

13. *Download* operation 13:

Once the requester receives the *DownloadInfo* message 12, he/she can begin the download phase 13.

Table 13 bellow illustrates the content format downloaded by the requester. As underlined previously, this content is encrypted preventing thus eavesdropping.

Fields of message	Description of the fields
***ContentDownload* format**	***{EncryptedContent}***
EncryptedContent	$E_{K_{content}}$ ***(CheckableContent)***
CheckableContent	***{HashedContent, Content}***
HashedContent (20 bytes)	Hash value of the *Content* field. This will be used to check that the content has been downloaded without any transmission problem.
Content (variable length)	Bought bitstream.

Table 13

We will now describe the preferred method to provide responders with their compensation for the distribution of digital content through the sharing network. Indeed, each time a content which has been distributed by a responder is bought by a requester, the responder should receive a corresponding payment from the central authority.

As previously stated, all responders who distribute digital contents through the sharing network must be registered with at least one central authority in order to receive compensation for this distribution. A same responder can be registered with several central authorities if he/she proposes copyrighted contents created by different content providers which are not linked to the same central authority.

In the preferred method for paying responders, it is proposed to create an account for each responder during the registration phase, this account being linked to the responder identifier. During the registration, the responder gives to the central authority all personal data (name, address, bank account number, etc.) needed by the central authority to perform account clearing. Then, on a regular basis, the central authority with which the responder is registered performs an account clearing resulting

CONFIRMATION COPY
Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0314
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

in the payment of the responder. The clearing method should be negotiated between the central authority and the responder during the registration phase, and is out of scope of the invention.

During the purchase of a copyrighted content, the central authority credits the responder's account once it receives the *Negotiation* message of the financial transaction 9. As underlined in section 9 above, this message contains the responder identifier, which has been delivered by the central authority. The central authority has thus all needed data to pay the responder.

An alternative solution would consist for the responder to present the *PaymentTicket* message data received from the requesters (in *FwdPaymentTicket* messages 11) to the central authority for being paid. Once the responder receives *PaymentTicket* message data, he/she stores it as a proof of selling. On the other side, the central authorities store all generated *PaymentTicket* messages. Then, the responder presents these messages to each central authority, which can verify the validity of the message before performing an online financial transaction with the responder.

CONFIRMATION COPY

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0315
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

CLAIMS

1. System for distributing a digital content to a requester (200) through a sharing network (110), characterized in that it comprises:

a central authority (201 – 204) ;

a responder (300), registered with said central authority, having means for distributing a data file corresponding to said content to said requester (200) in exchange of a proof of buying (11) received from said requester ;

wherein said central authority comprises :

- means for establishing a financial transaction (9) with said requester for the payment by the requester of the content proposed by said responder and for delivering the proof of buying (10) to said requester; and

- a responder compensation means for providing said responder with a compensation in exchange of the buying of a content by a requester.

2. Method for distributing a digital content through a sharing network (110) using the system according to claim 1, characterized in that it comprises the steps consisting for a responder (300) in:

a) in response to a request (1) for a digital content received from a requester (200) through said sharing network, sending content purchase information data (4) to said requester ;

said content purchase information data including a responder identifier generated by a central authority (201 – 204) and data identifying said central authority ;

b) receiving from said requester (200) a proof of buying (11) of said digital content, said proof of buying being delivered by said central authority ;

c) providing said requester (200) with a data file corresponding to said digital content ; and

d) receiving from said central authority a compensation for the distribution of said digital content.

3. Method according to claim 2, further comprising before step a) a registration step comprising:

receiving from said central authority a responder identifier.

4. Method according to claim 3, wherein said registration step further comprises:

CONFIRMATION COPY

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0316
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

receiving from said central authority a first symmetric encryption key (DK_{PR}) derived from a first central authority master key (MK_{PR}) and from said responder identifier.

5. Method according to claim 4, wherein said registration step further comprises:

receiving from said central authority a second symmetric encryption key (DK_{EC}) derived from a second central authority master key (MK_{EC}) and from said responder identifier.

6. Method for distributing a digital content through a sharing network (110) using the system according to claim 1, characterized in that it comprises the steps consisting for a requester (200) in:

i) sending through said sharing network a first message (1) to request a digital content ;

j) receiving content purchase information data (4) from a responder having a data file corresponding to said content ;

said content purchase information data including data identifying a central authority ;

k) in response to a financial transaction (9) with said central authority, receiving a proof of buying (10) of said digital content ;

l) sending said proof of buying to said responder (300) ; and

m) receiving a data file corresponding to said digital content.

7. Method according to claims 2 or 6, wherein said content purchase information data comprises content price data (3) received by said responder from said central authority, said content price data being determined by the central authority for each responder.

8. Method according to claim 7, wherein said content purchase information data further comprises a price time validity data.

9. Method according to claim 4, wherein said content purchase information data comprises content price data (3) received by said responder from said central authority, said content price data being determined by the central authority for each responder,

and wherein said content price data are sent in a message (3) encrypted using said first symmetric encryption key (DK_{PR}).

CONFIRMATION COPY

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0317
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

10. Method according to claim 5, wherein said proof of buying is sent in a message (11) encrypted using a symmetric session key (SSK),

said symmetric session key (SSK) being derived by the central authority from a random value and from said second symmetric encryption key (DK_{EC}) ,

said random value being sent in clear in the message (11) containing said encrypted proof of buying.

CONFIRMATION COPY
Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0318
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

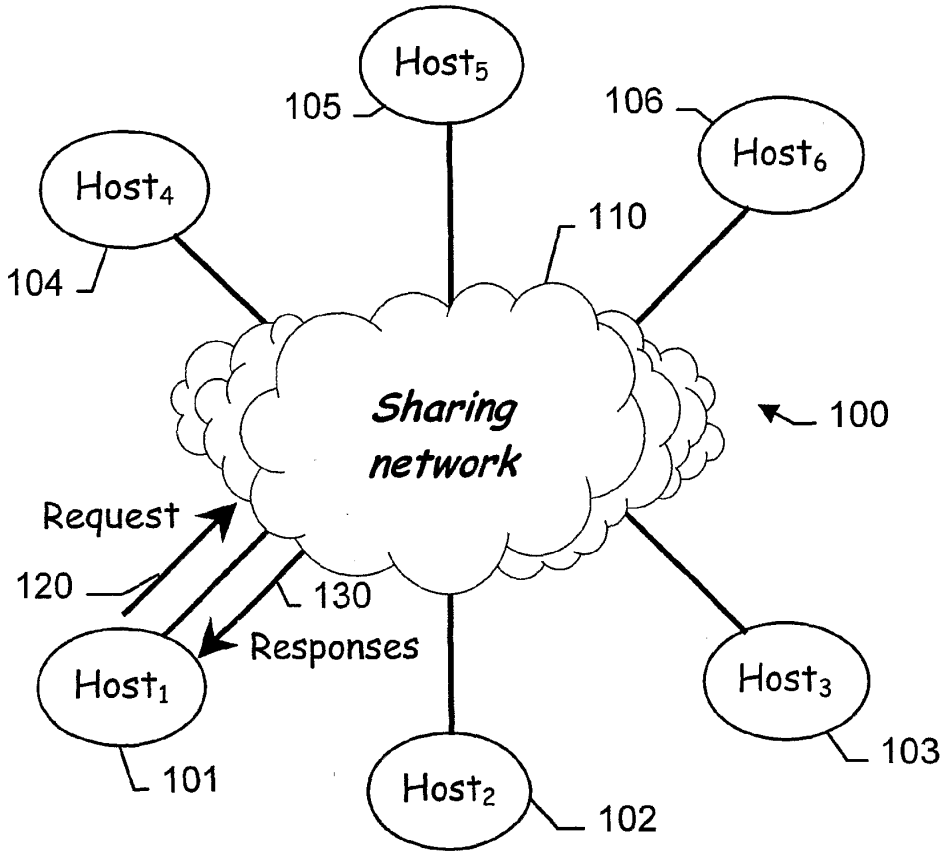


Fig. 1

CONFIRMATION COPY

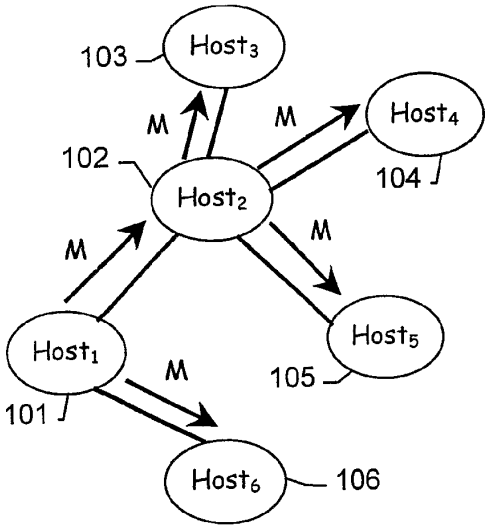


Fig. 2a

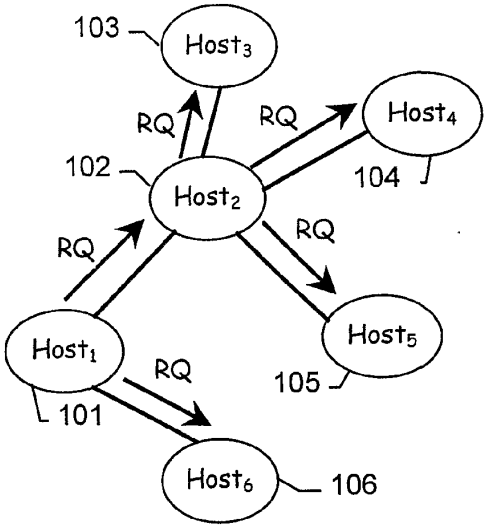


Fig. 2b

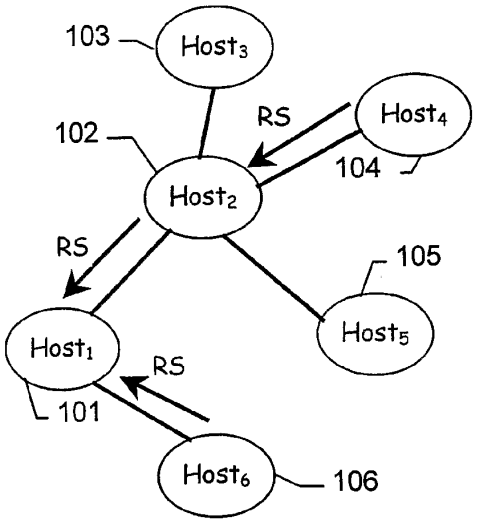


Fig. 2c

CONFIRMATION COPY

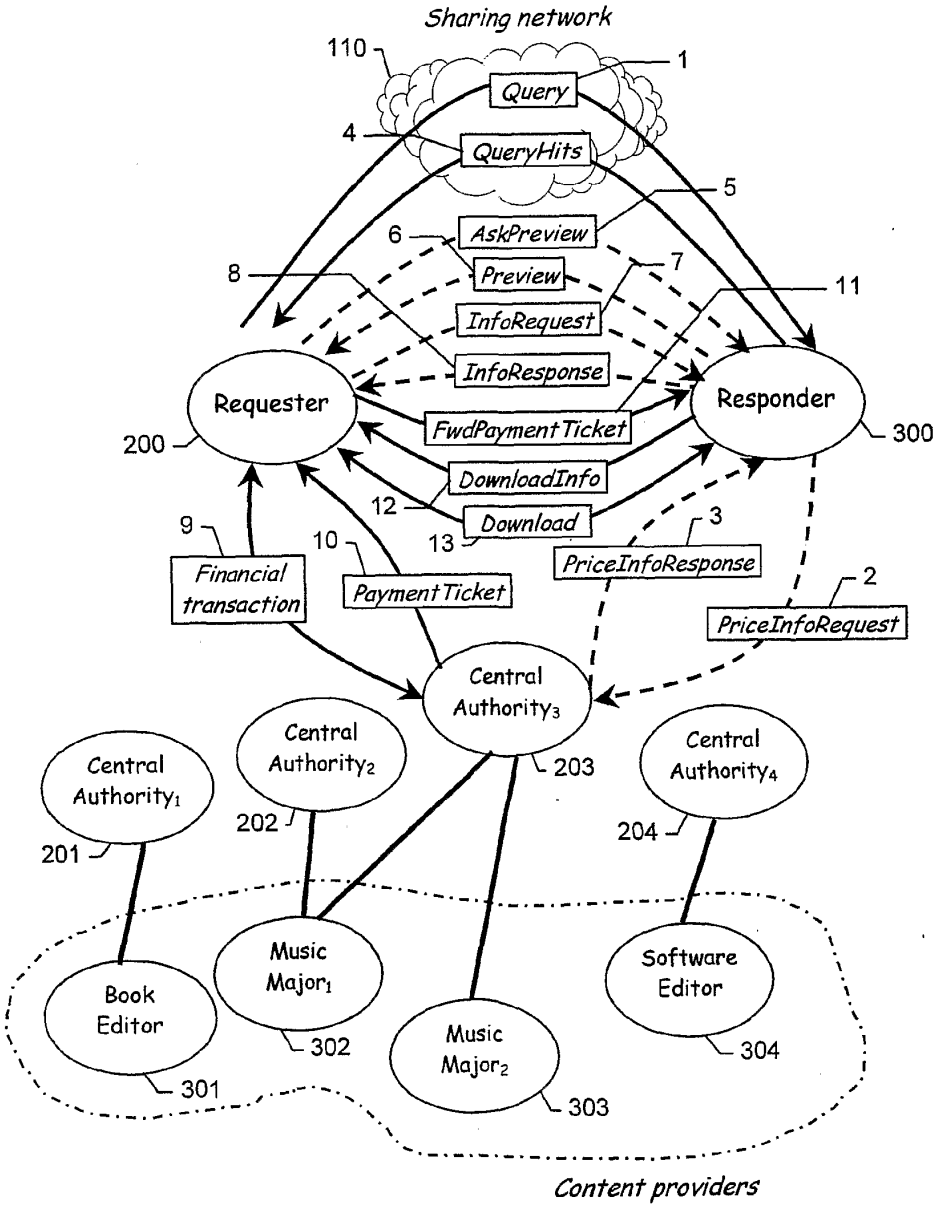


Fig. 3

CONFIRMATION COPY

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 November 2004 (25.11.2004)

PCT

(10) International Publication Number
WO 2004/102571 A1

(51) International Patent Classification[7]: G11B 27/32, 27/10, H04N 5/783, 7/173

(21) International Application Number: PCT/IB2004/050646

(22) International Filing Date: 12 May 2004 (12.05.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
03101371.7 16 May 2003 (16.05.2003) EP

(71) Applicant *(for all designated States except US)*: **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **RIJCKAERT, Albert, M., A.** [NL/NL]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: **GROENENDAAL, Antonius, W., M.**; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

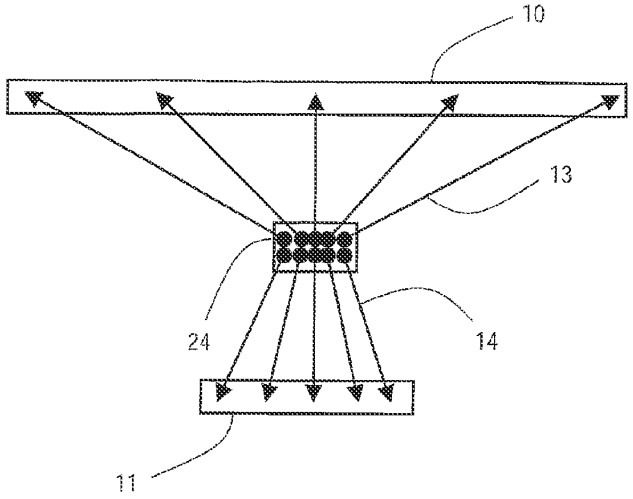
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ,*

[Continued on next page]

(54) Title: METHOD OF RECORDING AND OF REPLAYING AND VIDEO RECORDING AND REPLAY SYSTEMS



(57) Abstract: A video stream and different trickplay versions of that stream are stored as separate files in a randomly accessible storage medium. In order to facilitate seamless switching between streams linking information is provided, which links positions of content within the normal play stream to positions of corresponding content within the trickplay streams. Upon receiving a switch command for switching between trickplay modes or to or from a normal play mode the linking information is consulted to determine corresponding locations in different streams for the different modes and used to jump to a point within the new stream.

WO 2004/102571 A1

CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

Published:

— *with international search report*

---- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

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

METHOD OF RECORDING AND OF REPLAYING AND VIDEO RECORDING AND REPLAY SYSTEMS

The invention is related to recording and replaying video information from randomly accessible storage devices, such as discs. In particular, the invention is related to configurations in which more than one process concurrently has access to a randomly accessible disc, e.g. via time slot multiplexing. Such configurations may be present in situations where video on demand services are offered. In this case a video replay system outputs several concurrent video streams, which are all read from the disc. In some situations the same video is even replayed for different users, which started the video at different times.

It is desired to extend the options of the above described video replay system to permit the individual user to switch between different replay modes, as in home video recorders. In normal play mode a video is replayed at a rate, which is in accordance with an original recording speed. In a trickplay mode the video is replayed at another rate, e.g. fast forward or in reverse.

In home video recorders trickplay modes like fast forward and reverse are implemented by spooling the magnetic tape in the desired direction and with the desired speed along the magnetic head and by reading video frames at preselected instants from the tape. Video frames that are used during normal replay are also used for trickplay, but dedicated video frames for trickplay may be provided as well, near the positions on the tape where corresponding normal play frames are recorded. If a user gives a command to switch to another replay mode during spooling, the direction and the speed of the magnetic tape are adjusted. The video recorder continues to replay the video in the newly selected mode. Thus it is possible to switch between different replay modes at arbitrary instants in response to user commands.

From US 6 453 115 a video replay system is known that employs randomly accessible memory to store a stream and uses tables with pointers referring to so-called I-frames in the video stream in order to support trick play. I-frames represent a part of the video information in MPEG coded video data. Trickplay streams are generated by jumping to selected I-frames and by reading them in arbitrary order. However, jumping to different disc locations for retrieving the selected I-frames places a severe demand on the access bandwidth of the disc, so that the number of processes that may read the disc is relatively small. This is

in particular the situation if all these processes run in a trickplay mode, such as fast forward or fast reverse.

It is an object of the invention to enable switching between different replay modes at arbitrary instants during replay of a video stream while reducing the amount of access bandwidth of the randomly accessible memory that is required for access. Therefore a method of recording a video stream according to the invention comprises the steps of receiving a video stream; generating from the video stream a normal play stream and a trickplay stream representing the normal play stream at a trickplay rate by selecting and arranging data from the normal play stream; storing normal play stream data and trickplay stream data as separately accessible files on at least one randomly accessible storage device; and providing linking information, which links the selected data from the normal play stream in the trickplay stream with corresponding data in the normal play stream.

By storing a normal play stream and a trickplay stream as separately accessible files, which can each by itself be played in the same way as a normal stream, memory access optimization strategies may be applied to video streams for different trick play modes individually, such as storing successive parts of a file in successive tracks and sectors. Methods of storing separate files and file storage optimization strategies are well known per se, for example for computer (PC) hard disks. Such strategies make it possible to reduce the access bandwidth demand to access the randomly accessible storage device. By providing separate files for different play modes including a normal play mode and one or more trickplay modes, trickplay will not lead to a higher bandwidth use. As a result, more users can be connected to the video replay system, or more access bandwidth requiring operations can be performed on the at least one randomly accessible storage device. By providing linking information which links trickplay stream data with normal play stream data, the system is enabled to switch virtually seamlessly from the normal play mode to the trickplay mode, and vice versa. Storing the normal play stream and the trickplay stream as separately accessible files is also advantageous when the trickplay stream is generated and stored in semi real time from the normal play stream, i.e. when the generation of the trickplay stream takes place in a non-instantaneous way while the normal play stream is recorded.

The invention is also related to a method of replaying a video stream which comprises the steps of providing a randomly accessible memory on which normal play stream data and trickplay stream data are stored as separately accessible files, the trickplay

stream data representing the normal play stream data at a trickplay rate, being selected and arranged from the normal play stream, providing linking information, which links the selected data from the normal play stream in the trickplay stream with corresponding data in the normal play stream; retrieving one of a plurality of play stream data from the at least one randomly accessible storage device; generating part of a video stream from the retrieved play stream data; receiving a switch signal during replay of the generated part of the video stream, the switch signal representing a new play mode; reading the linking information; determining by means of the linking information a first position in the play stream according to the new play mode, the position corresponding to a second position in the part of the video stream that is displayed at the moment on which the switch signal is received; retrieving new play stream data from the at least one randomly accessible storage device according to the new play mode, starting with data related to the determined first position; and generating a new video stream from the retrieved new play stream data.

During replay a controller, which is provided on a video replay system, retrieves a play stream and generates a video stream according to a received signal representing a play mode. As an example, if an individual user selects a normal play mode, the controller generates a video stream by retrieving normal play stream data from a first file. If a user wants to switch to another, new replay mode at an arbitrary instant during replay of the video, he or she generates a signal representing the new play mode by communicating via an interface terminal. The controller receives this signal and retrieves new play stream data from a separate, second file, according to the new play mode. This is accomplished by starting with new data forming the new stream and corresponding to data at the position in the generated video stream according to the previously play mode where the switch occurred. Correspondence of these data is available, since linking information is provided during the record of the video stream. Again, as an example, if the user selects a trickplay mode during replay of the video, the controller retrieves trickplay stream data, starting from a position in the stream that corresponds to the present position in the normal play stream data. Due to the provided linking information which links corresponding image representation data, the controller is able to perform this operation. Then, the controller generates a new video stream from the retrieved new play stream data for replay at a replay terminal.

Thus the invention enables a video system offering video on demand services, to replay several videos for different users, and to switch each video stream from normal play mode to a trickplay mode and vice versa upon request of an individual user.

Other embodiments according to the invention are expressed in the dependent claims.

The objects and the advantages of the invention will be illustrated using exemplary embodiments shown in the drawing. In the drawing shows:

Fig. 1 a video recording system according to the invention;

Fig. 2 a flowchart representing a method of recording a video stream;

Fig. 3 a video replay system according to the invention;

Fig. 4 a flowchart representing a method of replaying a video stream;

Fig. 5 a scheme of video stream data according to the invention;

Fig. 6 a scheme according to Fig. 5 showing a table with pointers;

Fig. 7 a scheme of replaying a video using different play modes according to the invention; and

Fig. 8 a scheme according to Fig. 5 showing pointers in the video stream data.

In Fig. 1 a video recording system 1 is shown. The system 1 comprises a controller 2, which is connected to an input terminal 3, and a randomly accessible storage device 4, such as a disc. The disc 4 may comprise a magnetic disc, CD, or DVD. The controller 2 is also connected to a further memory device 6 comprising a table with linking information.

A flow chart of the recording process is shown in Fig. 2. In use, as a first step 30 the video recording system 1 receives the video stream data via the input terminal 3. In one embodiment the video stream is encoded, e.g. by means of an MPEG coding algorithm in order to save memory space, or even encrypted to prevent unauthorized access. In a second step 31 controller 2 generates a trickplay stream data from the received video stream. In a third step of the recording method, the controller 2 controls a storage process of data on the disc 4. More particularly at least two kinds of video stream data are stored as separately accessible file on the at least one disc 4, viz. as a file for normal play stream data and another file for trickplay stream data.

The normal play stream data represent the video data for replaying in a normal play mode, at a realistic rate, i.e. a rate that is in accordance with an original recording rate. The normal stream may be a copy of the received video data, or may be newly generated (for

example compressed and/or encrypted) by controller 2. The trickplay stream data generated by controller 2 represent the same video data as normal play stream data, but so that upon normal replay of this trickplay stream a trickplay effect occurs as compared with the normal stream, such as fast forward or fast reverse. Controller 2 generates trickplay stream data by selecting and arranging data from the normal play stream. In this way information from the normal play stream is extracted to form the trickplay stream. Preferably controller 2 compresses and/or encrypts the trickplay stream data before storage.

During the storing process, as a fourth step 33, the controller 2 writes linking data in a table that is stored in the further memory device 6. The table comprises linking information with respect to the video stream as will be explained below. Although a separate further memory device is shown, it will be appreciated that the table may also be stored on the same disc 4 as the streams (optionally as a table part, or distributed table parts in one or more of the streams), or that copies may be stored at multiple locations. In the fifth step 34, the processor checks if more video data is to be recorded. In that case the process continues with the first step 30. Otherwise, the controller awaits for the next video information.

In Fig. 3 a video replay system 7 is shown. The replay system 7 comprises partly the same elements as the video recording system 1. The controller 2 provided on the replay system 7 is connected to the disc 4 and to the further memory device 6. The controller 2 is further connected to a set of output terminals 8, which are all connectable to both a replay terminal 9 and an interface terminal 23. Each output terminal 8 interacts with an individual user via the replay terminal 9 and the interface terminal 23. Hence, the video replay system 7 is dedicated for video on demand (VOD) services for multiple users.

Fig. 4 schematically shows a flow chart of the method of replaying video streams by means of the video replay system 7. In a first step 35, a user selects a program, e.g. a film. The user communicates with the controller 2 via the interface terminal 23 and the output terminal 8. Upon selection of the program replay system 7 automatically selects a current play mode, preferably the normal play mode, for replaying the selected program. If desired, the user may command selection of another current play mode, e.g. trickplay mode at this time.

As a second step 36, the controller 2 retrieves from the disc 4 one or more frames from the video file that corresponds to the selected program in the current play mode. When the current play mode is the normal play mode, for example, frames from the file for normal play stream data are retrieved. In a third step 37 the controller generates a segment of a video stream from the retrieved frames for replay on the replay terminal 9 of the user. In the

fourth step 38 the user is enabled to select another play mode. If no selection is carried out, the replay process is continued from the same file returning to the second step 36.

If the controller 2 receives a switch signal representing a selection by the user of a new play mode via the above described communication chain 8, 23, the video replay system 7 will change the current play mode to the newly selected replay mode and start replaying the selected program in the new replay mode, e.g. a trickplay mode. Replay system 7 accomplishes this by retrieving frames for the new play stream data from another file, selected according to the new play mode in second step 36 and generating a new, second video stream from the retrieved new play stream data in third step 37, and outputting the new video stream to the output terminal 8.

In step 39, prior to executing from second step 36 for the newly selected replay mode, controller 2 reads the linking information that has been provided during the storing process described with reference to Fig. 2. The linking information may be read from disc 4 (optionally as a table from one of the streams, or as successive instalments of the table from an ongoing stream, or from a memory into which the linking information may be copied from disc 4, initially when play of the stream is started, or into which the linking information has been written during recording. In step 40, the controller 2 determines the position in the play stream data file for the newly selected play mode, which corresponds to the position in the play stream data file to which display had advanced during replay in the previous play mode.

After the controller 2 has determined the position in the play stream data file for the new play mode the process continues with the second step 36 and 37, i.e. retrieving video data from the newly selected video file, and generating a new video stream starting from the position that has been determined. Thus the controller 2 jumps from a first selected file to a new, second selected file, at a position that contains content that corresponds to the content in the original file, following the position to which display had advanced at the time of the switch.

Fig. 5 illustrates linking information. Fig. 5 schematically shows the normal replay stream 10 and two trickplay streams 11, 15. For particular positions in video streams the table comprises address information concerning data in the play streams that correspond to the particular positions. In a particular embodiment according to the invention the table may be represented as in table I

Table 1 Linking information

	position 1	position 2	position 3
stream 1	address 1	address1a	address1b
stream 2	address 2	address2a	...
stream 3	address 3	...	...
...	...	...	...

Hence, during the recording stage, address information of corresponding data in at least the normal play stream and at least one trickplay stream is stored in the table 24 as is indicated in Figure 6 with respect to the normal play stream 10 and one trickplay stream 11 for particular positions in a particular video stream. The address information, which is also called linking information, may also concern data from a second trickplay stream or from even more trickplay streams. The address information specifies addresses in the files for different play modes that contain corresponding content from the stream. By means of the linking information, the controller 2 is enabled to interconnect data in different video play streams of one particular video. In other words, corresponding data in different play streams 10,11 are interconnected by means of linking information 12 which is stored in the table during the recording process.

In particular, the address information contained in the table may point to memory locations in the files where sections of streams have been stored that represent the same frame or frames, e.g. an I-frame or groups of pictures (GOPs) in MPEG coded video which are represented as file packet numbers. The use of addresses of I-frames has the advantage that the image can immediately be replayed without retrieving data from other frames. In essence, the linking information of the table 24 comprise pointers 13, 14 referring to the sections.

Instead of pointing directly to memory corresponding locations in files, the linking information may also contain information that is sufficient to compute corresponding locations. A location of content x may be computed for example using a formula $L(x)=L0+R*x$ in case of a fixed compression rate stream. R, the replay rate is known for each stream. When L0 values are provided for each stream corresponding locations can be computed. Preferably, a plurality of L0 values is provided each for a respective section in the stream to permit more accurate computations. This works well for streams that use fixed rate compression (for example for part of the streams) but not for streams that use variable rate compression. In the latter case more L0 values may be provided for different sections of the

stream, together with local R values. Even if this does not provide accurate locations, it may be used to speed the search for the correct location, using PCR values for example. A similar technique may be used to compute corresponding PCR values in different streams.

The linking information may be stored as a separate table, or as a table part of one or more of the streams. The table for the whole stream need not be provided as a single table, but instead successive instalments of the table may be included in the stream, each for switching to another mode during a subsequent part of the stream. From the MPEG standard, for example, several techniques for including tables in a stream for other purposes are known, similar techniques may be used for including tables for switching between trickplay modes and a normal mode. In this case, instalments of the table are preferably loaded into a working memory each time when they are encountered.

If the video replay system 7 switches from a first play mode to a second play mode, the controller 2 searches in the table 24 for a position in the first play stream, also called reference point, which is close to a section 26 of the first play stream that represents an image which is replayed just before switching the play mode.

There are several ways of finding such a reference point in the first play stream. In one embodiment the controller 2 selects the reference point in the table 24, which corresponds to the address of the most recently replayed section 26 in the video stream before the switch. In another embodiment the controller 2 selects the reference point in the table 24 corresponding to the address of the section 26 next to the switch. In yet another embodiment the controller 2 selects the reference point in the table 24 which corresponds to the address of the section 26 which is chronologically most near the moment in the video stream at which the switch occurs. When the reference point in the table 24 has been selected, the pointer 13,14 relating to the play stream data 10, 11, 15 according to the second play mode, provides address information for finding the desired section 26 in the stream that represents an image, which needs to be retrieved in order to continue the process of generating the video stream 37. In this way the controller 2 switches from a first replay mode to a second replay mode and vice versa.

Fig. 7 shows again the normal replay stream 10 and one trickplay stream 11. Further a switching path 22 is schematically shown, starting with video data in the normal replay stream data 10. In this situation the user has selected a first, normal replay mode. At a particular moment the controller 2 retrieves video data from the trickplay stream data 11 as a response to the user which selects a second, trickplay mode. After some time the user selects the normal mode again, and the controller continues to generate a new video stream by

retrieving video information from the normal playstream data 10. Each time a nearly seamless switch is performed through the use of linking information.

In other embodiments of the invention the linking information is implemented in the video streams and not in a separate table. One embodiment makes use of MPEG PCR information to realize linking. In MPEG coded video streams, program clock references (PCRs) synchronize the replay rate with respect to the recording rate. The normal play stream and the trickplay stream have different PCR time bases, due to the different replay rate or time direction of the video play mode.

In an embodiment the linking information is stored in the form of information about PCR values of positions with corresponding content in the normal stream and the trick play stream or streams. The information about such corresponding PCR values may be stored in the files for each stream, or only in a subset of the files, for example only in the file that contains the stream for normal play. Such linking information may be provided in the form of sets of corresponding PCR values stored at various positions in a video stream for a particular play mode, the PCR values in each set specifying the PCR values of corresponding content in video streams for the same program in different play modes. The corresponding PCR value in the stream in which the set is stored may be part of the set, or may be implied by the PCR value that corresponds to the position in the stream where the set is stored in the stream. The embodiment in which the file for the stream for each play mode contains information about corresponding PCR values in the streams for other play modes will be illustrated first.

During a switch from the trickplay mode to the normal play mode, while a section 43 of the trickplay stream 11 is replayed, the controller 2 determines a reference point near the section 43 according to a search algorithm, e.g. as described above. Next, the controller 2 determines the PCR time value of the reference point in the normal play stream 10, from information about the corresponding PCR value stored in the trickplay stream. Then the controller 2 searches in the normal play stream 10 until the corresponding PCR time value has been found. The search activities are symbolically illustrated in Fig. 8 by means of arrows 16, 17. Although a chronological search from the start of the stream is used, it should be understood that other types of search may be used, for example a binary search (reading a PCR from midway the file, determining whether it is above or below the required PCR, reading a PCR from midway the section in front of or behind the midway position, dependent on whether the required PCR is lower or higher respectively and so on) or an indexed search (using a table of locations in the stream for a number of PCR values, finding a location of a PCR nearest the required PCR values and searching the stream from there). When the PCR

time base in the normal play stream has been found, the controller 2 starts retrieving normal play stream data at a section 44 corresponding to PCR value, to generate a new video stream for replay. The switch from the trickplay mode to the normal play mode has been performed.

An advantage of providing linking information in the video stream rather than in a separate table is that the linking information in the video stream is more dynamic and invariant for the sequence of a decoding and a new encoding step.

A switch from the normal play mode to a trickplay mode is performed in a similar way. When a user commands for a switch during replay of a section 41 in the normal play stream, the controller 2 determines a reference point near the section 41, finds the corresponding PCR value in the trick play stream from linking information in the normal stream and searches in the trickplay stream for the PCR value, and starts retrieving trickplay stream data at a section 42 corresponding to the reference point. The search activities of the controller 2 are symbolically illustrated by means of arrows 18 and 19.

A switch from a first trickplay mode to a second trickplay mode is performed along the same lines as a switch from a trickplay mode to the normal play mode, provided that the controller 2 searches in the second trickplay stream data for the stored PCR time base in the normal play stream 10 to find the corresponding section 45 in the second trickplay stream data. The search activities of the controller 2 are symbolically illustrated by means of arrows 20 and 21.

In another embodiment, linking information that specifies corresponding PCR values of different streams may be stored in a selected streams only, for example in the normal play stream. In this case a switch to the new play stream from another stream at a specific PCR value in that other stream involves a search in the normal play stream for a location where the specific PCR value for the other stream is stored, retrieval of the corresponding PCR value for the new stream (this may implicit in the location where the specific PCR value is stored if the switch is to the normal stream) and replay from the new stream, starting from the new PCR value. When the linking information about corresponding PCR values is stored in a trick play stream only a similar procedure hold mutatis mutandis. The use of a fast play stream for this purpose may be advantageous in this case if the speed of the search for the corresponding PCR value is important.

The above described embodiments are particularly suited for applications using MPEG coded video streams. The embodiments permit constant bit rate (CBR) as well as variable bit rate (VBR) coding schemes.

In yet another embodiment according to the invention it is assumed that CBR encoding schemes have been applied to the video streams. The linking information that is stored during the record stage contains the total length of each of the normal play stream and of one or more trickplay streams. During a switch from a normal play mode to a trickplay mode the controller 2 computes from the relative position in the normal play stream, the relative position in the trickplay stream, using the linking information, e.g. as a fraction of the total length. Then the controller 2 continues with retrieving data and generating the new play stream. Switching from a trickplay mode to the normal play mode or to another trickplay mode occurs also by means of computing relative positions in the play streams.

In another embodiment the controller 2 computes a relative time position in a normal play stream using the total time period of the stream which has been stored during a recording process as linking information, and the current PCR time base corresponding with a section which is currently replayed. For performing a switch from the normal play mode to a trickplay mode, the controller 2 determines from the relative time positions a relative file position in the trickplay stream, assuming the trickplay stream is coded with CBR schemes. This method is suited for application when the normal play stream is coded using VBR algorithms.

In yet another embodiment the controller 2 computes a relative file position in a trickplay stream from which new video data is to be retrieved, by using the total time period of the normal play stream being currently replayed, the total time period of the trickplay stream, and the current PCR time base corresponding with a section which is currently replayed. If a stored normal play stream PCR time base in the determined relative file position in the new play stream does not match with the section in the normal play stream, the controller 2 preferably performs a new iteration step, e.g. by linearization using the packet numbers in the normal play stream and trickplay stream, respectively, and the stored normal play stream PCR time base in the trickplay stream.

The invention is not restricted to the described embodiments. Many alternative video systems replaying video streams by means of linking information are possible.

It is noted that the sections of streams that represent images do not necessary contain GOPs or I-frames. Also P-frames or B-frames are possible.

Further, the invention is not restricted to one disc 4. The video recording system and/or the video replay system may comprise two or more discs on which normal play stream data files and trickplay stream data files are stored. In a preferred embodiment, normal play stream data and trickplay stream data are stored on different discs in order to

reduce access bandwidth of the discs and/or reduce the switching time. Thus activities relating to both the normal play stream and the trickplay stream can be executed more or less simultaneously.

In another embodiment the video streams (the normal stream and the trickplay streams) may be recorded in encrypted form or encrypted during replay, to prevent illegal use of video data. In this case, the linking information is preferably provided so that it can be accessed without decrypting the stream. This makes it possible to switch quickly between encrypted streams for normal and trick mode replay. The controller generates a trickplay stream from the normal play stream which is either compressed or uncompressed.

Further, it is advantageous to construct trickplay streams using I-frames or GOPs from the normal play stream, since the replay of I-frames and GOPs do not need information of other frames in the stream. This is in particular the case if the normal play stream is compressed. The above-mentioned approach saves decompression time for the controller.

In an embodiment according to the invention a reverse trickplay stream is generated. This is accomplished by generating the reverse trickplay stream from a forward trickplay stream. In a preferred embodiment the reverse trickplay stream is generated off-line when the entire normal play stream has been stored on disc. This approach saves bandwidth of the storage device and adjustments of timing information in the stream. When the reverse trickplay stream is generated, linking information is also generated and stored, for use during replay.

These embodiments are assumed to be obvious for the man skilled in the art and are considered to fall within the scope of the following claims.

CLAIMS:

1. A method of recording a video stream, comprising the steps of
- receiving a video stream (10);
- generating a trickplay stream (11, 15) from the video stream, by selecting and arranging data from the video stream (10), the trick play stream (11, 15), when played at normal rate, representing the video stream at a trickplay rate;
- storing the trickplay stream (11, 15) and a normal play stream (10) corresponding to the video stream (10) as separately accessible files on at least one randomly accessible storage device (4); and
- providing linking information (12), which links positions of content within the normal play stream (10) to positions of corresponding content within the trickplay stream (11, 15).

2. A method of replaying a video stream, comprising the steps of
- providing a randomly accessible storage device (4) in which a normal play stream (10) and a trickplay stream (11, 15) are stored as separately accessible files, the trickplay stream (11, 15) when played at normal rate representing the normal play stream (10) data at a trickplay rate;
- providing linking information (12), which links positions of content within the file for the normal play stream (10) to positions of corresponding content in the file for the trickplay stream (11, 15);
- replaying a part of a play stream (10, 11, 15) from one of the files in the at least one randomly accessible storage device (4);
- receiving a switch signal during replay of the part of the play stream (10, 11, 15), the switch signal for selecting a new play mode;
- reading the linking information (12);
- determining a first position in the file for the new play mode, the first position corresponding, according to the linking information (12), to a second position in the part of the play stream (10, 11, 15) that is replayed substantially at the time on which the switch signal is received;

- continuing replay with new play stream data from the file corresponding to the new play mode, starting with data determined by the first position.

3. A method of replaying according to Claim 2, wherein the normal stream and the trick play stream contain program clock references (PCR) for defining progress of time during play of the normal stream (10) and the trick play stream (11, 15) defined to respective time bases respectively, wherein the linking information specifies correspondence information items, each between program clock reference (PCR) values of corresponding positions in the respective streams (10, 11, 15), the method comprising retrieving a program clock reference (PCR) value for the first position from the linking information, and searching for the first position on the basis of the retrieved program clock reference value.

4. A method of replaying according to Claim 3, wherein the linking information is contained in and retrieved from the file that contains the play stream (10, 11, 15).

5. A method of replaying according to Claim 4 wherein the correspondence information items are stored in at least one of the files for the normal play stream (10) and the trick play stream (11, 15), each at a position substantially where the clock reference (PCR) value of the item assumes the value corresponding to the item.

6. A method of replaying a video stream according to claim 2, wherein the method further comprises the step of successively displaying video information decoded from the play stream (10, 11, 12) and the new play stream (10, 11, 12) on a display device.

7. A video recording system, comprising

- an input terminal (3) for receiving a video stream;
- at least one randomly accessible storage device (4);
- a controller (2) arranged to
  - generate a normal play stream (10) and the trickplay stream (11, 15) from the received video stream, the trickplay stream (11, 15) by selecting and arranging frames from the received video stream, so that the trickplay stream (11, 15) represents, when played at a normal rate, the normal play stream (10) at a trickplay rate

- store the normal play stream (10) and trickplay stream (11, 15), as separately accessible files in the randomly accessible storage device (4) and
- generate linking information (12) which links positions of content within the normal play stream (10) to positions of corresponding content within the trickplay stream (11, 15).

8. A video recording system according to Claim 7, wherein the normal stream (10) and the trick play stream (11, 15) contain program clock references (PCR) for defining progress of time during play of the normal stream (10) and the trick play stream (11, 15) defined to respective time bases respectively, the controller (2) being arranged to store linking information specifying correspondence information items, each between program clock reference values of corresponding positions in the respective streams.

9. A video recording system according to Claim 7 wherein the correspondence information items are stored in at least one of the files for the normal play stream and the trick play stream, each at a position substantially where the clock reference value of the item assumes the value corresponding to the item.

10. A video replay system, comprising

- at least one randomly accessible storage device (4) for storing a normal play stream (10) data and a trickplay stream (11, 15) in separately accessible files, the trickplay stream (11, 15), when played at normal rate, representing the normal play stream (10) at a trickplay rate;
- a controller (2) arranged to
- replay a part of a play stream (10, 11, 15) from one of the files in the at least one randomly accessible storage device (4);
- receive a switch signal during replay of the part of the play stream (10, 11, 15), the switch signal for selecting a new play mode;
- read the linking information which links positions of content within the normal play stream (10) to positions of corresponding content within the trickplay stream (11, 15);
- determine a first position in the file for the new play mode, the first position corresponding, according to the linking information, to a second position in the part of the play stream that is replayed substantially at the time on which the switch signal is received;

- continue replay with new play stream data from the file corresponding to the new play mode, starting with data determined by the first position.

11. A randomly accessible memory medium (4) comprising

- separate files that contain data representing a normal play stream (10) and a trickplay stream (11, 15) respectively, the trickplay stream (11, 15), when played at a normal rate, representing the normal play stream (10) at a trickplay rate, and
- linking information (12), which links positions of content within the normal play stream (10) to positions of corresponding content within the trickplay stream (11, 15).

12. A randomly accessible memory medium according to Claim 11, wherein the linking information comprises successive instalments of for successive parts of the streams (10, 11, 15) as tables in the streams (10, 11, 15).

13. A video play stream signal comprising successive instalments of linking information (12), which links positions of content within a normal play stream (10) to positions of corresponding content within one or more different trickplay versions (11, 15) of the video play stream.

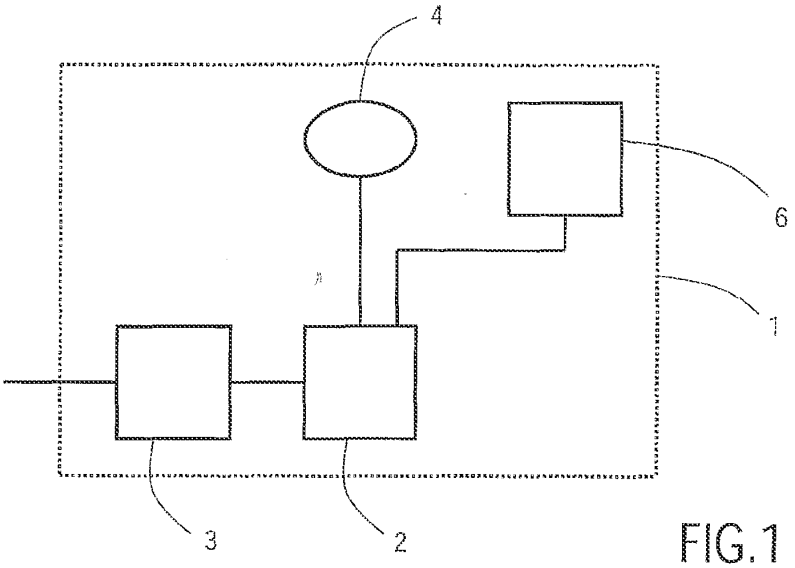


FIG.1

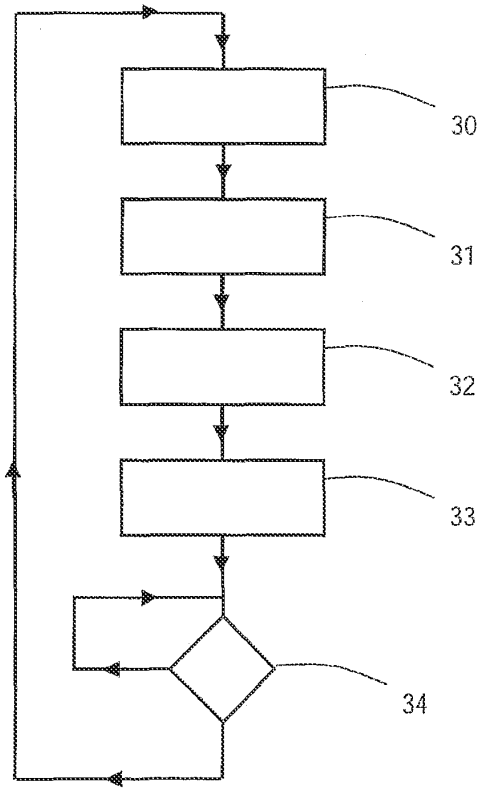


FIG.2

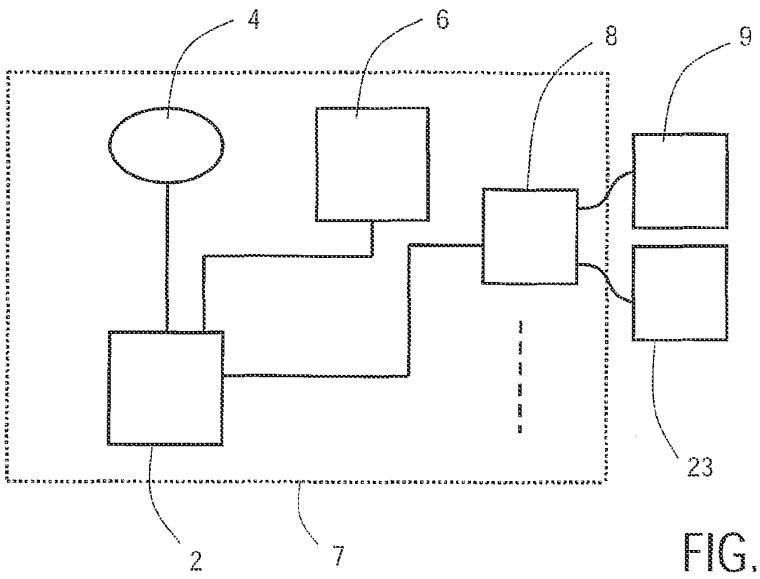


FIG.3

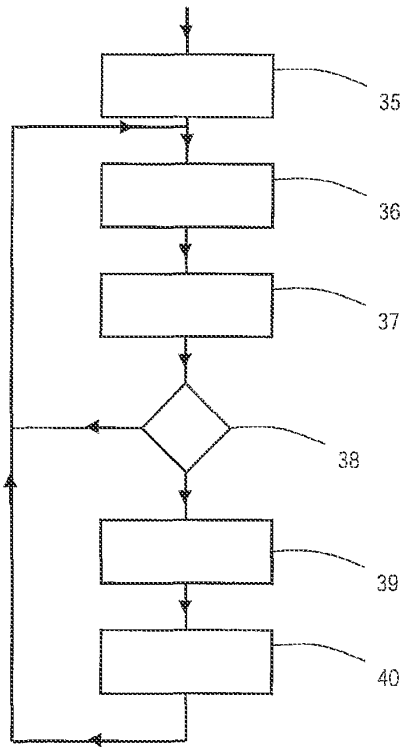


FIG.4

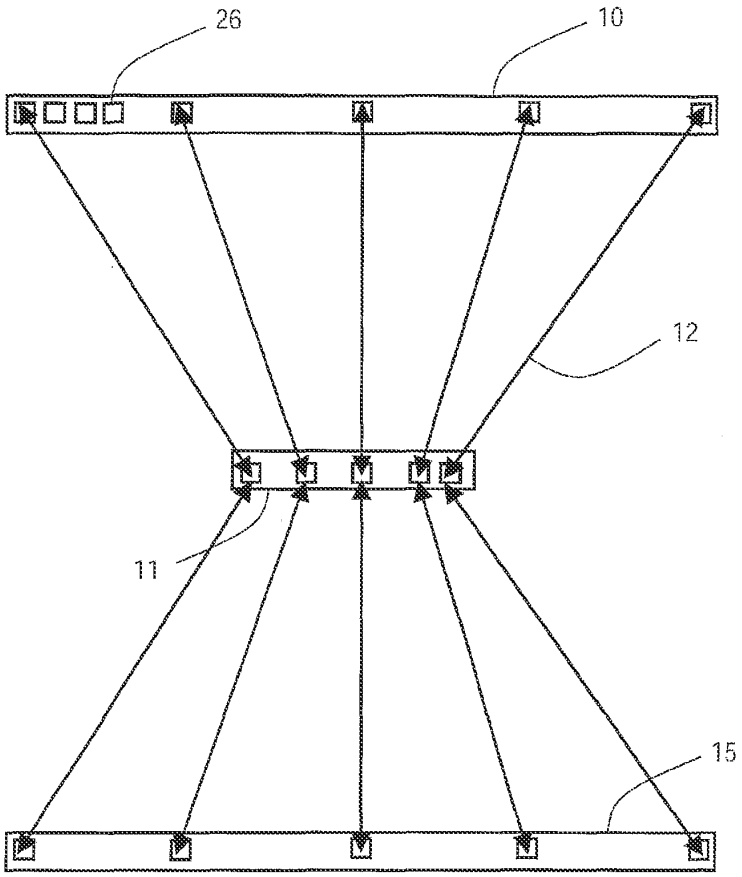


FIG.5

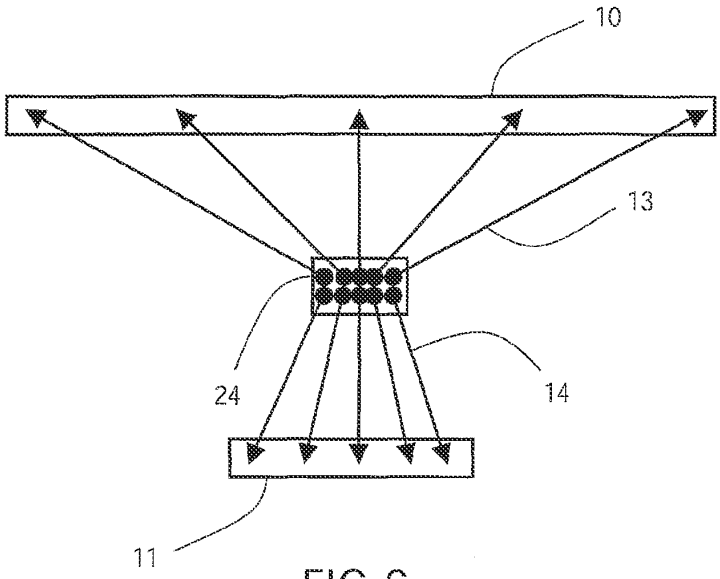


FIG.6

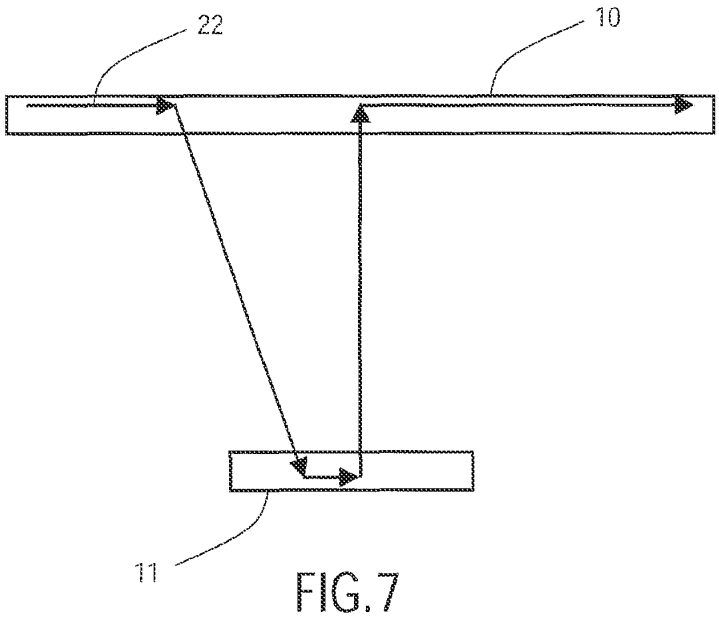


FIG.7

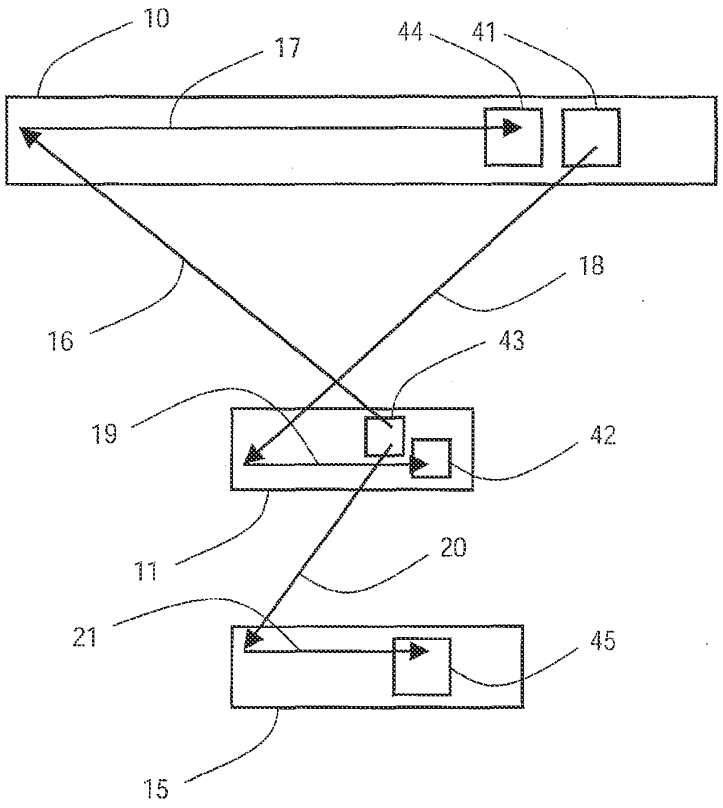


FIG.8

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB2004/050646

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G11B27/32 G11B27/10 H04N5/783 H04N7/173

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 7 G11B H04N

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 812 112 A (SUN MICROSYSTEMS INC) 10 December 1997 (1997-12-10) the whole document	1,2,6,7, 10-13
X	WO 02/35832 A (DAVENPORT WILLIAM; SEACHANGE INTERNATIONAL INC (US)) 2 May 2002 (2002-05-02) abstract page 5, line 9 - page 7, line 37 claims 25-30 figures 1-4	1,2,6,7, 10-13
Y	US 5 479 303 A (NISHIMURA KAZUTOSHI ET AL) 26 December 1995 (1995-12-26) the whole document	1,2,6,7, 10-13
Y	US 6 445 738 B1 (KAUBISCH WOLF-HASSO ET AL) 3 September 2002 (2002-09-03) the whole document	1,2,6,7, 10-13

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

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

"E" earlier document 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
29 July 2004	15/10/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax (+31–70) 340–3016	Sucher, R

2

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
T/IB2004/050646

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0812112 A	10-12-1997	US 6065050 A	16-05-2000
		DE 69727100 D1	12-02-2004
		EP 0812112 A2	10-12-1997
		JP 10075436 A	17-03-1998
WO 0235832 A	02-05-2002	AU 1169302 A	06-05-2002
		EP 1329101 A2	23-07-2003
		JP 2004515941 T	27-05-2004
		WO 0235832 A2	02-05-2002
US 5479303 A	26-12-1995	JP 2708683 B2	04-02-1998
		JP 6133262 A	13-05-1994
US 6445738 B1	03-09-2002	AU 2682297 A	12-11-1997
		CN 1220065 A	16-06-1999
		DE 69727372 D1	04-03-2004
		EP 0895694 A1	10-02-1999
		JP 2002511982 T	16-04-2002
		KR 2000010629 A	25-02-2000
		WO 9740623 A1	30-10-1997

Form PCT/ISA/210 (patent family annex) (January 2004)

WO 2004/084035 English translation of Japanese Patent Publication No. 2006-524007 (attached herewith)

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 September 2004 (30.09.2004)

PCT

(10) International Publication Number
WO 2004/084035 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number:
PCT/US2004/008202

(22) International Filing Date: 16 March 2004 (16.03.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/455,723 18 March 2003 (18.03.2003) US
10/760,642 20 January 2004 (20.01.2004) US

(71) Applicant (*for all designated States except US*): WIDEVINE TECHNOLOGIES, INC. [US/US]; 900 Fourth Avenue, Suite 3600, Seattle, WA 98164 (US).

(72) Inventors; and
(75) Inventor/Applicant (*for US only*): MORTEN, Glenn, A. [US/US]; 6035 133rd Avenue S.P., Bellevue, WA 98006 (US).

(74) Agents: BRANCH, John, W. et al.; Darby & Darby P.C., P.O. Box 5257, New York, NY 10150-5257 (US).

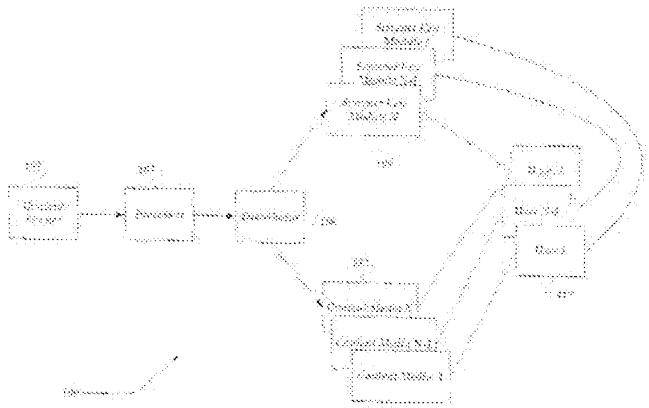
(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

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

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

(54) Title: SYSTEM, METHOD AND APPARATUS FOR SECURELY PROVIDING CONTENT VIEWABLE ON A SECURE DEVICE



(57) Abstract: A system, apparatus, and method are directed to providing and securely viewing secure content. In one embodiment, a secure player provides secure streaming/previewing of secure content, such as a motion picture, to a member of an awards organization. A content key is employed to selectively encrypt at least a portion of a content stream. The content key is encrypted with a screener key. The encrypted content key is embedded into the secure content. The screener key is encrypted using public/private key pair that is bound to the secure player. The secure content may be distributed on a medium, such as a DVD, high definition DVD, and the like. The secure player is configured to receive the medium, screener key, and a screener identity. The screener identity and screener key are employed by the secure player to decrypt and enable secure viewing of the content.

WO 2004/084035 A2

SYSTEM, METHOD, AND APPARATUS FOR SECURELY PROVIDING CONTENT VIEWABLE ON A SECURE DEVICE

Cross Reference To Related Applications

This application claims the benefit of U.S. Provisional Application Serial No. 60/455,723, filed March 18, 2003, the benefit of the earlier filing date of which is hereby claimed under 35 U.S.C. § 119 (e).

Field of the Invention

The present invention relates to data security, and more particularly, to a system, and method, and apparatus for providing and securely playing secure content.

Background of the Invention

Digital Versatile Discs (DVDs) are potentially the fastest growing and most rapidly adopted consumer electronics product of today. Interestingly, one of the main reasons that the DVD format is so innovative and attractive to consumers and the entertainment industry is exactly what makes it potentially vulnerable to illicit copying. Because DVDs store movies in a digital format that is perfectly reproducible every time movies are recorded and played on DVDs, for the first time one can view movies at home with crystal clarity and high quality audio. Additionally, the fact that the movies are stored digitally also means it is possible for movie companies, and others, to make virtually an infinite number of essentially perfect copies of DVD movies.

Such quality and ease of reproduction has made it extremely convenient for movie companies, for example, to send out thousands of pristine copies of first edition movies to members of the Academy of Motion Picture Arts and Sciences. These DVDs typically are intended to be viewed only by those individuals who vote for Oscars and other industry awards. However, many of the DVDs have fallen into unauthorized hands and have become the digital blueprint for bootleggers who have copied the DVDs and distributed them both online and in shops abroad. Many such

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0349
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

films then show up in pirated DVD form, and the like, shortly after their release into the theaters - and sometimes sooner. Since it is preferable to continue to use a high quality digital medium, such as DVDs, to distribute motion pictures, providing a relatively high level of security to protect the content is desirable. Unfortunately, the illicit copies are of such high quality that movie companies, and the like often lose millions of dollars as a result. In addition, many other content owners in the entertainment industry remain reluctant to provide content on DVDs until such content protection is available. Therefore, it is with respect to these considerations and others that the present invention has been made.

Brief Description of the Drawings

Non-limiting and non-exhaustive embodiments of the present invention are described with reference to the following drawings. In the drawings, like reference numerals refer to like parts throughout the various figures unless otherwise specified.

For a better understanding of the present invention, reference will be made to the following Detailed Description of the Preferred Embodiment, which is to be read in association with the accompanying drawings, wherein:

FIGURE 1 illustrates an exemplary environment in which the present invention may be practiced;

FIGURE 2 illustrates a block diagram of an exemplary apparatus for enabling the viewing of secure content;

FIGURE 3 illustrates one embodiment of a content stream for providing secure content;

FIGURE 4 illustrates a flow diagram generally showing one embodiment for an end-to-end process of providing and viewing secure content;

FIGURE 5 illustrates a flow diagram generally showing one embodiment for a process of generating secure content; and

FIGURE 6A-6B illustrate a flow diagram generally showing one embodiment for a process of viewing secure content, in accordance with the present invention.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0350
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Detailed Description of the Preferred Embodiment

In the following detailed description of exemplary embodiments of the invention, reference is made to the accompanied drawings, which form a part hereof, and which is shown by way of illustration, specific exemplary embodiments of which the invention may be practiced. Each embodiment is described in sufficient detail to enable those skilled in the art to practice the invention, and it is to be understood that other embodiments may be utilized, and other changes may be made, without departing from the spirit or scope of the present invention. The following detailed description is, therefore, not to be taken in a limiting sense, and the scope of the present invention is defined only by the appended claims.

Throughout the specification and claims, the following terms take the meanings explicitly associated herein, unless the context clearly dictates otherwise.

The terms "coupled," and "connected," includes a direct connection between the things that are connected, or an indirect connection through one or more either passive or active intermediary devices or components.

The term "screener," includes media content, and the like, that is to be viewed/screened, and otherwise enjoyed by a user, member of an awards organization, and the like. The term "screener" may also include a content media, such as a DVD, high definition formatted DVD, and the like.

The meaning of "a," "an," and "the" include plural references. The meaning of "in" includes "in" and "on."

Briefly stated, the present invention is directed to a system, apparatus, and method for securely providing secure content viewable on a secure player by a selected user. In one embodiment, the secure player is configured to receive a computer readable medium, such as a DVD. However, the invention is not limited to DVDs. For example, it is envisioned that the invention may be configured to securely provide and view secure content on other mediums, including but not limited to high quality digital media, such as High Definition DVDs, and the like.

Illustrative Environment

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0351
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

FIGURE 1 is a functional block diagram illustrating an exemplary operating environment 100 in which the invention may be implemented. Operating environment 100 is only one example of a suitable operating environment and is not intended to suggest any limitation as to the scope of use or functionality of the present invention. Thus, other well-known environments and configurations may be employed without departing from the scope or spirit of the present invention.

As shown in the figure, operating environment 100 includes content owner 102, processor 104, distributor 106, screener key module(s) 108 (1 through N), content media 112 (1 through N), and user(s) 114 (1 through N). Processor 104 is in communication with content owner 102 and distributor 106. Distributor 106 is also in communication with screener key module(s) 108 (1 through N) and content media 112 (1 through N). User(s) 114 (1 through N) are also in communication with screener key module(s) 108 (1 through N) and content media 112 (1 through N).

Content owner 102 includes producers, developers, and owners of media content that can be distributed to user(s) 114. Such content, sometimes called screeners, includes motion pictures, movies, videos, and the like. However, content owned by content owner 102 is not limited to video content only, and may include audio only services, without departing from the scope or spirit of the present invention. Thus, content is intended to include, but is not limited to, audio, video, still images, text, graphics, and other forms of content (screeners) directed towards user(s) 114.

Processor 104 receives content from content owner 102, selectively secures at least a portion of that content, and provides the secured content to distributor 106, as described in more detail below in conjunction with FIGURE 5. Briefly, however, processor 104 creates and embeds in a stream of the received content, selected information, such as a content key for decryption, a content identifier, access constraints, rights, entitlements, and the like. In one embodiment, the selected information is packaged into at least one key package (not shown), each of which is encrypted employing at least one screener key. In another embodiment, each content key is encrypted employing at least one screener key. In one embodiment, the content identifier may be left in the clear.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0352
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

The screener key(s) may be generated using any of a variety of encryption/decryption symmetric key mechanisms, including, but not limited to RSA algorithms, Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Skipjack, RC4, Advanced Encryption Standard (AES), and the like. In one embodiment, the screener key(s) employ a 256-bit AES algorithm for the encryption/decryption of the key package. However, screener key(s) are not limited to symmetric key mechanisms, and asymmetric key mechanisms may also be employed without departing from the scope or spirit of the present invention.

Processor 104 may obtain the screener key(s) and content key(s) from a variety of sources, including, but not limited to, content owner 102, a trusted third party, and the like. Processor 104 may also generate the screener key(s) and/or content key(s) itself. Moreover, the screener keys may reside within a key storage (not shown). Each screener key may be indexed in the key storage by a content identifier that is associated with particular content. The key storage may further include access constraints, rights, and the like, associated with a user, content, a targeted secure player, any combination of user, content, and targeted secure player, and the like.

Distributor 106 includes businesses, systems, and the like that obtain rights from content owner 102 to copy and distribute the secure content. Distributor 106 may obtain the rights to copy and distribute from one or more content owners. Distributor 106 may repackage, store, and schedule secure content for subsequent sale, distribution, and license to other distributors, user(s) 114, and the like, using content media 112.

Distributor 106 may copy the secure content onto a variety of content media 112, including, but not limited to a DVD, high definition DVD, Video Compact Disc (VCD), Super VCD (SVCD), Super Audio CD (SACD), and the like. For example, secure content may be copied and distributed on a Dynamic Digital Sound (DDS) content media. Moreover, distributor 106 may also copy and distribute secure content on a Read/Write DVD, CD-Recordable (CD-R), and substantially similar content media. Distributor 106 is not limited to copying and distributing secure content

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0353
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

on DVD and CD content media technologies, and virtually any other content media technology may be employed without departing from the scope of the present invention.

Distributor 106 may receive one or more screener keys associated with the one or more key packages. Distributor 106 may also receive authorization information from a variety of trusted sources that indicate whether a user has authorization to access the secure content. Provided that the user does have authorization, distributor 106 may package the received screener key(s) into screener key module 108. Distributor 106 may also include in screener key module 108 a content identifier associated with the secure content, fulfillment rights, access constraints, attributes associated with a targeted secure player, and the like. For example, distributor 106 may include in screener key module 108 attributes that indicate that the secure content is not playable within a selected geographic region.

Distributor 106 may further encrypt the screener key(s), and additional information included on screener key module 108, with a public key associated with the targeted secure player. The targeted secure player's public key may be generated employing a variety of asymmetric encryption mechanisms, including, but not limited to, Diffie-Hellman, RSA, Merkle-Hellman, PGP, X.509, and the like.

In one embodiment, distributor 106 employs a 2048-bit RSA asymmetric (public/private) key associated with the targeted secure player to encrypt the screener key(s). In another embodiment, the public/private key pair associated with the targeted secure player is generated in a Federal Information Processing Standard (FIPS) level 4 device. However, the present invention is not so limited, and another security level may be employed to generate the targeted secure player's public/private key pair.

In any event, the targeted secure player's public key may be made available to distributor 106 through a variety of approaches, including a trusted third party, a network, email, and the like. Moreover, the targeted secure player's private/public keys are bound to the targeted secure player such that they are unique to that particular targeted secure player. Moreover, the targeted secure player is configured to prevent removal of the targeted secure player's private key. Such action further binds the targeted secure player's private key to the targeted secure player.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0354
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Distributor 106 may distribute screener key module 108 to user(s) 114 employing a variety of mechanisms, including, but not limited to, a smart card, PCMCIA card, a memory stick, over a network, DVD, CD, tape, floppy disc, and similar removable mechanisms. Screener key module 108 may also be mailed to user(s) 114.

User(s) 114 include end-users, consumers of content, and the like. User(s) 114 further include members of an awards organization, and the like, that receive content (screeners) for review. User(s) 114 may employ various devices to enjoy the content, including but not limited to television appliances, mobile device, PDAs, personal computers, jukeboxes, and the like. User(s) 114 may further employ the secure player described in more detail below in conjunction with FIGURE 2 to securely provide the content to the above devices.

User(s) 114 may request content media 112 directly from content owner 102, or at any point along a market stream (e.g., from distributor 106). Moreover, user(s) 114 may receive content media 112 through multiple content owners 102, distributors 106, and the like. User(s) 114 may further receive screener key module(s) 108 from content owner 102, distributor 106, and the like. User(s) 114 may also receive an identity module, described below in conjunction with FIGURE 2, that provides user authentication and authorization for access to the secure content. User(s) 114 may employ screener key module(s) 108, and the identity module, to view the secure content on content media 112.

FIGURE 2 illustrates a block diagram of an exemplary apparatus for enabling the viewing of secure content. Briefly, secure player 200 is configured to receive content media 112 and screener key module 108 of FIGURE 1, and an identity module, and to enable viewing of the secure content on content media 112. As such, secure player 200 may be employed by user(s) 114 within, or coupled to a television appliance, digital recorder, set-top-box, cellular phone, mobile device, PDA, personal computer, jukebox, hybrid Internet-music-player/home-stereo-component-system, and the like.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0355
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

As shown in FIGURE 2, secure player 200 may include many more components than those shown; however, those shown are sufficient to disclose an illustrative embodiment for practicing the invention.

As shown in the figure, secure player 200 includes media drive 202, media player subsystem 204, decryption engine 206, COmpressor/DECompressor (CODEC) 208, key store/manager 210, screener key module 108, key loader 214, identity module 216, authentication module 218, tamper agent 220, and (optional) analog copy protection device 222. Components numbered similarly to those in FIGURE 1 operate in a substantially similar manner.

Media player subsystem 204 is in communication with media drive 202 and decryption engine 206. Decryption engine 206 is also in communication with CODEC 208 and key store/manager 210. CODEC 208 is in communication with optional anticopy protection device 222. Key store/manager 210 is further in communication with key loader 214. Key loader 214 is in communication with screener key module 108 and authentication module 218. Authentication module 218 is also in communication with identity module 216. Tamper agent 220 is in communication with decryption engine 206, CODEC 208, key store/manager 210, media player subsystem 204, authentication module 218, and key loader 214.

Media drive 202 includes virtually any device and related software that is configured to receive content media 112 of FIGURE 1. Such devices include, but are not limited to, a DVD drive, high definition DVD drive, Super Video CD (SVCD) drive, VCD drive, Super Audio CD (SACD) drive, and other content media devices. For example, media drive 202 may also be Dynamic Digital Sound (DDS) drive. Moreover, media drive 202 may also support write capabilities, such as through a DVD/RW drive, and the like. Media drive 202 and media player subsystem 204 however, are not limited to DVD, and CD technologies, and virtually any other content media technology may be employed without departing from the scope of spirit of the present invention.

Media player subsystem 204 operates in conjunction with media drive 202 to take secure content from the content media supported by media drive 202, and

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0356
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

provide it to decryption engine 206. Moreover, media player subsystem 204 and media drive 202 may include the capabilities to enable content media to be erased, destroyed, written over, and the like. For example, media player subsystem 204 may enable the erasure, destruction, disablement, and the like, of the secure content on the content media after a predetermined number of viewings, e.g. a single viewing, indication of unauthorized activity, and the like.

CODEC 208 includes any of a variety of compression/decompression mechanisms configured to receive compressed content and decompress it into a format capable of being rendered for the user's enjoyment. For example, CODEC 208 may employ Moving Pictures Experts Group (MPEG), Joint Photographic Experts Group (JPEG), wavelets, and other mechanisms for compression and decompression of received content.

Key loader 214 is enabled to receive a request to retrieve a screener key from screener key module 108. Key loader 214 may evaluate the request to determine whether the user has sufficient authorization to retrieve the screener key. Key loader 214 may request such authorization from authentication module 218. Key loader 214 may provide authentication module 218 a content identifier, or other information as part of its request for authorization. Additionally, key loader 214 may receive a request to load one or more screener keys, and other information, onto screener key module 108. Again, key loader 214 may seek authorization for such action from authentication module 218.

Authentication module 218 is configured to authenticate a user and to provide authorized access to screener key module 108. Authentication module 218 may receive a request from key loader 214 to access a screener key residing on screener key module 108. Authentication module 218 may also receive a request to store information on screener key module 108. In any event, authentication module 218 employs identity module 216 to determine the user's identity and associated authorization for access to screener key module 108.

Identity module 216 is enabled to provide the identity of a user, and entitlements and rights associated with a content identifier, user, and the like. Identity

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0357
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

module 216 may be deployed using a variety of mechanisms, including, but not limited to, biometric, smart card, user name/password, touch-pad code entry, and the like. In one embodiment, identity module 216 is configured to enable virtually any user of secure player 200 to be authenticated to virtually any secure content.

Key store/manager 210 is configured to store and manage encryption/decryption keys, including screener keys, secure player 200's public/private keys, associated information, and the like. The associated information may include entitlements, rights, and the like, associated with at least one of a screener key, user, content, any combination of screener key, user, and content, and the like. Key store/manager 210 may include a database or flat data file, and the like, configured to store and manage the keys, and the associated information in a secure manner. Key store/manager 210 may employ content identifiers to index the screener keys and associated information.

Key store/manager 210 typically securely retains the secure player 200's private/public keys until decryption engine 206 requests them for decryption/encryption of a screener key. Key store/manager 210, however, is configured to ensure that the secure player's private key is not made available beyond use within secure player 200.

Key store/manager 210 securely stores received screener keys until decryption engine 206 requests them for decryption of encrypted content. Key store/manager 210 may retrieve a screener key from screener key module 108 by making a request to key loader 214. Key store/manager 210 may also direct key loader 214 to deactivate screener key module 108 when a screener key has been retrieved from it. Key store/manager 210 may further direct key loader 214 to erase, or otherwise disable, a screener key on screener key module 108, based on an event, such as a pre-determined number of viewings of the associated secure content, unauthorized activity, and the like.

Key store/manager 210 may also employ secure player 200's public key to encrypt a screener key that is to be loaded onto screener key module 108.

Decryption engine 206 is configured to receive a stream of content units from media player subsystem 204. Upon receipt of at least one content unit, decryption

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0358
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

engine 206 may make a determination whether the content unit is encrypted. Where a content unit is encrypted, decryption engine 206 may extract one or more key packages from the content stream. Decryption engine 206 may request a screener key from key store/manager 210 to decrypt the key package to, in turn, enable the extraction of one or more content keys associated with the encrypted content unit. Decryption engine 206 employs the one or more content keys to decrypt the encrypted content unit. Decryption engine 206 may further provide the decrypted content unit to CODEC 208.

(Optional) anticopy protection device 222 enables additional protections of decompressed content by scrambling, dirtying, and otherwise encrypting the decompressed content prior to providing it to a descrambler device, and the like. As such anticopy protection device 222 enables a level of protection of the content after it leaves secure player 200.

Tamper agent 220 is enabled to monitor the components in secure player 200, to determine whether any component, including secure player 200, itself, is being tampered with, or otherwise associated with an unauthorized activity. In one embodiment, tamper detection & response protection device 220 operates at least at a FIPS security level 3.

Tamper agent 220 may provide a response based on the results of its monitoring. Such responses may include directing the erasing or otherwise disabling the secure content, locking secure player 200 from an operation, erasing of secure player's public/private keys, screener keys, content keys, and the like, and reporting the detected unauthorized activity.

FIGURE 3 illustrates one embodiment of a content stream for providing secure content. Content stream 300 is only one example of a suitable stream of content and is not intended to suggest any limitation as to the scope of use or functionality of the present invention. Thus, other well-known structures and configurations may be employed without departing from the scope of the present invention.

As shown in the figure, content unit stream 300 includes content units 301, 303-306, and key package 302. Although, only one key package (302) is

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0359
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

illustrated, it is noted that content stream 300 may include virtually any number of key packages.

Content units 301, and 303-306 may include a variety of content formats. For example, content may be formatted employing Motion Pictures Expert Group (MPEG) format. Content units 301, and 303-306 are not limited to MPEG content formats, and other content formats, including JPEG formats, MP3 formats, and the like, may be employed without departing from scope or spirit of the present invention. However, the MPEG format is employed herein as an example and for ease of illustration.

Briefly, MPEG is an encoding and compression standard for digital broadcast content. MPEG provides compression support for television quality transmission of video broadcast content. Moreover, MPEG provides for compressed audio, control, and even user broadcast content.

MPEG content streams include packetized elementary streams (PES), which typically include fixed (or variable sized) blocks or frames of an integral number of elementary streams (ES) access units. An ES typically is a basic component of an MPEG content stream, and includes digital control data, digital audio, digital video, and other digital content (synchronous or asynchronous). A group of tightly coupled PES packets referenced to substantially the same time base comprises an MPEG program stream (PS). Each PES packet also may be broken into fixed-sized transport packet known as MPEG Transport Streams (TS) that form a general-purpose approach of combining one or more content streams, possible including independent time bases. Moreover, MPEG frames include intra-frames (I-frames), forward predicted frames (P-frames), and bi-directional predicted frames (B-frames).

Content units 301, and 303-306 each may include a portion of the content stream that is partitioned into units of data based on a variety of criteria. For example, content units 301, and 303-306 may include portions of data extracted from the video elementary stream (ES), the audio ES, the digital data ES, and any combination of video, audio, data elementary streams of the content stream. For example, content units 301, and 303-306 may be composed of ten second portions of a

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0360
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

video ES. Moreover, content units 301, and 303-306 need not include the same length, density, and the like, of content from the content stream.

Content units 301, and 303-306 may be selectively encrypted using one or more content keys. That is, content units 301 and 303 may be encrypted, while content units 304-306 are left in the clear. Additionally, encryption may be selectively applied to at least a portion of the video elementary stream (ES), the audio ES, the digital data ES, and any combination and any portion of video, audio, data elementary streams that comprise content stream 300. Selective encryption may further include selectively encrypting at least a portion of an I-frame, P-frame, B-frame, and any combination of P, B, and I frames.

Key package 302 may include one or more content keys used to encrypt content units, and a content identifier associated with a content stream 300. The key package 302 may also include access constraints, entitlements, and the like, associated with content stream 300. Key package 302 may further include synchronization information that indicates which content key is associated with which content unit (301, 302-306) of content stream 300.

Key package 302 may be encrypted employing a targeted secure player's public/private key. In one embodiment, the targeted secure player's public/private keys are generated in a FIPS level 4 device. However, the present invention is not so limited, and lower security levels may be employed to generate the target secure player's public/private keys. In one embodiment, key package 302 is left in the clear, and only the content key(s) are encrypted with the targeted secure player's public/private key.

Generalized Operation

The operation of certain aspects of the present invention will now be described with respect to FIGURES 4-6.

FIGURE 4 illustrates a flow diagram generally showing one embodiment for an end-to-end process of providing and viewing secure content. Process 400 may operate, for example, within operating environment 100 in FIGURE 1.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0361
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Process 400 begins, after a start block, at block 402. Block 402 is described in more detail below in conjunction with FIGURE 5. Briefly, however, at block 402 secure content is created, by selectively encrypting at least one content unit within a content stream. The selective content unit is encrypted employing at least one content key. The employed content key(s), along with additional information, may be further encrypted and embedded within the content stream. The modified content stream is transferred to a content media, such as content media 112 in FIGURE 1.

Processing proceeds to block 404 where the content media and key package are distributed to a user, such as user(s) 114 in FIGURE 1. The content media may be distributed employing a variety of mechanisms, including mail, and the like. The screener key module may include a memory stick, a smart card, a DVD, disk, tape, and the like. The screener key module may be distributed to the user through a different distribution mechanism than employed for the content media. The screener key module may be distributed, for example, by employing the hard media described above, by transmission over a network, by mail, and by a variety of other distribution mechanisms.

Processing continues to block 406, which is described in more detail below in conjunction with FIGURE 6. Briefly, however, at block 406, a secure player, together with the screener key module, and an identity module, are employed to decrypt and view the content stream located on the content media. Upon completion of the actions at block 406, processing returns to processing other actions.

FIGURE 5 illustrates a flow diagram generally showing one embodiment for a process of generating secure content. Process 500 may operate, for example, within operating environment 100 in FIGURE 1.

Process 500 begins, after a start block, at block 502, where a stream of content units is created. A content owner, producer, and the like, may create the stream of content units, by subdividing a content stream into units of data based on a variety of criteria, as described above in conjunction with FIGURE 3.

Processing proceeds to block 504, where at least one content key is generated. A content key may be generated employing any of a number of

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0362
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

encryption/decryption symmetric mechanisms, including, but not limited to Advanced Encryption Standard (AES), RSA, RC6, IDEA, DES, RC2, RC5, Skipjack, and any other symmetric encryption algorithm. Moreover, such encryption algorithms may use, where appropriate, cipher block chaining mode, cipher feedback mode, CBC cipher text stealing (CTS), CFB, OFB, counter mode, and/or any other block mode. In one embodiment, content keys are generated employing an at least 128 bit AES encryption/decryption algorithm. However, content key generation is not limited to symmetric key mechanisms, and asymmetric key mechanisms may also be employed without departing from the scope of the present invention.

Processing continues to block 506, where at least one content key is employed to selectively encrypt a content unit in the content stream. Selective encryption may include selecting a content unit at random in the content stream for encryption, selecting every N/th content unit in the content stream, and the like. Selective encryption may also include selectively encrypting at least a portion of the content unit, such as at least a portion the video elementary stream (ES), the audio ES, the digital data ES, and any combination of video, audio, data elementary streams in the content unit. Selective encryption may further include encrypting a frame in the content unit, such as the I-frame, P-frame, B-frame, and any combination of P, B, and I frames of the content unit.

Moreover, selective encryption may further include varying the content key employed to encrypt selected content units. For example, in one embodiment, a set of content keys is rotated through on some basis, such as every ten seconds, to encrypt the content units.

Processing next proceeds to block 508, where a screener key module is created. The screener key module may include a content identifier associated with the content and a screener key. The screener key module may also include entitlements, rights and the like associated with the content. Moreover, the screener key may be encrypted employing a public/private key that is bound to the targeted secure player.

Processing continues to block 510, where a key package is created. The key package may include at least one content key, a content identifier associated with

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0363
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

the content, access constraints, entitlements, and the like, substantially as described above in conjunction with FIGURE 3. In one embodiment, the at least one content key is encrypted using the screener key. In another embodiment, the key package is encrypted. In still another embodiment, the content identifier associated with the content remains unencrypted.

Processing continues to block 512, where the key package is embedded into the content unit stream. Processing proceeds to block 514, where the modified content units are written to a content media, such as a DVD, high definition DVD, and the like. Upon completion of block 514, processing returns to perform other actions.

It is understood that several blocks of FIGURE 5 can be implemented in a different sequence, combination of sequences, and the like, without departing from the scope or spirit of the present invention. For example, block 506 may be performed prior to, or even in combination with, block 504.

FIGURES 6A-6B illustrate a flow diagram generally showing one embodiment for a process of viewing secure content. Process 600 may operate, for example, within secure player 200 of FIGURE 2.

Process 600 begins, after a start block, at block 602, where a content unit is read from a content media. Processing proceeds to decision block 604, where a determination is made whether the read content unit is encrypted. If it is determined that the read content unit is encrypted, processing branches to block 610; otherwise, processing branches to block 606.

At block 610, a key package is extracted from the content stream on the content media. Processing continues to block 614, where a content identifier is extracted from the key package. In one embodiment, the content identifier is already "in the clear." Processing proceeds to block 616, where the content identifier is employed as an index to locate a screener key associated with the secure content.

Processing continues to decision block 618, where a determination is made whether a screener key associated with the content identifier is located in an existing database, file, directory, and the like, of existing screener keys. If a screener

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0364
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

key is not located, processing branches to block 620; otherwise, processing branches to decision block 626.

At block 620, a request is made to obtain a user identity for authorizing access to a screener key module. The request may require entering a user name/password, a biometric entry, and the like. In one embodiment, the request may require the user to insert a smart card that includes an identification key. Processing continues to decision block 622, where a determination is made whether the received identity is valid. If the received identity is valid, processing branches to block 624; otherwise, processing returns to perform other actions. In one embodiment, such other actions, may include, but is not limited to, enabling the user to attempt to re-enter a valid identity, erasing the content media, locking the user from access of the content media, and the like.

At block 624, the valid user identity is employed to enable access to the screener key located on a screener key module. Processing continues to decision block 626.

At decision block 626, a determination is made whether the validated user has appropriate access rights, entitlements, and the like, to the content unit. If so, processing branches to block 628; otherwise, processing returns to perform other actions, such as described above, at decision block 622.

At block 628, the screener key is decrypted using the private key that is bound to the targeted secure player. Processing continues to block 630, where the decrypted screener key is employed to decrypt the content key. In one embodiment, the decrypted screener key is employed to decrypt the key package and extract the content key. Processing continues to block 632, where the decrypted content key is employed to decrypt the encrypted content unit. Processing continues to block 606.

At block 606, a CODEC is employed to decompress the current content unit. Processing then proceeds to block 608, where the decompressed content is provided to a device, such as a television, and the like, for user enjoyment. In one embodiment, at block 608, the decompressed content is further copy protected. Thus, the decompressed content may be passed through an optional anticopy protection

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0365
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

device, prior to forwarding the decompressed content. Upon completion of the actions at block 608, the process returns to performing other actions.

It will be understood that each block of the flowchart illustration, and combinations of blocks in the flowchart illustration, can be implemented by computer program instructions. These program instructions may be provided to a processor to produce a machine, such that the instructions, which execute on the processor, create means for implementing the actions specified in the flowchart block or blocks. The computer program instructions may be executed by a processor to cause a series of operational steps to be performed by the processor to produce a computer implemented process such that the instructions, which execute on the processor provide steps for implementing the actions specified in the flowchart block or blocks.

Accordingly, blocks of the flowchart illustration support combinations of means for performing the specified actions, combinations of steps for performing the specified actions and program instruction means for performing the specified actions. It will also be understood that each block of the flowchart illustration, and combinations of blocks in the flowchart illustration, can be implemented by special purpose hardware-based systems which perform the specified actions or steps, or combinations of special purpose hardware and computer instructions.

The above specification, examples, and data provide a complete description of the manufacture and use of the composition of the invention. Since many embodiments of the invention can be made without departing from the spirit and scope of the invention, the invention resides in the claims hereinafter appended.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0366
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

WE CLAIM:

1. A system for securely playing a content stream, comprising:

(a) a processor that is arranged to perform actions, including:

(1) selectively encrypting at least a portion of the content stream using a content key;

(2) encrypting the content key using a screener key; and

(3) encrypting the screener key using a public key; and

(b) a player that is arranged to receive the selectively encrypted content stream and encrypted screener key, and to perform actions, including:

(1) decrypting the encrypted screener key using a private key associated the public key, wherein the public key and the private key are bound to the player;

(2) decrypting the encrypted content key using the screener key; and

(3) decrypting the selectively encrypted content stream using the content key.

2. The system of claim 1, wherein the player is arranged to perform actions, further comprising, employing a user identity to enable access to the encrypted screener key.

3. The system of claim 1, wherein the player further comprises:

(a) an authentication module that is arranged to perform actions, including:

(1) receiving a user identity;

(2) authenticating the received user identity;

(2) determining an authorization associated with the user identity; and

(3) if the user identity is authorized to access the encrypted screener key, enabling the encrypted screener key to be retrieved.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0367
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

4. The system of claim 1, wherein the encrypted screener key resides on at least one of a smart card, PCMCIA card, memory stick, DVD, CD, tape, and a floppy disc.

5. The system of claim 1, wherein selectively encrypting at least a portion of the content stream further comprises encrypting at least a portion of at least one of a video elementary stream (ES), audio ES, intra-frames (I-frames), forward predicted frames (P-frames), and bi-directional predicted frames (B-frames).

6. The system of claim 1, wherein selectively encrypting at least a portion of the content stream further comprises employing another content key to encrypt at least another portion of the content stream.

7. The system of claim 1, wherein selectively encrypting at least a portion of the content stream further comprises rotating through a plurality of content keys, each of which is employed to selectively encrypt a different portion of the content stream.

8. An apparatus for securely playing content, comprising:

(a) a loader configured to receive a screener key associated with a selectively encrypted content stream, wherein the screener key is encrypted using a public key that is bound to the apparatus; and

(b) a decryption engine, coupled to the loader, that is configured to perform actions, including:

(1) receiving the selectively encrypted content stream;

(2) employing the loader to retrieve the screener key;

(3) decrypting the screener key using a private key associated with the public key, wherein the private key is constrained to the apparatus; and

(4) employing the screener key to decrypt a content key, wherein the content key enables decryption of the selectively encrypted content stream.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0368
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

9. The apparatus of claim 8, wherein the loader is configured to perform actions, further comprising:

(a) receiving a request for access to the screener key from the decryption engine;

(b) requesting authorization to provide access, from an authentication module; and

(c) if authorization is received, providing the encrypted screener key to the decryption engine.

10. The apparatus of claim 8, wherein the loader is further configured to store another screener key on a screener key module.

11. The apparatus of claim 10, wherein the screener key module comprises at least one of a smart card, PCMCIA card, memory stick, DVD, CD, tape, and a floppy disc.

12. The apparatus of claim 8, wherein the private key and public key associated with the apparatus are generated by a Federal Information Processing Standard (FIPS) level 4 device.

13. The apparatus of claim 8, further comprising a tamper agent configured to monitor for an unauthorized action and, if an unauthorized action is detected, to provide a response to the unauthorized action.

14. The apparatus of claim 13, wherein the response to the unauthorized action further comprises at least one of erasing the selectively encrypted content stream, locking the apparatus from an operation, erasing the private key, erasing the screener key, and reporting the unauthorized action.

15. A method for creating secure content for use in a player, the method comprising:

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0369
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

(a) selectively encrypting at least a portion of a content stream using a content key;

(b) generating a key package comprising the content key;

(c) encrypting the key package using a screener key;

(d) encrypting the screener key employing a public key bound to the player;

(e) embedding the encrypted key package into the selectively encrypted content stream.

16. The method of claim 15, further comprising, copying the selectively encrypted content stream including the embedded key package onto a content media.

17. The method of claim 16, wherein the content media further comprises at least one of a DVD, high definition DVD, Video Compact Disc (VCD), Super VCD (SVCD), Super Audio CD (SACD), Dynamic Digital Sound (DDS) media, Read/Write DVD, and a CD-Recordable (CD-R).

18. The method of claim 15, wherein the content key is generated employing a encryption/decryption algorithm comprising at least one of Advanced Encryption Standard (AES), RSA, International Data Encryption Algorithm (IDEA), and Data Encryption Standard (DES) algorithm.

19. The method of claim 15, wherein the key package further comprises at least one of synchronization information that indicates a relationship between the content key and the selectively encrypted content stream, and a content identifier associated with the content stream.

20. The method of claim 15, wherein the key package further comprises a content identifier associated with the content stream, wherein the content identifier remains unencrypted.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0370
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

21. The method of claim 15, further comprising, storing the encrypted screener key in a screener key module, wherein the screener key module is removable from the player.

22. The method of claim 15, wherein the screener key module further comprises at least one of a content identifier associated with the selectively encrypted content stream, an access constraint, and a fulfillment right.

23. The method of claim 15, wherein selectively encrypting at least a portion of a content stream further comprises selecting for encryption at least a portion of at least one of a video elementary stream (ES), audio ES, intra-frames (I-frames), forward predicted frames (P-frames), and bi-directional predicted frames (B-frames).

24. The method of claim 15, wherein the screener key is generated employing a encryption/decryption algorithm comprising at least one of an Advanced Encryption Standard (AES), RSA, International Data Encryption Algorithm (IDEA), Skipjack, RC4, and a Data Encryption Standard (DES) algorithm.

25. The method of claim 15, wherein selectively encrypting at least a portion of a content stream further comprises partitioning the content stream into content units.

26. A method for securely playing a content stream, comprising:

(a) receiving the content stream, wherein the content stream comprises at least one selectively encrypted content unit;

(b) receiving a key package, wherein the key package is encrypted using a screener key;

(c) retrieving the screener key, wherein the retrieved screener key is encrypted using a public key;

(d) decrypting the retrieved screener key using a private key associated with the public key;

(e) decrypting the key package using the decrypted screener key; and

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0371
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

(f) decrypting at least one selectively encrypted content unit using the decrypted content key.

27. The method of claim 26, wherein the private key is constrained to a player.

28. The method of claim 26, further comprising, decompressing the decrypted content unit.

29. The method of claim 26, wherein retrieving the screener key further comprises, determining an authorization to retrieve the screener key.

30. The method of claim 26, wherein the selectively encrypted content unit further comprises at least a portion of at least one of a video elementary stream (ES), audio ES, intra-frames (I-frames), forward predicted frames (P-frames), and bi-directional predicted frames (B-frames).

31. The method of claim 26, wherein the screener key is generated employing a encryption/decryption algorithm comprising at least one of an Advanced Encryption Standard (AES), RSA, International Data Encryption Algorithm (IDEA), Skipjack, RC4, and a Data Encryption Standard (DES) algorithm.

32. A computer-readable medium encoded with a data structure for use in securing content, the data structure comprising:

a first data field comprising at least one selectively encrypted content unit from a content stream;

a second data field comprising a key package, wherein the key package comprises at least one content key for decrypting the at least one selectively encrypted content unit, and a content identifier associated with the content stream.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0372
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

33. The computer-readable medium of claim 32, wherein the key package further comprises an access constraint associated with the content stream.

34. The computer-readable medium of claim 32, wherein the at least one content key is encrypted using a screener key, the screener key being encrypted using a public key bound to a targeted player.

35. The computer-readable medium of claim 32, wherein the second data field is interspersed between at least two content units.

36. The computer-readable medium of claim 32, wherein the content key is generated employing a encryption/decryption algorithm comprising at least one of Advanced Encryption Standard (AES), RSA, International Data Encryption Algorithm (IDEA), and Data Encryption Standard (DES) algorithm.

37. The computer-readable medium of claim 32, wherein the key package further comprises synchronization information that indicates a relationship between at least one content key and the selectively encrypted content unit.

38. The computer-readable medium of claim 32, wherein the selectively encrypted content unit further comprises at least a portion of at least one of a video elementary stream (ES), audio ES, intra-frames (I-frames), forward predicted frames (P-frames), and bi-directional predicted frames (B-frames).

39. The computer-readable medium of claim 32, wherein the content stream further comprises a plurality of content units, at least one content unit being of a different length.

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0373
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

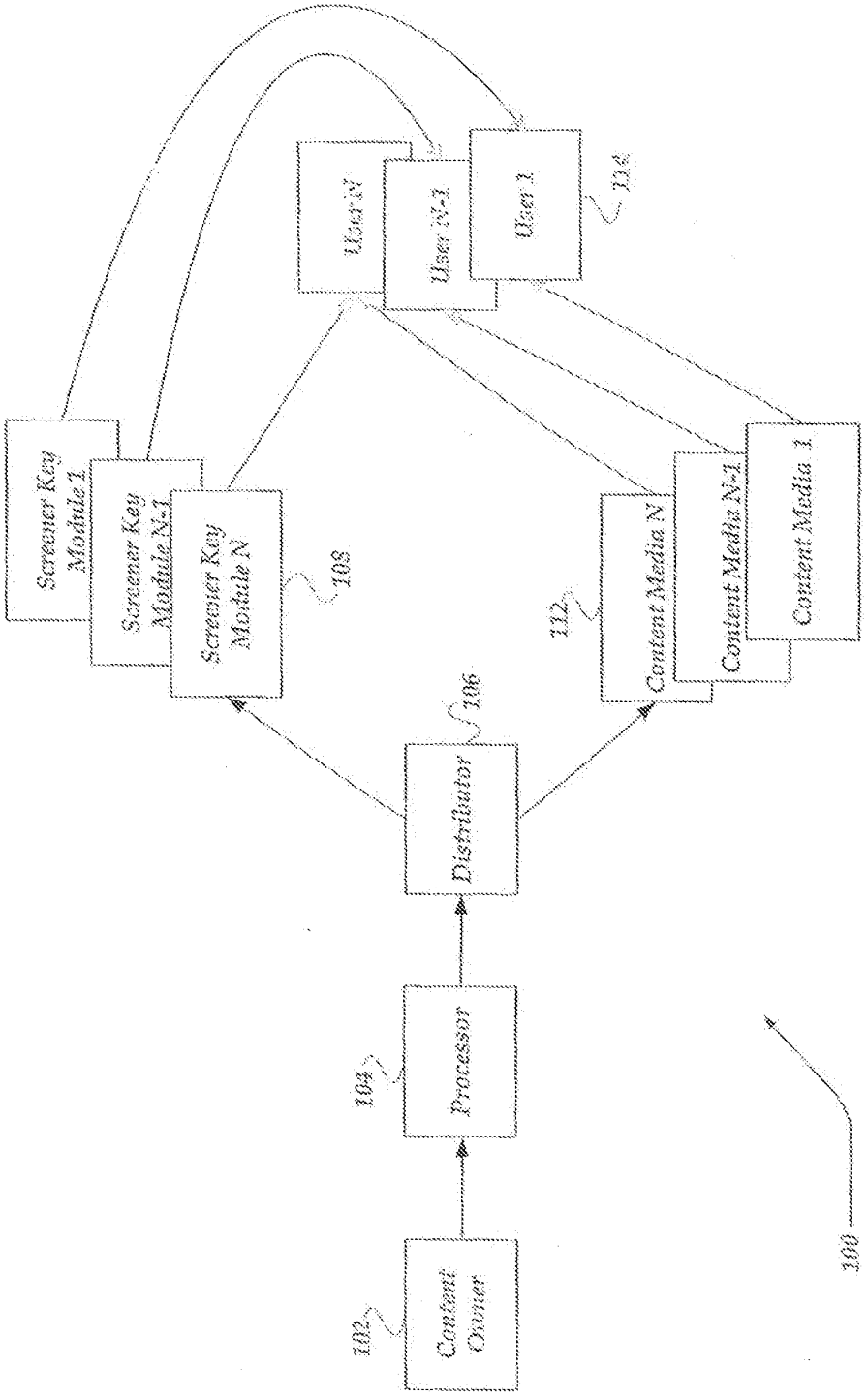

Content Owner
102
Processor
104
Distributor
106
Screener Key Module 1
Screener Key Module N-1
Screener Key Module N
108
Content Media N
Content Media N-1
Content Media 1
112
User N
User N-1
User 1
114
100

Fig. 1.

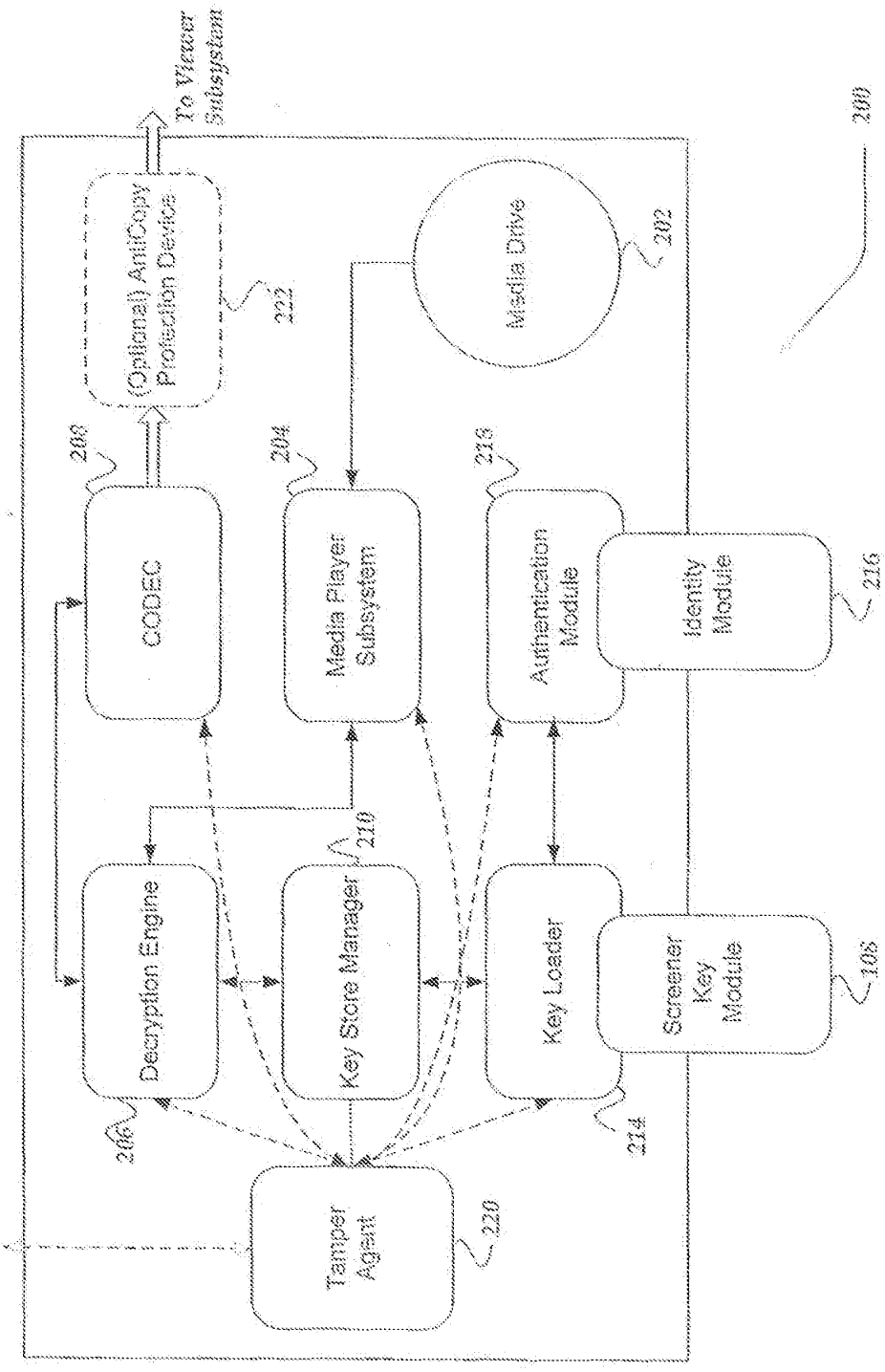

To Viewer Subsystem
200
(Optional) AntiCopy Protection Device
222
Media Drive
202
208
CODEC
204
Media Player Subsystem
213
Authentication Module
Identity Module
216
Decryption Engine
206
210
Key Store Manager
Key Loader
214
Screener Key Module
108
Tamper Agent
220

Fig. 2.

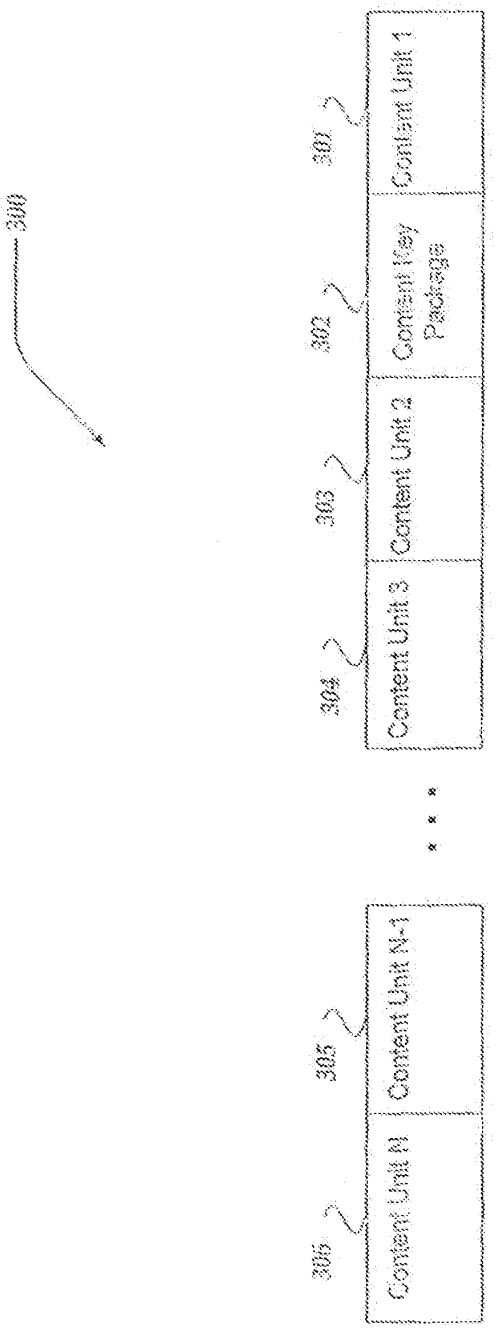

300
301
Content Unit 1
302
Content Key Package
303
Content Unit 2
304
Content Unit 3
305
Content Unit N-1
Content Unit N

Fig. 3.

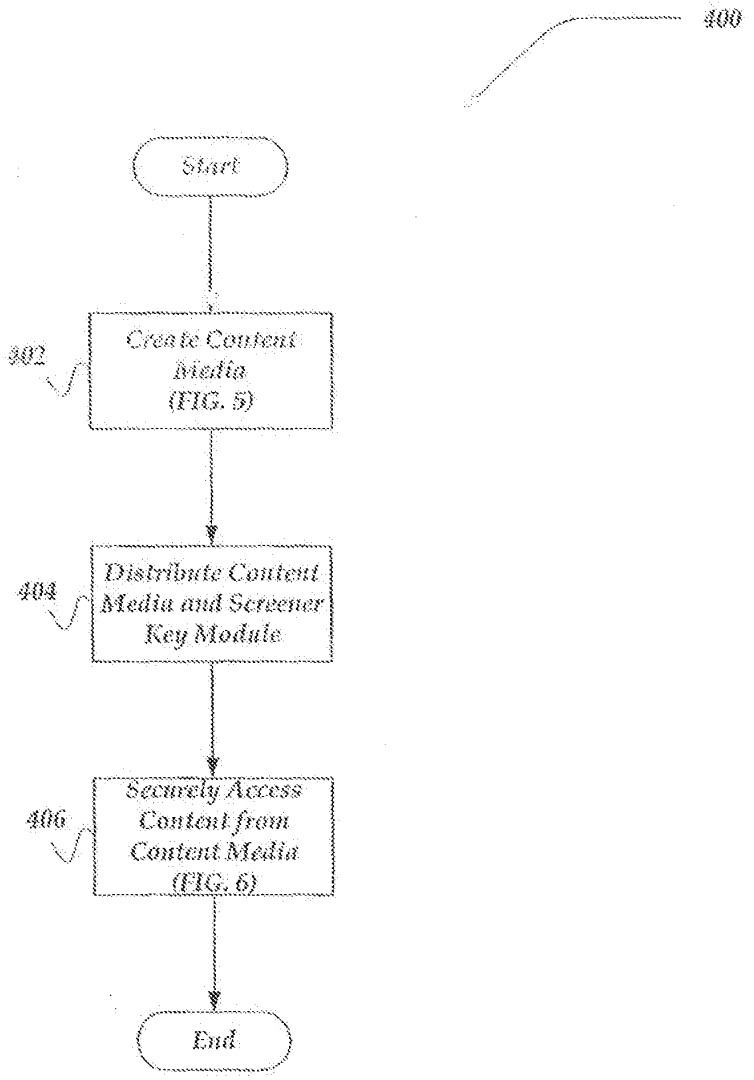

400
Start
302
Create Content Media (FIG. 5)
404
Distribute Content Media and Screener Key Module
406
Securely Access Content from Content Media (FIG. 6)
End

Fig. 4.

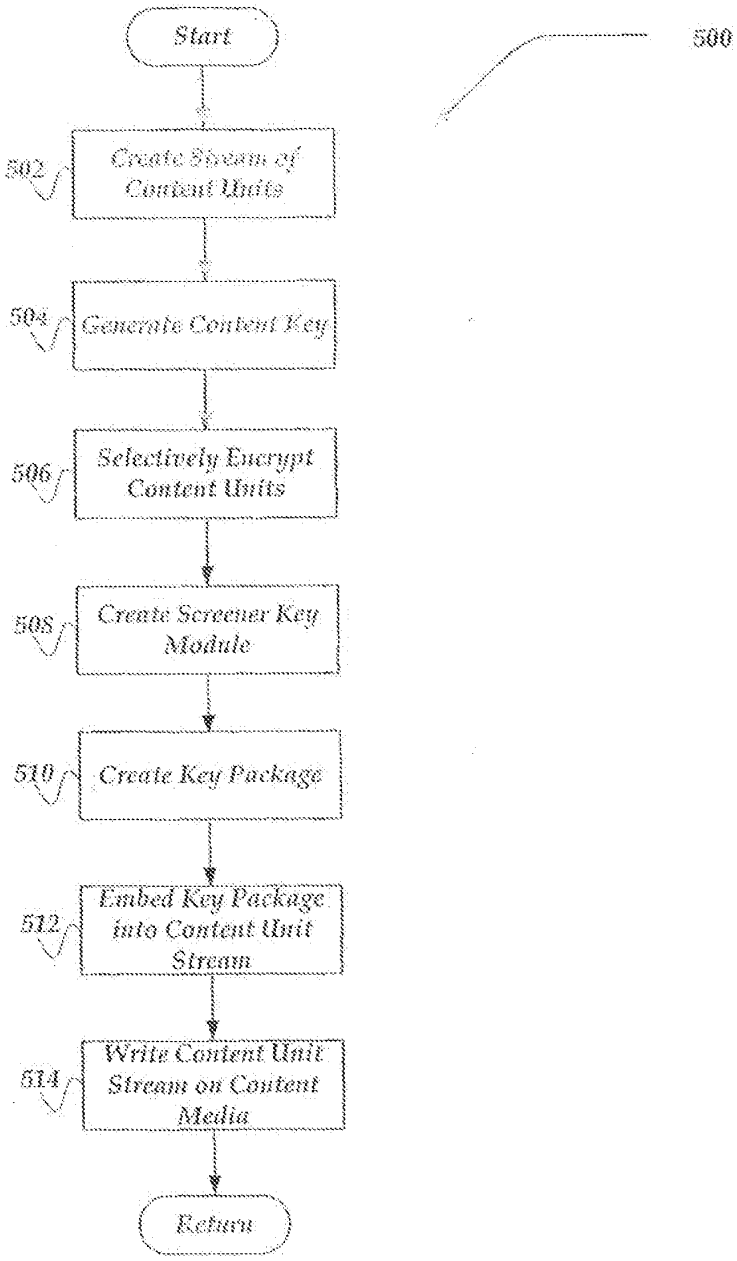

Start
500
502
Create Stream of Content Units
504
Generate Content Key
506
Selectively Encrypt Content Units
508
Create Screener Key Module
510
Create Key Package
512
Embed Key Package into Content Unit Stream
514
Write Content Unit Stream on Content Media
Return

Fig. 5.

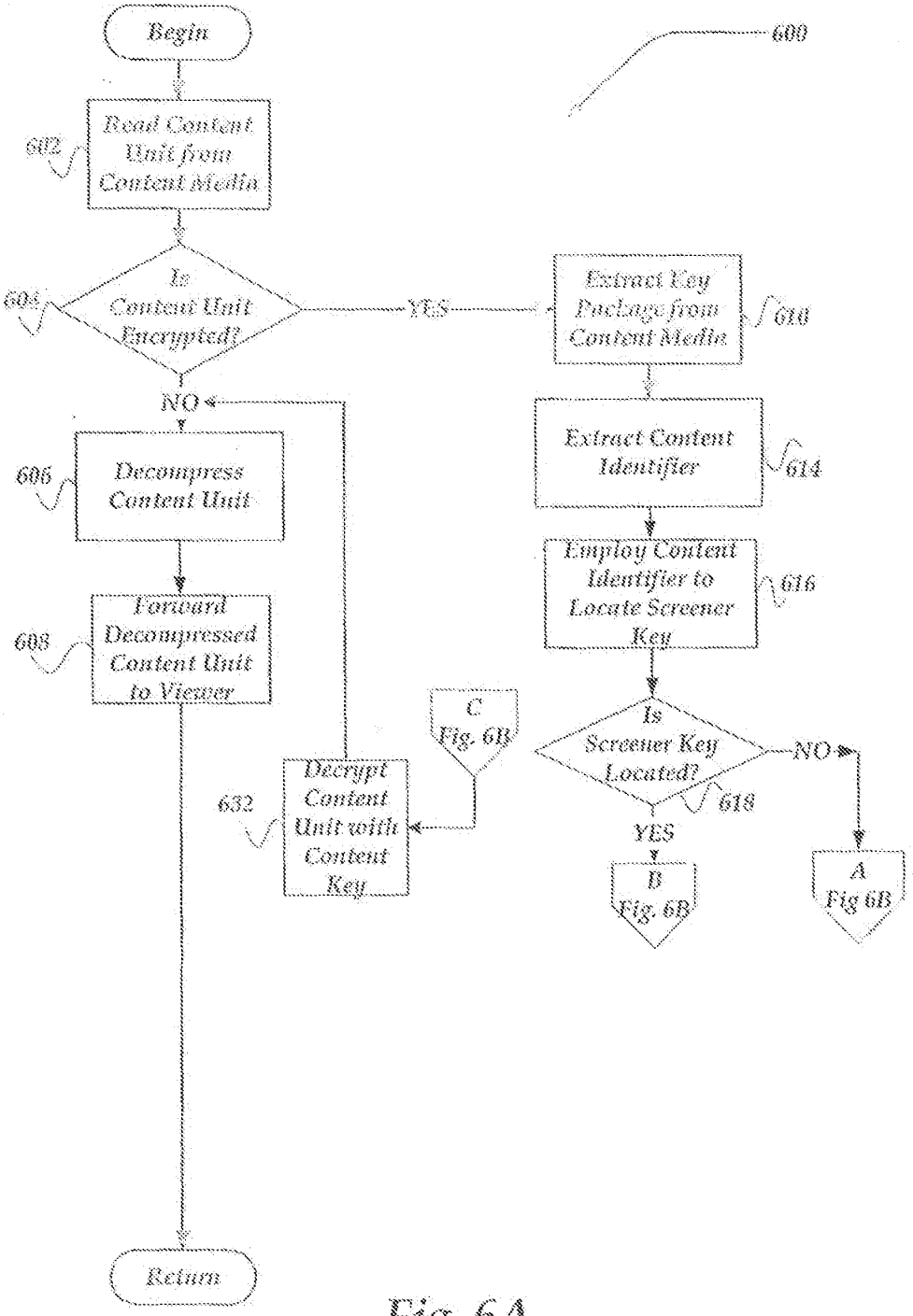

Begin
600
Read Content Unit from Content Media
602
Is Content Unit Encrypted?
604
YES
Extract Key Package from Content Media
610
NO
Extract Content Identifier
614
Employ Content Identifier to Locate Screener Key
616
Is Screener Key Located?
618
NO
YES
A Fig 6B
B Fig 6B
Decompress Content Unit
606
Forward Decompressed Content Unit to Viewer
608
C Fig 6B
Decrypt Content Unit with Content Key
632
Return

Fig. 6A.

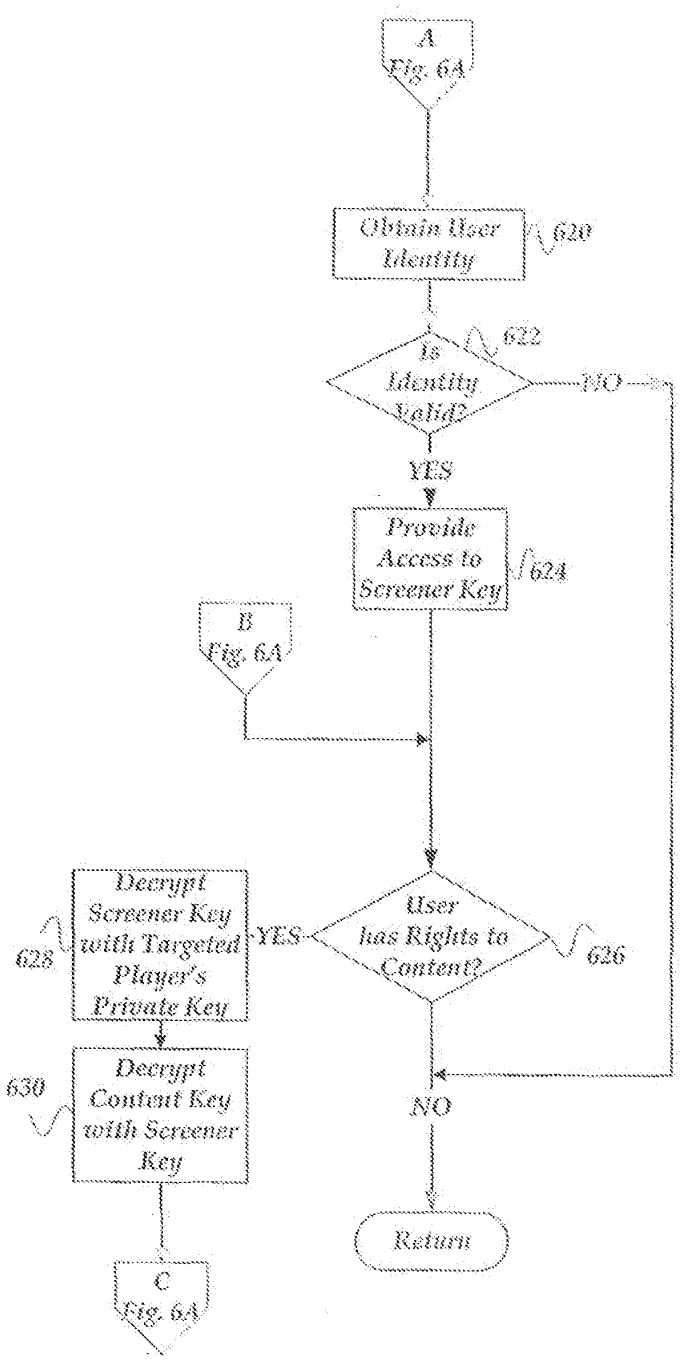

A
Fig. 6A
Obtain User Identity
620
Is Identity Valid?
622
NO
YES
Provide Access to Screener Key
624
B
Fig. 6A
Decrypt Screener Key with Targeted Player's Private Key
628
YES
User has Rights to Content?
626
Decrypt Content Key with Screener Key
630
NO
Return
C
Fig. 6A

Fig. 6B.

(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2006-524007
(P2006-524007A)
(43)公表日　平成18年10月19日(2006.10.19)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601B	5B017
G09C 1/00	(2006.01)	H04L	9/00	601E	5J104
G06F 21/24	(2006.01)	G09C	1/00	640E	
		G06F	12/14	540A	
		G06F	12/14	530B	

審査請求 有　予備審査請求 未請求　（全 22 頁）

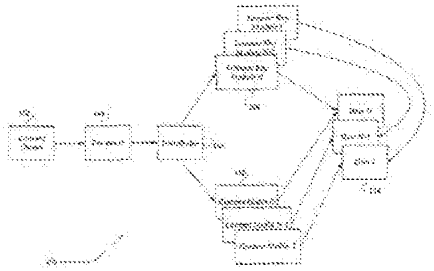
(21)出願番号　特願2006-507290(P2006-507290)
(86)(22)出願日　平成16年3月16日(2004.3.16)
(85)翻訳文提出日　平成17年11月18日(2005.11.18)
(86)国際出願番号　PCT/US2004/008202
(87)国際公開番号　WO2004/084035
(87)国際公開日　平成16年9月30日(2004.9.30)
(31)優先権主張番号　60/456,723
(32)優先日　平成15年3月18日(2003.3.18)
(33)優先権主張国　米国(US)
(31)優先権主張番号　10/760,642
(32)優先日　平成16年1月20日(2004.1.20)
(33)優先権主張国　米国(US)

(71)出願人　504417504
ワイドヴァイン・テクノロジーズ・インコーポレーテッド
アメリカ合衆国ワシントン州９８１６４，シアトル，フォース・アヴェニュー　９００，スイート　３４００
(74)代理人　100089705
弁理士　社本　一夫
(74)代理人　100076691
弁理士　増井　忠弐
(74)代理人　100075270
弁理士　小林　泰
(74)代理人　100080137
弁理士　千葉　昭男

最終頁に続く

(54)【発明の名称】セキュア装置上で閲覧可能なコンテンツを安全に提供するシステム、方法、および装置

(57)【要約】
システム（１００）、装置及び方法は、セキュア・コンテンツの提供及び安全な閲覧を対象とする。一実施形態では、セキュア・プレーヤは、管理局体の会社による映画等のセキュア・コンテンツの安全な上映／試写を提供する。コンテンツ・キーを用いて、コンテンツ・ストリームの少なくとも一部を選択的に暗号化する。コンテンツ・キーはスクリーナ・キー（１０８）で暗号化する。暗号化されたコンテンツ・キーはセキュア・コンテンツに埋め込む。スクリーナ・キー（１０８）は、セキュア・プレーヤに結びついた公開／秘密鍵対を用いて暗号化する。セキュア・コンテンツを、ＤＶＤ，高解像度ＤＶＤ等の媒体（１１２）で配布する。セキュア・プレーヤは，媒体スクリーナ・キー及びスクリーナＩＤを受け取る。スクリーナＩＤ及びスクリーナ・キー（１０８）は，セキュア・プレーヤで、コンテンツの暗号解読及び安全な閲覧を可能とするために用いる。



【特許請求の範囲】
【請求項１】
コンテンツ・ストリームを安全に再生するシステムであって、
（ａ）プロセッサであって、
（１）コンテンツ・キーを使用してコンテンツ・ストリームの少なくとも一部を選択的に暗号化することと、
（２）スクリーナ・キーを使用して前記コンテンツ・キーを暗号化することと、
（３）公開鍵を使用して前記スクリーナ・キーを暗号化することと
を含む動作を実施するように構成されたプロセッサと、
（ｂ）選択的に暗号化された前記コンテンツ・ストリームおよび暗号化された前記スクリーナ・キーを受け取るように構成されたプレーヤであって、
（１）前記公開鍵および該公開鍵に関連する秘密鍵が前記プレーヤに結びつけられており、前記公開鍵に関連する前記秘密鍵を使用して前記暗号化されたスクリーナ・キーを暗号解読することと、
（２）前記スクリーナ・キーを使用して前記暗号化されたコンテンツ・キーを暗号解読することと、
（３）前記コンテンツ・キーを使用して、前記選択的に暗号化されたコンテンツ・ストリームを暗号解読することと
を含む動作を実施するように構成されたプレーヤと
を備えるシステム。
【請求項２】
請求項１に記載のシステムであって、動作を実施するように構成された前記プレーヤが、ユーザＩＤを使用して、前記暗号化されたスクリーナ・キーへのアクセスを可能にする動作を更に含む、システム。
【請求項３】
請求項１に記載のシステムであって、前記プレーヤが、
（ａ）認証モジュールであって、
（１）ユーザＩＤを受け取ることと、
（２）受け取ったユーザＩＤを認証することと、
（２）前記ユーザＩＤに関連する許可について判定することと、
（３）前記ユーザＩＤが前記暗号化されたスクリーナ・キーへのアクセスを許可されている場合に、前記暗号化されたスクリーナ・キーを取り出すことを可能にすることと
を含む動作を実施するように構成された認証モジュール
を更に備える、
システム。
【請求項４】
請求項１に記載のシステムであって、前記暗号化されたスクリーナ・キーが、スマートカード、ＰＣＭＣＩＡカード、メモリ・スティック、ＤＶＤ、ＣＤ、テープ、およびフロッピィ（Ｒ）・ディスクのうちの少なくとも１つに在る、システム。
【請求項５】
請求項１に記載のシステムであって、前記コンテンツ・ストリームの少なくとも一部を選択的に暗号化することが、ビデオ・エレメンタリ・ストリーム（ＥＳ）、オーディオＥＳ、Ｉフレーム（intra-frames）、Ｐフレーム（forward predicted frames）およびＢフレーム（bi-directional predicted frames）のうちの少なくとも１つの少なくとも一部を暗号化することを更に含む、システム。
【請求項６】
請求項１に記載のシステムであって、前記コンテンツ・ストリームの少なくとも一部を選択的に暗号化することが、別のコンテンツ・キーを使用してコンテンツ・ストリームの少なくとも別の部分を暗号化することを更に含む、システム。
【請求項７】

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0382
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

請求項１に記載のシステムであって、前記コンテンツ・ストリームの少なくとも一部を選択的に暗号化することか、前記コンテンツ・キーを複数のコンテンツ・キーの中で交代させることを更に含み、それぞれの前記コンテンツ・キーは、前記コンテンツ・ストリームの異なる部分を選択的に暗号化するために使用される、システム。

【請求項８】

コンテンツを安全に再生する装置であって、

（ａ）選択的に暗号化されたコンテンツ・ストリームに関連するスクリーナ・キーを受け取るように構成されたローダであって、前記スクリーナ・キーが、前記装置に結びつけられた公開鍵を使用して暗号化されるものである、ローダと、

（ｂ）前記ローダに結合された暗号解読エンジンであって、

（１）前記選択的に暗号化されたコンテンツ・ストリームを受け取ることと、

（２）前記ローダを使用して前記スクリーナ・キーを取り出すことと、

（３）前記公開鍵に関連する秘密鍵が前記装置に対して束縛されており、前記公開鍵に関連する前記秘密鍵を使用して前記スクリーナ・キーを暗号解読することと、

（４）コンテンツ・キーは前記選択的に暗号化されたコンテンツ・ストリームの暗号解読を可能にするものであり、前記スクリーナ・キーを使用して前記コンテンツ・キーを暗号解読することと、

を含む動作を実施するように構成される暗号解読エンジンと

を備える装置。

【請求項９】

請求項８に記載の装置であって、前記ローダが、

（ａ）前記暗号解読エンジンから前記スクリーナ・キーへのアクセス要求を受け取ることと、

（ｂ）アクセスを実現するための許可を認証モジュールに要求することと、

（ｃ）許可を受け取った場合に、前記暗号化されたスクリーナ・キーを前記暗号解読エンジンに提供することと

を更に含む動作を実施するように構成される、

装置。

【請求項１０】

請求項８に記載の装置であって、前記ローダが更に、スクリーナ・キー・モジュール上へ別のスクリーナ・キーを格納するように構成される、装置。

【請求項１１】

請求項１０に記載の装置であって、前記スクリーナ・キー・モジュールが、スマートカード、ＰＣＭＣＩＡカード、メモリ・スティック、ＤＶＤ、ＣＤ、テープ、およびフロッピィ（Ｒ）・ディスクのうちの少なくとも１つを含む、装置。

【請求項１２】

請求項８に記載の装置であって、前記装置に関連する前記秘密鍵および前記公開鍵が、連邦情報処理標準（ＦＩＰＳ）レベル４の装置で生成される、装置。

【請求項１３】

請求項８に記載の装置であって、無許可の活動を監視し、無許可の活動を検出した場合、前記無許可の活動に対する応答を与えるように構成されたタンパ・エージェントを更に備える装置。

【請求項１４】

請求項１３に記載の装置であって、無許可の活動に対する前記応答が、前記選択的に暗号化されたコンテンツ・ストリームを消去すること、前記装置を動作しないようにロックすること、前記秘密鍵を消去すること、前記スクリーナ・キーを消去すること、および前記無許可の活動を報告することのうちの少なくとも１つを更に含む、装置。

【請求項１５】

プレーヤで使用するセキュア・コンテンツを作成する方法であって、

（ａ）コンテンツ・キーを使用してコンテンツ・ストリームの少なくとも一部を選択的

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0383
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

に暗号化するステップと、
（ｂ）前記コンテンツ・キーを含むキー・パッケージを生成するステップと、
（ｃ）スクリーナ・キーを使用して前記キー・パッケージを暗号化するステップと、
（ｄ）前記プレーヤに結びつけられた公開鍵を使用して前記スクリーナ・キーを暗号化するステップと、
（ｅ）前記選択的に暗号化したコンテンツ・ストリームに、前記暗号化したキー・パッケージを埋め込むステップと
を備える方法。
【請求項１６】
請求項１５に記載の方法であって、埋め込まれた前記キー・パッケージを含む、前記選択的に暗号化されたコンテンツ・ストリームを、コンテンツ媒体上にコピーするステップを更に含む方法。
【請求項１７】
請求項１６に記載の方法であって、
前記コンテンツ媒体が、ＤＶＤ、高精細度ＤＶＤ、ビデオ・コンパクト・ディスク（ＶＣＤ）、スーパーＶＣＤ（ＳＶＣＤ）、スーパー・オーディオＣＤ（ＳＡＣＤ）、ダイナミック・デジタル・サウンド（ＤＤＳ）媒体、リード／ライトＤＶＤ、ＣＤレコーダブル（ＣＤ－Ｒ）のうちの少なくとも１つを更に含む、方法。
【請求項１８】
請求項１５に記載の方法であって、前記コンテンツ・キーが、ＡＥＳ（次世代暗号化標準）、ＲＳＡ、国際データ暗号化アルゴリズム（ＩＤＥＡ）、およびＤＥＳ（データ暗号化規格）アルゴリズムのうちの少なくとも１つを含む暗号化／暗号解読アルゴリズムを使用して生成される、方法。
【請求項１９】
請求項１５に記載の方法であって、前記キー・パッケージが、コンテンツ・キーと選択的に暗号化したコンテンツ・ストリームとの間の関係を示す同期情報と、前記コンテンツ・ストリームに関連するコンテンツ識別子とのうちの少なくとも一つを更に含む、方法。
【請求項２０】
請求項１６に記載の方法であって、前記キー・パッケージが、前記コンテンツ・ストリームに関連するコンテンツ識別子を更に含み、前記コンテンツ識別子が暗号化されない状態にとどまる、方法。
【請求項２１】
請求項１５に記載の方法であって、前記暗号化されたスクリーナ・キーをスクリーナ・キー・モジュールに格納するステップを更に含み、前記スクリーナ・キー・モジュールが前記プレーヤから取外し可能である、方法。
【請求項２２】
請求項１５に記載の方法であって、前記スクリーナ・キー・モジュールが、前記選択的に暗号化されたコンテンツ・ストリームに関連するコンテンツ識別子と、アクセス制約と、履行権とのうちの少なくとも１つを更に含む、方法。
【請求項２３】
請求項１５に記載の方法であって、コンテンツ・ストリームの少なくとも一部を選択的に暗号化する前記ステップが、ビデオ・エレメンタリ・ストリーム（ＥＳ）、オーディオＥＳ、Ｉフレーム（intra-frames）、Ｐフレーム（forward predicted frames）、およびＢフレーム（bi-directional predicted frames）のうちの少なくとも１つの少なくとも一部を暗号化のために選択するステップを更に含む、方法。
【請求項２４】
請求項１５に記載の方法であって、前記スクリーナ・キーが、ＡＥＳ（次世代暗号化標準）、ＲＳＡ、ＩＤＥＡ（国際データ暗号化アルゴリズム）、スキップジャック、ＲＣ４、およびＤＥＳ（データ暗号化規格）アルゴリズムのうちの少なくとも１つを含む暗号化／暗号解読アルゴリズムを使用して生成される、方法。

【請求項２５】
請求項１５に記載の方法であって、コンテンツ・ストリームの少なくとも一部を選択的に暗号化する前記ステップが、前記コンテンツ・ストリームをコンテンツ・ユニットに区分するステップを更に含む、方法。
【請求項２６】
コンテンツ・ストリームを安全に再生する方法であって、
（ａ）少なくとも１つの選択的に暗号化されたコンテンツ・ユニットを含む前記コンテンツ・ストリームを受け取るステップと、
（ｂ）スクリーナ・キーを使用して暗号化されるキー・パッケージを受け取るステップと、
（ｃ）公開鍵を使用して暗号化されるスクリーナ・キーを取り出すステップと、
（ｄ）前記公開鍵に関連する秘密鍵を使用して、前記取り出したスクリーナ・キーを暗号解読するステップと、
（ｅ）前記暗号解読されたスクリーナ・キーを使用して、前記キー・パッケージを暗号解読するステップと、
（ｆ）前記暗号解読されたコンテンツ・キーを使用して、少なくとも１つの選択的に暗号化したコンテンツ・ユニットを暗号解読するステップと
を備える方法。
【請求項２７】
請求項２６に記載の方法であって、前記秘密鍵がプレーヤに束縛される、方法。
【請求項２８】
請求項２６に記載の方法であって、前記暗号解読されたコンテンツ・ユニットを圧縮解除するステップを更に含む方法。
【請求項２９】
請求項２６に記載の方法であって、前記スクリーナ・キーを取り出す前記ステップが、前記スクリーナ・キーを取り出す許可を判定するステップを更に含む、方法。
【請求項３０】
請求項２６に記載の方法であって、前記選択的に暗号化されたコンテンツ・ユニットが、ビデオ・エレメンタリ・ストリーム（ＥＳ）、オーディオＥＳ、Ｉフレーム（intra-frames）、Ｐフレーム（forward predicted frames）、およびＢフレーム（bi-directional predicted frames）のうちの少なくとも１つの少なくとも一部を更に含む、方法。
【請求項３１】
請求項２６に記載の方法であって、前記スクリーナ・キーが、ＡＥＳ（次世代暗号化標準）、ＲＳＡ、ＩＤＥＡ（国際データ暗号化アルゴリズム）、スキップジャック、ＲＣ４、およびＤＥＳ（データ暗号化規格）アルゴリズムのうちの少なくとも１つを含む暗号化／暗号解読アルゴリズムを使用して生成される、方法。
【請求項３２】
コンテンツを保護する際に使用するデータ構造で符号化されたコンピュータ読み取り可能な媒体であって、前記データ構造が、
コンテンツ・ストリームからの少なくとも１つの選択的に暗号化されたコンテンツ・ユニットを含む第１データ・フィールドと、
キー・パッケージを含む第２データ・フィールドであって、前記キー・パッケージが、前記少なくとも１つの選択的に暗号化されたコンテンツ・ユニットを暗号解読する少なくとも１つのコンテンツ・キーと、前記コンテンツ・ストリームに関連するコンテンツ識別子とを含む、第２データ・フィールドと
を備えるコンピュータ読み取り可能な媒体。
【請求項３３】
請求項３２に記載のコンピュータ読み取り可能な媒体であって、前記キー・パッケージが、前記コンテンツ・ストリームに関連するアクセス制約を更に含む、コンピュータ読み取り可能な媒体。

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0385
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

【請求項３４】
請求項３２に記載のコンピュータ読み取り可能な媒体であって、前記少なくとも１つのコンテンツ・キーが、スクリーナ・キーを使用して暗号化され、前記スクリーナ・キーが、対象とされるプレーヤに結びつけられた公開鍵を使用して暗号化される、コンピュータ読み取り可能な媒体。
【請求項３５】
請求項３２に記載のコンピュータ読み取り可能な媒体であって、前記第２データ・フィールドが、少なくとも２つのコンテンツ・ユニットの間に点在される、コンピュータ読み取り可能な媒体。
【請求項３６】
請求項３２に記載のコンピュータ読み取り可能な媒体であって、前記コンテンツ・キーが、ＡＥＳ（次世代暗号化標準）、ＲＳＡ、ＩＤＥＡ（国際データ暗号化アルゴリズム）、およびＤＥＳ（データ暗号化規格）アルゴリズムのうちの少なくとも１つを含む暗号化／暗号解読アルゴリズムを使用して生成される、コンピュータ読み取り可能な媒体。
【請求項３７】
請求項３２に記載のコンピュータ読み取り可能な媒体であって、前記キー・パッケージが、少なくとも１つのコンテンツ・キーと前記選択的に暗号化されたコンテンツ・ユニットとの間の関係を示す同期情報を更に含む、コンピュータ読み取り可能な媒体。
【請求項３８】
請求項３２に記載のコンピュータ読み取り可能な媒体であって、前記選択的に暗号化されたコンテンツ・ユニットが、ビデオ・エレメンタリ・ストリーム（ＥＳ）、オーディオＥＳ、Ｉフレーム（intra-frames）、Ｐフレーム（forward predicted frames）、およびＢフレーム（bi-directional predicted frames）のうちの少なくとも１つの少なくとも一部を更に含む、コンピュータ読み取り可能な媒体。
【請求項３９】
請求項３２に記載のコンピュータ読み取り可能な媒体であって、前記コンテンツ・ストリームが複数のコンテンツ・ユニットを更に含み、少なくとも１つのコンテンツ・ユニットが異なる長さである、コンピュータ読み取り可能な媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本願は、２００３年３月１８日出願の米国仮出願第６０／４５５７２３号の特典を主張するものである。その初期の出願日の特典が３５Ｕ．Ｓ．Ｃセクション１１９（ｅ）の下で主張される。
【０００２】
本発明はデータ・セキュリティに関し、より詳細には、セキュア・コンテンツを提供することおよび安全に再生するシステム、方法、および装置に関する。
【背景技術】
【０００３】
デジタル・バーサタイル・ディスク（ＤＶＤ）は、恐らくは今日の最も急速に成長し、最も迅速に受け入れられた消費者向け電子機器製品である。興味深いことに、ＤＶＤフォーマットが非常に革新的で消費者およびエンターテイメント産業にとって魅力的である主な理由の１つは、まさに違法コピーに弱いことである。ＤＶＤは、映画が記録されＤＶＤで再生されるごとに完璧に再現可能なデジタル・フォーマットで映画を保存するので、初めて家庭で明瞭かつ高品質な音声で映画を閲覧することができる。更に、映画がデジタル式に記憶されるということは、映画会社およびその他の者がほぼ無限の数の本質的に完全なＤＶＤ映画のコピーを作成することが可能となることも意味する。
【発明の開示】
【課題を解決するための手段】
【０００４】

そのような品質および複製の容易さにより、映画会社が、例えば映画芸術科学アカデミーのメンバに初版の映画の数千のオリジナル・コピーを送るのに極めて好都合となった。これらのＤＶＤは、通常、オスカーおよびその他の業界の賞の投票を行う人だけが閲覧するためのものである。しかし、ＤＶＤの多くは、不正な管理下に置かれ、ＤＶＤをコピーしてそれをオンラインで及び外国の市で配布する違法な業者のデジタル写真となってきた。次いで、そのような多くの映画は、映画館での封切りのすぐ後、時にはそれよりも前に、海賊版ＤＶＤの形態で現れる。映画を配布するためにＤＶＤなどの高品質デジタル媒体を引き続き使用することが好ましいので、コンテンツを保護するために比較的高いレベルのセキュリティを提供することが望ましい。遺憾ながら、違法コピーは高い品質であり、映画会社などが住々にして結果として数百万ドルを損失する。更に、エンターテイメント産業の他の多くのコンテンツ所有者は、そのようなコンテンツ保護が利用可能となるまで、ＤＶＤでコンテンツを提供したがらない。従って、こうした考慮すべき点およびその他に対して、本発明がなされた。

【０００５】

添付の図面を参照しながら、本発明の非限定的かつ非網羅的な実施形態を説明する。図面では、別段の指定がない限り、様々な図を通して同様の参照番号は同様の部分を指す。

本発明をより良く理解できるように、添付の図面と関連して読まれるべき以下の好ましい実施形態の詳細な説明を参照する。

【発明を実施するための最良の形態】

【０００６】

本発明の例示的な実施形態の以下の詳細な説明では、本明細書の一部を形成し、本発明を実施することのできる特定の例示的な実施形態を例として示す添付の図面を参照する。当業者が本発明を実施することができるように各実施形態を十分詳細に説明するが、本発明の精神または範囲から逸脱することなく他の実施形態を使用でき、また、他の変更を行えることを理解されたい。従って、以下の詳細な説明を限定的な意味で理解すべきではなく、本発明の範囲は添付の特許請求の範囲によってのみ定義される。

【０００７】

明細書および特許請求の範囲を通して、以下の用語は、文脈が明らかにそうでないことを求めるのでない限り、本明細書に関連した明示的な意味を持つ。

用語「結合（ｃｏｕｐｌｅｄ）」および「接続（ｃｏｎｎｅｃｔｅｄ）」は、接続された物の間の直接接続、あるいは１または複数の受動的または能動的な中間装置または構成要素を介する間接接続を含む。

【０００８】

用語「スクリーナ（ｓｃｒｅｅｎｅｒ）」は、ユーザ、賞を付与する団体のメンバなどによって閲覧／上映される、あるいは楽しまれる媒体コンテンツなどを含む。用語「スクリーナ」はまた、ＤＶＤ、高精細度フォーマットＤＶＤなどのコンテンツ媒体も含む。

【０００９】

「ａ（１つの）」、「ａｎ（１つの）」、および「ｔｈｅ（その）」の意味は複数を言及することを含む。「ｉｎ（中）」の意味は、「ｉｎ（中）」および「ｏｎ（上）」を含む。

【００１０】

簡潔に述べると、本発明は、選択されたユーザによってセキュア・プレーヤ（安全なプレーヤ）上で閲覧可能なセキュア・コンテンツを安全に提供するシステム、装置、および方法に関する。一実施形態では、セキュア・プレーヤは、ＤＶＤなどのコンピュータ可読媒体を受けるように構成される。しかし、本発明はＤＶＤに限定されない。例えば、限定はしないが、高精細度ＤＶＤなどのような高品質デジタル媒体を含む他の媒体上でセキュア・コンテンツを安全に提供および閲覧するように本発明を構成することが想定される。

【００１１】

例示的な環境

図１は、本発明を実施することのできる例示的な動作環境１００を示す機能ブロック図

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0387
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

である。動作環境１００は、適切な動作環境の一例に過ぎず、本発明の使用法または機能の範囲に関して何らかの制限を示唆するものではない。従って、本発明の範囲または精神から逸脱することなく、他の周知の環境および構成を使用することができる。

【００１２】

図に示すように、動作環境１００は、コンテンツ所有者１０２、プロセッサ１０４、配給部（ディストリビュータ）１０６、スクリーナ・キー・モジュール１０８（１からＮ）、コンテンツ媒体１１２（１からＮ）、ユーザ１１４（１からＮ）を含む。プロセッサ１０４は、コンテンツ所有者１０２およびディストリビュータ１０６と通信する。ディストリビュータ１０６はまた、スクリーナ・キー・モジュール１０８（１からＮ）およびコンテンツ媒体１１２（１からＮ）と通信する。ユーザ１１４（１からＮ）はまた、スクリーナ・キー・モジュール１０８（１からＮ）およびコンテンツ媒体１１２（１からＮ）と通信する。

【００１３】

コンテンツ所有者１０２は、ユーザ１１４へ配布することのできる媒体コンテンツのプロデューサ、開発者、および所有者を含む。スクリーナと呼ばれることもあるそのようなコンテンツは、動画、映画、ビデオなどを含む。しかし、コンテンツ所有者１０２によって所有されるコンテンツはビデオ・コンテンツだけに限定されず、本発明の範囲または精神から逸脱することなく、音声のみのサービスを含むこともできる。従って、コンテンツは、限定はしないが、ユーザ１１４に向けて送られる音声、ビデオ、静止画像、テキスト、グラフィックス、およびその他の形態のコンテンツ（スクリーナ）を含むものとする。

【００１４】

プロセッサ１０４は、図３に関連して以下でより詳細に説明するように、コンテンツ所有者１０２からコンテンツを受け取り、コンテンツの少なくとも一部を選択的に保護し、保護されたコンテンツをディストリビュータ１０６へ提供する。しかし、簡潔に言うと、プロセッサ１０４は、選択された情報、例えば、暗号解読のためのコンテンツ・キー、コンテンツ識別子、アクセス制約、権利、資格などを作成し、受け取ったコンテンツのストリームへ埋め込む。一実施形態では、選択した情報は、少なくとも１つのキー・パッケージ（図示せず）にパッケージ化されるものであり、各キー・パッケージは、少なくとも１つのスクリーナ・キーを使用して暗号化される。別の実施形態では、各コンテンツ・キーが、少なくとも１つのスクリーナ・キーを使用して暗号化される。一実施形態では、コンテンツ識別子を明文にしておくことができる。

【００１５】

限定はしないが、ＲＳＡアルゴリズム、データ暗号化規格（Data Encryption Standard）（ＤＥＳ）、国際データ暗号化アルゴリズム（International Data Encryption Algorithm）（ＩＤＥＡ）、スキップジャック、ＲＣ４、次世代暗号化標準（Advanced Encryption Standard）（ＡＥＳ）などを含む様々な暗号化／暗号解読対称鍵機構のいずれかを使用して、スクリーナ・キー（１又は複数）を生成することができる。一実施形態では、スクリーナ・キー（１又は複数）は、キー・パッケージの暗号化／暗号解読のために２５６ビットＡＥＳアルゴリズムを使用する。しかしながら、スクリーナ・キーは対称鍵機構に限定されず、本発明の範囲または精神から逸脱することなく非対称鍵機構を使用することもできる。

【００１６】

プロセッサ１０４は、限定はしないが、コンテンツ所有者１０２、承認された第３者などを含む様々なソースから、スクリーナ・キー（１又は複数）およびコンテンツ・キー（１又は複数）を得ることができる。プロセッサ１０４はまた、プロセッサ１０４自体でスクリーナ・キー（１又は複数）および／またはコンテンツ・キー（１又は複数）を生成することもできる。更に、スクリーナ・キーは、キー・ストレージ（図示せず）内に格納することができる。各スクリーナ・キーは、キー・ストレージ内で、特定のコンテンツに関連するコンテンツ識別子によって索引付けすることができる。キー・ストレージは、ユーザや、コンテンツや、対象のセキュア・プレーヤや、ユーザとコンテンツと対象のセキュ

ア・プレーヤとの任意の組合せなどに関連するアクセス制約、権利などを更に含むことができる。

【００１７】

ディストリビュータ１０６は、セキュア・コンテンツをコピーおよび配布するためにコンテンツ所有者１０２から権利を得るビジネス、システムなどを含む。ディストリビュータ１０６は、コピーおよび配布するための権利を１または複数のコンテンツ所有者から得る。ディストリビュータ１０６は、他のディストリビュータ、ユーザ１１４などに対しての、コンテンツ媒体１１２を用いた後の販売、配布、およびライセンス（認可）のためにセキュア・コンテンツを再パッケージ化、格納、およびスケジューリングする。

【００１８】

ディストリビュータ１０６は、限定はしないが、ＤＶＤ、高精細度ＤＶＤ、ビデオ・コンパクト・ディスク（ＶＣＤ）、スーパーＶＣＤ（ＳＶＣＤ）、スーパー・オーディオＣＤ（ＳＡＣＤ）などを含む様々なコンテンツ媒体１１２にセキュア・コンテンツをコピーすることができる。例えば、ダイナミック・デジタル・サウント（ＤＤＳ）コンテンツ媒体にセキュア・コンテンツをコピーして配布することができる。更に、ディストリビュータ１０６は、Ｒｅａｄ／Ｗｒｉｔｅ（書込／読出） ＤＶＤ、ＣＤ－Ｒｅｃｏｒｄａｂｌｅ（ＣＤ－Ｒ）、および本質的にこれらと類似のコンテンツ媒体でセキュア・コンテンツのコピーおよび配布することもできる。ディストリビュータ１０６は、ＤＶＤおよびＣＤコンテンツ媒体技術上でのセキュア・コンテンツのコピーおよび配布に限定されず、本発明の範囲から逸脱することなく、実質的に何れの他のコンテンツ媒体技術も使用することができる。

【００１９】

ディストリビュータ１０６は、１または複数のキー・パッケージに関連する１または複数のスクリーナ・キーを受け取ることができる。ディストリビュータ１０６はまた、ユーザがセキュア・コンテンツにアクセスする許可を有するかどうかを示す許可情報を様々な信頼のおけるソースから受け取ることができる。ユーザが許可を有することを条件として、ディストリビュータ１０６は、受け取ったスクリーナ・キー（１または複数）をスクリーナ・キー・モジュール１０８へとパッケージ化する。ディストリビュータ１０６はまた、セキュア・コンテンツに関連するコンテンツ識別子、履行権、アクセス制約、対象のセキュア・プレーヤに関連する属性などを、スクリーナ・キー・モジュール１０８に含めることもできる。例えば、ディストリビュータ１０６は、選択された地理範囲内でセキュア・コンテンツが再生可能ではないことを示す属性を、スクリーナ・キー・モジュール１０８に含めることができる。

【００２０】

ディストリビュータ１０６は更に、ターゲット（対象）とされるセキュア・プレーヤに関連する公開鍵で、スクリーナ・キー（１又は複数）、スクリーナ・キー・モジュール１０８上に含まれる追加の情報を暗号化する。対象のセキュア・プレーヤの公開鍵は、限定はしないが、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ（ディフィーヘルマン）、ＲＳＡ、Ｍｅｒｋｌｅ－Ｈｅｌｌｍａｎ（メルクルヘルマン）、ＰＧＰ、Ｘ．５０９などを含む様々な非対称暗号化機構を使用して生成することができる。

【００２１】

一実施形態では、ディストリビュータ１０６は、対象のセキュア・プレーヤに関連する２０４８ビットＲＳＡ非対称（公開／秘密）鍵を使用してスクリーナ・キー（１又は複数）を暗号化する。別の実施形態では、対象のセキュア・プレーヤに関連する公開／秘密鍵対が、連邦情報処理標準（ＦＩＰＳ）レベル４装置で生成される。しかし、本発明はそのように限定されるものではなく、別のセキュリティ・レベルを使用して対象のセキュア・プレーヤの公開／秘密鍵対を生成することができる。

【００２２】

いずれにしても、対象のセキュア・プレーヤの公開鍵を、信頼された第３者、ネットワーク、Ｅメールなどを含む様々な手法を介して、ディストリビュータ１０６が利用できる

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0389
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

ようにすることができる。更に、対象のセキュア・プレーヤの秘密／公開鍵は、対象のセキュア・プレーヤに、その特定の対象のセキュア・プレーヤに対して秘密／公開鍵が固有となるように、結びつけられる。更に、対象のセキュア・プレーヤは、対象のセキュア・プレーヤの秘密鍵の除去を防止するように構成される。そのような措置により、更に、対象のセキュア・プレーヤの秘密鍵が対象のセキュア・プレーヤに結びつけられる。

【００２３】

ディストリビュータ１０６は、限定はしないがスマートカード、ＰＣＭＣＩＡカード、メモリ・スティック、ネットワーク経由、ＤＶＤ、ＣＤ、テープ、フロッピィ（Ｒ）・ディスク、および類似の取外し可能な機構を含む様々な機構を使用して、スクリーナ・キー・モジュール１０８をユーザ１１４（１又は複数）へ配布することができる。スクリーナ・キー・モジュール１０８をユーザ１１４へメールで送ることもできる。

【００２４】

ユーザ１１４（１又は複数）は、エンド・ユーザ、コンテンツの消費者などを含む。ユーザ１１４は、検討のためにコンテンツ（スクリーナ）を受け取る資付与団体のメンバなどを更に含む。ユーザ１１４は、限定はしないかテレビジョン機器、モバイル装置、ＰＤＡ、パーソナル・コンピュータ、ジュークボックスなどを含む様々な装置を使用してコンテンツを楽しむことができる。ユーザ１１４は更に、図２に関連して以下でより詳細に説明するセキュア・プレーヤを使用して、コンテンツを上記の装置へ安全に提供することができる。

【００２５】

ユーザ１１４は、直接にコンテンツ所有者１０２にコンテンツ媒体１１２を要求することができ、また、マーケット・ストリームに沿った任意の点で（例えばディストリビュータ１０６に）コンテンツ媒体１１２を要求することができる。更に、ユーザ１１４は、複数のコンテンツ所有者１０２、ディストリビュータ１０６などを介してコンテンツ媒体１１２を受け取ることができる。ユーザ１１４は更に、コンテンツ所有者１０２、ディストリビュータ１０６などからスクリーナ・キー・モジュール１０８を受け取ることができる。ユーザ１１４はまた、図２に関連して以下で説明する、セキュア・コンテンツへのアクセスのためのユーザ認証および許可を与える識別モジュールも受け取ることができる。ユーザ１１４は、スクリーナ・キー・モジュール１０８および識別モジュールを使用して、コンテンツ媒体１１２上のセキュア・コンテンツを閲覧することができる。

【００２６】

図２に、セキュア・コンテンツの閲覧を可能にする例示的装置のブロック図を示す。簡単に言うと、セキュア・プレーヤ２００は、図１のコンテンツ媒体１１２およびスクリーナ・キー・モジュール１０８と、識別モジュールとを受け、コンテンツ媒体１１２上のセキュア・コンテンツの閲覧を可能にするように構成される。従って、ユーザ１１４は、テレビジョン機器、デジタル・レコーダ、セットトップ・ボックス、セルラ電話、モバイル装置、ＰＤＡ、パーソナル・コンピュータ、ジュータボックス、ハイブリット・インターネット音楽プレーヤ／ホーム・ステレオ・コンポーネント・システムなどの中にある、またはそれらに結合されたセキュア・プレーヤ２００を使用することができる。

【００２７】

図２に示すように、セキュア・プレーヤ２００は、図示するよりも多くの構成要素を含むことができる。しかし、図示する構成要素は、本発明を実施する例示的実施形態を開示するのに十分である。

【００２８】

図に示すように、セキュア・プレーヤ２００は、媒体ドライブ２０２、メディア・プレーヤ・サブシステム２０４、暗号解読エンジン２０６、コンプレッサ／デコンプレッサ（COmpressor/DECompressor）（ＣＯＤＥＣ）２０８、キー・ストア／マネージャ２１０、スクリーナ・キー・モジュール１０８、キー・ローダ２１４、識別モジュール２１６、認証モジュール２１８、タンパ（tamper）・エージェント２２０、およびコピー防止保護装置２２２（オプション）を含む。図１に示す構成要素と同様に番号付けした構成要素は実

質的に同様に動作する。

【００２９】

メディア・プレーヤ・サブシステム２０４は、媒体ドライブ２０２および暗号解読エンジン２０６と通信する。暗号解読エンジン２０６はＣＯＤＥＣ２０８およびキー・ストア／マネージャ２１０とも通信する。ＣＯＤＥＣ２０８は、オプションのコピー防止保護装置２２２と通信する。キー・ストア／マネージャ２１０は更に、キー・ローダ２１４と通信する。キー・ローダ２１４は、スクリーナ・キー・モジュール１０８および認証モジュール２１８と通信する。認証モジュール２１８は識別モジュール２１６とも通信する。タンパ・エージェント２２０は、暗号解読エンジン２０６、ＣＯＤＥＣ２０８、キー・ストア／マネージャ２１０、メディア・プレーヤ・サブシステム２０４、認証モジュール２１８、およびキー・ローダ２１４と通信する。

【００３０】

媒体ドライブ２０２は、図１のコンテンツ媒体１１２を受けるように構成される実質的に何れの装置および関連ソフトウェアも含む。そのような装置は、限定はしないがＤＶＤドライブ、高精細度ＤＶＤドライブ、スーパービデオＣＤ（ＳＶＣＤ）ドライブ、ＶＣＤドライブ、スーパー・オーディオＣＤ（ＳＡＣＤ）ドライブ、およびその他のコンテンツ媒体装置を含む。例えば、媒体ドライブ２０２は、ダイナミック・デジタル・サウンド（ＤＤＳ）ドライブでもよい。更に、媒体ドライブ２０２は、ＤＶＤ／ＲＷドライブなどを介しての書込み機能もサポートすることができる。しかし、媒体ドライブ２０２およびメディア・プレーヤ・サブシステム２０４はＤＶＤおよびＣＤの技術に限定されず、本発明の精神の範囲から逸脱することなく実質的にその他の何れのコンテンツ媒体技術も使用することができる。

【００３１】

メディア・プレーヤ・サブシステム２０４は、媒体ドライブ２０２と共に動作して、媒体ドライブ２０２でサポートされるコンテンツ媒体からセキュア・コンテンツを得て、それを暗号解読エンジン２０６へ提供することができる。更に、メディア・プレーヤ・サブシステム２０４および媒体ドライブ２０２は、コンテンツ媒体の消去、破壊、上書きなどを可能にする機能を含むことができる。例えば、メディア・プレーヤ・サブシステム２０４は、所定の閲覧回数、例えば一回の閲覧の後や、許可されていない活動が示された後などに、コンテンツ媒体上のセキュア・コンテンツの消去、破壊、使用不可とすることなどを可能にする。

【００３２】

ＣＯＤＥＣ２０８は、圧縮されたコンテンツを受け取り、それをユーザが楽しむためにレンダリングすることのできるフォーマットへと圧縮解除（解凍）するように構成された様々な圧縮／解凍機構のいずれかを含む。例えば、ＣＯＤＥＣ２０８は、ＭＰＥＧ（Moving Picture Experts Group）、ＪＰＥＧ（Joint Photographic Experts Group）、ウェーブレット、および受け取ったコンテンツの圧縮および解凍のためのその他の機構を使用することができる。

【００３３】

キー・ローダ２１４は、スクリーナ・キー・モジュール１０８からスクリーナ・キーを取り出す要求を受け取ることを可能にされる。キー・ローダ２１４は、要求を評価して、スクリーナ・キーを取り出すのに十分な許可（authorization）をユーザが有するかどうかを判定する。キー・ローダ２１４は、そのような許可を認証モジュール２１８に要求することができる。キー・ローダ２１４は、その許可に関する要求の一部として、コンテンツ識別子またはその他の情報を認証モジュール２１８へ提供することができる。更に、キー・ローダ２１４は、スクリーナ・キー・モジュール１０８へ１または複数のスクリーナ・キーおよびその他の情報をロードする要求を受け取ることができる。この場合も、キー・ローダ２１４は、そのような措置に対する許可について、認証モジュール２１８に要求することができる。

【００３４】

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0391
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

認証モジュール２１８は，ユーザを認証し、スクリーナ・キー・モジュール１０８への許可されたアクセスを与えるように構成される。認証モジュール２１８は，スクリーナ・キー・モジュール１０８に在るスクリーナ・キーにアクセスするためにキー・ローダ２１４から要求を受け取る。認証モジュール２１８は、スクリーナ・キー・モジュール１０８に情報を格納するための要求も受け取ることができる。いずれにしても、認証モジュール２１８は、識別モジュール２１６を使用して、ユーザのＩＤと，スクリーナ・キー・モジュール１０８へアクセスするための関連の許可とを判定する。

【００３５】

識別モジュール２１６は、ユーザのＩＤと，コンテンツ識別子やユーザなどに関連する資格および権利を与えるように構成される。限定はしないがバイオメトリクス、スマートカード、ユーザ名／パスワード、タッチ・パッド・コード・エントリなどを含む様々な機構を使用して，識別モジュール２１６を配備することができる。一実施形態では、識別モジュール２１６は、セキュア・プレーヤ２００の実質的に何れのユーザも実質的に何れの任意のセキュア・コンテンツに対して認証されることを可能にするように、構成される。

【００３６】

キー・ストア／マネージャ２１０は、スクリーナ・キー、セキュア・プレーヤ２００の公開／秘密鍵、関連情報などを含む暗号化／暗号解読鍵を格納および管理するように構成される。関連情報は、スクリーナ・キー、ユーザ、コンテンツ、スクリーナ・キーとユーザとコンテンツとの任意の組合せなどのうち少なくとも１つに関連する資格，権利などを含むことができる。キー・ストア／マネージャ２１０は、セキュア（安全）に鍵および関連情報を格納および管理するように構成されたデータベースまたはフラット・データ・ファイルなどを含むことができる。キー・ストア／マネージャ２１０は、コンテンツ識別子を使用して、スクリーナ・キーおよび関連情報を索引付けする。

【００３７】

キー・ストア／マネージャ２１０は、典型的には、暗号解読エンジン２０６がスクリーナ・キーの暗号解読／暗号化のためにセキュア・プレーヤ２００の秘密／公開鍵を要求するまで、それらを安全に保持する。しかし、キー・ストア／マネージャ２１０は、セキュア・プレーヤの秘密鍵がセキュア・プレーヤ２００内での使用を超えて利用可能とならないことを保証するように、構成される。

【００３８】

キー・ストア／マネージャ２１０は、受け取ったスクリーナ・キーを暗号解読エンジン２０６が暗号化コンテンツの暗号解読のために要求するまで，その受け取ったスクリーナ・キーを安全に格納する。キー・ストア／マネージャ２１０は、キー・ローダ２１４に対して要求を行うことによってスクリーナ・キー・モジュール１０８からスクリーナ・キーを取り出すことができる。キー・ストア／マネージャ２１０はまた、スクリーナ・キーがスクリーナ・キー・モジュール１０８から取り出されたときに、キー・ローダ２１４に対して、スクリーナ・キー・モジュール１０８を非活動化するように指示することもできる。キー・ストア／マネージャ２１０は更に，関連するセキュア・コンテンツの所定の回数の閲覧、無許可の活動などのイベントに基づいて，キー・ローダ２１４がスクリーナ・キー・モジュール１０８上のスクリーナ・キーを消去または使用不能にするように、指示することができる。

【００３９】

キー・ストア／マネージャ２１０はまた，セキュア・プレーヤ２００の公開鍵を使用して、スクリーナ・キー・モジュール１０８へロードされるスクリーナ・キーを暗号化することができる。

【００４０】

暗号解読エンジン２０６は、メディア・プレーヤ・サブシステ２０４からコンテンツ・ユニットのストリームを受け取るように構成される。少なくとも１つのコンテンツ・ユニットを受信すると、暗号解読エンジン２０６は、コンテンツ・ユニットが暗号化されているか否かを判定する。コンテンツ・ユニットが暗号化されている場合、暗号解読エンジン

Netflix, Inc. and Hulu, LLC - Ex. 1004, Page 0392
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)