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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 March 2008 (06.03.2008)

PCT

(10) International Publication Number
WO 2008/027774 A1

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

(21) International Application Number:
PCT/US2007/076590

(22) International Filing Date: 23 August 2007 (23.08.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/469,627 1 September 2006 (01.09.2006) US

(71) Applicant *(for all designated States except US)*: **NBC UNIVERSAL, INC.** [US/US]; 30 Rockefeller Plaza, New York, NY 10112 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **NG, Sheau** [US/US]; 26 Campbell Road, Wayland, MA 01778 (US). **MANDEL, Bill** [US/US]; 13708 Stagecoach Trail, Moorpark, CA 93021 (US). **REITMEIER, Glenn, Arthur** [US/US]; 193 Cinnabar Lane, Yardley, PA 19067 (US).

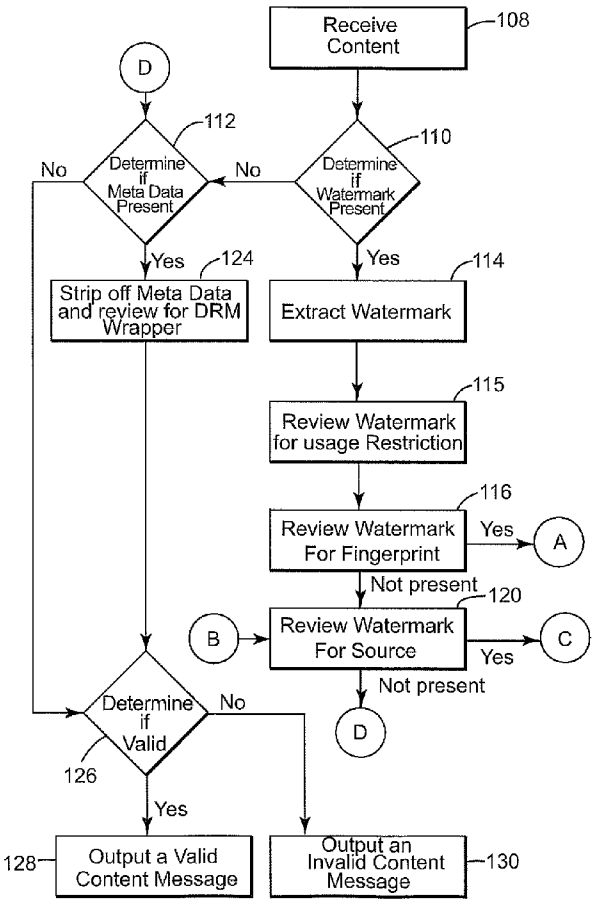
(74) Agents: **PHILLIPS, Roger, C.** et al.; General Electric Company, Global Patent Operation, 187 Danbury Road, Suite 204, Wilton, CT 06897 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL,

[Continued on next page]

(54) Title: CONTENT VALIDATION FOR DIGITAL NETWORK



(57) Abstract: A method of validating content for use on at least one node of a network, includes identifying whether the content has at least one adjunct; reviewing the at least one adjunct, where found, to determine whether the content is valid for use on the at least one node; and indicating that the content is unauthorized for use on the at least one node where no adjunct is found and/or where an adjunct is found that is not able to render the content valid for use on the at least one node.

WO 2008/027774 A1

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

Declarations under Rule 4.17:

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

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

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

Content Validation for Digital Network

Background of the Invention

Field of the Invention

[001] The subject matter described herein relates generally to networks and, more particularly, to the validation of content entering a node.

Related Art

[002] Various methods and devices are currently available for adding and/or modifying an adjunct to digital data content. For example, International Publication No. WO 2005/043358 describes recording content distribution information into authorized copies of content by modifying an adjunct to content with content distribution information. This is accomplished using a functional transformation each time an authorized copy of the content is generated. By modifying the adjunct to content, a trail of content distribution information is stored in the adjunct that is extractable from the adjunct in any of such generated copies by sequentially performing an inverse transformation on the adjunct until information of an original copy is detected.

[003] In another example, U.S. Patent No. 6,507,299 to Nuijten describes an arrangement for embedding supplemental data such as a watermark in an information signal. The arrangement involves a conventional sigma-delta modulator for encoding an audio signal and modifying means for periodically replacing a bit of the encoded signal by a bit of the watermark. In the same manner, a sync pattern is

embedded in the signal. The sync bits are embedded at a smaller distance than the watermark bits. The sync pattern is a pattern of contiguous bits that is not typically generated by the encoder. For the sigma-delta modulator, such a pattern is a run of ones followed by a substantially equally long run of zeroes, or vice versa.

[004] Also, adjuncts to digital data content may be added to authenticate data on a computer. International Publication No. WO 2004/111752 describes a method for providing authentication data and data authentication software to an electronic device that is stored in a secure storage location inaccessible to the user or operating system of the device. When digital data is requested from a transaction party that requests a digital signature, the authentication software is activated to generate the digital signature and embeds the digital signature in the digital data. Digital data digitally signed may only be accessed if the embedded digital signature is identical to a regenerated digital signature that is regenerated by the authentication software, using user inaccessible authentication data installed on the device. If the embedded and regenerated digital signatures are not identical, the data may not be accessed and an error signal is generated.

[005] However, to date, no suitable device or method is available for validating digital data content entering a node of a network.

Brief Description of the Invention

[006] In accordance with an embodiment of the present invention, a method of validating content for use on at least one node of a network comprises identifying whether the content comprises at least one adjunct; reviewing the at least one

adjunct, where found, to determine whether the content is valid for use on the at least one node; and indicating that the content is unauthorized for use on the at least one node where no adjunct is found and/or where an adjunct is found that is not able to render the content valid for use on the at least one node.

[007] In accordance with another aspect of the present invention, a circuit for validating content entering at least one node of a network comprises a display, a memory and means for identifying whether the content comprises an adjunct. The identifying means also being configured to indicate whether the content is unauthorized for use on a node where no adjunct is found and/or where an adjunct is found that is not able to render the content valid for entry to the at least one node. The identifying means being interconnected with the display and the memory.

Brief Description of the Drawings

[008] The following detailed description is made with reference to the accompanying drawings, in which:

[009] Figure 1 is a flow diagram showing a method of validating content on a network in accordance with an embodiment of the present invention;

[010] Figure 2 is a flow diagram showing further details of the method of Figure 1;

[011] Figure 3 is a block diagram of a circuit for validating content on a network in accordance with the embodiment of Figure 1;

[012] Figure 4 is a flow diagram showing further details of the method of Figure 1; and

[013] Figure 5 is a flow diagram showing further details of the method of Figure 1.

Detailed Description of the Preferred Embodiment

[014] One embodiment of the present invention concerns a method and a device for validating content such as digital data entering a node of a network. The content is reviewed to determine whether an adjunct is present and, where present, whether it provides a sufficient basis for validating the content for use on the node and throughout the network.

[015] As used herein, the term adjunct refers to something that is associated with the content but not an underlying work. Adjuncts commonly contain information about the content and/or rights associated with the content. Examples of adjuncts include meta data included in a carrier containing rights associated with the content such as in a digital rights management (DRM) wrapper, a watermark that is added or embedded in the content, or a signature such as a digital signature or a message that is related to the content, added to, joined with, or otherwise associated to the content.

[016] As used herein the term content refers to any data compilation such as audio and/or video data, for example comprising a film composition, a musical composition, a game, etc.

[017] As used herein the term watermark refers to any information embedded in a content that concerns the content but is separable from the work of the content. The watermark may be in a video format and/or an audio format and the watermark(s) may be visible, such as the NBC PEACOCK logo visible on a display during playback, and/or on that is invisible during playback. Likewise, the watermark(s) may

be audible and/or inaudible during playback. A watermark may also contain information as to prior transferor(s) that the content was transferred from.

[018] Referring now to Figure 3, a circuit for validating content in accordance with one embodiment of the present invention is illustrated generally at 10. In this embodiment, the circuit 10 is located at a node 8 and comprises an input/output control 12, a display 14, at least one peripheral 16, and an analog to digital converter 18. The input/output control 12 is any known device that is capable of providing communication between the node 8 and a network router 20 (also a known device) via a wired or wireless path 22. The network router 20 is also interposed in a known manner between the Internet 24 and additional nodes 26 and 28 via wired or wireless paths 30, 32 and 34. It will be understood that while two additional nodes are shown, any number of nodes are contemplated in optional embodiments of the present invention. The display 14, the peripheral 16, e.g., a compact disk (CD) or a digital versatile disk (DVD) drive and the analog to digital converter 18 are also well known devices. The peripheral 16 may comprise multiple CD and/or DVD drives or other known or future developed devices and communicates with the analog to digital converter via a wired or wireless connection 35.

[019] In accordance with this embodiment, the circuit 10 also comprises a processor 36 and associated memory 38, a stripper 40 and an extractor 42. Although not described herein, it will be understood that in an optional embodiment, the processor 36 may also be configured to provide the below described function of the stripper 40 and/or the extractor 42 via, e.g., additional software.

[020] Also, in accordance with this embodiment, the processor 36 is connected to each of the input/output control 12, the display 14, the analog to digital converter 18 and the memory 38 via paths 44, 46, 48 and 50. The processor 36 comprises, e.g., a known integrated circuit capable of numerous calculations per second and is configured to process, as described in more detail below, content received from the peripheral 16 and/or input/output control 12. The processor 36 is configured to provide an indication as to whether the content is valid for entry to the node 8, such as for viewing on the display 14, and, where not valid, to provide a message to the other nodes 26 and 28.

[021] The stripper 40 communicates with the processor 36 via a path 52 and similar to the processor 36 comprises, in one embodiment, an integrated circuit that is configured to receive the content from the processor and determine whether the content comprises meta data such as a digital rights management (DRM) wrapper. A DRM wrapper may provide copy control information indicating whether the content may be copied and/or how many times it may be copied.

[022] Where a DRM wrapper is determined to be present in the content, the stripper 40 then strips and reads the data to determine whether there are sufficient rights granted for use on the node 8. This may be accomplished by the steps described below. Additional details of a process for validating rights available in a DRM wrapper is available in PCT Publication No. WO 2005/043358, incorporated herein by reference only to the extent necessary to make and practice the present invention.

[023] In another embodiment, the stripper 40 may comprise a special-purpose high-speed Digital Signal Processor (DSP) or general-purpose processor including embedded processor logic such as ARM or MIPS based architecture.

[024] The extractor 42 communicates with the processor 36 via a path 54 and also similar to the processor 36 comprises, in one embodiment, an integrated circuit that is configured to receive the content from the processor and determine whether the content has information such as a watermark embedded therein. As described above, the content may include video and/or audio watermarks that are visible and/or invisible and audible and/or inaudible during playback.

[025] If a watermark is determined to be present, the extractor 42 extracts the watermark and reads the watermark to determine what information is provided. For example, the watermark may assert that there must be rights associated with the content that bears the particular watermark, the watermark may specify usage restrictions such as that the content is "not for home use" or the watermark may identify the source of the content and/or any previous transferors of the watermark. This may be accomplished in functional steps as described below.

[026] In another embodiment, the extractor 42 may comprise circuit components used in an audio Digital Signal Processor (DSP) such as that described in U.S. Patent Nos. 5,940,135, 6,430,301, 6,737,957 and 7,046,808 assigned to the Verance Corporation also incorporated herein by reference to the extent necessary to make and use the present invention.

[027] Referring now to Figure 1, a method of validating content in accordance with an embodiment of the present invention is illustrated generally at 100. In this

embodiment, the method 100 comprises identifying whether the content comprises at least one adjunct at 102. Thereafter, reviewing the at least one adjunct, where found, to determine whether the content is valid at 104 for entry to a node and, then, outputting an indication that the content is unauthorized for use on the node where either no adjunct is found or where the content is not determined to be valid 106.

[028] Further details of the method of this embodiment of Figure 1 are shown in Figure 2. As shown, digital data content is first received at 108 and then may be reviewed for whether a watermark is present at 110. Where a watermark is found not to be present, in this embodiment, it is next questioned whether meta data, such as a DRM wrapper is present at 112, as described further below. While not illustrated herein, it will be appreciated that the order of determining whether a watermark is present or whether meta data is present may be accomplished in either order or contemporaneously. Also, it will be apparent that the order of many of the additional steps described below may be interchanged or accomplished contemporaneously.

[029] In the event that a watermark is found to be present in the content, then it is next extracted at 114 and then it may be reviewed for usage restrictions at 115. Next, the watermark may be reviewed for a "fingerprint" or an indication of one or more prior transferor's information at 116. Thereafter, if available, as shown in Figure 4, the prior transferor(s) are identified at 118. Once the prior transferors are identified or no fingerprint is identified, the watermark may be reviewed for an indication of the source of the underlying work at 120 and, if available, the source is identified at 122 as illustrated in Figure 5.

[030] Thereafter, and not having previously determined if metadata is present at

112, it is determined whether metadata is present and where available the metadata is reviewed at 124 for a DRM wrapper. Next, a decision function is carried out to take the information stripped and extracted from the adjunct and make a flexible determination whether the content is valid for entry to the node 8 at 126. For example, it may be determined whether the rights granted are sufficient to allow use of the content by the node 8, whether the usage restrictions given can be met through use on the node, or whether a transferor is identified and compared with the rights granted in the DRM. Other decisions include restriction on storage of the content, duplication of the content, and transcoding including format conversion of the content. A restriction is typically a time-related restriction, such as one that renders the content valid for a particular duration of time.

[031] Where the content is determined to be valid at 126 for one or more particular processing procedures (such as storage, duplication, decoding, transcoding/format conversion, or rendition thereof), a proper signal will be sent with the content to display 14 by the processor 36 that there is valid content for entry to the node 8 at 128. Similarly, signals are also sent to the other nodes 26 and 28. Otherwise, a signal is sent to the display that the content is invalid and the other network nodes are notified that the content is invalid at 130, and a proper signal indicating the content status of invalidity is attached to the content.

[032] In the present embodiment, the processor may be configured to carry out the operations described at 108, 126, 128 and 130, the stripper may be configured to carry out the operations described at 112 and 124 and the extractor 42 may be configured to carry out the operations at 110, 114, 115, 116, 118, 120 and 122.

[033] Technical effects of the herein described systems and methods include determining whether the content entering a node is self-validating. Other technical effects include determining whether the content comprises an adjunct and, if so, whether the adjunct comprises metadata and/or a watermark.

[034] While the present invention has been described in connection with what are presently considered to be the most practical and preferred embodiments, it is to be understood that the present invention is not limited to these herein disclosed embodiments. Rather, the present invention is intended to cover all of the various modifications and equivalent arrangements included within the spirit and scope of the appended claims.

What is Claimed is:

1. A method of validating content for use on at least one node of a network, comprising:

identifying whether the content comprises at least one adjunct;

reviewing the at least one adjunct, where found, to determine whether the content is valid for use on the at least one node; and

indicating that the content is unauthorized for use on a node where no adjunct is found and/or where an adjunct is found that is not able to render the content valid for use on the at least one node.

2. The method of claim 1, wherein identifying whether the content comprises an adjunct comprises at least one of determining whether there is meta data attached to the content and determining whether there is information embedded in the content.

3. The method of claim 2, wherein determining whether there is meta data attached to the content comprises determining whether the content comprises a digital rights management wrapper.

4. The method of claim 2, wherein determining whether there is information embedded in the content comprises determining whether the content comprises a watermark.

5. The method of claim 2, wherein determining whether there is information embedded in the content comprises determining whether the content comprises at least one of a video watermark and an audio watermark.

6. The method of claim 2, wherein reviewing the at least one adjunct, where found, to determine whether the content is valid comprises identifying whether the at least one adjunct provides a source of the content.

7. The method of claim 2, wherein reviewing the at least one adjunct, where found, to determine whether the content is valid comprises identifying whether the at least one adjunct provides restrictions on use on the node.

8. The method of claim 2, wherein reviewing the at least one adjunct, where found, to determine whether the content is valid comprises identifying whether the at least one adjunct provides rights associated with the content that allows use on the node.

9. The method of claim 2, wherein the at least one adjunct comprises a plurality of adjuncts and wherein reviewing the at least one adjunct, where found, to determine whether the content is valid comprises:

identifying whether a first adjunct provides rights associated with the content; and

identifying whether a second adjunct provides a restriction on use of the content.

10. The method of claim 2, wherein reviewing the at least one adjunct, where found, to determine whether the content is valid comprises identifying whether the at least one adjunct grants any transfer rights and identifying whether the at least one adjunct provides at least one prior transferor and comparing the transfer rights with the prior transferor to determine if the content was validly transferred.

11. The method of claim 2, wherein reviewing the at least one adjunct, where found, to determine whether the content is valid comprises identifying at least one of whether the at least one adjunct provides rights associated with the content and whether the at least one adjunct provides a restriction on use of the content; and

further comprising identifying whether the at least one adjunct provides a prior location the content was transferred from and comparing the rights associated with the content or the restriction on use of the content with the prior location to determine if it was transferred according to the rights or restrictions.

12. The method of claim 2, further comprising a plurality of nodes of a network and wherein outputting an indication that the content is unauthorized comprises at least one of indicating that the content may not be run on the node, notifying other nodes in the network that this content is not valid for use on any of the nodes of the network and preventing transfer of the content to other nodes.

13. The method of claim 12, further comprising outputting an indication that the content is authorized where found to be valid.

14. The method of claim 1, wherein the content comprises digital data.

15. The method of claim 4, wherein the watermark is visible.

16. A circuit for validating content entering at least one node of a network, comprising:

a display;

a memory;

means for identifying whether the content comprises an adjunct and for indicating whether the content is unauthorized for use on a node where no adjunct is found and/or where an adjunct is found that is not able to render the content valid for use on the at least one node, the identifying means being interconnected with the display and the memory.

17. The circuit of claim 16, wherein the identifying and indicating means comprises a processor interconnected with the display.

18. The circuit of claim 17, wherein the identifying and indicating means further comprises a stripper communicating with the processor, the stripper being configured

to identify meta data in the content and then the strip meta data from the content for communication to the processor.

19. The circuit of claim 18, wherein the identifying and indicating means further comprises an extractor communicating with the processor, the extractor being configured to identify embedded information in the content and then extract the embedded information in the content for communication to the processor.

20. The circuit of claim 19, wherein the processor is further configured to communicate whether the content is valid to other nodes in the network.

21. A method of validating content for use on at least one node of a network, comprising:

identifying whether the content comprises at least one adjunct;

reviewing the at least one adjunct, where found, to determine whether the content is valid for use on the at least one node; and

indicating that the content is unauthorized for use on a node where an adjunct is found that is not able to render the content valid for use on the at least one node.

Fig. 1

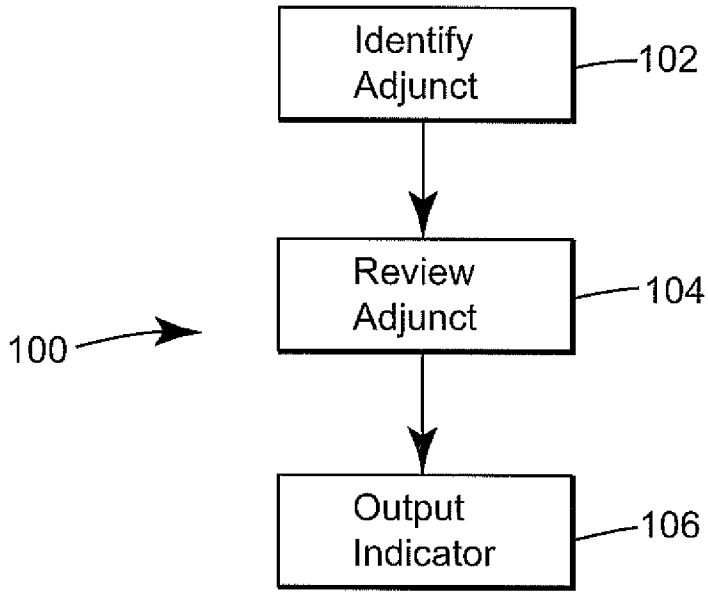
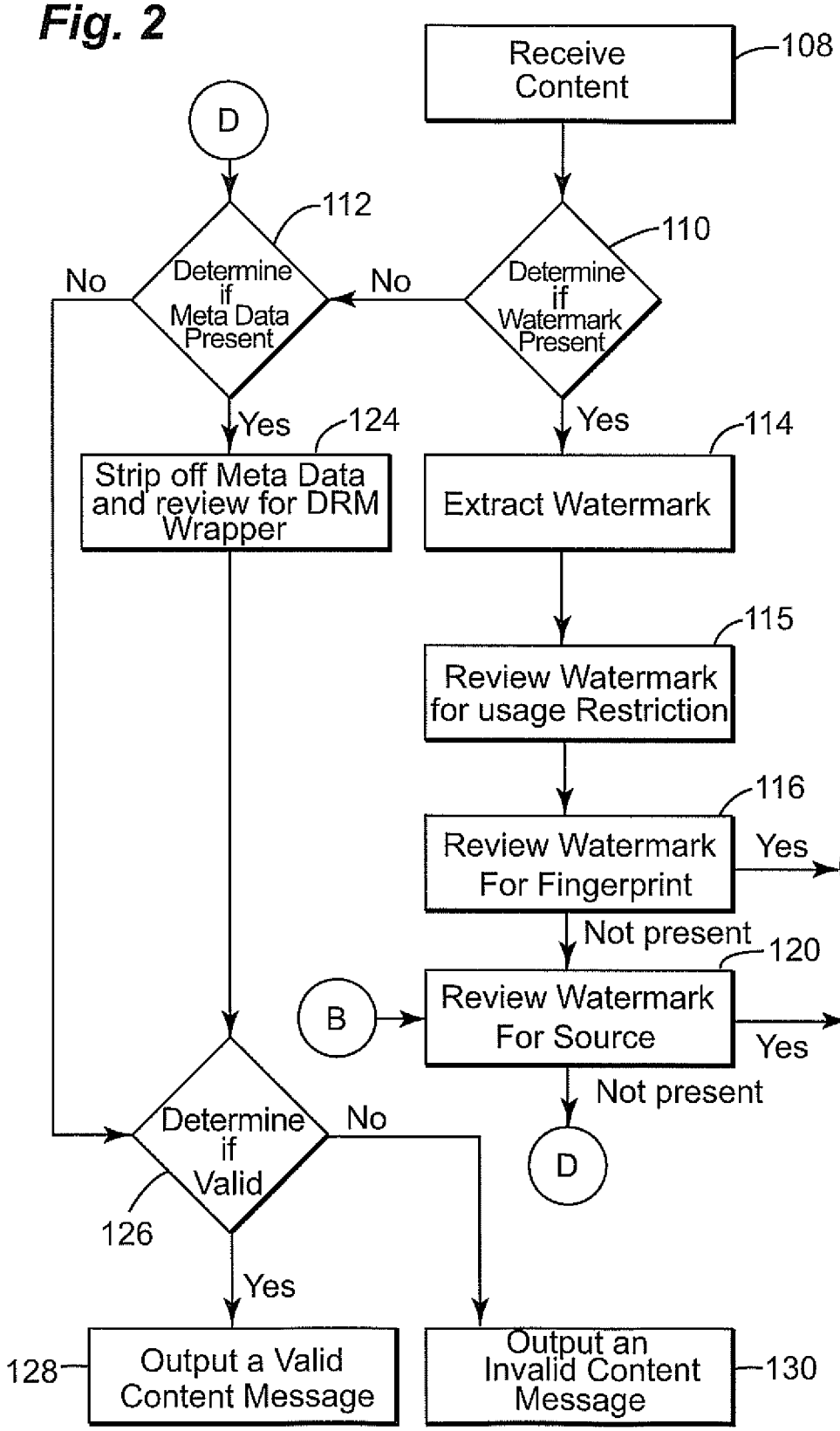

Identify Adjunct
102
Review Adjunct
104
100
Output Indicator
106

Fig. 2


Receive Content
108
D
112
Determine if Meta Data Present
110
Determine if Watermark Present
No
No
Yes
124
Yes
114
Strip off Meta Data and review for DRM Wrapper
Extract Watermark
115
Review Watermark for usage Restriction
116
Review Watermark For Fingerprint
Yes
A
Not present
120
B
Review Watermark For Source
C
Yes
Not present
D
Determine if Valid
No
126
Yes
128
Output a Valid Content Message
Output an Invalid Content Message
130

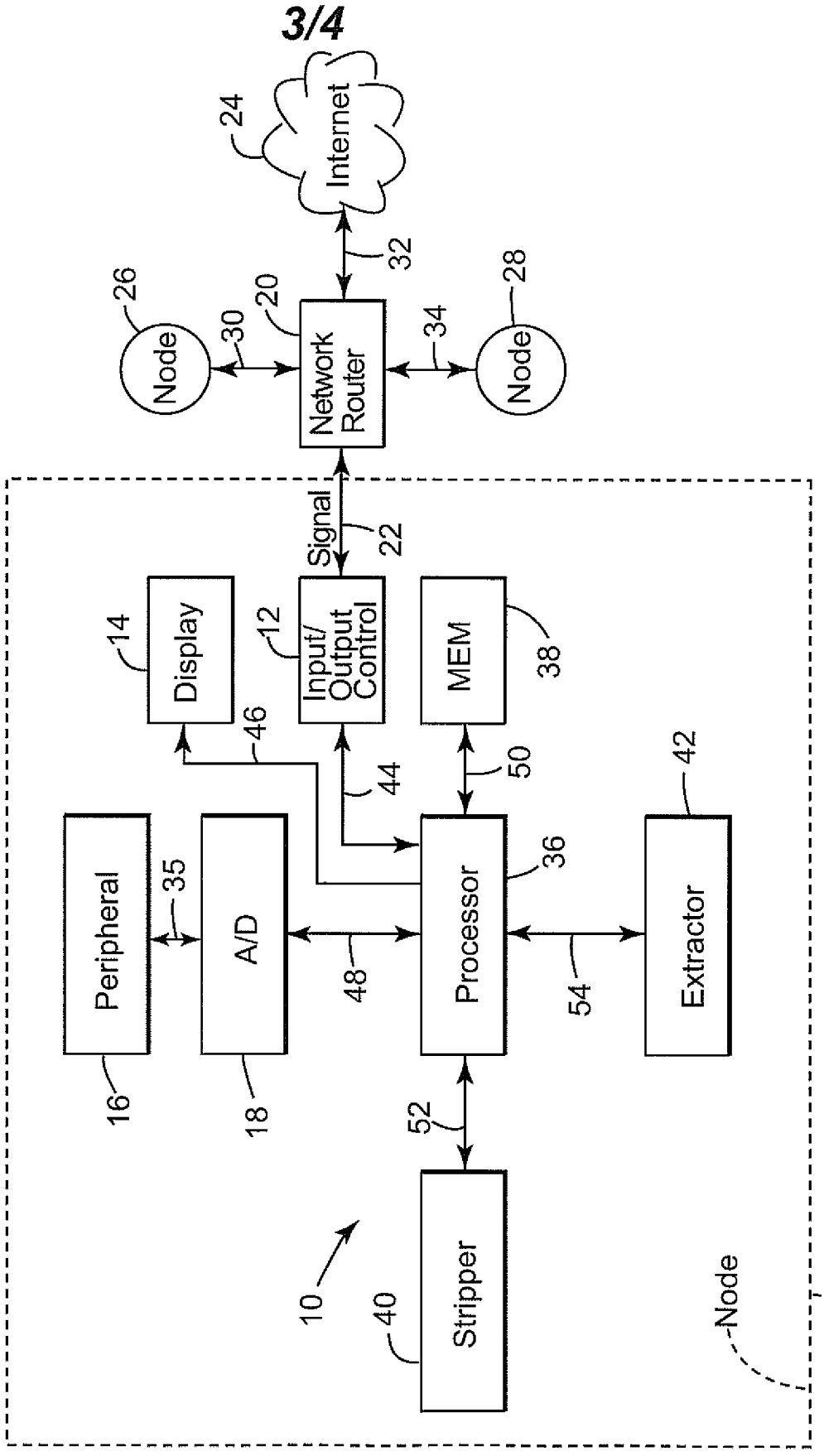

Internet
24
32
Node
26
30
20
Network Router
34
Node
28
Signal
22
Display
14
Input/ Output Control
12
MEM
38
46
44
50
42
Peripheral
35
A/D
48
Processor
36
54
Extractor
16
18
52
10
Stripper
40
Node
8

Fig. 3

Fig. 4

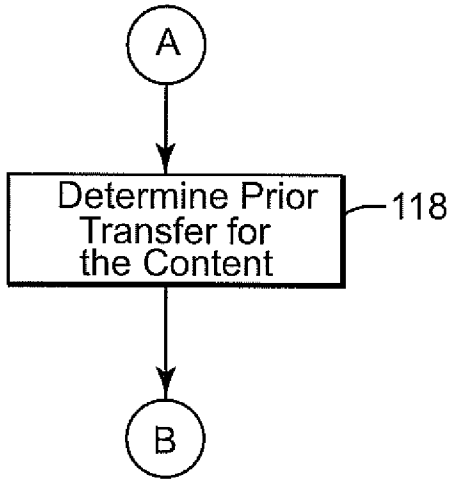
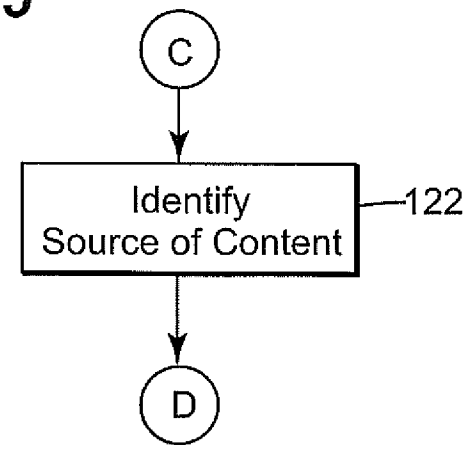

A
Determine Prior Transfer for the Content
118
B

Fig. 5


C
Identify Source of Content
122
D

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2007/076590

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00

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)
G06F

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2006/051043 A (THOMSON LICENSING [FR]; DURAND ALAIN [FR]; TANG-TALPIN YAN-MEI [FR]) 18 May 2006 (2006-05-18) page 5, column 35 - page 6, column 11 page 11, line 24 - page 12, line 26	1-21
X	WO 03/034408 A (NOKIA CORP [FI]; NOKIA INC [US]) 24 April 2003 (2003-04-24) page 2, line 14 - page 3, line 5 page 6, lines 5-12 page 9, lines 6-17 page 11, line 22 - page 12, line 3	1-21
X	WO 03/098931 A (KONINKL PHILIPS ELECTRONICS NV [NL]; KAMPERMAN FRANCISCUS L A J [NL];) 27 November 2003 (2003-11-27) page 16, line 30 - page 17, line 26	1-21

-/--

[X] Further documents are listed in the continuation of Box C.

[X] 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 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
14 December 2007	27/12/2007

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	Alecu, Mihail

2

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

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	"SDMI SECURE DIGITAL MUSIC INITIATIVE" SDMI PORTABLE DEVICE SPECIFICATION VERSION 1.0, XX, XX, no. PART 1, 8 July 1999 (1999-07-08), pages 1-35, XP000997330 pages 6-9 page 21	1-21
X	WO 03/083627 A (KONINKL PHILIPS ELECTRONICS NV [NL]; KAMPERMAN FRANCISCUS L A J [NL];) 9 October 2003 (2003-10-09) abstract page 1, lines 1,2 page 1, lines 23-30 page 2, lines 10-15 page 3, lines 19-35	1-21

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2007/076590

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 2006051043	A	18-05-2006	NONE		
WO 03034408	A	24-04-2003	AU	2002362952 A1	28-04-2003
			CN	1650559 A	03-08-2005
			EP	1444690 A2	11-08-2004
			US	2003076955 A1	24-04-2003
WO 03098931	A	27-11-2003	AU	2003228007 A1	02-12-2003
			CN	1656803 A	17-08-2005
			JP	2005526330 T	02-09-2005
			US	2005210261 A1	22-09-2005
WO 03083627	A	09-10-2003	AU	2003206088 A1	13-10-2003
			CN	1643474 A	20-07-2005
			JP	2005521934 T	21-07-2005
			US	2005177875 A1	11-08-2005