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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 March 2012 (22.03.2012)

PCT

(10) International Publication Number
WO 2012/037420 A2

(51) **International Patent Classification**:
G06F 21/20 (2006.01) *G06F 21/24* (2006.01)

(21) **International Application Number**:
PCT/US2011/051855

(22) **International Filing Date**:
15 September 2011 (15.09.2011)

(25) **Filing Language**: English

(26) **Publication Language**: English

(30) **Priority Data**:

61/383,693	16 September 2010 (16.09.2010)	US
13/080,598	5 April 2011 (05.04.2011)	US
13/080,605	5 April 2011 (05.04.2011)	US
13/080,593	5 April 2011 (05.04.2011)	US

(71) **Applicant** *(for all designated States except US)*: **VERANCE CORPORATION** [US/US]; 4435 Eastgate Mall, Suite 350, San Diego, CA 92121 (US).

(72) **Inventors; and**

(75) **Inventors/Applicants** *(for US only)*: **WINOGRAD, Joseph, M.** [US/US]; 4435 Eastgate Mall, Suite 350, San Diego, CA 92121 (US). **PETROVIC, Rade** [US/US]; 4435 Eastgate Mall, Suite 350, San Diego, CA 92121 (US). **ZHAO, Jian** [US/US]; 4435 Eastgate Mall, Suite 350, San Diego, CA 92121 (US).

(74) **Agent**: **TEHRANCHI, Babak**; Perkins Coie LLP, P.O. Box 1247, Seattle, WA 98111-1247 (US).

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

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,

[Continued on next page]

(54) **Title**: SECURE AND EFFICIENT CONTENT SCREENING IN A NETWORKED ENVIRONMENT

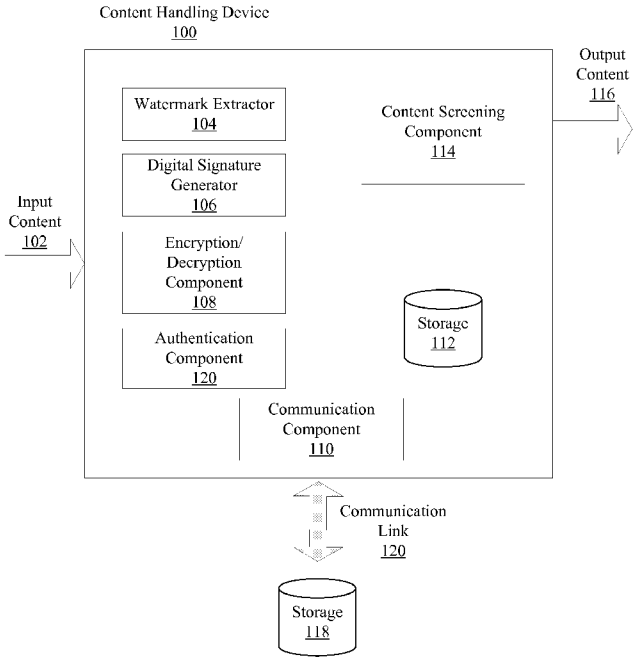

FIG. 1

(57) **Abstract**: Methods, devices, and computer program products facilitate the application of content usage rules based on watermarks that are embedded in a content. Watermark extraction and content screening operations, which can include the application of content usage enforcement actions, may be organized such that some or all of the operations can be conducted at different times by different devices. These operations can be conducted by one or more trusted devices that reside in a networked environment. The authenticity of various devices can be verified through the exchange of certificates that can further enable such devices to ascertain capabilities of one another. Based on the ascertained capabilities, an operational configuration for conducting watermark extraction and content screening can be determined.

WO 2012/037420 A2

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

Declarations under Rule 4.17:

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

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

SECURE AND EFFICIENT CONTENT SCREENING IN A NETWORKED ENVIRONMENT

RELATED APPLICATIONS

[0001] This application claims priority from U.S. Patent Application Nos. 13/080,593, 13/080,605, and 13/080,598, all of which were filed on April 5, 2011. Each of the before-mentioned patent applications claims benefit of U.S. Provisional Application No. 61/383,693 filed on September 16, 2010. The entire contents of the before-mentioned patent applications are incorporated by reference as part of the disclosure of this application.

FIELD OF INVENTION

[0002] The present invention generally relates to the field of content management. More particularly, the disclosed embodiments relate to efficient and secure extraction of watermarks from media content to enable content management.

BACKGROUND

[0003] This section is intended to provide a background or context to the disclosed embodiments that are recited in the claims. The description herein may include concepts that could be pursued, but are not necessarily ones that have been previously conceived or pursued. Therefore, unless otherwise indicated herein, what is described in this section is not prior art to the description and claims in this application and is not admitted to be prior art by inclusion in this section.

[0004] Digital watermarks have been proposed and used for copyright protection of signals such as audio, video, images and the like. In a typical watermarking scenario an auxiliary information signal is hidden within a host content in such a way that it is substantially imperceptible, and at the same time, difficult to remove without damaging the host content. The auxiliary information that is hidden within the host content can then allow content management to be carried out to varying degrees. In some embodiments, content management includes, but is not limited to, the management of the use of content in accordance with one or more policies. For example, the auxiliary information may merely convey that the host content is not allowed to be copied (i.e., a "no copy allowed" watermark). Once extracted and interpreted by a compliant device, copying of the content is prevented. A compliant device can include, but is not limited to, a device that performs

screening, or otherwise operates in a manner consistent with a content use policy. Content use (or the uses of content) can include, but is not limited to, operations involving content such as playback, copy, record, transfer, stream, or other operations. Additionally, or alternatively, the embedded auxiliary information can identify the rightful owner(s), author(s) and/or author(s) of the content or can provide a serial number associated with the content or other content identifying information. The auxiliary information can also be used for other applications, such as to monitor the usage of the embedded host content, resolve ownership disputes, and keep track of royalties and the like.

[0005] In order to extract and utilize the watermarks embedded in various content, substantial resources such as CPU cycles, digital memory, and communication resources may be engaged. This, in turn, can delay access to the content, increase the cost of manufacturing devices that are designed with a minimum processing load objective, increase battery consumption in mobile devices, etc. The processing burden associated with extracting such watermarks is often exacerbated by a need to perform certain additional content transformation operations, such as decryption, decompression, de-multiplexing, etc., that are must be performed before watermark extraction can be attempted.

SUMMARY OF THE INVENTION

[0006] This section is intended to provide a summary of certain exemplary embodiments and is not intended to limit the scope of the embodiments that are disclosed in this application.

[0007] The disclosed embodiments improve the efficiency of watermark extraction and the associated processing by reducing the overall resource engagement, utilizing spare resources whenever possible, and distributing resource engagement in time to achieve low peak requirements and optimize cost-performance tradeoff. These and other features of the disclosed embodiments are effected while maintaining appropriate levels of security associated with the usage of watermarks. The disclosed embodiments further enhance the capabilities of connected (e.g., networked) devices to effect watermark extraction, content screening and content management through cooperative efforts. Watermark extraction and content screening operations, which can include the application of content usage enforcement actions, may be organized such that some or all of the operations can be conducted at different times by different devices. Secure and efficient content watermark extraction and

content screening operations can be carried out by exchanging certificates between the various devices in a network. The exchanged certificates can further enable the exchange of device capabilities, thereby facilitating the allocation of operational configuration to conduct watermark extraction and content screening operations.

[0008] One aspect of the disclosed embodiments relates to a method that includes receiving a request for access to a content at a first device from a second device, where the first device operates in a network. This method further comprises performing device authentication to ascertain a trusted status associated with one or both of the first and second devices, and determining an operational configuration for performing watermark extraction and/or screening operations using of one or more trusted devices. In one embodiment, the second device is a trusted content client device, and the second device is configured to perform the watermark extraction and screening operations.

[0009] In another embodiment, the second device is also a trusted content client device. But in this embodiment, a trusted slave device is configured to perform the watermark extraction operation and provide information associated with the extraction information to the second device. Moreover, the second device is configured to perform the screening operation. In still another embodiment, where the second device is a trusted content client device, a trusted delegated device is configured to perform the watermark extraction and screening operations.

[0010] According to another embodiment, the first device is a trusted content server, and the first device is configured to perform the watermark extraction and screening operations. In another embodiment, the first device is similarly a trusted content server. However, in this embodiment, a trusted slave device is configured to perform the watermark extraction operation and provide information associated with the extraction information to the first device. Further, the first device is configured to perform the screening operation.

[0011] In another embodiment, where the first device is a trusted content server, a trusted delegated device is configured to perform the watermark extraction and screening operations. In yet another embodiment, the first device is a trusted content server and the second device is a trusted content client device. According to this embodiment, the first device is configured to perform the watermark extraction operation and the second device is configured to perform the screening operation.

[0012] In another embodiment, where the first device is a trusted content server and the second device is a trusted content client device, the second device is configured to perform the watermark extraction operation. In this embodiment, the first device is configured to perform the screening operation.

[0013] According to one embodiment, the network in the above described method is a home network. For example, such a home network can be a digital living network alliance (DLNA) network. While in another embodiment, the second device also operates in the network, in another embodiment, the second device operates outside of the network.

[0014] According to one embodiment, the first device is a non-compliant device and the second device is a compliant device. In another embodiment, the first device is a compliant device but the second device is a non-compliant device. In still another embodiment, both the first and the second devices are non-compliant devices.

[0015] Another aspect of the disclosed embodiments relates to a device that includes a processor and a memory, including processor executable code. The processor executable code when executed by the processor configures the device to receive a request for access to a content at a first device from a second device, where the first device operates in a network. The processor executable code when executed by the processor also configures the device to perform device authentication to ascertain a trusted status associated with one or both of the first and the second devices. The processor executable code when executed by the processor further configures the device to determine an operational configuration for performing watermark extraction and/or screening operations using one or more trusted devices.

[0016] Another aspect of the disclosed embodiments relates to a computer program product that is embodied on a non-transitory computer readable medium. The computer program product comprises program code for receiving a request for access to a content at a first device from a second device, the first device operating in a network. The computer program product also includes program code for performing device authentication to ascertain a trusted status associated with one or both of the first and the second devices. The computer program product further includes program code for determining an operational configuration for performing watermark extraction and/or screening operations using one or more trusted devices.

[0017] Another aspect of the disclosed embodiments relates to a device that comprises means for receiving a request for access to a content at a first device from a second device, the first device operating in a network and means for performing device authentication to ascertain a trusted status associated with one or both of the first and the second devices. Such a device further includes means for determining an operational configuration for performing watermark extraction and/or screening operations using one or more trusted devices.

[0018] Another aspect of the disclosed embodiments relates to a method that comprises receiving a request for access to a content at a gateway device configured to coordinate operations of a plurality of devices within a network. Such a request is received from a second device for access to the content that is accessible to the first device, where the first device is configured to operate within the network. Such a method further includes coordinating, at the gateway device, device authentication to ascertain a trusted status associated with one or both of the first and second devices, and determining, at the gateway device, an operational configuration for performing watermark extraction and content screening operations using of one or more trusted devices.

[0019] In one embodiment, the second device is a device that is configured to operate within the network, while in another embodiment, with the second device is a device that is configured to operate outside of the network. In another embodiment, the gateway device is configured to communicate with the one or more trusted devices to commence the watermark extraction and/or screening operations. In another example, the gateway device is configured to revoke a trusted status of a device within the network. In still other examples, the gateway device is configured to retain usage rules associated with embedded watermarks. In one variation, the gateway device is also configured to communicate the usage rules to various trusted devices.

[0020] Another aspect of the disclosed embodiments relates to a gateway device that comprises a processor, and a memory, comprising processor executable code. The processor executable code when executed by the processor configures the gateway device to receive a request for access to a content at the gateway device that is configured to coordinate operations of a plurality of devices within a network. The request is received from a second device for access to the content that is accessible to the first device, where the first device is configured to operate within the network. The processor executable code when executed by the processor further configures the gateway device to coordinate device authentication to

ascertain a trusted status associated with one or both of the first and second devices. The processor executable code when executed by the processor also configures the gateway device to determine an operational configuration for performing watermark extraction and content screening operations using of one or more trusted devices.

[0021] Another aspect of the disclosed embodiments relates to a computer program product, embodied on a non-transitory computer readable medium, that comprises computer code for receiving a request for access to a content at the gateway device that is configured to coordinate operations of a plurality of devices within a network. The request is received from a second device for access to the content that is accessible to the first device, where the first device is configured to operate within the network. The computer program product also comprises computer code for coordinating device authentication to ascertain a trusted status associated with one or both of the first and second devices, and computer code for determining an operational configuration for performing watermark extraction and content screening operations using of one or more trusted devices.

[0022] Another aspect of the disclosed embodiments relates to a device that comprises means for transmitting a request for access to a content from a second device to a first device, the first device operating in a network. This device also includes means for performing device authentication to ascertain a trusted status associated with the first device, and means for determining an operational configuration for performing watermark extraction and/or screening operations using one or more trusted devices.

[0023] Another aspect of the disclosed embodiments relates to a method that includes transmitting a request for access to a content from a second device to a first device, where the first device operating in a network. This method also includes performing device authentication to ascertain a trusted status associated with the first device, and determining an operational configuration for performing watermark extraction and/or screening operations using one or more trusted devices.

[0024] Another aspect of the disclosed embodiments relates to a device that comprises a processor and a memory, including processor executable code. The processor executable code when executed by the processor configures the device to transmit a request for access to a content from a second device to a first device, the first device operating in a network, and to perform device authentication to ascertain a trusted status associated with the first device.

The processor executable code when executed by the processor further configures the device to determine an operational configuration for performing watermark extraction and/or screening operations using one or more trusted devices.

[0025] Another aspect of the disclosed embodiments relates to a computer program product that is embodied on a non-transitory computer readable medium. The computer program product includes program code for transmitting a request for access to a content from a second device to a first device, where the first device operates in a network. The computer program product also includes program code for performing device authentication to ascertain a trusted status associated with the first and device, and program code for determining an operational configuration for performing watermark extraction and/or screening operations using one or more trusted devices.

[0026] An aspect of the disclosed embodiments relates to a method that comprises receiving a device authentication certificate at a first device from a second device and verifying an authenticity of the certificate. This method also includes ascertaining capabilities of the second device and determining an operational configuration for conducting watermark extraction and/or screening operations associated with a content. In one embodiment, the certificate contains information indicative of at least a portion of the capabilities of the second device. In one example, the certificate is a digital transmission content protection over Internet protocol (DTCP-IP) certificate, and the information regarding the capabilities of the second device is carried as part of that DCTP-IP certificate. In another embodiment, at least a portion of the capabilities of the second device is ascertained from a source other than the certificate. For example, at least a portion of the capabilities of the second device can be received through an additional communication with the second device.

[0027] According to another embodiment, the ascertained capabilities of the second device includes a capability to conduct some or all of the watermark extraction operation and/or content screening operations. In such a scenario, the operational configuration can designate the second device to perform at least one of the watermark extraction and content screening operations. In another embodiment, the ascertained capabilities of the second device include a capability to grant computational and memory resources to other devices.

[0028] In one embodiment, the above-noted method further includes receiving a device authentication certificate at the second device from the first device, verifying the authenticity of the certificate received from the first device and ascertaining capabilities of the first device. In one variation, the certificate that is received from the first device contains information indicative of at least a portion of the capabilities of the first device. In one example, the certificate that is received from the first device is a digital transmission content protection over Internet protocol (DTCP-IP) certificate and the information regarding the capabilities of the first device is carried as part of that DCTP-IP certificate. In another example, at least a portion of the capabilities of the first device is ascertained from a source other than the certificate. For instance, at least a portion of the capabilities of the first device can be received through an additional communication with the first device. In another embodiment, the ascertained capabilities of the first device comprise a capability to conduct some or all of the watermark extraction and/or content screening operations.

[0029] In one embodiment, the ascertained capabilities of the first device comprise a capability to grant computational and memory resources to other devices. In one variation, the determination of the operational configuration for conducting watermark extraction and/or screening operations is conducted in accordance with the ascertained capabilities of the first device and the second device. In another embodiment, the operational configuration designates the first device to perform at least one of the watermark extraction and the content screening operations. In still another embodiment, the operational configuration designates the first and the second devices to collaboratively perform the watermark extraction and the content screening operations.

[0030] According to another embodiment, the operational configuration designates at least one of the first and the second devices to conduct the watermark extraction and content screening operations in accordance with a factor selected from the group consisting of: availability of computational resources, availability of watermark extraction and screening capabilities, integration complexity for a device manufacturer, consumer experience, processing performance, and an overall preference ranking. In one embodiment, at least one of the first and second devices are configured to operate in a home network. For example, such a home network can be a digital living network alliance (DLNA) network.

[0031] Another aspect of the disclosed embodiments relates to a device that includes a processor and a memory, including processor executable code The processor executable

code when executed by the processor configures the device to receive a device authentication certificate at a first device from a second device and verify an authenticity of the certificate. The processor executable code when executed by the processor also configures the device to ascertain the capabilities of the second device and determine an operational configuration for conducting watermark extraction and/or screening operations associated with a content.

[0032] Another aspect of the disclosed embodiments relates to a computer program product that is embodied on a non-transitory computer readable medium. The computer program product comprises program code for receiving a device authentication certificate at a first device from a second device and program code for verifying an authenticity of the certificate. The computer program product also includes program code for ascertaining capabilities of the second device and program code for determining an operational configuration for conducting watermark extraction and/or screening operations associated with a content.

[0033] Another aspect of the disclosed embodiments relates to a device that comprises means for receiving a device authentication certificate at a first device from a second device and means for verifying an authenticity of the certificate. The device also includes means for ascertaining capabilities of the second device and means for determining an operational configuration for conducting watermark extraction and/or screening operations associated with a content.

[0034] Another aspect of the disclosed embodiments relates to a method that includes detecting an operation in a content handling device, where such an operation requires access to a content. The method also includes retrieving an existing watermark extraction record associated with the content and authenticating the content in accordance with the existing watermark extraction record. This method also includes effecting content screening in accordance with usage rules associated with the content. In one embodiment, the operation that requires access to the content can be at least one of: a copying operation, a transferring operation, a rendering operation, a playback operation and a recording operation.

[0035] In one embodiment, the existing watermark extraction record is retrieved from a location outside of the content handling device. In another embodiment such a location is at least one of: a private virtual locker on a cloud, a universal virtual locker on a cloud, a storage on a device that is compliant to DLNA (Digital Living Network Alliance) within a home network, a storage location within a digital living network alliance (DLNA) compliant

network, a storage location within another device that is communicatively connected to the content handling device and a removable computer-readable storage medium.

[0036] In another embodiment, the existing watermark extraction record comprises at least one of: an extracted watermark payload, a number of extracted watermarks, a time stamp associated with an extracted watermark payload, a content authentication information, a digital signature associated with the extraction record, the usage rules associated with the content, and an enforcement action associated with the usage rules and an extracted watermark payload.

[0037] In still another embodiment, at least one of the retrieval of the existing watermark extraction record and authentication of the content file fails, and the content is subjected to a new watermark extraction operation. In such an embodiment, the method can further include producing a new watermark extraction record. In such an embodiment, the usage rules can prescribe an enforcement action in accordance with a result of the new watermark extraction operation. For example, the prescribed enforcement action can be stored as part of the new watermark extraction record. In another embodiment, the usage rules prescribe an enforcement action in accordance with the existing watermark extraction record.

[0038] According to another embodiment, the content screening comprises at least one of: muting at least a portion of the content, blanking at least a portion of the content, displaying a copyright notice, denying access to the content, and deleting the content. In yet another embodiment, the content handling device is digital living network alliance (DLNA) compliant device.

[0039] In one embodiment, the operation that requires access to the content requires real-time access to the content. In this embodiment, the existing watermark extraction record comprises a segmented authentication information corresponding to a plurality of content segments, and the authentication is carried out for at least a segment of the content in accordance with the segmented authentication information. In such a scenario, the existing extraction information can accompany a streaming content. In one example, the segmented authentication information comprises a segmented hash value. In another example, the authentication is carried out for sequential segments of the content, while in a different example, the authentication is carried out for non-sequential segments of the content.

[0040] In one embodiment, the screening is effected by evaluating the information contained within the existing watermark extraction record in conjunction with content use information associated with a predetermined time period. For example, the content use information can comprise an extracted watermark payload and an associated time stamp within a time interval immediately preceding the detection of the operation that requires content access.

[0041] According to another embodiment, the operation that requires content access in the content handling device requires access to a plurality of contents, where one or more of the plurality of the contents have a size below a particular threshold. In this scenario, the content screening is effected by first concatenating the plurality of the contents with a size below the particular threshold and conducting a new watermark extraction operation on the concatenated content. The content screening is further effected by aggregating the results associated with the new watermark extraction operation and the information obtained from the existing watermark extraction record that correspond to one or more of the plurality of the contents with a size above or equal to the particular threshold. These operations are followed by producing an enforcement action in accordance the aggregated results.

[0042] Another aspect of the disclosed embodiments relates to a device that comprises a processor and a memory that includes processor executable code. The processor executable code when executed by the processor configures the device to detect an operation in a content handling device, where such an operation requires access to a content. The processor executable code when executed by the processor further configures the device to retrieve an existing watermark extraction record associated with the content. The processor executable code when executed by the processor also configures the device to authenticate the content in accordance with the existing watermark extraction record and effect content screening in accordance with usage rules associated with the content.

[0043] Another aspect of the disclosed embodiments relates to a computer program product that is embodied on a non-transitory computer readable medium. The computer program code comprises computer code for detecting an operation in a content handling device, where such an operation requires access to a content. The computer program product also includes computer code for retrieving an existing watermark extraction record associated with the content, computer code for authenticating the content in accordance with the existing

watermark extraction record, and computer code for effecting content screening in accordance with usage rules associated with the content.

[0044] Another aspect of the disclosed embodiments relates to a device that comprises means for detecting an operation in a content handling device, where such an operation requires access to a content. The device further comprises means for retrieving an existing watermark extraction record associated with the content. The device also includes means for authenticating the content in accordance with the existing watermark extraction record and means for effecting content screening in accordance with usage rules associated with the content.

[0045] These and other advantages and features of disclosed embodiments, together with the organization and manner of operation thereof, will become apparent from the following detailed description when taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0046] The disclosed embodiments are described by referring to the attached drawings, in which:

[0047] FIG. 1 is a block diagram of a content handling device in accordance with an example embodiment;

[0048] FIG. 2 is a flow diagram of certain watermark extraction and content screening operations in accordance with an example embodiment;

[0049] FIG. 3 is a flow diagram of certain watermark extraction operations in accordance with an example embodiment;

[0050] FIG. 4 illustrates a block diagram of a invocation model device configuration in accordance with an example embodiment;

[0051] FIG. 5 illustrates a block diagram of a delegation model device configuration in accordance with an example embodiment;

[0052] FIG. 6 illustrates a block diagram of a content server and content client device configuration in accordance with an example embodiment;

[0053] FIG. 7 illustrates an authentication procedure in accordance with an example embodiment;

[0054] FIG. 8 illustrates collaborative watermark extraction and content screening operation in accordance with an example embodiment;

[0055] FIG. 9 illustrates a block diagram of a content distribution architecture in accordance with an example embodiment; and

[0056] FIG. 10 illustrates a block diagram of an exemplary device that can accommodate the disclosed embodiments.

DETAILED DESCRIPTION OF CERTAIN EMBODIMENTS

[0057] In the following description, for purposes of explanation and not limitation, details and descriptions are set forth in order to provide a thorough understanding of the disclosed embodiments. However, it will be apparent to those skilled in the art that the present invention may be practiced in other embodiments that depart from these details and descriptions.

[0058] Additionally, in the subject description, the word "exemplary" is used to mean serving as an example, instance, or illustration. Any embodiment or design described herein as "exemplary" is not necessarily to be construed as preferred or advantageous over other embodiments or designs. Rather, use of the word exemplary is intended to present concepts in a concrete manner.

[0059] Some of the disclosed embodiments are described in the context of a Digital Living Network Alliance (DLNA) compliant network. DLNA is a cross-industry organization of leading consumer electronics, computing industry and mobile device companies. DLNA's vision is a wired and wireless network of interoperable consumer electronics (CE), personal computers (PC) and mobile devices in the home and on the road, enabling a seamless environment for sharing and growing new digital media and content services. DLNA is focused on delivering interoperability guidelines based on open industry standards to complete the cross-industry digital convergence.

[0060] In order for commercial digital content to be made available for use with DLNA devices, content must be protected from unauthorized copying and use. Digital rights

management (DRM) technologies are widely available and used to protect the commercial content and manage the usage rights associated with content acquired through different channels (cable, satellite, Internet, etc.) and models (VOD, DVD, rental, etc.). DRM, however, is outside of current DLNA, which leaves the option of DRM implementation to the device manufacturer. Moreover, neither a list of approved DRM technologies nor DRM interoperability has been included in the current version of DLNA.

[0061] Link Protection is the only content protection mechanism in DLNA, which is an optional implementation for a DLNA-compliant device. The primary use case for Link Protection applies to a commercial content that is stored on a media server and protected by a DRM technology. Link Protection provides that such a content can be decrypted and re-encrypted using a Link Protection technology by the media server before being sent to a client device (such as a television). The client device then decrypts the received content and renders/displays it. DLNA Link Protection thus enables view-only sharing of commercial content on all devices in, for example, a home network. However, Link Protection is not able to prevent pirated commercial content from being shared and consumed in the home network. In fact, since a decrypted copy of the content is available within the home network, DLNA-enabled content sharing can result in easier and wider sharing of pirated content.

[0062] The absence of an appropriate content protection in DLNA has been a barrier for commercial content to be made widely available in DLNA-compliant networks. The disclosed embodiments utilize watermarks that are embedded within a host content to identify unauthorized or pirated content in a network, such as DLNA-compliant networks, and to enable the communication and enactment of use policies for content across a broad range of distribution channels and devices. In some embodiments, screening and/or content screening are used to refer to operations that include, but are not limited to, examination of a content by a device to determine whether a use conforms to a content use policy. The content use policy can, for example, include one or more rules governing the use of content, including, but not limited to, the conditions under which certain uses result in the taking of a specified action. It should be also noted that the term extraction can refer to operations that include, but are not limited to, examination of a content to determine the presence of a watermark, and possible assessment of the auxiliary data within the detected watermark. During extraction, the watermark is typically not removed from the content. However, the disclosed embodiments can also readily accommodate watermark extraction algorithms that remove the embedded

watermarks during the extraction process. According to the disclosed embodiments, by way of various operations, such as the extraction of watermarks from a content, the assessment of usage rules associated with the extracted watermarks and the application of appropriate enforcement actions, can be distributed among one or more trusted entities. In some embodiments, such enforcement actions include, but are not limited to, the elements of a content use policy that relate to an operation or a function that is performed when a specified type of use occurs. As such, not all the devices within a network are required to possess the full range of watermark extraction and content screening capabilities in order to comply with a particular content management scheme. Further, the disclosed embodiments enable a device to determine if another device is trustworthy, and to ascertain the extent of watermark extraction and/or screening capabilities of that device. It should be noted that while some of the disclosed embodiments are described in the context of DLNA and DLNA-compliant devices and networks, the disclosed embodiments are equally applicable to other protocols, standards, networked environments and devices that are associated with the production, transmission, discovery, storage, control and presentation of media content, such as movies, audio tracks, images and the like.

[0063] As noted earlier, watermarks can be used to protect audio or audio-visual content from unauthorized uses. For example, movies that are being released to theaters can be embedded with watermarks that carry a "No-Home-Use" (NHU) code, indicating that they are only to be duplicated by professional replicators and played back on professional projection equipment. In another example, content that is released on Blu-ray Disc, DVD, or by authorized download services, can be embedded with watermarks that carry a "Trusted Source" (TS) code, indicating that such content is intended for consumer use, but with limitations that they must be protected by trusted DRM technologies. In another example, content can be embedded with watermarks carrying codes that uniquely identify the content, such as with an industry standard identification code such as the International Standard Audiovisual Number (ISAN), International Standard Recording Code (ISRC), Global Release Identifier (GRID), International Standard Book Number (ISBN), Universal Product Code (UPC), or a value assigned from another numbering system, and for which a mechanism is provided to use the identification code to "look up" more detailed descriptive information about the content and the permissions (or "rights") associated with its use, such as in a locally stored or online database. The embedded watermarks that are provided in accordance with the disclosed embodiments can be embedded within the audio, video and/or image portions of the

content and are designed to remain with the content, wherever it appears, including after copying, conversion to different formats, capturing by a camcorder, and other intentional and unintentional content manipulations. Content handling devices, such as Blu-ray Disc players, can detect the presence of the embedded watermarks and limit the use of the content when certain unauthorized uses are identified. For example, playback or copying of unauthorized copies of the content may be stopped or an audio portion of the content may be muted, depending on which embedded code is extracted and what operation is being performed by the content handling device.

[0064] In some embodiments, significant improvements in watermark extraction efficiency are achieved by executing watermark extraction prior to the use (e.g., playback, copying, transmission, display, etc.) of the content. In such embodiments, the watermark extraction operation is sometimes referred to as "background" watermark extraction. A watermark extraction operation that is conducted prior to the usage of a content can produce an extraction record for secure storage in order to reduce the need for real-time extraction on the same content at the time of a future use. In some embodiments, a real-time extraction is performed on content at the time that content is being used. In some instances, watermark extraction can also be real-time extraction. As a result of watermark extraction (e.g., background watermark extraction) an extraction record can be created that includes, but is not limited to, information representing the results of a background extraction operation in a form suitable for storage. Furthermore, it is understood that the term "background" in the context of the disclosed embodiments is not intended to convey that the associated operations are necessarily performed through background processing within a multitasking operating system. Rather, background extraction can be performed as part of foreground processing, background processing, or combinations thereof. In some embodiments, the content use may be delayed until the watermark extraction process is at least partially completed. In yet other embodiments, watermark extraction and content usage are interleaved in time so that watermark extraction is always ahead of content use. In still other embodiments, watermark extraction may take place in real-time, during, and in synchronization with, the transfer or the usage of the content.

[0065] According to the disclosed embodiments, the results of watermark extraction are stored in a secure fashion so that they can be retrieved at a different time, such as at the start of content usage. In this context, the watermark extraction is carried out by a watermark

extractor that can be configured to extract, process, decode and analyze the embedded watermarks to discern the presence of watermarks and/or to obtain the payload value of the embedded watermarks. In some embodiments, the watermark extraction may further include discerning some or all of the usage rules associated with the embedded watermarks. The extraction of watermarks is typically a passive operation that does not affect the integrity of the host content. A watermark extractor, which may be implemented in software, hardware and/or firmware, can be further configured to designate potential enforcement actions that must be initiated based on the extracted watermarks and in conformance with the associated usage rules. In one example, where an unauthorized usage of the content is detected through the assessment of embedded watermarks, the content may be purged (i.e., deleted). Alternatively, the content may be preserved and the user may be informed of the content status at a convenient moment (e.g. at the start of a playback attempt). In other embodiments, the user may be advised as to one or more recommended corrective actions, such as purchasing a license that allows authorized playback of the content. The above scenarios only provide a few exemplary enforcement actions that may be commenced upon the extraction of one or more embedded watermarks. However, it is understood that additional enforcement actions may additionally or alternatively be effected.

[0066] In some embodiments, if the content has no embedded watermarks, information indicating the absence of an embedded watermark is stored (e.g., in an associated meta data file) for further use. For example, at the moment of actual content usage, the stored information, indicative of the absence of watermarks, can be used to allow content usage without a need to undertake watermark extraction. In some embodiments, the extraction process may produce watermarks that are insufficient to trigger an enforcement action. For instance, enforcement rules associated with a trusted source (TS) watermark require the extraction of watermarks over an extended period of time before triggering an enforcement action. For example, an enforcement action logic for a feature movie may require finding the TS watermarks in at least 7 out of 9 sequential 200-second screening intervals in order to trigger an enforcement action. On the other hand, for a short audio-visual content (e.g., shorter than one hour such as a TV show), an enforcement logic may require finding the TS watermarks in at least 7 out of 9 sequential 100-second screening intervals in order to trigger an enforcement action. In some embodiments, such an enforcement logic includes, but is not limited to, the elements of a content use policy that relate to the types of use of content that will result in a specified enforcement action. To facilitate the operations of a content

handling device in these and other similar scenarios, upon the extraction of watermarks during the watermark extraction, a list of extracted watermarks with associated time stamps are stored for later use.

[0067] The stored information must be secured against manipulation in a secure way. In one example, digital signatures are used to ensure that the stored information is authentic and free of tampering. It is also desirable to ensure user privacy by preventing unauthorized third parties from accessing the stored information. This can be achieved by utilizing encryption techniques to protect the stored data from unauthorized access. In particular, in DLNA, digital transmission content protection over Internet protocol (DTCP-IP) is the mandatory technology when a device implements Link Protection. As such, all DTCP-IP compliant devices are assigned a unique device identification code and a device public/private key pair. In this scenario, the stored extraction information can be digitally signed by the private key of the DLNA-compliant device and encrypted using the public key of that device. In some embodiments, extraction information can include, but is not limited to, information that is obtained from performing an extraction operation. As a result, only that device can create new digital signatures and decrypt the stored extraction information, while anyone with the associated public key can detect tampering attempts to the stored information.

[0068] FIG. 1 illustrates an exemplary content handling device 100 that may be used to accommodate the disclosed embodiments. The content handling device may conduct one or more operations such as rendering, recording, copying, transferring and/or playback of an input content 102. The input content 102 may be communicated to the content handling device 100 through one or more communication channels comprising wired and/or wireless communication channels, magnetic, optical, Flash and/or other computer readable media, or other sources. As such, the content handling device 100 can be configured to detect the presence of the input content 102. The same or a different component within the content handling device can detect a request for the input content 102 that is received from another entity. The detection of the input content 102 or the reception of a request for the input content 102 can be carried out by a detector/receiver component within the content handling device 100. Such a detector/receiver component can be part of, or a separate component from, the commutation component 110. In embodiments where the content handling device 100 is configured to request a content from another entity, a component, such as a processor that is executing a program code, within the content handling device 100 can generate such a

request for the content and transmit the request to another device through, for example, the communication component 110. In one example, the content handling device 100 is DLNA-compliant device, which may be in communication with one or more other DLNA-compliant devices. The content handling device comprises a watermark extractor 104 that screens the input content for the presence of watermarks. As noted earlier, the watermark extractor 104 can extract, process, decode and/or analyze the embedded watermarks and to discern the usage rules associated with the embedded content. The content handling device can also include a digital signature generator 106, which can be configured to produce digital signatures in accordance with one or more algorithms.

[0069] Further, an encryption/decryption component 108 within the content handling device 100 can be configured to encrypt/decrypt some or all of the input content 102 and/or extraction information that is produced by the watermark extractor 104. The encryption/decryption component 108 can be configured to implement a variety of public- and/or private-key encryption and/or decryption algorithms. The content handling device 100 can further include an authentication component 120 that can produce authentication parameters associated with the input content 102, authentication information associated with extraction information, and/or device authentication information (e.g., certificates). For example, the authentication component 120 can include a hash generation component that generates hash values for a sequence of input values. The authentication component 120 can further compare newly generated authentication information with a previously stored authentication information to verify an integrity of a content. The authentication component 120 can be configured to implement a variety of hashing algorithms, such as MD5, SHA-1 and SHA-2. The authentication component 120 may further be configured to carry out the necessary operations to effect device authentication. As such, the authentication component 120 can generate and communicate requests for device authentication, authentication information, exchange authentication certificates and verify the trustworthiness of another device.

[0070] FIG. 1 also illustrates one or more storage units 112 that can reside within the content handling device 100. Such storage units 112 can store the input content 102 (e.g., in encrypted, partially encrypted or clear format), the information produced by the watermark extractor 104 and the associated indexing information and meta data, content authentication information, compliance rules associated with the usage of embedded content and the

associated enforcement actions, as well as computer program code that can be retrieved in order to implement any one of the functionalities of the disclosed embodiments. As such, the storage unit 112 can be in communication with various components of the content handling device 100, such as the watermark extractor 104, the digital signature generator 106, the encryption component 108, the authentication component 120, one or more processors within the content handling device 100 and the like. These components can retrieve and utilize the information, the computer codes and the content that are stored on the storage units 112. FIG. 1 also shows a storage unit 118 that may reside outside of the content handling device 100. The outside storage unit 118, which may be in communication with the content handling device 100 through the communication component 110 via the communication link 120, can store some or all of the above noted input content 102, watermark extraction records, as well as other data and program code. The communication component 110 may further allow the content handling device 100, or particular modules or components with the content handling device 100, to communicate with the outside storage unit 188 and/or outside entities and users.

[0071] FIG. 1 also depicts a compliance enforcer 114 that can be configured to evaluate the enforcement logic associated with the extracted watermarks of a particular content, and enforce the rules associated with enforcement actions. For example, such enforcement actions can include aborting the desired operation (e.g., not outputting the output content 116), muting the audio and/or blanking the screen associated with the output content 116, and/or presenting a copyright restriction notice. It should be understood that the content handling device 100 can also include additional components, one or more processors or controllers and additional memory devices that are not explicitly shown in FIG. 1. For example, a component within the content handling device may receive information associated with other devices that can communicate with the content handling device 100. Such information can be received, for example, through the communication component 110. The same, or a separate, component within the content handling device 100 can make decisions regarding the delegation of some or all of the screening operations (such as watermark extraction, screening, etc.) to the components within the content handling device 100 (e.g., to watermark extractor 104, compliance enforcer 114, etc.) and/or to other devices that can communicate with the content handling device 100. The components within the content handling device 100 can be implemented in hardware or software, or combinations thereof. In addition, while the media handling device 100 of FIG. 1 is depicted as a single device, one

or more of the components or modules associated with the content handling device 100 may be implemented as part of a separate device. For example, the watermark extractor 104 may be implemented in a first device that is separate from a second device that implements the compliance enforcer 114.

[0072] The watermark extraction that is carried out in accordance with the disclosed embodiments can be executed whenever a new content is detected (e.g., within a home network, such as a DLNA-compliant network) and whenever spare resources are available to certain trusted device within the DLNA-compliant network. This way, peak processing loads on any given device can be decreased by distributing the processing load over time and/or over other devices with the home network. The disclosed embodiments further enable background watermark extraction to be carried out in conjunction with other trusted devices that may reside outside of the home network and/or trusted devices that are part of a different network. For example, the background processing operations may be conducted, at least in-part, by trusted devices that reside within a DLNA-compliant network that can, directly or indirectly, communicate with devices that may reside in a non-centralized network of devices in a secure fashion. Further details as to how trusted devices are identified and utilized to carry out all, or part of, the content screening operations will be discussed in the sections that follow. In some examples, the background watermark extraction is executed with a low priority to ensure the availability of computational and memory resources for other higher-priority operations and to improve user's experience.

[0073] To facilitate access and retrieval of the extraction information, extraction records can be indexed by the content file name (which, for example, includes the file folder name or the path to the file), by a universal resource locator (URL) associated with the watermark extraction records. The extraction records can also contain the file size of the associated content. Presence of a new content can be detected by periodically searching for new file names on the device or additional/affiliated devices that may reside within the home network. Alternatively, or additionally, the presence of a new content can be detected whenever the opportunity for watermark extraction arises, such as in situations where spare computational and memory resources become available.

[0074] FIG. 2 illustrates the operations associated with the generation of extraction information and the usage of such information in accordance with an exemplary embodiment. The process starts at 202, where watermark extraction is performed. The results of the

watermark extraction can include the payload value of extracted watermarks and an associated time stamp that designates the temporal location of the extracted watermark within the content. The extraction information can further include a file name, a file size and other information associated with the content. At 204, content authentication information is generated. This information can be used to verify that the content has not been modified or tampered with. For example, at 204, a hash value associated with the content can be generated. As will be described in the sections that follow, hash value generation can ensure authenticity of the content and its proper correspondence to the associated extraction information. At 206, a digital signature associated with the extraction information is calculated. In one example, the digital signature is appended to the extraction information. At 208, at least a portion of the extraction information and the associated digital signature are encrypted. In one example, only the extraction information is encrypted, while in another example, both the extraction information and the associated digital signature are encrypted. The fully, or partially, encrypted extraction record is then stored on a storage media at 210. Certain additional operations, such as indexing of the content items, compressing the content items, etc., may also be carried out at some point after watermark extraction 202 but before storage of extraction information 208.

[0075] Referring to FIG. 2, the stored extraction information may be retrieved at a later instance in time (e.g., at the time of playback of the content). At 212, authenticity of the content is verified. Authentication of the content will be described in further details in the sections that follow. If content authentication does not succeed ("NO" at 214), watermark extraction operations are conducted for the content by, for example, returning to block 202. If content authentication succeeds ("YES" at 214), the usage rules associated with the extraction information are checked at 216. For example, the usage rule associated with a No Home Use watermark payload can prevent the playback of the content on a consumer device. The usage rules may be stored at a storage location internal or external to the content handling device. Additionally, or alternatively, the usage rules may be received from an outside entity, such as a trusted authority. At 218, the applicable enforcement actions (if any) are effected. For example, an audio portion of the output content can be muted, or a copying operation can be aborted. It should be noted that, in some embodiments, the usage rules associated with the extracted watermarks are stored along with the extraction information in step 210. In these embodiments, prior to the application of the enforcement action at 218, it must be ensured that the stored usage rules are up to date. In another embodiment, the

applicable enforcement actions may also be stored along with the extraction information at 210.

[0076] The operations that are illustrated in the block diagram of FIG. 2 are also applicable to the embodiments where the extraction of watermarks are carried out in real-time (e.g., as the content is being rendered, displayed, etc.). In such embodiments, the extraction information, at 202, is produced in parallel with, or slightly earlier than, rendering a particular segment of the content. The extraction information, which is stored, at least temporarily, at a storage location, can be accessed to determine if an enforcement action is needed in conformance with the associated usage rules. In real-time applications, the creation of a digital signature, at 206, and encryption of the extraction information, at 208, may not be feasible due to a lack of computational resources. In these scenarios, the extraction information may be stored within a tamper-resistant portion of the watermark extractor. Implementation of tamper-resistant modules within a device (i.e., a software and/or a hardware device) can be carried out in accordance with tamper-resistant techniques and algorithms that are known in the art.

[0077] FIG. 3 illustrates the operations that are commenced upon the detection of a new content file at a content handling device. In some embodiments, a new content is detected when a device encounters a new content and commences the subsequent actions for obtaining the associated extraction records. In such scenarios, a "new content" is any content that does not have a matching file and/or path names in the extraction records. In other embodiments, a content handling device may monitor certain operations, such as "save" and "import" operations, and trigger additional operations if particular conditions are satisfied. In these embodiments, a content that has a matching path and file name is still considered a new content. Referring back to FIG. 3, at 302, the presence of a new content is detected. If, at 304, it is detected that the file name is new (i.e., a content file name match cannot be found in the extraction records), the file is designated to be subject to watermark extraction at 318. For example, the content can be placed on a waiting list to be processed for watermark extraction. In one embodiment, a content file is considered a new file if the file's base name (regardless of the file's full path name) does not exist within the device or an associated entity, such as a connected database. If the content file is not new (i.e. "NO" at 304), it is determined, at 306, if the new content and the existing content have an identical file size. If the file sizes do not match (i.e., "NO" at 306), the process moves to 318, where the content is

designated for watermark extraction. If, at 306, the file sizes do match (i.e., "YES" at 306), a content authentication operation is triggered at 308 (content authentication procedures will be described in the sections that follow). If content authentication fails (i.e., "NO" at 310), the content is designated for watermark extraction at 318. Otherwise (i.e., "YES" at 310), it is determined, at 312, if the content path name is new (i.e., via comparing the path name of the new content against the existing path name that is saved in the extraction record). If the path names are identical (i.e., "NO" at 312), watermark extraction is omitted at 316. Otherwise, if the path names are different (i.e., "YES" at 312), the extraction record is updated with the new file location at 314 and watermark extraction is omitted at 316.

[0078] The flow diagram of FIG. 3 is intended to facilitate the understanding of the disclosed embodiments. Therefore, additional or fewer steps may be undertaken in order to implement the various embodiments. It should be also noted that in order to facilitate the search for new and/or duplicate files, the stored content files and/or the associated extraction records may be indexed using a variety of indexing techniques and parameters. For instance, the file name may be used as an index for searching a database of content files.

[0079] In other embodiments, the device further verifies if the previously analyzed files (e.g., files that have previously been subjected to watermark extraction) are still present on the device. This process can be executed in association with the process of searching for new files, or it can be performed independently when spare resources are available, or when a delete action is executed on the device. If the content associated with an extraction record is removed from the device, the extraction record may also be removed to conserve memory resources and to reduce the computational efforts in searching through stored extraction records.

[0080] In some embodiments, where extraction information is not available at the time of content use, watermark extraction can be executed at real-time (i.e. on-the-fly). If enough computational and/or memory resources are not available for both the execution of a real-time extraction and usage of the content, the content use can be delayed until the watermark extraction process is at least partially completed. In some examples, watermark extraction and content usage are interleaved in time (e.g., watermark extraction over one segment is followed by usage of that segment) so that watermark extraction is always ahead of content use.

[0081] An important security consideration is the possibility of content modifications or substitutions after the watermark extraction has been completed. For example, an unmarked content may be initially imported, and then an external program may attempt to replace watermark-bearing component of the content with a new content (which may have embedded watermarks). In this process, an attacker may intentionally preserve the same file name and file size to prevent the content from being designated for watermark extraction. To foil this attempt, the device must authenticate the content before using the stored extraction information. This operation was previously described in connection with step 212 in FIG. 2.

[0082] Content authentication can be quickly and securely carried out using one-way cryptographic hash function such as MD5, SHA-1 or SHA-2. During the watermark extraction process on a newly imported file, a hash value is calculated and saved together with the extraction results, as depicted in FIG. 2, steps 204 to 210. When content usage is commenced, a hash value for the content is computed and compared to the previously stored hash value (e.g., at 212 in FIG. 2). If the newly computed values match the stored hash values, the content is deemed to be authentic and, therefore, the associated extraction information can be used to effect any applicable enforcement actions. Otherwise, if the calculated and stored hash values do no match, the usage of the content may be fully or partially disabled (e.g., copying aborted, playback stopped, copyright notice displayed, etc.). Additionally, or alternatively, the content can be designated to undergo a new watermark extraction operation (see, e.g., FIG. 2, "NO" at step 214 and Fig. 3, "NO" at step 310).

[0083] In some embodiments, the content authentication information (e.g., a hash value) is produced (e.g. at step 204 in FIG. 2) when the content is in encrypted format. This way, when content authentication is conducted (e.g., at step 212 in FIG. 2), there is no need to decrypt the content before verifying the content's authenticity. Therefore, at the moment of content use, the disclosed embodiments only require the generation of the content authentication information (e.g., a hash value) rather than undertaking a full watermark extraction operation. This aspect of the disclosed embodiments provides a substantial improvement in efficiency of operations of a content handling device, especially in cases where content transformations, such as decryption, decompression, de-multiplexing etc., are required prior to watermark extraction. Many hash functions can be implemented efficiently in hardware and/or software. In some instances, where the watermark extraction records are encrypted (see, e.g., FIG. 2, step 208), the stored extraction information must be decrypted in

order to retrieve the stored hash values. However, since the size of the stored watermark extraction record is relatively small, such a decryption operation is not likely to present a significant processing burden.

[0084] A critical requirement in selecting a hash function is the pre-image resistance, defined as follows: given a hash value *h*, it should be hard (almost certainly beyond the reach of any adversary) to find a message *m* such that *h = hash(m).* This requirement is related to an attack where a pirate tries to substitute a marked content with an unmarked content, which has the same hash value, in order to create an extraction-free watermark extraction report. In this attack scenario, after the content handling device conducts a watermark extraction on an unmarked content, the attacker may attempt to replace the unmarked content with a marked content with the same hash value to avoid the screening of marked content.

[0085] It should be noted that the above noted pre-image requirement is easier to satisfy than a collision resistance requirement. The collision resistance requirement can be defined as follows: it should be hard to find two different messages *m1* and *m2* such that *hash(m1) = hash(m2).* This requirement, which is more common if hash functions are used for indexing schemes, typically necessitates the use of more demanding hash functions, such as the SHA-2 family of hash functions. However, in scenarios where the less stringent pre-image resistance provides the sufficient protection, simpler and less computationally demanding hash functions, such as MD5 and SHA-1 may be used.

[0086] In some embodiment, further reductions in processing load associated with hash function calculation can be achieved by selecting only a subset of data from the content to be input to hash function calculation. In one example, the selection process is maintained as a secret. For instance, random content segments can be selected using a random number generator that uses the device private key as a seed.

[0087] The disclosed embodiments further provide for the operation of a content handling device by considering security concerns related to mosaic attacks. A mosaic attack is defined as breaking up a content into multiple segments such that each content segment can individually evade an enforcement action. In this attack scenario, a content is divided into segments that are individually subject to watermark extraction. During the actual content use, the segments are assembled again for presentation to the user using, for example, a playlist feature at content rendering instance. A coarse mosaic attack typically involves

producing relatively large content segments. For example, a feature movie may be segmented into several 10-minute chunks in order to avoid Trusted Source (TS) enforcement on individual segments. This attack can be successful for a TS-marked content since, as noted earlier, repeated watermark extractions in several content segments are required to trigger an enforcement action.

[0088] In one embodiment, a coarse mosaic attack can be circumvented in a compliant device by safely storing the content use history associated with that device, and subsequently retrieving and analyzing the content use history with each new content use. The content use history provides a record of all watermark extractions, together with an associated time stamp, within a predefined interval (e.g., for at least the last 20 minutes content use by the device). Watermark extraction results for any new content use can then be appended to the retrieved content use history data in order to evaluate if an enforcement condition is present. In the case of a mosaic attack that utilizes a playlist, the evaluation of an enforcement condition can be based on an aggregate of a retrieved content use history and the extraction record for each item on the playlist in the listed order. This way, the enforcement condition can be efficiently evaluated without having to conduct a real-time watermark extraction operation content use commences.

[0089] Another attack scenario relates to a fine mosaic attack, in which a content is divided into a large number of segments with fine granularity such that watermark extraction from each individual segment is not feasible. A fine mosaic attack implies a significant overhead due to small file handling and, therefore, may not be practical for many devices. For example, a feature movie may be segmented into one-second clips and saved as a string of independent files that are later concatenated using some kind of playlist function. Nonetheless, in accordance with the disclosed embodiments, fine mosaic attacks can be effectively thwarted by properly recognizing the presence of such an attack. In one embodiment, the existence of content files below a certain size limit triggers a fine mosaic countermeasure. For example, the detection of audio-visual content files that are less than five seconds long may be a flag that triggers fine mosaic countermeasures during a watermark extraction process.

[0090] In one embodiment, a fine mosaic attack is thwarted by requiring watermark extraction over a number of concatenated files provided in a playlist. Watermark extraction over the concatenated files can be carried out prior to the content use, or in real-time, during

the content use. In one embodiment, if the concatenated file contains a mix of files below and above the size limit, watermark extraction is performed only for the set of adjacent short files with a total length above the size limit. The result of this extraction process can be combined with the results of extraction information for the files above the size limit (which should have been previously conducted), and used for enforcement logic evaluation and/or enforcement.

[0091] In an alternative embodiment, an advanced watermark extractor may be instantiated upon the detection of a fine mosaic attack. The advanced extractor can perform the bulk of the processing in the background mode, and save intermediate data for future use. For example, the intermediate data can consist of content features that are relevant for watermark extraction and have a size that can be much smaller than the original content. This feature of the disclosed embodiments can result in a significant reduction in the usage of computational and memory resources. Therefore, upon the detection of a fine mosaic attack, the device can quickly and efficiently extract the embedded watermarks just by evaluating the intermediate data as opposed to attempting to extract the watermarks from the original content. For example, in a system that uses spread spectrum watermarking, the intermediate data can comprise correlation values between a known spread spectrum carrier and the content samples with a particular granularity. At the moment of content use, the intermediate data is concatenated, watermark extraction is attempted and enforcement condition is evaluated based on any watermarks extracted from the intermediate data. As noted earlier, in some embodiments, if the concatenated file contains a mix of files that are below and above the size limit, the intermediate data concatenation and watermark extraction are needed only for the set of adjacent short files with total length above the size limit. The result of this extraction process can be combined with the extraction information associated with the files above the size limit, and used for enforcement logic evaluation and/or enforcement.

[0092] In scenarios where a network of trusted devices can be established, it may be advantageous to use the network to share the watermark extraction and enforcement responsibilities. In one embodiment, if a device with a new content item is not able to interpret the content's format, the device may entrust all, or a portion of, the watermark extraction operations to another device that can interpret the content format. The device that performs the watermark extraction may report the extraction information to the delegating device for further action and/or secure storage.

[0093] FIG. 4 illustrates an exemplary embodiment in which an invocation model is used to enable cooperative watermark extraction. In this embodiment, a master device 404, which receives an input content 402, is tasked with performing an operation (e.g., copying, transferring, playing, recording, etc.) that produces an output content 406. As depicted in FIG. 4, the master device 404 invokes a slave device 412 to perform watermark extraction on a selected content 408 that is communicated to the slave device 412. Upon full or partial completion of watermark extraction by the slave device 412, the master device 404 receives the extraction information 410 and decides if the selected content 408 will be delivered to the destination device and/or if additional enforcement actions, such as muting or displaying a warning message, are warranted. This invocation model can be applied in situations where the master device 404 doesn't have the capability of watermark extraction or it is overloaded (e.g. in case of multiple instances of streaming or watermark extraction tasks) or it does not have appropriate codecs to handle the selected content.

[0094] FIG. 5 illustrates another exemplary embodiment in which a delegation model is used to enable cooperative watermark extraction. In this embodiment, a delegating device 504, which is tasked with performing an operation on an input content 402 (e.g., copying, transferring, playing, recording, etc.), completely delegates the watermark extraction to a delegated device 510. The delegated device 510 receives the selected content 508 from the delegating device 504 and performs the watermark extraction operations. The delegated device 510 further decides whether or not to forward the requested content (i.e., the trusted content 512 if the decision is made to forward the content) to a destination device 514 in accordance with usage rules associated with the extraction information 514. In one scenario, the delegated device performs the watermark extraction and screening operations while streaming the content until the usage rules limit the use of the contents (e.g. stop of the streaming or muted audio). In another scenario, the transfer of the content to the destination may start only after the partial or full completion of the watermark extraction and screening. Further, the delegated device 510 may or may not return the extraction information 514 to the delegating device 504 (this optional operation is depicted by the dashed arrow in FIG. 5 that starts from the delegated device 510 and terminates at the delegating device 504). The delegating model can be used in various scenarios where the delegating device 504 doesn't have the capability of watermark extraction or it is overloaded (e.g. in case of multiple instances of streaming or watermark extraction tasks) or it does not have appropriate codecs to handle the requested content. In particular, this model is useful in the scenarios where the

presence of a bridge device (e.g., the delegated device 510) is needed to enable a content transformation, such as converting a high-definition content to an MPEG-4 mobile version, and the like.

[0095] In both invocation and delegation models, the devices that may cooperatively perform screening may be aware of the codecs capability bilaterally or unilaterally. They may inquire or exchange the codecs capability before or at the beginning of the transfer of the selected content. For example, in DLNA that adopts HTTP protocol for content transfer, a device uses the MIME-TYPE values that are defined in DLNA Media Format Profiles as values for Content-Type in a HTTP request or response to specify the codecs of the requested content. Other content transfer protocols such as RTP (Real-time Transport Protocol) also support exchange of codecs capability.

[0096] In some systems that utilize invocation or delegation models, it may be possible that the sender of the selected content (either master device 404 or delegating device 504) is not aware of the codec capability of a receiving device (either a slave device 410 or a delegated device 510). In some embodiments, in such situations, if the receiving device does not have the appropriate codecs that are required to process the requested content, the receiving device informs the sender of the exception immediately (as part of extraction information 514). The receiving device may also optionally request the sender to convert and re-transfer the content in a media format that can be processed by the receiving device.

[0097] In real-time watermark extraction scenarios, cooperative watermark extraction in accordance with the disclosed embodiments can be implemented in situations where a first device accesses the content and a second device renders (e.g., displays) that content. In these scenarios, the content-accessing device is usually unable to interpret the content, while the rendering device (which is, of course, able to interpret the content) is not trusted. In this case, the content-accessing device may initiate a search to discover a trusted device that can interpret the content. Such a trusted device must also be able to execute watermark extractions at a rate faster than, or equal to, the real-time rendering of the content. The trusted device may, for example, be identified by consulting a list of trusted devices that can be securely accessed by the content-accessing device. Such a list can also be communicated securely to the content accessing device from a trusted authority. In another embodiment, the list is created during device discovery based on UPnP (Universal Plug and Play) networking protocols. For example, DLNA uses UPnP for discovery and description of device types and

capabilities. In other embodiments, a device authentication procedure is commenced to verify the trustworthiness of a device and to ascertain its capabilities. Device authentication procedures will be further described in the sections that follow. The extraction results and/or enforcement events that are produced by the trusted device may be returned to the content accessing device for further action and/or secure storage.

[0098] The above-noted real-time watermark extraction scenario can be considered an example of the invocation model described above. This example scenario allows a commercial content to be delivered on a legacy rendering device (e.g. DLNA TV without a watermark extractor). To encourage the adoption of trusted rendering devices, incentives may be provided by the content owners, PayTV companies and Over-the-top (OTT) and on-demand content providers to the users who render the premium content directly on a trusted rendering device. Alternatively, a flag in a DRM-protected commercial content may be inserted by the content distributor to indicate that the content must be rendered by a trusted client.

[0099] In some embodiments, if a real-time watermark extraction operation is not feasible (even with the cooperation of additional trusted devices), a delayed watermark extraction operation may, nevertheless, be conducted whenever the necessary resources become available. The results that are produced by the delayed watermark extraction operation may be stored as part of the extraction record for that content. For example, the watermark extraction record may be stored at a database, where it can be accessed in the future by one or more trusted devices. In scenarios that a delayed watermark extraction operation is performed, any subsequent real-time access to that content can be readily screened using the stored extraction records.

[0100] Another aspect of real-time applications (e.g., live streaming of a video content) is that only a fraction of the content is made available before its rendering. In these cases, it may not possible to execute watermark extraction, using only locally available resources, prior to the content use. Therefore, as noted earlier, a real-time watermark extraction operation may be needed. In some embodiment, the need for conducting a real-time watermark extraction may be eliminated by providing an extraction record that is produced by a trusted device to accompany the streaming content. As noted earlier, content authentication can ensure the integrity of the content and its proper correspondence with an existing extraction record. However, in the context of a streaming application, full

authentication of the streaming content may not be possible during the streaming of the content since the full content only becomes available at the end of the streaming session.

[0101] In some embodiments, authentication of one or more portions of a content is enabled by utilizing segmented hash values. In particular, the content is divided into segments of a particular size (e.g., 10 seconds in time or 1MB in size) and a hash value is generated for each content segment and stored together with the corresponding watermark extraction record. This way, a content may be authenticated in smaller units according to the granularity of content segments with the calculated hash values. During the streaming operation, a received content segment (e.g., that resides in a buffer) can be authenticated by calculating its corresponding hash value and comparing it to the hash value stored in the extraction record. The segments can be selected sequentially and contiguously for authentication as they become available during the streaming operation. Alternatively, a subset of content segments can be selected for authentication. In one embodiment, a subset of segments may be selected according to a deterministic pattern (e.g., every third segment is selected) or according to a random/pseudo-random selection pattern (e.g., random selection with uniform distribution). An authentication failure, for even one segment, can signal that the content has been manipulated and, therefore, trigger the real-time extraction operation. Alternatively, a detection of content manipulation can abort the content use.

[0102] According to the disclosed embodiments, a segmented hash value is composed of a sequence of hash values, where each hash value is calculated from a segment of content. The segment can be defined by a fixed time period or fixed byte size of the content. Moreover, the final content may be padded to produce a segment with the pre-defined fixed size. One exemplary algorithm for generating a segmented hash function is described as follows. Let's assume that C is an audio-visual content, and c_1, c_2, ...c_n are consecutive segments of C, or randomly selected segments of C. In case of selection of segments, the flexibility between authentication granularity and performance can be achieved. For example, for better computation performance, fewer segments can be selected. The size of segment will also have an impact on the performance as measured by computational and resource efficiency. In particular, smaller segments require fewer computations for authenticating that particular segment. However, a minimum segment size limit may be required to ensure the security of the hash function.

[0103] In one embodiment, the security of the generated hash values can further be enhanced by providing a segment size that varies within a particular range, as determined by, for example, a random number generator. An exemplary algorithm for generating hash values associated with variable segment sizes is described as follows. Let's assume HF is a hash function that accepts a seed value, s, and a block of data, c_n, to produce a hash value, h_n. The hash values for segments $c_1, c_2, \ldots c_n$ can be calculated using the following set of operations:

$$h_1 = \mathrm{HF}(s, c_1); \qquad (1)$$

$$h_2 = \mathrm{HF}(h_1, c_2);$$

$$\ldots$$

$$h_n = \mathrm{HF}(h_{n-1}, c_n).$$

[0104] A hash value, H_i, for a content up to the segment c_i ($1< i <n$) can be calculated as follows.

$$H_i = \mathrm{HF}(s, h_1+h_2+\ldots+h_i) \qquad (2)$$

[0105] One major advantage of using hash values for content identification is that the hash function takes the streaming content as a binary stream, regardless of the content format, whether or not the content is encrypted and which cryptographic algorithms are used for the encryption. The disclosed embodiments can be used in conjunction with different hash functions. For example, an MD5 implementation in software on a Pentium 90 MHz computer can process the input data at 45 mega bits per second. To further speed up the hashing process, instead of every byte, some selective bytes from each segment can be taken as the input to the hash function.

[0106] In another real-time watermark extraction scenario, cooperative watermark extraction in accordance with the disclosed embodiment may be implemented in situations where a content-accessing device lacks the processing power to simultaneously carry out content access, transmission, rendering, and watermark extraction. In particular, such a scenario may arise when the same device is configured to conduct simultaneous access and transmission of multiple content streams. In these scenarios, watermark extraction can be delegated to a capable and trusted device. The extraction information and/or enforcement events may be returned to the content-accessing device for further action and/or secure

storage. This real-time cooperative watermark extraction is another example of the invocation model described above.

[0107] FIG. 6 illustrates another example embodiment, in which a content is delivered to a content client device 604 by a content server 602. The content server 602 and/or the content client device 604 may be in communication with a storage unit 606, a slave device 608 and/or a delegated device 610. Depending on the system configuration, the content server 602 and/or the client content device 604 may communicate as a master device with the slave device 608, as discussed earlier in connection with the invocation model of FIG. 4. Similarly, depending on the system configuration, the content server 602 and/or the client content device 604 may communicate as a delegating device with the delegated device 610, as discussed earlier in connection with the delegation model of FIG. 5. The communication links 612 that are depicted in FIG. 6 enable communications of content, extraction information and other information between the devices that are shown in FIG. 6. For example, one or more of the communication links 612 can allow secure communications (e.g., through link encryption) between the different devices. Further, one or more of the content server 602, content client device 604, storage unit 606, slave device 608 and delegated device 610 may reside within a home network, such as a DLNA. In other embodiments, one or more of the content server 602, the content client device 604, the storage unit 606, the slave device 608 and the delegated device 610 may reside outside of a home network.

[0108] With reference to FIG. 6, it can be appreciated that watermark extraction and implementation of applicable screening operations and enforcement actions can be carried out using one or more of the depicted devices in real-time and non-real time applications. Further, the content handling devices that are depicted in FIG. 6 may reside within a network (such as a DLNA-compliant network) that can include a plurality of other server devices, client devices, storage units and the like, that can, directly or indirectly communicate with each other. In addition, the devices that are located within such a network may be in communication with a plurality of other devices that reside outside of the network. In some embodiments, a gateway device 614 may be in communication, through a communication link 612, with one or more of the other devices that are depicted in FIG. 6 and/or other devices that reside within or outside of a home network. The gateway device 614 can, for example, coordinate the operations of various devices to facilitate watermark extraction,

transfer of extraction records, authentication operations, communication and/or acquisition of trusted device lists, and the like. Further details regarding the operations of the gateway device 614 will be discussed in the sections that follow.

[0109] In some scenarios, a large number of content handling devices, such as the ones that are depicted in FIG. 6, may be in communication with one another to exchange content files or to conduct other operations. However, it is likely that only a subset of such content handling devices have the capability to conduct watermark extraction, evaluate the extraction records against content usage rules and/or effect enforcement actions. Therefore, the task remains as to how to properly identify trustworthy devices that have all, or a portion of, such capabilities. It is further necessary to determine the most effective and secure way to distribute the required workload among the various devices, and to conduct various communications between the devices.

[0110] Device authentication, which is carried out in accordance with the disclosed embodiments, enables each device to verify that another device is a "trusted" device. By establishing the trustworthiness of the devices, the capabilities of each device may be communicated to one another. FIG. 7 illustrates an authentication procedure that may be carried out between Device A 702 and Device B 704 in accordance with an example embodiment. In operation 706, Device A 702 transmits its certificate to Device B 704. In operation 708, Device B 704 verifies the received certificate of Device A 702, thereby determining Device A's trustworthiness, as well as some or all capabilities of Device A 702. In one example, trusted device authentication enables Device B 704 to verify that the certificate provided by Device A 702 is issued from a trusted authority. Analogously, in operation 710, Device B 704 may transmit its certificate to Device A 702. In operation 712, Device A 702 determines if Device B 704 is a trusted device and further ascertains Device B's capabilities. It should be noted that the authentication process can include additional operations that are known in the art. For instance, the authentication process can also include the communication of one or more challenges, and the corresponding responses, between Device A 702 and Device B 704. In some embodiments, these additional operations are conducted to ensure that the communicated information is not being merely copied from cached locations.

[0111] In some embodiments, device authentication may be carried out using a DCTP-IP authentication protocol. DTCP-IP specification includes a mandatory Full Authentication

and an optional Extended Full Authentication procedure. DTCP-IP uses Advanced Encryption Standard (AES)-128 for content encryption. Both authentication procedures of DTCP-IP employ a public key based Elliptic Curve Digital Signature Algorithm (EC-DSA) for signing and verification. Device Certificate issued by the Digital Transmission Licensing Administrator (DTLA) (i.e., the licensing administrator and developer of DTCP-IP) is stored in the compliant device and used during the authentication process. All compliant devices are also assigned a unique Device ID and device public/private key pair generated by the DTLA. The Device Certificate comprises a plurality of fields that include information regarding certificate format, Device ID, digital signature, DTCP public key and the like. The use of DTCP-IP authentication protocol allows the authenticating device to confirm that the authenticated device is in possession of private keys issued by the DTLA after certifying that the device is compliant.

[0112] In one exemplary embodiment, some of the reserved bits associated with a DTCP-IP Device Certificate may be used to signal the device's content screening (e.g., watermark extraction and enforcement) capabilities. Therefore, such a Device Certificate can be used to determine if a device is a trusted device and to obtain information regarding the device's screening capabilities. In other embodiments, additional information such as a location of an extraction record database may be exchanged between the two devices. The devices may further exchange information regarding their processing and storage capabilities.

[0113] In another embodiment, device authentication may employ remote attestation to obtain increased assurance that the authenticated device is compliant. Remote attestation employs a cryptographic protocol between the authenticating and authenticated devices to enable the authenticating device to establish that the authenticated device was certified as compliant and has not been modified. The protocol requires that the authenticated device perform specific computations (or "measurements") of its internal processing state (such as computing hashes of data or code or performing timing measurements on its computing operations) whose results provide the authenticating device with certainty that its operation at the time of measurement match those that were performed at the time the device was certified as behaving in a compliant manner. In one exemplary embodiment, remote attestation may be performed using a "hardware root of trust" such as a Trusted Platform Module (TPM) or other secure processing unit. A TPM is a hardware device that can securely store passwords, certificates, encryption keys, and other values in an internal memory and apply a very limited

set of cryptographic primitives to those values, based on instructions and other data values received from a more general purpose computer processor such as a CPU. The values stored in internal memory of a TPM are maintained as secret and can only be accessed through the limited cryptographic functions of the TPM. The TPM typically is contained in a separate computer chip from the CPU (such as affixed to the motherboard of a PC) but may also be incorporated into a system-on-a-chip that contains both the TPM and one or more CPU and other hardware functions. Storing this data on the hardware chip, instead of on a computer hard drive or within memory directly accessible by a general purpose CPU enables the establishment of a "hardware root of trust" for the device's behavior and significantly increases the security of the entire platform. This hardware storage location ensures that the stored information is more secure from external software attack and physical theft. TPM provides three kinds of security functionality: 1) secure storage of any data that is encrypted by keys only available to the TPM; 2) measurement and reporting of integrity of platform including BIOS, boot sector, operating system and application software; and 3) authentication of a platform or application-specific data via digital signatures using signing keys that are protected by TPM.

[0114] To enable device authentication in a TPM platform, a trusted party (e.g.. the Certificate Authority) will sign the signing keys that are protected by TPM. Such certificates that are also protected by TPM are used to prove that a signing key really does belong to a valid TPM. Two devices with TPM-protected certificates and signing keys may carry out the authentication process in the same matter as discussed above based on DTCP-IP authentication. The only difference is that the signing keys in a TPM platform is more secure.

[0115] A TPM-enabled device may authenticate another non-TPM-enabled device. Such authentication may result in unequal trustworthiness which then can be used by a service provider to offer distinct services. For example, a high-value content (e.g., a high-definition or an earlier release of a content) may only be delivered to TPM-enabled devices while other content can be delivered to both TMP-enabled and non-TPM-enabled devices.

[0116] The TPM contains a number of 160-bit registers called platform configuration registers (PCRs) to measure and report the status of a platform's environment in a trusted matter. Starting from a root of trust, it enables a trusted entity to obtain unforgeable information about the platform state. An executable program can measure another program

by computing its hash code and combine the current measurement with the hash value and store the combination in a PCR. Thus, PCRs represent an accumulated measurement of the history of executed programs from power-on to the present. Such a chain of trust provides a powerful defense against malicious programs, such as viruses, spyware and attacks on vulnerable programs. It can also be used to detect and disable unauthorized programs such as pirated software or unlawful programs.

[0117] A software media player, especially in a PC environment, has been a weak point in most content protection systems. Extending the chain of trust to the media player on a TPM platform strengthens the security by enabling the detection and further disabling of unauthorized programs and/or modifications to the software player.

[0118] TPM can create migratable or non-migratable keys for data encryption. Migratable keys never leave the TPM that creates them while migratable keys can exported to other platforms (devices). Therefore, a content can be locked into a TPM-enabled device by encrypting the content using a TPM-created non-migratable key so that the content can only be decrypted and played on that device. This is understood to be but one approach to performing remote attestation using a "hardware root of trust." However, other methods and devices which are currently known, or may become known in the future, may be used to accomplish the purpose of device authentication.

[0119] Based on the assessment of the trusted status of various devices and their capabilities, the various operations that are required to ensure the proper watermark extraction and screening operations associated with a content can be shared among those devices. In order to facilitate the discussion, the operations associated with providing a content from the content server to the content client device (see, e.g., the content server 602 and the content client device 604 of FIG. 6) can be divided into (1) watermark extraction and (2) screening. For example, watermark extraction can include, but is not limited to, the extraction of watermarks, the calculation of content authentication information, the generation of digital signatures, and the storage of the results in a secure location. Screening on the other hand, can include, but is not limited to, the verification of content authenticity, the acquisition and verification of usage rules and the implementation of enforcement actions (if needed). It is also understood that some overlap between watermark extraction and screening operations can exist. For example, certain operations, such as the acquisition and verification of compliance rules, can be conducted as part of one or both the watermark

extraction and the screening operations. Therefore, the above-noted division of operations is merely presented to facilitate understanding of the underlying concepts and is not intended to limit the scope of the disclosed embodiments.

[0120] Depending on whether or not a device is trusted (i.e. authenticated as compliant), the extent of availability of computational resources, compliance capability, the required security of operations, architecture and design complexity, the user experience considerations, preferences of the content owners and other factors, watermark extraction and screening operations can be conducted by one or more devices that may reside within and/or outside of a home network. For example, Table 1 provides a listing of how the responsibility of watermark extraction and screening can be shared among the various devices in eight exemplary scenarios.

Table 1 - Example Division of Operations

Scenario	Responsible Device(s)	Watermark Extraction	Screening
1	Content Client Device	Content Client Device	Content Client Device
2	Content Client Device	Slave Device	Content Client Device
3	Content Client Device	Delegated Device	Delegated Device
4	Content Server	Content Server	Content Server
5	Content Server	Slave Device	Content Server
6	Content Server	Delegated Device	Delegated Device
7	Content Client Device and Content Server	Content Server	Content Client Device
8	Content Client Device and Content Server	Content Client Device	Content Server

[0121] Table 1 illustrates that, in scenario 1, both the watermark extraction and screening operations are carried out at the content client device while, in scenario 4, both operations are carried out at the content server. In the remaining scenarios, the watermark extraction and screening operations are conducted through cooperation of the content client device, the

content server, a delegated device and/or a slave device. In particular, in scenario 2, the content client device invokes a slave device which conducts the watermark extraction. For example, such a slave device can be another trusted content client device or trusted server device with watermark extraction capabilities. In scenario 3, the content client device, which is a trusted device, delegates both the watermark extraction and screening operations to a trusted delegated device. Scenarios 4 through 6 provide analogs of scenarios 1 through 3. But in scenarios 4 through 6 the content server is the responsible device which may undertake the screening operations on its own, invoke a slave device to conduct the screening operations, or delegate these operations to a delegated device. In scenario 7, the content server conducts the watermark extraction operation and the content client device performs the screening. In scenario 8, the content client device conducts the watermark extraction operation and the content server performs the screening.

[0122] It can be appreciated that the exemplary listings of Table 1 do not provide an exhaustive listing of all cooperative scenarios. For example, a variation of scenario 7 can be constructed where the watermark extraction is implemented by the content server through invocation of a slave device. As noted earlier, the selection of one or more trusted devices to conduct a particular operation in cooperation with one or more trusted devices can be influenced by a variety of factors, such as the user preferences, complexity of implementation and the like. Table 2 provides an exemplary evaluation of the eight scenarios of Table 1 based on six different factors.

Table 2 - Exemplary Evaluation of Scenarios 1 to 8

Scenario	Processing Performance	Integration Complexity for Device Manufacturer	Consumer Experience	Architecture Complexity	Availability of Content in Suitable Format	Overall Preference Rank
S1	Very Good	Medium	Very Good	High	Yes	1
S2	Fair	High	Potential Poor	Medium to High	May be	7
S3	Fair	Medium to High	Fair to Good	Medium to High	Likely	8
S4	Potential Poor	Medium	Very Good	Low	Likely No	2
S5	Fair	High	Potential Poor	Low to Medium	May Be	6
S6	Fair to Good	Medium to High	Fair to Good	Low to Medium	Likely	4
S7	Potential Poor	Medium	Very Good	Low	Likely No	5
S8	Very Good	medium	Very Good	High	Yes	3

[0123] The exemplary evaluations of Table 2 provide a rough assessment of the merits for each configuration of devices in scenarios 1 through 8. Table 2 further includes a limited number of factors for illustration purposes. However, it is understood that additional factors, such as computational load and memory capabilities of each device, preferences of the content owner and the like, can also be considered in making an assessment of each scenario. The right-most column of Table 2 provides an overall preference ranking for each scenario. This overall ranking may be produced by considering all the evaluated items that are listed in Table 2 and/or additional factors that are not listed in Table 2. In one embodiment, such an overall preference ranking is used as a default setting, which prescribes a particular configuration of devices in the absence specific instructions that favors other configurations.

[0124] A review of Table 2 reveals that, even if both the content server and the content client device are capable of performing watermark extraction and/or screening operation, it may be preferred to assign certain operations to one or both of the devices (or even a third device such as a delegated or slave device) to accommodate particular preferences. In accordance with the disclosed embodiments, if both the client content device and the content server are trusted entities, then they can ascertain the capabilities of one another, and decide how to most effectively conduct the watermark extraction and screening operations. If only

one of the devices is a trusted device, then that device must determine how to independently, or in cooperation with other trusted devices, carry out the necessary watermark extraction and screening operations.

[0125] FIG. 8 is a flow diagram associated with watermark extraction and screening operations that are conducted in a collaborative fashion in accordance with an exemplary embodiment. At 802, a request for access to a content is detected. Such a request is typically initiated by a content client device and is directed to a content server. However, in some examples, the requests may be communicated between content client devices, content servers and/or other devices. At 804, device authentication is performed. For example, a device authentication that was described in connection with FIG. 7 may be performed to determine the trusted status of the devices and to obtain certain device capabilities. If it is determined, at 806, that both devices are trusted (i.e., "YES" at 806), certain device capabilities may be optionally exchanged between the two trusted devices at 808. As noted earlier, some or all of the device capabilities may be exchanged during device authentication step at 804. However, in some embodiments, device authentication and acquisition of device capabilities may be conducted in separate steps. For example, certain device capabilities, such as whether or not a device can perform watermark extraction or screening, can be ascertained during the authentication step (i.e., at 804), while other device capabilities, such as whether or not a device has spare computational resources to conduct additional operations, are ascertained during a subsequent information exchange operation (i.e., at 808).

[0126] Referring back to FIG. 8, at 810, the two devices collaboratively determine the proper operational configuration. This step allows the division of labor between the two trusted devices (and/or additional trusted devices) based on a desired criterion. For example, an operational configuration that correspond to one of scenarios S1 through S8 (see Table 1) can be selected based on a preference that is listed in Table 2. Alternatively, an available operational configuration may be selected with the highest overall preference ranking. At 812, watermark extraction and/or content screening operations are conducted by the appropriate devices that were selected at 810. It should also be noted that content screening operations at 812 may simply comprise receiving an existing watermark extraction record from a trusted device (or from a secure storage location that is known to a trusted device) and conducting screening in accordance with the received extraction record (e.g., see steps 212 to 218 of FIG. 2). In other embodiments, where a pre-existing watermark extraction record

does not exist (or cannot be accessed), watermark extraction and/or content screening operations can be performed, at 812, by one or more trusted devices.

[0127] If, at 806 in FIG. 8, the determination is "NO", the process moves to 814, where it is determined if only one device is trusted. Such a determination can be made when, for example, a trusted content client device fails to authenticate a content server. Alternatively, as will be described in the sections that follow, a central authority can make such a determination. If only one device is trusted (i.e., "YES" at 814), the trusted device determines the proper configuration for conducting the watermark extraction and/or screening operations, at 816. In doing so, the trusted device may utilize the services of other trusted devices inside or outside of the home network. Upon determining the proper configuration, the process moves to 812, where watermark extraction and/or content screening operations are conducted. If, at 814, it is determined that none of the devices are trusted (i.e., "NO" at 814), the process may be aborted (e.g., content access is denied) at 818. Alternatively, the content may be provided in a protected format (e.g., in encrypted format). In some embodiments, the content is delivered in a degraded format. In still other embodiments, only a part of the content is delivered.

[0128] The operations that are described in FIG. 8 may be repeated, at least in-part, when each device within a home network is attempting to acquire a content, to provide a content, or solicit screening services/information from another device within the home network. Further, the above noted operations may also be carried out when at least one of the devices resides outside of the home network, if a mechanism for authentication between the devices inside and outside of the network exists.

[0129] Table 3 provides an exemplary listing of device configuration possibilities that is organized based on the trusted status of the two devices and the availability of watermark extraction and screening capabilities at the two devices. S1 through S8 represent the device configurations that were previously discussed in connection with the exemplary scenarios 1 through 8, respectively.

Table 3 - Operational Configuration Possibilities based on Screening Capabilities

				Content Client Device				
				Trusted				Not Trusted
				Watermark Extraction Available		Watermark Extraction Not Available		
				Screening Available	Screening Not Available	Screening Available	Screening Not Available	
Content Server	Trusted	Watermark Extraction Available	Screening Available	S1, S2, S3, S4, S5, S6, S7, S8	S3, S4, S5, S6, S8	S2, S3, S4, S5, S6, S7	S3, S4, S5, S6	S4, S5, S6
			Screening Not Available	S1, S2, S3, S6, S7	S3, S6	S2, S3, S6, S7	S3, S6	S6
		Watermark Extraction Not Available	Screening Available	S1, S2, S3, S5, S6, S8	S3, S5, S6, S8	S2, S3, S5, S6	S3, S5, S6	S5, S6
			Screening Not Available	S1, S2, S3, S6	S3, S6	S2, S3, S6	S3, S6	S6
	Not trusted			S1, S2, S3	S3	S2, S3	S3	N/A

[0130] Table 3 illustrates the availability of different operational configurations based on the trusted status of each device and the available screening capabilities in accordance with an exemplary embodiment. Once it is determined which of the operational configurations are available, a particular configuration can be selected to effect the desired screening operations. For example, as noted earlier, a configuration that provides the best overall preference ranking may be selected.

[0131] By providing watermark extraction and screening capabilities to various devices and at various points of content distribution, secure distribution of content can be enabled. Separation of watermark extraction and screening operations further facilitates the proliferation of "compliant" devices with limited computational resources (such as mobile devices). Such compliant devices are trusted devices that can, for example, implement only a portion of watermark extraction and/or screening capabilities, and rely on other devices to provide the remaining operational capabilities. FIG. 9 is an exemplary diagram of different content distribution scenarios involving a compliant content server 902, a non-compliant

content server 904, a compliant content client device 906, a non-compliant content client device 908, as well as protected and unprotected content. A protected content can be protected by a content protection mechanism, such as encryption. In such a scenario, as illustrated at 910, the protected content can be played by, and is thus delivered to, a compliant content client device 906 that is capable of decrypting the content. This is illustrated at 910. However, it should be noted that such a protected content may also be delivered to, at 920, the non-compliant content client device 908. The non-compliant content client device 908 may be able to use the protected content, if, for example, it has acquired the necessary decryption capability. Such a capability can be acquired, for example, illegally (e.g., a device is hacked or encryption keys are stolen), or legally (e.g., if the content owner decides to temporarily grant the capability to a non-compliant client device 908).

[0132] Referring back to FIG. 9, the unprotected content, at 912, may be delivered from the compliant content server 902 to the compliant content client device 906, which performs the watermark extraction and/or screening operations. An unprotected content may also be delivered, at 916, from the non-compliant content server 904 to the compliant content client device 906, which screens the content. The compliant content device 906 may employ one of the previously noted cooperative methods to efficiently screen the unprotected content. FIG. 9 also illustrates that an unprotected content may be delivered, at 914, from the compliant content server 902 to a non-compliant client content device 908. In this scenario, the compliant content server 902 performs the necessary watermark extraction and screening prior to delivering the content.

[0133] The exemplary content delivery architecture that is depicted in FIG. 9 also accounts for the delivery, at 918, of an unprotected content (e.g., a pirated content) from the non-compliant content server 904 to the non-compliant content client device 908. As noted earlier, to reduce the likelihood of unauthorized content use, the proliferation of compliant content client devices may be encouraged by providing incentives to the content users. Further, blocking the delivery of protected content (or delivery of a partial content), at 920, to a non-compliant client device 908 can encourage the user to acquire a compliant device. Such an upgrade is facilitated in accordance with the disclosed embodiments, since the non-compliant content client device 908 may only be required to acquire some or all of the screening capabilities. Acquisition of such screening capabilities enables the device to receive protected content (e.g., at 920). In addition, through the use of cooperative extraction

methods described earlier, the device can receive and screen unprotected content from a non-compliant content server 904.

[0134] As discussed earlier, it is possible that the compliant device, e.g. 902 or 906, does not have the appropriate codecs that are required to perform watermark extraction and/or screening of a content that is encoded in a specific media format. One of the following polices may be applied to this situation: 1) stop the transfer or use of the content; 2) use one of the invocation or delegation models to conduct the watermark extraction and/or screening; 3) allow the limited or unlimited transfer or use of the content (the limitations may include a maximum number of times that such transfer or usage is allowed).

[0135] In another embodiment that is particularly applicable to centralized architectures, cooperative watermark extraction in accordance with the disclosed embodiment may be implemented in situations where a special trusted device (e.g., a "gateway" 614 that is depicted in FIG. 6) coordinates and controls other devices to enable content sharing and consumption, as well as watermark extraction, screening and digital rights management. As such, the gateway device may coordinate watermark extraction, transfer of extraction records, authentication operations, communication and/or acquisition of trusted device lists, and the like. The gateway device typically resides inside of a home network (e.g., a DLNA-compliant network). In some embodiments, the communications between the gateway and the various devices are encrypted.

[0136] The gateway device, which may be controlled directly by a service provider, can be responsible for assigning watermark extraction tasks to one or more capable and trusted devices in a home network. For example, the gateway device can be the only device that is authorized to acquire and decrypt a protected content and/or to serve such a protected content in a home network. The gateway device may further be able to control a compliant content server for content discovery, exposure, serving and transport. The gateway device can also control a compliant content client device for content rendering.

[0137] In another example, the gateway device may be, additionally or alternatively, responsible for determining the appropriate operational configurations that are necessary to conduct the various screening operations. The gateway device may also direct and synchronize the trusted devices to conduct the screening operations. For example, the gateway may use one of the invocation and delegation models to effect the necessary

screening operations. In some embodiments, trusted device authentication operations may also be conducted by the gateway device. Additionally, the gateway device may maintain a revocation list and may have the authority to revoke the trusted status of a device within the network. Further, the gateway device may retain usage rules associated with different embedded watermarks. Such usage rules may be used to prescribe various enforcement actions. Such usage rules may also be communicated to various trusted devices. The gateway device may also control screening and update the usage rules for policy enforcement.

[0138] In still other embodiments, the gateway device may be in communication with one or more external device (e.g., another gateway device, a content server device, a content client device, etc.) that reside outside of the home network. In these embodiments, the gateway device may control the flow of content, authentication information and other information between the home network and the external devices.

[0139] According to some embodiments, all watermark extraction records may be stored in a central location that is accessible by the gateway. The watermark extraction records may additionally be duplicated on other devices on a home network. Further improvements in screening efficiency can be achieved by secure and private exchange of watermark extraction records. The exchange must be conducted between trusted devices either within the home network (e.g., a DLNA-compliant network) or from a cloud space via Internet. Exchange of extraction records may occur during the authentication of two devices so that the security, including confidentiality and integrity, is ensured. For example, using the DTCP-IP's authentication protocol, any information (such as the extraction records) can be securely exchanged between the two devices.

[0140] A need for the exchange of extraction records between two devices may arise if one of the devices does not have the extraction records. In this scenario, the records may be copied from one device onto the other device. In another scenario, an exchange of records may be necessary to merge and synchronize the records of both devices. In these situations, the exchange of records may be conducted in the following manner. If an extraction record of a content item identified by its file name or hash code on the first device does not exist in the records on the second device, the missing record can be added to the second device (and vice verse). If, on the other hand, a record for the same content item exists on both devices,

the record with the latest date and time stamp (e.g., last modification date and time) is used to synchronize the contents of the two devices.

[0141] When the extraction records associated with a user are kept in the cloud, they can be considered as part of a central "virtual records" repository which allows or denies the user to render a content. These virtual records can be organized in several ways. In one example embodiment, each user has a private virtual locker in the cloud for the extraction records corresponding to the content files in his/her home network. The advantage of this configuration is that the user can ubiquitously access the records to receive permissions to render his/her content. In another example embodiment, all virtual records from all users (e.g., all users in a geographic region or all users of a service provider) are stored in a universal locker. The extraction records can be indexed by the hash code. Thus, only one record is needed to be stored in the cloud for a content item, from which a unique hash code can be produced. One advantage of such organization is that these records are anonymous and less redundant.

[0142] In some embodiments, only a portion of the extraction records is stored in the cloud. In one example, only the extraction records that correspond to successful content access requests are stored in the cloud. In another example, only the extraction records that correspond to unsuccessful content access requests are stored in the cloud. In other embodiments, the privacy of the users is protected by either using a trusted service or by obfuscating the source of the query. In still other embodiments, certain users are given enhanced privileges to facilitate access and exchange of extraction records. For example, such privileges may be granted to users with no record of unsuccessful content access requests, whereas users with a history of unsuccessful content access requests may have to accept some delays associated with additional authentication and verification operations.

[0143] It is understood that the various embodiments of the present invention may be implemented individually, or collectively, in devices comprised of various hardware and/or software modules and components. These devices, for example, may comprise a processor, a memory unit, an interface that are communicatively connected to each other, and may range from desktop and/or laptop computers, to consumer electronic devices such as media players, mobile devices and the like. For example, FIG. 10 illustrates a block diagram of a device 1000 within which the various disclosed embodiments may be implemented. The device 1000 comprises at least one processor 1002 and/or controller, at least one memory 1004 unit

that is in communication with the processor 1002, and at least one communication unit 1006 that enables the exchange of data and information, directly or indirectly, through the communication link 1008 with other entities, devices and networks. The communication unit 1006 may provide wired and/or wireless communication capabilities in accordance with one or more communication protocols, and therefore it may comprise the proper transmitter/receiver antennas, circuitry and ports, as well as the encoding/decoding capabilities that may be necessary for proper transmission and/or reception of data and other information. The exemplary device 1000 that is depicted in FIG. 10 may be integrated into as part of a content handling device 100, a master device 404, a slave device 412, a delegating device 504, a delegated device 510 and/or a destination device 514 that are depicted in FIGs. 1, 4 and 5.

[0144] Referring back to FIG. 1, any one of the watermark extractor 104, the digital signature generator 106, the encryption component 108, the authentication component 120 and the like may be implemented in software, hardware, firmware, or combinations thereof. Similarly, the various components or sub-components within each module may be implemented in software, hardware or firmware. The connectivity between the modules and/or components within the modules may be provided using any one of the connectivity methods and media that is known in the art, including, but not limited to, communications over the Internet, wired, or wireless networks using the appropriate protocols.

[0145] Various embodiments described herein are described in the general context of methods or processes, which may be implemented in one embodiment by a computer program product, embodied in a computer-readable medium, including computer-executable instructions, such as program code, executed by computers in networked environments. A computer-readable medium may include removable and non-removable storage devices including, but not limited to, Read Only Memory (ROM), Random Access Memory (RAM), compact discs (CDs), digital versatile discs (DVD), etc. Therefore, the computer-readable media that is described in the present application comprises non-transitory storage media. Generally, program modules may include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types. Computer-executable instructions, associated data structures, and program modules represent examples of program code for executing steps of the methods disclosed herein. The particular sequence of such executable instructions or associated data structures represents

examples of corresponding acts for implementing the functions described in such steps or processes.

[0146] The foregoing description of embodiments has been presented for purposes of illustration and description. The foregoing description is not intended to be exhaustive or to limit embodiments of the present invention to the precise form disclosed, and modifications and variations are possible in light of the above teachings or may be acquired from practice of various embodiments. The embodiments discussed herein were chosen and described in order to explain the principles and the nature of various embodiments and its practical application to enable one skilled in the art to utilize the present invention in various embodiments and with various modifications as are suited to the particular use contemplated. The features of the embodiments described herein may be combined in all possible combinations of methods, apparatus, modules, systems, and computer program products.

CLAIMS

What is claimed is:

1. A method, comprising:

receiving a request for access to a content at a first device from a second device, the first device operating in a network;

performing device authentication to ascertain a trusted status associated with one or both of the first and second devices; and

determining an operational configuration for performing watermark extraction and content screening operations using of one or more trusted devices.

2. The method of claim 1, wherein

the second device is a trusted content client device; and

the second device is configured to perform the watermark extraction and screening operations.

3. The method of claim 1, wherein

the second device is a trusted content client device;

a trusted slave device is configured to perform the watermark extraction operation and provide information associated with the watermark extraction to the second device; and

the second device is configured to perform the screening operation.

4. The method of claim 1, wherein

the second device is a trusted content client device; and

a trusted delegated device is configured to perform the watermark extraction and screening operations.

5. The method of claim 1, wherein

the first device is a trusted content server; and

the first device is configured to perform the watermark extraction and screening operations.

6. The method of claim 1, wherein

the first device is a trusted content server;

a trusted slave device is configured to perform the watermark extraction operation and provide information associated with the watermark extraction to the first device; and

the first device is configured to perform the screening operation.

7. The method of claim 1, wherein

the first device is a trusted content server; and

a trusted delegated device is configured to perform the watermark extraction and screening operations.

8. The method of claim 1, wherein

the first device is a trusted content server;

the second device is a trusted content client device; and

the first device is configured to perform the watermark extraction operation; and

the second device is configured to perform the screening operation.

9. The method of claim 1, wherein

the first device is a trusted content server;

the second device is a trusted content client device; and

the second device is configured to perform the watermark extraction operation; and

the first device is configured to perform the screening operation.

10. The method of claim 1, further comprising:

receiving a device authentication certificate at the first device from the second device;

verifying an authenticity of the certificate; and

ascertaining capabilities of the second device.

11. The method of claim 10, wherein

the certificate comprises information indicative of at least a portion of the capabilities of the second device; and

ascertained capabilities of the second device comprises a capability to conduct some or all of the watermark extraction and content screening operations.

12. The method of claim 11, wherein:

the certificate is a digital transmission content protection over Internet protocol (DTCP-IP) certificate; and

information regarding the capabilities of the second device is carried as part of the DCTP-IP certificate.

13. The method of claim 10, wherein the ascertained capabilities of the second device comprises a capability to grant computational and memory resources to other devices.

14. The method of claim 1, further comprising;

receiving a device authentication certificate at the second device from the first device;

verifying an authenticity of the certificate received from the first device; and

ascertaining capabilities of the first device.

15. The method of claim 14, wherein the ascertained capabilities of the first device comprises a capability to conduct some or all of the watermark extraction and/or content screening operations.

16. The method of claim 1, wherein the operational configuration designates at least one of the first and the second devices to conduct the watermark extraction and content screening operations in accordance with a factor selected from the group consisting of:

availability of computational resources;

availability of watermark extraction and screening capabilities;

an integration for a

a consumer

a processing performance; and

an overall preference ranking.

17. The method of claim 1, wherein the request for access to the content is initially received at a gateway device configured to:

coordinate operations of a plurality of devices within a network;

coordinate device authentication to ascertain a trusted status associated with one or both of the first and second devices; and

determine the operational configuration for performing watermark extraction and content screening operations using of one or more trusted devices.

18. The method of claim 17, wherein the gateway device is configured to communicate with the one or more trusted devices to commence the watermark extraction and/or content screening operations.

19. The method of claim 17, wherein the gateway device is configured to revoke a trusted status of a device within the network.

20. The method of claim 17, wherein the gateway device is configured to retain a content use policy associated with embedded watermarks.

21. A device, comprising:

a processor; and

a memory, including processor executable code, the processor executable code when executed by the processor configures the device to:

receive a request for access to a content at a first device from a second device, the first device operating in a network;

perform device authentication to ascertain a trusted status associated with one or both of the first and the second devices; and

determine an operational configuration for performing watermark extraction and content screening operations using one or more trusted devices.

22. The device of claim 21, wherein processor executable code when executed by the processor configures the device to:

receive a device authentication certificate at the first device from the second device;

verify an authenticity of the certificate; and

ascertain capabilities of the second device.

23. The device of claim 22, wherein

the certificate comprises information indicative of at least a portion of the capabilities of the second device; and

ascertained capabilities of the second device comprises a capability to conduct some or all of the watermark extraction and content screening operations.

24. The device of claim 22, wherein:

the certificate is a digital transmission content protection over Internet protocol (DTCP-IP) certificate; and

information regarding the capabilities of the second device is carried as part of the DCTP-IP certificate.

25. The device of claim 22, wherein the ascertained capabilities of the second device comprises a capability to grant computational and memory resources to other devices.

26. A computer program product, embodied on a non-transitory computer readable medium, comprising:

program code for receiving a request for access to a content at a first device from a second device, the first device operating in a network;

program code for performing device authentication to ascertain a trusted status associated with one or both of the first and the second devices; and

program code for determining an operational configuration for performing watermark extraction and content screening operations using one or more trusted devices.

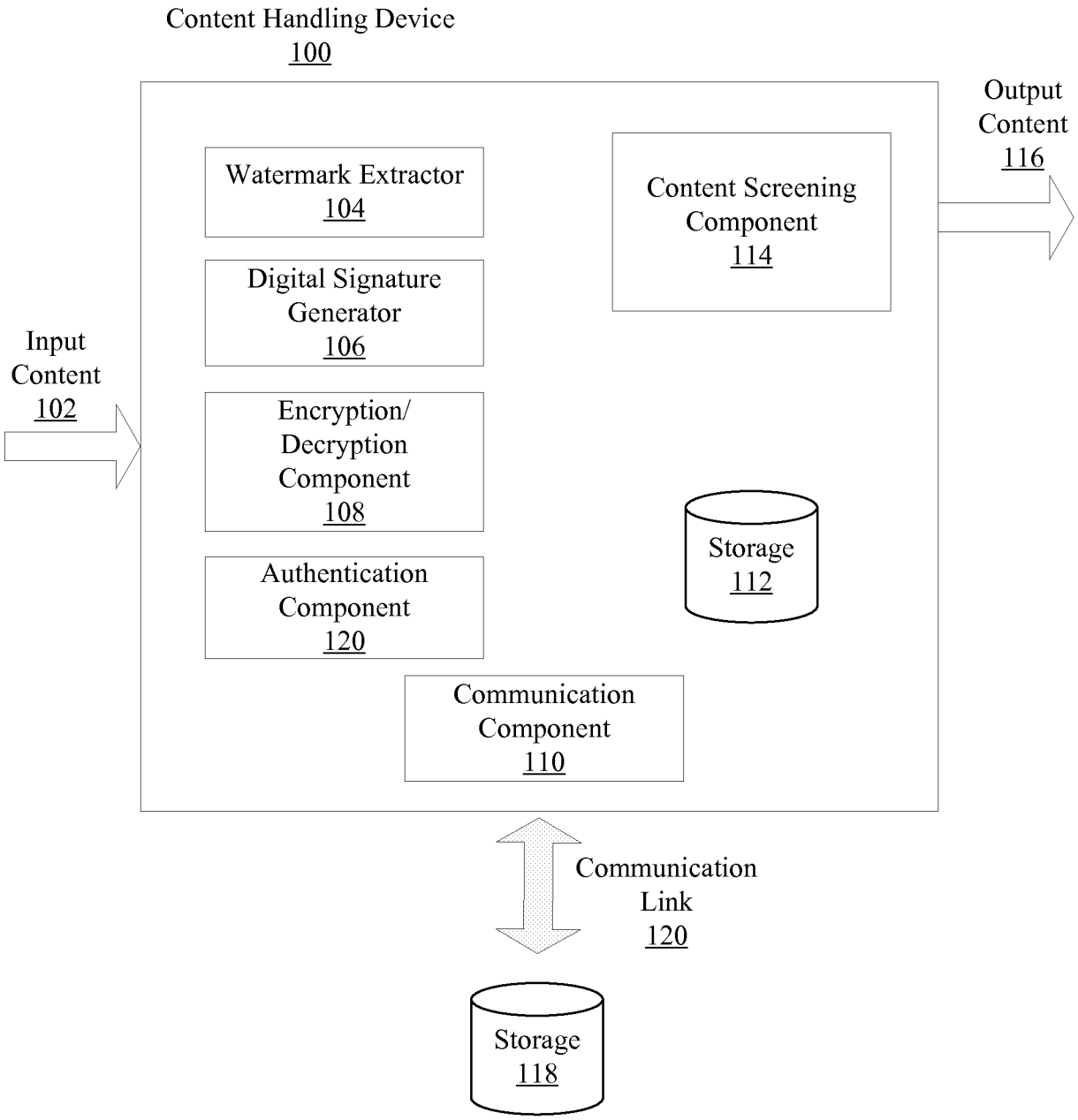
Content Handling Device
100
Watermark Extractor
104
Digital Signature
Generator
106
Encryption/
Decryption
Component
108
Authentication
Component
120
Content Screening
Component
114
Storage
112
Communication
Component
110
Input
Content
102
Output
Content
116
Communication
Link
120
Storage
118

FIG. 1

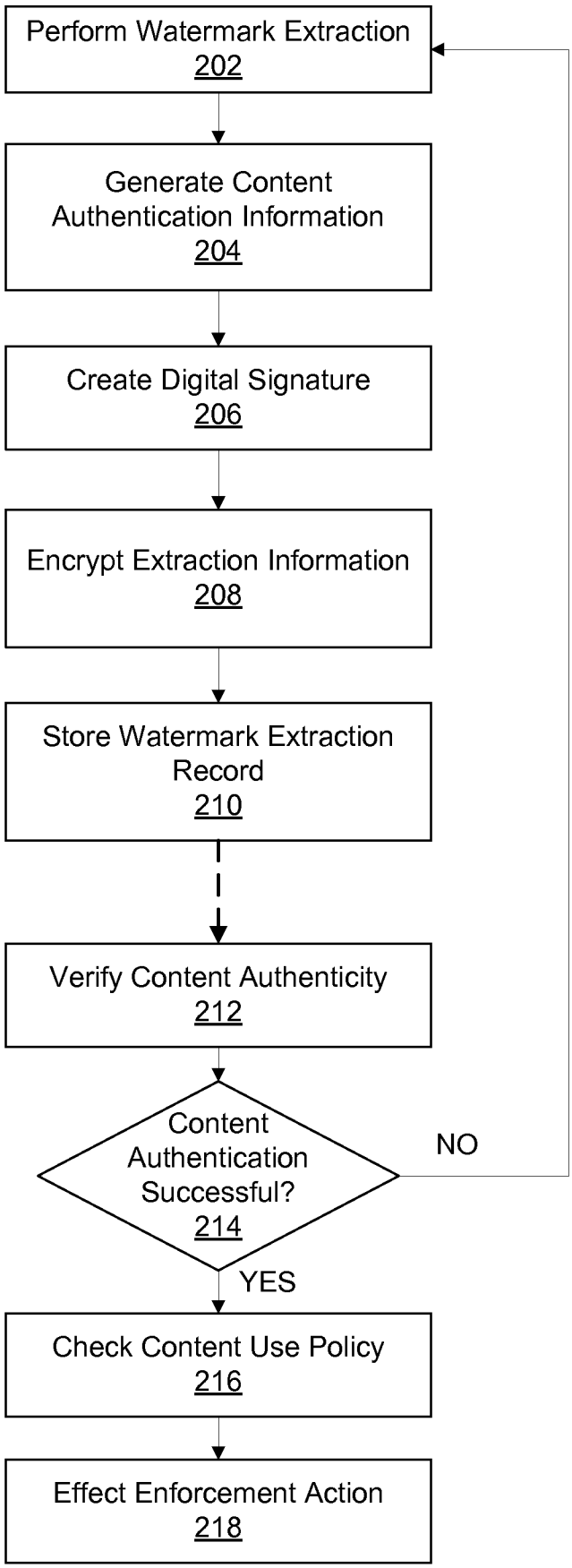
Perform Watermark Extraction
202
Generate Content Authentication Information
204
Create Digital Signature
206
Encrypt Extraction Information
208
Store Watermark Extraction Record
210
Verify Content Authenticity
212
Content Authentication Successful?
214
NO
YES
Check Content Use Policy
216
Effect Enforcement Action
218

FIG. 2

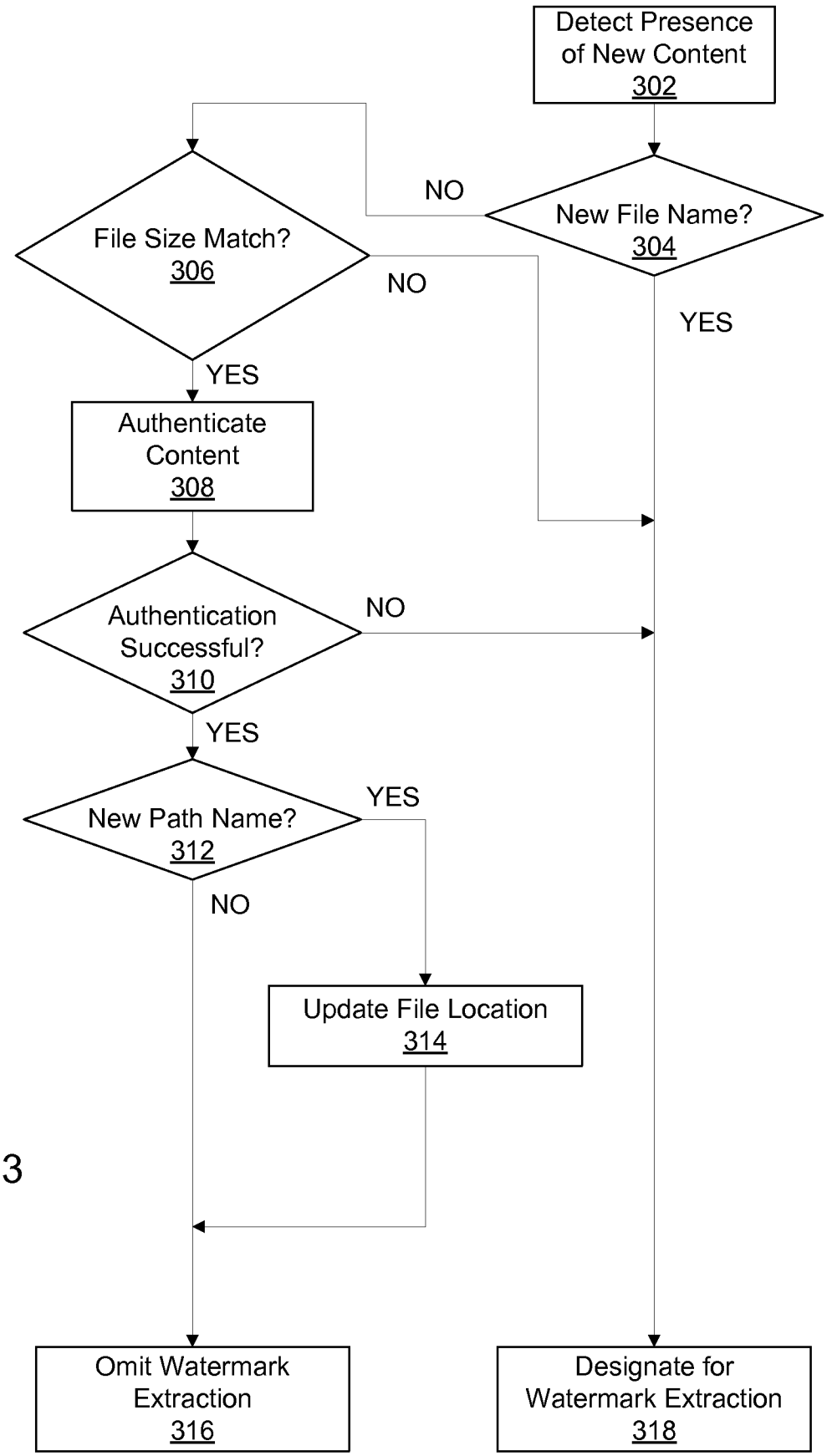
Detect Presence of New Content 302
New File Name? 304
NO
File Size Match? 306
NO
YES
YES
Authenticate Content 308
Authentication Successful? 310
NO
YES
New Path Name? 312
YES
NO
Update File Location 314
Omit Watermark Extraction 316
Designate for Watermark Extraction 318

FIG. 3

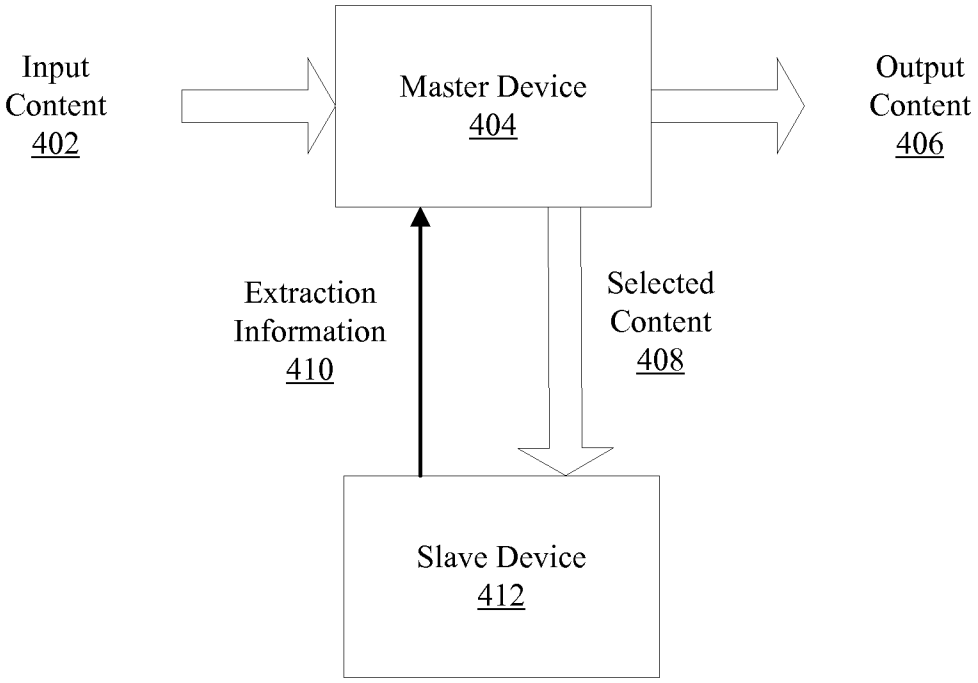
Input
Content
402
Master Device
404
Output
Content
406
Extraction
Information
410
Selected
Content
408
Slave Device
412

FIG. 4

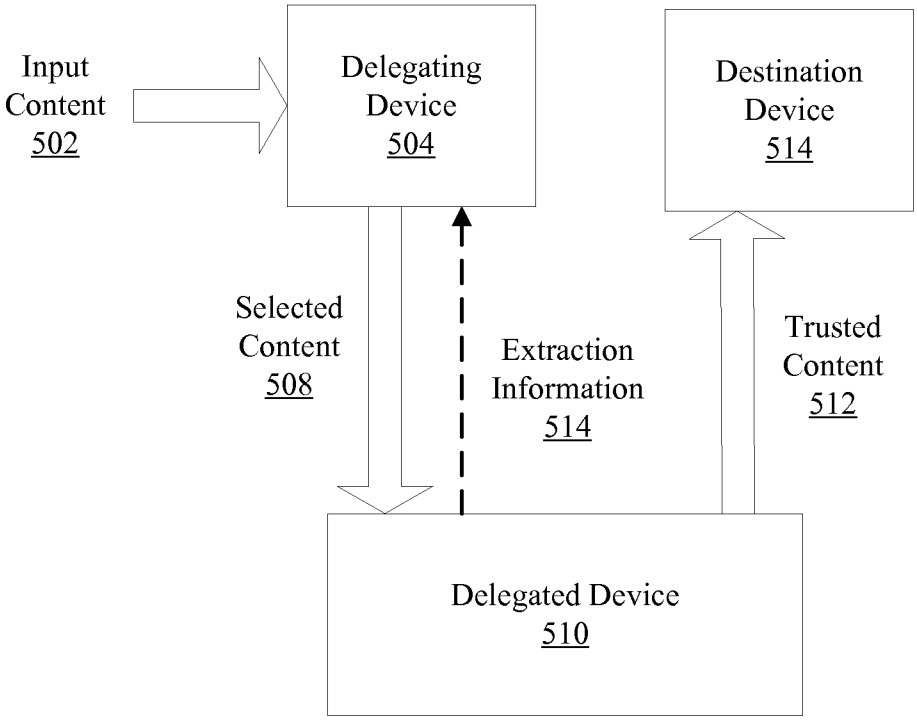
Input
Content
502
Delegating
Device
504
Destination
Device
514
Selected
Content
508
Extraction
Information
514
Trusted
Content
512
Delegated Device
510

FIG. 5

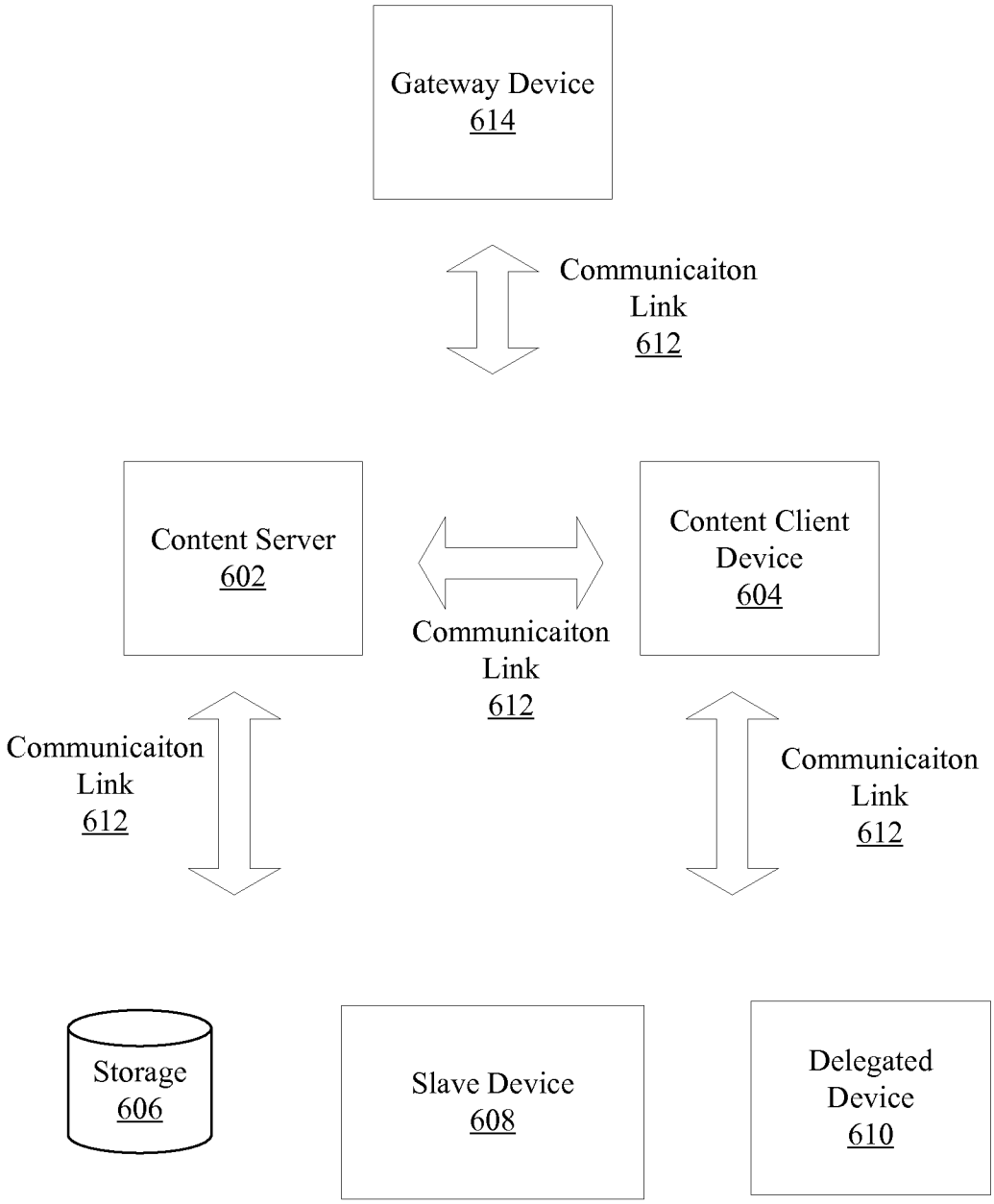
Gateway Device
614
Communicaiton
Link
612
Content Server
602
Communicaiton
Link
612
Content Client
Device
604
Communicaiton
Link
612
Communicaiton
Link
612
Storage
606
Slave Device
608
Delegated
Device
610

FIG. 6

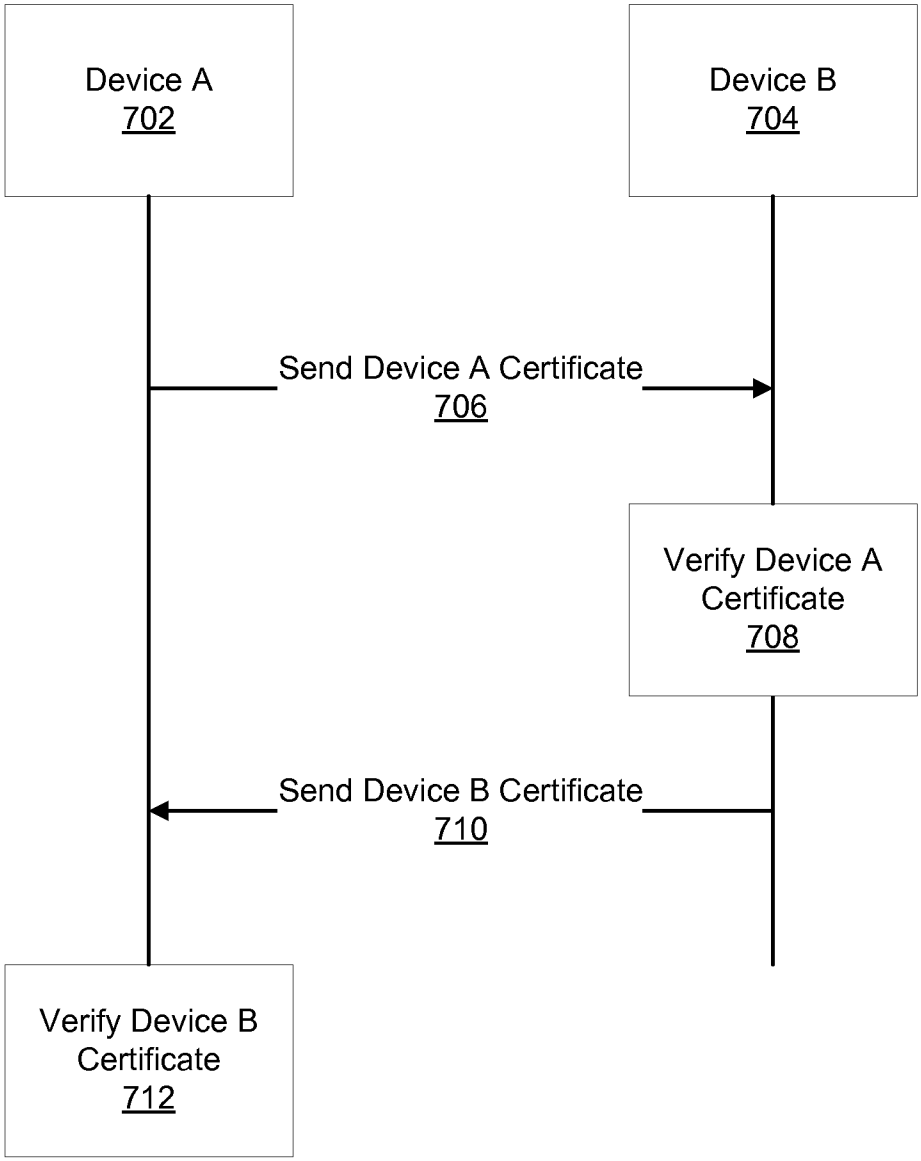
Device A
702
Device B
704
Send Device A Certificate
706
Verify Device A Certificate
708
Send Device B Certificate
710
Verify Device B Certificate
712

FIG. 7

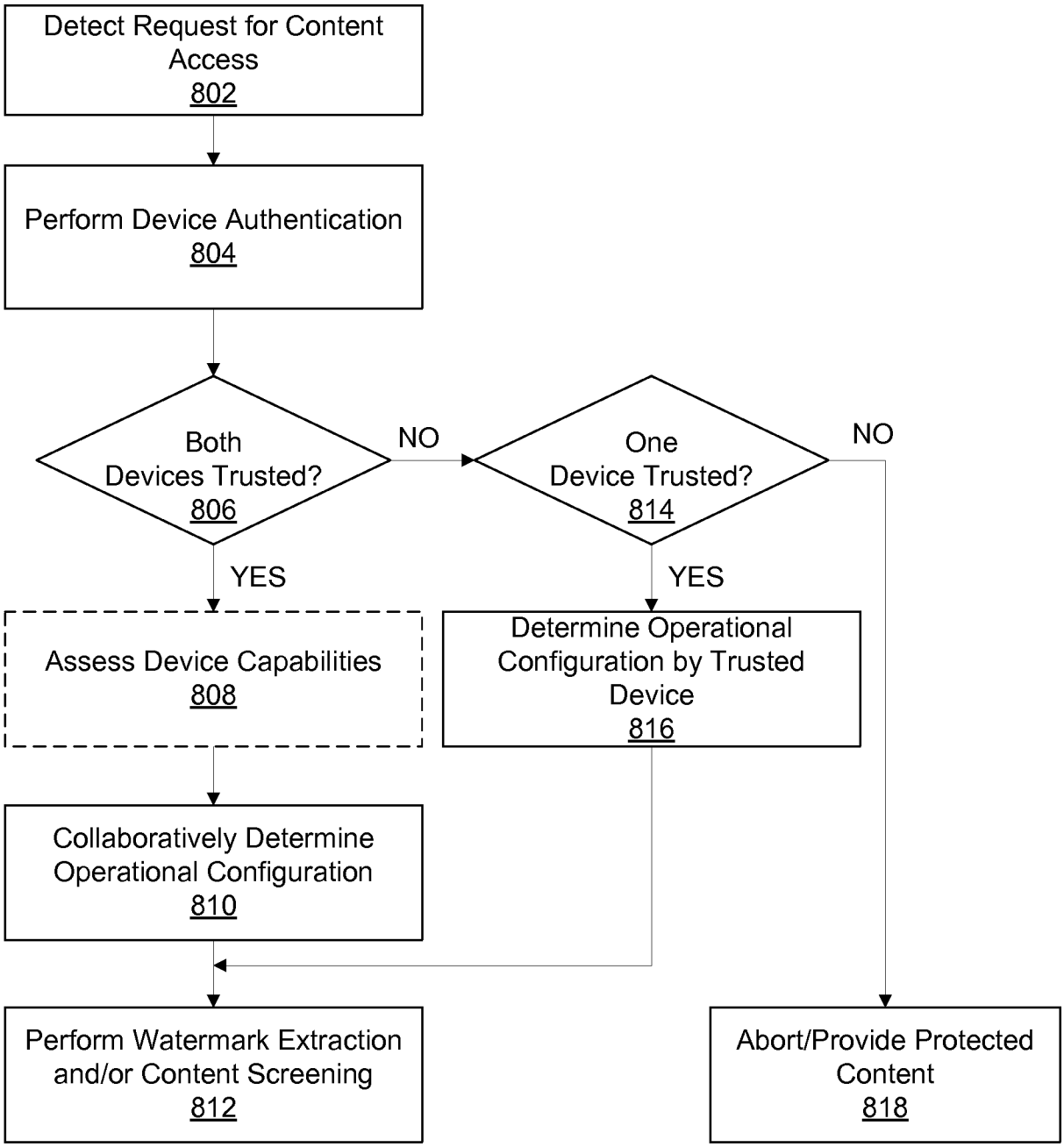
Detect Request for Content Access
802
Perform Device Authentication
804
Both Devices Trusted?
806
NO
One Device Trusted?
814
NO
YES
YES
Assess Device Capabilities
808
Determine Operational Configuration by Trusted Device
816
Collaboratively Determine Operational Configuration
810
Perform Watermark Extraction and/or Content Screening
812
Abort/Provide Protected Content
818

FIG. 8

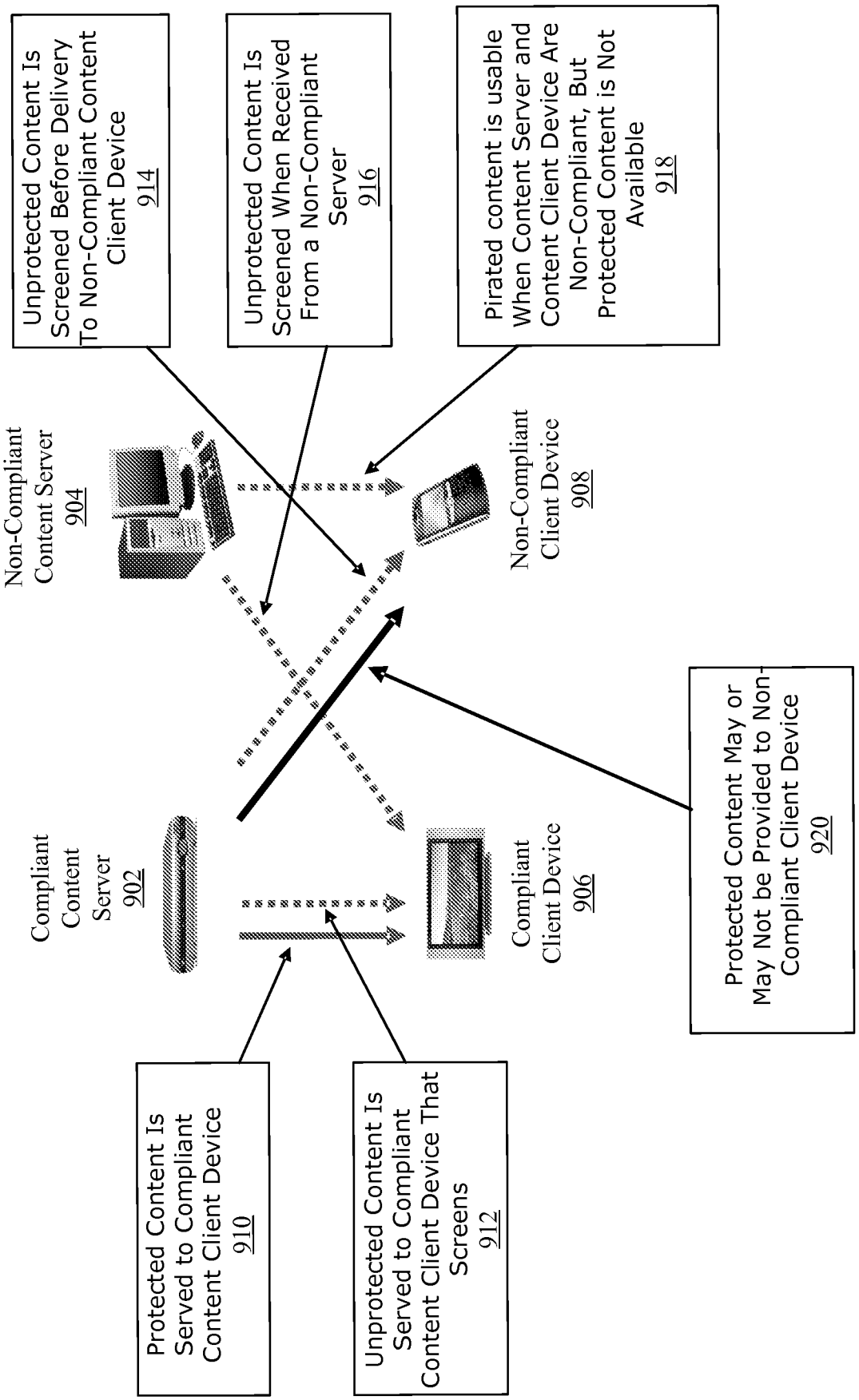
Unprotected Content Is Screened Before Delivery To Non-Compliant Content Client Device 914
Unprotected Content Is Screened When Received From a Non-Compliant Server 916
Pirated content is usable When Content Server and Content Client Device Are Non-Compliant, But Protected Content is Not Available 918
Non-Compliant Content Server 904
Non-Compliant Client Device 908
Compliant Content Server 902
Compliant Client Device 906
Protected Content May or May Not be Provided to Non-Compliant Client Device 920
Protected Content Is Served to Compliant Content Client Device 910
Unprotected Content Is Served to Compliant Content Client Device That Screens 912

FIG. 9

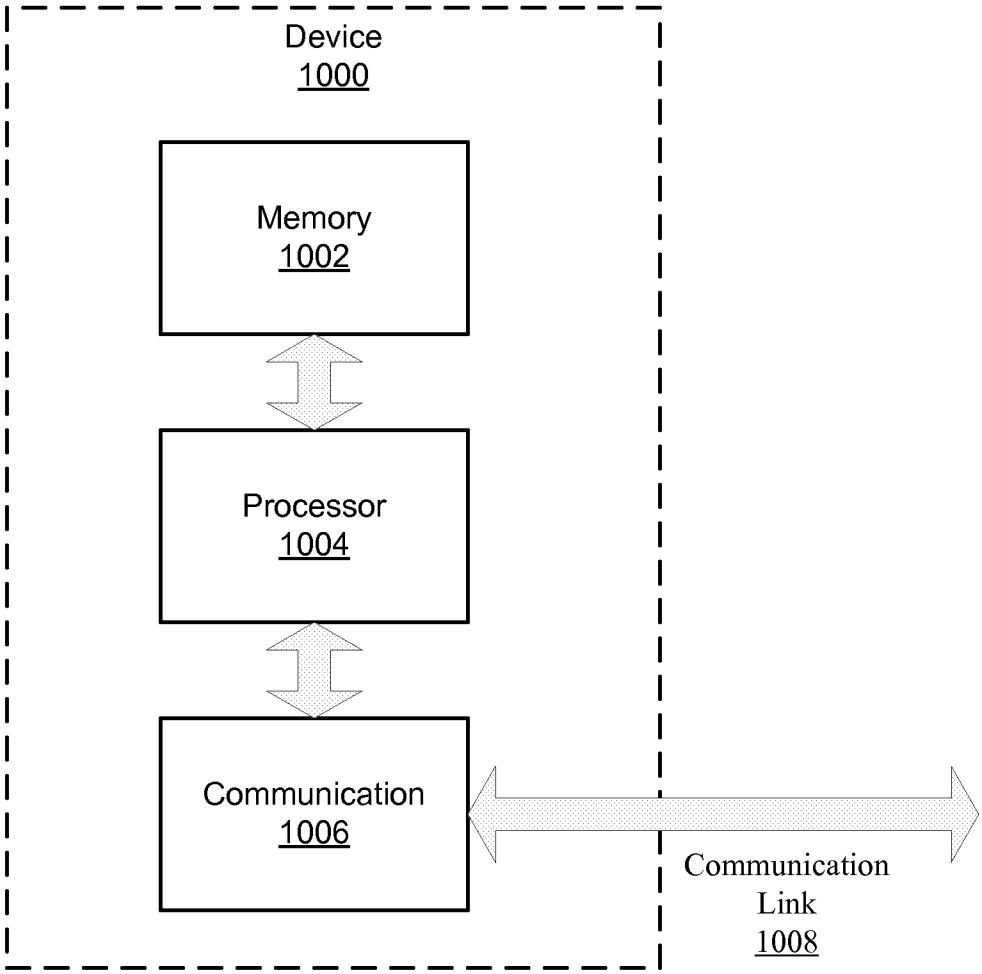
Device
1000
Memory
1002
Processor
1004
Communication
1006
Communication
Link
1008

FIG. 10