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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 July 2008 (24.07.2008)

PCT

(10) International Publication Number
WO 2008/088201 A1

(51) **International Patent Classification:**
G06F 17/00 (2006.01)

(21) **International Application Number:**
PCT/KR2008/000378

(22) International Filing Date: 21 January 2008 (21.01.2008)

(25) Filing Language: Korean

(26) Publication Language: English

(30) Priority Data:

60/885,748	19 January 2007 (19.01.2007)	US
60/886,130	23 January 2007 (23.01.2007)	US
60/887,949	2 February 2007 (02.02.2007)	US
60/889,794	14 February 2007 (14.02.2007)	US
60/890,269	16 February 2007 (16.02.2007)	US
60/891,275	23 February 2007 (23.02.2007)	US
60/894,050	9 March 2007 (09.03.2007)	US
60/980,452	17 October 2007 (17.10.2007)	US

(71) **Applicant** *(for all designated States except US):* **LG ELECTRONICS INC.** [KR/KR]; 20, Yeouido-dong, Yeongdeungpo-gu, Seoul 150-721 (KR).

(72) Inventors; and

(75) Inventors/Applicants *(for US only):* **CHO, Sung Hyun** [KR/KR]; NAS Group, DM Lab., LG R & D Campus, #16, Umyeon-dong, Seocho-gu, Seoul 137-724 (KR). **CHUNG, Min Gyu** [KR/KR]; NAS Group, DM Lab., LG R & D Campus, #16, Umyeon-dong, Seocho-gu, Seoul 137-724 (KR). **PAK, Koo Yong** [KR/KR]; NAS Group, DM Lab., LG R & D Campus, #16, Umyeon-dong, Seocho-gu, Seoul 137-724 (KR). **PARK, Il Gon** [KR/KR]; NAS Group, DM Lab., LG R & D Campus, #16, Umyeon-dong, Seocho-gu, Seoul 137-724 (KR). **JEONG, Man Soo** [KR/KR]; NAS Group, DM Lab., LG R & D Campus, #16, Umyeon-dong, Seocho-gu, Seoul 137-724 (KR).

(74) **Agent: YANG, Moon Ock;** S & IP Patent & Law Firm, Pangaea Bldg., 2F., #67-8, Yangjae-dong, Seocho-gu, Seoul 137-130 (KR).

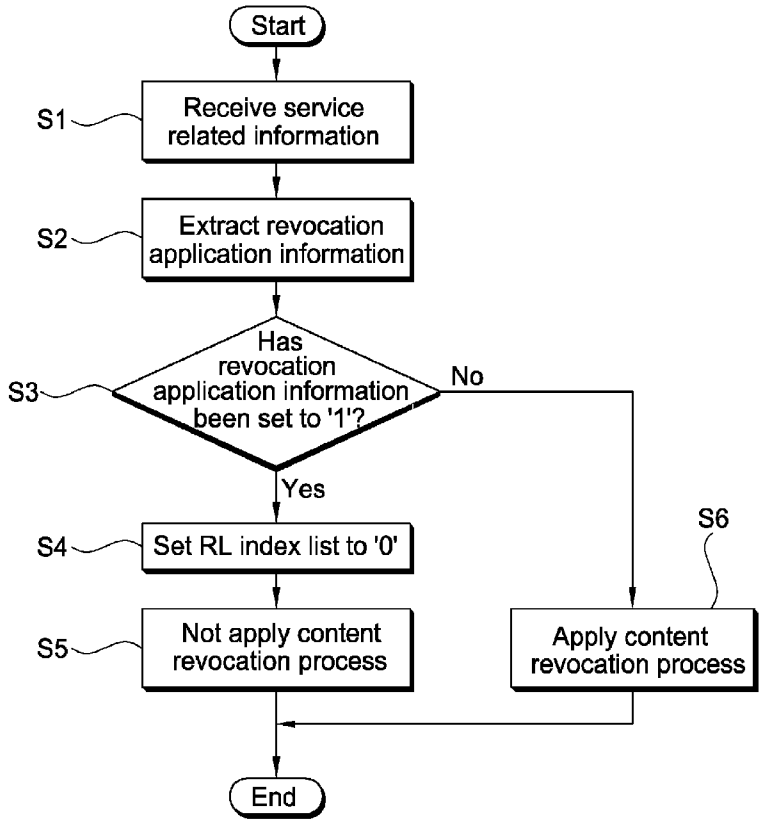
(81) **Designated States** *(unless otherwise indicated, for every kind of national protection available):* AE, AG, AL, AM, AO, AT, **AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ,** CA, **CH,** CN, CO, CR, **CU, CZ, DE, DK, DM, DO, DZ,** EC, EE, EG, ES, **FI, GB, GD,** GE, **GH, GM,** GT, **HN, HR, HU, ID,**

[Continued on next page]

(54) Title: METHOD FOR PROTECTING CONTENT AND METHOD FOR PROCESSING INFORMATION

(57) Abstract: Disclosed are a method of protecting content and a method of processing information. The method of protecting content can include service related information including revocation application information of content from the outside by employing a content management and protection system, and apply or not apply a content revocation process on the content according to the revocation application information. Accordingly, whether to apply a content revocation process can be controlled according to revocation application information.

[Fig. 4]



WO 2008/088201 A1

IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available):* ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *with amended claims and statement*

Description

METHOD FOR PROTECTING CONTENT AND METHOD FOR PROCESSING INFORMATION

Technical Field

[1] The present invention relates to a method of protecting content and a method of processing information, and more particularly, to content protection and information processing technologies which can control whether or not to perform a content revocation process by employing revocation application information included in a specific information signal received from the outside.

Background Art

[2] In recent years, as the commercialization of wired/wireless Internet, the intelligence and networking of home appliances, and so on are carried out, digital convergence, which creates new types of services through the convergence of different digital services, has been accelerated. Digital convergence provides service providers with an opportunity to create new profits and expand business and also users with user-oriented services that are able to satisfy complicated and diversified needs.

[3] In line with such digital convergence, the existing broadcasting services have changed to various types of digital broadcasting services by expanding their areas to content services through wired/wireless networks. Digital broadcasting can provide a good quality of broadcasting content through a wired network or a wireless network and also provide an expanded concept of services through association with digital home environments, etc. A representative example of the expanded concept of service may include a content sharing service, etc., in which broadcasting content is stored using a personal recorder, and the like and then moved to another devices for use purpose within digital home environments.

[4] However, for the purpose of this content sharing service, and the like, there is a need for a security system capable of preventing illegal use or export of content. In particular, it is necessary to consistently protect content in local areas, such as digital home environments, because broadcasting content is out of the protection range of a security system for content protection when the broadcasting content is transmitted upon content sharing (for example, a CAS (Conditional Access System)).

[5] Accordingly, there have recently been proposed content protection management systems, which can consistently protect pertinent content when broadcasting content is stored in digital home environments, personal recorders, and so on. Active research has been done on technologies which can support the content protection management systems, such as technologies related to content handling, license creation and

management, domain management, revocation application and process, etc.

Disclosure of Invention

Technical Problem

[6] A technical object of the present invention is to provide a technology, which can control whether or not to apply a content revocation process based on revocation application information input from the outside through a specific information signal.

Technical Solution

[7] To achieve the above technical object, the present invention provides a method of protecting content in an aspect. The content protection method may include the steps of receiving revocation application information from an external system, deciding a revocation process mode based on the revocation application information, and mapping revocation information based on the revocation process mode in order to distribute the content to devices on a domain corresponding to an internal system.

[8] To achieve the above technical object, the present invention provides a method of protecting content in another aspect. The content protection method may include the steps of creating revocation application information based on a content attribute, and transmitting the revocation application information so that distribution of the content is controlled based on the revocation application information. Here, a revocation process mode may be decided based on the revocation application information, and the revocation information may be mapped based on the revocation process mode.

[9] To achieve the above technical object, the present invention provides a method of protecting content in still another aspect. The content protection method may include the steps of receiving content distributed based on revocation information, and using the content according to previously set authority information. Here, the revocation information may be mapped based on a revocation process mode and the revocation process mode may be based on revocation application information.

[10] To achieve the above technical object, the present invention provides a method of processing information in further still another aspect. The information processing method may include the steps of, in a method of processing information employing a content management and protection system, receiving service related information, including revocation application information of content, from the outside, and applying or not applying a content revocation process on the content according to the revocation application information. Here, the service related information may be received in the form of a FTA (Free To Air) broadcasting signal.

[11] The revocation application information may be set to any one of a first value, indicating that the content revocation process should not be applied, and a second value, indicating that the content revocation process should be applied.

[12] When the revocation application information is set to the first value, the step of applying or not applying the content revocation process may include the step of setting specific information, which is included in a content license associated with the content, to a specific value on which the content revocation process is not applied. At this time, the specific information may be a revocation list index list associated with the content.

[13] Meanwhile, the information processing method may further include the steps of receiving external content, receiving a great number of information related to the external content, converting the external content into content that can be managed and protected in the content management and protection system, and creating a content license associated with the content by employing the great number of information related to the external content.

[14] Here, the great number of information may include content management and protection information including usage rules information for protecting and managing the content within the content management and protection system, the service related information including generic content protection information for a content providing service, and revocation related information for prohibiting the content from being used in unauthorized devices.

[15] The content management and protection information may include at least any one of copy and movement control information for controlling the copy and movement of content, consumption control information for controlling the consumption of content, propagation control information for controlling content propagation between devices within a domain, output control information for controlling the output of content, and ancillary control information of content.

[16] The content license may include at least any one of content license identification information including information for identifying the content license, content license creator information including information for identifying a creator that has created the content license, compliance/robustness regime information indicating a compliance/robustness regime associated with the content, revocation information associated with the content, authorized domain identification information including identification information of an authorized domain in which the content can be used, descrambling information of the content, and the content management and protection information.

[17] The revocation information may include a list of a revocation list index. Here, the revocation index may be numeric information that is increased by a specific value whenever a new revocation list is issued.

Advantageous Effects

[18] As described above, according to the present invention, whether or not to apply a content revocation process can be controlled according to revocation application in-

formation input through a specific information signal (i.e., a FTA broadcasting signal) from the outside. In particular, the content revocation process may not be applied to specific content based on the revocation application information. Accordingly, content such as urgent messages and public notices, which should be seen by anyone without limitation to devices or domains, can be utilized easily when the content is transmitted.

Brief Description of the Drawings

[19] FIG. 1 is a block diagram schematically showing the concept of a CMP (Content Management and Protection) system;

[20] FIG. 2 is a conceptual view illustrating a function construction of a CMP module shown in FIG. 1;

[21] FIG. 3 is an exemplary view illustrating the format of a CMP content license; and

[22] FIG. 4 is a flowchart illustrating a method of processing information in accordance with a preferred embodiment of the present invention.

[23] <Description of reference numerals of principal elements in the drawings>

[24] CD: CMP device

[25] CM: CMP module

[26] 10: acquisition module

[27] 20: storage module

[28] 30: processing module

[29] 40: consumption module

[30] 50: export module

Mode for the Invention

[31] Hereinafter, the present invention will be described in detail in connection with preferred embodiments with reference to the accompanying drawings in order for those skilled in the art to be able to implement the invention. In the preferred embodiments of the present invention, specific technical terminologies are used for clarity of the content. However, It is to be understood that the present invention is not limited to specific selected terminologies and each specific terminology includes all technical synonyms operating in a similar way in order to accomplish a similar object.

[32] FIG. 1 is a block diagram schematically showing the concept of a CMP system.

[33] As shown in FIG. 1, a CMP system 100 forms a domain 5. The domain 5 is a collection of authorized CMP devices (CDs) and can refer to a region whose reliability for the legal use of content is guaranteed. Content can be moved and used between CMP devices (CDs) registered with the domain 5 within an authorized authority range. This domain 5 can be implemented in a local environment such as a digital home environment.

[34] The CMP device (CD) may refer to a device equipped with a CMP module (CM).

The CMP module (CM) functions to protect and manage content input from the outside to the CMP system 100. For example, the CMP module (CM) can convert content, which is input to the CMP system 100, into a specific type of content, for example, CMP content and can generate a specific type of a CMP content license through which the CMP content can be used. The CMP module (CM) can also protect and manage generated CMP content by controlling the use of the CMP content based on a CMP content license.

[35] The CMP device (CD) can receive content, CMP information (hereinafter abbreviated as CMPI) associated with the content, various pieces of content related information associated with the content, and so on through a wireless network, a wired network or a storage medium. The information can be transmitted to a CMP device (CD) through each defined format, root, and channel.

[36] The CMPI may refer to usage rules information for protecting and managing CMP content in the CMP system 100.

[37] The CMPI can include copy and movement control information for controlling the copy and movement of CMP content, consumption control information for controlling the consumption of CMP content, propagation control information for controlling the propagation of CMP content between CMP devices within a domain, output control information for controlling the output of CMP content, ancillary control information of CMP content, and so on.

[38] The content related information can include service related information, revocation related information, Compliance/Robustness Regime (hereinafter, referred to as C/R regime) related information, etc. of content.

[39] The service related information may refer to generic content protection information for a content providing service. This content service related information can be transmitted from a service provider to a CMP device in the form of a FTA (Free to Air) broadcasting signal. The service related information can include revocation application information, information to indicate whether or not to perform scrambling, remote access control information, and the like.

[40] The revocation related information includes information for preventing content from being used in fraudulent devices, unauthorized devices, etc. For example, the revocation related information can include a revocation list (hereinafter abbreviated as RL) or RL related information. The revocation related information can be transmitted from a service provider side, a server for CMP revocation management, etc. to a CMP device (CD).

[41] The C/R regime related information may refer to information pertinent to policy application rules with respect to content on the service provider side. This C/R regime related information can include information of a C/R regime of a content protection

system applied to content, for example, CA (Conditional Access) or DRM (Digital Rights Management). The C/R regime related information can be transmitted from a service provider side, a content protection system service, etc. to a device.

[42] FIG. 2 is a conceptual view illustrating a function construction of the CMP module shown in FIG. 1.

[43] The CMP module (CM) can include, as shown in FIG. 2, an acquisition module 10, a consumption module 40, an export module 50, a storage module 20, and a processing module 30. The acquisition module 10, the consumption module 40, and the export module 50 can have the concept of a point at which access to the outside exists, and the storage module 20 and the processing module 30 can have the concept of an internal entity.

[44] The acquisition module 10 functions to convert content and content related information, which are input from the outside to the CMP system 100, into a type that can be used within the CMP system 100.

[45] For example, the acquisition module 10 can receive content transmitted from the outside, scramble the received content in a form defined in the CMP system 100, and convert the scrambled content into CMP content (CC). The CMP content (CC) may refer to content of a type that can be protected and managed under the CMP system 100. The acquisition module 10 also generates a CMP content license (CCL) for using CMP content (CC) using externally received CMPI information and content related information.

[46] Content transmitted from the outside to a CMP device (CD) can be clean content, which is received through a trusted transmission method with guaranteed reliability, or scrambled content, which is protected by a content protection system with guaranteed reliability, for example, a CAS or DRM system. In the latter case, pertinent content can be received by a CMP device (CD), scrambled through a CAS module or a DRM module (existing outside the CMP module) included in the CMP device (CD), converted into the form of clean content, and then transmitted to the acquisition module 10. Here, a key for scrambling the content can be obtained by performing an ECM (Entitle Control Message)/EMM (Entitlement Management Message) process on content related information associated with the content.

[47] Meanwhile, a CMP content license (CCL) generated by the acquisition module 10 is bound so that it is associated with corresponding CMP content (CC). At this time, the CMP content license (CCL) can be included in the CMP content (CC) in an embedded form or a form separated from the CMP content (CC).

[48] FIG. 3 is an exemplary view illustrating the format of the CMP content license (CCL).

[49] The CMP content license (CCL) can include, as shown in FIG. 3, a CMP content

license identification information field 62, a CMP content license creator information field 63, a C/R regime information field 64, a revocation information field 65, an authorized domain identification information field 66, a descrambling information field 67, a CMPI field 68, a CMP content license management data field 69, and so on.

[50] The CMP content license identification information field 62 is a field into which CMP content license identification information is inserted. The CMP content license identification information may refer to unique identification information for identifying a corresponding CMP content license.

[51] The CMP content license creator information field 63 is a field into which CMP content license creator information for identifying a creator who has created a CMP content license (CCL) is inserted. For example, the CMP content license creator information may refer to identification information of a CMP module (CM) that has created a corresponding CMP content license (CCL).

[52] The C/R regime information field 64 is a field into which C/R regime information associated with a corresponding CMP content (CC) is inserted. Here, the C/R regime information may refer to information for identifying a C/R regime associated with the CMP content (CC).

[53] The C/R regime may refer to a policy rule of a service provider side or a content protection system (for example, a CAS or DRM) with respect to content. A plurality (for example, eight) of the C/R regimes may be associated with one CMP content (CC). In other words, a plurality of different policy rules defined on the service provider side can be applied to one CMP content (CC). The C/R regime information can be configured to include plural bits, which can be set to, for example, T or '0', and to identify a C/R regime(for example, RL) associated with CMP content.

[54] The revocation information field 65 is a field into which revocation information of a corresponding CMP content (CC) is inserted. The revocation information includes information on which a RL, including information of a CMP device (or a CMP module) or a domain that limits the use of a corresponding CMP content (CC), can be found.

[55] For example, the revocation information may refer to a RL index list. Here, the revocation information field of the RL index can include a RL index list (i.e., the list of RL indices). Here, the RL index is information included in a RL to idenfity the RL. For example, the RL index is a number that is increased by 1 whenever a new RL is issued. In other words, the RL index may refer to information for identifying the most recently issued RL. The RL index list is the list of RL indices and helps to find the most recent RL when using CMP content. Meanwhile, if it is not necessary to apply a RL when using content, the RL in RL index list can be set to, for example, '0'.

[56] The authorized domain identification information field 66 is a field into which domain identification information is inserted. The domain identification information

may refer to identification information of a domain 5 in which CPM content can be used. If CPM content (CC) can be used without limitation to the range of the domain 5, the domain identification information can be set to, for example, '0'.

[57] The descrambling information field 67 is a field into which descrambling information of CMP content (CC) is inserted. The descrambling information can include information about a scrambler that has scrambled the CMP content (CC), descrambling key information, and so on.

[58] The CMPI field 68 is a field into which CMPI is inserted. The CMPI may refer to usage rules information for protecting and managing CMP content (CC) within the CMP system 100. As mentioned earlier, the CMPI can include copy and movement control information, consumption control information, propagation control information, output control information, ancillary control information, etc. of CMP content (CC).

[59] The CMP content license management data information field 69 is a field into which CMP content license management data information is inserted. The CMP content license management data information field 69 can include length information of a CMP content license (CCL), information about an issuer who has issued CMP content license (CCL) finally (for example, certificate information, etc. of a CMP module that has issued a CMP content license finally), and so on.

[60] The information included in the CMP content license (CCL) can be used as license information for controlling use authority of content when the functions of the consumption module 40, the export module 50, the storage module 20, and the processing module 30 are performed on the content.

[61] The consumption module 40 functions to consume CMP content (CC), such as playing CMP content (CC) through sound or video or outputting CMP content (CC) via a digital or analog interface. For example, in order to consume CMP content (CC), the consumption module can extract a descrambling key from a CMP content license (CCL), descramble the CMP content (CC), decode the CMP content (CC), and then output the decoded CMP content (CC), or convert decoded content into analog information and then output or play the converted content. This consumption of the CMP content (CC) can be controlled according to consumption control information, output control information, etc., which are included in CMPI of a CMP content license (CCL).

[62] The export module 50 can function to export CMP content (CC) to another CMP device. In order to export CMP content (CC), not only control information included in CMPI of a CMP content license (CCL), but also C/R regime information, revocation information, and the like of a CMP content license (CCL) can be considered. For example, if the export of specific CMP content (CC) is permitted in control in-

formation of CMPI, but is not authorized in C/R regime information, etc., the content may not be exported.

[63] The storage module 20 can function to store CMP content (CC) in a CMP device (CD). This storage of CMP content (CC) can be controlled according to copy and movement control information, and so on which are included in CMPI of a CMP content license (CCL).

[64] The processing module 30 can function to process CMP content (CC). For example, the processing module 30 can perform a function of trans-coding CMP content (CC) into content with a different compressed format, video resolution, video frame rate, and audio sampling rate, a function of applying video or audio effects, a function of inserting selective data or content factors, a function of extracting still images from video streams, and so on.

[65] FIG. 4 is a flowchart illustrating a method of processing information in accordance with a preferred embodiment of the present invention. This drawing shows a process of determining whether or not to apply a RL according to revocation application information, which is included in service related information of content and received.

[66] Referring to FIG. 4, a CMP device can receive service related information of content from the outside (step: Sl). For example, the CMP device can receive a FTA broadcasting signal from a service provider side. The service related information can include revocation application information, information to indicate whether or not to perform scrambling, remote access control information, and so on.

[67] The revocation application information is information to indicate whether or not to apply a content revocation process for content. Here, the content revocation process may refer to a process of prohibiting access to a device (or a CMP module) or a domain, which exists in a revocation list associated with a corresponding CMP content, by checking the revocation list upon access to a corresponding CMP content.

[68] This revocation application information can be information of 1 bit, which is set to a specific value, for example, a first value (in the present embodiment, it is assumed to be T) or a second value (in the present embodiment, it is assumed to be '0'). Here, when the revocation application information is set to T , it may indicate that the content revocation process should not be applied, and when the revocation application information is set to '0', it may indicate that the content revocation process should be applied.

[69] Meanwhile, a CMP module can convert content into CMP content and create a CMP content license associated with the CMP content.

[70] The CMP module that has received the service related information extracts revocation application information included in the service related information (step: S2) and then determines whether the extracted revocation application information is set

to a first value (for example, T) or a second value (for example, '0') (step: S3).

[71] If the revocation application information is set to the first value, the CMP module sets specific information of the CMP content license to information, indicating that the content revocation process should not be applied. For example, if the revocation application information is set to the value T indicating that the content revocation process should not be applied, the CMP module can set revocation information (i.e., a RL index list) of the CMP content license to '0' (step: S4). Accordingly, the content revocation process is not applied since the RL index list is set to '0' when using the CMP content (step: S5).

[72] On the other hand, when the revocation application information is set to the second value, the CMP module does not need to perform a special setting process since the content revocation process has to be performed normally. In this case, the list of RL indices is included in the revocation information (i.e., the RL index list) of the CMP content license. Accordingly, when performing the content revocation process, the CMP module can perform the revocation process by finding requested RL in the RL index list (step: S6).

[73] As described above, the application of the content revocation process to specific content can be prohibited according to revocation application information transmitted through the FTA broadcasting signal. This processing procedure can be utilized when transmitting content, which should be seen by anyone without limitation to devices or domains, such as urgent messages and public notices.

[74] Meanwhile, the information, which is included in the service related information and indicates whether or not to perform scrambling, may refer to information indicating whether or not to apply scrambling for the purpose of content protection when creating CMP content. For example, the information indicating whether or not to perform scrambling may be information of 1 bit, which is set to a specific value, for example, T or '0'. Here, when the information indicating whether or not to perform scrambling is set to T , it may indicate that scrambling of content should not be performed, and when the information indicating whether or not to perform scrambling is set to '0', it may indicate that scrambling of content should be performed.

[75] The information indicating whether or not to perform scrambling may be inserted into a specific field (for example, an ancillary control information insert field) of CMPI of a CMP content license, which is associated with a pertinent content.

[76] Further, the remote access control information included in the service related information may refer to control information used to prevent unauthorized redistribution of content. This remote access control information may be information of 2 bits, which can be set to four kinds of values, for example, '0', T , '2' and '3'. For example, '0' may indicate that remote access is permitted through an Internet or another transmission

network, and T to '3' may indicate that strict remote access is required step by step.

[77] This scrambling remote access control information can be inserted into a specific field of CMPI of a CMP content license associated with a pertinent content (for example, a specific field of propagation control information).

[78] Hereinafter, a process of applying revocation when a service provider, for example, a broadcasting station propagates content to a CMP device and the CMP device distributes the content to another CMP device within a domain (referred to as an end point device) is described.

[79] The broadcasting station first creates revocation application information, indicating whether or not to apply revocation on a specific content. Here, the broadcasting station can create revocation application information based on an attribute of the content. For example, it is preferred that information, such as an urgent message, be viewed in all devices without applying a revocation process. Thus, the broadcasting station can create revocation application information, including information to indicate that revocation information should not be applied.

[80] Thereafter, the broadcasting station can transmit the revocation application information to a CMP device through, for example, a FTA signal. The CMP device can receive the revocation application information, and apply or not apply a revocation process for the use of a pertinent content according to an instruction of the revocation application information.

[81] For example, the CMP device can receive the revocation application information and decide a revocation process mode based on the revocation application information. In order to distribute content to other devices of a domain, the CMP device can map the revocation information based on the revocation process mode. Here, when the revocation process mode indicates an application mode, the CMP device can map the revocation information so that the export of content is restricted based on previously set revocation information. When the revocation process mode indicates a non-application mode, the CMP device can map the revocation information so that the export of content is not restricted based on previously set revocation information. Upon mapping, the CMP device can map the revocation information per on a list basis. For example, the CMP device can map the revocation information per on a revocation-list basis based on the revocation process mode. Further, an attribute of the revocation application information can be based on at least one of content and a device and can be one-time and non one-time. When the attribute is non one-time, the CMP device can store the revocation application information.

[82] Meanwhile, an end point device can receive content, which is distributed based on revocation information, from the CMP device and use the content according to previously set authority information. Here, the revocation information can be mapped

based on a revocation process mode and the revocation process mode can be based on revocation application information.

[83] Although the present invention has been described in connection with the embodiment of the present invention illustrated in the accompanying drawings, it is not limited thereto. It will be apparent to those skilled in the art that various substitutions, modifications and changes may be made thereto without departing from the scope and spirit of the invention.

Claims

[1] A method of protecting content, comprising the steps of:
receiving revocation application information from an external system;
deciding a revocation process mode based on the revocation application information; and
mapping revocation information based on the revocation process mode in order to distribute the content to devices on a domain corresponding to an internal system.

[2] The method of claim 1, wherein an attribute of the revocation application information is based on at least one of content and a device.

[3] The method of claim 1, wherein an attribute of the revocation application information is any one of one-time and non one-time, and when the attribute is non one-time, the revocation application information is stored.

[4] The method of claim 1, wherein when the revocation process mode indicates an application mode, the step of mapping the revocation information includes the step of mapping the revocation information so that export of the content is restricted based on previously set revocation information.

[5] The method of claim 1, wherein when the revocation process mode indicates a non-application mode, the step of mapping the revocation information includes the step of mapping the revocation information so that export of the content is not restricted based on previously set revocation information.

[6] The method of claim 1, wherein the revocation information includes information of a revocation list index list.

[7] A method of protecting content, comprising the steps of:
creating revocation application information based on a content attribute; and
transmitting the revocation application information so that distribution of the content is controlled based on the revocation application information,
wherein a revocation process mode is decided based on the revocation application information, and the revocation information is mapped based on the revocation process mode.

[8] The method of claim 7, wherein an attribute of the revocation application information is based on at least one of content and a device.

[9] The method of claim 7, wherein an attribute of the revocation application information is any one of one-time and non one-time, and when the attribute is non one-time, the revocation application information is stored.

[10] The method of claim 7, wherein when the revocation process mode indicates an application mode, the revocation information is mapped so that export of the

content is restricted based on previously set revocation information.

[11] The method of claim 7, wherein when the revocation process mode indicates a non-application mode, the revocation information is mapped so that export of the content is not restricted based on previously set revocation information.

[12] The method of claim 7, wherein the revocation information includes information of a revocation list index list.

[13] A method of protecting content, comprising the steps of:
receiving content distributed based on revocation information; and
using the content according to previously set authority information,
wherein the revocation information is mapped based on a revocation process mode and the revocation process mode is based on revocation application information.

[14] The method of claim 13, wherein an attribute of the revocation application information is based on at least one of content and a device.

[15] The method of claim 13, wherein an attribute of the revocation application information is any one of one-time and non one-time, and when the attribute is non one-time, the revocation application information is stored.

[16] The method of claim 13, wherein when the revocation process mode indicates an application mode, the revocation information is mapped so that export of the content is restricted based on previously set revocation information.

[17] The method of claim 13, wherein when the revocation process mode indicates a non-application mode, the revocation information is mapped so that export of the content is not restricted based on previously set revocation information.

[18] The method of claim 13, wherein the revocation information includes information of a revocation list index list.

[19] A method of processing information employing a content management and protection system, the method comprising the steps of:
receiving service related information, including revocation application information of content, from the outside; and
applying or not applying a content revocation process on the content according to the revocation application information.

[20] The method of claim 19, wherein the revocation application information is set to any one of a first value, indicating that the content revocation process should not be applied, and a second value, indicating that the content revocation process should be applied.

[21] The method of claim 20, wherein when the revocation application information is set to the first value, the step of applying or not applying the content revocation process includes the step of setting specific information, which is included in a

content license associated with the content, to a specific value on which the content revocation process is not applied.

[22] The method of claim 21, wherein the specific information includes a revocation list index list associated with the content.

AMENDED CLAIMS
received by the International Bureau on 26 June 2008 (26.06.2008)
+ STATEMENT

1. (Amended) A computer-implemented method comprising:

receiving data indicating whether to apply revocation of content;

mapping the received data to revocation information; and

determining whether to apply a content revocation process to the content based on the revocation information.

2. (Amended) The method of claim 1, wherein the receiving the data indicating whether to apply revocation of content further comprises:

receiving the data over free to air broadcast signals.

3. (Amended) The method of claim 1, wherein the received data comprises first or second values, indicating that the content revocation process should not or should be applied, respectively.

4. (Amended) The method of claim 3. wherein, if the received data comprises the first value, mapping the received data to revocation information further comprises:

setting a specific parameter in the revocation information to a specific value indicating that the content revocation process is not be applied.

5. (Amended) The method of claim 1, wherein a license of the content includes the revocation information.

6. (Deleted)

7. (Deleted)

8. (Deleted)

9. (Deleted)

10. (Deleted)

11. (Deleted)

12. (Deleted)

13. (Deleted)

14. (Deleted)

15. (Deleted)

16. (Deleted)

17. (Deleted)

IS. (Deleted)

19. (Deleted)

20. (Deleted)

21. (Deleted)

22. (Deleted)

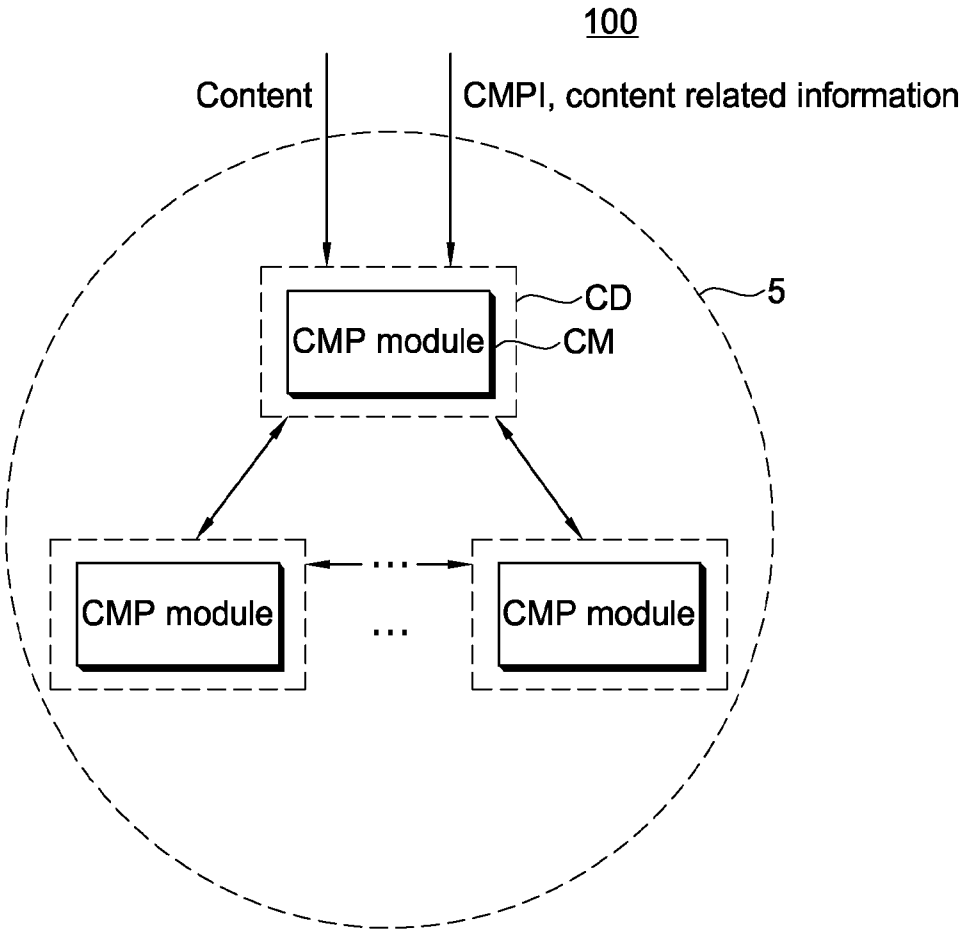
The end.

STATEMENT UNDER ARTICLE 19(1)

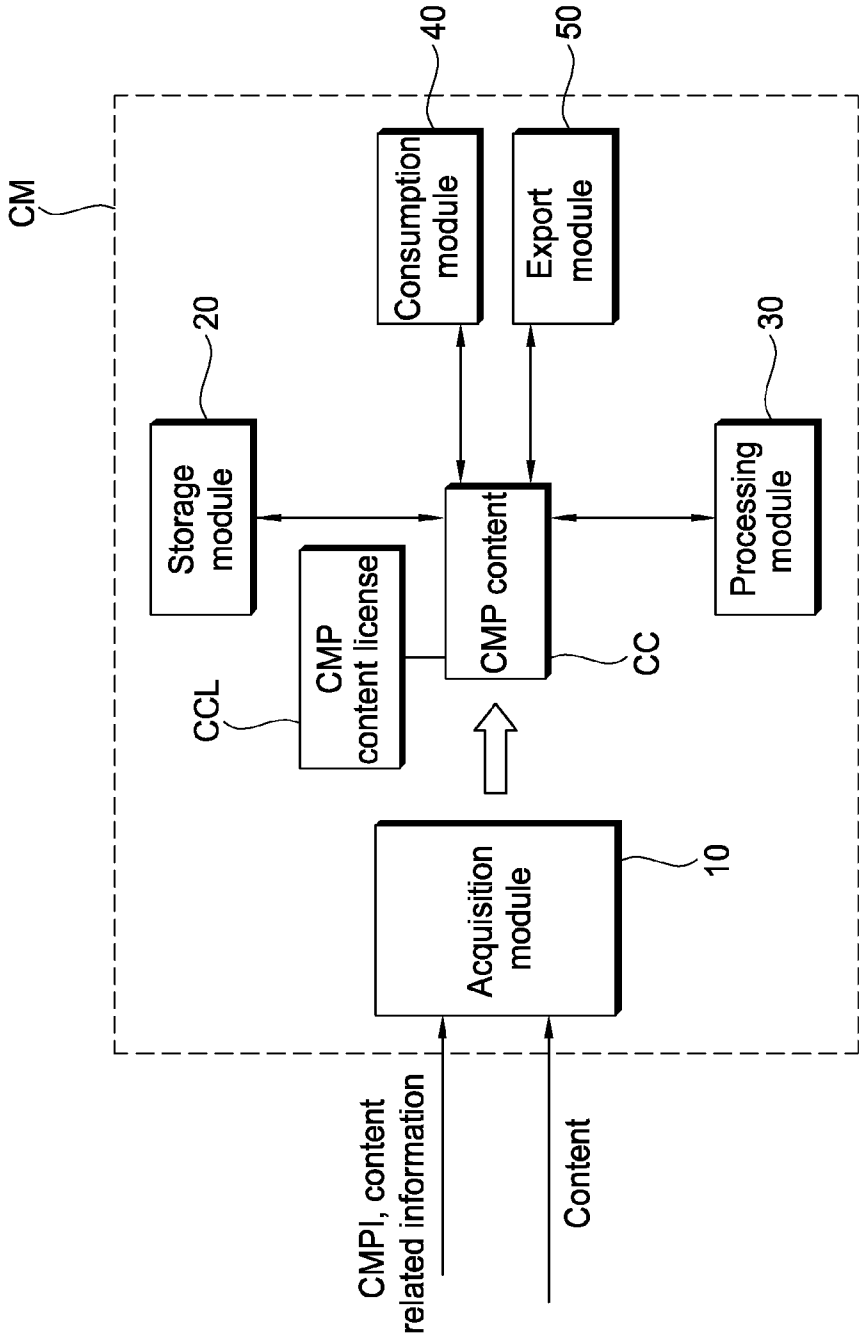
Please replace original claims 1-22 by amended claims 1-5 and deleted claims 6-22 of the Replacement sheet attached hereto.

In the Replacement sheet, claims 1 through 5 are amended to change "XHTML" into "XHTML-Print", claims 6 through 22 are deleted.

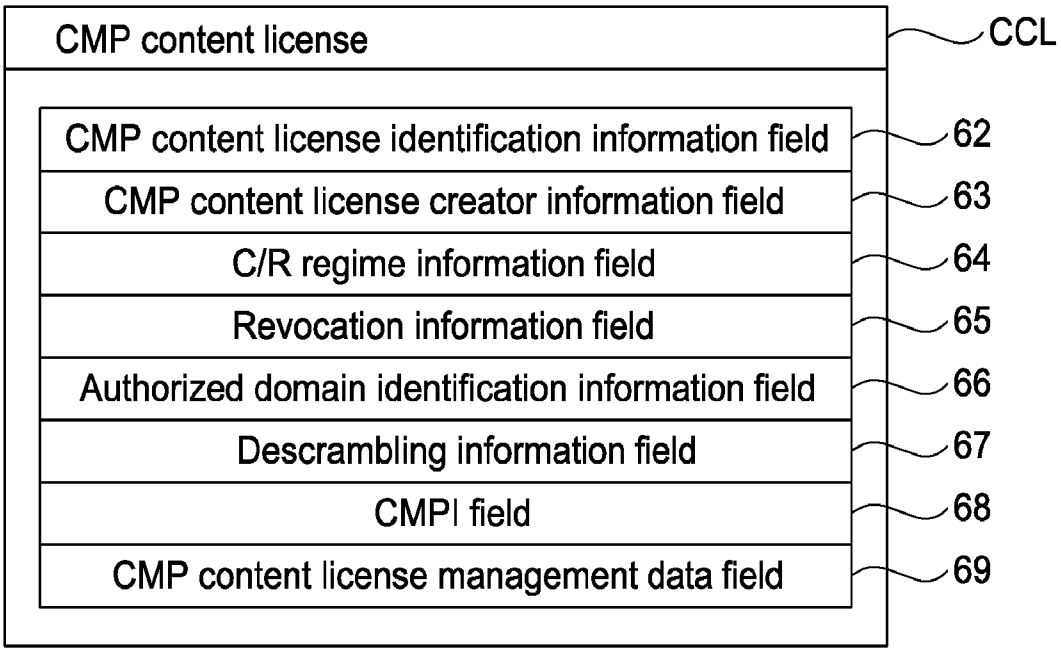
[Fig. 1]


100
Content
CMPI, content related information
CD
5
CMP module
CM
CMP module
CMP module

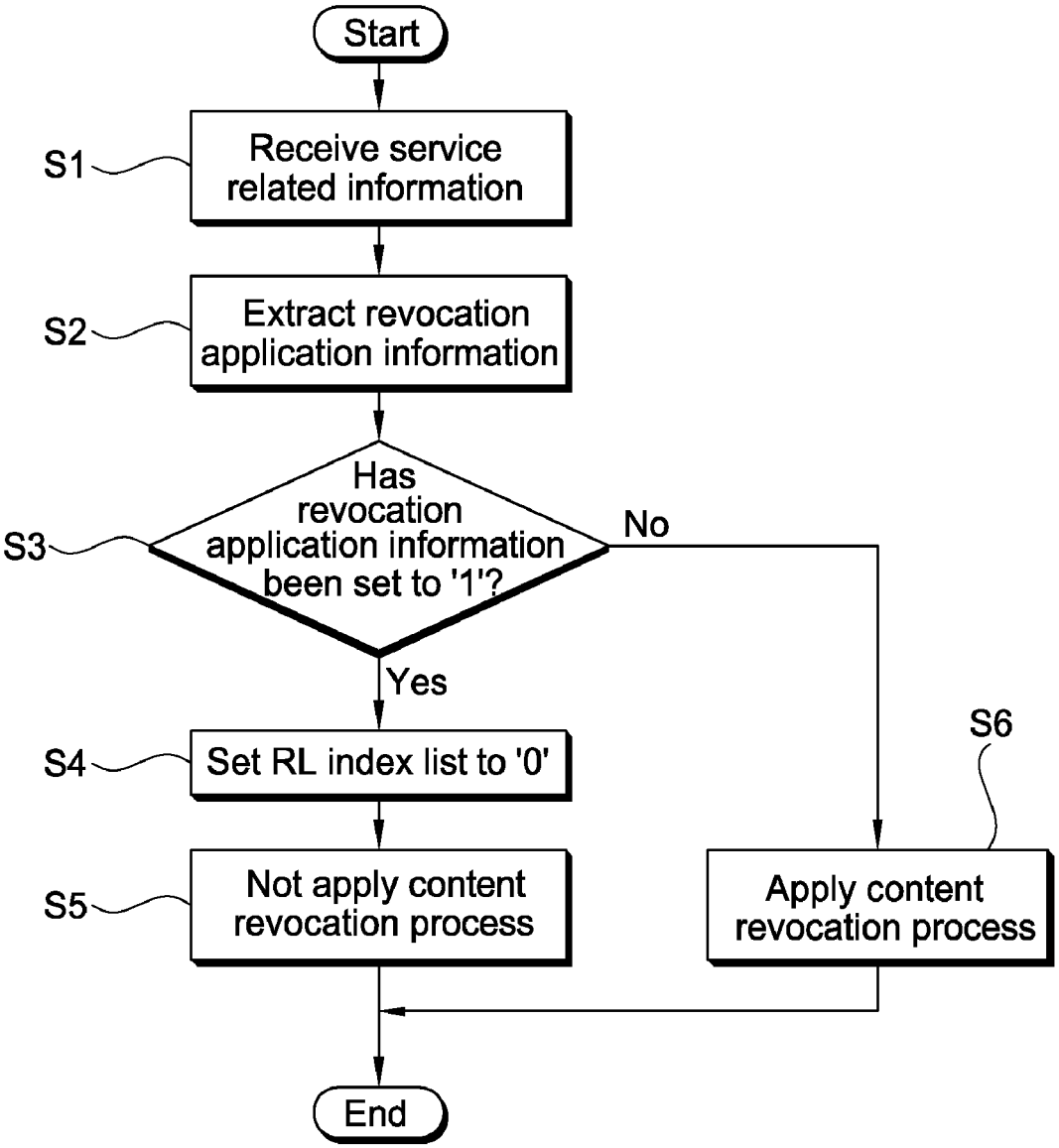
[Fig. 2]


CM
40
50
Consumption module
Export module
20
30
Storage module
CMP content
Processing module
CMP content license
CCL
CC
Acquisition module
10
CMPI, content related information
Content

[Fig. 3]


CMP content license
CCL
CMP content license identification information field
62
CMP content license creator information field
63
C/R regime information field
64
Revocation information field
65
Authorized domain identification information field
66
Descrambling information field
67
CMPI field
68
CMP content license management data field
69

[Fig. 4]


Start
S1
Receive service related information
S2
Extract revocation application information
S3
Has revocation application information been set to '1'?
No
Yes
S4
Set RL index list to '0'
S5
Not apply content revocation process
S6
Apply content revocation process
End

INTERNATIONAL SEARCH REPORT

International application No
PCT/KR2008/000378

A. CLASSIFICATION OF SUBJECT MATTER

G06F 17/00(2006.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 8 G06F 17/00

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

Korean Utility models and applications for Utility models since 1975
Japanese Utility models and applications for Utility models since 1975

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

eKIPASS(KIPO internal) & keyword unrevoke, revocation, mode, content

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No
A	SANDRA MURPHY et al , 'Code revocation for active networks', Open Architectures and Network Programming, 2003 IEEE Conference, pages 12 - 22, 4 April 2003 See pages 15-19, Figures 1-3	1 - 22
A	WO 2004/086235 A1 (MATSUSHITA ELECTRONIC INDUSTRIAL CO , LTD) 7 October 2004 See the abstract, Claims 1-2, Figures 9, 13	1 - 22
A	WO 02/33880 A1 (SONY CORPORATION) 25 April 2002 See the abstract, Claims 1, 10, Figures 41-1, 41-2	1 - 22

☐ Further documents are listed in the continuation of Box C

☒ See patent family annex

* Special categories of cited documents
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance, the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance, the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 APRIL 2008 (30 04 2008)	30 APRIL 2008 (30.04.2008)

Name and mailing address of the ISA/KR

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

Facsimile No 82-42-472-7140

Authorized officer

SHIN, Jun Ho

Telephone No 82-42-481-5643

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/KR2008/000378

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
W02004086235A1	07.10.2004	CN1764907A	26.04.2006
		EP1617332A1	18.01.2006
		JPW02004/086235	07.10.2004
		KR1020060006897	20.01.2006
		US20060171391A1	03.08.2006
W00233880A1	25.04.2002	CN1397123	12.02.2003
		EP1235380A1	28.08.2002
		JP2002135243A2	10.05.2002
		KR1020020064945	10.08.2002
		TW550923B	01.09.2003
		TW550923A	01.09.2003
		US20020184259A1	05.12.2002
		W0200233880C2	04.03.2004