IPRally

Search case export

US7715564B2

Exported on 2022-09-02

Summary

#	Publication number	Title	Applicants	Score
1	US20020184515A1	Rights management unit	Individual	58
2	JP2002288448A	LICENSE RECORDER	Sanyo Electric Co Ltd	57
3	US7725399B2	Content usage device and network system, and license information acquisition method	Panasonic Corp	57
4	US7395245B2	Content usage management system and server used in the system	Matsushita Electric Industrial Co Ltd	56
5	US20020136405A1	Data recording device allowing obtaining of license administration information from license region	Sanyo Electric Co Ltd	55
6	JP2002344921A	CONTENTS RECEIVER	Fujitsu Ltd	55
7	JP4593764B2	Data terminal equipment	Fujitsu Ltd, PFU Ltd, Sanyo Electric Co Ltd, Renesas Electronics Corp	55
8	JP4151274B2	Information processing apparatus and method, license server, and program	Sony Corp	55
9	US7149722B1	Retail transactions involving distributed and super-distributed digital content in a digital rights management (DRM) system	Microsoft Corp	55
10	US20020107806A1	Content usage management system and content usage management method	Individual	55
11	JP2002297816A	INFORMATION PROCESSING DEVICE AND METHOD, RECORDING MEDIUM, AND PROGRAM	Sony Corp	54
12	US7203966B2	Enforcement architecture and method for digital rights management system for roaming a license to a plurality of user devices	Microsoft Corp	54
13	JP4737857B2	Data terminal equipment	Sanyo Electric Co Ltd	54
14	JP3895940B2	Information terminal equipment	Sanyo Electric Co Ltd	54
15	US7925591B2	Retail transactions involving digital content in a digital rights management (DRM) system	Microsoft Corp	54
16	US6873975B1	Content usage control system, content usage apparatus, computer readable recording medium with program recorded for computer to execute usage method	Fujitsu Ltd	54
17	US7073063B2	Binding a digital license to a portable device or the like in a digital rights management (DRM) system and checking out/checking in the digital license to/from the portable device or the like	Microsoft Corp	54
18	US20030028490A1	System, apparatus, and method of contents distribution, and program and program recording medium directed to the same	Individual	54
19	JP3502035B2	Content user system, recording medium, and content usage control method	Fujitsu Ltd	54
20	US7010808B1	Binding digital content to a portable storage device or the like in a digital rights management (DRM) system	Microsoft Corp	54
21	US7136838B1	Digital license and method for obtaining/providing a digital license	Microsoft Corp	54
22	JP2003058660A	CONTENTS USE MANAGEMENT SYSTEM AND SERVER USED FOR THE SAME	Matsushita Electric Industrial Co Ltd	54
23	JP4409081B2	Data terminal equipment	Renesas Technology Corp, Fujitsu Ltd, PFU Ltd, Sanyo Electric Co Ltd	54
24	US20050120232A1	Data terminal managing ciphered content data and license acquired by software	Fujitsu Ltd, Hitachi Ltd, Sanyo Electric Co Ltd	53
25	US7024393B1	Structural of digital rights management (DRM) system	Microsoft Corp	53
26	US20050076208A1	Data terminal capable of transferring ciphered content data and license acquired by software	Fujitsu Ltd, Sanyo Electric Co Ltd	53
27	US6775655B1	Rendering digital content in an encrypted rights-protected form	Microsoft Corp	53
28	US7260721B2	Information processing method, information processing apparatus and recording medium	Sony Corp	53
29	WO2000059151A2	RENDERING DIGITAL CONTENT IN AN ENCRYPTED RIGHTS-PROTECTED FORM	MICROSOFT CORP	53
30	US7162745B2	Protecting decrypted compressed content and decrypted decompressed content at a digital rights management client	Microsoft Corp	53
31	US7383205B1	Structure of a digital content package	Microsoft Corp	53
32	US7359883B2	License management system, license management device, relay device and terminal device	Matsushita Electric Industrial Co Ltd	53
33	JP4553472B2	Data terminal equipment	Sanyo Electric Co Ltd	53
34	US7680744B2	Method for interdependently validating a digital content package and a corresponding digital license	Microsoft Corp	53
35	US9246916B2	Specifying rights in a digital rights license according to events	Microsoft Technology Licensing LLC	53
36	JP4170670B2	Usage rights management device	Panasonic Corp, Matsushita Electric Industrial Co Ltd	53

37	JP2002297034A	INFORMATION PROCESSOR, INFORMATION PROCESSING METHOD, RECORDING MEDIUM, PROGRAM, AND FORMAT FOR RECORDING MEDIUM	Sony Corp	53
38	US6772340B1	Digital rights management system operating on computing device and having black box tied to computing device	Microsoft Corp	52
39	US7065507B2	Supervised license acquisition in a digital rights management system on a computing device	Microsoft Corp	52
40	JP4157535B2	Content usage management system, server device and terminal device used therefor, content usage management method, license information transmission method, and content usage control method	Panasonic Corp, Matsushita Electric Industrial Co Ltd	52
41	US7010809B2	Reproduction device stopping reproduction of encrypted content data having encrypted region shorter than predetermined length	Sanyo Electric Co Ltd	52
42	US7134144B2	Detecting and responding to a clock rollback in a digital rights management system on a computing device	Microsoft Corp	52
43	US7099846B1	Apparatus and system for providing fee-based content	Sony Corp	52
44	US20020138442A1	Content provision device and method and license server capable of facilitating circulation of encrypted content data	Sanyo Electric Co Ltd	52
45	US6772133B1	Information recording device and information reproducting device	Toshiba Corp	52
46	US7239708B2	Protecting decrypted compressed content and decrypted decompressed content at a digital rights management client	Microsoft Corp	52
47	JP2002297032A	DEVICE AND METHOD FOR PROCESSING INFORMATION, RECORDING MEDIUM AND PROGRAM	Sony Corp	52
48	US20050097368A1	Specifying security for an element by assigning a scaled value representative of the relative security thereof	Microsoft Corp	52
49	JP3606148B2	Digital content usage control method and system	NEC Corp	52
50	US6829708B1	Specifying security for an element by assigning a scaled value representative of the relative security thereof	Microsoft Corp	51
51	JP4554801B2	Data terminal equipment	Fujitsu Ltd, PFU Ltd, Sanyo Electric Co Ltd, Renesas Electronics Corp	51
52	US7412061B2	Encrypting a digital object on a key ID selected therefor	Microsoft Corp	51
53	US8744969B2	Releasing decrypted digital content to an authenticated path	Microsoft Corp	51
54	US20020012432A1	Secure video card in computing device having digital rights management (DRM) system	Microsoft Corp	51
55	JP2006320018A	INFORMATION PROCESSING APPARATUS, INFORMATION PROCESSING METHOD, RECORDING MEDIUM, AND PROGRAM	Sony Corp	51
56	US7336791B2	Information processing apparatus	Sony Corp	51
57	US7216368B2	Information processing apparatus for watermarking digital content	Sony Corp	51
58	JP2002099743A	DATA REPRODUCING DEVICE AND LICENSE MANAGING METHOD	Sanyo Electric Co Ltd	51
59	JP4601153B2	Data terminal device and control method of data terminal device	Fujitsu Ltd, PFU Ltd, Sanyo Electric Co Ltd, Renesas Electronics Corp	51
60	US7028340B1	Apparatus, a system and method for controlling access to contents	Fujitsu Ltd	51
61	US6389538B1	System for tracking end-user electronic content usage	International Business Machines Corp	51
62	US8055899B2	Systems and methods using digital watermarking and identifier extraction to provide promotional opportunities	Digimarc Corp	51
63	US20020026424A1	License issuing device/method and contents reproducing device/method	Matsushita Electric Industrial Co Ltd	50
64	US7319759B1	Producing a new black box for a digital rights management (DRM) system	Microsoft Corp	50
65	JP2002373216A	LICENSE PURCHASE AND SALE MEDIATION METHOD AND LICENSE MANAGEMENT DEVICE	Hitachi Ltd	50
66	JP4540202B2	Data reproduction apparatus and data terminal apparatus	Sanyo Electric Co Ltd	50
67	JP2002203071A	LICENSE SALES SYSTEM, CONTENT DISTRIBUTING SYSTEM, LICENSE SALES METHOD, AND MEMORY MEDIA	Canon Inc	50
68	US20030182236A1	Information processor	Sony Corp	50
69	JP2002094500A	DATA TERMINAL DEVICE	Sanyo Electric Co Ltd	50
70	US20030028622A1	License management server, terminal device, license management system and usage restriction control method	Individual	50
71	JP2002342518A	SYSTEM AND METHOD FOR CONTENTS USE MANAGEMENT	Matsushita Electric Industrial Co Ltd	50
72	EP1277305B1	SECURE DIGITAL CONTENT LICENSING SYSTEM AND METHOD	Blockbuster LLC	50
73	RU2287851C2	DISTRIBUTION DEVICE, TERMINAL DEVICE, PROGRAM AND METHOD USED IN THESE DEVICES	MATSUSHITA ELECTRIC IND CO LTD	49
74	US7353541B1	Systems and methods for content distribution using one or more distribution keys	Sony Corp	49
75	US7343495B2	Information recording apparatus, information reproducing apparatus, and information distribution system	Toshiba Corp	49

76	JP4766762B2	Data playback device	Sanyo Electric Co Ltd	49
77	JP2003178163A	LICENSE MANAGING SERVER, TERMINAL DEVICE, LICENSE MANAGING SYSTEM AND UTILIZATION LIMIT CONTROL METHOD	Matsushita Electric Industrial Co Ltd	49
78	US7103663B2	License management server, license management system and usage restriction method	Matsushita Electric Industrial Co Ltd	49
79	US6983371B1	Super-distribution of protected digital content	International Business Machines Corp	49
80	JP2002117167A	METHOD AND DEVICE FOR MANAGING COPYRIGHT	Nippon Telegraph and Telephone Corp	49
81	US7945517B2	Data distribution system and recording device for use therein	Fujitsu Ltd, Sanyo Electric Co Ltd, Renesas Electronics Corp	49
82	AU2003227202B2	System for Tracking End-user Electronic Content Usage	Wistron Corp	49
83	US7426639B2	Information processing apparatus and method for managing grouped devices in an encrypted environment	Sony Corp	49
84	US6959288B1	Digital content preparation system	International Business Machines Corp	49
85	US7155415B2	Secure digital content licensing system and method	Movielink LLC	49
86	JP4177040B2	Content utilization apparatus, network system, and license information acquisition method	Panasonic Corp, Matsushita Electric Industrial Co Ltd	49
87	JP3831596B2	Data terminal equipment	Sanyo Electric Co Ltd	49
88	JP4294266B2	License management server, license management system, and usage restriction control method	Panasonic Corp, Matsushita Electric Industrial Co Ltd	49
89	US7487128B2	Updating usage conditions in lieu of download digital rights management protected content	International Business Machines Corp	48
90	WO2001052471A1	PRODUCING A NEW BLACK BOX FOR A DIGITAL RIGHTS MANAGEMENT (DRM) SYSTEM	MICROSOFT CORP	48
91	US20020107803A1	Method and system of preventing unauthorized rerecording of multimedia content	International Business Machines Corp	48
92	US6389403B1	Method and apparatus for uniquely identifying a customer purchase in an electronic distribution system	International Business Machines Corp	48
93	US20020077988A1	Distributing digital content	Hewlett Packard Development Co LP	48
94	EP1045387B1	Data management apparatus, data management method, and record medium recording data management program	Matsushita Electric Industrial Co Ltd	48
95	JP3793220B2	Recording method and recording apparatus	Toshiba Corp	48
96	JP2003016288A	DATA TERMINAL EQUIPMENT AND DATA RE-ACQUIRING METHOD	Sanyo Electric Co Ltd	48
97	US7051005B1	Method for obtaining a black box for performing decryption and encryption functions in a digital rights management (DRM) system	Microsoft Corp	48
98	US20030159033A1	Information processing apparatus	Sony Corp	48
99	US6611812B2	Secure electronic content distribution on CDS and DVDs	International Business Machines Corp	48
100	US7124443B2	Information transaction system	Sony Corp	48

1. Rights management unit

US20020184515A1 | Individual

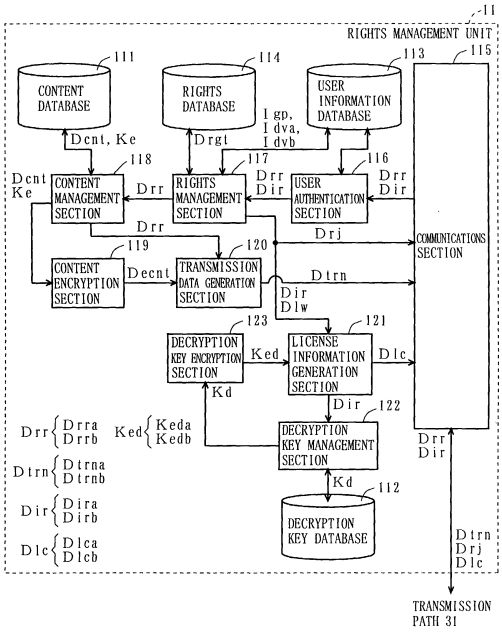
Bibliographic data

Publication date: 2002-12-05
Application date: 2002-05-29
Earliest priority date: 2001-05-29

Inventors: OHO MASAHIRO, OKAMOTO RYUICHI, YAMAMOTO MASAYA, UESAKA YASUSHI, TOKUDA KATSUMI, INOUE MITSUHIRO

CPC classification: G06F 17/00, G06F 21/105, G06Q 10/10
IPC classification: G06Q 10/00, G06F 21/10

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

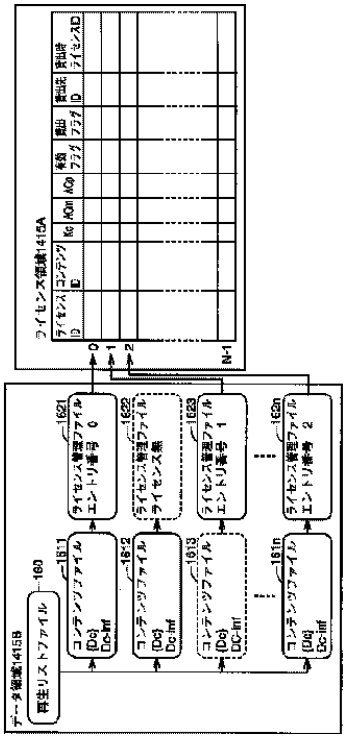
A device 201 of a licensee γ generates an issue request for a permission to use content data by using a media identifier in a portable recording medium 101 of a licensee β, and forwards the resulting issue request to a rights management unit 71. The rights management unit 71 is managing rights information of the content data provided to the licensee β, and based on the rights information together with the issue request, generates permission information to allow the portable recording medium 101 to use the content data. Based on the permission information, the rights management unit 71 then generates license information with which the use of the content data in the device connected to the portable recording medium 101 is controlled, and transmits the license information to the device 201. The device 201 then processes the license information to control the use of the content data. In such a manner, provided is a license information management system with which the licensee β can use the content data with his or her own rights information on the device belonging to the licensee γ.

First claim

A unit for managing rights information representing a right for a plurality of devices to use content data, the unit comprising:
a rights database (hereinafter, rights DB) including the rights information each assigned to the plurality of devices;
a rights management section operable to generate, in response to an issue request from any one of the plurality of devices, permission information which represents a permission for the device to use the content data, by using the rights information corresponding to the device in the rights DB;
a license information generation section operable to generate license information which at least includes the permission information generated by the rights management section; and
a communications section operable to transmit the license information generated by the license information generation section to the device from which the issue request is forwarded.

2. LICENSE RECORDER

JP2002288448A | Sanyo Electric Co Ltd



Bibliographic data

Publication date: 2002-10-04
Application date: 2001-03-26
Earliest priority date: 2001-03-26

Inventors: HORI YOSHIHIRO, YOSHIKAWA TAKATOSHI

CPC classification:
IPC classification: G06Q 10/00, G06K 19/07, G06Q 50/00, G06K 17/00, G06F 21/10, G06Q 30/06, G06Q 50/10

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

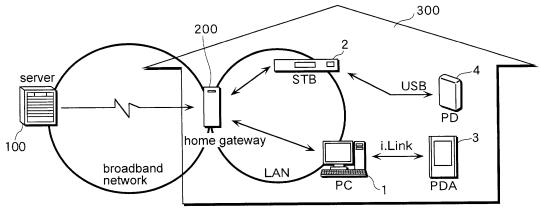
(57) [Summary] [PROBLEMS] To provide a license recording device capable of providing a backup of a rented license. SOLUTION: The memory card has a license area 141. 5A. The license area 1415A stores licenses (license ID, content ID, license key K c, access control information ACm, and reproduction count control information ACp), a valid flag, a lending flag, a lending destination ID, and a lending license ID. When the license is lent, “lending” is set in the lending flag, a public encryption key unique to the memory card of the lending destination is stored in the lending destination ID, and the lending license ID is stored in the lending license ID. Is stored.

First claim

A license recording apparatus for generating a renting license from a license for decrypting encrypted content data and renting the renting license to another license recording apparatus, wherein the license and the license A license holding unit for holding a lending flag indicating whether or not lending is possible, lending destination identification information for specifying the lending destination of the lending license, and lending license identification information for identifying the lending license; The control unit, in response to the license lending request, for specifying license designation information for designating a license to be lent to the other license recording device and the renting license. License specification information for borrowing from the outside, and receives the license specified by the license specification information. Reading the sense from the license holding unit, generating the rental license included in the read license, and replacing the license specification information with the license specification information for specifying the read license, Set the lending flag during lending,
License recording device.

3. Content usage device and network system, and license information acquisition method

US7725399B2 | Panasonic Corp



Bibliographic data

Publication date: 2010-05-25
Application date: 2002-07-15
Earliest priority date: 2001-07-17

Inventors: NAKAHARA TOHRU, NAKANISHI MASANORI, UESAKA YASUSHI, MIURA KOUJI, HIGASHI AKIO, NAMBA TAKAAKI

CPC classification: G06F 17/00, G06F 21/10, G06F 2221/0797, G06Q 20/102, G06Q 20/382, H04N 2005/91364, H04N 21/2541, H04N 21/43615, H04N 21/4627, H04N 21/8355, H04N 7/162
IPC classification: H04N 7/16, H04N 5/913, G06F 21/10

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

A content usage device includes (i) a license management unit that holds license information and (ii) a content output unit that uses a content in compliance with license information and outputs the content in at least one manner of a sound, video and data. The license management unit, upon receiving a request of license information from the content output unit, requests a license management unit of another content usage device to transfer the license information and acquires the license information, and passes the acquired license information to the content output unit. The content output unit uses a content in compliance with the license information passed from the license management unit.

First claim

A content usage device connected to (i) a server that is located outside a defined network in which a gateway apparatus is located and (ii) a plurality of other content usage devices within the defined network, each of the other content usage devices being for using content, and each of the other content usage devices and the content usage device being connected, from within the defined network, to the gateway apparatus that provides a connection to the server located outside the defined network, the server storing license information of a content, the content usage device comprising:

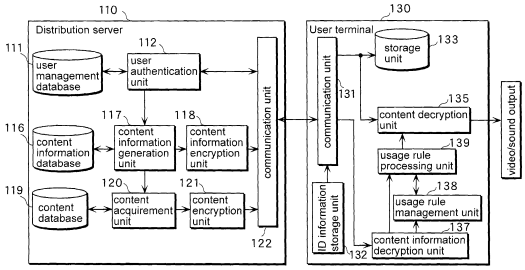
a license management device configured to manage the license information of the content, the license information of the content enabling usage of the content; and

an output device configured to output the content in compliance with the license information of the content, wherein the license management device of the content usage device receives a request for the license information of the content from the output device,

wherein , upon receipt of the request for the license information from the output device and when the license management device of the content usage device does not contain the license information requested by the output device, the license management device of the content usage device (i) searches, from within the defined network, for and identifies a first content device of the plurality of other content usage devices that includes a license management device containing the license information of the content requested by the output device, (ii) requests, from within the defined network, the license management device of the identified first content usage device to transfer the license information of the content to the content usage device, (iii) receives, from the identified first content usage device having the license information of the content and being within the defined network, the license information of the content without receiving the license information of the content from the server, the license information of the content being received by the identified first content usage device from the server via the gateway apparatus, and (iv) passes the received license information of the content to the output device, and wherein the output device outputs the content in compliance with the license information passed from the license management device of the content usage device.

4. Content usage management system and server used in the system

US7395245B2 | Matsushita Electric Industrial Co Ltd



Bibliographic data

Publication date: 2008-07-01
Application date: 2002-06-05
Earliest priority date: 2001-06-07

Inventors: OKAMOTO RYUICHI, TOKUDA KATSUMI, MIURA KOUJI

CPC classification: G06F 17/00, G06F 21/10
IPC classification: G06F 1/00, G06Q 50/00, H04L 9/32, G06Q 30/06, G06Q 50/10, G06F 21/62

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

A content usage management system includes a terminal device using content as digital production and a server device managing usage of the content on the terminal device. The server device includes a license information memory unit that memorizes license information indicating a usage rule of the content based on a user of the terminal device, and a license ticket issuance unit that generates a license ticket as right information indicating a part or all of a usage rule on the license information corresponding to the user based on a request from the user. The terminal device includes a requesting unit that requests usage of the content to the server device according to the user's designation, a receiving unit that receives the license ticket sent from the server device, and a content usage control unit that controls usage of the content according to the usage rule indicated on the received license ticket. The requesting unit makes a request by sending expected information indicating content to be requested and a usage volume of the content, and the license ticket issuance unit generates a license ticket according to the expected information sent from the requesting unit and sends the license ticket to the terminal device.

First claim

A content usage management system comprising:
a first terminal device for sending a license request comprising terminal capability information indicating a capability of said first terminal device with regard to content usage control, said first terminal device including a secure clock, and the terminal capability information including information indicating that said first terminal device includes a secure clock;
a second terminal device for sending a license request comprising terminal capability information indicating a capability of said second terminal device with regard to content usage control, said second terminal device not including a secure clock, and the terminal capability information including information indicating that said second terminal device does not include a secure clock; and
a server device for managing a usage rule of a user, receiving the terminal capability information from the first and second terminal devices, generating a first license ticket including part or all of the usage rule for processing content based on the terminal capability information sent from said first terminal device, sending the first license ticket to said first terminal device, generating a second license ticket including: part or all of the usage rule for processing content; a content identification; and a license ticket status flag set to indicate that the license information must be consumed upon receipt without being written on a recording medium based on the terminal capability information sent from said second terminal device, which indicates that the second terminal device does not include a secure clock, and sending the second license ticket to said second terminal device;
wherein said first terminal device controls content usage in accordance with the usage rule included in the first license ticket; and
said second terminal device determines the status of the license ticket status flag in the second license ticket and controls content usage, in accordance with the usage rule included in the second license ticket, thereby immediately executing the content identified by the content identification in response to the license ticket status flag being set to indicate that the license ticket must be consumed upon receipt without being written on a recording medium.

5. Data recording device allowing obtaining of license administration information from license region

US20020136405A1 | Sanyo Electric Co Ltd

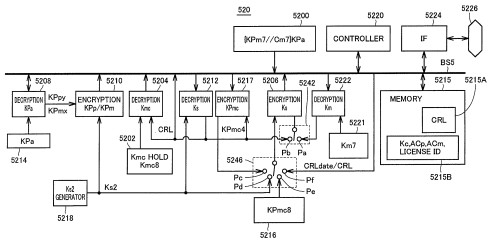
Bibliographic data

Publication date: 2002-09-26
Application date: 2001-09-07
Earliest priority date: 2001-03-23

Inventors: HORI YOSHIHIRO

CPC classification: G06F 21/10, G06Q 20/1235, G06Q 20/16, G07F 17/0014
IPC classification: H04L 9/08, G06F 12/14, G06K 19/073, G07F 7/00, G09C 1/00, H04L 9/10, G07F 17/16, G06F 21/10, G06F 21/60, G06F 21/62

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

A memory includes a license region and a data region. Licenses (license ID, license key Kc, access control information ACm and reproduction time control information ACp) are stored in the license region. The license ID includes a content ID. A license administration file including information other than the license key and others are stored in the data region. When the content ID is externally input, the license including the content ID thus input is read out from the license region, and is externally output via an interface and a terminal. As a result, the license administration information, which can be output from a memory card for display, in the license can be obtained from the license region.

First claim

A data recording device for recording a license including a license key for decrypting encrypted data and data specifying information for specifying said encrypted data at least, comprising:
a license storing unit subjected to tamper resistant processing disabling direct external access and storing the license;
an interface for external transmission; and
a control unit, wherein said control unit obtains said data specifying information and a request for retrieving the license input via said interface, retrieves the license stored in said license storing unit based on said data specifying information, reads out the license including said data specifying information from said license storing unit, selects unconfidential information with the exception of said license key out of the read license, and externally outputs said selected information via said interface.

6. CONTENTS RECEIVER

JP2002344921A | Fujitsu Ltd

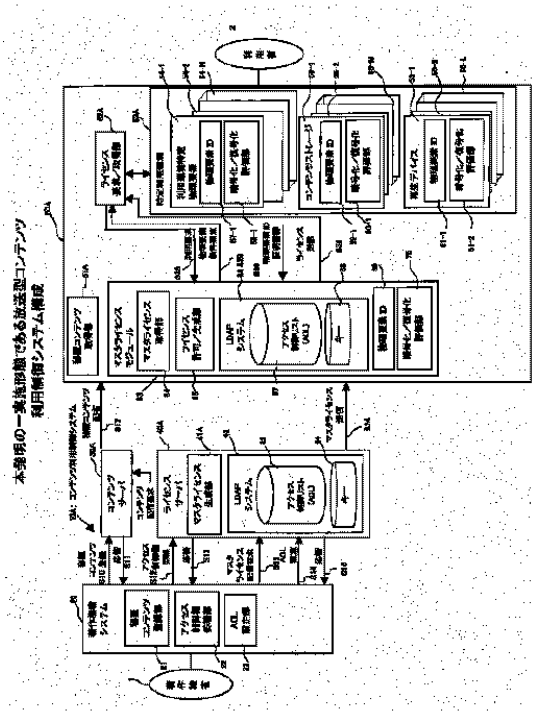
Bibliographic data

Publication date: 2002-11-29
Application date: 2001-05-21
Earliest priority date: 2001-05-21

Inventors: KOMURO TOMOKAZU, SAITO TAKASHI

CPC classification:
IPC classification: G06Q 10/00, G06F 15/00, G06Q 50/00, H04N 7/16, G06F 21/00, G06F 12/14, G06F 21/10, G06Q 30/06, G06Q 30/04, H04N 21/266, G06Q 50/10, H04N 21/6334, G06F 21/62, H04N 21/4623

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

PROBLEM TO BE SOLVED: To provide a contents receiver that allows a user to be able to use contents without the need for accessing a contents provider. SOLUTION: The contents receiver includes a memory means that stores encrypted contents, a storage means that receives and stores a utilization permission condition of the encrypted contents through a one-way network, an acquisition means that acquires the utilization permission condition stored in the storage means, a discrimination means that discriminates whether or not the acquired utilization permission condition is satisfied, and a utilization means including a decoding means that obtains a decoding key of the encrypted contents when the utilization permission condition is satisfied to decode the encrypted contents.

First claim

A storage unit for storing encrypted content, a storage unit for receiving and storing the use permission condition of the encrypted content through a one-way network, and acquiring the use permission condition stored in the storage unit. Acquisition means, determination means for determining whether or not the obtained use permission condition is satisfied, and decryption means for obtaining a decryption key for the encrypted content and decrypting the encrypted content when the use permission condition is satisfied. And a use means.

7. Data terminal equipment

JP4593764B2 | Fujitsu Ltd, PFU Ltd, Sanyo Electric Co Ltd, Renesas Electronics Corp

Bibliographic data

Publication date: 2010-12-08
Application date: 2000-11-28
Earliest priority date: 2000-11-28

Inventors: 堀 吉宏, 上村 透, 宮園 真也, 畠山 卓久, 高橋 政孝, 常広 隆司, 大森 良夫

CPC classification:
IPC classification: G06Q 50/00, H04L 9/08, H04L 9/32, G06F 13/00, G06F 12/14, G11B 20/10, G09C 5/00, G06F 21/10, G06Q 30/06, G06Q 50/10, G06F 21/60, G06F 21/62, G10K 15/02

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

(57) [Summary] [PROBLEMS] To provide a data terminal device capable of ripping content data according to the usage regularity of content data. SOLUTION: A watermark detecting means 5400 is provided. The watermark is detected from the music data, and the watermark determination unit 5401 determines whether the usage rule of the detected watermark has regularity. And The license generation unit 5403 generates a license according to the regularity of the watermark usage rule. The remark unit 5402 replaces the watermark in which the music data copy condition has been changed according to the regularity of the watermark use rule. The music encoder 5404 encodes the music data from the remark unit 5402 in a predetermined format. The encryption means 5405 includes a music encoder 5404 Is encrypted with the license key generated by the license generation unit 5403.

First claim

A data terminal device that obtains plaintext content data and generates encrypted content data obtained by encrypting the content data, and a local license for decrypting and reproducing the encrypted content data,
Encrypted content generation means for generating the local license based on duplication permission information included in the content data, and generating the encrypted content data by encrypting the content data with a license key included in the generated local license When,
An encryption processing means for generating an encrypted local license obtained by applying an original encryption to the generated local license;
Storage means for storing the encrypted local license and encrypted content data;
A control unit,
The control unit gives the acquired content data to the encrypted content generation unit, gives the local license to the encryption processing unit,
The encrypted content generation means includes:
Copy permission / inhibition information detection means for detecting the copy permission / inhibition information from the content data;
Duplication availability information determination means for determining the detected duplication availability information;
A copy condition changing means for changing the copy condition based on the determination result of the copy permission / inhibition information determining means and writing it in the content data;
Encoding means for encoding the content data from the duplication condition changing means into a predetermined method;
License generation means for generating the local license based on the determination result of the duplication permission information determination means;
And encryption means for encrypting the content data encoded in the predetermined scheme with the license key,
The license generating means includes a content identifier for specifying the encrypted content data, a communication identifier for specifying communication when the encrypted content data and the license are lent to another device, the license key, and the encryption key. Generating a local license comprising recording device access conditions for a data recording device that records encrypted content data and the local license, and playback device access

conditions for a data playback device that decrypts and plays back the encrypted content data using the license A data terminal device.

8. Information processing apparatus and method, license server, and program

JP4151274B2 | Sony Corp

Bibliographic data

Publication date: 2008-09-17
Application date: 2002-02-06
Earliest priority date: 2001-02-09

Inventors: 田中 浩一, 河上 達, 黒田 壽祐, 石黒 隆二

CPC classification:
IPC classification: H04L 9/08, H04L 9/00, H04L 9/32, G09C 5/00

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

(57) [Summary] [Problem] Content can be freely distributed, Make content available only to authorized users. A client receives encrypted content from a content server. In the header of the content, license specifying information for specifying a license required when using the content is described, and the client requests a license from the license server based on the license specifying information. Upon receiving the license request, the license server performs a billing process and transmits the corresponding license to the client. The client decrypts and reproduces the content on condition that the client holds the license.

First claim

In an information processing apparatus that permits the use of content on condition that a license is held,
Content storage means for storing the content including license specifying information for specifying the license to permit use of the content, encrypted content data, and key information necessary for decrypting the content data;
License storage means for storing a license including content specifying information for specifying the content permitted to be used;
Determining means for determining whether or not a license capable of permitting use of the content is stored in the license storage means;
Decrypting means for decrypting the content data of the content on condition that the determination means determines that a license is stored;
The encrypted content data is composed of an arbitrary number of encrypted blocks, and each encrypted block is encrypted with an initial vector, a seed, and a block key that are different for each encrypted block. Composed of
The block key is generated by calculating a content key included in the key information and the seed using a hash function,
An information processing apparatus characterized in that block data of a preceding encrypted block is set as the initial vector of a succeeding encrypted block.

9. Retail transactions involving distributed and super-distributed digital content in a digital rights management (DRM) system

US7149722B1 | Microsoft Corp

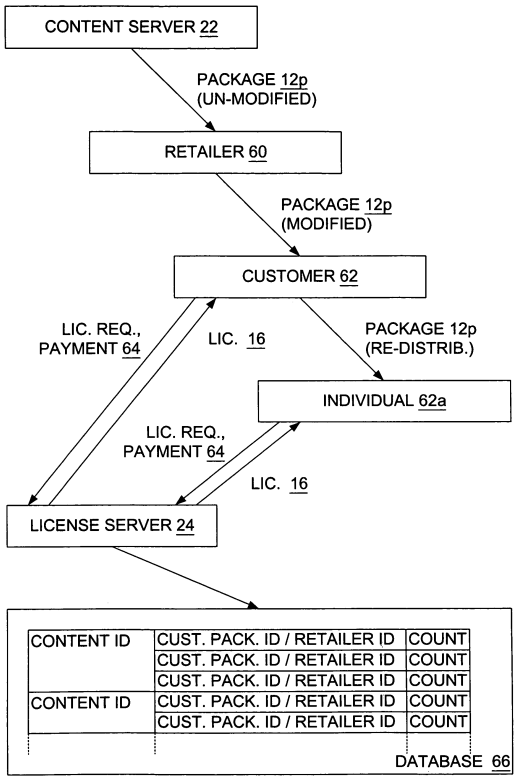
Bibliographic data

Publication date: 2006-12-12
Application date: 2000-09-28
Earliest priority date: 2000-09-28

Inventors: ABBURI RAJASEKHAR

CPC classification: G06F 21/10, G06F 2221/2135, H04L 2209/56, H04L 2209/603, H04L 63/0428, H04L 63/08, H04L 9/08, H04L 9/3247
IPC classification: H04K 1/00

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

To distribute digital content from a retailer to a customer, the content as issued by a content provider is retrieved. The as issued content has license acquisition information for acquiring a corresponding license attached thereto, where the license acquisition information includes a site identifier identifying a site at which the customer may obtain a digital license corresponding to the content. The site identifier includes an additional information field attached thereto. The additional information field is modified to include retailer information identifying the retailer, and the content is delivered with the modified additional information field to the customer. Thus, a license request sent from the customer is addressed to the site identified by the site identifier in the license acquisition information and includes the modified additional information field attached thereto. The corresponding digital license is issued to the customer after receiving the license request at the site identified by the site identifier, and after payment is received at such site from the customer in connection with the license request. The retailer information from the license request is retrieved and the retailer is identified therefrom, and such identified retailer is credited for a portion of the payment received.

First claim

A method of issuing digital licenses from a licensor for a corresponding piece of digital content, the content originally having been issued by a retailer, the method comprising performing a plurality of transactions, each transaction comprising:
the licensor receiving a first license request for a first license from a first customer in connection with the content and issuing a first license in response thereto, the first customer having received a copy of the content from the retailer, the first request including retailer information associated with the corresponding piece of digital content and identifying the retailer;
the licensor receiving a payment from the first customer in connection with the first license request;
the licensor retrieving the retailer information from the first license request and identifying the retailer therefrom;
the licensor crediting the identified retailer for a portion of the payment received in connection with the first license request;
the licensor receiving a second license request for a second license from a second customer in connection with the

content and issuing a second license in response thereto, the second customer having received a copy of the content from the first customer, the second request including first customer information associated with the corresponding piece of digital content and identifying the first customer;
the licensor receiving a payment from the second customer in connection with the second license request;
the licensor retrieving the first customer information from the license request and identifying the first customer therefrom;
the licensor crediting the first customer for a portion of the payment received in connection with the second license request,
wherein crediting the first customer comprises recording the first customer information in a database for accounting purposes, the database including an entry for each first customer information, each entry including a count for counting the number of times a license has been issued for the specific first customer information combination, such recording comprising:
finding the first customer information entry in the database corresponding to the first customer information of the second request, or creating such sub-entry if none is present;
incrementing the count in such entry,
whereby over the plurality of transactions the count in the entry is accumulated,
the method further comprising providing the portions of the payments to the first customer based on the accumulated count.

10. Content usage management system and content usage management method

US20020107806A1 | Individual

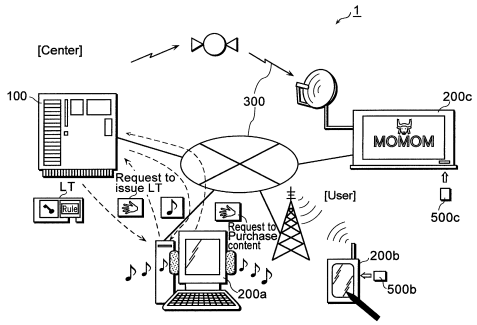
Bibliographic data

Publication date: 2002-08-08
Application date: 2002-02-01
Earliest priority date: 2001-02-02

Inventors: HIGASHI AKIO, MURAKAMI HIROKI, MATSUO TAKASHI, NAKAHARA TOHRU, NAMBA TAKAAKI, GOTO YOSHIMASA, NAKANISHI MASANORI, MIYAZAKI MASAYA, KOZUKA MASAYUKI

CPC classification: G06F 15/16, G06F 21/105, G06Q 30/06, H04N 21/65
IPC classification: G06F 17/00, G06F 1/00, G06F 15/16, H04N 7/16, G06F 21/10

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

A content usage management system 1 comprises a user terminal 200 a using a content as a digital production and a server 100 managing usage of the content in the user terminal 200 a over a communication network 300; wherein the sever 100 includes a user right information DB 120 that memorizes right information regarding a usage right of the content entitled to a user who uses the terminal 200 a and a content information generation unit 170 that generates LT which is right information indicating a part of usage right entitled to the user based upon a request from the user and that sends the LT to the sever terminal 200 a ; and the user terminal 200 a includes a communication unit that receives the LT sent from the server 100 and a license information processing unit 260 that controls usage of the content according to the usage right indicated on the received LT.

First claim

A content usage management system that comprises a terminal device that uses a content as a digital production, and a server device that manages usage of the content on the terminal device via a transmission line,
wherein the server device includes:
a right information memory unit operable to memorize right information related to a usage right of the content entitled to a user who uses the terminal device; and
a license ticket issuance unit operable to generate a license ticket based on a request from a user as right information that indicates a part of the usage right entitled to the user and to send the license ticket to the terminal device, and
the terminal device includes:
a receiving unit operable to receive the license ticket from the server device; and
a content usage control unit operable to control usage of the content according to the usage right indicated on the received license ticket.

11. INFORMATION PROCESSING DEVICE AND METHOD, RECORDING MEDIUM, AND PROGRAM

JP2002297816A | Sony Corp

Bibliographic data

Publication date: 2002-10-11
Application date: 2001-03-29
Earliest priority date: 2001-03-29

Inventors: ISHIGURO RYUJI

CPC classification:
IPC classification: G06Q 10/00, G06Q 50/00, G06F 12/14, G06F 21/10, G06Q 30/02, G06Q 30/06, G06Q 50/10, G06F 21/60, G06F 21/62

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

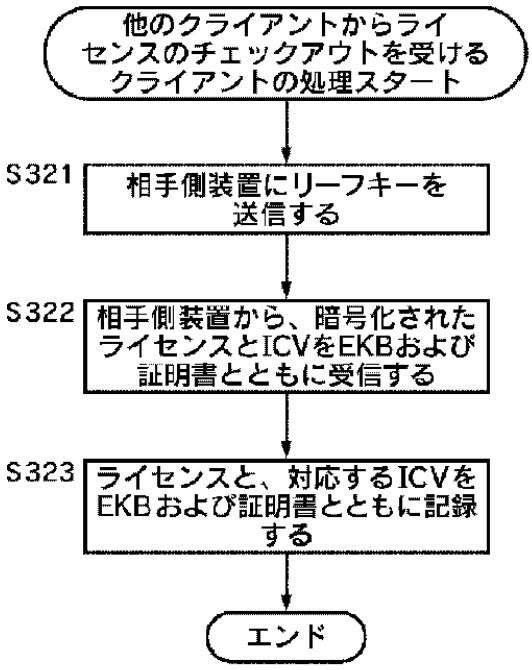


図42

Abstract

PROBLEM TO BE SOLVED: To make easily usable contents in a random device by acquiring the number of outputs of a license for using the contents. SOLUTION: A leaf key is sent to a counterpart device (step S321), and an encrypted license and an EKB(an Enabling Key Block) to be used as key information for deciphering it is sent from the counterpart device and recorded (step S322).

First claim

An information processing apparatus that manages a license that defines a use condition of a content, wherein the first obtaining means obtains the license to be output to another information processing apparatus; and the first obtaining means obtains the license. Second obtaining means for obtaining the number of times the license can be output, third obtaining means for obtaining the actual number of times of outputting the license obtained by the first obtaining means, and the second obtaining means. Comparing means for comparing the number of times of output obtained by the means with the number of times of output obtained by the third obtaining means; output means for outputting the license to the other information processing apparatus; Control means for controlling output of the license by the output means to the other information processing apparatus based on a comparison result by the comparison means. Information processing device.

12. Enforcement architecture and method for digital rights management system for roaming a license to a plurality of user devices

US7203966B2 | Microsoft Corp

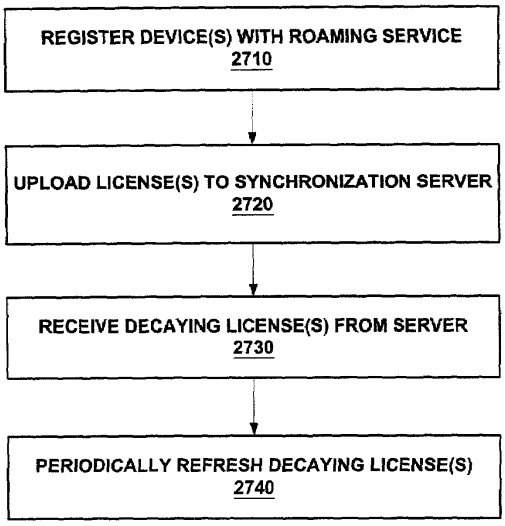
Bibliographic data

Publication date: 2007-04-10
Application date: 2001-06-27
Earliest priority date: 2001-06-27

Inventors: ABBURI RAJASEKHAR, ALKOVE JAMES M, MCNEILL WILLIAM P, MCKUNE JEFFREY R

CPC classification: G06F 21/10, G06F 2221/0797
IPC classification: G06F 21/22, G06F 21/00, G06F 21/20, G06F 21/24

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

An enforcement architecture and method for implementing roaming digital rights management are disclosed. A license distributed from a license server to a computing device of a user may be uploaded to a license synchronization server, and rebound to other devices registered with the service, thereby enabling access to the licensed content from other computing devices. A second digital license of a second computing device is set to expire prior to a first digital license of a first computing device. Reactivating a decayed first digital license, that is deactivated during transmission of the second digital license, to the second device to access content of the first computing device.

First claim

A method of enabling the use of a digital license on a plurality of devices, said digital license permitting the use of a content item and being bound to a first of said plurality of devices by a first public/private key pair associated with said first device, said method comprising:
receiving a first digital license from said first device, said first digital license associated with a first expiration date;
receiving a second public/private key pair associated with a second of said plurality of devices, said second key pair being different from said first key pair;
creating a second digital license bound to said second device using said second key pair, said second digital license being based on said first digital license, wherein said second digital license is set to expire prior to said first expiration date on a second expiration date;
disabling said first digital license;
transmitting said second digital license to said second device;
deactivating said second digital license past said second expiration date, wherein failure of said second device to contact a license synchronization server prior to said second expiration date results in removal of said second device from a registration store on said license synchronization server;
reactivating said first digital license to said first device and accessing digital content through said first device using said reactivated first digital license.

13. Data terminal equipment

JP4737857B2 | Sanyo Electric Co Ltd

Bibliographic data

Publication date: 2011-08-03
Application date: 2001-03-26
Earliest priority date: 2001-03-26

Inventors: 堀 吉宏, 上村 透

CPC classification:
IPC classification: G06Q 10/00, G06Q 50/00, H04L 9/08, H04L 9/32, G06F 12/14, H04N 7/173, G06F 21/10, G06Q 50/10, G06F 21/60, G06F 21/62, H04N 21/4623

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

PROBLEM TO BE SOLVED: To provide a data terminal equipment capable of moving enciphered contents data and a license received by software or hardware to another data terminal equipment in the same way. SOLUTION: A hard disk 530 of a personal computer is provided with license management files 1521-152n. A license managing device 520 stores a binding license for managing a license obtained by software and a license obtained by hardware corresponding to entry numbers included in the license management files 1521-152n of the hard disk 530 in a license area 5215B of a memory. The license management files 1521-152n include security information obtained by enciphering the license obtained by the software by the binding key included in the binding license.

First claim

The content data to a data terminal device that stores a license to obtain the original plain text by decrypting the encrypted encrypted content data and said encrypted content data,
A device unit that is detachable from a data terminal device that manages the license at the first security level;
A module unit for managing the license at a second security level lower than the first security level;
A storage unit for storing the encrypted content data ;
A control unit ,
The device part is
A license storage unit for storing a license managed at the first security level;
A license input / output unit that constructs an encryption path and obtains the license from the outside and stores it in the license storage unit, or constructs an encryption path and stores the license stored in the license storage unit;
A first management file including a first management number for specifying a storage position of a license stored in the license storage unit; an encrypted license generated by the module unit; and a binding stored in the license storage unit A management file storage unit for storing a second management file including a second management number for specifying a storage location of the license for use,
The module part is
The license managed at the second security level is encrypted with the binding key included in the binding license managed at the first security level by acquiring the license from outside by constructing an encryption path An encryption license is generated, the second management file including a first management number for the binding license including the generated encryption license and the used binding key is generated, and the generated second management file is stored in the device. Stored in the management file storage
Further, the second management file stored in the management file storage unit is read out, and the license for binding is obtained from the license input / output unit based on the second management number included in the read out second management file. A license is extracted from the acquired binding key included in the acquired binding license and the encrypted license included in the read second management file, and includes the extracted license or the license key included in the extracted license Build the encryption path and provide the newly generated license to the outside.
The controller is
When acquiring the license managed at the first security level, control is performed so that the device unit acquires the license, and the first management file including a first management number for the acquired license is generated.

Storing the generated first management file in the management file storage unit;
When acquiring the license managed at the second security level, the module unit controls to acquire the license;
When obtaining encrypted content data,
Acquiring the encrypted content data, storing the acquired encrypted content data in a storage unit ;
When the license managed at the first security level is provided, the first management file stored in the management file storage unit is read, and based on the first management number included in the read first management file.
Control to provide the license from the license input / output unit,
Controlling to provide the license from the module unit when providing the license managed at the second security level;
When providing encrypted content data,
A data terminal device that reads and provides encrypted content data stored in the storage unit.

14. Information terminal equipment

JP3895940B2 | Sanyo Electric Co Ltd

Bibliographic data

Publication date: 2007-03-22
Application date: 2001-03-27
Earliest priority date: 2001-03-27

Inventors: 安田 朝明

CPC classification:
IPC classification: G06F 17/30, G06Q 10/00, G06Q 50/00, G06F 12/00, H04L 9/08, G06F 12/14, H04W 12/08, H04W 4/06, G06F 21/10, G06Q 30/06, G06Q 50/10, G06F 21/60, G06F 21/62

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

PROBLEM TO BE SOLVED: To provide an information terminal which retrieves a storage place on of ciphered contents data, which a user wants to acquire, and acquires ciphered contents data from this retrieved storage place. SOLUTION: When wanting to newly purchase music of an artist A, the user of a mobile phone 100 receives the retrieval result of the artist A from a delivery server 10. The mobile phone 100 retrieves a memory card, where ciphered contents data included in the retrieval result received from the delivery server 10 is stored, on the basis of a database. When ciphered contents data is stored in a memory card 111, the mobile phone 100 copies ciphered contents data from a mobile phone 101 and receives a license from the delivery server 10.

First claim

Information is created in a plurality of information terminal device, and to acquire the license to play multiple databases were searched to said encrypted content data the encrypted content data to manage encrypted content data A terminal equipment,
And transmitting and receiving unit for exchanging data with external,
A key operation unit for inputting instructions,
A storage unit for storing the list and the plurality of databases,
And a control unit,
And a display unit for giving the user a variety of information as visual information,
Each of the databases of the plurality, the license information that indicate the content identification information of a plurality for identifying the encrypted content data, a plurality of whether the license corresponding to the encrypted content data, the encrypted content data and and a recording device identification information of multiple for identifying the data recording device in which the license is recorded,
The list includes the terminal identification information of the plurality of identifying information terminal device generated database specifying a plurality of information for identifying the data base of the plurality, each of the databases of the plurality,
The control unit, in response to the purchase request of the encrypted content data, the search criteria for purchasing the content that is input through the key operation unit through the transmission and reception unit is transmitted to the distribution server, matching the search criteria that is received via the transceiver the content identification information from the distribution server of the content, and the license information and the terminal identification information content identification information that matches the received content identification information corresponding to the matching content identification information extracting from the plurality of databases and the list, the extracted content identification information, and creates a search results database containing license information and the terminal identification information, license information indicating content identification information, the presence or absence of the license, and the terminal identification information the filters to see on the display unit reads from the search results database, information terminal equipment.

15. Retail transactions involving digital content in a digital rights management (DRM) system

US7925591B2 | Microsoft Corp

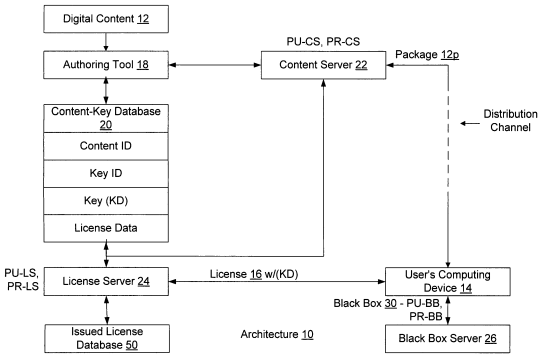
Bibliographic data

Publication date: 2011-04-12
Application date: 2006-03-28
Earliest priority date: 2000-09-28

Inventors: GAJJALA VIJAY K, GANESAN KRISHNAMURTHY, MCKUNE JEFFREY R

CPC classification: G06F 21/10, G06Q 30/0241, G06Q 30/06, G06Q 30/0621
IPC classification: G06F 21/00

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

A retailer facilitates issuance of a digital license from a licensor to a customer for a corresponding piece of digital content. The retailer receives payment for the license from the customer, where the payment is to be shared with the licensor in a pre-determined manner. The retailer also receives customer-based information from the customer. The retailer then composes an actual license request including the obtained customer-based information, and including retailer-based information identifying the retailer to the licensor and acknowledging to the licensor that the retailer owes a portion of the received payment to the licensor. Thereafter, the retailer forwards the actual license request to the licensor. The licensor notes based on the retailer-based information in the actual license request that the retailer identified thereby owes the licensor at least a portion of the forwarded payment. If an individual sends a license request directly to the licensor and thus fails to forward payment for the license to a retailer, the actual license request as composed by the individual fails to include the retailer-based information. Accordingly, the licensor refuses to issue a license as requested based on the lack of retailer-based information.

First claim

A method comprising:
receiving, from a customer, a selection of digital content and payment for the selected digital content;
delivering to a customer computing device a package containing license acquisition information including a site location for an executable controller, the package being without the digital content;
downloading the executable controller to the customer computing device, the customer computing device including a digital rights management (DRM) system to ensure that the digital content is rendered in accordance with the license, the executable controller, after downloading, directing the DRM system to send the package to a retailer with customer-based information;
receiving the package with the customer-based information, and adding retailer-based information to the package generating a modified package comprising an actual license request;
sending the actual license request to a licensor;
providing to the licensor the actual license request the actual license request including the customer-based information obtained from the customer and including the retailer-based information, the retailer-based information identifying the retailer to the licensor and acknowledging to the licensor that the retailer owes the licensor a portion of the payment received from the customer for the selected digital content in accordance with a defined business relationship between the retailer and licensor;
providing to the customer computing device, a digital license corresponding to the actual license request, the license acknowledging that the retailer owes the portion of the received payment to the licensor, wherein the digital content is downloaded to the DRM system of the customer using the executable controller after the executable controller senses receipt of the license;
determining, from the defined business relationship, the manner in which the received payment is to be shared between the retailer and the licensor;
providing to the licensor from the retailer the portion of the received payment.

16. Content usage control system, content usage apparatus, computer readable recording medium with program recorded for computer to execute usage method

US6873975B1 | Fujitsu Ltd

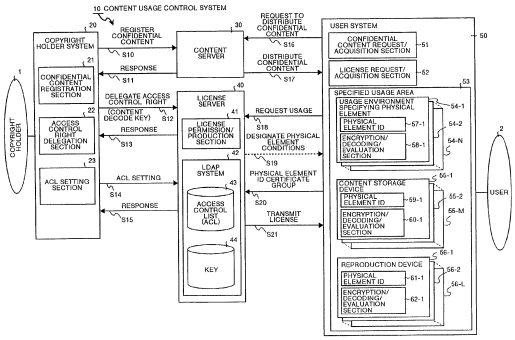
Bibliographic data

Publication date: 2005-03-29
Application date: 2000-03-08
Earliest priority date: 1999-04-06

Inventors: HATAKEYAMA TAKAHISA, YOSHIOKA MAKOTO, MIYAZAWA YUJI

CPC classification: G06Q 40/04
IPC classification: G06Q 40/00, G06F 15/00, H04L 9/00, G06F 21/00, G06F 12/14, G06F 21/32, G06F 21/10, G06Q 40/04, G06F 21/62, G06F 21/34, G06F 21/31, G06F 21/33

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

A content usage control system comprises a copyright holder system, content server, license server and user system. The ACL setting section of the copyright holder system sets a license ACL expressed as a structure by a combination of logic sums and logic products of a plurality of partial licenses for the content, based on the user ID and a plurality of physical element IDs including media used in the user system, and stores the license ACL in an access control list. The license server controls the usage of the content by the user utilizing the access control list.

First claim

A content usage control system which controls the usage of content supplied by an authorized information supplier including a content producer who is also an information producer and those persons authorized by the information producer, said system comprising:

a user unit which enables a user to use the content, said user unit including a plurality of physical elements;

a setting unit which sets a license as a structure expressed by a combination of logic sums and logic products of a plurality of partial licenses for the content based on ID information of the physical elements of said user unit including media used in said user unit and ID information of the user; and

a usage control unit which controls the usage of the content by said user unit by using license information that is encrypted in a multiplex way in a predetermined order, at the request of the user unit intending to use the content, from the license set by said setting unit and a content decode key by the ID information of the physical elements through which the license information is passed in sequence until the content is decoded by use of the content decode key,

wherein the license information is partially decoded by one of said physical elements, in inverse to said predetermined order, and then said partially decoded license information is sent to another of said physical elements to be decoded.

17. Binding a digital license to a portable device or the like in a digital rights management (DRM) system and checking out/checking in the digital license to/from the portable device or the like

US7073063B2 | Microsoft Corp

Bibliographic data

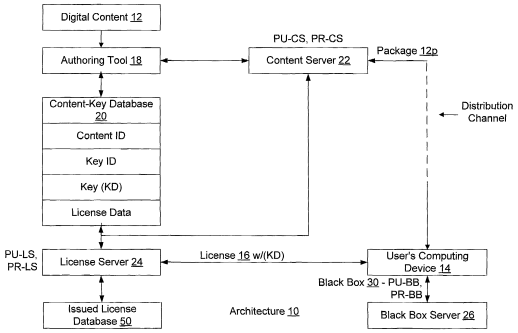
Publication date: 2006-07-04
Application date: 2001-06-27
Earliest priority date: 1999-03-27

Inventors: PEINADO MARCUS

CPC classification: G06F 21/10, G06F 21/71, G06F 2211/008, G06F 2221/0795, G06F 2221/0797, G06F 2221/2101, G06F 2221/2105, G06F 2221/2137, G06F 2221/2145, G07F 9/002, H04L 2463/101, H04L 63/0442, H04L 63/068, H04L 63/0823, H04L 63/12

IPC classification: G06F 1/00, H04L 9/08, H04L 9/00, H04L 9/32, G06F 21/00, H04L 29/06, G06F 12/14, G06F 21/32, G06F 21/10, G06Q 30/06, G06Q 50/10, G06F 21/60, G06F 21/44, G06F 21/62, G06F 21/33

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

To render digital content encrypted according to a content key (KD) on a first device having a public key (PU 1) and a corresponding private key (PR 1), a digital license corresponding to the content is obtained, where the digital license includes the content key (KD) therein in an encrypted form. The encrypted content key (KD) from the digital license is decrypted to produce the content key (KD), and the public key (PU 1) of the first device is obtained therefrom. The content key (KD) is then encrypted according to the public key (PU 1) of the first device (PU 1 (KD)), and a sub-license corresponding to and based on the obtained license is composed, where the sub-license includes (PU 1 (KD)). The composed sub-license is then transferred to the first device.

First claim

A method for a user at a second computing device to render encrypted digital content on a first computing device distinct from the second device, the first device having a public key (PU1) and a corresponding private key (PR1), the second device having a public key (PU2) and a corresponding private key (PR2), the digital content being encrypted according to a content key (KD), the method comprising:
the user at the second device obtaining from a licensor distinct from the second device a digital license corresponding to the content and the second device the digital license including the content key (KD) therein encrypted according to the public key (PU2) of the second device (PU2 (KD)), and also including rules for determining whether the license permits issuance of a sub-license from the second device to the first device;
the user at the second device determining that the rules of the license do in fact permit issuance of a sub-license from the second device to the first device;
the user at the second device decrypting (PU2 (KD)) from the digital license with the corresponding private key (PR2) to produce the content key (KD);
the user at the second device obtaining from the first device the public key thereof (PU1);
the user at the second device encrypting the content key (KD) according to the public key (PU1) of the first device (PU1 (KD));
the user at the second device composing the sub-license corresponding to and based on the obtained license for the first device, the sub-license including (PU1 (KD)), and transferring the composed sub-license to the first device, wherein the first device can decrypt (PU1 (KD)) with the private key thereof (PR1) to produce the content key (KD), and can render the encrypted content on the first device with the produced content key (KD).

18. System, apparatus, and method of contents distribution, and program and program recording medium directed to the same

US20030028490A1 | Individual

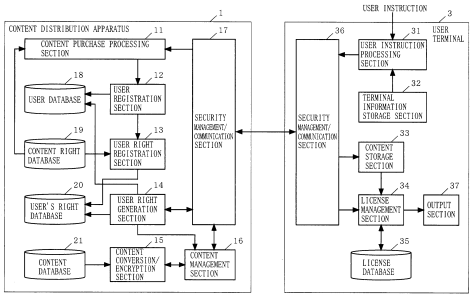
Bibliographic data

Publication date: 2003-02-06
Application date: 2002-07-31
Earliest priority date: 2001-07-31

Inventors: MIURA KOJI, YAMAMOTO MASAYA, OHO MASAHIRO

CPC classification: G06F 21/10, G06Q 30/06, H04M 15/68, H04M 15/84, H04M 2215/0196, H04M 2215/22, H04M 2215/32, H04M 2215/8129
IPC classification: G06Q 30/00, G06F 21/10

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

There is provided a content distribution system which is capable of a distributing a content in accordance with a requested data format or the capabilities of a terminal used, and which can eliminate inequity associated with content distribution in different data formats, by altering a usage rule. During content purchase processing, in a content distribution apparatus 1 , information concerning use of a content purchased by a user is registered in the user's right database 20 based on a user database 18 and a content right database 19 . For each content, the content right database 19 previously stores one or more units of information concerning content usage including usage rules for different usage modes. During content use processing, based on the registered information, the content distribution apparatus 1 transmits to the user terminal 3 a license stipulating a usage rule corresponding to the usage mode of a requested content.

First claim

A content distribution system in which a content distribution apparatus distributes a content to at least one user terminal,
wherein , in response to a request for use of a content transmitted from the at least one user terminal, and based on information concerning content usage including usage rules which are prescribed respectively corresponding to a plurality of usage modes, the content distribution apparatus dynamically generates a license stipulating a usage rule corresponding to a usage mode of the requested content, and transmits the generated license to the user terminal, and
the user terminal controls use of the content in accordance with the received license.

19. Content user system, recording medium, and content usage control method

JP3502035B2 | Fujitsu Ltd

Bibliographic data

Publication date: 2004-03-02
Application date: 2000-11-02
Earliest priority date: 2000-11-02

Inventors: 畠山 卓久, 吉岡 誠, 宮澤 雄司

CPC classification:
IPC classification: G06Q 10/00, G06F 15/00, G06Q 50/00, H04L 9/08, H04L 9/32, G06F 21/00, G06F 12/14, G06F 21/32, G06F 21/10, G06Q 30/06, G06Q 50/10, G06F 21/60, G06F 21/62, G06F 21/31, G06F 21/33

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

PROBLEM TO BE SOLVED: To provide a license server, copyrighter system, user system, system, recording medium and contents use control method for allowing an information providing authorized person including a person approved by an information prepare such as a copyrighter to execute contents use control, and for highly precisely preventing the illegal use of the contents. SOLUTION: In a license serve for managing the use of contents, a use condition for approving the use of contents and the name of an operation for the contents are accepted, and the accepted use condition for approving the use of contents is registered so as to be made correspond to the name of the operation for the contents.

First claim

A licensee for decrypting secret contents
License from the license server that manages
Content user system that uses confidential content
A computer-readable recording medium storing a program to be executed in Temu, the steps of the distribution request of the confidential contents, the content user con acquires the confidential content
The process of storing in the Tents storage device and the license for using the secret content are licensed.
When requesting the sense server, the content
Of the content user system, including
Corresponds to each of multiple physical elements that specify the usage environment.
Identifiers obtained from the plurality of physical elements
Generate a group of identifiers consisting of physical element identifiers,
An identifier sending step of sending the Nsusaba, La to obtain a license encrypted by the license server by using all the identifiers of the plurality of physical elements that were sent by the identifier sending step from the license server
The license acquisition process and the license acquisition process
A license decryption step for decrypting the obtained license, and a license decryption step for executing the license decryption step.
There are means for each physical element, and each license
Decoding means is based on the identifier for each physical element.
It has been partially decoded license to Ki, the near point
The confidential contents stored in the storage device can be used.
A computer-readable recording medium recording a program for causing a content user system to operate to decrypt a license for use.

20. Binding digital content to a portable storage device or the like in a digital rights management (DRM) system

US7010808B1 | Microsoft Corp

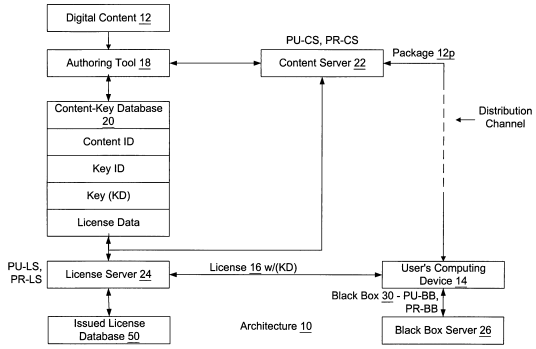
Bibliographic data

Publication date: 2006-03-07
Application date: 2000-08-25
Earliest priority date: 2000-08-25

Inventors: LEUNG YUEN YU, PEINADO MARCUS, STROM CLIFFORD P

CPC classification: G06F 21/10, H04L 63/10, H04N 21/41407, H04N 21/4405, H04N 21/4627
IPC classification: H04L 9/00, H04L 9/32, H04N 7/16

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

Digital content is rendered on a device by transferring the content to the device and obtaining a digital license corresponding to the content. A sub-license corresponding to and based on the obtained license is composed and transferred to the device, and the content is rendered on the device only in accordance with the terms of the sub-license. The content is encrypted and decryptable according to a content key, and the sub-license includes the content key encrypted and decryptable according to a secret. The sub-license also includes indexing information identifying the secret to the device. The indexing information in the sub-license is obtained to identify the secret, and the secret is acquired based at least in part on the indexing information. The secret is then applied to the encrypted content key to decrypt and obtain the content key, and the obtained content key is applied to the encrypted content to decrypt and obtain the content. To compose the sub-license and also to render the content, the secret is derived by obtaining a device identifier, acquiring a super-secret, and applying the obtained device identifier and super-secret to a function to derive the secret.

First claim

A method for enabling the rendering of digital content on a device, the method comprising:
transferring the content to the device;
obtaining a digital license corresponding to the content;
composing a sub-license corresponding to and based on the obtained license and transferring the composed sub-license to the device, to enable rendering of the content on the device only in accordance with the terms of the sub-license on the device, wherein the composed sub-license is transferred to the device after transferring the content to the device,
wherein the content is encrypted and decryptable according to a content key and wherein the license includes the content key encrypted into a form un-decryptable by the device, the composing of the sub-license comprising re-encrypting the content key into a form that is decryptable by the device and placing the re-encrypted content key in the sub-license, and
wherein the composing of the sub-license further comprises placing indexing information in the sub-license, the indexing information identifying a secret to the device that the device employs to decrypt the encrypted content key.

21. Digital license and method for obtaining/providing a digital license

US7136838B1 | Microsoft Corp

Bibliographic data

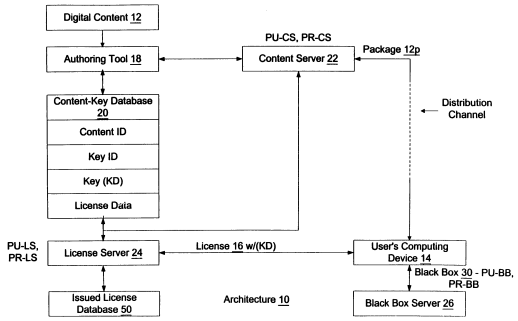
Publication date: 2006-11-14
Application date: 2000-01-13
Earliest priority date: 1999-03-27

Inventors: PEINADO MARCUS, ABBURI RAJASEKHAR, ENGLAND PAUL, GANESAN KRISHNAMURTHY, BELL JEFFREY R C, BLINN ARNOLD N, JONES THOMAS C

CPC classification: G06F 21/10, G06F 21/71, G06F 2211/007, G06F 2221/0797, G06F 2221/2105, G06F 2221/2137, G06Q 20/3678, G06Q 30/06, G07F 9/002, H04L 2463/101, H04L 63/0442, H04L 63/068, H04L 63/0823, H04L 63/12

IPC classification: G06F 1/00, G06F 21/00, H04L 29/06, H04N 7/167, G06Q 30/06, G06Q 20/36

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

To obtain a digital license for rendering a piece of digital content, a license requester contacts a license provider and sends a license request. The license provider checks the license request for validity and negotiates with the license requestor terms and conditions for the requested license. The license provider generates the requested license and issues the generated license to the license requestor.

First claim

A method for a server to provide to a client computer a digital license of one or more rights to render digital content, the digital content encrypted with a decryption key, the method comprising:
receiving, from the client computer, a license request, the license request containing a key identifier that identifies the decryption key and a client certificate associated with the client computer, the client certificate including a public key associated with the client computer;
responsive to the request, generating a license response including a digital rights license, the decryption key identified by the key identifier, and at least one server certificate to be used by the client computer to validate the license response;
transmitting the license response to the client computer,
wherein the generating comprises:
applying the key identifier as an input to an algorithm by which the decryption key is produced;
encrypting the decryption key with the public key to obtain an encrypted decryption key;
generating the license response including the encrypted decryption key, and at least one certificate to be used by the client computer to validate the license response.

22. CONTENTS USE MANAGEMENT SYSTEM AND SERVER USED FOR THE SAME

JP2003058660A | Matsushita Electric Industrial Co Ltd

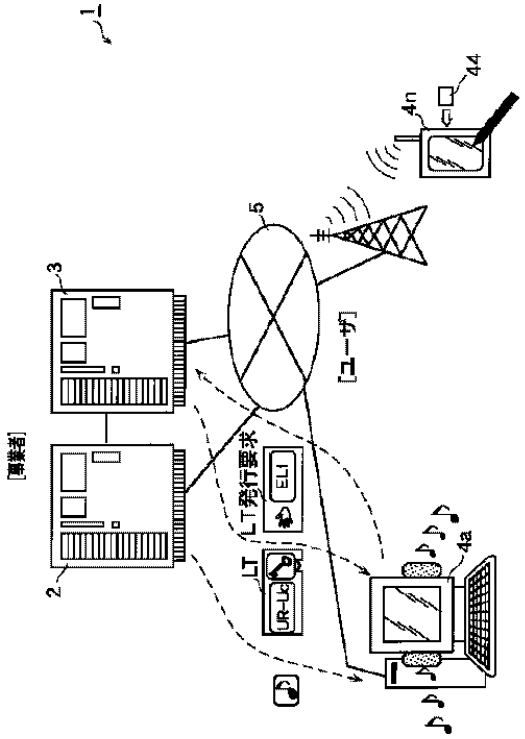
Bibliographic data

Publication date: 2003-02-28
Application date: 2002-05-27
Earliest priority date: 2001-06-07

Inventors: OKAMOTO RYUICHI, TOKUDA KATSUMI, MIURA YASUSHI

CPC classification:
IPC classification: G06F 15/00, G06Q 50/00, H04N 7/16, G06F 13/00, G06F 21/24, G06F 21/10, G06Q 30/06, H04N 21/266, G06Q 50/10, H04N 21/6334, G06F 21/62, H04N 21/4627

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

(57) [Summary] [PROBLEMS] To provide a content use management system in which a distribution server can reliably and optimally control the use of content in a user terminal and reduce the load on the user terminal. SOLUTION: User terminals 4a,..., 4n request the use condition management server 3 to use the content (LT issue request) in accordance with a user's instruction. The LT issuance request includes expectation information (ELI) indicating the requested content and the usage amount of the content. Usage condition management server 3 Holds license information indicating usage conditions of content for each user, and, based on a request from the user, expects a part or all of the usage conditions indicated by the license information corresponding to the user to be included in the LT issuance request. Information (ELI) And the right information (UR-Uc) , And transmits them to the user terminals 4a,..., 4n.

First claim

A content usage management system comprising: a terminal device that uses digital copyrighted content; and a server device that manages usage of the content in the terminal device, wherein the server device includes the terminal device. A license information storage unit that stores license information indicating usage conditions of contents for each user to be used, and a right indicating a part or all of the usage conditions indicated by the license information corresponding to the user based on a request from the user. A license ticket issuing unit for generating a license ticket, which is information, and transmitting the license ticket to the terminal device, the terminal device requesting the server device to use the content according to a user's instruction; and the server device. Receiving means for receiving the license ticket sent from Content usage control means for controlling the usage of the content according to the usage conditions indicated by the license ticket, and the requesting means transmits expected information indicating the requested content and the usage amount of the content to the server device. The content use management system according to claim 1, wherein the license ticket issuing unit generates the license ticket according to the expected information transmitted from the requesting unit and transmits the license ticket to the terminal device.

23. Data terminal equipment

JP4409081B2 | Renesas Technology Corp, Fujitsu Ltd, PFU Ltd, Sanyo Electric Co Ltd

Bibliographic data

Publication date: 2010-02-03
Application date: 2000-11-28
Earliest priority date: 2000-11-28

Inventors: 堀 吉宏, 上村 透, 宮園 真也, 畠山 卓久, 高橋 政孝, 常広 隆司, 大森 良夫

CPC classification:
IPC classification: G06Q 10/00, G06Q 50/00, H04L 9/08, H04L 9/32, G06F 13/00, G06F 12/14, H04N 7/167, G06F 21/10, H04N 21/2347, G06Q 30/06, H04N 21/266, G06Q 50/10, H04N 21/835, G06F 21/60, G06F 21/62, G10K 15/02

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

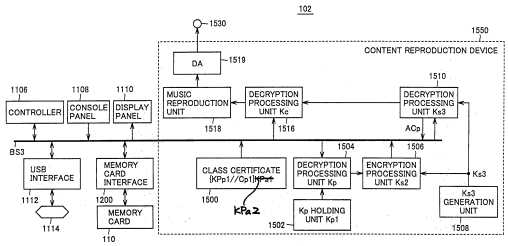
(57) [Problem] To provide a data terminal device capable of managing encrypted content data having different security levels according to the security level. SOLUTION: A content list file 150 includes content files 1531 to 1535 and license management files 1521 to 1525. The content files 1531 to 1535 correspond to the encrypted content data $ D received at different security levels. The file name of c @ Kc and the additional information Dc-inf is recorded. Also, the license management files 1521 to 152 5 are content files 1531 to 153, respectively. 5, and manages licenses received at different security levels.

First claim

A data terminal device that obtains an encrypted content data obtained by encrypting content data and a license for obtaining the original plaintext by decrypting the encrypted content data, and manages the encrypted content data and the license,
A device unit for acquiring the encrypted content data and the license at a first security level, and managing the license at the first security level;
A dedicated license obtained by acquiring the encrypted content data and the license at a second security level lower than the first security level, and applying encryption suitable for management at the second security level to the license A module part for generating
A storage unit for storing data;
A control unit,
The device unit includes a recording unit that records the license in association with a management number;
The storage unit
A plurality of encrypted content data; a plurality of first management files including a management number corresponding to a license managed by the device unit;
A plurality of second management files including the dedicated license;
A content list indicating a relationship between the first management file or the second management file and the encrypted content data;
When the control unit acquires a license at the first and second security levels, the control unit generates the first and second management files, and the acquired first and second management files and the acquired A data terminal device that writes encrypted content data to the storage unit and gives the device unit a license acquired at the first security level.

24. Data terminal managing ciphered content data and license acquired by software

US20050120232A1 | Fujitsu Ltd, Hitachi Ltd, Sanyo Electric Co Ltd



Bibliographic data

Publication date: 2005-06-02
Application date: 2003-10-09
Earliest priority date: 2000-11-28

Inventors: HORI YOSHIHIRO, KAMIMURA TORU, MIYAZONO SHINYA, HATAKEYAMA TAKAHISA, TAKAHASHI MASATAKA, TSUNEHIRO TAKASHI, OHMORI YOSHIO

CPC classification: G06F 21/10, G06Q 30/06, H04L 2209/08, H04L 2209/56, H04L 2209/60, H04L 9/0891, H04L 9/3268, H04L 9/3273
IPC classification: G06Q 30/00, H04L 9/08, H04L 9/32, G09C 1/00, G06F 21/10

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

A hard disk (530) of a personal computer has a content list file (150) and an encrypted private file (162). A license administration device (520) stores a binding key Kb in a license region (5215 B) of a memory. The encrypted private file (162) can be decrypted and encrypted with the binding key Kb stored in the license administration device (520). The license of the obtained and encrypted content data is stored as private information in the encrypted private file (162). Consequently, the encrypted content data and the license distributed by software can be shifted to another data terminal device.

First claim

A data terminal device obtaining encrypted content data prepared by encrypting content data and a license for decrypting said encrypted content data to obtain original plaintext, and providing said encrypted content data and said license to another data terminal device, comprising:
a module unit administering the obtaining, storing and providing of said license;
a device unit producing an encrypted private file by encrypting a private file including a plurality of licenses, and storing a binding license including a binding key for decrypting said encrypted private file to extract the private file in a dedicated region;
a storing unit storing data; and
a control unit, wherein said storing unit stores:
a plurality of encrypted content data, and
an encrypted private file including said plurality of license, and encrypted with said binding key;
in providing said license,
said control unit reads said encrypted private file from said storing unit, and provides said encrypted private file to said module unit;
said module unit obtains the binding license from said device unit, extracts the binding key from the obtained binding license, and provides the license obtained by decrypting said encrypted private file with the extracted binding key.

25. Structural of digital rights management (DRM) system

US7024393B1 | Microsoft Corp

Bibliographic data

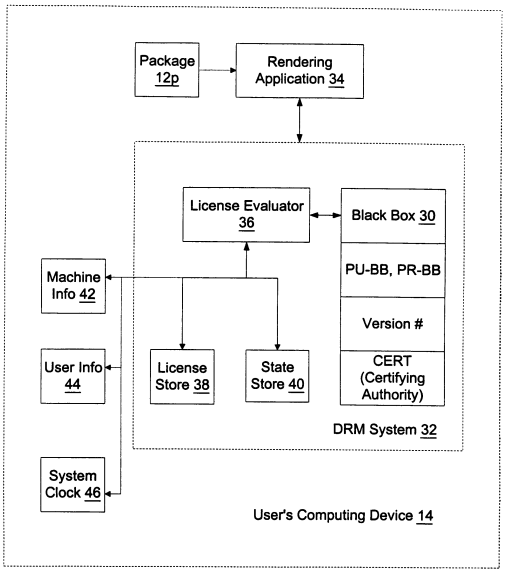
Publication date: 2006-04-04
Application date: 2000-01-13
Earliest priority date: 1999-03-27

Inventors: PEINADO MARCUS, ABBURI RAJASEKHAR, BELL JEFFREY R C

CPC classification: G06F 21/10, G06F 21/71, G06F 21/84, G06F 2211/007, G06F 2221/0795, G06F 2221/0797, G06F 2221/2105, G06F 2221/2137, H04L 2463/101, H04L 63/0442, H04L 63/068, H04L 63/0823, H04L 63/12

IPC classification: G06F 1/00, G06Q 50/00, H04L 9/00, G06F 21/00, H04L 29/06, G06F 12/14, G06F 21/24

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

A digital rights management (DRM) system operates on a computing device when a user requests that a protected piece of digital content be rendered by the computer device in a particular manner. The DRM system has a license store, a license evaluator, and a state store. The license store stores digital licenses on the computing device. The license evaluator determines whether any licenses stored in the license store correspond to the requested digital content and whether any such corresponding licenses are valid, reviews license rules in each such valid license, and determining based on such reviewed license rules whether such license enables the requesting user to render the requested digital content in the manner sought. The state store maintains state information corresponding to each license in the license store, where the state information is created and updated by the license evaluator as necessary.

First claim

A digital rights management (DRM) system operating on a computing device when a user requests that a protected piece of digital content be rendered by the computer device in a particular manner, the system comprising:
a rendering application by which the requested digital content is rendered;
a license store for storing one or more digital licenses on the computing device, the license store providing access to the one or more digital licenses separately from the requested digital content;
a license evaluator for determining whether any licenses stored in the license store correspond to the requested digital content, for determining whether any such corresponding licenses are valid, for reviewing license rules in each such valid license, and for determining based on such reviewed license rules whether such license enables the requesting user to render the requested digital content in the manner sought;
a state store for maintaining state information corresponding to each license in the license store, the state information being created and updated by the license evaluator as necessary; and
a black box for performing encryption and decryption functions as part of the evaluation of any license,
wherein the license evaluator selects an enabling, valid license and works with the black box to obtain a decryption key (KD) from the selected license, and wherein the black box employs such decryption key (KD) to decrypt the protected digital content, and
wherein the black box decrypts the protected digital content when the license evaluator determines that a license in fact enables the requesting user to render the requested digital content in the manner sought.

26. Data terminal capable of transferring ciphered content data and license acquired by software

US20050076208A1 | Fujitsu Ltd, Sanyo Electric Co Ltd

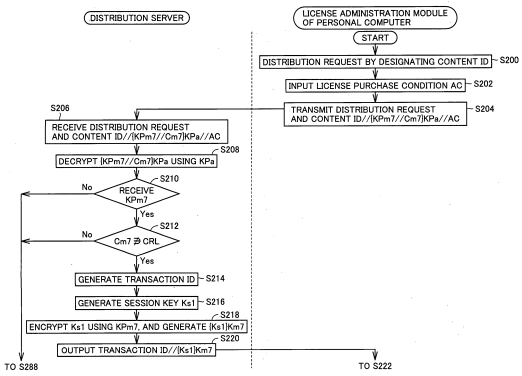
Bibliographic data

Publication date: 2005-04-07
Application date: 2003-09-16
Earliest priority date: 2000-11-24

Inventors: HORI YOSHIHIRO, KAMIMURA TORU, MIYAZONO SHINYA, HATAKEYAMA TAKAHISA, HASEBE TAKAYUKI, TAKAHASHI MASATAKA, TSUNEHIRO TAKASHI, OHMORI YOSHIO

CPC classification: G06F 21/10, G06F 2221/0771
IPC classification: G06K 19/00, G06Q 50/00, H04L 9/08, H04L 9/32, G06F 13/00, G06F 12/14, G06F 21/10, G06Q 30/06, G06Q 50/10, G06F 21/60, G06F 21/62

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

A personal computer 50 holds encrypted contents data and a license acquired from a distribution server (10) over an Internet network (30) or from a music CD (60) using a CD-ROM drive. The personal computer (50), which is connected to a portable reproduction terminal (100) through a USB cable (70), performs a checkout operation for lending out, the encrypted contents data and the license to a memory card (110) attached to the portable reproduction terminal (100), and a checkin operation for returning the lent encrypted contents data and the lent license. As a result, it is possible to shift the encrypted contents data and the license acquired by software to the other device.

First claim

A data terminal device for lending and returning encrypted contents data obtained by encrypting contents data and a license for decrypting said encrypted contents data to obtain the original contents data or for lending and returning said license, to and from a data recording device, the data terminal device comprising:
a storage unit storing said encrypted contents data, said license and lending information which is information for administrating said lending;
a control unit; and
an interface controlling data exchange between said data recording device and said control unit, wherein in said lending out,
said control unit receives an inherent ID capable of specifying said data recording device and allocated inherently to each data recording device from said data recording device through said interface, generates a lending ID inherent to each lending and for specifying a lending license for lending said encrypted contents data and said license or for lending said license, generates a lending license including said generated lending ID and for decrypting said encrypted contents data to obtain the original content based on said license stored in said storage unit, transmits the generated lending license or said lending license and said encrypted contents data to said data recording device through said interface, and adds said received inherent ID and said generated lending ID to said lending information while associating said received inherent ID with said generated lending ID, and
in said return,
when said control unit checks that said inherent ID is received from said data recording device through said interface, the received inherent ID coincides with the inherent ID included in said lending information, and that the lending license including said lending ID associated with said inherent ID included in said lending information is recorded in said data recording device, said control unit returns said lending license recorded on said data recording device or said lending license and said encrypted contents data decryptable based on said lending license from said data recording device, and deletes the lending ID and the inherent ID corresponding to said returned lending license from

said lending information.

27. Rendering digital content in an encrypted rights-protected form

US6775655B1 | Microsoft Corp

Bibliographic data

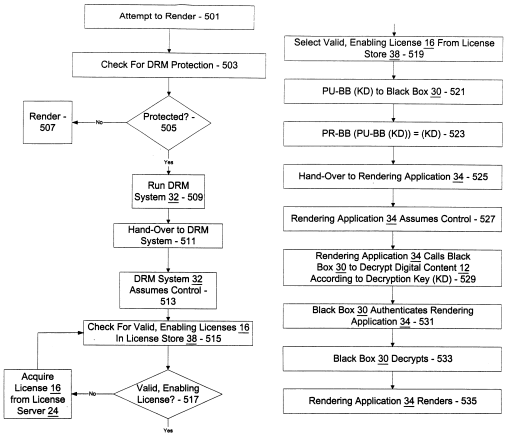
Publication date: 2004-08-10
Application date: 1999-11-24
Earliest priority date: 1999-03-27

Inventors: PEINADO MARCUS, MANFERDELLI JOHN L, BELL JEFFREY R C

CPC classification: G06F 21/10, G06F 21/71, G06F 21/84, G06F 2211/007, G06F 2221/0797, G06F 2221/2105, G06F 2221/2137, G06Q 30/0601, G07F 9/002, H04L 2463/101, H04L 63/0442, H04L 63/068, H04L 63/0823, H04L 63/12

IPC classification: G06F 1/00, H04L 9/08, H04L 9/32, G06F 21/00, H04L 29/06, G06F 12/14, G06F 21/24, G06Q 30/06

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

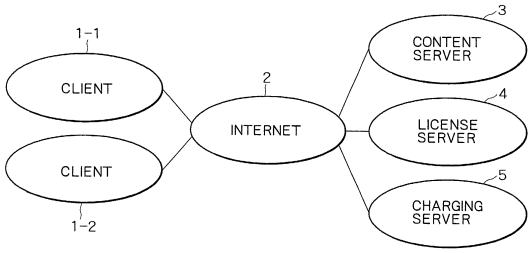
A rendering application determines that digital content is in an encrypted rights-protected form and invokes a Digital Rights Management (DRM) system which includes a license store having at least one digital license stored therein. Each license corresponds to a piece of digital content and includes a decryption key (KD) for decrypting the corresponding digital content. The DRM system locates each license in the license store corresponding to the digital content to be rendered, selects one of the located licenses, obtains (KD) from the selected license, decrypts the digital content with (KD), and returns the decrypted digital content to the rendering application for actual rendering.

First claim

A method for rendering digital content in an encrypted rights-protected form, the method comprising:
determining, by a rendering application, that the digital content is in the encrypted rights-protected form;
invoking, by the rendering application, a Digital Rights Management (DRM) system, the DRM system including a license store having at least one digital license stored therein, each license corresponding to a piece of digital content and including a decryption key (KD) for decrypting the corresponding digital content;
locating, by the DRM system, each license in the license store corresponding to the digital content to be rendered;
selecting, by the DRM system, one of the located licenses;
obtaining, by the DRM system, (KD) from the selected license;
decrypting, by the DRM system, the digital content with (KD);
returning, by the DRM system, the decrypted digital content to the rendering application for actual rendering, wherein the DRM system further includes a public key (PU) and a private key (PR), wherein the at least one license corresponding to the digital content includes a decryption key (KD) encrypted with the public key (PU) of the DRM system (PU(KD)), and wherein obtaining (KD) from the selected license comprises: obtaining, by the DRM system, (PU(KD)) from the selected license;
decrypting, by the DRM system, (PU(KD)) with (PR) to produce (KD).

28. Information processing method, information processing apparatus and recording medium

US7260721B2 | Sony Corp



Bibliographic data

Publication date: 2007-08-21
Application date: 2002-02-08
Earliest priority date: 2001-02-09

Inventors: TANAKA KOICHI, KAWAKAMI ITARU, KURODA YOSHISUKE, ISHIGURO RYUJI

CPC classification: G06F 17/00, G06F 21/10, G06F 2221/0753, G06F 2221/0771, G06F 2221/2135, G06F 2221/2137, G06Q 20/3821
IPC classification: G06F 17/00, G06F 1/00, H04N 7/167, G06F 21/10

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

A client receives encrypted content from content server. The header of the content includes license-identifying information for identifying a license required to utilize the content. The client requests a license server to transmit the license identified by the license-identifying information. When receiving the request for a license, the license server carries out a charging process before transmitting the license to the client. The client stores the license received from the license server. The stored license serves as a condition for encrypting and playing back the content. As a result, content can be distributed with a high degree of freedom and only an authorized user is capable of utilizing the content.

First claim

An information processing apparatus for allowing usage of content by requiring a license for using said content, said information processing apparatus comprising:
a content storage unit operable to store license-identification information for specifying said license for using said content, encrypted data of said content and key information required for decrypting said encrypted data of said content;
a license storage unit operable to store said license for using said content, including content-specifying information for specifying said content and terminal-identification information which identifies the information processing apparatus, the use of which is allowed by said license;
a judgment unit operable to determine whether said license for using said content has been stored in said license storage unit;
a decryption unit operable to decrypt said encrypted data of said content if said license for using said content has been stored in said license storage unit;
a device-node-key storage unit operable to store a device node key which is assigned the information processing apparatus from the license server when registering, wherein said key information includes an EKB (Enabling Key Block); and
said decryption unit is operable to decrypt said EKB (Enabling Key Block) using said device node key to obtain a root key, and to decrypt said data of said content using said root key.

29. RENDERING DIGITAL CONTENT IN AN ENCRYPTED RIGHTS-PROTECTED FORM

WO2000059151A2 | MICROSOFT CORP

Bibliographic data

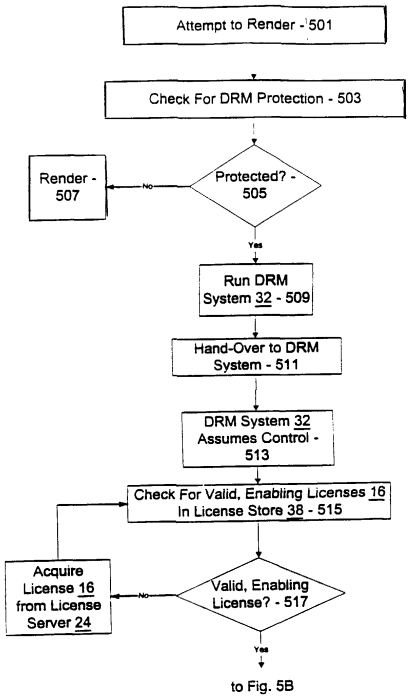
Publication date: 2000-10-05
Application date: 2000-02-25
Earliest priority date: 1999-03-27

Inventors: PEINADO MARCUS, MANFERDELLI JOHN L, BELL JEFFREY R C

CPC classification: G06F 21/10, G06F 21/71, G06F 21/84, G06F 2211/007, G06F 2221/0704, G06F 2221/0797, G06F 2221/2105, G06F 2221/2137, H04L 2463/101, H04L 63/0442, H04L 63/068, H04L 63/0823, H04L 63/12

IPC classification: G06F 1/00, H04L 29/06, G06F 21/10, G06F 21/71, G06F 21/84

External links: Google Patents, Espacenet, EP Register, Patentscope, PatBase Express, PatBase, Orbit



Abstract

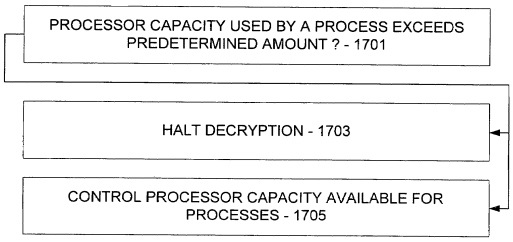
A rending application determines that digital content is in an encrypted rights-protected form and invokes a Digital Rights Management (DRM) system which includes a license store having at least one digital license stored therein. Each license corresponds to a piece of digital content and includes a decryption key (KD) for decrypting the corresponding digital content. The DRM system locates each license in the license store corresponding to the digital content to be rendered, selects one of the located licenses, obtains (KD) from the selected license, decrypts the digital content with (KD), and returns the decrypted digital content to the rendering application for actual rendering.

First claim

A 'method for rendering digital content in an encrypted rights-protected form, the method comprising:
determining, by a rendering application, that the digital content is in the encrypted rights-protected form;
invoking, by the rendering application, a Digital Rights Management
(DRM) system, the DRM system including a license store having at least one digital license stored therein, each license corresponding to a piece of digital content and including a decryption key (KD) for decrypting the corresponding digital content;
locating, by the DRM system, each license in the license store corresponding to the digital content to be rendered;
selecting, by the DRM system, one of the located licenses;
obtaining, by the DRM system, (KD) from the selected license;
decrypting, by the DRM system, the digital content with (KD);
returning, by the DRM system, the decrypted digital content to the rendering application for actual rendering.

30. Protecting decrypted compressed content and decrypted decompressed content at a digital rights management client

US7162745B2 | Microsoft Corp



Bibliographic data

Publication date:	2007-01-09
Application date:	2005-07-07
Earliest priority date:	2001-06-27
Inventors:	ENGLAND PAUL, PEINADO MARCUS, SANKARANARAYAN MUKUND
CPC classification:	G06F 21/10
IPC classification:	G06F 1/26, G06F 21/00, H04N 7/167, G08B 13/00
External links:	Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

Theft of decompressed digital content as the content is being rendered is prevented. A requested slow-down of the rendering of the content is detected. Transfers of relatively large amounts of data are detected. A re-compressor-based requested slow-down of the rendering of the content is detected. A re-compressor re-compressing the content is detected. In each situation, the detected activity is presumably initiated by a content thief attempting to steal the content. In each situation, the detected activity is responded to in a manner designed to frustrate the presumed attempt of the content thief to steal the content.

First claim

A method of preventing theft of decompressed digital content as the content is being rendered, the method comprising:

detecting transfers of amounts of data above a predetermined amount, wherein the detected transfers are presumably initiated by a content thief attempting to steal the content;

responding to the detected transfers in a manner designed to frustrate the presumed attempt of the content thief to steal the content,

wherein rendering of the content occurs on a processor having an amount of capacity, and wherein responding comprises reserving an amount of the capacity of the processor above a predetermined amount for rendering, the reserved capacity not being available to the content thief for use in stealing the content.

31. Structure of a digital content package

US7383205B1 | Microsoft Corp

Bibliographic data

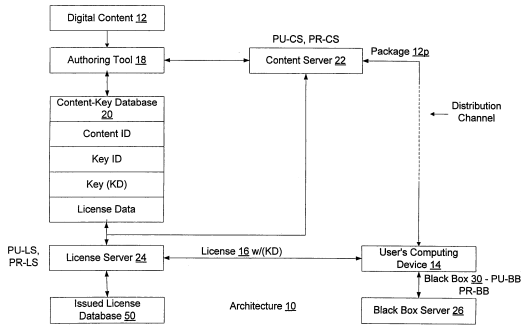
Publication date: 2008-06-03
Application date: 2000-01-13
Earliest priority date: 1999-03-27

Inventors: PEINADO MARCUS, ABBURI RAJASEKHAR, BLINN ARNOLD N, JONES THOMAS C, BELL JEFFREY R C

CPC classification: G06F 21/10, G06F 21/71, G06F 2211/007, G06F 2221/0797, G06F 2221/2105, G06F 2221/2137, G06Q 40/04, H04L 2463/101, H04L 63/0442, H04L 63/068, H04L 63/0823, H04L 63/12

IPC classification: G06F 1/00, G06F 21/00, H04L 29/06, G06Q 40/04

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

A digital content package includes encrypted digital content to be rendered in accordance with a corresponding digital license and is separate and apart from the license. The encrypted digital content is decrypt-able according to a decryption key (KD) obtained from the license. The package also includes a content/package ID that identifies one of the digital content and the package, and license acquisition information including a location of a license provider for providing the license.

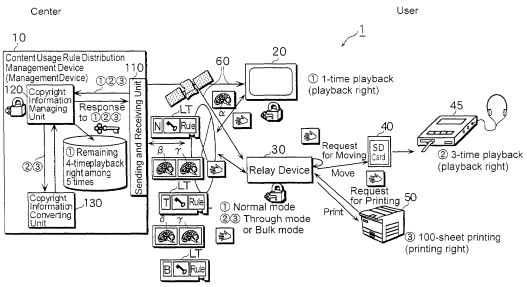
First claim

A method for using digital rights management to enforce rights in digital content, the digital content located in a digital content package, the method comprising:
distributing the digital content package from a content server to a computing device of a user, wherein the digital content package is provided to the content server by a content provider having a public key and a private key, wherein the digital content package comprises:
a first data field containing the digital content to be rendered in accordance with a corresponding digital license, the digital content being encrypted, the digital content being decrypt-able according to a decryption key (KD) obtained from the corresponding digital license;
a second data field containing a content ID or a package ID identifying one of the digital content and the digital content package respectively, the corresponding digital license also having the content ID or the digital content package ID such that the content ID or the digital content package ID from the digital content package is employed to locate the corresponding digital license;
a third data field containing license acquisition information including a location of a license provider for providing the license after identifying the digital content ID or the digital content package ID to the license provider, wherein the license acquisition information is in an unencrypted form;
a fourth data field containing the content provider public key, wherein the corresponding license including a content provider digital certificate issued and signed by the content provider private key to show permission from the content provider to the license provider to provide the corresponding digital license, such that the content provider public key from the digital content package is employed to validate the content provider digital certificate of the corresponding digital license;
receiving the distributed digital content package at the computing device;
attempting to render the digital content by way of a rendering application;
invoking, by the rendering application, a Digital Rights Management (DRM) system upon the rendering application attempting to render the digital content, the DRM system employing a trusted black box to perform decryption and encryption functions;
determining, by the DRM system, whether a right to render the digital content in the manner sought exists based on any digital license stored in the computing device and corresponding to the digital content;
if the right does not exist:

requesting from a license server a particular digital license that corresponds to and is separate from the digital content;
issuing, by the license server, the particular digital license to the DRM system only if the license server trusts the DRM system to abide by the particular digital license;
receiving, by the computing device and from the license server, the issued particular digital license corresponding to the digital content;
storing the received particular digital license on the computing device;
rendering the digital content using the rendering application and the stored particular digital license.

32. License management system, license management device, relay device and terminal device

US7359883B2 | Matsushita Electric Industrial Co Ltd



Bibliographic data

Publication date: 2008-04-15
Application date: 2002-10-11
Earliest priority date: 2001-04-19

Inventors: NAMBA TAKAAKI, MATSUO TAKASHI, HIGASHI AKIO, NAKAHARA TOHRU, MURAKAMI HIROKI, NAKANISHI MASANORI, UESAKA YASUSHI, MIURA KOUJI

CPC classification: G06F 17/00, H04N 21/2541, H04N 21/26613, H04N 21/4117, H04N 21/4516, H04N 21/454, H04N 21/472, H04N 21/63345, H04N 21/8355, H04N 7/165
IPC classification: H04K 1/00, H04N 5/00, H04N 7/16

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

A management device of a license management system acquires a usage request of a content from an SD card or a printer via a relay device, analyzes the acquired usage request, acquires usage environment information of the SD card or the printer from the relay device, analyzes the acquired usage environment information, generates license information including a usage rule corresponding to the analysis results of the usage request and the usage environment information, generates instruction information indicating how to handle the license information in the relay device based on the analysis result of the usage environment information, embeds the generated instruction information in the license information, and sends the license information to the relay device. The relay device receives the license information in which the instruction information is embedded, and transfers the received license information to the SD card or the printer according to the instruction information which is embedded in the license information with performing certain processing or without performing any processing to the license information.

First claim

A license management system for distributing license information to a terminal device of a user, the license information allowing use of a content under a predetermined usage rule, the license management system comprising:
a management device programmed to distribute the license information;
a relay device programmed to receive the license information distributed from said management device and transfer the license information; and
a terminal device programmed to receive the license information transferred from said relay device and use the content according to the license information,
wherein said management device includes:
a usage request analyzing unit programmed to obtain a usage request for the content from said terminal device via said relay device, and to analyze the obtained usage request;
a usage environment information analyzing unit programmed to obtain, from said relay device, first usage environment information indicating a usage rule processing capability of said terminal device and second usage environment information indicating a usage rule processing capability of said relay device, and to analyze the obtained first and second usage environment information;
a license information generating unit programmed to generate the license information including a usage rule corresponding to the analysis results of the usage request and the first and second usage environment information, the license information including sets of usage rules having different use formats and the same rights details;
an instruction information generating unit programmed to generate instruction information indicating how to handle the license information in said relay device, based on a comparison result obtained by comparing the first usage environment information and the second usage environment information; and
a license information sending unit programmed to embed the generated instruction information in the license

information, and to send the license information to said relay device,
wherein said relay device includes:
a first usage environment information holding unit programmed to hold the first and second usage environment information:
a first notifying unit programmed to notify said management device of the first and second usage environment information held by said first usage environment information holding unit;
a license information receiving unit programmed to receive the license information sent from said management device in which the instruction information is embedded; and
a transferring unit programmed to perform one of:
selecting at least one usable usage rule from a set of usage rules from the license information and transferring the at least one selected usage rule to said terminal device, when the instruction information embedded in the license information received from said management device indicates a first mode, and (ii) transferring the set of usage rules to said terminal device without selecting any usage rule, and
wherein said instruction information generating unit in said management device is programmed to compare the first usage environment information and the second usage environment usage information, and determine the instruction information as one of
a through mode which indicates that said relay device transmits the license information to said terminal device, when the usage rule processing capability of said terminal device is higher than the usage rule processing capability of said relay device,
a normal mode which indicates that said relay device decrypts and transmits the license information to said terminal device, when the usage rule processing capability of said relay device is higher than the usage rule processing capability of said terminal device, and
a bulk mode which indicates that the license information is expressed in a plurality of formats, when the first usage environment information is unclear because the first usage environment information cannot be understood, and
said transferring unit in said relay device is programmed to
when the instruction information in the license information received by said license information receiving unit indicates the through mode, transfer the received license information to said terminal device by passing the license information without performing any processing on the license information,
when the instruction information indicates the normal mode, said license information receiving unit is programmed to decrypt the received license information and to transfer the decrypted license information to said terminal device, and
when the instruction information indicates the bulk mode, said terminal device is programmed to select a usage rule for a license format that said terminal device can interpret from among the usage rules of a plurality of formats of the license information, to generate license information which includes only the selected usage rule and to transfer the license information to said terminal device.

33. Data terminal equipment

JP4553472B2 | Sanyo Electric Co Ltd

Bibliographic data

Publication date: 2010-09-29
Application date: 2000-09-20
Earliest priority date: 2000-09-20

Inventors: 堀 吉宏

CPC classification:
IPC classification: G06Q 50/00, G06F 12/00, G06F 21/00, G06F 12/14, G06F 21/10, G06Q 30/06, G06F 21/62, G06F 21/33, G10K 15/02

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

(57) [Problem] To provide a portable terminal device that receives only necessary encrypted content data and / or a license key from a distribution server. SOLUTION: When a request for receiving encrypted content data {Data} Kc is input from a user, the mobile phone sets a content ID in the attached memory card, The license key Kc, the reproduction count restriction information AC1, the reproduction expiration date, and the recording status of the encrypted content data {Data} Kc are searched. Then, the encrypted content data {Data} Kc not recorded in the license area 1415A and the data area 1415B of the memory card, and the license (content ID, license key Kc, Only the number-of-reproductions restriction information AC1 and the reproduction time limit are received from the distribution server.

First claim

A recording unit for receiving encrypted content data, a license key for decrypting the encrypted content data, and a license including reproduction restriction information for restricting reproduction of the encrypted content data, and recording the recording unit on a recording unit;
A reproduction unit for reproducing the content data based on the license key and the reproduction restriction information ;
A controller that searches for the presence or absence of a license capable of reproducing the encrypted content data ,
The control unit requests the distribution of the license when the encrypted content data is recorded in the recording unit and the license is not recorded in the recording unit.

34. Method for interdependently validating a digital content package and a corresponding digital license

US7680744B2 | Microsoft Corp

Bibliographic data

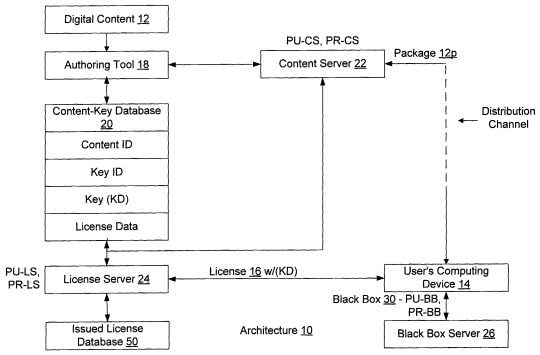
Publication date: 2010-03-16
Application date: 2005-04-28
Earliest priority date: 1999-03-27

Inventors: BLINN ARNOLD N, JONES THOMAS C

CPC classification: G06F 21/10, G06F 21/445, G06F 21/71, G06F 2211/007, G06F 2221/0791, G06F 2221/0797, G06F 2221/2105, G06F 2221/2137, G06F 2221/2141, G06Q 20/3674, G06Q 20/3829, G06Q 30/06, G06Q 50/188, G07F 9/002, H04L 2463/101, H04L 63/0442, H04L 63/068, H04L 63/0823, H04L 63/12

IPC classification: G06F 1/00, G06Q 99/00, G06F 21/00, H04L 29/06, G06Q 30/06, G06Q 20/38, G06Q 50/18, G06Q 20/36

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

A method is disclosed for a device to interdependently validate a digital content package having a piece of digital content in an encrypted form, and a corresponding digital license for rendering the digital content. A first key is derived from a source available to the device, and a first digital signature is obtained from the digital content package. The first key is applied to the first digital signature to validate the first digital signature and the digital content package. A second key is derived based on the first digital signature, and a second digital signature is obtained from the license. The second key is applied to the second digital signature to validate the second digital signature and the license.

First claim

A computer-readable storage medium having stored thereon computer-executable instructions for operating a digital rights management (DRM) system on a computing device, the instructions performing the steps of:
storing one or more digital licenses in a license store;
maintaining in a state store information corresponding to each of the one or more digital licenses in the license store, including maintaining a rendering corresponding to at least one of the one or more digital licenses;
receiving a request from a user to render protected digital content in a particular manner on the computing device;
determining if at least one of the one or more digital licenses stored in the license store corresponds to the protected digital content, wherein if none of the one or more digital licenses stored in the license store corresponds to the protected digital content, acquiring a corresponding digital license;
if at least one of the one or more digital licenses stored in the license store corresponds to the protected digital content, evaluating the corresponding digital license at least in part by performing a decryption function, the evaluation of the corresponding digital license comprising performing the steps of:
determining whether the corresponding digital license is valid;
reviewing license rules in the corresponding digital license, wherein the license rules specify a type of rendering permitted by the corresponding digital license; and
determining, based on the type of rendering permitted by the license rules and on the rendering in the information maintained in the state store, whether the requesting user is permitted to render the protected digital content in the requested particular manner, wherein the information maintained in the state store is updated with each evaluation of a digital license; and
if the requesting user is permitted to render the protected digital content in the requested particular manner, obtaining a decryption key from the corresponding digital license and decrypting the protected digital content using the decryption key.

35. Specifying rights in a digital rights license according to events

US9246916B2 | Microsoft Technology Licensing LLC

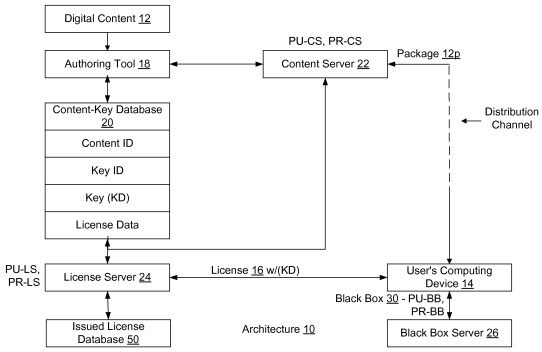
Bibliographic data

Publication date: 2016-01-26
Application date: 2009-09-28
Earliest priority date: 1999-03-27

Inventors: GANESAN KRISHNAMURTHY

CPC classification: G06F 21/10, G06F 2221/2107, H04L 2463/101, H04L 63/10
IPC classification: G06F 1/00, G06F 7/04, G06F 21/00, H04L 29/06, G06F 21/10

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

A digital license specifies rights with regard to corresponding digital content, and in particular specifies at least one event and for the at least one event at least one of a condition precedent to allowing the event to proceed and an action to be taken once the event has occurred. To respond to a request for an event from a rendering application with regard to the content, event code corresponding to the event is located in the license, and the condition within the event code is evaluated. If evaluated as true, the requested event is allowed to proceed, whereby the rendering application performs the event, and the action within the event code is executed. If evaluated as false, the requested event is denied.

First claim

A computer-readable storage device having stored thereon computer-executable instructions that when executed by a computing device implement a method of specifying rights with regard to digital content, the method comprising:
providing a digital license having license attributes or scripts specifying rights under the digital license with respect to associated digital content, said digital license including event code that sets forth a test for a condition that is a condition precedent that must occur prior to effectuating at least one specified event comprising at least one of storage of the license on a computer storage device, selection of the digital license for use in rendering the associated digital content, a request for a rendering-action with respect to the digital license during rendering of the associated digital content, a request to delete the digital license, and a detected clock rollback that is a presumed attempt to subvert a dateor time-based license term by rolling back a clock referred to by the digital license, and specifying for the at least one specified event an action to be taken with respect to license state information and/or the associated digital content once the specified event has occurred;
detecting the specified event; and
allowing the specified event to proceed if said condition precedent has occurred and/or taking said action once the specified event has occurred,
wherein detecting the request for the rendering-action with respect to the digital license during rendering of the associated digital content comprises detecting an action comprising modifying state information corresponding to at least one of the digital license and the associated digital content.

36. Usage rights management device

JP4170670B2 | Panasonic Corp, Matsushita Electric Industrial Co Ltd

Bibliographic data

Publication date: 2008-10-22
Application date: 2002-05-28
Earliest priority date: 2001-05-29

Inventors: 大穂 雅博, 上坂 靖, 山本 雅哉, 岡本 隆一, 徳田 克己, 井上 光啓

CPC classification:
IPC classification: G06F 15/00, G06Q 50/00, H04L 9/08, H04L 9/32, G06F 21/00, G06F 12/14, G06F 21/10, G06Q 30/06, G06Q 50/10, G06F 21/60, G06F 21/62, G06F 21/31

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

(57) [Summary] [Problem] To provide a usage right management device that can use content data on another device using its own usage right information. , Using the media identifier in the portable recording medium 101 of the contractor β, generates an issuance request for receiving permission to use the content data, and transmits the request to the usage right management device 71. Usage right management device 7 1 manages the usage right information of the content data given to the contractor β, and uses the usage right information and the issuance request to transmit the usage permission information for permitting the use of the content data to the portable recording medium 101. Generate. Further, the usage right management device 71 generates license information for controlling the use of the content data in the device connected to the portable recording medium 101 based on the usage permission information, and transmits the generated license information to the device 201. The device 201 processes the license information, Control use of content data.

First claim

A device for managing usage right information representing a right for a plurality of devices to use the same content data,
A user information database (hereinafter referred to as user information DB) in which device identifiers for uniquely identifying each of the plurality of devices belonging to a predetermined group are registered;
A usage right database (hereinafter referred to as a usage right DB) in which the usage right information in which content identifiers uniquely specifying content data and device identifiers of the plurality of devices are associated is registered for each content data;
An issuance request including the content identifier of the content data to be used and its own device identifier is received from the device, and authentication is performed as to whether or not the device identifier included in the received issuance request is registered in the user information DB. A user authentication unit to
The usage right DB is searched for the usage right information associated with the content identifier and the device identifier included in the issuance request authenticated as being registered in the user information DB by the user authentication unit. Use permission information indicating use permission for the content data to be used identified by the content identifier associated with the right information, and the use permission range is within the right range represented by the searched use right information A usage right management unit for generating permission information;
A license information generating unit that generates license information including at least the usage permission information generated by the usage right management unit;
Based on the device identifier included in the issuance request authenticated as being registered in the user information DB by the user authentication unit, the device that has transmitted the issuance request is identified. A communication unit that transmits the license information generated by the license information generation unit;
Input from a device whose device identifier is registered in the user information DB by a user who operates a registered identifier that is his / her device identifier and a device identifier that is unregistered in the user information DB When a temporary registration request including a registration target identifier is received , a temporary registration flag indicating that the registration target identifier is temporarily registered based on the registered

identifier and the registration target identifier included in the received temporary registration request And registering the registration target identifier in association with the registered identifier in the user information DB, temporarily registering the registration target identifier, and after temporary registration, from a device whose device identifier is not registered in the user information DB, A registration target identifier included in the temporary registration request and a registered identifier included in the temporary registration request and not registered. If the user operating the equipment has received the registration request including the registered identifier input, based on the registered identifier and registration target identifier included in the registration request the received, the registration in the user information DB A user information management unit for performing main registration of the registration target identifier temporarily registered in association with the registered identifier in the user information DB by deleting the temporary registration flag registered in association with the completed identifier. , Usage right management device.

37. INFORMATION PROCESSOR, INFORMATION PROCESSING METHOD, RECORDING MEDIUM, PROGRAM, AND FORMAT FOR RECORDING MEDIUM

JP2002297034A | Sony Corp

Bibliographic data

Publication date: 2002-10-09
Application date: 2001-03-29
Earliest priority date: 2001-03-29

Inventors: ISHIGURO RYUJI

CPC classification:
IPC classification: G11B 27/00, H04L 9/08, G10L 11/00, G11B 20/10, G11B 20/12, G09C 5/00, G09C 1/00, G10K 15/02

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

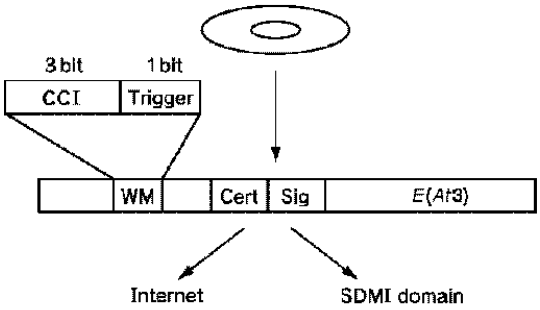


図24

Abstract

(57) [Summary] (With correction) [Problem] To enable a watermark to be detected quickly. SOLUTION: Since a watermark is extracted from a content and added to a header, it is possible to provide a content capable of quickly detecting a watermark. The watermark is It is composed of 3-bit copy management information (CCI) and a 1-bit trigger. Since the output of the content is controlled based on the detection result of the watermark detected from the header, it is possible to realize a format in which it can be quickly determined whether or not the content can be copied.

First claim

An information processing apparatus for outputting a content, comprising: an obtaining unit for obtaining the content to be output; an extracting unit for extracting a watermark added to the content obtained by the obtaining unit; Means for creating a header including the watermark extracted by the means, encryption means for encrypting the content acquired by the acquisition means, the header created by the header creation means, An information processing apparatus comprising: a formatting unit that formats the content encrypted by the encryption unit into a file format and outputs the file format.

38. Digital rights management system operating on computing device and having black box tied to computing device

US6772340B1 | Microsoft Corp

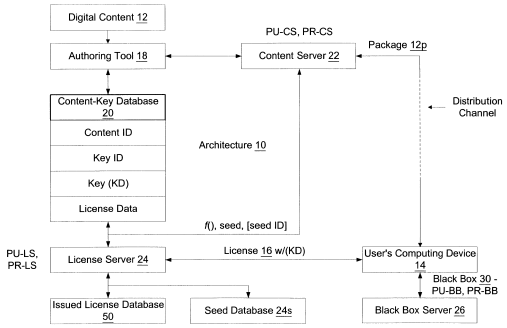
Bibliographic data

Publication date: 2004-08-03
Application date: 2000-03-15
Earliest priority date: 2000-01-14

Inventors: PEINADO MARCUS, LIU DONNA, GANESAN KRISHNAMURTHY

CPC classification: G06F 21/10, G06F 2221/2107
IPC classification: G06F 1/00, G06F 21/00

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

A digital rights management (DRM) system operates on a computing device when a user requests that an encrypted piece of digital content be rendered by the computer device. The computing device has an identifier. A black box performs decryption and encryption functions in the DRM system. The black box includes a key file and an executable. The key file includes at least one black box public key and is expected to include the identifier of the computing device, the black box thus being tied to the computing device by inclusion of such first identifier. A digital license corresponding to the digital content is resident in the DRM system and includes a decryption key for decrypting the encrypted digital content. The decryption key is expected to be encrypted according to a black box public key of the key file of the black box, the license thus being tied to the black box and by extension the computing device. If the identifier of the computing device is in fact different than the identifier in the key file of the black box, a different key file is produced based on the black box public key(s) of the key file and the different identifier of the computing device.

First claim

A digital rights management (DRM) system operating on a computing device when a user requests that an encrypted piece of digital content be rendered by the computer device, the computing device having an identifier, the DRM system comprising a black box for performing decryption and encryption functions in the DRM system, the black box containing a copy of the identifier of the computing device, the black box thus being tied to the computing device.

39. Supervised license acquisition in a digital rights management system on a computing device

US7065507B2 | Microsoft Corp

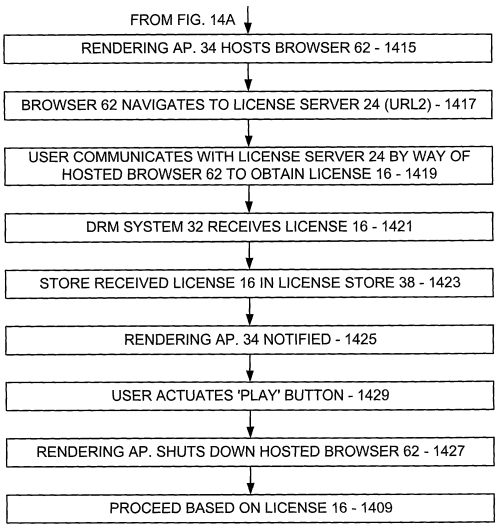
Bibliographic data

Publication date: 2006-06-20
Application date: 2001-03-26
Earliest priority date: 2001-03-26

Inventors: MOHAMMED SOHAIL BAIG, OLSON KIPLEY J, MCKUNE JEFFREY R, GANESAN KRISHNAMURTHY

CPC classification: G06F 21/10, G06F 2221/0737, G06F 2221/2137, G06Q 20/3829, G06Q 30/06
IPC classification: G06F 21/00, G06Q 30/06, G06Q 20/38

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

A rendering application on a computing device requests a digital rights management (DRM) system on the computing device to authorize digital content rendering based on a corresponding digital license. If unavailable, the DRM system attempts to silently acquire the license from a license server without the intervention of a user. In the course thereof, the rendering application receives status information from the DRM system relating to the attempted license acquisition thereby and displays the received status information in a rendering application status display portion. If silent acquisition fails, the rendering application hosts a browser, causes the browser to navigate to a license server, allows a user to communicate with the license server by way of the hosted browser to acquire the license, and shuts down the hosted browser upon reception of the license from the license server.

First claim

A method of acquiring a digital license that authorizes rendering of corresponding digital content, the digital license to be acquired upon a rendering application on a computing device requesting a digital rights management (DRM) system on the computing device for authorization for such rendering based on such digital license and upon the DRM system notifying the rendering application that such digital license is not available on the computing device, the method comprising:
hosting, by the rendering application, a browser that is initiated by the rendering application, under the control of such rendering application, and viewed within the context of the rendering application;
causing, by the rendering application, the browser to navigate to a license server;
allowing a user to communicate with the license server by way of the hosted browser to acquire the digital license;
receiving the digital license from the license server;
shutting down, by the hosting rendering application, the hosted browser upon receiving the digital license.

40. Content usage management system, server device and terminal device used therefor, content usage management method, license information transmission method, and content usage control method

JP4157535B2 | Panasonic Corp, Matsushita Electric Industrial Co Ltd

Bibliographic data

Publication date: 2008-10-01
Application date: 2005-03-24
Earliest priority date: 2001-06-07

Inventors: 岡本 隆一, 徳田 克己, 三浦 康史

CPC classification:
IPC classification: G06Q 50/00, G06F 13/00, H04N 7/167, H04N 7/173, G06Q 30/06, H04N 21/266, G06Q 50/10, H04N 21/835

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

PROBLEM TO BE SOLVED: To provide a content use management system in which a distribution server can reliably and optimally control the use of content on a user terminal and reduce the burden on the user terminal. User terminals 4a,..., 4n request the use condition management server 3 to use content (LT issue request) in accordance with a user instruction. The LT issue request includes expectation information (ELI). The usage condition management server 3 holds license information for each user, and based on a request from the user, the expected information included in the LT issue request includes a part or all of the usage conditions indicated by the license information corresponding to the user. The license ticket (LT) including the cut right information (UR-Uc) is generated according to (ELI), and transmitted to the user terminals 4a,. The user terminals 4a,..., 4n control the use of the content based on the received license ticket (LT) right information (UR-Uc). [Selection] FIG.

First claim

A content usage management system including a server device and a terminal device that acquires license information from the server device and performs content usage control according to the acquired license information,
The terminal device requests the server device to transmit the license information, and acquires license information acquisition means for acquiring the license information;
Based on the license information acquired by the license acquisition means, content usage control means for controlling the use of content,
The server device includes usage right management means for managing usage rights for content;
License information generating means for generating the license information in response to a transmission request for the license information from the terminal device;
License information transmitting means for transmitting the license information generated by the license information generating means to a terminal device requesting transmission of the license information;
The license information acquisition unit transmits terminal capability information related to a secure function of the terminal device when requesting the server device to transmit the license information.
The license information generating means generates license information based on the usage right managed by the usage right management means and terminal capability information related to a secure function transmitted from the terminal device ,
The license information includes immediate use instruction information for instructing whether or not the terminal device must use the license information immediately after obtaining the license information,
The terminal capability information includes information indicating whether or not the terminal device has a secure clock,
When the terminal capability information indicates that the terminal device does not have a secure clock, the license information generating means must use the immediate use instruction information included in the generated license information immediately. Set the information to instruct,
The content usage control means is the license information acquired by the license information acquisition means.

If the information indicating that the immediate use instruction information included in the information is to be used immediately is set, control is performed so that the license information is used immediately and the content is used. A feature content management system.

41. Reproduction device stopping reproduction of encrypted content data having encrypted region shorter than predetermined length

US7010809B2 | Sanyo Electric Co Ltd

Bibliographic data

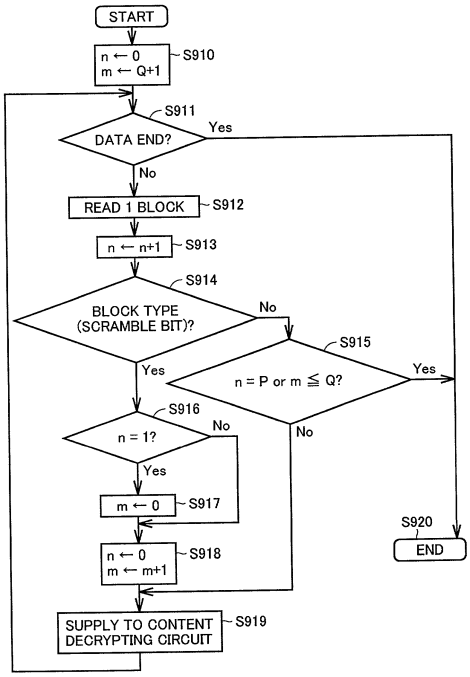
Publication date: 2006-03-07
Application date: 2001-09-10
Earliest priority date: 2001-03-13

Inventors: HORI YOSHIHIRO, YOSHIKAWA TAKATOSHI

CPC classification: G06F 21/10, G06F 21/78, G06F 2221/2107, H04N 2005/91364, H04N 21/41407, H04N 21/4184, H04N 21/44055, H04N 5/907, H04N 5/913, H04N 7/1675

IPC classification: G06F 11/30, H04L 9/00, H04N 5/00, H04L 9/32, G10L 19/00, G06F 12/14, H04N 7/167, G11B 20/10, H04L 9/12, H04N 5/907, H04N 5/913, G06F 21/10, H04N 21/418, H04N 21/4405, H04N 21/414, G06F 21/62, G10K 15/02

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

A controller of a reproduction terminal determines whether a block read from a memory card is an encrypted block or a non-encrypted block, and then applies the read block to a content decrypting circuit. The controller stops supplying the block to the content decrypting circuit when a predetermined number of non-encrypted blocks are continuously read from the memory card. Consequently, reproduction of the encrypted content data can be stopped if the encrypted content data includes a continuous non-encrypted portion in which the number of non-encrypted blocks is equal to or larger than a predetermined non-zero number.

First claim

A reproducing device for decrypting and reproducing encrypted content data divided into a plurality of blocks formed of an encrypted block including encrypted data and a non-encrypted block including non-encrypted data, comprising:
a decrypting circuit for detecting whether each of said plurality of blocks is said encrypted block or said non-encrypted block, and operating:
in the case of the encrypted block, to decrypt said encrypted data and output the resulting non-encrypted data: and
in the case of the non-encrypted block, to output said non-encrypted data from the non-encrypted block; and
a control circuit, wherein said control circuit receives a result of detection in said decrypting circuit, and stops supplying said block to said decrypting circuit when the number of the detected non-encrypted blocks in said content data is equal to or larger than a predetermined non-zero number.

42. Detecting and responding to a clock rollback in a digital rights management system on a computing device

US7134144B2 | Microsoft Corp

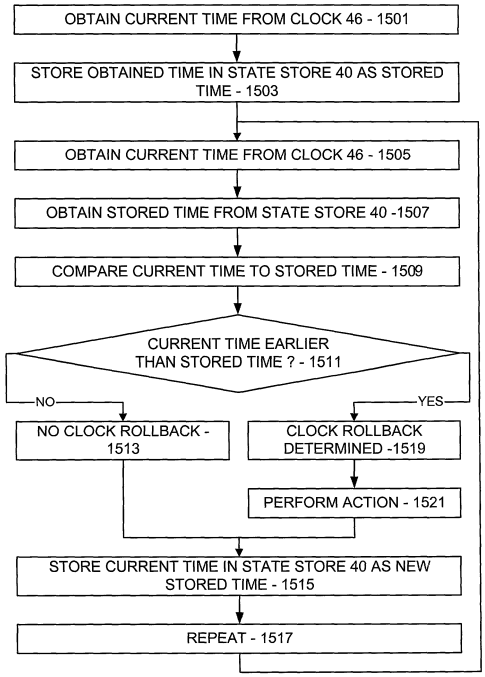
Bibliographic data

Publication date: 2006-11-07
Application date: 2001-03-01
Earliest priority date: 2001-03-01

Inventors: MCKUNE JEFFREY R

CPC classification: G06F 21/10
IPC classification: G06F 7/04, G06F 11/30, G06F 21/00, G06F 1/04

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

A rollback of a clock on a computing device is detected and responded to. A current time from the clock and a stored time from a secure store are obtained and compared to determine whether the obtained current time is earlier than the obtained stored time. If so, a predetermined course of action is taken based on the determination.

First claim

A method of detecting and responding to a rollback of a clock on a computing device to prevent misuse of digital content, the method comprising:
obtaining a current time from the clock;
obtaining a stored time from a secure store of the computing device, the secure store comprising a state store of a digital rights management system on the computing device;
comparing the obtained current time to the obtained stored time to determine whether the obtained current time is earlier than the obtained stored time;
determining that a clock rollback has occurred if the current time is earlier than the stored time, and taking a predetermined course of action based on the determination that the clock rollback has occurred,
the method performed in connection with the digital rights management system on the computing device for rendering digital content on the computing device in accordance with a corresponding digital license on the computing device, wherein taking a predetermined course of action based on the determination that the clock rollback has occurred comprises examining the corresponding digital license for event code corresponding to a determined clock rollback, and if present running the event code to prevent misuse of digital content.

43. Apparatus and system for providing fee-based content

US7099846B1 | Sony Corp

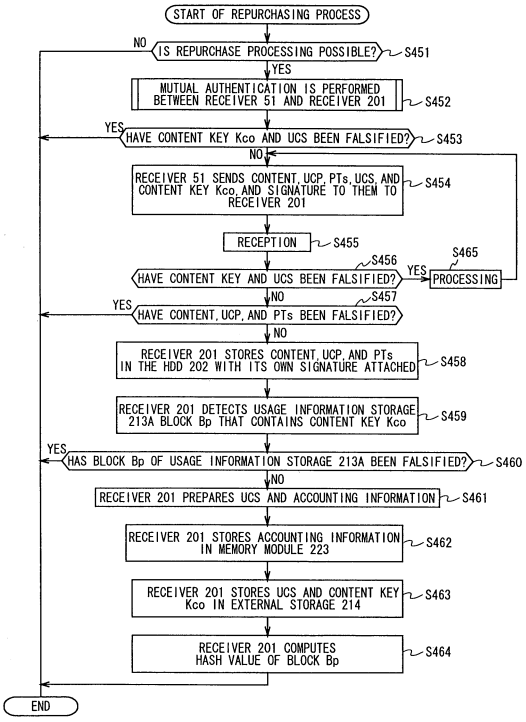
Bibliographic data

Publication date: 2006-08-29
Application date: 2001-02-12
Earliest priority date: 1999-04-09

Inventors: ISHIBASHI YOSHIHITO, MATSUYAMA SHINAKO, OISHI TATEO, MUTO AKIHIRO

CPC classification: G06Q 30/02, G06Q 30/06
IPC classification: G06Q 10/00, G06Q 50/00, H04L 9/08, H04L 9/00, H04L 9/32, G11B 20/10, G09C 1/00, G06F 21/10, G06Q 30/02, G06Q 30/06, G06Q 30/04, G06Q 50/10

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

A user who repeatedly purchases the same electronic content is entitled to receive a discount price for the additional purchases. This is accomplished by establishing an “Accounting History” of accounting information that is prepared when the electronic content is repurchased. The price of the repurchased electronic content is set to “Discount Price,” which is less than the original price at which the electronic content was purchased for the first time. Since accounts are settled based on the accounting information with “Accounting History” set to “Discount Price,” the user who is purchasing the same content again can buy it at a discount price.

First claim

An information processing system which includes a server and one or more information processing apparatuses and enables the information processing apparatuses to purchase rights to decrypt and use encrypted information, comprising:

first preparation means, located at the server, for preparing a first usage control status which identifies first usage details describing purchased rights and pricing details corresponding to said first usage details;

storage means for storing, located at the server, said encrypted information, said first usage control status, a usage control policy that contains a second use type that describes rights available for purchase at a subsequent time based on the first usage details of said purchased rights, price tags that contain pricing details corresponding to second usage details, and a key needed to decrypt said encrypted information; and

second preparation means, located at the server, for preparing a second usage control status that identifies said second usage details and pricing details corresponding to said second usage details, based on said usage control policy and said price tags, when rights are purchased again by said one or more information processing apparatuses;

wherein said encrypted information is accessed, at a first information processing apparatus, for a first pre-selected period of time, as a function of said purchased rights and usage control policy,

wherein said encrypted information is accessed, by a second information processing apparatus, using second rights, for a second pre-selected period of time, wherein the second information processing apparatus accesses said encrypted information independent of a connection to the first information processing apparatus,

wherein the first usage control status and the second usage control status includes at least system registration information; and

wherein the system registration information includes at least an equipment number, a settlement number, account-settling user information, subordinate user information, and use point information.

44. Content provision device and method and license server capable of facilitating circulation of encrypted content data

US20020138442A1 | Sanyo Electric Co Ltd

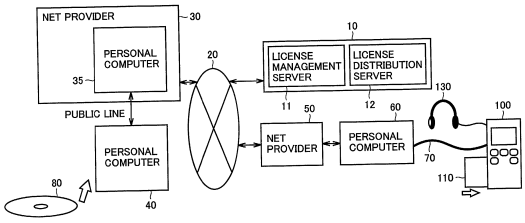
Bibliographic data

Publication date: 2002-09-26
Application date: 2001-09-12
Earliest priority date: 2001-03-26

Inventors: HORI YOSHIHIRO, HIOKI TOSHIAKI

CPC classification: G06F 21/10
IPC classification: G06Q 10/00, G06Q 50/00, H04L 9/08, H04N 7/167, H04N 7/173, G06F 21/10, H04N 21/418, G06Q 30/06, H04N 21/266, G06Q 50/10, H04N 21/4623

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

A personal computer obtains music data and identification information of the music data from a CD and transmits the identification information to a license management server on the Internet. The personal computer receives an encryption key and additional information of the music data from the license management server. The personal computer encodes the music data in an MP3 system to generate content data and encrypts the content data with an encryption key to generate encrypted content data, and uploads the encrypted content data to the personal computer together with the additional information. Thus, while copyright can be protected, encrypted content data can be generated and provided to a site allowing each user to obtain the same.

First claim

A content provision device obtaining content data and using an encryption key to encrypt said content data to provide encrypted content data, comprising:
an interface controlling communication with a recording medium having said content data recorded therein;
a transmission and reception unit allowing external communication;
an encryption unit using said encryption key to encrypt said content data to generate said encrypted content data; and
a control unit obtaining said content data and identification information of said content data from said recording medium through said interface, transmitting said identification information via said transmission and reception unit to a license management server holding said encryption key, receiving said encryption key from said license management server via said transmission and reception unit, providing to said encryption unit said content data and said encryption key received, and providing externally via said transmission and reception unit said encrypted content data generated by said encryption unit.

45. Information recording device and information reproducting device

US6772133B1 | Toshiba Corp

Bibliographic data

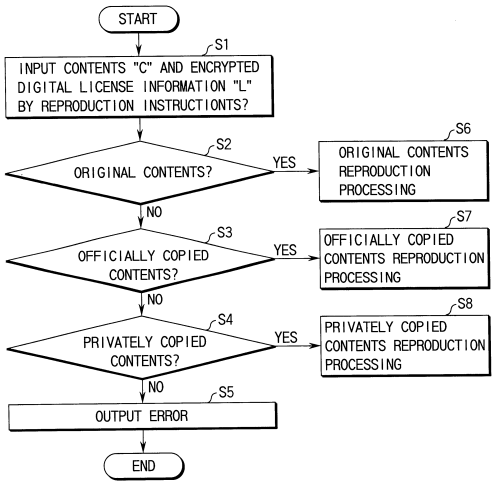
Publication date: 2004-08-03
Application date: 2000-03-03
Earliest priority date: 1999-03-05

Inventors: KAMBAYASHI TORU, AKIYAMA KOICHIRO, HANDA YUTAKA, OHMORI YOSHIHIRO

CPC classification: G06Q 30/06, G11B 20/00115, G11B 20/00173, G11B 20/00181, G11B 20/0021, G11B 20/00224, G11B 20/00347, G11B 20/00514, G11B 20/00557, G11B 20/0071, G11B 20/00753, G11B 20/00797, G11B 20/0084, G11B 20/00847, G11B 20/00884, G11B 20/02, G11B 20/10

IPC classification: G11B 20/00, G06F 12/14, G11B 20/10, G06F 3/06, G06F 21/10, G11B 20/02, G06Q 30/06, G06F 21/62

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

The information reproduction device for reproducing contents information based on license information added to the contents information and required for reproducing the contents information, includes a determining section for determining whether encrypted contents information is the officially copied contents information or privately copied contents information based on the contents of the license information, and a reproduction section configured to reproduce the contents information determined as the privately copied contents information by the determining section under more severe restriction than the officially copied contents information. Thus, the contents copied by the proper route (officially copied contents) can be distributed in a more advantageous form than the contents copied without proper authorization.

First claim

An information reproduction device comprising:
a contents inputting unit configured to receive contents information and license information, the license information including first information indicating whether the contents information is officially copied contents information which is copied under a right for selling the contents information or privately copied contents information which is copied without a right for selling the contents information;
a determining unit configured to determine whether the contents information is the officially copied contents information or the privately copied contents information based on the first information of the license information; and
a reproducing unit configured to reproduce the contents information based on a determination by the determining unit, the reproducing unit reproducing the officially copied contents information by using one of a first digital reproduction device, a second digital reproduction device of which quality is lower than a quality of the first digital reproduction device, and an analog reproduction device and reproduces the privately copied contents information by using one of the second digital reproduction device and the analog reproduction device.

46. Protecting decrypted compressed content and decrypted decompressed content at a digital rights management client

US7239708B2 | Microsoft Corp

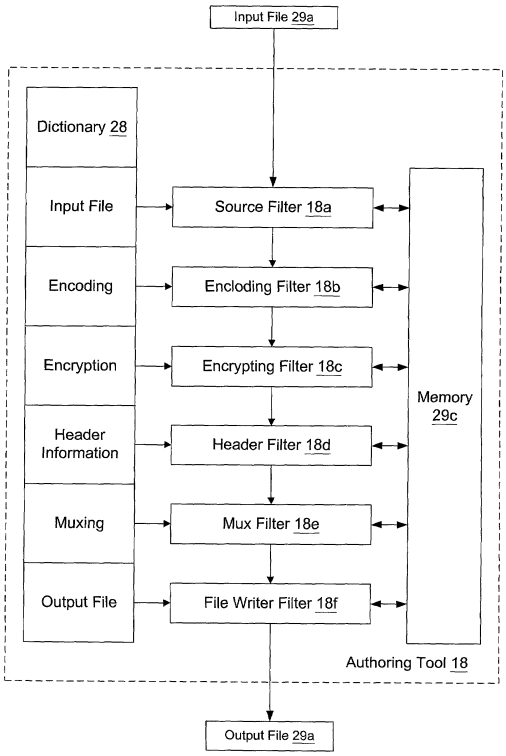
Bibliographic data

Publication date: 2007-07-03
Application date: 2001-06-27
Earliest priority date: 2001-06-27

Inventors: ENGLAND PAUL, PEINADO MARCUS, SANKARANARAYAN MUKUND

CPC classification: G06F 21/10, G06F 2221/0737, G06F 2221/0797, G06F 2221/2137, G11B 20/00007, G11B 20/0021
IPC classification: H04K 1/00, G11B 20/00, G06F 21/00

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

Encrypted compressed content is produced by encrypting content based at least in part on a content key, and compressing the content based at least in part on the content key. Thus, the content key is employed to encrypt the content and also to compress the content. Similarly, decrypted decompressed content is produced from the encrypted compressed content by decrypting the content based at least in part on a content key, and decompressing the content based at least in part on the content key. Thus, the content key is employed to decrypt the content and also to decompress the content.

First claim

A computer system for receiving encrypted compressed content and for producing decrypted decompressed content based on the received encrypted compressed content, the system comprising:
a decryption element for developing a content key and for decrypting the content based at least in part on the developed content key; and
a decompression element for decompressing the content based at least in part on the content key, the decryption element supplying the content key to the decompression element,
wherein the content key is employed to decrypt the content and also to decompress the content,
wherein the decompression element has a plurality of adjustable parameters and wherein the decompression element employs the content key as at least one of the adjustable parameters,
wherein the decompression element includes a quantizer for performing a lossy quantization step, and wherein the quantizer is de-dithered according to the content key,
wherein the decompression element includes an internal representation that includes DCT coefficients of macroblocks, and wherein such coefficients are de-scrambled and de-noised according to the content key, and
wherein the decryption element and the decompression element are closely physically related to one another so as to protect the content key as supplied by the decryption element to the decompression element, such close physical relationship comprising one of the decompression element residing in a process address space of the decryption element on the computer system and the decryption element residing in a process address space of the decompression element on the computer system.

47. DEVICE AND METHOD FOR PROCESSING INFORMATION, RECORDING MEDIUM AND PROGRAM

JP2002297032A | Sony Corp

Bibliographic data

Publication date: 2002-10-09
Application date: 2001-03-29
Earliest priority date: 2001-03-29

Inventors: ISHIGURO RYUJI

CPC classification:
IPC classification: G06F 15/00, H04L 9/08, H04L 9/32, G06F 21/00, G06F 12/14, G06F 21/24, G09C 1/00

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

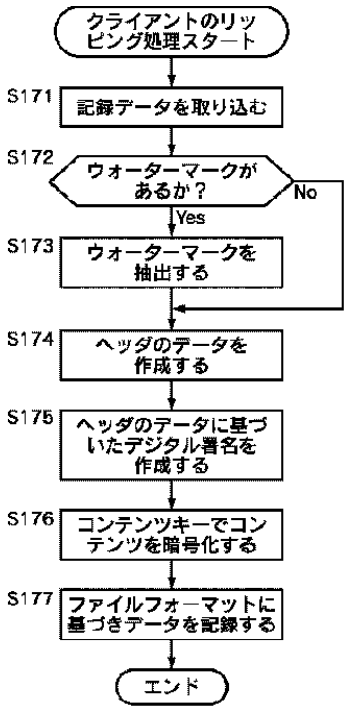


図23

Abstract

PROBLEM TO BE SOLVED: To prevent circulation of contents which have been copied illegally by enabling the author of the contents so as to very by the contents. SOLUTION: When a watermark exists in the data fetched by a step S171, the watermark is extracted in a step S173, and the watermark is added to a header in a step S174. A digital signature, based on the header is generated in a step S175 using a secret key of a user, and the key is recorded in a file format in a step S177.

First claim

An information processing apparatus for outputting a content, an acquisition unit for acquiring the content to be output, a header creation unit for creating a header of the content acquired by the acquisition unit, and a header created by the header creation unit Signature creation means for creating a digital signature based on the data of the header, encryption means for encrypting the content acquired by the acquisition means, the header created by the header creation means, An information processing apparatus comprising: a formatter that formats the content encrypted by the encryptor into a file format and outputs the file format.

48. Specifying security for an element by assigning a scaled value representative of the relative security thereof

US20050097368A1 | Microsoft Corp

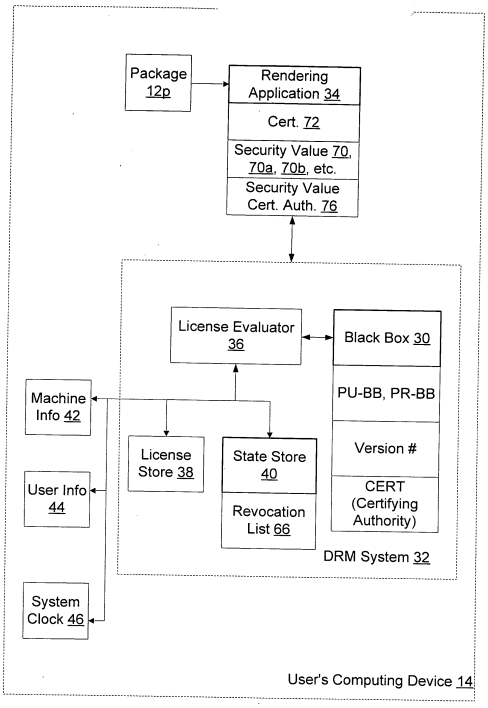
Bibliographic data

Publication date: 2005-05-05
Application date: 2004-11-05
Earliest priority date: 2000-01-14

Inventors: PEINADO MARCUS, ABBURI RAJASEKHAR, BELL JEFFREY R

CPC classification: G06F 21/10, G06F 2221/2107
IPC classification: G06F 1/00, G06F 21/00

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

To determine whether digital content can be released to an element such as a computer application or module, a scaled value representative of the relative security of the element is associated therewith, and the digital content has a corresponding digital license setting forth a security requirement. The security requirement is obtained from the digital license and the scaled value is obtained from the element, and the scaled value of the element is compared to the security requirement of the digital license to determine whether the scaled value satisfies the security requirement. The digital content is not released to the element if the scaled value does not satisfy the security requirement.

First claim

A computer-readable medium having computer-executable instructions for determining whether digital content can be released to a computer-type operational element, a scaled numerical value representative of the relative security of the element being associated therewith, the scaled numerical value being selected from a number scale, the digital content having a corresponding digital license setting forth a security requirement specifying a minimum value, the computer-executable instructions performing:
obtaining the minimum value of the security requirement from the digital license;
obtaining from the element the scaled numerical value; and
comparing the scaled numerical value of the element to the minimum value of the security requirement of the digital license to determine whether the scaled numerical value satisfies the security requirement, wherein the digital content is not released to the element if the scaled numerical value does not satisfy the minimum value of the security requirement.

49. Digital content usage control method and system

JP3606148B2 | NEC Corp

Bibliographic data

Publication date: 2005-01-05
Application date: 2000-01-06
Earliest priority date: 2000-01-06

Inventors: 中江 政行

CPC classification:
IPC classification: G06F 15/00, G06F 12/00, G06F 21/00, G06F 12/14, H04L 9/14, G06F 21/24

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

(57) [Summary] [PROBLEMS] For digital content in which individual component data in content such as images and texts is encrypted with different keys, the definition of a set of components to be controlled can be changed even after distribution of the content. I do. SOLUTION: Property information defining a set of element data constituting the content is added to the encapsulated digital content in advance, and a use condition description describing a use permission code for each of the component sets is used as a use permission server. Register in 1. First, property information is updated from the use permission server 1 to the playback device 2 that uses the content, and a use certificate including a use permission code is distributed. After that, the playback device 2 acquires the decryption key of the component data included in the component set from the use permission server 1 in exchange for the use permission code.

First claim

A digital content use control method for controlling the use of digital content in a system in which a playback device and a use permission server are connected via a network,
The digital content includes a plurality of component data encrypted with different encryption keys,
The usage permission server manages each component data of the digital content divided into a plurality of component sets and manages a use permission code for each component set and a decryption key for each component data, When a usage permit request designating a request condition including a set of components to be played back and a usage method is sent from the playback device, if the usage method in the request condition is permitted, the specified A usage certificate including a usage code corresponding to the component set is sent to the playback device;
When the usage certificate is sent from the usage authorization server, the playback device sends a decryption key sequence request including the usage authorization code in the usage license to the usage authorization server,
When the decryption key sequence request is sent from the playback device, the use permission server performs authentication based on the use permission code in the decryption key sequence request and the use permission code managed by the own server Then, a digital content usage control method, wherein a decryption key for each component data included in the component set corresponding to the use permission code is sent to the playback device.

50. Specifying security for an element by assigning a scaled value representative of the relative security thereof

US6829708B1 | Microsoft Corp

Bibliographic data

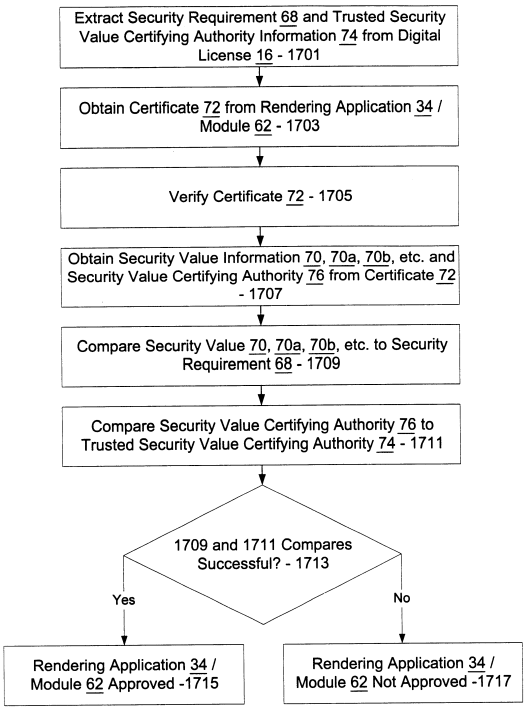
Publication date: 2004-12-07
Application date: 2000-03-15
Earliest priority date: 1999-03-27

Inventors: PEINADO MARCUS, ABBURI RAJASEKHAR, BELL JEFFREY R C

CPC classification: G06F 21/10, G06F 21/71, G06F 21/84, G06F 2211/007, G06F 2221/0797, G06F 2221/2105, G06F 2221/2107, G06F 2221/2137, G06Q 30/06, G07F 9/002, H04L 2463/101, H04L 63/0442, H04L 63/068, H04L 63/0823, H04L 63/12

IPC classification: G06F 1/00, G06F 21/00, H04L 29/06, G06Q 30/06

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

To determine whether digital content can be released to an element such as a computer application or module, a scaled value representative of the relative security of the element is associated therewith, and the digital content has a corresponding digital license setting forth a security requirement. The security requirement is obtained from the digital license and the scaled value is obtained from the element, and the scaled value of the element is compared to the security requirement of the digital license to determine whether the scaled value satisfies the security requirement. The digital content is not released to the element if the scaled value does not satisfy the security requirement.

First claim

A method of specifying security for a computer-type operational element, the method comprising:
assigning a scaled numerical value representative of the relative security of the element, the scaled numerical value being selected from a number scale with a first value indicative of an element that has been deemed not secure, and with a second value indicative of an element that has been deemed highly secure;
associating the scaled value with the element,
wherein a determination of whether digital content can be released to the element is made based on the assigned and associated scaled value numerical thereof.

51. Data terminal equipment

JP4554801B2 | Fujitsu Ltd, PFU Ltd, Sanyo Electric Co Ltd, Renesas Electronics Corp

Bibliographic data

Publication date: 2010-09-29
Application date: 2000-11-29
Earliest priority date: 2000-11-29

Inventors: 堀 吉宏, 上村 透, 畠山 卓久, 高橋 政孝, 常広 隆司, 大森 良夫

CPC classification:
IPC classification: H04L 9/08, H04L 9/32, G10L 11/00, G06F 13/00, G06F 12/14, G06F 21/24, G09C 1/00, G10K 15/02

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

(57) [Summary] [Problem] To provide a data terminal device for acquiring a license for reproducing encrypted content data when acquiring the encrypted content data from a recording medium. SOLUTION: The personal computer is a CD-RO. M to encrypted content data, content file 6 01 to 60n and the server information file are copied to the hard disk 530, and a request for distribution of the license of the encrypted content data is made to the distribution server based on the access means and the access destination address included in the server information file, and the license is received. . Then, the received license is stored in the license area 5215B of the memory of the built-in license management device 520.

First claim

The encrypted content data is obtained from a recording medium including a plurality of encrypted content data and a server information file necessary for obtaining a license for reproducing the plurality of encrypted content data, and based on the server information file A data terminal device for obtaining the license from a distribution server,
A medium driving unit that acquires encrypted content data specified by a user from a plurality of encrypted content data recorded on the recording medium and the server information file from the recording medium;
In accordance with the contents of the server information file acquired by the medium driving unit, a connection unit with the distribution server is determined to acquire a license for reproducing the encrypted content data designated by the user, and the determination A controller that connects to the distribution server by the connecting means to request distribution of the license, and receives the license from the distribution server;
A storage unit for storing encrypted content data acquired by the medium driving unit;
A data terminal device comprising a device unit for storing a license received from the distribution server.

52. Encrypting a digital object on a key ID selected therefor

US7412061B2 | Microsoft Corp

Bibliographic data

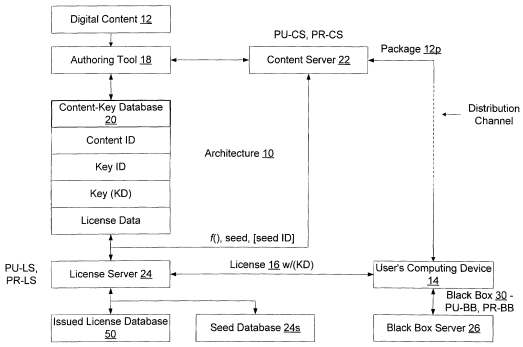
Publication date: 2008-08-12
Application date: 2004-11-05
Earliest priority date: 1999-03-27

Inventors: PEINADO MARCUS, VENKATESAN RAMARATHNAM

CPC classification: G06F 21/10, G06F 21/71, G06F 21/84, G06F 2211/007, G06F 2221/0797, G06F 2221/2105, G06F 2221/2107, G06F 2221/2137, G06Q 30/06, G07F 9/002, H04L 2209/603, H04L 2463/101, H04L 63/0442, H04L 63/068, H04L 63/0823, H04L 63/12, H04L 9/083, H04L 9/0869

IPC classification: G06F 1/00, H04L 9/00, G06F 21/00, H04L 29/06, H04L 9/30, G06Q 30/06

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

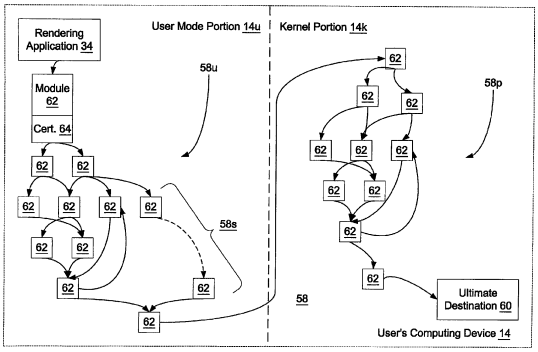
To encrypt a digital object, a key ID is selected for the digital object, and a function $f( )$ having an input and an output is selected. The selected key ID is then employed as the input to the function $f( )$, and the output of such function $f( )$ is employed as the key (KD) for the digital object: f(key ID) key (KD). The digital object is then according to such key (KD), and the encrypted digital object is distributed.

First claim

A computer-readable medium having computer-executable instructions for producing a key (KD) for decrypting a digital object, the digital object having been encrypted by:
selecting a key ID for the digital object;
selecting a function $f( )$ having an input and an output;
employing the selected key ID as the input to the function $f( )$;
employing the output of such function $f( )$ as the key (KD) for the digital object:
f(key ID)key (KD),
encrypting such digital object according to such key (KD); and
distributing such encrypted digital object, along with the key ID, the computer-readable medium comprising instructions for:
receiving a request for the key (KD) from a requestor, the request including the key ID;
approving the request;
employing the included key ID as the input to the function $f( )$;
employing the output of such function $f( )$ as the requested key (KD):
f(key ID)key (KD); and
distributing such key (KD) to the requestor.

53. Releasing decrypted digital content to an authenticated path

US8744969B2 | Microsoft Corp



Bibliographic data

Publication date: 2014-06-03
Application date: 2007-10-02
Earliest priority date: 2000-01-14

Inventors: PEINADO MARCUS, ENGLAND PAUL, YERRACE FRANK

CPC classification: G06F 21/10, G06F 2221/2107
IPC classification: G06F 1/00, G06F 21/00

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

Digital content is released to a rendering application for forwarding by such rendering application to an ultimate destination by way of a path therebetween. The path is defined by at least one module, and the digital content is initially in an encrypted form. An authentication of at least a portion of the path is performed to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing therethrough. The encrypted digital content is decrypted if in fact each such defining module is to be trusted, and the decrypted digital content is forwarded to the rendering application for further forwarding to the ultimate destination by way of the authenticated path.

First claim

A system comprising:
a processor;
a memory storing executable instructions that when executed by the processor causes the processor to perform the method steps of:
forwarding digital content from a rendering application to a destination, and
defining a path between said rendering application and said destination, said path being defined by at least one module; and
a digital rights management system including a black box that releases encrypted digital content to said rendering application for distribution to said destination by way of said path, said black box comprising a black box processor and a memory storing executable instructions that when executed by the black box processor causes the black box processor to perform an authentication of at least a portion of the path to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing therethrough, wherein said black box processor performs the authentication by performing the steps of:
traversing the at least a portion of the path to develop a map of each module in the path,
authenticating each module in the map, and
for each module in the at least a portion of the path, receiving from the module a certificate as issued by a certifying authority, determining from the received certificate whether such received certificate is acceptable for purposes of authenticating the module, checking a revocation list to ensure that the received certificate has not been revoked, and refusing to decrypt the encrypted digital content if at least one module in the at least a portion of the path fails to provide an acceptable certificate,
said black box decrypting the encrypted digital content if in fact each such defining module is to be trusted and forwarding the decrypted digital content to the rendering application for further forwarding to the destination by way of the authenticated path.

54. Secure video card in computing device having digital rights management (DRM) system

US20020012432A1 | Microsoft Corp

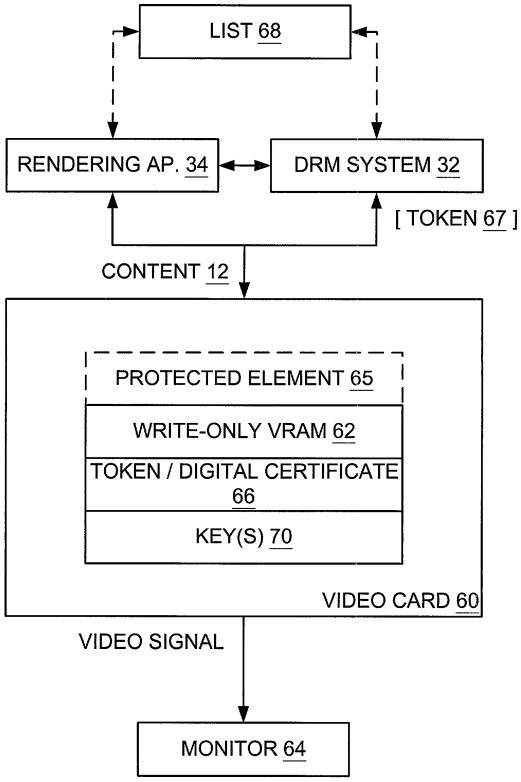
Bibliographic data

Publication date: 2002-01-31
Application date: 2001-06-28
Earliest priority date: 1999-03-27

Inventors: ENGLAND PAUL, PEINADO MARCUS, SANKARANARAYAN MUKUND

CPC classification: G06F 21/71, G06F 21/84, G06F 2221/2105, H04L 2463/101, H04L 63/0442, H04L 63/068, H04L 63/0823, H04L 63/12
IPC classification: G06F 21/00, H04L 29/06, G06F 12/14, G06F 21/24

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

A computing device includes a digital rights management (DRM) system thereon for allowing rendering of protected digital content on the computing device. The content includes video content to be displayed on a monitor coupled to the computing device. The computing device also includes a video section therein for receiving the content and for producing a video signal to be sent to the monitor based on the received content. The video section includes video memory for storing the received content, and the video memory is configured to be write-only except with regard to the video section. The video section further includes an authentication device for authenticating to the DRM system that the video memory is configured to be write-only except with regard to the video section.

First claim

A computing device including a system thereon for allowing rendering of protected digital content on the computing device, the content including a type of content to be rendered on a corresponding rendering device coupled to the computing device, the computing device also including a section therein for receiving the type of content in a non-protected form, the section including memory for storing the received content, the memory being configured to be write-only except with regard to the section.

55. INFORMATION PROCESSING APPARATUS, INFORMATION PROCESSING METHOD, RECORDING MEDIUM, AND PROGRAM

JP2006320018A | Sony Corp

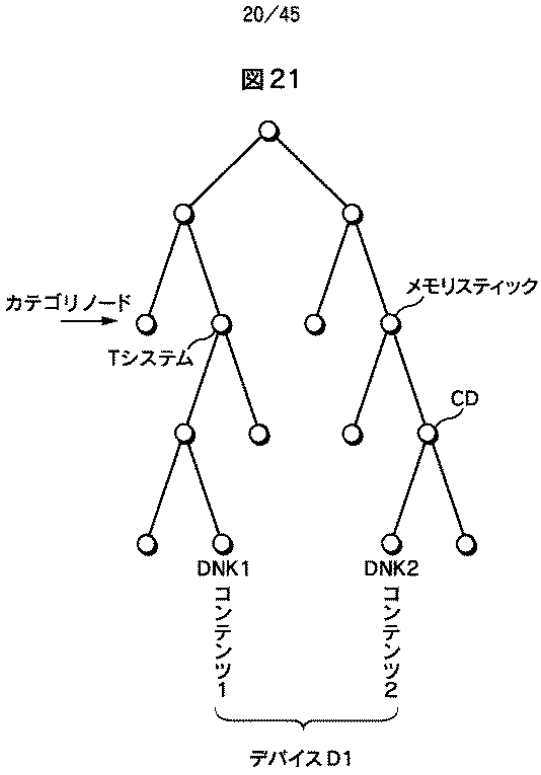
Bibliographic data

Publication date: 2006-11-24
Application date: 2006-07-27
Earliest priority date: 2001-03-29

Inventors: ISHIGURO RYUJI

CPC classification:
IPC classification: G06Q 50/00, H04L 9/08, G06Q 30/06, G06Q 50/10

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

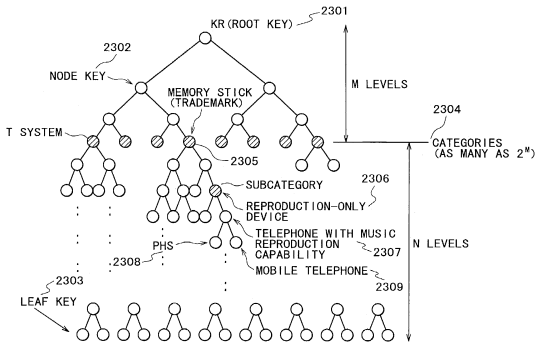
PROBLEM TO BE SOLVED: To utilize contents that belong to different categories, using a single device. SOLUTION: A category node in a node within a tree structure is associated with a T system and a predetermined device (e.g. memory stick). A device node key (DNK1), corresponding to a content associated with a node under the T system and a device node key (DNK2) that correspond to the content associated with a node under the memory stick, are allowed to be handled simultaneously and by the identical device. COPYRIGHT: (C)2007,JPO&INPIT

First claim

An information processing apparatus that provides a key for decrypting encrypted content to the other information processing apparatus based on access from the other information processing apparatus,
Receiving means for receiving a key request from the other information processing apparatus;
Generating means for assigning the other information processing apparatus to a leaf of a key management hierarchical tree structure and generating a device node key;
An information processing apparatus comprising: transmission means for transmitting the device node key generated by the generation means to the other information processing apparatus.

56. Information processing apparatus

US7336791B2 | Sony Corp



Bibliographic data

Publication date: 2008-02-26
Application date: 2003-04-28
Earliest priority date: 2001-03-29

Inventors: ISHIGURO RYUJI

CPC classification: G11B 20/00181, G11B 20/0021, G11B 20/00507, G11B 20/00731, G11B 20/00884, H04L 2209/60, H04L 9/0836, H04N 21/2541, H04N 21/2543, H04N 21/25875, H04N 21/4753, H04N 21/63345, H04N 21/6581, H04N 21/835, H04N 7/1675

IPC classification: G11B 20/00, H04L 9/08, H04L 9/00, H04L 9/30, H04N 7/167, H04L 9/20, H04N 7/24, H04N 21/2543, H04N 21/254

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

Upon receipt of a service data request from a client, a license server offering a key to decrypt a content transmits a user information request to the client. On receiving the user information request, the client displays a message prompting its user to enter such user information as the user's personal information and accounting information. The user information thus entered is sent from the client to the license server. On receiving the user information, the license server assigns a leaf of a key-managed hierarchical tree structure to the client, generates a set of node keys as a device node key, sends to the client the device node key together with a leaf ID and a private key of the client in question, and records the user information in correspondence with the leaf ID.

First claim

An information processing apparatus for providing a second information processing apparatus with a key to decrypt an encrypted content when said information processing apparatus is accessed by said second information processing apparatus, said information processing apparatus comprising:
receiving means adapted to receive a key request and a license request for using content from said second information processing apparatus;
key generating means adapted to generate a device node key by assigning said second information processing apparatus to a leaf of a key-managed hierarchical tree structure according to the received key request;
license generating means adapted to generate a license including leaf identification information and content use condition according to the received license request; and
transmitting means adapted to transmit to said second information processing apparatus said device node key generated by said key generating means and the leaf identification information for identifying the leaf assigned to said second information processing apparatus, and to transmit said license to said second information processing apparatus;
wherein the device node key is provided to said second information processing apparatus to decrypt an encrypted key set provided with the encrypted content data.

57. Information processing apparatus for watermarking digital content

US7216368B2 | Sony Corp

Bibliographic data

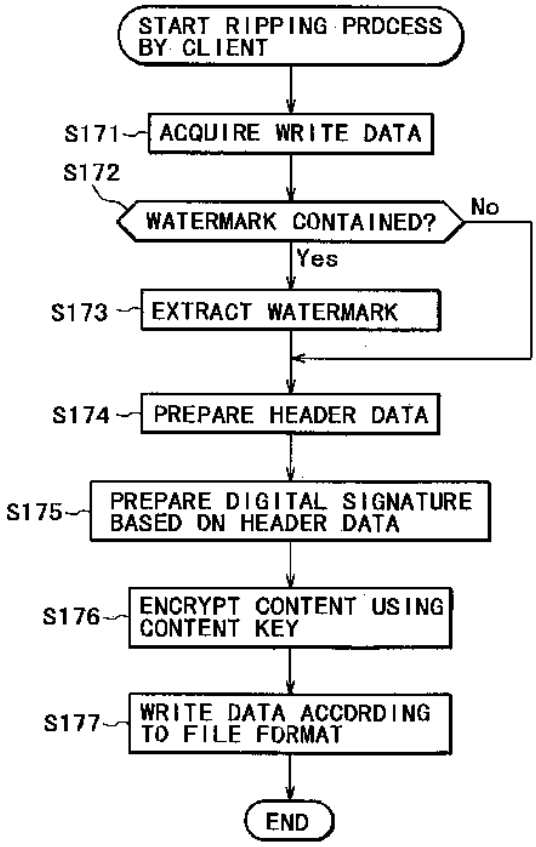
Publication date: 2007-05-08
Application date: 2003-05-21
Earliest priority date: 2001-03-29

Inventors: ISHIGURO RYUJI

CPC classification: G06F 17/00, G06F 21/10, G06F 2221/0706, G06F 2221/0755, G06T 1/0021, G06T 2201/0064, G11B 20/00144, G11B 20/00152, G11B 20/0021, G11B 20/00333, G11B 20/00507, G11B 20/0071, G11B 20/00753, G11B 20/0084, G11B 20/00855, G11B 20/00884, H04L 2209/56, H04L 2209/608, H04L 9/0836, H04L 9/3247, H04L 9/3263

IPC classification: G06Q 10/00, G06F 7/04, G06Q 50/00, G06T 1/00, G11B 20/00, H04L 9/00, G06Q 99/00, H04N 7/173, G06F 21/10, H04N 21/2347, G06Q 30/06, G06Q 50/10, G06Q 50/26, H04N 21/21, H04N 21/835, G06F 21/60, G06F 21/64, G06F 21/62

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

This invention relates to an information processing apparatus for managing copyrights under SDMI provisions as well as the copyrights for contents distributed over the Internet. Data Enc(Kc, Content) generated by encrypting a given content using a content key Kc are recorded, along with a header (Header), certificate (Cert), data Enc(KR, Kc) generated by encrypting the content key Kc using a root key KR, and an enabling key block (EKB). The header includes a content ID (CID), a license ID (LID), a URL, and a watermark (WM), supplemented with a header signature Sig(Header). The inventive apparatus is applied to devices that provide contents.

First claim

An information processing apparatus for providing content, said apparatus comprising:
content acquiring means for acquiring data that includes the content and an embedded watermark;
extracting means for extracting the embedded watermark from the acquired data;
header preparing means for preparing a header that is appended to the content and placing the extracted watermark into the header;
digital signature preparing means for preparing, using a private key, a digital signature based on data in the header;
encrypting means for encrypting the content;
key information acquiring means for acquiring key information that includes key information needed to decrypt the encrypted content; and
formatting means for formatting the header, the digital signature, the encrypted content, and the acquired key information according to a file format before being outputted.

58. DATA REPRODUCING DEVICE AND LICENSE MANAGING METHOD

JP2002099743A | Sanyo Electric Co Ltd

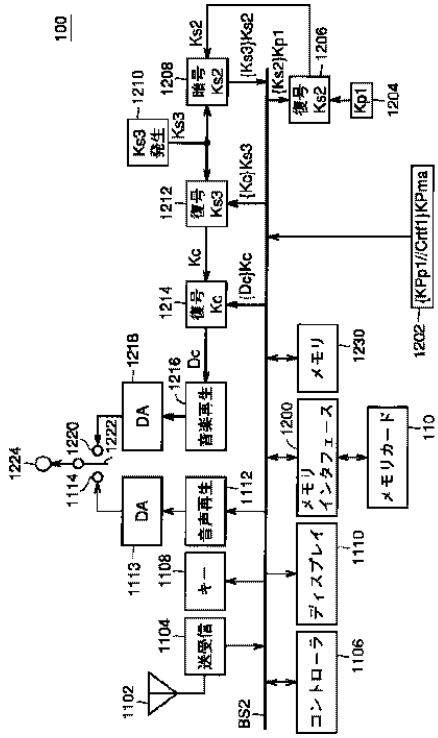
Bibliographic data

Publication date: 2002-04-05
Application date: 2000-09-22
Earliest priority date: 2000-09-22

Inventors: MORIAI SHINSUKE

CPC classification:
IPC classification: G06Q 10/00, G06Q 50/00, G09C 1/00, G06F 21/10, G06Q 30/06, G06Q 50/10, G10K 15/02

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

PROBLEM TO BE SOLVED: To provide a data reproducing device and a license managing method with a procedure where the selection of music and the management of contents are simplified. SOLUTION: A portable telephone set 100 includes a controller 1106, a display 1110, a key operation part 1108, a memory 1230, a memory card 110 and a reproduction system circuit. In a music reproducing mode, information (reproduced music list) on reproducible contents data is displayed on the display 1110 based on an inter-media music list recorded in the memory card 110. A user selects music from pertinent display. In a media managing mode, compiling work is possible corresponding to the inter-media music list showing the data contents recorded in the memory card 110.

First claim

An encrypted content data obtained by encrypting content data and license information relating to the encrypted content data are downloaded and recorded in a data recording device, and the encrypted content data recorded in the data recording device is downloaded. A data reproducing apparatus for reproducing data, comprising: a communication unit for performing external communication; an interface for controlling data transfer; a control unit; and a display unit, wherein the control unit is capable of reproducing at the time of the reproduction. A data reproducing device that displays a content list related to the encrypted content data on the display unit.

59. Data terminal device and control method of data terminal device

JP4601153B2 | Fujitsu Ltd, PFU Ltd, Sanyo Electric Co Ltd, Renesas Electronics Corp

Bibliographic data

Publication date: 2010-12-22
Application date: 2000-11-29
Earliest priority date: 2000-11-29

Inventors: 堀 吉宏, 上村 透, 畠山 卓久, 高橋 政孝, 常広 隆司, 大森 良夫

CPC classification:
IPC classification: H04L 9/08, H04L 9/32, G06F 13/00, G06F 12/14, G06F 21/24, G09C 1/00, G10K 15/02

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

(57) [Summary] [PROBLEMS] To provide a data terminal device capable of moving encrypted content data and a license delivered by software to another data terminal device. A hard disk of a personal computer has a content list file and an encrypted confidential file. The license management device 520 stores the binding key Kb in the license area 5215B of the memory. Encrypted confidential file 16 0 can be decrypted and encrypted with the binding key Kb stored in the license management device 520. Then, the license of the obtained encrypted content data is stored as confidential information in the encrypted confidential file 160.

First claim

Encrypted content data obtained by encrypting content data and data for obtaining the original plaintext by decrypting the encrypted content data and outputting the encrypted content data and the license to another data terminal device
A terminal device,
A module unit for acquiring the encrypted content data and the license by software;
A storage unit for storing the encrypted content data, the license management file, and the encrypted confidential file;
A device unit for decrypting the encrypted confidential file and storing a binding license including a binding key for encrypting the decrypted confidential file in a dedicated area;
The confidential file includes confidential information including the license as a component,
The license management file, in correspondence with the encrypted content data, and, viewed contains a management number of the confidential information contained in the confidential file,
When initializing the encrypted confidential file,
The module unit generates the binding license including the binding key, generates a confidential file with empty confidential information, encrypts the generated confidential file with the generated binding key, and generates the encrypted confidential file. And generating the generated binding license to the device unit,
When obtaining the license,
The module unit decrypts the encrypted confidential file read from the storage unit with the binding key acquired from the device unit, and writes the acquired license as confidential information in the decrypted confidential file. Update the secret file, encrypt the updated secret file with the binding key, update and record the encrypted encrypted secret file in the storage unit, and set the management number of the secret information including the written license as a constituent element. A data terminal device that creates a license management file including the file and writes the file to the storage unit.

60. Apparatus, a system and method for controlling access to contents

US7028340B1 | Fujitsu Ltd

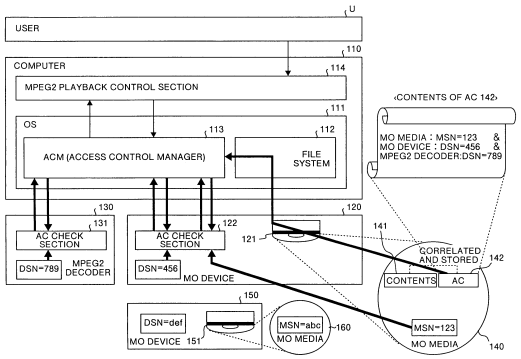
Bibliographic data

Publication date: 2006-04-11
Application date: 2000-07-28
Earliest priority date: 1999-09-17

Inventors: KAMADA JUN, KOTANI SEIGO, ONO ETSUO, HATANAKA MASSAYUKI, YOSHIDA MASATOSHI, NAKAI TAKAHIRO

CPC classification: G06F 21/10, G11B 20/00137, G11B 20/0021, G11B 20/00246
IPC classification: G06K 9/00, G06F 17/30, G06Q 10/00, G06F 1/00, G06F 7/04, H04K 1/00, G06Q 50/00, G11B 20/00, G10L 19/00, G06F 13/00, G06F 12/14, H03M 1/68, G06F 21/10, G06Q 30/06, G06Q 50/10, G06F 21/62, G10L 25/51

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

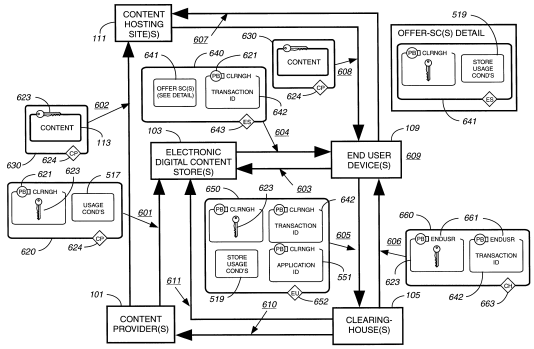
The apparatus controls access to the contents. The apparatus comprises MO device, MPEG2 decoder, and MO media as physical elements. Information for identifying these physical elements (identifying information) is allocated to each of these physical elements. License information, indicating whether access to the contents is to be allowed or not, is recorded on a MO media. Access to the contents recorded on the MO media is controlled based on the license information and the identifying information.

First claim

A contents access control apparatus which provides a control on an access to contents to be provided by an authenticated information provider to a user, said apparatus comprising:
a utilization unit which utilizes the contents stored in a recording medium which stores contents and license information, the utilization unit including a plurality of physical elements for reading out and decoding the contents and the recording medium, to which identifying information are respectively allocated, wherein the contents, and the identifying information of the physical elements for reading out and decoding the contents and the recording medium are recorded on the recording medium in correlation with each other, and a logical product of at least three identifying information is set in the license information; and
an access control unit which controls access to the contents based on the identifying information allocated to physical elements for reading out and decoding the contents and the recording medium of said utilization unit and the license information regarding the access to the contents, wherein the license information is recorded on said recording medium.

61. System for tracking end-user electronic content usage

US6389538B1 | International Business Machines Corp



Bibliographic data

Publication date: 2002-05-14
Application date: 1998-10-22
Earliest priority date: 1998-08-13

Inventors: GRUSE GEORGE GREGORY, DORAK JR JOHN J, MILSTED KENNETH LOUIS

CPC classification: G06F 21/10, G06F 2221/0737, G06F 2221/2135, G06Q 20/3674, G06Q 20/3829, G06Q 30/0617, G06Q 30/0623, G06Q 30/0633, H04L 2209/603, H04L 2463/101, H04L 2463/102, H04L 63/0428, H04L 69/329, H04L 9/0822, H04L 9/0825, H04W 4/029

IPC classification: G06F 1/00, H04L 29/08, H04L 9/08, G06F 21/00, H04L 29/06, H04N 7/167, H04N 7/173, G06F 21/24, H03M 7/30, G09C 1/00, H04L 9/10, G06Q 30/06, G06Q 20/38, G06Q 20/36, G10K 15/02

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

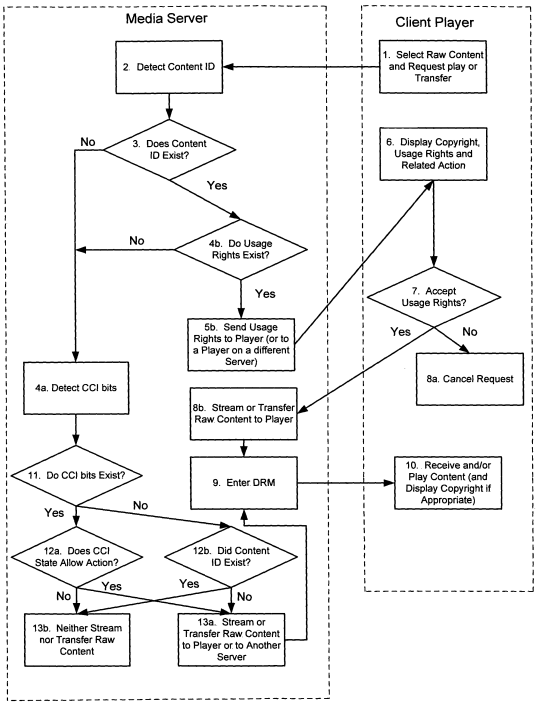
A system for tracking usage of digital content on user devices. Electronic stores coupled to a network sell licenses to play digital content data to users. Content players, which receive from the network the licensed content data, are used to play the licensed content data. Additionally, a logging site that is coupled to the network tracks the playing of the content data. In particular, the logging site receives play information from the network, and the play information includes the number of times that the content data has been played by the associated content player. Also provided is a method for tracking usage of digital content on user devices. According to the method, a license to play digital content data is sold to a user, and the licensed content data is transmitted to a content player for the user. Further, information is transmitted to a logging site whenever the content data is played by the content player or copied from the content player to an external medium so that usage of the licensed content data can be tracked.

First claim

A digital content data player for playing digital content data stored on a storage device and for providing usage information related to the digital content to a remote site, said data player comprising:
an interface for connecting with a storage device;
a receiver for receiving previously encrypted digital content data which has been encrypted with a first encrypting key, and the receiver receiving a from a clearing house an encrypted first decrypting key which has been encrypted with an encrypting key from the digital content player;
a tamper resistant environment for decrypting the first decrypting key with a decrypting key from the digital content player, wherein the tamper resistant environment forming reencrypted digital content data by reencrypting the digital content data with a locally generated digital content player encrypting key, wherein the previously encrypted digital content has been decrypted with the first decrypting key, and the tamper resistant environment storing the reencrypted digital content on the storage device;
a player coupled to the interface for decrypting and playing the stored reencrypted digital content data and generating usage information describing the reencrypted digital content; and
a transmitter for transmitting the usage information to a remote logging site, the usage information informing the remote logging site of at least one of a playing of the reencrypted digital content data by the player and a copying of at least part of the reencrypted digital content data from the storage device to an external medium.

62. Systems and methods using digital watermarking and identifier extraction to provide promotional opportunities

US8055899B2 | Digimarc Corp



Bibliographic data

Publication date: 2011-11-08
Application date: 2005-08-19
Earliest priority date: 2000-12-18

Inventors: LEVY KENNETH L, MEYER JOEL R, ANDREWS III HOYET HARRISON

CPC classification: G06F 21/10, G06F 2221/0733, G06F 2221/0737, G06F 2221/0759, G06Q 30/0601, G11B 20/00768, G11B 20/00855, G11B 20/00884, H04N 21/2541, H04N 21/2543, H04N 21/43615, H04N 21/44204, H04N 21/47202, H04N 21/8355, H04N 21/8358, H04N 7/162, H04N 7/17318

IPC classification: H04N 7/16, G06F 21/00, H04L 29/06, H04N 7/173

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

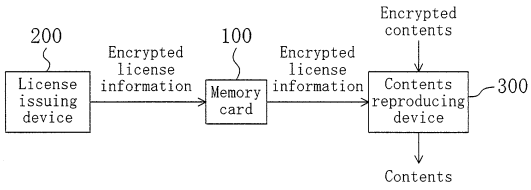
The present disclosure relates to processing media content (e.g., video or audio signals). One claim recites a method including: receiving first content comprising a video portion or an audio portion, the first content being received over a network from a user; utilizing a multi-purpose electronic processor programmed as a content identifier module, deriving identifying data from data representing picture portions of the video portion or from data representing audible portions of the audio portion of the first content; with reference to a computerized database or computerized repository, determining a first promotional opportunity associated with the identifying data, in which the first proportional opportunity comprises an opportunity to purchase second content, the second content being related to—but different than—the first content, and determining a second, different promotional opportunity associated with the identifying data if another instance of the identifying data is thereafter received; and providing information regarding the first promotional opportunity or the second, different promotional opportunity. Of course, other claims and combinations are provided too.

First claim

A method comprising:
initiating a search of raw content, using an electronic processor, for a content identifier steganographically embedded in data representing audio content or in data representing video content, wherein the content identifier steganographically embedded in the data signifies that the raw content was previously subject to digital rights management (DRM);
finding the content identifier in the raw content;
sending the content identifier to an online content store, wherein the online content store is remote to a media server;
receiving from the online content store at least one option associated with the content identifier, wherein the at least one option comprises at least one option from a group of options comprising: purchase content associated with the content identifier subject to the DRM, purchase other content that is related to the raw content, and receive copyright information associated with the raw content;
sending a selected option to the online content store from the media server.

63. License issuing device/method and contents reproducing device/method

US20020026424A1 | Matsushita Electric Industrial Co Ltd



Bibliographic data

Publication date: 2002-02-28
Application date: 2001-08-31
Earliest priority date: 2000-08-31

Inventors: AKASHI TERUO

CPC classification: G06F 21/10, G06F 2221/0797
IPC classification: G06F 15/00, G06F 1/00, G06Q 50/00, H04L 9/08, H04L 9/32, G06F 21/00, G06F 12/14, G06F 21/10, G06Q 30/06, G06Q 50/10, G06F 21/44, G06F 21/62, G06F 21/12, G06F 21/14, G06F 21/33

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

A license issuing device encrypts license information of contents desired by a user with device ID of a memory card carried by the user, and writes the encrypted license information in the memory card. A contents reproducing device decrypts the license information written in the memory card carried by the user with the device ID of the memory card. The contents reproducing device decrypts encrypted contents corresponding to the contents of which use is permitted in the decrypted license information and reproduces the decrypted contents.

First claim

A license issuing device for writing license information permitting use of contents in a portable license storing device, the license storing device having uniquely identifiable device ID and a function of verifying the validity of a partner device, the license issuing device comprising:
verification means for verifying the validity of a license storing device carried by a user;
means for producing license information permitting use of contents designated by the user when the license storing device carried by the user is verified as valid by the verification means; and
first encryption means for encrypting the license information produced by the means for producing license information with the device ID of the license storing device carried by the user and writing the encrypted license information in the license storing device carried by the user.

64. Producing a new black box for a digital rights management (DRM) system

US7319759B1 | Microsoft Corp

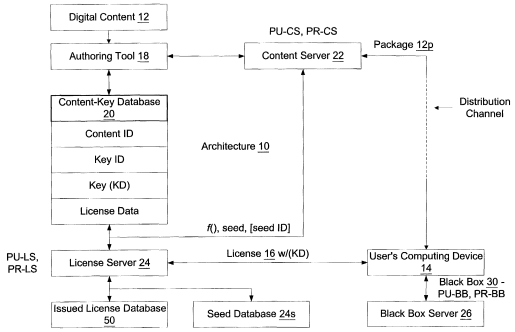
Bibliographic data

Publication date: 2008-01-15
Application date: 2000-03-15
Earliest priority date: 1999-03-27

Inventors: PEINADO MARCUS, VENKATESAN RAMARATHNAM, DAVIS MALCOLM

CPC classification: H04L 2209/603, H04L 9/0825, H04L 9/083, H04L 9/0891
IPC classification: H04L 9/32

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

A new ((n)th) black box is produced for a digital rights management (DRM) system. The (n)th black box is for being installed in and for performing decryption and encryption functions in the DRM system. The (n)th black box is produced and delivered to the DRM system upon request and includes a new ((n)th) executable and a new ((n)th) key file. The (n)th key file has a new ((n)th) set of black box keys and a number of old sets of black box keys. The request includes an old ((n−1)th) key file having the old sets of black box keys. A code optimizer/randomizer receives a master executable and randomized optimization parameters as inputs and produces the (n)th executable as an output. A key manager receives the (n−1)th key file and the (n)th set of black box keys as inputs, extracts the old sets of black box keys from the (n−1)th key file, and produces the (n)th key file including the (n)th set of black box keys and the old sets of black box keys as an output. The (n)th executable and the (n)th key file are forwarded to the requesting DRM system.

First claim

An apparatus for producing a new ((n)th) black box for a digital rights management (DRM) system, the (n)th black box for being installed in the DRM system and for performing decryption and encryption functions in the DRM system, the (n)th black box being produced and delivered to the DRM system upon request therefrom and including a new ((n)th) executable and a new ((n)th) key file, the (n)th key file having a new ((n)th) set of black box keys and a number of old sets of black box keys, the request including an old ((n−1)th) key file having the old sets of black box keys, the apparatus comprising:

a code optimizer/randomizer receiving a master executable and randomized optimization parameters as inputs and producing the (n)th executable as an output; and

a key manager receiving the (n−1)th key file and the (n)th set of black box keys as input, extracting the old sets of black box keys from the (n−1)th key file, and producing the (n)th key file including the (n)th set of black box keys and the old sets of black box keys as an output;

wherein the (n)th executable and the (n)th key file are to be forwarded to the requesting DRM system,

the key manager producing the (n)th key file encrypted according to a secret, the apparatus further comprising an injector receiving the (n)th executable from the code optimizer/randomizer as an input, injecting the secret into the (n)th executable in a pre-determined location, and producing the injected (n)th executable as an output, wherein the injected (n)th executable and the encrypted (n)th key file are to be forwarded to the requesting DRM system,

wherein the DRM system resides on a computing device having a hardware ID (HWID) associated therewith, wherein the HWID is included in and obtained from the (n−1)th key file, and wherein the injector injects the obtained HWID into the (n)th executable in a pre-determined location.

65. LICENSE PURCHASE AND SALE MEDIATION METHOD AND LICENSE MANAGEMENT DEVICE

JP2002373216A | Hitachi Ltd

Bibliographic data

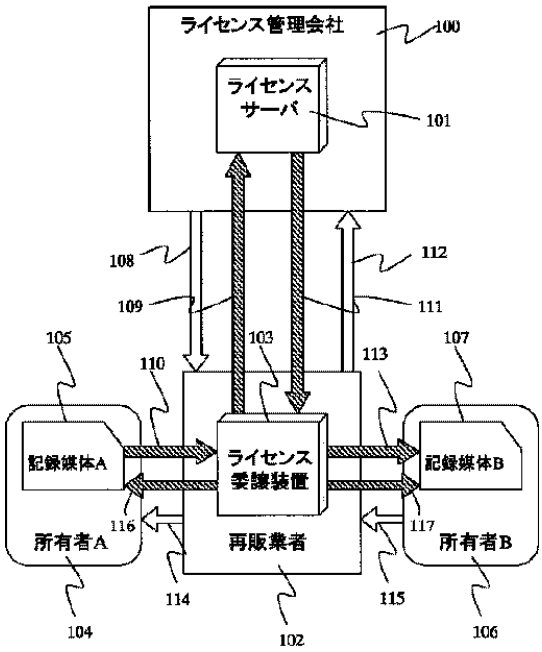
Publication date: 2002-12-26
Application date: 2001-06-18
Earliest priority date: 2001-06-18

Inventors: IGUCHI SHINYA, TSUNODA MOTOYASU, TSUNEHIRO TAKASHI, MIZUSHIMA EIGA, MARUYAMA JUNICHI, KANEHIRA AKIRA, KATAYAMA KUNIHIRO

CPC classification:
IPC classification: G06F 15/00, G06Q 50/00, G06F 21/00, G06F 12/14, G06F 21/10, G06Q 30/06, G06Q 30/04, G06Q 50/10, G06F 21/60, G06F 21/44, G06F 21/62

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

図1



Abstract

(57) [Summary] The present invention provides license discount information and additional information to a person who has sold a license or a person who has purchased a license, thereby facilitating the buying and selling of licenses and obtaining licenses in the market. SOLUTION: A license server 101 which manages licenses and additional information, a license transfer device 103 which extracts licenses from a recording medium A105, accumulates the licenses, records discount information on a recording medium A105, and moves the discount information to a recording medium B107. Is provided.

First claim

A system for mediating the purchase and sale of a license for releasing the use restriction of the content whose use is restricted,
In the license buying and selling intermediation method using a computer, the license is read from a first recording medium used by a first user, and is used when the first user purchases another license on the first recording medium. A license trading mediation method for writing possible discount information and writing the license on a second recording medium used by a second user.

66. Data reproduction apparatus and data terminal apparatus

JP4540202B2 | Sanyo Electric Co Ltd

Bibliographic data

Publication date: 2010-09-08
Application date: 2000-09-20
Earliest priority date: 2000-09-20

Inventors: 中村 康章, 堀 吉宏

CPC classification:
IPC classification: G06F 15/00, G06Q 50/00, H04L 9/08, G06F 13/00, G06F 21/00, G06F 21/10, G06Q 30/06, G06Q 50/10, G06F 21/62, G06F 21/34, G06F 21/33

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

(57) [Summary] [PROBLEMS] To provide a data reproducing device and a data terminal device capable of determining access conditions for encrypted content data based on the same reference time. SOLUTION: A mobile phone 100 receives time information of a distribution server together with encrypted content data and a license key by a transmission / reception unit 1104. Then, controller 1106 sets the time of clocks 1209 and 1232 based on the received time information. AC determination unit 12 11 judges whether or not the access condition acquired from the memory card 110 is within the reproduction restriction period based on the time acquired from the clock 1209. When the access condition is within the reproduction restriction period, the decryption processing unit 1214 The encrypted content data from 0 is decrypted.

First claim

Encrypted content data encrypted content data, and
A license key that is a decryption key for decrypting the encrypted content data;
A data reproduction device for reproducing the content data from a data recording device that records an access condition indicating a condition for decrypting the encrypted content data,
A data decryption processing unit for decrypting the encrypted content data with the license key;
A determination unit that determines whether or not content data can be reproduced based on the access condition;
A clock having a date and time set based on the time information received from the distribution server holding the license key ;
An authentication data holding unit for holding authentication data for the data recording device;
A secret decryption key holding unit for holding a secret decryption key paired with the public encryption key;
A first decryption processing unit that decrypts with the secret decryption key a first session key that is generated in the data recording device and encrypted with the public encryption key;
A session key generation unit for generating a second session key;
An encryption processing unit that encrypts the second session key with the first session key decrypted by the first decryption processing unit;
A second decryption processing unit that obtains the license key and the access condition encrypted by the second session key from the data recording device, and decrypts the license key and the access condition by the second session key ;
The determination unit acquires the access condition from the data recording device after the authentication data is authenticated by the data recording device, and the date and time acquired from the clock is the access condition acquired from the data recording device. Determine whether the specified playback permission deadline has passed,
The data decryption processing unit decrypts the encrypted content data with the license key from the data recording device when a determination result in the determination unit is within a reproduction permission deadline ,
The authentication data includes a public encryption key,
The first decryption processing unit obtains a first session key encrypted by the public encryption key after the authentication data is authenticated in the data recording device,
The data reproduction apparatus , wherein the second decryption processing unit gives the decrypted license key to the data decryption processing unit, and gives the access condition to the determination unit.

67. LICENSE SALES SYSTEM, CONTENT DISTRIBUTING SYSTEM, LICENSE SALES METHOD, AND MEMORY MEDIA

JP2002203071A | Canon Inc

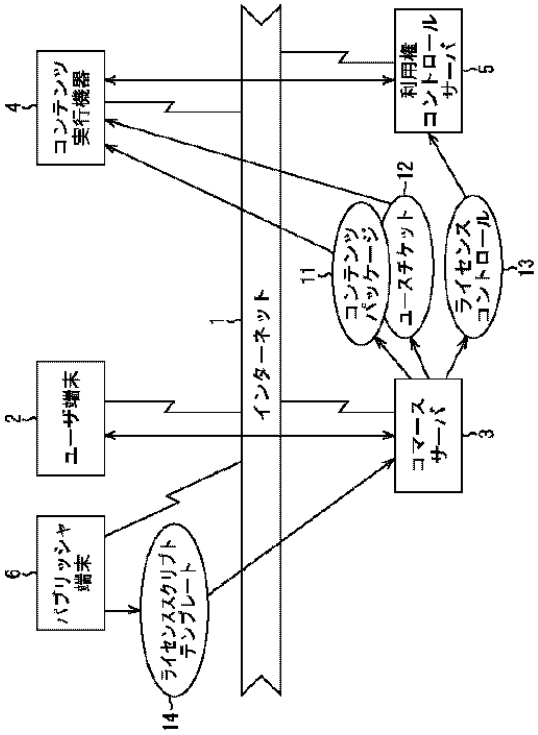
Bibliographic data

Publication date: 2002-07-19
Application date: 2001-10-23
Earliest priority date: 2000-10-27

Inventors: HISAGAI MASAMI

CPC classification:
IPC classification: G06Q 10/00, G06Q 50/00, G06F 12/14, G06F 21/10, G06Q 30/06, G06Q 50/10, G06F 21/62

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

(57) [Summary] [PROBLEMS] To enable a business in which a license sale of digital contents and a license sale of a service can be performed by making use conditions selectable according to user's preference while preventing unauthorized use. SOLUTION: A publisher or a service provider creates a license script template which is a framework for generating a license script in which a license use condition and a charge condition are described in detail for each user, and based on the use condition selected by the user. Create a license script based on the license script, provide an authentication means to authenticate the use qualification when executing the above license, and sell each license according to the user's preference instead of selling licenses under uniform conditions Set the most appropriate usage right and billing method so that they can be used.

First claim

A license script creating means for creating a license script describing a license, a license script storing means for storing the license script, a license selling means for selling the license, and an authentication of possession of the license And a license distribution unit for distributing the license, wherein the license script creation unit modifies a license script template prepared in advance to generate the license script. A license selling device characterized by creating a license sale device.

68. Information processor

US20030182236A1 | Sony Corp

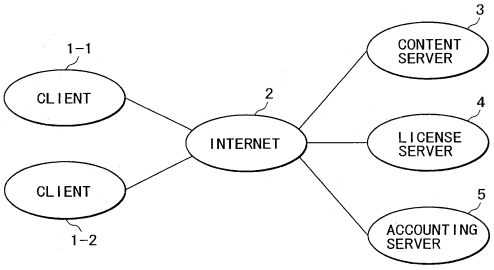
Bibliographic data

Publication date: 2003-09-25
Application date: 2003-05-09
Earliest priority date: 2001-03-29

Inventors: TANAKA KOICHI, ISHIGURO RYUJI

CPC classification: G06F 21/10, G06Q 10/10, G06Q 30/06
IPC classification: G06Q 10/00, G06Q 30/00, G06F 21/10

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

This invention relates to an information processing apparatus for permitting relatively unrestrained distribution of contents while managing the contents individually. Contents are separated from licenses granting the right to their use. To each content are added use conditions specifying how the content is to be used. The content is furnished with a mark which comprises a leaf ID, an ownership flag, a use start time-stamp, and a copy count. This invention may be applied to any apparatus for offering contents.

First claim

An information processing apparatus which provides a license for the use of content to a client when accessed by said client, said information processing apparatus comprising:
first acquiring means for acquiring from said client designation information for designating said license;
second acquiring means for acquiring use status information about said license designated by said designation information acquired by said first acquiring means; and
providing means for generating mark information corresponding to said use status information acquired by said second acquiring means in order to provide said client with the generated mark information.

69. DATA TERMINAL DEVICE

JP2002094500A | Sanyo Electric Co Ltd

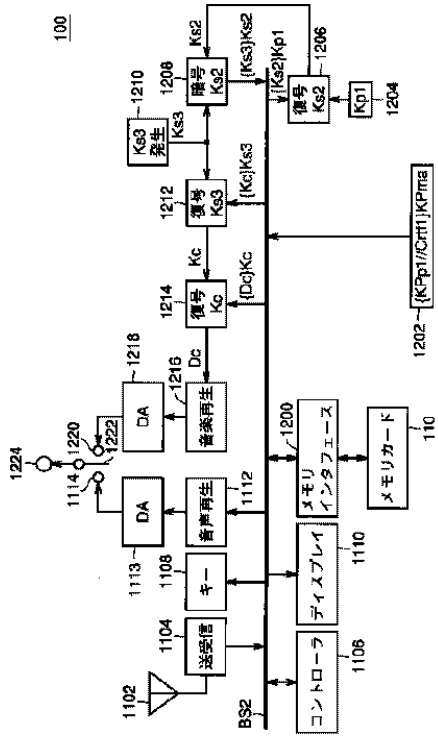
Bibliographic data

Publication date: 2002-03-29
Application date: 2000-09-20
Earliest priority date: 2000-09-20

Inventors: TAKEMURA KOJI, HORI YOSHIHIRO

CPC classification:
IPC classification: H04M 1/00, H04L 9/08, H04L 9/32, G06F 12/14, H04N 7/167, G06F 21/10, H04N 21/442, H04N 21/4405, G06F 21/62

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

(57) [Problem] To provide a data terminal device capable of reproducing encrypted content data even when the encrypted content data is received from the outside. SOLUTION: When a mobile phone 100 newly receives encrypted content data from another device and stores the encrypted content data in a memory card 110, a license for decrypting the encrypted content data is stored in the memory card 110. Memory interface 1 whether or not it exists Search through 200. Then, when the license does not exist, the mobile phone 100 requests the distribution server to distribute the license via the transmission / reception unit 1104, receives the license from the distribution server, and outputs the license to the memory card 110.

First claim

A distribution server in which encrypted content data obtained by encrypting content data and a license including a license key serving as a decryption key for decrypting the encrypted content data are stored in a storage server. And / or a data terminal device for receiving a license and playing back the encrypted content data, a communication unit for performing external communication, a data recording unit on which the encrypted content data and the license are recorded, An interface for controlling transmission and reception of data to and from the data recording unit; a decryption processing unit for decrypting the encrypted content data with the license key; and a control unit. The license capable of decrypting the recorded encrypted content data is When not recorded in the recording unit, the communication unit is controlled to request distribution of a license capable of decrypting the encrypted content data recorded in the data recording unit from the distribution server via the communication unit. A data terminal device that, when the communication unit receives the license from the distribution server, records the received license in the data recording unit via the interface.

70. License management server, terminal device, license management system and usage restriction control method

US20030028622A1 | Individual

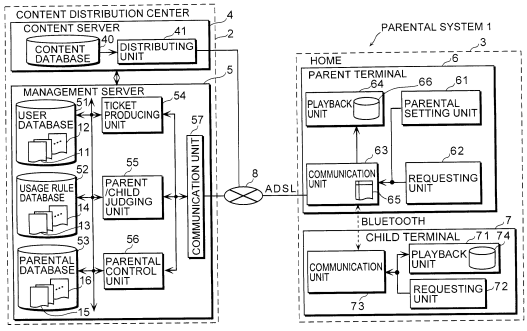
Bibliographic data

Publication date: 2003-02-06
Application date: 2002-08-05
Earliest priority date: 2001-08-06

Inventors: INOUE MITSUHIRO, OKAMOTO RYUICHI

CPC classification: G06F 17/00, G06F 21/6218, G06F 2221/2149, H04L 2463/101, H04L 63/10, H04L 69/329, H04N 21/4623, H04N 21/4627, H04N 21/8352, H04N 21/8355
IPC classification: H04L 29/08, H04L 29/06, G06F 21/62

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

A management server (5) manages usage rules in accordance with which terminals use contents, and includes a usage rule database (52), a parental control unit (56), a parental database (53), and a ticket producing unit (54). The usage rule database (53) stores usage rule information (13˜14) that associates each user with the usage rules. The parental control unit (56) obtains, from a parent terminal (6), parental information (15˜16) that is a request made by the parent terminal (6) for placing a restriction on content usage by a child terminal (7), and the parental database (53) stores the obtained parental information (15˜16). On receiving, from the parent terminal (6), a content request made by a user of the child terminal (7) for content use, the ticket producing unit (54) adds a restriction shown in the stored parental information for the child terminal (7) to a usage rule shown in the stored rule information for the child terminal (7) to produce a new usage rule, produces a license ticket that permits content use under the new usage rule, and sends the license ticket to the parent terminal (6).

First claim

A license management server that manages usage rules in accordance with which terminal devices use contents, wherein the terminal devices include a first terminal device used by a first user and a second terminal device used by a second user, comprising:
an information storing unit operable to store license information that associates a usage rule with either (a) each of the first terminal device and the second terminal device or (b) each of the first user and the second user;
a restriction managing unit operable to obtain restriction information from either the first terminal device or the first user and to store the restriction information, which shows a restriction on content use by either the second terminal device or the second user; and
a ticket issuing unit operable to (1) obtain a usage request from either the first terminal device or the first user, the obtained usage request requesting content use by either the second terminal device or the second user, (2) add, in response to the obtained usage request, the restriction shown in the restriction information in the restriction managing unit to a usage rule associated by the license information with one of the first terminal device, the first user, the second terminal device, and the second user to produce a new usage rule, (3) produce a first license ticket that permits content use under the new usage rule, and (4) send the first license ticket to either the first terminal device or the first user.

71. SYSTEM AND METHOD FOR CONTENTS USE MANAGEMENT

JP2002342518A | Matsushita Electric Industrial Co Ltd

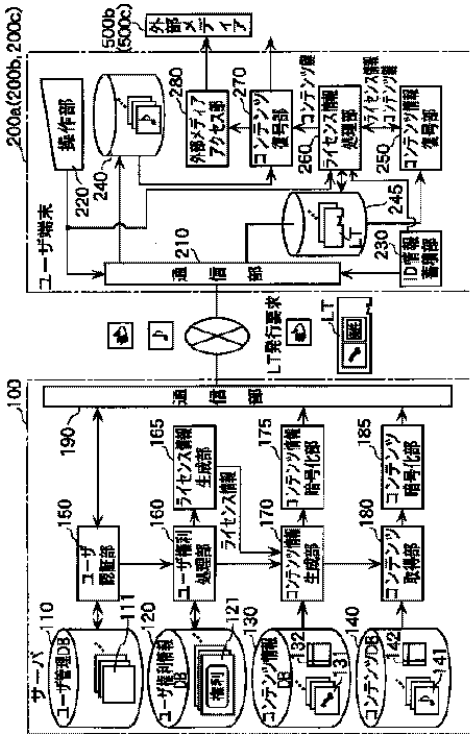
Bibliographic data

Publication date: 2002-11-29
Application date: 2002-01-31
Earliest priority date: 2001-02-02

Inventors: AZUMA AKIO, MURAKAMI HIRONORI, MATSUO TAKASHI, NAKAHARA TORU, NANBA TAKAAKI, GOTO YOSHIMASA, NAKANISHI MASANORI, MIYAZAKI MASAYA, KOZUKA MASAYUKI

CPC classification:
IPC classification: G06F 15/00, G06Q 50/00, H04N 5/91, H04N 5/765, H04N 7/16, G06F 21/00, G06F 12/14, H04N 7/173, G06F 21/10, G06Q 30/06, G06Q 50/10, H04N 21/237, G06F 21/44, G06F 21/62, G06F 21/33, G06F 21/42

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

PROBLEM TO BE SOLVED: To provide a contents use management system, etc., which enables a server to surely and easily control the use of contents on a user terminal without placing any load on the user terminal. SOLUTION: The server 100 of the contents use management system is equipped with a user right information DB 120 which stores right information regarding the right to use contents that the user using the user terminal 200a has and a contents information generation part 170 which generates LT as right information showing part of the use right that the user has at a request made by the user and sends it to the user terminal 200a. The user terminal 200a, on the other hand, is equipped with a communication part 210 which receives the LT sent from the server 100 and a license information processing part 260 which controls the use of the contents according to the use right that the received LT shows.

First claim

A content use management system comprising: a terminal device that uses content that is a digital work; and a server device that manages use of the content in the terminal device via a transmission path, wherein the server device A right information storage unit for storing right information relating to a right to use the content owned by the user using the terminal device; and a right indicating a part of the right to use owned by the user based on a request from the user. A license ticket issuing unit that generates a license ticket as information and transmits the license ticket to the terminal device, wherein the terminal device receives a license ticket transmitted from the server device, and receives the license ticket. Use of the content that controls the use of the content according to the use authority indicated by A content use management system, comprising: a control unit.

72. SECURE DIGITAL CONTENT LICENSING SYSTEM AND METHOD

EP1277305B1 | Blockbuster LLC

Bibliographic data

Publication date: 2011-09-21
Application date: 2001-04-06
Earliest priority date: 2000-04-07

Inventors: RUSSELL JOHN CHRISTOPHER PARK, OUTTEN TODD AVERY, SPAULDING BRYAN GENTRY, SHERR SCOTT JEFFREY, LANDAU YAIR, BARNETT JEREMY ELI, RUBENSTEIN IRA STEVEN, LAKAMP BRIAN DAVID, CHEY DOUGLAS DAISEUNG, ARRIETA MICHAEL R, MANDYAM HARISH, MOSSON ANDREW, ABRAHAM MARY, KORMAN MARY, RODRIGUEZ THOMAS M, BRODERSOHN ERNESTO

CPC classification: G06F 21/10, G06F 2221/0708, G06F 2221/2137, G06Q 10/10, G06Q 30/06, H04L 2463/101, H04L 2463/102, H04L 63/0428, H04L 63/12, H04L 67/1008, H04L 67/1095, H04N 21/2181, H04N 21/2225, H04N 21/23116, H04N 21/23473, H04N 21/2393, H04N 21/2405, H04N 21/2543, H04N 21/25841, H04N 21/26609, H04N 21/4622, H04N 21/6125, H04N 7/17318

IPC classification: G06F 17/30, G06Q 10/00, G06Q 30/00, H04L 29/08, H04L 9/08, H04L 9/00, H04N 5/765, G06F 13/00, H04L 29/06, H04N 7/167, H04N 7/173, H04N 7/08, G06F 21/10, H04N 7/081

External links: Google Patents, Espacenet, EP Register, PatBase Express, PatBase, Orbit

Abstract

Rental of the digital content occurs within an online environment including one or more user network-enabled devices and one or more server network devices connected by a communications link to the one or more user network-enabled devices. A user selects content displayed on a main website and requests download of the selected content to the user network-enabled device. To be able to access the content the user must obtain a license. The user's request for a license for specific content comprises information about a desired rental model, an expiration date for the rental model, and information that identifies the user's user network-enabled device, along with other information. A license for the content is generated which comprises the above information and also includes an encryption key for the selected movie. Media player and security technology residing on the user network-enabled device provides protection against unauthorized access to the content by ensuring that only licensed content is viewed and is accessed according to the rental model contained in the license.

First claim

A system for secure licensing of content to a user on a user network-enabled device (102, 202, 302), the system comprising:
at least one server network device (104, 106) communicatively coupled to the user network-enabled device (102, 202, 302);
wherein the at least one server network device (104, 106) is programmed to transfer selected encrypted content to the user network-enabled device (102, 202, 302);
a license generator (214, 314) the license generator being programmed to receive a license request comprising user network-enabled device identification information (322) and media player identification information (324) identifying a media player residing on the user network-enabled device and to generate an encrypted license (309) associated with the selected encrypted content, the encrypted license comprising
access information (318, 320, 322, 324, 326) defining conditions for controlling the user network-enabled device;

an encryption key (328) to enable the user network-enabled device (102, 202, 302) to produce a user-perceptible form of the selected encrypted content when the conditions defined by the access information are met and to inhibit production of a user-perceptible form of the selected encrypted content when the conditions defined by the access information are not met;
the user network-enabled device identification information; and
the media player identification information;
a root key for decrypting the encrypted license (309) to allow the access information and the encryption key (328) in the encrypted license to be accessed by a media player and security technology (424) programmed on the user network-enabled device (102, 202, 302), the media player and security technology (424) being configured to control a specific media player (440) on the user network-enabled device (102, 202, 302) to produce the user-perceptible form of the selected encrypted content, the specific media player being determined by the media player identification informations included in the encrypted license
wherein the user-perceptible form of the encrypted content can be produced only by the specific media player (440) indicated by said media player identification information and by the user network enabled device indicated by said network enabled device identification information.

73. DISTRIBUTION DEVICE, TERMINAL DEVICE, PROGRAM AND METHOD USED IN THESE DEVICES

RU2287851C2 | MATSUSHITA ELECTRIC IND CO LTD

Bibliographic data

Publication date: 2006-11-20
Application date: 2001-12-06
Earliest priority date: 2000-12-08

Inventors: OKAMOTO RIUITI, KOZUKA MASAJUKI, MINAMI MASATAKA, INOUE MITSUKHIRO

CPC classification:
IPC classification: G06F 17/30, G06F 21/22

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

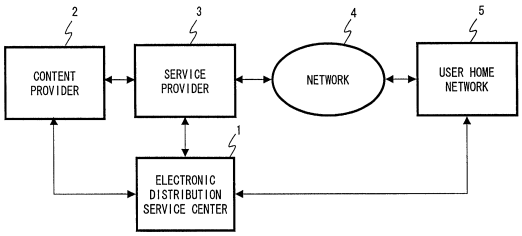
FIELD: distribution devices, terminal devices.

First claim

A distribution device comprising a storage device (19) for storing rights management information;
a license certificate (LU) transmission device (24) for transmitting a license certificate to a terminal device together with digital information content, the license certificate indicating, as a license, a part of the license information indicated by the rights management information; a data update module (25) when moving from a system for updating rights management information such that license information indicated by rights management information stored in a memory device (19) for storing rights management information is a residual part of the license indicated by the license certificate ; a receiving device for receiving the license certificate after the update, when the license certificate is returned after the update, indicating a decrease in the license in accordance with the use of information content by the terminal device; a data update module (26) when moving to a system which, upon receipt of a license certificate returned by the terminal device that updated the license certificate and indicating a decrease in the license in accordance with the use of information content by the terminal device, is intended to increase the license information indicated by the rights management information, by updating the rights management information stored in the storage device based on the license certificate after updating Nia.

74. Systems and methods for content distribution using one or more distribution keys

US7353541B1 | Sony Corp



Bibliographic data

Publication date: 2008-04-01
Application date: 2000-09-07
Earliest priority date: 1999-09-07

Inventors: ISHIBASHI YOSHIHITO, OISHI TATEO, MUTO AKIHIRO, KITAHARA JUN, SHIRAI TAIZOU

CPC classification: G06F 15/00, G06F 21/10, G10K 15/04, G11B 20/00166, G11B 20/0021, H04L 9/0894, H04L 9/3247, H04N 2005/91342, H04N 2005/91364, H04N 21/4334, H04N 21/4532, H04N 21/4627, H04N 21/8355, H04N 5/913, H04N 5/9206, H04N 7/1675

IPC classification: G06K 9/00, G06F 17/30, G06F 1/00, G06F 7/04, H04K 1/00, G11B 20/00, H04L 9/00, H04L 9/32, H04N 7/167, H04N 5/92, G10K 15/04, H04N 5/913, H03M 1/68, G06F 21/10

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

An information receiving apparatus receives identification information and encrypted identification information and makes a comparison between them to allow prevention of illegal utilization of contents data. Also, a data storage apparatus can record contents data encrypted by a content key and the content key so that the contents data can be reproduced on other apparatuses to improve versatility. Moreover, a management apparatus can manage the contents data in the data storage apparatus to allow other apparatuses to utilize it. And also, an information regulating apparatus can verify a signature on available data to prevent illegal utilization of the contents data. Furthermore, the data storage apparatus can store the content key, its handling policies, the contents data encrypted by the content key and its license conditions information so as to safely provide the contents data. In addition, an information recording apparatus can select favorite contents data and store it on the data storage apparatus. Furthermore, the information receiving apparatus can prevent utilization of provision-prohibited contents data by a provision prohibition list.

First claim

A multimedia content delivery system for sending predetermined content data from an information sending apparatus to an information receiving apparatus, wherein the information sending apparatus comprises:
means for holding first identification information with an individual key, wherein the first identification information identifies the information sending apparatus and the individual key is unique to the information sending apparatus, and further wherein the first identification information with the individual key is encrypted by a distribution key that is unique to the information receiving apparatus;
means for adding second identification information to the content data, wherein the second identification information is identical to the first identification information;
means for encrypting the second identification with the content data by a content key;
means for encrypting the content key by the individual key;
means for sending the encrypted first identification information with the individual key, the encrypted second identification information with the content data, and the encrypted content key to the information receiving apparatus; and
wherein the information receiving apparatus comprises:
means for holding the distribution key;
means for receiving the encrypted first identification information with the individual key, the encrypted second identification information with the content data, and the encrypted content key to the information receiving apparatus;
means for decrypting the encrypted first identification information with the individual key using the distribution key to acquire the first identification information and the individual key;
means for decrypting the encrypted content key using the individual key to acquire the content key;

means for decrypting the encrypted second identification information with the content data by using the content key to acquire the second identification information and the content data; and
means for comparing the first identification information with the second identification information.

75. Information recording apparatus, information reproducing apparatus, and information distribution system

US7343495B2 | Toshiba Corp

Bibliographic data

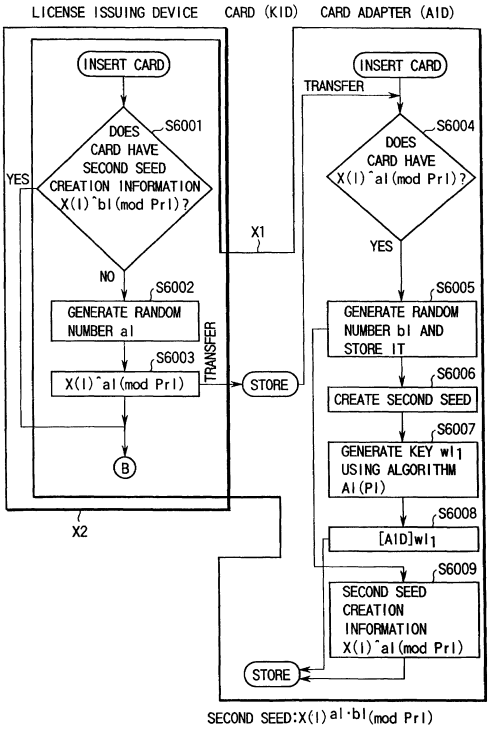
Publication date: 2008-03-11
Application date: 2002-08-27
Earliest priority date: 1997-05-13

Inventors: KAMBAYASHI TORU, AKIYAMA KOICHIRO, TSUJIMOTO SHUICHI, SUMITA KAZUO, HIRAKAWA HIDEKI, SUGAYA TOSHIHIRO

CPC classification: G06F 21/10, G06F 2211/007, G06F 2221/0795, G06F 2221/2135, G06Q 30/018, G11B 20/0021, G11B 20/00224, G11B 20/00246, G11B 20/00253, G11B 20/00536, G11B 20/00557, G11B 20/0084, G11B 20/00847, H04L 2209/603, H04L 9/0891

IPC classification: G06F 1/00, H04K 1/00, G11B 20/00, H04L 9/08, H04L 9/32, H04N 9/16, G06F 21/10

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

An information recording apparatus comprises an encryption section encrypting contents information and also a license condition referred to to limit use of the contents information and a decoding key for decoding the encrypted contents information to generate license information, and a recording section recording the encrypted contents information and the generated license information on a recording medium. An information reproducing apparatus comprises a decoder unit decoding the license information recorded on the recording medium using a second decoding key for decoding the license information and deciding on the basis of the license condition contained in the decoded license information whether the contents information can be used. If it is decided that the contents information can be used, the encrypted contents information recorded on the recording medium is decoded using the first decoding key contained in the decoded license information.

First claim

A method of moving license information comprising:
reading, from a first removable computer readable recording medium recording contents and capable of being inserted into a computer,
the license information to enable use of the contents recorded in the first removable computer readable recording medium and (b) a first unique medium ID of the first removable computer readable recording medium;
receiving a second removable computer readable recording medium;
reading a second unique medium ID of the second removable computer readable recording medium;
processing the license information in accordance with the first unique medium ID of the first removable computer readable recording medium to obtain first processed license information;
processing the first processed license information in accordance with the second unique medium ID of the second removable computer readable recording medium to obtain second processed license information;
writing the second processed license information to the second removable computer readable recording medium;
deleting the license information stored in the first removable computer readable recording medium.

76. Data playback device

JP4766762B2 | Sanyo Electric Co Ltd

Bibliographic data

Publication date: 2011-09-07
Application date: 2001-03-26
Earliest priority date: 2001-03-26

Inventors: 堀 吉宏, 日置 敏昭

CPC classification:
IPC classification: G06Q 10/00, G06Q 50/00, G06F 12/14, H04L 9/16, G06F 21/10, G06Q 30/06, G06Q 50/10, G06F 21/62

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

PROBLEM TO BE SOLVED: To provide a contents providing method for distributing enciphered contents data divided into a plurality of blocks and a plurality of licenses for decoding and reproducing the enciphered data included in those blocks. SOLUTION: Enciphered contents data 90 or 93 obtained by enciphering music data are composed of trial enciphered music data 91 or 94 and main enciphered music data 92 or 95. The enciphered music data 91 and 94 are decoded by a license key Kc1, and the enciphered music data 92 and 95 are decoded by a license key Kc2. A distributing server holds the enciphered contents data 90 and 93 and the license keys Kc1 and Kc2, and distributes the trial enciphered music data 91 or 94 and the license key Kc1, and the main enciphered music data 92 or 95 and the license key Kc2 in this order in response to a distribution request.

First claim

A data reproduction device for decrypting and reproducing encrypted content data composed of a plurality of blocks with a plurality of licenses corresponding to the plurality of blocks,
An interface for exchanging with the encrypted content data and a data recording device in which the plurality of licenses are recorded;
An operation unit for inputting instructions;
A content reproduction unit that decrypts and reproduces the encrypted content data with a license key that decrypts the encrypted content data included in each of the plurality of licenses;
A control unit,
The controller is
Giving the content playback unit the encrypted content data composed of the plurality of blocks according to a playback order;
When the one block of the encrypted content data is decrypted by the license key included in one license among the plurality of licenses in the content reproduction unit, a license to be used next is passed through the interface. In accordance with the playback conditions included in the acquired license, it is determined whether or not playback is possible using the license. If it is determined that playback is possible, the encrypted content is A data reproduction apparatus that provides a license key included in the acquired license to the content reproduction unit when decoding of a block next to the plurality of blocks of data is started.

77. LICENSE MANAGING SERVER, TERMINAL DEVICE, LICENSE MANAGING SYSTEM AND UTILIZATION LIMIT CONTROL METHOD

JP2003178163A | Matsushita Electric Industrial Co Ltd

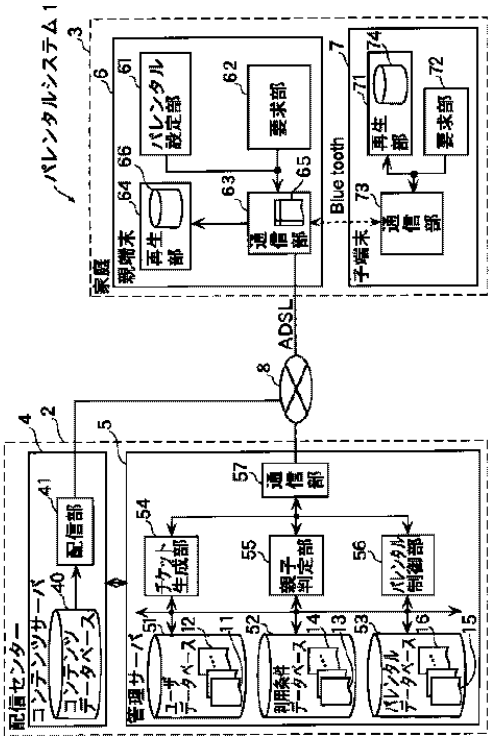
Bibliographic data

Publication date: 2003-06-27
Application date: 2002-08-06
Earliest priority date: 2001-08-06

Inventors: INOUE MITSUHIRO, OKAMOTO RYUICHI

CPC classification:
IPC classification: G06Q 50/00, G06F 12/14, G06F 21/10, G06Q 50/10, G06F 21/60, G06F 21/62

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

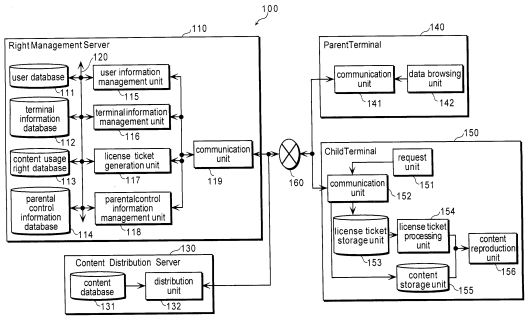
(57) [Summary] [Problem] To provide a license management system capable of setting more various usage restrictions. A management server (5) manages usage conditions of contents in a terminal device, and stores a usage condition database (52) storing contents usage conditions (13) to (14) corresponding to the usage conditions for each user; Parental control unit 56 that acquires parental information 15 to 16 as an instruction to restrict use of content by child terminal 7 user And a parental database 53 storing parental information 15-16, and when a content use request by the user of the child terminal 7 is acquired from the parent terminal 6, the parental database The ticket generation unit 54 adds a restriction indicated by the parental information stored in 53, generates a license ticket as information for permitting use of the content, and transmits the license ticket to the parent terminal 6.

First claim

A license management server for managing usage conditions of contents in a terminal device, wherein the license information storage means stores license information in which the usage conditions are associated with each terminal device or user, and a first terminal. A usage restriction information management unit for acquiring and storing usage restriction information, which is an instruction to restrict usage of the content by the second terminal apparatus or the second user, from the apparatus or the first user, and the first terminal apparatus Alternatively, when an instruction to request the use of the content by the second terminal device or the second user is acquired from the first user, the use indicated by the corresponding license information stored in the license information storage means is displayed. In a usage condition in which a restriction indicated by the corresponding usage restriction information stored in the usage restriction information management means is added to the condition,
A license ticket, which is information indicating that the use of the content is permitted, is generated, and the license ticket is generated.
A license management server, comprising: a ticket issuing means for transmitting to a user.

78. License management server, license management system and usage restriction method

US7103663B2 | Matsushita Electric Industrial Co Ltd



Bibliographic data

Publication date: 2006-09-05
Application date: 2002-06-10
Earliest priority date: 2001-06-11

Inventors: INOUE MITSUHIRO, OKAMOTO RYUICHI

CPC classification: G06F 17/00, G06F 21/10, G06F 21/6218, G06F 2221/2149, H04L 2463/101, H04L 63/104, H04M 3/38, H04N 21/2541, H04N 21/25816, H04N 21/25875, H04N 21/4627, H04N 21/4751, H04N 21/8355, H04N 7/165, H04N 7/17318

IPC classification: G06F 1/00, G06F 15/16, H04N 7/16, H04L 29/06, H04N 7/173, G06F 21/10, H04M 3/38, G06F 21/62

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

A right management server manages usage of a content on a parent terminal and a child terminal. The right management server includes content usage right database that stores right information indicating a usage rule of a content for each terminal ID or user ID, and a parental control information management unit that acquires, from the parent terminal or the parent user, parental control information that is an instruction to put a restriction on usage of a content on the child terminal or by a child user, and stores the parental control information in a parental control information database. The right management server also includes a license ticket generation unit that acquires a license ticket issuance request from the child terminal or the child user, generates a license ticket that is information for permitting usage of the content on the child terminal or by the child user, under a usage rule with a restriction indicated by the parental control information which is held in the parental control information management unit, and sends the license ticket to the child terminal or the child user.

First claim

A license management server device for managing content usage on a terminal device, the license management server device comprising:
a license information storage unit operable to store license information indicating a usage rule of a content for each terminal device or user;
a usage restriction information management unit operable to acquire from a first terminal device or a first user an instruction to put a restriction on content usage on a second terminal device or by a second user, and usage restriction information indicating details of the restriction, and hold the usage restriction information; and
a ticket issuance unit operable to acquire an instruction to request the content usage from the second terminal device or the second user, generate a license ticket that is information for permitting the content usage on the second terminal device or by the second user, under a usage rule with the restriction indicated by the usage restriction information which is held in the usage restriction information management unit, and send the license ticket to the second terminal device or the second user.

79. Super-distribution of protected digital content

US6983371B1 | International Business Machines Corp

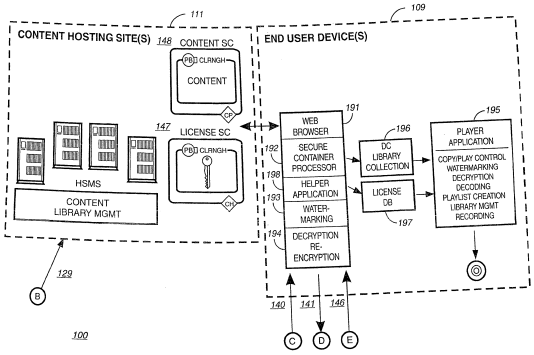
Bibliographic data

Publication date: 2006-01-03
Application date: 2000-11-13
Earliest priority date: 1998-10-22

Inventors: HURTADO MARCO M, MAHLBACHER JAMES C, SPAGNA RICHARD L

CPC classification: G06F 21/10, G06Q 20/401, H04L 2209/60, H04L 9/083, H04L 9/321
IPC classification: H04K 1/00, G06F 11/00, H04L 9/00

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

Briefly according to the present invention, a system, computer readable medium and method to deliver encrypted digital content to from a first system for playing the content to a second system for playing the content. The method on the first user system comprising the steps of: reading from a computer readable medium metadata which has previously been associated with the content; selecting from the metadata associated content to decrypt; establishing a secure connection with an authorization authority, such as a clearinghouse, for decrypting the key used to encrypt the content; receiving a secure container containing the decrypting key for decrypting at least part of the previously encrypted content as permitted; decrypting the content and then encrypting the content with a new encryption key that is generated locally on the end user system.

First claim

A method to deliver encrypted digital content from a first system for playing the content to a second system for playing the content, the method on the second system comprising the steps of:
reading on a second system from a computer readable medium metadata which has previously been associated with a portion of content, wherein the content is encrypted with a first key associated with the first system;
selecting from the metadata associated content to decrypt;
establishing a secure transmission with an authorization authority for decrypting the content;
receiving a decrypting key for decrypting at least part of the previously encrypted content stored on the computer readable medium as permitted by the authorization authority;
decrypting at least part of the previously encrypted content as permitted by the authorization authority;
reencrypting the decrypted content utilizing a unique local decrypting key;
storing the content in a library;
decrypting at least part of the content from the library using the unique local decrypting key.

80. METHOD AND DEVICE FOR MANAGING COPYRIGHT

JP2002117167A | Nippon Telegraph and Telephone Corp

Bibliographic data

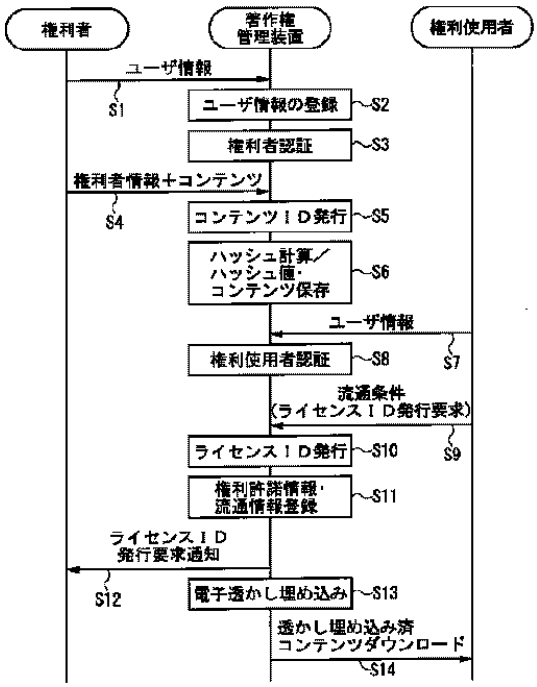
Publication date: 2002-04-19
Application date: 2000-10-05
Earliest priority date: 2000-10-05

Inventors: AZUMA SHOZO, MINAMI MASAKI, YAMADA MASANORI, SANO MUTSUO

CPC classification:
IPC classification: G06Q 10/00, G06Q 50/00, G06F 12/00, H04L 9/32, G06F 12/14, G09C 5/00, G06F 21/10, G06Q 30/06, G06Q 50/10, G06F 21/60, G06F 21/62

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

本発明の原理を説明するための図



Abstract

(57) [Summary] (Modified) [Problem] To hold a relationship between a right and a plurality of licenses related to the right, a relationship between a content and a license condition, and detect an ID embedded in the content. Provides a copyright management method capable of identifying a right user. SOLUTION: When right holder information and content are received after the right holder has been authenticated and established, a content ID for uniquely identifying the content is issued, the right information and the content are stored, and the right user receives the content. Upon receiving a license ID issuance request including the ID and a distribution condition for the content designated by the content ID, a license ID for uniquely identifying the right user is issued, and the right user issues a license ID issuance request. At the same time, a digital watermark is embedded in the content, and the content is downloaded to the right user terminal.

First claim

Registering information by issuing unique IDs at the time of content creation and distribution and holding role information of users including right holders and right users and access permission information for each data item. In a copyright management method for controlling access to management information including update, search, a copyright management device that manages copyright, when storing contents, the copyright management device, Receiving and registering the user information from the right holder terminal of the right holder, authenticates the right holder using the user information, and after the authentication is established, when the right holder information and the content are received, the content is uniquely identified. A content ID to be specified is issued, the right information and the result of hash calculation of the content are registered, and the content is stored. It receives user information from, to authenticate the right user by using the user information of the rights a user who has been registered in advance, after the authentication is established,

Upon receiving a license ID issuance request including a content ID and a distribution condition for the content specified by the content ID, issues a license ID that uniquely identifies the right user, registers the license information and the distribution information, Notify the right holder that the license user has issued the license ID issuance request, and at the same time, embed a digital watermark in the content, and send the digital watermark embedded content to the right user terminal. Copyright management method characterized by downloading.

81. Data distribution system and recording device for use therein

US7945517B2 | Fujitsu Ltd, Sanyo Electric Co Ltd, Renesas Electronics Corp

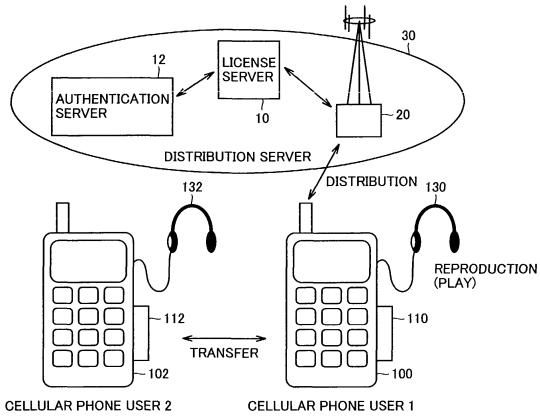
Bibliographic data

Publication date: 2011-05-17
Application date: 2002-06-04
Earliest priority date: 1999-12-06

Inventors: HORI YOSHIHIRO, HIOKI TOSHIAKI, KANAMORI MIWA, TAKAHASHI MASATAKA, HASEBE TAKAYUKI, YOSHIOKA MAKOTO, HATAKEYAMA TAKAHISA, TONEGAWA TADAAKI, ANAZAWA TAKEAKI

CPC classification: G06F 21/10, G06F 2221/0797
IPC classification: G06Q 10/00, G06F 1/00, G06Q 50/00, G06F 11/00, H04L 9/00, G06F 21/00, H04W 88/02, H04W 12/06, H04W 12/04, H04W 4/06, G06F 21/10, G06Q 30/06, G06Q 50/10, G06F 21/62, G06F 21/31

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

A memory card (110) stores access restriction information (AC 1) to a license information hold unit (1440) arranged in a TRM area. Access restriction information (AC 1) has information for example of a frequency of reproduction allowed and a number of licenses owned. A controller (1420) in reproducing and transferring content initially confirms access restriction information (AC 1) and thereafter effects reproduction and transfer and after the reproduction and transfer are effected updates access restriction information (AC 1), as required, for storage in a license information hold unit (1440).

First claim

A recording device, comprising:
an interface unit for externally communicating data;
a storage unit for storing therein data storage and access restriction information received through said interface unit, said access restriction information being used to control outputting said data storage from said recording device;
an authentication data hold unit holding a first public encryption key determined to correspond to said recording device and encrypted in a state decryptable with an authentication key, for external output via said interface unit when said data storage and said access restriction information are received;
a first key hold unit holding a first private decryption key provided to decrypt data encrypted with said first public encryption key;
a first decryption unit receiving externally via said interface unit a first symmetric key encrypted with said first public encryption key, and decrypting said first symmetric key;
a second key hold unit holding a second public encryption key different for each said recording device;
a session key generation unit producing a second symmetric key updated whenever said data storage is communicated;
a first encryption unit encrypting said second symmetric key and said second public encryption key with said first symmetric key for output externally via said interface unit;
a second decryption unit receiving said data storage and access restriction information input via said interface unit, for decryption with said second symmetric key, said data storage and access restriction information being encrypted with said second symmetric key and said second public encryption key;
a third key hold unit holding a second private decryption key provided to decrypt data encrypted with said second public encryption key;
a third decryption unit using said second private decryption key to decrypt said data storage and access restriction information encrypted;
a control unit operative, when an external instruction is issued to output said data storage recorded in said storage unit, to refer to said access restriction information in said storage unit to determine whether reproduction information

for said data storage may be output, wherein said storage unit records therein said data storage in one of a state encrypted with said second public encryption key and a state decrypted by said third decryption unit, and
when said control unit determines that said data storage may be output said data storage is output and thereafter as required said control unit changes said access restriction information recorded in said storage unit.

82. System for Tracking End-user Electronic Content Usage

AU2003227202B2 | Wistron Corp

Author/publisher identities should be

Bibliographic data

Publication date: 2006-08-10
Application date: 2003-06-16
Earliest priority date: 1999-08-12

Inventors: MEDINA CESAR, LOTSPIECH JEFFREY, DORAK JOHN JR, HURTADO MARCO, MILSTED KENNETH, LEHMAN CHRISTOPHER, DOWNS EDGAR, GRUSE GEORGE GREGORY

CPC classification:
IPC classification: G06F 1/00, H04L 29/06

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

First claim

A digital content data player for playing digital content data stored on a storage device and for providing usage information related to the digital content to a remote site, s said data player comprising: an interface for connecting with the storage device; a player coupled to the interface for playing the stored digital content data and generating usage information describing the digital content; and a transmitter for transmitting the usage information to a remote logging site on a 1o network, the usage information informing the remote logging site of at least one of a playing of the stored digital content data by the player and a copying of at least part of the digital content data from the storage device to an external medium.

83. Information processing apparatus and method for managing grouped devices in an encrypted environment

US7426639B2 | Sony Corp

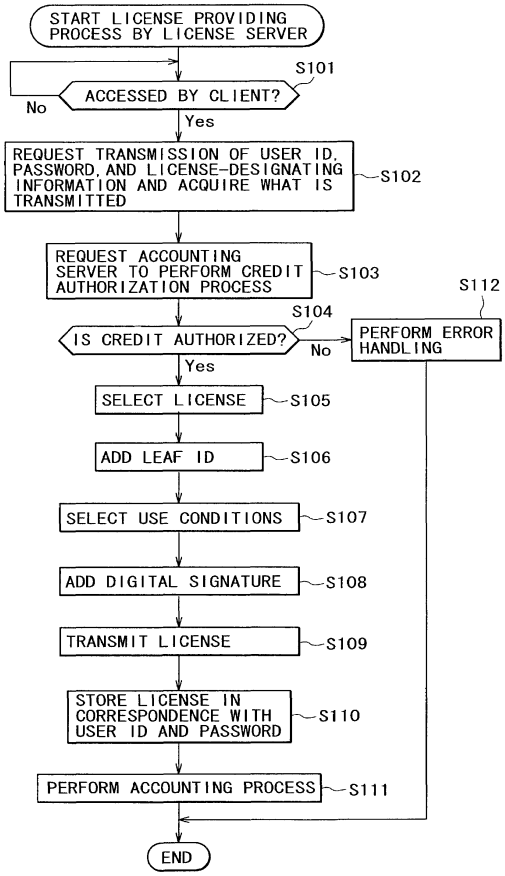
Bibliographic data

Publication date: 2008-09-16
Application date: 2003-05-13
Earliest priority date: 2001-03-29

Inventors: ISHIGURO RYUJI

CPC classification: G06F 17/00, G06F 21/10, H04L 2209/60, H04L 2463/101, H04L 63/062, H04L 63/0823, H04L 9/0825, H04L 9/083, H04L 9/3263
IPC classification: H04L 9/00, H04L 29/06, G06F 21/10

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

This invention relates to an information processing apparatus for permitting so-called grouping without recourse to group keys. A content server retains in advance certificates of devices subject to grouping. Each certificate contains a public key of the corresponding device. When providing a content, the content server authenticates the certificates of the grouped devices for which the content is destined (step S 281), encrypts a content key by use of public keys of the authenticated certificates (step S 283), and transmits the content key thus encrypted to each of the devices making up the group (step S 284) together with the content. The inventive apparatus is applied to devices that provide contents.

First claim

An information processing apparatus, comprising:
means for acquiring at least one certificate from each of a plurality of devices belonging to a group, each certificate including identification data allocated to a respective one of the plurality of grouped devices and a public key associated with the respective device;
means for storing each of the certificates as a certificate group directly corresponding to the group of devices;
means for authenticating the certificates for the group of devices when a content request from one of the plurality of devices is obtained by the acquiring means, including using tags based on leaf identifiers included in each of the certificates to trace associated enabling key blocks to eliminate any revoked certificates;
means for encrypting an encryption key using the public keys of each of the authenticated certificates from the plurality of grouped devices to obtain encrypted data composed of a set of encrypted encryption keys associated with each valid device in the group, the encryption key encrypting requested content; and
means for providing the encrypted requested content together with the encrypted encryption key to each of the valid devices in the group, wherein the encrypted requested content is configured to be decrypted by each of the devices

using a decrypted version of the encrypted encryption key.

84. Digital content preparation system

US6959288B1 | International Business Machines Corp

Bibliographic data

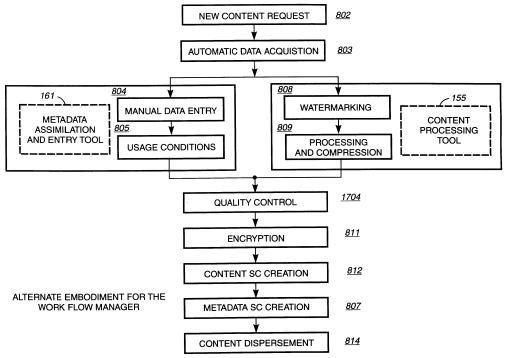
Publication date: 2005-10-25
Application date: 1999-02-01
Earliest priority date: 1998-08-13

Inventors: MEDINA CESAR, GONG QING, MILSTED KENNETH LOUIS

CPC classification: G06Q 20/3829, G06T 1/0021, G06T 2201/0064, H04L 2209/30, H04L 2209/56, H04L 2209/608, H04L 2463/101, H04L 63/0464, H04L 63/06, H04L 9/302, H04L 9/3249, H04L 9/3263

IPC classification: G06T 1/00, H04L 9/08, H04L 9/00, H04L 9/32, H04L 29/06, H04L 9/30

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

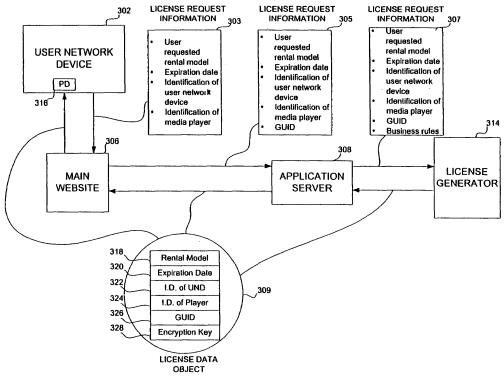
A digital content preparation system that includes a metadata acquisition tool for acquiring metadata associated with the digital content, and a digital content processor for processing the digital content by performing at least one of watermarking, encoding, and encrypting. A work flow manager manages processings by the metadata acquisition tool and the digital content processor. In one preferred embodiment, the metadata acquisition tool includes an automatic metadata acquisition tool and a manual metadata acquisition tool, and the digital content processor includes an encoder and an encrypter. The present invention also provides a method for preparing digital content. According to the method, metadata associated with the digital content is acquired, and the digital content is processed by at least one of watermarking, encoding, and encrypting. Processings in the acquiring step and the processing step are managed. In a preferred method, the acquiring step includes automatically retrieving at least a portion of the metadata and allowing manual entry of at least a portion of the metadata, and the processing step includes encoding the digital content and encrypting the encoded digital content.

First claim

A digital content preparation system comprising:
a metadata acquisition tool for acquiring metadata and content usage conditions, the metadata being associated with the digital content but not including the digital content itself; and
a digital content processor for processing the digital content to produce processed digital content, the digital content processor including at least one of a watermarker for watermarking the digital content, an encoder for encoding the digital content, and an encrypter for encrypting the digital content,
wherein the metadata acquisition tool includes an automatic metadata acquisition tool for automatically filling in at least some data fields of a metadata template by using a mapping table to retrieve the metadata for the data fields from a preexisting database, the mapping table mapping at least a portion of the data fields of the metadata template to locations within the database where the corresponding metadata can be found.

85. Secure digital content licensing system and method

US7155415B2 | Movielink LLC



Bibliographic data

Publication date: 2006-12-26
Application date: 2001-04-06
Earliest priority date: 2000-04-07

Inventors: RUSSELL CHRIS, OUTTEN TODD AVERY, SPAULDING BRYAN GENTRY, SHERR SCOTT JEFFREY, RUBENSTEIN IRA STEVEN, LANDAU YAIR, LAKAMP BRIAN DAVID, BARNETT JEREMY ELI, CHEY DOUGLAS DAISEUG, ARRIETA MICHAEL R, KORMAN MARY, MANDYAM HARISH, RODRIGUEZ THOMAS M, MOSSON ANDREW, BRODERSOHN ERNESTO, ABRAHAM MARY

CPC classification: G06F 21/10, G06F 2221/2137, G06Q 10/10, H04L 2209/603, H04L 2463/101, H04L 2463/102, H04L 63/0428, H04L 63/12, H04L 9/3268, H04L 9/3297
IPC classification: G06F 21/00, H04L 29/06, G06Q 10/10

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

Embodiments of the present invention overcome the problems in the existing art described above by providing a secure digital content licensing system and method. Rental of the digital content occurs within an online environment including one or more user network-enabled devices and one or more server network devices connected by a communications link to the one or more user network-enabled devices. A user selects content displayed on a main website and requests download of the selected content to the user network-enabled device. To be able to access the content the user must obtain a license. The user's request for a license for specific content comprises information about a desired rental model, an expiration date for the rental model, and information that identifies the user's user network-enabled device, along with other information. A license for the content is generated which comprises the above information and also includes an encryption key for the selected movie. Media player and security technology residing on the user network-enabled device provides protection against unauthorized access to the content by ensuring that only licensed content is viewed and is accessed according to the rental model contained in the license. Media player and security technology also provides security against tampering by performing integrity checks on its various components and other components within the user network-enabled device. Revocation of access rights is made possible by revocation certificates that inhibit accessing of particular content for various reasons including compromised files or components.

First claim

A system for secure licensing of content to a user on a user network-enabled device, the system comprising:
at least one server network device communicatively coupled to the user network-enabled device;
wherein the at least one server network device is programmed to transfer selected encrypted content to the user network-enabled device; and
a license generator, the license generator being programmed to generate an encrypted a license associated with the selected encrypted content, the encrypted license comprising
access information defining conditions for controlling the user network-enabled device, and
an encryption key to enable the user network-enabled device to produce a user-perceptible form of the selected encrypted content when the conditions defined by the access information conditions are met and to inhibit production of a user-perceptible form of the selected encrypted content when the conditions defined by the access information are not met; and
a root key for decrypting the encrypted license to allow the access information and the encryption key in the encrypted license to be accessed by a media player and security technology programmed on the user network-enabled device,

the media player and security technology controlling a specific media player on the user network-enabled device to produce the user-perceptible form of the selected encrypted content.

86. Content utilization apparatus, network system, and license information acquisition method

JP4177040B2 | Panasonic Corp, Matsushita Electric Industrial Co Ltd

Bibliographic data

Publication date: 2008-11-05
Application date: 2002-07-12
Earliest priority date: 2001-07-17

Inventors: 中原 徹, 中西 正典, 上坂 靖, 三浦 康史, 東 吾紀男, 難波 孝彰

CPC classification:
IPC classification: H04N 5/91, H04N 5/765, G06F 21/22, G06F 13/00, G06F 21/00, G06F 12/14, H04N 7/173, G06F 21/24, G06F 21/10, H04N 21/258, G06F 21/60, G06F 21/44, G06F 21/62, H04N 21/4367, H04N 21/4363, H04N 21/432, H04N 21/4623

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

(57) [Summary] [PROBLEMS] To provide a content use device, a network system, and a license information acquisition method for effectively utilizing license information already distributed from a server. A usage right management unit includes a usage right management unit that holds license information, and a content output unit that uses content based on the license information and outputs the content in at least one form of audio, video, and data. Upon receiving the license information request from the content output unit 1b, the unit 1a requests the license information from the use right management unit of another content using device and obtains the license information, and transmits the obtained license information to the content output unit. 1b, and the content output unit 1b The content is used based on the license information passed from a.

First claim

One content utilization device in a network system composed of a plurality of content utilization devices that are connected to each other via a communication network and use content that is a digital work,
Connected to a server that provides content and license information that enables the use of the content via a broadband network, or connected to another content usage device via a LAN or local line, and used for the server or the other content A right-of-use management means for acquiring the license information from a device and holding the license information;
Using content acquired from the server based on license information, and output means for outputting in at least one form of audio, video and data,
When the usage right management unit receives a request for license information from the output unit, the license information is transmitted to the server via the broadband network when the usage right management unit does not have the requested license information. Before requesting, the usage right management means of the other content utilization device holding the license information is searched via the LAN or local line, and the other content utilization device holding the license information is searched. Requesting and obtaining the license information, passing the obtained license information to the output means,
The content utilization apparatus, wherein the output unit uses content based on license information passed from the usage right management unit.

87. Data terminal equipment

JP3831596B2 | Sanyo Electric Co Ltd

Bibliographic data

Publication date: 2006-10-11
Application date: 2000-10-05
Earliest priority date: 2000-10-05

Inventors: 樋口 剛司

CPC classification:
IPC classification: H04M 3/42, G10L 19/00, H04M 3/493, H04M 11/08, G10K 15/02

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

PROBLEM TO BE SOLVED: To provide a data terminal device which is highly convenient to users. SOLUTION: A portable telephone 100 has a contents information holding section 1203 and a mail forming section 1226. The contents information holding section 1203 holds the contents information received through a signal transmission and reception section 1104. The mail forming section 1226 forms the contents mail added with the contents information holding section 1203 to the mail. A controller 1106 sends the contents mail formed by the mail forming section 1226 through the signal transmission and reception section 1104.

First claim

And interfaces, and a transmitting and receiving unit, and a key operation unit, and the additional information holding unit, and a data terminal device and a control unit,
Interface performs the data exchange with the data recording device,
Transceiver, the distribution server, and communicates with other data terminal equipment,
The key operation unit, and can input an instruction from the user,
Additional information holding unit, and capable of holding the additional information,
Additional information includes a content name, a content ID, the distribution server ID,
The control unit performs a normal distribution process, and the additional information transmitting process, and the additional information receiving process, the request processing,
The normal distribution process, and the encrypted content data transmitted from the distribution server in response to the distribution request, and the license, and receives the additional information, records the received encrypted content and the license to a data recording apparatus via the interface and is allowed, allowed to hold the received additional information to the additional information storage unit,
Additional information transmission process, to display the content name of the additional information stored in the additional information storage unit on the display means, the additional information corresponding to the instruction content name, and sends the other data terminal device is instructed,
Additional information reception processing, to hold the additional information received from the other data terminal equipment in the additional information holding section,
Request processing, to display the content name of the additional information received by the additional information receiving process on the display means, the content ID corresponding to the instruction content name, the distribution server of the distribution server ID corresponding to the instruction content name performing a distribution request of the encrypted content data is transmitted to the data terminal equipment.

88. License management server, license management system, and usage restriction control method

JP4294266B2 | Panasonic Corp, Matsushita Electric Industrial Co Ltd

Bibliographic data

Publication date: 2009-07-08
Application date: 2002-06-11
Earliest priority date: 2001-06-11

Inventors: 井上 光啓, 岡本 隆一

CPC classification:
IPC classification: G06F 1/00, G06Q 50/00, G06F 21/00, H04N 7/173, G06F 21/10, H04N 21/475, H04N 21/454, G06Q 30/06, G06Q 50/10, H04N 21/21, G06F 21/62

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

(57) [Summary] [Problem] To provide a parental control system capable of setting usage restrictions in accordance with the growth of a child. A rights management server is a server that manages use of contents in a parent terminal and a child terminal, and a contents use right database storing rights information indicating use conditions of contents for each user ID. Parental information, which is an instruction to restrict use of content by the child terminal 150 from the parent terminal 140, and stores the parental information management unit 118 in the parental information database 114. When the license ticket issuance request is acquired from the child terminal 150, the usage conditions indicated by the corresponding right information 400 include: Under usage conditions with restrictions indicated by parental information 600, A license ticket generation unit 117 that generates a license ticket, which is information indicating that the use is permitted, and transmits the generated license ticket to the child terminal 150.

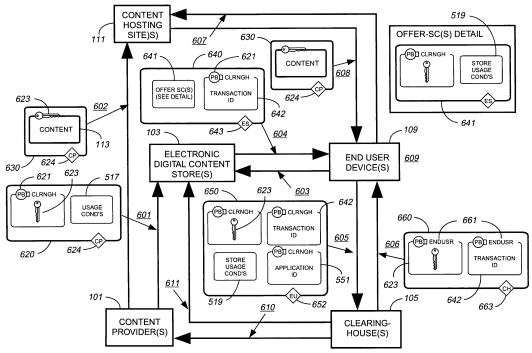
First claim

A license management server that manages the use of content in a terminal device,
License information storage means for storing license information indicating usage conditions of content for each terminal device or user;
An instruction to restrict the use of content by the second terminal device or the second user and use restriction information indicating the details of the restriction are acquired from the first terminal device or the first user, and the use restriction information is obtained. Usage restriction information management means for storing;
Payment information for specifying a payment method of each user when purchasing a license from the license management server is managed for the first terminal device or the first user and the second terminal device or the second user. Of the terminal device or user in which the same payment information is registered with the payment information management means, one terminal device or one user is the first terminal device or the first user.
Identification information management means for accepting registration of identification information for identifying the personal information storage means for storing personal information relating to the first user and the second user,
When an instruction to request the use of content is acquired from the second terminal device or the second user, the use condition indicated by the license information corresponding to the requested use stored in the license information storage unit is satisfied. Information indicating that the use of the content is permitted under a use condition to which a restriction indicated by the use restriction information corresponding to the second terminal device or the second user stored in the use restriction information management unit is added. Ticket issuing means for generating a license ticket and transmitting it to the second terminal device or the second user ;
The usage restriction information management means is configured to obtain the second terminal acquired from the first user when there is a certain relationship between the first user and the second user based on the personal information. Storing the use restriction information for the device or the second user;
The usage restriction information management means is configured to select the same payment information from among the terminal devices or users registered in accordance with a request from the first terminal device or the first user having the registered identification information. The second terminal device or the second user is registered, and the use restriction information is stored for the registered second terminal device or the second user.

License management server, wherein a call.

89. Updating usage conditions in lieu of download digital rights management protected content

US7487128B2 | International Business Machines Corp



Bibliographic data

Publication date: 2009-02-03
Application date: 2005-10-11
Earliest priority date: 1998-08-13

Inventors: SPAGNA RICHARD L, HURTADO MARCO M, RETTIG PAUL R, ZHAO TING

CPC classification: G06F 21/10, G06F 2211/007, G06F 2221/0708, G06F 2221/2107, G06F 2221/2135, G06Q 20/40, G06Q 30/00, G06T 1/0021, G06T 2201/0064, G11B 20/0021, G11B 20/00884, H04L 2463/101, H04L 2463/102, H04L 63/0428, H04L 69/04, H04L 69/329, H04W 4/02

IPC classification: G06F 1/00, H04K 1/00, G06T 1/00, H04L 29/08, H04L 9/00, G06F 21/00, H04L 29/06

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

A method on an end user system for creating additional copies onto at least one computer readable medium such as CDs, DVDs, ZipDisks™, tape, Flash memory, and RAM. The method comprising the steps of: receiving encrypted content with associated usage conditions and a first hash value; receiving a selection from an end user to create at least one copy of the encrypted content onto at least one computer readable medium; sending a request to an online electronic store of the encrypted content selected to be copied; receiving from the electronic store a description of the content selected to be copied along with a second hash value; and determining if the first hash value received is identical to the second hash value and if the first hash and the second hash value is identical authorizing the creating additional copies onto at least one computer readable medium.

First claim

A method on an end user system encoding watermarks with usage conditions of previously received encrypted digital content without receiving additional copies of the encrypted digital content, the method comprising:
sending to an electronic store a request from a user to acquire additional usage rights for encrypted digital content which has been previously received, wherein included with the encrypted digital content is:
at least one usage right;
a first watermark identifying a source of the encrypted digital content, wherein the first watermark includes transaction information and an identification of a clearing house which is separate from an identification of a store from which the encrypted digital content was purchased;
at least one watermarking instruction containing parameters and information for creating a second watermark on an end user system with transaction information to track each distribution of the encrypted digital content;
receiving from the electronic store a hash value which uniquely identifies the encrypted digital content associated with the request to acquire additional usage rights for the encrypted digital content;
comparing the hash value received from the electronic store with a previously stored hash value corresponding to the previously received encrypted digital content;
updating the usage conditions associated with the encrypted digital content in response to the hash value received from the electronic store matching the previously stored hash value, wherein the watermarking instruction has been updated by a clearing house which is separate from a store from which the encrypted digital content was purchased;
generating the second watermark, on the end user system, based upon the parameters and information in the watermarking instruction and the usage conditions which have been updated without re-receiving another copy of the encrypted digital content, wherein the generating the second watermark is performed in a tamper resistant environment so as to deter unauthorized access to the watermarking instruction;
applying the second watermark to the encrypted digital content so as to overwrite the first watermark;
decrypting the encrypted digital content with a first decrypting key;

reencrypting the digital content along with the second water mark with a second encryption key, wherein the second encrypting key is a symmetric key locally generated at the end user device.

90. PRODUCING A NEW BLACK BOX FOR A DIGITAL RIGHTS MANAGEMENT (DRM) SYSTEM

WO2001052471A1 | MICROSOFT CORP

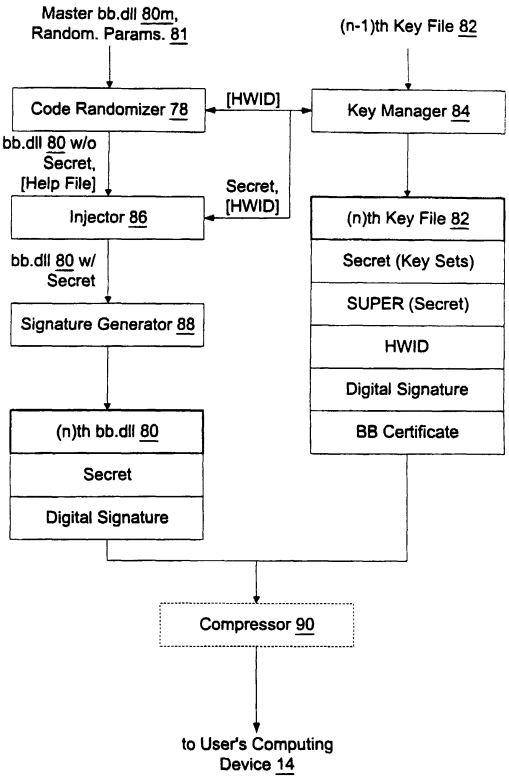
Bibliographic data

Publication date: 2001-07-19
Application date: 2000-08-22
Earliest priority date: 2000-01-14

Inventors: PEINADO MARCUS, VENKATESAN RAMARATHNAM, DAVIS MALCOLM

CPC classification: G06F 21/10
IPC classification: G06F 21/10

External links: Google Patents, Espacenet, EP Register, Patentscope, PatBase Express, PatBase, Orbit



Abstract

A new ((n)th) black box is produced for a digital rights management (DRM) system. The (n)th black box is for being installed in and for performing decryption and encryption functions in the DRM system. The (n)th black box is produced and delivered to the DRM system upon request and includes a new ((n)th) executable and a new ((n)th) key file (82). The (n)th key file (82) has a new ((n)th) set of black box keys and a number of old sets of black box keys. The request includes an old ((n-1)th) key file (82) having the old sets of black box keys. A code optimizer/randomizer (78) receives a master executable (80m) and randomized optimization parameters (81) as inputs and produces the (n)th executable as an output. A key manager (84) receives the (n-1)th key file (82) and the (n)th set of black box keys as inputs, extracts the old sets of black box keys from the (n-1)th key file (82), and produces the (n)th key file (82) including the (n)th set of black box keys and the old sets of black box keys as an output. The (n)th executable and the (n)th key file (82) are forwarded to the requesting DRM system.

First claim

An apparatus for producing a new ((n)th) black box for a digital rights management (DRM) system, the (n)th black box for being installed in the DRM system and for performing decryption and encryption functions in the DRM system, the (n)th black box being produced and delivered to the DRM system upon request therefrom and including a new ((n)th) executable and a new ((n)th) key file, the (n)th key file having a new ((n)th) set of black box keys and a number of old sets of black box keys, the request including an old ((n-l)th) key file having the old sets of black box keys, the apparatus comprising: a code optimizer / randomizer receiving a master executable and randomized optimization parameters as inputs and producing the (n)th executable as an output; and a key manager receiving the (n-l)th key file and the (n)th set of black box keys as input, extracting the old sets of black box keys from the (n-l)th key file, and producing the (n)th key file including the (n)th set of black box keys and the old sets of black box keys as an output; wherein the (n)th executable and the (n)th key file are to be forwarded to the requesting DRM system.

91. Method and system of preventing unauthorized rerecording of multimedia content

US20020107803A1 | International Business Machines Corp

Bibliographic data

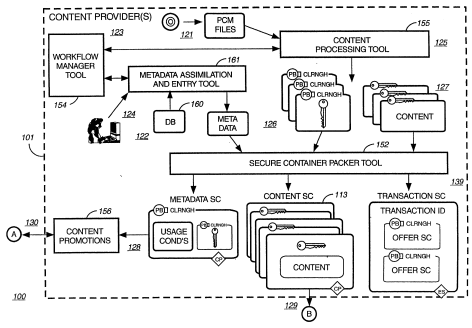
Publication date: 2002-08-08
Application date: 2001-08-23
Earliest priority date: 1998-08-13

Inventors: LISANKE MICHAEL G, MILSTED KENNETH L, NUSSER STEFAN, TANTLINGER BRUCE A, WILHELM GEORGE W

CPC classification: G06F 21/10, G06F 2211/007, G06F 2221/0708, G06F 2221/2107, G06F 2221/2135, G06T 1/0021, G06T 2201/0064, G11B 20/00173, G11B 20/0021, G11B 20/00224, G11B 20/0071, G11B 20/00753, G11B 20/00884, H04L 2463/101, H04L 2463/102, H04L 63/0428, H04L 69/04, H04L 69/329, H04W 4/02

IPC classification: G06F 1/00, G06T 1/00, G11B 20/00, H04L 29/08, G06F 21/00, H04L 29/06, G11B 20/10, G06F 21/24

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

A method, system and computer readable medium for the blocking of recording digital content at an end user multimedia end-user-system during the rendering of encrypted digital multimedia files. Before the process of rendering of encrypted digital multimedia can be started all rendered media stream during playback are opened to ensure that this multimedia content is not recorded. This blocks the usage of the devices and/or ports that can be used to store un-encrypted content that has been decrypted for the purposes of playing or rendering. The method also includes an exception, which allows recording with permission from the present invention.

First claim

A method on an end-user-system to prevent an unauthorized recording of multimedia content as a result of rendering of at least part of the multimedia content, the method comprising:
opening all multimedia content input devices and/or ports which are connected to an end-user-system that can receive at least a part of a multimedia content;
decrypting at least part of the multimedia content;
rendering the at least part of the multimedia content which has been decrypted.

92. Method and apparatus for uniquely identifying a customer purchase in an electronic distribution system

US6389403B1 | International Business Machines Corp

Bibliographic data

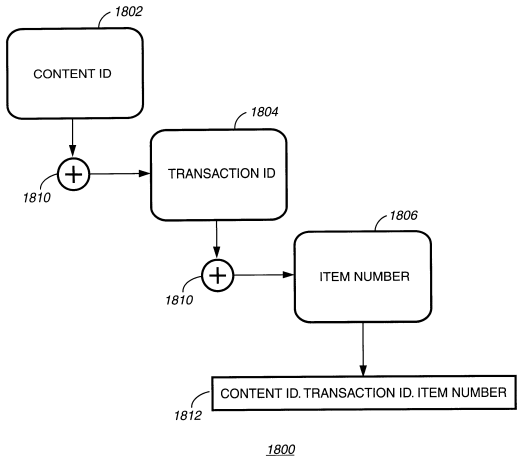
Publication date: 2002-05-14
Application date: 1999-09-17
Earliest priority date: 1998-08-13

Inventors: DORAK JR JOHN J

CPC classification: G06F 21/10, G06F 2221/0737, G06F 2221/0775, G06F 2221/0795, G06F 2221/2101, G06F 2221/2107, G06F 2221/2115, G06F 2221/2119, G06F 2221/2129, G06F 2221/2135, G06Q 30/06, G06Q 50/10, H04L 2463/101, H04L 2463/102, H04L 63/0428, H04N 21/266, H04N 21/8352

IPC classification: G06Q 30/00, G06F 1/00, H04L 29/08, H04L 9/08, G06F 13/00, G06F 21/00, H04L 29/06, G06F 12/14, H04N 7/167, H04N 7/173, G06F 21/06, G06F 21/24, H03M 7/30, H04N 7/08, G09C 1/00, H04L 9/10, H04N 7/081, G10K 15/02

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

A system for tracking usage of digital content on user devices. Content sites for distributing digital content over a computer readable medium to users. The content sites associate unique content identifier with the content associated. Electronic stores coupled to a network sell licenses to play digital content data to users. The licenses contain a unique transaction identifier for uniquely identifying the transaction, and the licenses contain a unique item identifier for uniquely identifying at least one item in the transaction. Content players, which receive from the network the licensed content data, are used to play the licensed content data. The content players produce a purchase identifier based upon the mathematical combination of the content identifier, the transaction identifier and the item identifier.

First claim

A method for uniquely identifying digital content on a digital content player wherein more than one piece of the identical digital content may be present, the digital content delivered to the digital content player over a telecommunications network or via computer readable medium, the method on the digital content player comprising the steps of:

receiving two or more pieces of identical digital content in an encrypted secured container;

receiving a first identifier which uniquely identifies the content received from a content provider;

receiving a second identifier which uniquely identifies a transaction by which the content was received;

receiving a third identifier for each piece of content received in the encrypted secured container, the third identifier based upon an item number or position number in the encrypted secured container for each piece of content received, so that if there are two or more pieces of identical content present in the encrypted secured container then a unique third identifier is assigned to each piece of content respectively;

producing a fourth unique identifier based upon a mathematical combination of the first identifier, the second identifier, and the third identifier;

associating the fourth unique identifier with each piece of digital content received so to uniquely identify each piece of content by the fourth identifier even when there are two or more pieces of identical content present in the encrypted secured container.

93. Distributing digital content

US20020077988A1 | Hewlett Packard Development Co LP

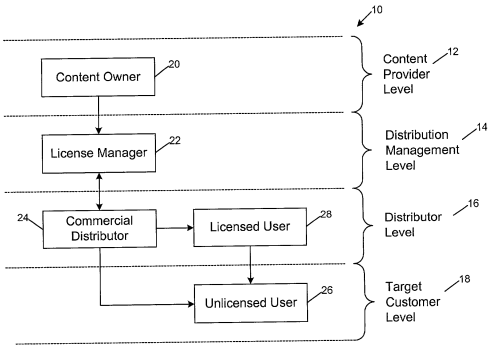
Bibliographic data

Publication date: 2002-06-20
Application date: 2000-12-19
Earliest priority date: 2000-12-19

Inventors: SASAKI GARY D, HANS MATHIEU C

CPC classification: G06F 21/10, G06F 2221/0742, G06F 2221/2101, G06F 2221/2117, G06Q 30/02
IPC classification: G06F 21/00, G06Q 30/02

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

Systems and methods of distributing digital content are described. In one aspect, a portable media device includes a memory, a wireless transceiver, an output, and a controller. The memory is configured to store digital content. The wireless transceiver is configured to wirelessly transmit and receive digital content. The output is configured to render digital content. The controller is coupled to the memory, the wireless transceiver and the output, and is configured to control wireless transmission of digital content based upon meta-data associated with the digital content. In another aspect, a digital content distribution system includes two or more portable media devices and a license manager. Each of the portable media devices comprises a memory for storing digital content and a transceiver for wirelessly transmitting digital content to and wirelessly receiving digital content from another portable media device. The license manager is configured to associate digital content with meta-data for controlling wireless transmission and rendering of digital content from one portable media device to another. A content tracking and incentives system that encourages commercial distributors, broadcasters and users to distribute digital content to new potential customers also is described.

First claim

A portable media device, comprising:
a memory configured to store digital content;
a wireless transceiver configured to wirelessly transmit and receive digital content;
an output configured to render digital content; and
a controller coupled to the memory, the wireless transceiver and the output, the controller being configured to control wireless transmission and rendering of digital content based upon meta-data associated with the digital content.

94. Data management apparatus, data management method, and record medium recording data management program

EP1045387B1 | Matsushita Electric Industrial Co Ltd

Bibliographic data

Publication date: 2007-01-17
Application date: 2000-04-13
Earliest priority date: 1999-04-14

Inventors: SYODA YUKIE, KOZUKA MASAYUKI, HIRATA NOBORU, OHTANI YUKAKO

CPC classification: G06F 21/10, G06F 2211/007, G06F 2221/0777, G11B 20/00181, G11B 20/0021, G11B 20/00528, G11B 20/00666, G11B 20/0084, G11B 2220/2545, G11B 2220/2562
IPC classification: G06F 1/00, G11B 20/00, G06F 21/10

External links: Google Patents, Espacenet, EP Register, PatBase Express, PatBase, Orbit

Abstract

The data type identification unit 103 obtains a circulation content from an external source or obtains a not encrypted content from a record medium. When the obtained content has the CD type, the data registration unit 104 encrypts the obtained content and writes the encrypted content to the data storage unit 106. The data registration unit 104 obtains the rights information from the rights management table 102, writes the data ID, encryption information, rights information, and file name to the data management table 105, and writes the encryption information and the rights information to the data storage unit 106. When the obtained content is a circulation content, the data registration unit 104 writes the circulation content to the data storage unit 106, and writes the data ID, encryption information, rights information, and file name to the data management table 105.

First claim

A data management apparatus for managing digital contents distributed in a market, with corresponding rights information, the data management apparatus comprising:
a rights information storage means (102; 803) for prestoring a separate piece of rights information for each type of digital content, each piece of rights information including play rights information indicating whether reproduction is permitted for contents of the type corresponding to the piece of play rights information;
a content storage means (106; 805);
a content obtaining means for obtaining a digital content from one of a plurality of external sources via one of a plurality of routes (158, 159) respectively corresponding to the plurality of external sources, wherein each route (158, 159) determines whether rights information has been added to digital contents thereon;
a protection judging means for judging, based on the particular route (158, 159) via which the digital content is obtained, whether rights information has been added to the obtained digital content;
a type identification means (103; 801) for identifying a type of the obtained digital content if the protection judging means has judged that rights information has not been added to the obtained digital content;
a rights information reading means for reading rights information from the rights information storage means (102; 803) that corresponds to the type of the obtained digital content;
a content writing means (104; 802, 804) for writing the obtained digital content to the content storage means (106; 805); and
a rights information writing means for writing the read rights information to the content storage means (106; 805) so as to correspond to digital content written by the content writing means (104; 802, 804).

95. Recording method and recording apparatus

JP3793220B2 | Toshiba Corp

Bibliographic data

Publication date: 2006-07-05
Application date: 2005-05-10
Earliest priority date: 1997-05-13

Inventors: 上林 達, 秋山 浩一郎, 辻本 修一, 住田 一男, 平川 秀樹, 菅谷 寿鴻, 梶浦 正浩

CPC classification:
IPC classification: G06Q 50/00, G06F 12/14, G09C 1/00, G06F 21/10, G06Q 30/06, G06Q 50/10, G06F 21/60, G06F 21/62

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

Abstract

[PROBLEMS] Distributing digitized works distributed via a network or a recording medium quickly and easily, and facilitating the use environment of digital information on the premise of copyright protection by charging for the use of digital information. To build. A medium for acquiring first license information used for using content information recorded on a first recording medium, and identifying the second recording medium from a second recording medium The second license information is generated by reading the ID, erasing or rewriting the usage conditions included in the first license information, and writing the media ID, and this second license information is stored in the second recording medium. Record. [Selection] Figure 45

First claim

From the first recording medium for recording the content information, a first reading means for reading a media ID for identifying the first recording medium,
Generating means for generating a first license information that is used to utilize the content information,
At least a recording means for recording the first license information generated by said generating means to said first recording medium,
A recording method in a recording apparatus including,
Wherein the first readout means, from the first recording medium, a first step of reading a media ID for identifying the first recording medium,
The generating means, a second step of obtaining the second license information used in order to use the content information recorded on the second recording medium,
The generating means, erase or rewrite the usage conditions included in the second license information acquired in the second step, the first by writing the media ID read in the first step and a third step of generating the license information,
A fourth step of said recording means, for recording the first license information generated by the third step on the first recording medium,
Recording method is characterized in that it has.

96. DATA TERMINAL EQUIPMENT AND DATA RE-ACQUIRING METHOD

JP2003016288A | Sanyo Electric Co Ltd

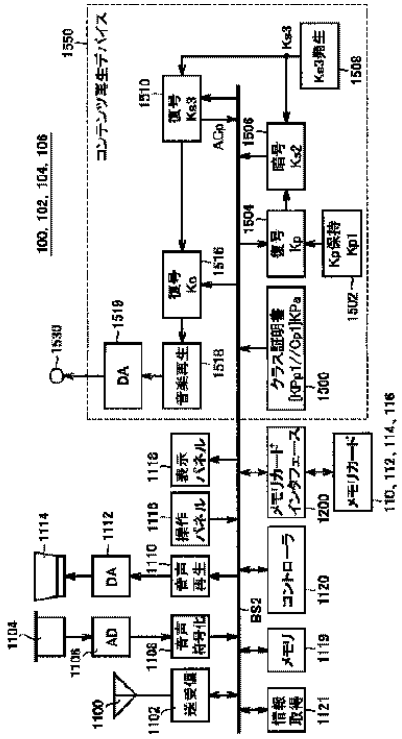
Bibliographic data

Publication date: 2003-01-17
Application date: 2001-06-29
Earliest priority date: 2001-06-29

Inventors: HIGUCHI GOJI

CPC classification:
IPC classification: G06Q 10/00, G06Q 50/00, H04L 9/08, G06F 12/14, G06F 21/10, G06Q 30/06, G06Q 50/10, G10K 15/02

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

(57) [Summary] [PROBLEMS] To provide a data terminal device and a data reacquisition method capable of easily reacquiring previously received content data by a data terminal device that has received copied content data. SOLUTION: A memory 1119 stores a database in which information on a copy source is registered. Mobile phone 102 When the request for reacquisition of the copied content data is input via the operation panel 1116, the controller 1120 of the controller 1120 accesses the mobile phone 100 as the copy source based on the information on the copy source stored in the memory 1119, When copying of the content data is permitted in the mobile phone 100, the content data is transferred to the mobile phone 10 Re-acquire from 0.

First claim

A data terminal device for receiving data including duplicated content data, additional information of the content data, and unique information of a duplication source of the content data, and managing information on the duplication source. An interface for exchanging data with a data recording device for recording the content data, a transmitting / receiving means for exchanging data with the outside, an information managing means for managing information about the copy source, An acquisition unit that acquires the content data, the unique information, and the additional information; and a control unit, and when the control unit receives the data via the transmission / reception unit, the received data is transmitted to the acquisition unit. The content data acquired by the acquisition means via the interface. A data terminal device, which records the data in a data recording device and stores the unique information and the additional information acquired by the acquisition means in the information management means as information about the copy source.

97. Method for obtaining a black box for performing decryption and encryption functions in a digital rights management (DRM) system

US7051005B1 | Microsoft Corp

Bibliographic data

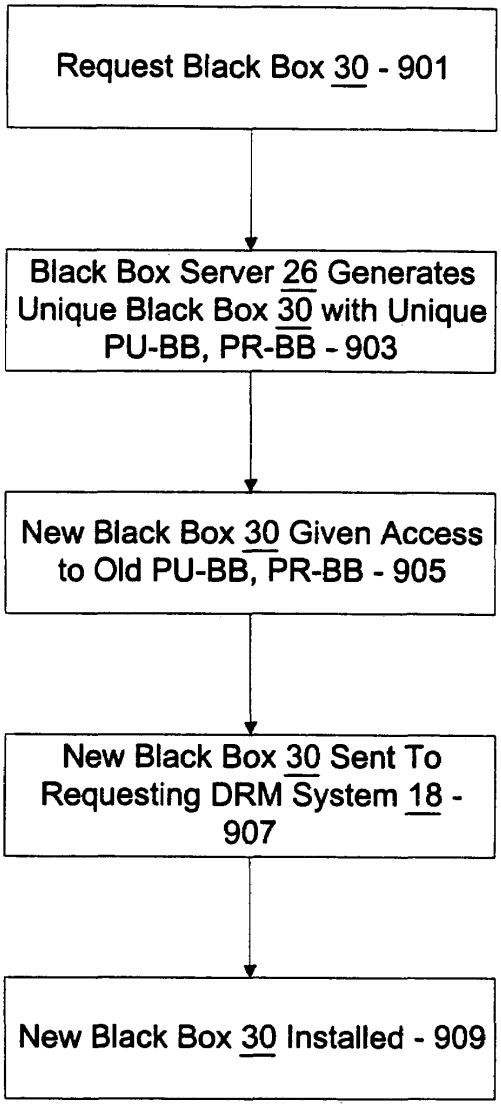
Publication date: 2006-05-23
Application date: 2000-01-13
Earliest priority date: 1999-03-27

Inventors: PEINADO MARCUS, ABBURI RAJASEKHAR, BLINN ARNOLD N, JONES THOMAS C, MANFERDELLI JOHN L, BELL JEFFREY R C, VENKATESAN RAMARANTHNAM, ENGLAND PAUL, JAKUBOWSKI MARIUSZ H, YU HAI YING VINCENT

CPC classification: G06F 21/10, G06F 21/71, G06F 21/84, G06F 2211/007, G06F 2221/0704, G06F 2221/0797, G06F 2221/2105, G06F 2221/2137, G06Q 30/06, G06Q 50/188, G07F 9/002, H04L 2463/101, H04L 63/0442, H04L 63/068, H04L 63/0823, H04L 63/12

IPC classification: G06F 1/00, G06F 21/00, H04L 29/06, G06Q 30/06, G06Q 50/18

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

A digital rights management (DRM) system operates on a computing device and requires a black box for performing decryption and encryption functions. To obtain the black box from a black box server, the DRM system requests such black box from such black box server. The black box server in response generates the black box, where such black box is unique and has a public/private key pair. The black box server then delivers the generated black box to the DRM system and the DRM system installs the delivered black box in such DRM system.

First claim

In combination with a digital rights management (DRM) system operating on a computing device, the DRM system requiring a black box for performing decryption and encryption functions, a method of obtaining the black box by the DRM system from a black box server, the method comprising:
requesting, by the DRM system, a first black box from the black box, server;
generating, by the black box server, the first black box, such generated first black box being unique and having a public/private key pair and electronic code for employing the key pair within the DRM system on the computing device;
delivering, by the black box server, the generated first black box to the DRM system; and
installing, by the DRM system, the delivered first black box in such DRM system,

the DRM system further providing code for periodically determining whether the first black box is current or not current and for upgrading at least the public/private key pair in the first black box from the black box server to result in a second black box when the first black box is not current.

98. Information processing apparatus

US20030159033A1 | Sony Corp

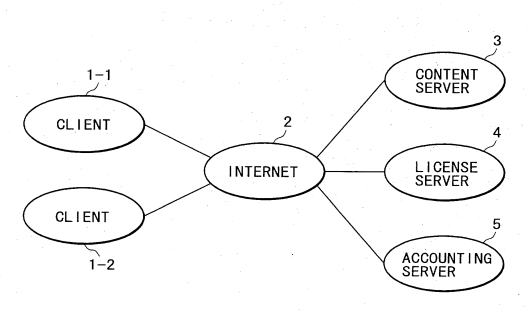
Bibliographic data

Publication date: 2003-08-21
Application date: 2003-04-09
Earliest priority date: 2001-03-29

Inventors: ISHIGURO RYUJI

CPC classification: G06F 21/10, G06F 2221/2135, G06F 2221/2137, H04L 2209/60, H04L 9/0822, H04L 9/0836, H04L 9/0891
IPC classification: G06F 1/00, G06F 21/10

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit



Abstract

A license server offering a content decryption key assigns leaves of a key-managed hierarchical tree structure to clients, and generates a set of node keys as a device node key for transmission to each client together with a leaf ID and a private key of the client in question. When an intermediate node of the tree structure is deemed to be the top, all nodes subordinate to the top are established as nodes related to a category defined for the top node. In this setup, a manufacturer, a content provider, or like entity managing the top node assigned the category generates uniquely an enabling key block that defines the node in question as the top, and distributes the enabling key block to devices belonging to nodes subordinate to the top node. The scheme allows the managing entity to renew the key without affecting devices belonging to any other category.

First claim

An information processing apparatus for providing a device node key used to decrypt an enabling key block included in a content, said information processing apparatus comprising:
assigning means which, in a key-managed hierarchical tree structure having a content provision category assigned to a first node on a given level of the structure, assigns uniquely a second information processing apparatus to a leaf subordinate to said first node; and
providing means for providing said second information processing apparatus with said device node key corresponding to a path between said leaf assigned by said assigning means and said first node.

99. Secure electronic content distribution on CDS and DVDs

US6611812B2 | International Business Machines Corp

Bibliographic data

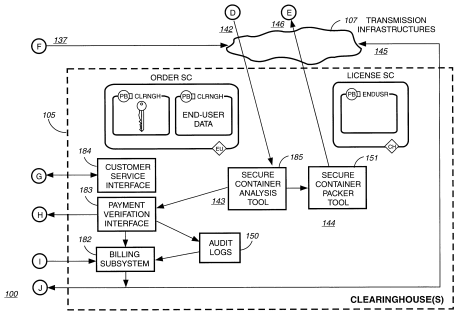
Publication date: 2003-08-26
Application date: 1999-08-17
Earliest priority date: 1998-08-13

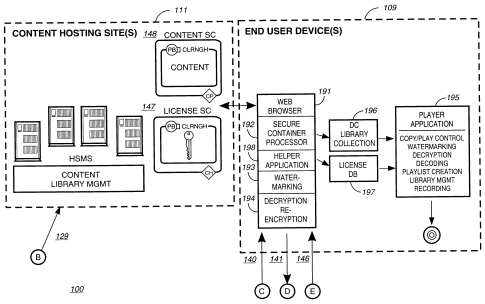
Inventors: HURTADO MARCO M, MILSTED KENNETH L, GRUSE GEORGE G, DOWNS EDGAR, LEHMAN CHRISTOPHER T, SPAGNA RICHARD L, LOTSPIECH JEFFREY B

CPC classification: G06F 15/00, G06F 21/10, G06F 2211/007, G06F 2221/0737, G06F 2221/2107, G06F 2221/2135, G06Q 20/3821, G06Q 20/401, H04L 2463/101, H04L 2463/102, H04L 63/0428, H04L 69/04, H04L 69/329, H04W 4/02

IPC classification: G06F 15/00, G06F 1/00, G06T 1/00, H04L 29/08, H04L 9/08, G06F 21/00, H04L 29/06, H04N 7/167, H04N 7/173, G06F 21/24, H03M 7/30, G09C 1/00, H04L 9/10, G06Q 20/40, G06Q 20/38, G10K 15/02

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit





Abstract

A method to delivery encrypted digital content to a end user system for playing the content comprising the steps of: reading from a computer readable medium metadata which has previously associated with the content. A user selects from the metadata associated content to decrypt and the end user system establishes a secure connection with an authorization authority for decrypting the content. The end user system receives a secure container containing the decrypting key for decrypting at least part of the previously encrypted content as permitted. The system creates a secure container using the encrypting key from a clearing house, wherein the secure container has an encrypting key therein from the end user system; transferring the secure container to the clearing house for authentication of permission to decrypt the content. The system receives from the clearing house, a secure container encrypted using the encrypting key of the end user system containing the decrypting key for decrypting at least part of the previously encrypted content stored on the computer readable medium as permitted; and playing at least part of the previously encrypted content by decrypting the secure container using the encrypting key of the end user system to access the decrypting key for decrypting at least part of the encrypted content.

First claim

A method to deliver encrypted digital content to a system for rendering the content, the method on the end user system comprising the steps of:
reading from a computer readable medium metadata which has previously associated with encrypted content, wherein the computer readable medium is coupled to the end user system;
selecting from the metadata the encrypted content to decrypt;
establishing a secure transmission between the end user system and an authorization authority for authorizing the decrypting of at least part of the encrypted content;
transferring, from the end user system, an end user system encrypting key and a content decrypting key stored on the computer readable medium which is encrypted, to the clearing house for authentication of permission to decrypt at least part of the content;
receiving from a clearing house a content decrypting key which has been encrypted with an end user system encrypting key, so that when content decrypting key is decrypted with the a end user system decrypting key corresponding to the end user system encrypting key, the content decrypting key is no longer encrypted and is usable for decrypting at least part of the encrypted content stored on the computer readable medium, wherein the decrypting of the encrypted content is performed in a tamper-resistant environment for deterring unauthorized access to the content decrypting key.

100. Information transaction system

US7124443B2 | Sony Corp

Bibliographic data

Publication date: 2006-10-17
Application date: 2001-10-12
Earliest priority date: 2000-02-15

Inventors: ISHIBASHI YOSHIHITO, SHIRAI TAIZO

CPC classification: G06Q 20/04, G06Q 20/1235, G11B 20/00123, G11B 20/0021, G11B 20/00731, H04L 2463/101, H04L 2463/102, H04L 63/0442, H04L 63/0464, H04L 63/123

IPC classification: G06Q 10/00, G06Q 50/00, G06F 15/18, G11B 20/00, G06F 11/00, G06F 11/30, H04L 9/08, H04L 9/32, G06F 12/16, G06F 21/00, H04L 29/06, G06F 12/14, G06F 11/36, G06F 11/34, G06F 11/22, G06F 11/32, G07F 7/08, G07F 17/00, G09C 1/00, G06F 21/10, G06Q 30/06, G06F 21/44, G06F 21/64, G06F 21/62, G06F 21/33

External links: Google Patents, Espacenet, PatBase Express, PatBase, Orbit

CONTENTS ID	SERIAL NUMBER	NUMBER OF TIMES OF SALE	PURCHASER INFORMATION	USER DISCRIMINATION DATA	USER EQUIPMENT DISCRIMINATION DATA	OTHERS
01234567	0000123	0				REPRINT IMPOSSIBLE
01234567	0000124	0				REPRINT IMPOSSIBLE
99999999	0000125	1	ACD22222	BCD38432	ABA23255	REPRINT POSSIBLE
99999999	0000126	2	BBF33333	BBB28756	BBC37854	REPRINT POSSIBLE
22222222	0000127	5	CBD36578	CDA15683	BBA36529	MAX NUMBER OF TIMES OF SALE N
22222222	0000128	N-1	BDD28215	ABB19653	CBB35532	MAX NUMBER OF TIMES OF SALE N

Abstract

A content use rights discrimination card corresponding to encrypted content is sold to a user. The user transmits data recorded on the content use rights discrimination card to a content use rights management center. The content use rights management center then verifies the content and the card, based on data in the received content use rights discrimination card, to encrypt a decoding key for decoding the content together with, for example, a session key, to transmit the encrypted content key to the user. The content use rights discrimination card, when sold to the user, can be set for enabling resale and transferred between different users so that the decoding key can be transmitted plural times from the content use rights management center. This procedure enables content to be utilized without executing any on-line settlement processing.

First claim

A method of obtaining a decoding key for decoding encrypted content, said method comprising:
acquiring, by a second content user from a first content user, a medium on which identification data, the encrypted content, and possibility of resale information are recorded, the first content user having previously accessed and decoded the encrypted content at a first user terminal associated with the first content user;
transmitting the identification data and the possibility of resale information to a content use rights management center using a second user terminal associated with the second content user;
receiving, from the content use rights management center using the second user terminal, a decoding key based on the transmitted identification data when the content use rights management center determines based on the transmitted possibility of resale information that the content use rights may be sold;
decoding, using the second user terminal, the encrypted content using the decoding key.