

SPECIFICATION

SYSTEM FOR PREVENTING UNAUTHORIZED USE OF DIGITAL CONTENT

TECHNICAL FIELD

The present invention relates to a system for preventing unauthorized play of digital content which can prevent unauthorized use of digital content distributed/delivered to a user via a recording medium such as a CD or a DVD, the Internet line and a telephone line.

BACKGROUND ART

As such prior art example, the following system is proposed. Basically, the system has: a distributing recording medium such as a CD-ROM on which encrypted digital content are recorded; management means for managing a charge for use of the digital content of a user; and a digital content playing device which is a device used for playing the digital content by the user who has obtained the distributing recording medium and can be connected via the Internet line to the management means, wherein when a request to play the digital content under authentication and charging conditions is inputted by the user to the digital content playing device, the digital content playing device transmits the request via the Internet line to the management means, the management means checks authentication and charging

of the user related to the request to transmit decryption key data via the Internet line to the digital content playing device, and the digital content playing device uses the decryption key data to decrypt and play the digital content on the distributing recording medium (for example, see Patent Document 1). "Patent Document 1: Japanese Patent Application Laid-Open No. 2002-334172"

In the above prior art example, however, when the digital content on the distributing recording medium are once decrypted by the digital content playing device, the digital content can be not only played but also easily copied. There is an essential disadvantage that secondary unauthorized use cannot be prevented.

Although addition of a function of automatically deleting the digital content when a predetermined period has elapsed from the play request can at least prevent the secondary unauthorized use, there is another disadvantage that collection of a charge for the secondary use cannot be expected. This is not a specific problem faced only when distributing the digital content via the distributing recording medium to the user, and is alike when delivering the digital content via the Internet line to the user. The advantage to be originally obtained by such as a content holder is lost in an unauthorized manner. In this point, under the current circumstances, the distribution of the digital content is prevented from being promoted.

The present invention has been made under the above background and an object of the present invention is to provide a system for preventing unauthorized use of digital content which can prevent unauthorized use of digital content and can reliably collect a charge for secondary use.

DISCLOSURE OF THE INVENTION

To solve the above problems, a first system for preventing unauthorized use of digital content according to the present invention has: a distributing recording medium which is a recording medium on which a content file having header information and a data body is recorded and lacks part of the header information to prevent unauthorized play and unauthorized copy of the data body; management means which is means managing use of the content file on the distributing recording medium and can transfer the prepared part of the header information as piece data via a communication line; and a digital content playing device which is a device used for at least playing the content file on the distributing recording medium and has a function of communicating via the communication line with the management means, wherein when a request to play the content file under authentication and charging conditions is inputted by a user to the digital content playing device, the digital content playing device transfers the request via the communication line to the management means, the management means

checks authentication and charging of the user related to the request to transfer the piece data via the communication line to the digital content playing device, and the digital content playing device uses the header information on the distributing recording medium and the piece data only in play operation to play the data body on the distributing recording medium.

Alternatively, the first system for preventing unauthorized use of digital content has: a distributing recording medium on which a content file having header information and a data body is recorded in a state of lacking at least part of the header information (that is, play information indispensable for playing the data body included in the header information); management means which is means managing use of the content file on the distributing recording medium and can transmit the prepared part of the header information as piece data via a communication line; and a digital content playing device which is a device used for at least playing the content file on the distributing recording medium and has a function of communicating via the communication line with the management means, wherein when a request to play the content file is inputted by a user to the digital content playing device, the digital content playing device transmits the request via the communication line to the management means, the management means checks authentication of the user related to the request to transmit the piece data of the content file related to the request via

the communication line to the digital content playing device, and the digital content playing device uses the header information on the distributing recording medium and the piece data in play operation to play the data body on the distributing recording medium. In this case, the request to play the content file by the user is desirably made under an authentication and/or charging condition of the user.

A distributing recording medium fabrication device used for the system for preventing unauthorized play of digital content used for the first system for preventing unauthorized use of digital content separates piece data from a content file having header information and a data body for recording and records the content file separated from the piece data on a set recording medium to create a distributing recording medium.

A digital content playing device used for the first system for preventing unauthorized play of digital content has functions of: when a request to play a content file under an authentication condition is inputted by the user, transmitting the request via the communication line to the management means; and thereafter, when piece data is transmitted from the management means via the communication line, using the header information on the distributing recording medium and the piece data in play operation to play the data body on the distributing recording medium. Playing software used for the first system for preventing unauthorized play of digital content is alike.

A second system for preventing unauthorized use of digital content according to the present invention has: delivery management means delivering a content file having header information and a data body via a communication line and managing use of the data body; and a digital content playing device capable of communicating via the communication line with the delivery management means and used for at least playing the content file delivered from the delivery management means, wherein when a request to download the content file is inputted by a user to the digital content playing device, the digital content playing device transfers the request via the communication line to the delivery management means, and the delivery management means transfers the content file related to the request via the communication line to the digital content playing device by lacking part of the header information to prevent unauthorized play and unauthorized copy thereof, thereafter, when a request to play the content file under authentication and charging conditions is inputted by the user to the digital content playing device, the digital content playing device transfers the request via the communication line to the delivery management means, the delivery management means checks authentication and charging of the user related to the request to transfer the prepared part of the header information as piece data via the communication line to the digital content playing device, and the digital content playing device uses the header information of the

transferred content file and the piece data only in play operation to play the data body of the content file.

Alternatively, the second system for preventing unauthorized use of digital content has: delivery management means which is a server in which a content file having header information and a data body is prepared in a state of lacking part of the header information (that is, play information indispensable for playing the data body included in the header information) and the part of the header information is prepared as piece data, delivers the content file via a communication line, and manages use of the data body; and a digital content playing device capable of communicating via the communication line with the delivery management means and used for at least playing the content file delivered from the delivery management means, wherein when a request to download the content file is inputted by a user to the digital content playing device, the digital content playing device transmits the request via the communication line to the delivery management means, and the delivery management means transmits the content file related to the request via the communication line to the digital content playing device, thereafter, when a request to play the content file is inputted by the user to the digital content playing device, the digital content playing device transmits the request via the communication line to the delivery management means, the delivery management means checks authentication of the user

related to the request to transmit the piece data of the content file related to the request via the communication line to the digital content playing device, and the digital content playing device uses the header information of the transmitted content file and the piece data in play operation to play the data body of the content file. In this case, the request to play the content file by the user is desirably made under an authentication and/or charging condition of the user.

A digital content playing device used for the second system for preventing unauthorized play of digital content has functions of: when a request to download a content file is inputted by the user, transmitting the request via the communication line to the delivery management means; after the content file is transmitted from the delivery management means, when a request to play the content file under an authentication condition is inputted by the user, transmitting the request via the communication line to the delivery management means; and thereafter, when piece data is transmitted from the delivery management means via the communication line, using the header information of the transmitted content file and the piece data in play operation to play the data body of the content file. Playing software used for the second system for preventing unauthorized play of digital content of the present invention is alike.

In the first or second system for preventing unauthorized

play of digital content of the present invention, preferably, when the playing software is prepared in the management means or the delivery management means, and when a request to download the playing software is inputted by the user to the digital content playing device, the digital content playing device transmits the request via the communication line to the management means or the delivery management means, the management means or the delivery management means transmits the playing software related to the request via the communication line to the digital content playing device, and the digital content playing device downloads the playing software.

The digital content playing device desirably has functions of: determining an elapsed period from the point of time at which piece data is transmitted from the management means or the delivery management means; and when the elapsed period reaches a predetermined period, deleting the transmitted piece data. Playing software is desirably alike. The digital content playing device can also have functions of: determining an elapsed time from the point of time at which, aside from piece data, a content file is transmitted from the delivery management means; and when the elapsed period reaches a predetermined period, deleting the transmitted content file.

In a digital content unauthorized play prevention method of the present invention, provided that to prevent unauthorized play and unauthorized copy of a data body of a content file having

header information and the data body in a digital content playing device, part of the header information is lacked from the content file, and that the part of the header information is prepared as piece data in management means which is means managing use of the content file in the device and communicable via a communication line with the device, when a request to play the content file under authentication and charging conditions is inputted by a user to the device, the device transfers the request via the communication line to the management means, the management means checks authentication and charging of the user related to the request to transfer the piece data via the communication line to the device, and the device uses the header information of the content file and the piece data only in play operation to play the data body of the content file.

Alternatively, in the digital content unauthorized play prevention method, provided that to prevent unauthorized play of a data body of a content file having header information and the data body in a digital content playing device, part of the header information is lacked from the content file, and that the part of the header information is prepared as piece data in management means which is means managing use of the content file in the device and communicable via a communication line with the device, when a request to play the content file under an authentication condition is inputted by a user to the device, the device transmits the request via the communication line to

the management means, the management means checks authentication of the user related to the request to transmit the piece data on the content file related to the request via the communication line to the device, and the device uses the header information of the content file and the piece data in play operation to play the data body of the content file.

EFFECT OF THE INVENTION

In the system for preventing unauthorized play of digital contents according to claims 1 and 2 of the present invention, a content file is recorded on a distributing recording medium in a state of lacking part of header information. Unless there is piece data as the part of the header information, the data body of the content file cannot be played. Unless play operation is authorized, the data body of the content file cannot be played. Therefore, it is possible to prevent unauthorized use of digital content and to reliably collect a charge for secondary use. The advantage to be originally obtained by such as a content holder can be secured. In this point, the distribution of digital content can be promoted.

In the distributing recording medium fabrication device according to claim 3 of the present invention, part of header information is separated as piece data from a content file for recording on a recording medium, thereby creating a distributing recording medium. It has the merit of preventing unauthorized

use of digital content.

In the digital content playing device according to claim 4 and the playing software according to claim 5 of the present invention, a request to play a content file is transmitted to management means, and only upon reception of the piece data transmitted from the management means, the data body of the content file is played. Therefore, unauthorized use of digital content can be prevented.

In the system for preventing unauthorized play of digital contents according to claims 6 and 7 of the present invention, a content file in a state of lacking part of header information and piece data as the lacked part of the header information are prepared in delivery management means. Unless the piece data is obtained by an authorized play request, a data body of the content file cannot be played. Therefore, it is possible to prevent unauthorized use of digital content and to reliably collect a charge for secondary use. The advantage to be originally obtained by such as a content holder can be secured. In this point, the distribution of digital content can be promoted.

In the digital content playing device according to claim 8 and the playing software according to claim 9 of the present invention, a request to play a content file is transmitted to delivery management means, and only upon reception of the piece data transmitted from the management means, the data body of

the content file is played. Therefore, it is possible to prevent unauthorized use of digital content.

In the system for preventing unauthorized play of digital content according to claim 10 of the present invention, when a predetermined period is reached from the point of time at which piece data is transmitted from the management means or delivery management means, the transmitted piece data is deleted. Unauthorized secondary use can be prevented.

In the digital content playing device according to claim 11 and the playing software according to claim 12 of the present invention, the same effect as that of claim 10 can be obtained.

In the system for preventing unauthorized play of digital content according to claim 13 of the present invention, the same effect as that of the unauthorized play prevention system according to claim 1, 2, 6 or 7 can be obtained.

In the digital content unauthorized play prevention method according to claim 14 of the present invention, the same effect as that of the unauthorized play prevention system according to claim 1 or 6 can be obtained.

In the system for preventing unauthorized play of digital content according to claim 15 of the present invention, a request to play a content file by a user is made under an authentication and/or charging condition of the user. Therefore, unless authentication and/or charging of the user is completed, the play request cannot be accepted. It is difficult to obtain piece

data for an unauthorized purpose.

In the system for preventing unauthorized play of digital content according to claim 16, the digital content playing device used for the system according to claim 17, and the playing software used for the system according to claim 18 of the present invention, an elapsed period is determined from the point of time at which, aside from piece data, a content file is transmitted from the delivery management means, and when the elapsed period reaches a predetermined period, the transmitted content file is deleted. The data body of the content file can be prevented from being recorded into the digital content playing device of the user beyond a predetermined period. There is the merit of preventing the data body of the content file from being copied for an unauthorized purpose.

In the digital content unauthorized play prevention method according to claim 19 of the present invention, the same effect as that of the unauthorized play prevention system according to claim 2 or 7 can be obtained.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a diagram for explaining a first embodiment of the present invention, being a block diagram of a system for preventing unauthorized play of digital content, including a block diagram of a distributing recording medium fabrication device used for the system.

FIG. 2 is a flowchart of playing software used for the system.

FIG. 3 is a flowchart of recording medium creating software executed by a computer as the distributing recording medium fabrication device used for the system.

FIG. 4 is a diagram for explaining a second embodiment of the present invention, being a block diagram of a system for preventing unauthorized play of digital content, including a block diagram of a distributing recording medium fabrication device used for the system.

FIG. 5 is a flowchart of playing software used for the system.

FIG. 6 is a flowchart of recording medium creating software executed by a computer as the distributing recording medium fabrication device used for the system.

FIG. 7 is a block diagram of the system for preventing unauthorized play of digital content.

FIG. 8 is a flowchart of playing software used for the system.

FIG. 9 is a block diagram of the system for preventing unauthorized play of digital content.

FIG. 10 is a flowchart of playing software used for the system.

FIG. 11 is a block diagram of the system for preventing unauthorized play of digital content.

FIG. 12 is a flowchart of playing software used for the system.

EXPLANATION OF THE REFERENCE NUMERALS

α Distributing recording medium

100, 200 System for preventing unauthorized use of digital content

110, 210 Management center

120, 220 Digital content playing device

140, 240 Distributing recording medium fabrication device

300, 400, 500 System for preventing unauthorized use of digital content

310, 410, 510 Delivery management center

320, 420, 520 Digital content playing device

BEST MODE FOR CARRYING OUT THE INVENTION

Embodiments of the present invention will be described below.

Embodiment 1

A first embodiment of the present invention will be described with reference to FIGS. 1 and 2. FIG. 1 is a block diagram of a system for preventing unauthorized play of digital content, including a block diagram of a distributing recording medium fabrication device used for the system. FIG. 2 is a

flowchart of playing software used for the system.

A system for preventing unauthorized use of digital content 100 shown in FIG. 1 is a system preventing unauthorized use of a content file on a distributing recording medium α distributed for renting it to a user. Rented is the content file, not the distributing recording medium α itself.

Basically, the system has: a distributing recording medium α which is a recording medium on which a content file having header information "A" and a data body "B" is recorded and lacks part of the header information "A" to prevent unauthorized play and unauthorized copy of the data body "B"; a management center 110 which is management means managing use of the content file on the distributing recording medium α and can deliver the prepared part of the header information "A" as piece data via a communication line β ; and a digital content playing device 120 which is a device used for playing and copying the content file on the distributing recording medium α and has the function of communicating via the communication line β with the management center 110. The digital content playing device 120 is a computer here. Playing software processed by the computer is prepared in the management center 110.

The communication line β is an Internet line or a telephone line which is used to perform mutual communication between the management center 110, a bank or credit card company 130 and the digital content playing device 120.

The distributing recording medium α is a general recording medium such as a CD or DVD. The content file on the distributing recording medium α has a data structure having the data body "B" of a user area as the file of such as music, moving image, still image, text, application software or application data, and header information a' (not shown) of a non-user area as content information accompanying the data body "B". Such digital content are recorded in an encrypted form on the distributing recording medium α including the later-described content ID.

The digital content playing device 120 is a device used for playing and copying the content file on the distributing recording medium α distributed for renting it to the user, as described above. In its function, to play and copy the data body "B" of the content file, unless all of the content of the header information a' are set in a predetermined registry, the data body "B" cannot be, of course, played from the distributing recording medium α and cannot be copied to another distributing recording medium.

The system actively uses the characteristic of the digital content playing device 120, lacks, from the header information a' of the content file, part of data (piece data) included therein (showing the lacked header information a' as the header information a), and includes the header information "A" together with the data body "B" in the content file on the distributing recording medium α , thereby preventing unauthorized play and

unauthorized copy of the data body "B" .

The piece data is pre-recorded in an encrypted form on a piece data DB 111 of the management center 110. Since the management center 110 manages all uses of many kinds of content files, a content ID showing the kind of the content file is added to the piece data on the piece data DB 111. The content file on the distributing recording medium α includes the same content ID in an encrypted form in an available area in which the piece data of the header information "A" enters.

Using the content IDs, the content file on the distributing recording medium α is matched with the piece data on the piece data DB 111. The management center 110 checks whether the content IDs are matched with each other or not before transferring the piece data to the digital content playing device 120. Therefore, the content IDs are useful for preventing unauthorized use. The content IDs need not be used if one content file is to be managed in the management center 110, aside from the problem of unauthorized use prevention.

The digital content playing device 120 is a general-purpose computer used by the user. In the drawing, the numeral 121 denotes a control section such as a CPU; the numeral 122, an output section such as a monitor or speaker; the numeral 123, an operation section such as a keyboard or mouse; the numeral 124, a play copy section performing read/write of data from/onto the distributing recording medium α ; the numeral 125, a memory

section such as a hard disk; and the numeral 126, a communication section for performing communication.

Other than the basic program, playing software shown in FIG. 2 is recorded on the memory section 125. The playing software is free software downloaded from the management center 110 via the communication line β and is application software necessary for playing the content file on the distributing recording medium α . A player key allocated to the digital content playing device 120 is also pre-recorded on the memory section 125. The piece data transferred from the management center 110 and the piece data transfer date are further recorded thereon.

The content of the playing software will be described later. The software is processed by the control section 121 so that the computer can exhibit the function as the digital content playing device 120.

The digital content playing device 120 has functions of: when a request to play the content file under authentication and charging conditions is inputted by the user, transferring the request via the communication line β to the management center 110; and thereafter, when piece data is transferred from the management center 110 via the communication line β , using the header information "A" of the content file on the distributing recording medium α and the piece data only in play operation to play the data body "B" of the content file.

The management center 110 is a server operated by a person

performing business of renting the data body "B" on the distributing recording medium α to the user under contract with the copyright holder of a publication included in the data body "B" and collecting its rental fee from the user. In the drawing, the numeral 111 denotes a piece data DB on which piece data and a content key necessary for decrypting a content file are pre-recorded in an encrypted form; the numeral 112, a control section such as a computer; the numeral 113, a communication section for performing communication; the numeral 114, a charging DB on which information on authentication and charging of the user is sequentially recorded; and the numeral 115, a software DB on which the playing software is pre-recorded.

The operation of the thus-configured digital content unauthorized use prevention system 100 will be described. Along with it, the content of the playing software and the operation of the management center 110 will be described.

First, the user sets the obtained distributing recording medium α to his/her own computer (computer corresponding to the digital content playing device 120 in a state that the playing software shown in FIG. 2 is not downloaded), and operates the operation section 123 to access the management center 110 via the communication line β for performing necessary user registration. The management center 110 performs user registration according to this and transfers an ID and password of the user via the communication line β to the computer of the

user.

Then, the user operates his/her own computer to access the management center 110 and inputs a request to download the playing software to the digital content playing device 120. In this case, the ID and password of the user are necessary. The computer of the user transfers the request via the communication line β to the management center 110. Upon reception of the request, the management center 110 reads the playing software on the software DB 115 and transfers it via the communication line β to the computer of the user. The playing software shown in FIG. 2 is downloaded on the memory section 125 of the computer to be executed.

The digital content playing device 120 decides whether it is the first time that the playing software is executed or not (s1). Immediately after downloading the playing software, it is the first time. Therefore, a predetermined flag is set and the digital content playing device 120 accesses the management center 110 to transfer a message to perform play request processing via the communication line β to the management center 110. The management center 110 transfers data necessary for the play request processing via the communication line β to the digital content playing device 120. The digital content playing device 120 display outputs the play requesting screen on the output section 122 based on the data (s2).

The user sequentially inputs a rental period, a rental

money amount and a payment condition (his/her own bank account number or credit card number) via the operation section 123 as indicated on the play requesting screen. Finally, when the ID and password of the user are inputted as a play request of the distributing recording medium α via the operation section 123 (s3), the digital content playing device 120 switches the displayed output of the output section 122 to the authentication screen and transfers the inputted request data via the communication line β to the management center 110. In this case, the content ID included in the header information "A" on the distributing recording medium α and the player key on the memory section 125 are read and transferred to the management center 110 together with the request (s4).

The management center 110 checks authentication and charging of the user related to the request. That is, it refers to the transferred player key of the user to check whether the user related to the request is a person corresponding to a prepared inadequate persons list or not. It also refers to the transferred bank account number, credit card number or the like of the user to access a bank or credit card company 130, and requests the bank or credit card company 130 via the communication line β to pay a money amount corresponding to the rental fee of the content file on the distributing recording medium α to the company of the management center 110.

When the management center 110 confirms that the user

related to the request is a person corresponding to the inadequate persons list, and when a reply indicating that payment is not possible is transferred via the communication line β from the bank or credit card company 130, in either case, it transfers a message to deny the request of the user via the communication line β to the digital content playing device 120.

On the other hand, when the management center 110 confirms that the user related to the request is a person not corresponding to the inadequate persons list and a payment completion reply is transferred from the bank or credit card company 130 via the communication line β , it records the information on the player key of the user and the like and the information on collected charge on the charging DB 114, searches the piece data DB 111 to read the piece data and the content key corresponding to the content ID, and transfers them as a reply to approve the request of the user via the communication line β to the digital content playing device 120.

As for payment of the rental fee of the user to the management center 110, the user may directly request the bank or credit card company 130 to pay it using the digital content playing device 120 via the communication line β , or transfer it into the account of the company of the management center 110 without using the communication line β . In these cases, as for checking charging to the user, the management center 110 checks whether payment of the user is completed, not whether payment can be

made from the bank or credit card company 130.

When the message to deny the request of the user is transferred from the management center 110 via the communication line β (s5), the digital content playing device 120 display outputs on the output section 122 a message that the authentication and charging conditions of the user are not met (s6) to end the processing of the software.

On the other hand, when the piece data and content key are transferred as the reply to approve the request of the user from the management center 110 via the communication line β (a5), the authentication and charging conditions of the user are met (s6) to record the piece data and content key on the memory section 125. At the same time, the clock function of the computer is used to record the piece data transfer date on the memory section 125. The header information "A" on the distributing recording medium α and the piece data on the memory section 125 and the like are used only in play operation to play the data body "B" on the distributing recording medium α (s7). When such setting is ended, the processing of the program is ended.

When the digital content playing device 120 is play operated by the user, it reads and decrypts the content key on the memory section 125, reads the header information "A" of the content file on the distributing recording medium α to decrypt it using the content key, and reads the piece data on the memory section 125 to decrypt it using the content key. When the content

information is registered into a predetermined registry, the data body "B" of the content file on the distributing recording medium α is decrypted and played using the content key.

Thus, the digital content playing device 120 plays the data body "B" of the content file on the distributing recording medium α as operated. On the other hand, when the user sets another distributing recording medium to the digital content playing device 120 for copy operation, the digital content playing device 120 copies the content file on the distributing recording medium α as it is to another distributing recording medium. Since this cannot include the piece data, new distributing recording medium α is only created.

Therefore, when the user operates the digital content playing device 120 to execute the playing software, it is decided whether it is the first time that the playing software is executed or not is decided (s1). Since it is not immediately after downloading the playing software and the flag is set, the piece data transfer date on the memory section 125 is read to decide whether the current date is within the rental period or not. That is, the difference between the piece data transfer date and the current date is determined as an elapsed period from the point of time at which the piece data is transferred. When the elapsed period reaches the rental period included in the rental information, it is decided that it is not within the rental period, and when it has not reached the rental period, it is

decided that it is within the rental period (s8).

As the result of the decision, when it is not within the rental period, the message is display outputted on the output section 122 to delete the piece data and the content key on the memory section 125 (s9) for ending the processing of the software. When it is within the rental period, the processing of the software is directly ended. In this case, in quite the same manner as the case immediately after downloading the playing software, the digital content playing device 120 plays the data body "B" of the content file on the distributing recording medium α as operated. When the user sets another distributing recording medium to the digital content playing device 120 for copy operation, new distributing recording medium α is only created.

In the system, when the user uses the digital content playing device 120 for play operation, unless authentication and payment of the rental fee to the management center 110 are completed, the data body "B" of the content file on the distributing recording medium α cannot be played. The case of using a general digital content playing device instead of the digital content playing device 120 is alike. Primary, secondary and tertiary unauthorized uses of the content file on the distributing recording medium α can thus be prevented.

When using the digital content playing device 120 to play the content file on the distributing recording medium α not within the rental period, the piece data and the like on the memory

section 125 is only deleted automatically at this point and the content file on the distributing recording medium α remains the same. Within the rental period, the digital content playing device 120 can be used to create a new distributing recording medium α by copying the content file. To play the content file on the distributing recording medium α , the digital content playing device 120 can be used to reliably collect charges for secondary and tertiary uses since authentication and payment of the rental fee to the management center 110 are necessary.

A distributing recording medium fabrication device 140 used for creating the distributing recording medium α will be described here with reference to FIGS. 1 and 3.

The distributing recording medium fabrication device 140 is a device used by the company of the management center 110 or a person related to this, and separates piece data from a content file having the header information a' and the data body "B" for recording, and records the content file separated from the piece data on a set recording medium to create the distributing recording medium α . Here, a computer is used.

In FIG. 1, the numeral 141 denotes an input section playing a recording medium such as a DVD on which digital content obtained from the content holder are recorded; the numeral 142, a control section such as a CPU processing the recording medium creating software shown in FIG. 3; the numeral 143, a recording section which can set a recording medium such as a CD or DVD and records

a content file on the recording medium; and the numeral 144, a piece data memory recording piece data separated from the content file.

The content of the recording medium creating software shown in FIG. 3, and the operation of the distributing recording medium fabrication device 140 will be described.

A recording medium such as a DVD is set to the recording section 143 of the distributing recording medium fabrication device 140. A DVD or the like on which digital content are recorded is set to the input section 141. In this state, the recording medium creating software is executed.

First, the digital content recorded on the set DVD are read by the input section 141 (s1). Piece data is separated from a header part a' included in the digital content, and the separated piece data is encrypted to be recorded on the piece data memory 144 (s2). Then, the digital content separated from the piece data is encrypted (s3), and the encrypted digital content are recorded on a recording medium such as a DVD set to the recording section 143 (s4). The software is ended. The distributing recording medium a is created.

The first embodiment can be design changed to a system preventing unauthorized use of the content file on the distributing recording medium α transferred to the user for pay or for free, not rented. In this case, it has the same merit as above. The playing software used in this case may only delete

a series of processing according to whether it is within or not within the rental period. The digital content playing device, without downloading the playing software from the management center 110, may download it via a recording medium such as a CD. As a matter of course, it may be an exclusive device, not a computer. The digital content playing device has functions of: when a request to play a content file under authentication and charging conditions is inputted by the user, transferring the request via the communication line β to the management center 110; and thereafter, when piece data is transferred from the management center 110 via the communication line β , using the header information on the distributing recording medium α and the piece data only in play operation to play the data body "B" on the distributing recording medium α . The digital content playing device which has such function may be of any configuration.

Embodiment 2

A second embodiment of the present invention will be described with reference to FIGS. 4 and 5. FIG. 4 is a block diagram of a system for preventing unauthorized play of digital content, including a block diagram of a distributing recording medium fabrication device used for the system. FIG. 5 is a flowchart of playing software used for the system.

A system for preventing unauthorized use of digital content

200 shown in FIG. 4 is a system preventing unauthorized use of a content file on distributing recording medium α distributed for renting it to a user. Rented is the content file, not the distributing recording medium α itself.

Basically, the system has: a distributing recording medium α on which a content file having header information "A" and a data body "B" is recorded in a state of lacking part of the header information "A" (that is, play information "A1" indispensable for playing the data body "B" included in the header information a); a management center 210 which is management means managing use of the content file on the distributing recording medium α and can deliver the prepared lacked play information "A1" included in the header information "A" as piece data via a communication line β ; and a digital content playing device 220 which is a device used for playing and copying the content file on the distributing recording medium α and has a function of communicating via the communication line β with the management center 210. The digital content playing device 220 is a computer here. Playing software processed by the computer is prepared in the management center 210.

The communication line β is a digital line such as an optical communication line or an analog line such as a telephone line. This is used to perform mutual communication between the management center 210 and the digital content playing device 220.

The distributing recording medium α is a general recording medium such as a CD or DVD. The content file on the distributing recording medium α has a data structure having the data body "B" as data of music, moving image, still image, text, game or software, and content information "A2" such as information on the WEB address of the management center 210 in which a content ID allocated to the data body "B" and piece data "D" are stored. The play information "A1" included in the header information "A" is lacked from the content file having the header information "A" (the play information "A1" and the content information "A2") and the data body "B" for encryption. The play information "A1" refers to data showing the address value of a sector to be read of the data body "B", the size of the data body "B" and the like.

The digital content playing device 220 is a general-purpose computer used by the user. In the drawing, the numeral 221 denotes a control section such as a CPU; the numeral 222, an output section such as a monitor or speaker; the numeral 223, an operation section such as a keyboard or mouse; the numeral 224, a play copy section performing read/write of data from/onto the distributing recording medium α ; the numeral 225, a memory section such as a hard disk; and the numeral 226, a communication section for performing communication.

Other than the basic program, playing software shown in FIG. 5 is recorded on the memory section 225. The playing software is software for pay or for free downloaded from the

management center 210 via the communication line β under a user registration condition and is application software necessary for playing the content file on the distributing recording medium α . A player ID allocated to the playing software is also transmitted to the memory section 225 together with the playing software from the management center 210 to be recorded. Further, the piece data "D", the decryption key and the like transmitted from the management center 210 are recorded on the memory section 225, and the piece data transmission date and the rental information showing the rental period are recorded thereon.

The content of the playing software will be described later. The software is processed by the control section 221 so that the computer can exhibit the function as the digital content playing device 220.

That is, the digital content playing device 220 has functions of: when a request to play the content file under an authentication condition is inputted by the user, transmitting the request via the communication line β to the management center 210; and thereafter, when piece data "D" is transmitted from the management center 210 via the communication line β , using the header information "A" of the content file on the distributing recording medium α and the piece data "D" in play operation to play the data body "B" of the content file, and functions of: determining an elapsed period from the point of time at which the piece data "D" is transmitted from the management center

210, and when the elapsed period reaches a predetermined period, deleting the transmitted piece data.

The management center 210 is a server operated by a person performing business of renting the data body "B" on the distributing recording medium α to the user under contract with the copyright holder of a publication included in the data body "B" and collecting its rental fee from the user. In the drawing, the numeral 211 denotes a piece data DB on which encrypted piece data "D" and a decryption key necessary for decrypting the piece data "D" and a content file are recorded; the numeral 212, a control section such as a computer; the numeral 213, a communication section for performing communication; the numeral 214, a user information DB on which user information is recorded and information on authentication and charging based on this is sequentially recorded; and the numeral 215, a software DB on which the playing software is pre-recorded.

A content ID showing the corresponding content file is added to the piece data "D" on the piece data DB 211. The content IDs are used to match the content file on the distributing recording medium α with the piece data d on the piece data DB 211. The user ID and player ID of the corresponding user are added to the user information on the user information DB. The user ID or player ID is used for matching with the user information of each user on the user information DB. The management center 210 checks (that is, authenticates) the user ID and password

before transmitting the piece data "D" to the digital content playing device 220, and also checks whether the content IDs are matched with each other or not. The content IDs are useful to prevent unauthorized use.

The operation of the thus-configured system for preventing unauthorized use of digital content 200, and the content of the playing software and the operation of the management center 210 will be described.

First, the user operates the operation section 223 of his/her own computer (computer corresponding to the digital content playing device 220 in a state that the playing software shown in FIG. 5 is not downloaded) to access the management center 210 via the communication line β for performing user registration (specifically, registering his/her name and address, and a payment condition "his/her own bank account number or credit card number"). The management center 210 creates a user ID and password according to this, registers the user information to the user information DB 214, and transmits the user ID and password via the communication line β to the computer of the user. The user may input the user ID and password at user registration.

Then, the user operates his/her own computer to access the management center 210 and inputs a request to download the playing software. In this case, the user ID and password are necessary. The computer of the user transmits the request via the communication line β to the management center 210. Upon

reception of the request, the management center 210 reads the playing software on the software DB 215 and transmits it via the communication line β to the computer of the user. The playing software shown in FIG. 5 is downloaded on the memory section 225 of the computer to be installed. Thus, the computer becomes the digital content playing device 220.

The digital content playing device 220 to which the distributing recording medium α is set by the user display outputs the playing software on the output section 222 when the playing software is executed. A play list showing rented content is displayed on the screen of the playing software (s1). That is, the content file in which a predetermined flag showing that play is requested is set, is displayed on the play list. Based on the play list, whether play operation is performed via the operation section 223 or not is decided (s2).

When it is decided that the play operation is not performed, whether a distributing recording medium α read operation (DISC LOAD operation) is performed via the operation section 223 or not is decided (s3). When the DISC LOAD operation is performed, a content list showing content files not play requested is display outputted on the output section 222 (s4). That is, content files in which a predetermined flag is not set are displayed on the content list.

Therefore, when the user makes a request to play the content file on the content list, the management center 210 is accessed

to read content information "A2" included in the header information "A" of the content file on the distributing recording medium α for transmitting the content ID via the communication line β to the management center 210 based on the WEB address included in the content information "A2" . Thus, a message to perform play request processing is transmitted. The management center 210 transmits data necessary for the play request processing via the communication line β to the digital content playing device 220, which display outputs the play requesting screen on the output section 222 based on the data (s5).

The user sequentially inputs or selects a rental period (by which a rental fee amount is determined) via the operation section 223 as indicated on the play requesting screen. Finally, when the user ID and password are inputted as a play request of the distributing recording medium α via the operation section 223 (s6), the digital content playing device 220 switches the displayed output of the output section 222 to the authentication screen and transmits the inputted request data via the communication line β to the management center 210. In this case, the content ID of the content information "A2" on the distributing recording medium α and the player ID on the memory section 225 are read and transmitted to the management center 210 together with the request data (s7).

The management center 210 checks authentication of the user related to the request. That is, it refers to the

transmitted user ID and player ID of the user, and reads the user information of the user from the user information DB 214 to check whether the user is an authorized user or not. The management center 210 having prepared an inadequate persons list of persons having over predetermined nonpayment of rental fee on the user information DB 214, checks whether the user is a person corresponding to the inadequate persons list or not together with the authentication (The check of the inadequate persons list is arbitrary.).

When the management center 210 confirms that the user related to the request is an unauthorized user or a person corresponding to the inadequate persons list although he/she is an authorized user, it transmits a message to deny the request of the user via the communication line β to the digital content playing device 220.

On the other hand, when the management center 210 confirms that the user related to the request is an authorized user and a person not corresponding to the inadequate persons list, it refers to the player ID and the like of the user to record a charge in the user information on the user information DB 214 of the user, searches the piece data DB 211 to read the piece data "D" and the decryption key corresponding to the content ID, and transmits them as a reply to approve the request of the user via the communication line β to the digital content playing device 220.

For charging, based on the user information DB 214 for each predetermined period, the rental fee is charged to a bank or credit card company 230 or is charged directly to the user to let him/her transfer it into an account or pay it at a convenience store or the like. When the management center 210 has been still connected via the communication line β to the bank or credit card company 230, immediate payment can be, of course, made.

The digital content playing device 220, when the message to deny the request of the user is transmitted from the management center 210 via the communication line β (s8), display outputs an error message on the output section 222 (s9).

On the other hand, when the piece data "D" and the decryption key are transmitted as the reply to approve the request of the user from the management center 210 via the communication line β (a8), a predetermined flag is set, and the piece data "D" and the decryption key are recorded on the memory section 225 (s10). At the same time, the clock function of the computer is used to record the piece data transmission date on the memory section 225. The play list is display outputted on the output section 222 (s1).

Therefore, the digital content playing device 220, reads the decryption key from the memory section 225 to decrypt the piece data "D" when the content file is play operated via the operation section 223 based on the play list (s2). Based on

the piece data "D", the data body d is read from the memory section 225 to read another decryption key from the memory section 225 to decrypt and play the data body d (s11). The program of the playing software is ended by performing ending processing by the user.

The playing software has the above basic function and a piece data management function resident in the digital content playing device 220 of managing the piece data "D" when the power of the digital content playing device 220 is turned on. By the piece data management function, the piece data "D" on the memory section 225 is managed, and the difference between the piece data transmission date and the current date is determined as an elapsed period from the point of time at which the piece data "D" is transmitted. When this reaches the rental period included in the rental information, it is decided that it is not within the rental period to delete the piece data "D" and the decryption key on the memory section 225 to unset a predetermined flag.

In the system, when the user uses the digital content playing device 220 for play operating the distributing recording medium α , unless the piece data "D" is obtained as an authorized play requester from the management center 210, the data body "B" of the content file on the distributing recording medium α cannot be played. This can prevent temporal unauthorized use of the content file on the distributing recording medium α . The piece data "D" of the content file whose rental period has elapsed

is deleted to prevent secondary unauthorized use. When the distributing recording medium α is copied to another distributing recording medium by the user, the play information "A1" included in the header information "A" is lacked from the content file recorded on another distributing recording medium. Therefore, unless the piece data "D" is obtained as an authorized play requester, it cannot be played. Thus, tertiary unauthorized use can be also prevented.

Not within the rental period of the distributing recording medium α , the piece data and the like on the memory section 225 is only deleted automatically. The content file on the distributing recording medium α remains the same. Within the rental period, the digital content playing device 220 can be used to create a new distributing recording medium α by copying the content file. To play the content file on the distributing recording medium α , the digital content playing device 220 can be used to reliably collect charges for secondary and tertiary uses since authentication and payment of the rental fee to the management center 210 are necessary.

Aside from the distributing recording medium α , a charge for the data body d of the content file is collected in play request. Therefore, the distributing recording medium α is distributed for free, and after that, charging can be performed to the play requester. Alternatively, the distributing recording medium α is sold at a price related to this, and after

that, charging can be performed to the play requester. When the content of the content file recorded on the distributing recording medium α include a technical book such as a medical book, the content of the technical book such as a medical book are divided into items to record each of the items as a content file on the distributing recording medium α for requesting to play each of the items. An expensive technical book can be provided at home to play request (rent) each of the items for reference as necessary. The system is used to respond to various new business forms.

When a plurality of content files are recorded on the distributing recording medium α , the user can rent only the content file which he/she desires to view or listen to. A person creating the distributing recording medium α can create distributing recording medium α on which an arbitrary content file is recorded without consideration of the taste of the user and trend. Therefore, the cost for creating the distributing recording medium α can be reduced.

A distributing recording medium fabrication device 240 used for creating the distributing recording medium α will be described here with reference to FIGS. 4 and 6. FIG. 6 is a flowchart of recording medium creating software executed by a computer as a distributing recording medium fabrication device used for the system.

The distributing recording medium fabrication device 240

is a device used by the company of the management center 210 or a person related to this, and separates play information "A1" included in header information "A" as piece data "D" from a content file having the header information "A" and data body "B" for recording and records the content file separated from the piece data "D" on a set recording medium to create the distributing recording medium α . Here, a computer is used.

In FIG. 4, the numeral 241 denotes an input section reading digital content from a master disc; the numeral 242, a control section such as a CPU processing the recording medium creating software shown in FIG. 6; the numeral 243, a recording section which can set a recording medium such as a CD or DVD and records a content file on the recording medium; and the numeral 244, a piece data memory recording piece data "D" separated from the content file.

The content of the recording medium creating software shown in FIG. 6, and the operation of the distributing recording medium fabrication device 240 will be described.

When the distributing recording medium fabrication device 240 is turned on, it executes the recording medium creating software. A master disc is manually or automatically set to the input section 241. A recording medium such as a DVD is automatically sequentially set to the recording section 243.

First, a content file is read from the set master disc by the input section 241 (s1). Play information "A1" included

in header information "A" is separated as piece data "D" from the header information "A" included in the content file, and the separated piece data "D" is encrypted to be recorded on the piece data memory 244 (s2). Then, the content file is encrypted (s3), and is recorded on a recording medium such as a DVD set to the recording section 243 (s4). The software is ended. The piece data "D" recorded on the piece data memory 244 is recorded on the recording medium to be transmitted to the management center 210. The distributing recording medium a is thus created.

The system for preventing unauthorized play of digital content 200 has: a distributing recording medium which is a recording medium on which a content file having header information and a data body is recorded and lacks part of the header information to prevent unauthorized play of the data body; management means which is means managing use of the content file on the distributing recording medium and can transmit the prepared part of the header information as piece data via a communication line; and a digital content playing device which is a device used for at least playing the content file on the distributing recording medium and has the function of communicating via the communication line with the management means, wherein when a request to play the content file under an authentication condition is inputted by a user to the digital content playing device, the digital content playing device transmits the request via the communication line to the

management means, the management means checks authentication of the user related to the request to transmit the piece data via the communication line to the digital content playing device, and the digital content playing device uses the header information on the distributing recording medium and the piece data in play operation to play the data body on the distributing recording medium. Any design change can be made to the system for preventing unauthorized play of digital content 200 of such configuration.

As for the distributing recording medium α , the content file having the header information "A" and the data body "B" is recorded in a state of lacking the play information "A1" included in the header information a. It can be, of course, recorded in a state of adding other information. As for other information, there is a program or the like which decides whether the playing software is installed on the computer of the user or not, and when deciding that it is not installed, automatically accesses the HP of the management center 210. When the program is recorded and the user sets the obtained distributing recording medium α to his/her own computer (computer corresponding to the digital content playing device 220 in a state that the playing software is not downloaded), the WEB address of the management center 210 is read to access the management center 210 based on this. Therefore, when obtaining the playing software by the above procedure, the content file on the distributing recording

medium α can be played.

The content of the playing software are only an example. Changing timing at which user registration and user authentication are performed and changing the content or the like is arbitrary.

The second embodiment can be design changed to a system preventing unauthorized use of the content file on the distributing recording medium α transferred to the user for pay or for free, not rented. In this case, it has the same merit as above. The playing software used in this case may only delete a series of processing according to whether it is within or not within the rental period. The digital content playing device, without downloading the playing software from the management center 210, may install it via the recording medium such as a CD. As a matter of course, it may be an exclusive device, not a computer. The digital content playing device has functions of: when a request to play a content file under authentication and charging conditions is inputted by the user, transmitting the request via the communication line β to the management center 210; and thereafter, when the piece data "D" is transmitted from the management center 210 via the communication line β , using the header information on the distributing recording medium α and the piece data "D" only in play operation to play the data body "B" on the distributing recording medium α . The digital content playing device which has such function may be of any

configuration.

Embodiment 3

A third embodiment of the present invention will be described with reference to FIGS. 7 and 8. FIG. 7 is a block diagram of a system for preventing unauthorized play of digital content. FIG. 8 is a flowchart of playing software used for the system.

A system for preventing unauthorized use of digital content 300 shown in FIG. 7 is a system preventing unauthorized use of a content file delivered for renting it to a user.

The system has a delivery management center 310 as delivery management means delivering a content file having header information "A" and a data body "B" via a communication line β and managing use of the data body "B" of the content file; and a digital content playing device 320 communicable via the communication line β with the delivery management center 310 and used for playing and copying the content file delivered from the delivery management center 310. The digital content playing device 320 is a computer here. Playing software processed by the computer is prepared in the delivery management center 310.

The communication line β is an Internet line or a telephone line and performs mutual communication between the delivery management center 310, a bank or credit card company 330 and the digital content playing device 320.

The content file here has a data structure having the data body "B" of a user area as the file of such as music, moving image, still image, text, application software or application data, and header information a' (not shown) of a non-user area as content information accompanying the data body "B". Such content file is pre-recorded in an encrypted form on a digital content DB 311 of the delivery management center 310.

The digital content playing device 320 is a device used for playing and copying the content file delivered for renting it to the user, as described above. In its function, to play and copy the data body "B" of the content file, unless all of the content of the header information a' are set in a predetermined registry, the data body "B" cannot be, of course, played from the distributing recording medium α and cannot be copied to another distributing recording medium.

The system actively uses the function of the digital content playing device 320, lacks, from the header information a' of the content file, part of data (piece data) included therein (showing the lacked header information a' as the header information a), and includes the header information "A" together with the data body "B" in the content file of the distributing recording medium α , thereby preventing unauthorized play and unauthorized copy of the data body "B".

The content file having the header information "A" and the data body "B" is pre-recorded in an encrypted form on the

digital content DB 311 of the delivery management center 310. The piece data, the content key and the like are also pre-recorded in an encrypted form on the digital content DB 311.

The digital content playing device 320 is a general-purpose computer used by the user. In the drawing, the numeral 321 denotes a control section such as a CPU; the numeral 322, an output section such as a monitor or speaker; the numeral 323, an operation section such as a keyboard or mouse; the numeral 324, a play copy section performing read/write of data from/onto the distributing recording medium α and the like; the numeral 324, a memory section such as a hard disk; and the numeral 326, a communication section for performing communication.

Other than the basic program, playing software shown in FIG. 8 is recorded on the memory section 324. The playing software is free software downloaded from the delivery management center 310 via the communication line β and is application software necessary for playing the content file. Piece data, a content key and the like transferred from the delivery management center 310 are recorded and the piece data transfer date is recorded thereon.

The content of the playing software will be described later. The software is processed by the control section 321 so that the computer can exhibit the function as the digital content playing device 320.

The digital content playing device 320 has functions of:

when a request to download the digital content is inputted by the user, transferring the request via the communication line β to the delivery management center 310; after the content file is transferred from the delivery management center 310, when a request to play the content file under authentication and charging conditions is inputted by the user, transferring the request via the communication line β to the delivery management center 310; and thereafter, when the piece data is transferred from the delivery management center 310 via the communication line β , using the header information "A" of the transferred content file and the piece data only in play operation to play the data body "B" of the content file.

The delivery management center 310 is a server operated by a person performing business of renting the content file to the user under contract with the copyright holder of a publication included in the data body "B" of the content file to be delivered and collecting its rental fee from the user. In the drawing, the numeral 311 denotes a digital content DB on which a content file to be delivered is pre-recorded in an encrypted form together with a content ID; the numeral 312, a control section such as a computer; the numeral 313, a communication section for performing communication; the numeral 314, a charging DB on which information such as authentication and charging of the user is sequentially recorded; and the numeral 315, a software DB on which the playing software is pre-recorded.

The operation of the thus-configured system for preventing unauthorized use of digital content 300, and the content of the playing software will be described.

First, the user operates the operation section 323 of his/her own computer (computer corresponding to the digital content playing device 320 in a state that the playing software shown in FIG. 8 is not downloaded), and accesses the delivery management center 310 via the communication line β for performing necessary user registration. The delivery management center 310 performs user registration according to this and transfers the ID and password of the user via the communication line β to the computer of the user.

Then, the user operates his/her own computer to access the delivery management center 310 and inputs a request to download the playing software to the digital content playing device 320. In this case, the ID and password of the user are necessary. The computer of the user transfers the request via the communication line β to the delivery management center 310. Upon reception of the request, the delivery management center 310 reads the playing software on the software DB 315 and transfers it via the communication line β to the computer of the user. The playing software shown in FIG. 8 is downloaded on the memory section 324 of the computer to be executed.

First, the digital content playing device 320 decides whether it is the first time that the playing software is executed

or not (s1). Since immediately after downloading the playing software, it is the first time, a predetermined flag is set and the digital content playing device 320 accesses the delivery management center 310 to transfer a message to perform play request processing via the communication line β to the delivery management center 310. The delivery management center 310 transfers data necessary for the play request processing via the communication line β to the digital content playing device 320. The digital content playing device 320 display outputs the play requesting screen on the output section 322 based on the data (s2).

The user sequentially inputs a rental period, a rental money amount and a payment condition (his/her own bank account number or credit card number) via the operation section 323 as indicated on the play requesting screen. Finally, when the ID and password of the user are inputted as a play request of the distributing recording medium α via the operation section 323 (s3), the digital content playing device 320 switches the displayed output of the output section 322 to the authentication screen and transfers the inputted request data via the communication line β to the delivery management center 310.

The management center 110 checks authentication and charging of the user related to the request. That is, it refers to the transferred user ID or the like of the user to check whether the user related to the request is a person corresponding to

a prepared inadequate persons list or not. It also refers to the transferred bank account number, credit card number or the like of the user to access the bank or credit card company 330 to request the bank or credit card company 330 via the communication line β to pay a money amount corresponding to the rental fee of the content file to the company of the delivery management center 310.

When the delivery management center 310 confirms that the user related to the request is a person corresponding to the inadequate persons list, and when a reply indicating that payment is not possible is transferred via the communication line β from the bank or credit card company 330, in either case, it transfers a message to deny the request of the user via the communication line β to the digital content playing device 320.

When confirming that the user related to the request is not a person corresponding to the inadequate persons list and when a payment completion reply from the bank or credit card company 330 is transmitted via the communication line β , the information on the user ID of the user and the information on collected charge are recorded on the charging DB 314, the digital content DB 311 is searched to read the content file on the digital content DB 311. While the piece data is lacked to prevent unauthorized play and unauthorized copy, the piece data and the player key are transferred via the communication line β to the digital content playing device 320.

On the other hand, the digital content are transferred from the delivery management center 310 via the communication line β as a reply to approve the request of the user (a5), the authentication and charging conditions of the user are met (s6) to record the content file and the like on the memory section 324. At the same time, the clock function of the computer is used to record the piece data transfer date on the memory section 324. The header information "A" of the content file, the piece data and the like are used only in play operation to play the data body "B" of the content file (s7). When such setting is ended, the processing of the program is ended.

When the digital content playing device 320 is play operated by the user, it reads and decrypts the content key on the memory section 324, reads the header information "A" of the content file to decrypt it using the content key, and reads the piece data on the memory section 324 to decrypt it using the content key. When the header information and the piece data are registered into the predetermined registry, the data body "B" of the content file is decrypted and played using the content key.

Thus, the digital content playing device 320 plays the data body "B" of the content file as operated. On the other hand, when the user sets a distributing recording medium to the digital content playing device 320 for copy operation, the digital content playing device 320 copies the content file as

it is to the distributing recording medium to only create distributing recording medium α .

When the user operates the digital content playing device 320 to execute the playing software, whether it is the first time that the playing software is executed or not is decided (s1). Since it is not immediately after downloading the playing software and the flag is set, the piece data transfer date on the memory section 324 is read to decide whether the current date is within the rental period or not. The difference between the piece data transfer date and the current date is determined as an elapsed period from the point of time at which the piece data is transferred. When it has reached the rental period included in the rental information, it is decided that it is not within the rental period. When it has not reached the rental period, it is decided that it is within the rental period (s8).

After the decision, when it is not within the rental period, the message is display outputted on the output section 322 to delete the piece data and the content key on the memory section 324 (s9) to end the processing of the software. When it is within the rental period, the processing of the software is directly ended. In this case, in quite the same manner as the case immediately after downloading the playing software, the digital content playing device 320 plays the data body "B" of the content file as operated. When the user sets a distributing recording medium to the digital content playing device 320 for copy

operation, a new distributing recording medium α is only created.

In the system, when the user uses the digital content playing device 320 for play operation, unless authentication and payment of the rental fee to the delivery management center 210 are completed, the data body "B" of the content file cannot be played. The case of playing the distributing recording medium α created by the digital content playing device 320 by another computer is alike. Not only primary, but also secondary and tertiary unauthorized uses of the content file can be prevented.

When using and playing the digital content playing device 320 not within the rental period of the digital content, the piece data and the like on the memory section 324 is automatically deleted at this point and the content file remains the same. Within the rental period, the digital content playing device 320 can be used to create the distributing recording medium α . To play the content file on the distributing recording medium α , the digital content playing device 320 can be used to reliably collect charges for secondary and tertiary uses since authentication and payment of the rental fee to the delivery management center 310 are necessary.

The third embodiment can be design changed to a system preventing unauthorized use of the content file delivered for pay or for free, not rented. In this case, it has the same merit as above. The playing software used in this case may only delete processing when the delivered content file is not within the

rental period. The digital content playing device 320, without downloading the playing software from the delivery management center 310, may download it via a recording medium such as a CD. As a matter of course, it may be an exclusive device, not a computer.

Embodiment 4

A fourth embodiment of the present invention will be described with reference to FIGS. 9 and 10. FIG. 9 is a block diagram of a system for preventing unauthorized play of digital content. FIG. 10 is a flowchart of playing software used for the system.

A system for preventing unauthorized use of digital content 400 shown in FIG. 9 is a system preventing unauthorized use of a content file delivered for renting it to a user.

The system has: a delivery management center 410 which is a server in which a content file having header information "A" and a data body "B" is prepared in a state of lacking part of the header information "A" (that is, play information "A2" included in the header information a) and the lacked play information "A2", aside from the content file, is prepared as piece data "D" and is delivery management means delivering the content file via a communication line and managing use of the data body "B"; and a digital content playing device 420 communicable via the communication line β with the delivery

management center 410 and used for playing and copying the content file delivered from the delivery management center 410. The digital content playing device 420 is a computer here. Playing software processed by the computer is prepared in the delivery management center 410.

The content file here has a data structure having the data body "B" as data of such as music, moving image, still image, text, game or software, and the content information "A2" such as information on the WEB address of the management center 110 in which a content ID allocated to the data body "B" and piece data "D" are stored. The play information "A1" included in the header information "A" is lacked from the content file having the header information "A" (the play information "A1" and the content information "A2") and the data body "B" for encryption. The play information "A1" refers to data showing the address value of a sector to be read of the data body "B", the size of the data body "B" and the like.

The digital content playing device 420 is a general-purpose computer used by the user. In the drawing, the numeral 421 denotes a control section such as a CPU; the numeral 422, an output section such as a monitor or speaker; the numeral 423, an operation section such as a keyboard or mouse; the numeral 424, a play copy section performing read/write of data from/onto the distributing recording medium α or the like; the numeral 424, a memory section such as a hard disk; and the numeral 426,

a communication section for performing communication.

Other than the basic program, playing software shown in FIG. 10 is recorded on the memory section 424. The playing software is software for pay or for free downloaded from the delivery management center 410 via the communication line β under a user registration condition and is application software necessary for playing the content file. Information on the WEB address of the delivery management center 410 in which a player ID allocated to the playing software and the piece data "D" are stored is transmitted to the memory section 424 together with the playing software from the delivery management center 410 to be recorded. Further, the piece data "D", the decryption key and the like transmitted from the delivery management center 410 are recorded on the memory section 424 and the piece data transfer date and the rental information showing the rental period are recorded thereon.

The content of the playing software will be described later. The playing software shown in FIG. 10 is processed by the control section 421 so that the computer can exhibit the function as the digital content playing device 420.

That is, the digital content playing device 420 has functions of: when a request to download the content file is inputted by the user, transmitting the request via the communication line β to the delivery management center 410; after the content file is transmitted from the delivery management

center 410, when a request to play the content file under an authentication condition is inputted by the user, transmitting the request via the communication line β to the delivery management center 410; and thereafter, when the piece data "D" is transmitted from the delivery management center 410 via the communication line β , using the header information "A" of the transmitted content file and the piece data "D" in play operation to play the data body "B" of the content file, and functions of: determining an elapsed period from the point of time at which the piece data "D" is transmitted from the delivery management center 410; and when the elapsed period reaches a predetermined period, deleting the transmitted piece data.

The delivery management center 410 is a server operated by a person performing business of renting the content file to the user under contract with the copyright holder of a publication included in the data body "B" of the content file to be delivered and collecting its rental fee from the user. In the drawing, the numeral 411 denotes a digital content DB on which a content file to be delivered is pre-recorded in an encrypted form together with a content ID; the numeral 412, a control section such as a computer; the numeral 413, a communication section for performing communication; the numeral 414, a user information DB on which user information is recorded and information on authentication and charging and the like based on this is sequentially recorded; the numeral 415, a software DB on which

the playing software is pre-recorded; and the numeral 416, a piece data DB on which piece data "D" and a decryption key necessary for decrypting the piece data "D" and the content file are pre-recorded in an encrypted form together with the content ID.

The operation of the thus-configured system for preventing unauthorized use of digital content 400, and the content of the playing software will be described.

First, the user operates the operation section 423 of his/her own computer (computer corresponding to the digital content playing device 420 in a state that the playing software is not downloaded) to access the delivery management center 410 via the communication line β for performing necessary user registration as in Embodiment 1. The delivery management center 410 creates a user ID and password according to this, registers the user information into the user information DB 414, and transmits the user ID and password via the communication line β to the computer of the user. The user may input the user ID and password at user registration.

Then, the user operates his/her own computer to access the delivery management center 410 and inputs a request to download the playing software. In this case, the user ID and password are necessary. The computer of the user transmits the request via the communication line β to the delivery management center 410. Upon reception of the request, the delivery management center 410 reads the playing software on the software

DB 415 and transmits it via the communication line β to the computer of the user. The playing software is downloaded on the memory section 424 of the computer to be installed. The computer becomes the digital content playing device 420.

When obtaining the content file, the digital content playing device 420 accesses the delivery management center 410 according to the operation via the operation section 423 of the user. The delivery management center 410 transmits data of the content files list to the digital content playing device 420. The digital content playing device 420 display outputs the content files list on the output section 422 based on the data. The delivery management center 410 may be accessed based on the WEB address recorded together with the playing software after executing the software, or may be accessed based on the WEB address registered by the user into the Internet browser.

The user selects the content file to be rented from the content files list via the operation section 423. Data of the request of the selected content file is transmitted to the delivery management center 410.

When the delivery management center 410 receives the data of the request, it refers to a content ID included in this to search for and read the content file corresponding to the content ID from the digital content DB 411 and transmits it to the digital content playing device 420. When the digital content playing device 420 receives the content file, it records it on the registry

of the memory section 424 or a recording medium set to the copy section 425.

Thereafter, when the playing software is executed by the user (When the content file is recorded on a recording medium, the playing software is executed and the recording medium is set.), the digital content playing device 420 display outputs the playing software on the output section 422. The content information "A2" of the content file recorded on the memory section 424 is read, and the content file is displayed on the play list on the screen of the playing software (s1). The play list displays the file name of the content file and the message that the content file is rented. Thus, it displays a message that the content file, in which a predetermined flag showing that play is requested is set, is rented. Based on the play list, whether the rented content file is play operated via the operation section 423 or not is decided (s2).

When it is decided that the play operation is not performed, whether a play request operation of the unrented content file displayed on the play list is performed via the operation section 423 or not is decided (s3). When it is decided that the play request operation is not performed, whether a recording medium read operation (LOAD operation) is performed via the operation section 423 or not is decided (s4). When the LOAD operation is performed, the content list showing content files not play requested is display outputted on the output section 422 (s5).

That is, content files on the recording medium in which a predetermined flag is not set are displayed on the content list.

When the user makes a request to play the content file on the play list or the content list, the content information "A2" included in the header information "A" of the content file on the memory section 424 or the recording medium is read to transmit the content ID via the communication line β to the delivery management center 410 based on the WEB address included in the content information "A2" . In this way, a message to perform play request processing is transmitted. The delivery management center 410 transmits data necessary for the play request processing via the communication line β to the digital content playing device 420. The digital content playing device 420 display outputs the play requesting screen on the output section 422 based on the data (s6).

Thereafter, the user sequentially inputs or selects a rental period (by which a rental fee amount is automatically determined) via the operation section 423 as indicated on the play requesting screen. Finally, when the user ID and password are inputted as a play request of the content file via the operation section 423 (s7), the digital content playing device 420 switches the displayed output of the output section 422 to the authentication screen and transmits the inputted request data via the communication line β to the delivery management center 410. In this case, the content ID of the content information

"A2" on the memory section 424 or the recording medium and the player ID on the memory section 424 are read and transmitted to the delivery management center 410 together with the request data (s8).

Then, the delivery management center 410 checks authentication of the user related to the request. That is, it refers to the transmitted user, player ID and the like of the user, and reads the user information of the user from the user information DB 414 to check whether the user is an authorized user or not. The delivery management center 410 prepares an inadequate persons list indicating persons having over predetermined nonpayment of rental fee in the user information DB 414 and checks whether the user is a person corresponding to the inadequate persons list together with the authentication (The check of the inadequate persons list is arbitrary.).

When the delivery management center 410 confirms that the user related to the request is an unauthorized user or a person corresponding to the inadequate persons list although he/she is an authorized user, a message to deny the request of the user is transmitted via the communication line β to the digital content playing device 420.

On the other hand, when the delivery management center 410 confirms that the user related to the request is an authorized user and a person not corresponding to the inadequate persons list, it refers to the player ID or the like of the user to record

a charge in the user information on the user information DB 414 of the user, searches the piece data DB 416 to read the piece data "D" and the decryption key corresponding to the content ID, and transmits them as a reply to approve the request of the user via the communication line β to the digital content playing device 420.

For charging, based on the user information DB 414 for each predetermined period, the rental fee is charged to a bank or credit card company 430 or is charged directly to the user to let him/her transfer it into an account or pay it at a convenience store or the like. When the delivery management center 410 has been still connected via the communication line β to the bank or credit card company 430, immediate payment can be, of course, made.

Thereafter, the digital content playing device 420, when the message to deny the request of the user is transmitted from the delivery management center 410 via the communication line β (s9), display outputs an error message on the output section 422 (s10).

When the piece data "D" and the decryption key are transmitted as the reply to approve the request of the user from the delivery management center 410 via the communication line β (a9), a predetermined flag is set, and the piece data "D" and the decryption key are recorded on the memory section 424 (s11). At the same time, the clock function of the computer is used

to record the piece data transmission date on the memory section 424. The play list is display outputted on the output section 422 (s1).

Thereafter, the digital content playing device 420, when the content file is play operated via the operation section 423 based on the play list (s2), reads the decryption key from the memory section 424 to decrypt the piece data "D". Based on the piece data "D", the data body d is read to read another decryption key from the memory section 424 to decrypt and play the data body d (s12). The program of the playing software is ended by performing ending processing by the user.

The playing software has the above basic function and a piece data management function resident in the digital content playing device 420 of managing the piece data "D" when the power of the digital content playing device 420 is turned on. By the piece data management function, the piece data "D" on the memory section 424 is managed, and the difference between the piece data transmission date and the current date is determined as an elapsed period from the point of time at which the piece data "D" is transmitted. When this reaches the rental period included in the rental information, it is decided that it is not within the rental period to delete the piece data "D" and the decryption key on the memory section 424 to unset a predetermined flag.

In the unauthorized play prevention system 400, when the user uses the digital content playing device 420 for play

operating the content file, unless the piece data "D" is obtained as an authorized play requester from the delivery management center 410, the data body "B" of the content file cannot be played. This can prevent temporal unauthorized use of the content file. The piece data "D" of the content file whose rental period has elapsed is deleted to prevent secondary unauthorized use. When the content file is copied to another recording medium by the user, the play information "A1" included in the header information "A" is lacked from the content file recorded on the recording medium. Therefore, unless the piece data "D" is obtained as an authorized play requester, it cannot be played. Tertiary unauthorized use can be also prevented.

Not within the rental period of the digital content, the piece data "D" on the memory section 424 is only automatically deleted, and the content file remains the same. Within or not within the rental period, the digital content playing device 420 can be used to copy the content file to another recording medium. To play the content file on the recording medium, the digital content playing device 420 can be used to reliably collect charges for secondary and tertiary uses since authentication and payment of the rental fee to the delivery management center 410 are necessary.

In the system, as described above, the computer having a write function is used to easily record the content file on the recording medium. Instead of displaying a recording medium

such as a video tape, CD or DVD, a rental video shop can be provided with the computer. In this manner, the recording medium need not be returned. There is a merit for both the shop and customer. Since what content file is downloaded cannot be recognized by the shop clerk, the customer can easily rent digital content depending on its type. In this case, a form of a rental video shop need not be taken. Needless to say, it is possible to provide the service of an Internet cafe. The content DB may be provided at a rental video shop or Internet cafe.

The unauthorized play prevention system 400 has: delivery management means which is a server in which a content file having header information and a data body is prepared in a state of lacking part of the header information and the part of the header information is prepared as piece data and delivers the content file via a communication line and manages use of the data body; and a digital content playing device capable of communicating via the communication line with the delivery management means and used for at least playing the content file delivered from the delivery management means, wherein when a request to download the content file is inputted by a user to the digital content playing device, the digital content playing device transmits the request via the communication line to the delivery management means, the delivery management means transmits the content file related to the request via the communication line to the digital content playing device, thereafter, when a request to play the

content file under an authentication condition is inputted by the user to the digital content playing device, the digital content playing device transmits the request via the communication line to the delivery management means, the delivery management means checks authentication of the user related to the request to transmit the piece data of the content file related to the request via the communication line to the digital content playing device, and the digital content playing device uses the header information of the transmitted content file and the piece data in play operation to play the data body of the content file. Any design change can be made to the unauthorized play prevention system 400 of such configuration.

The delivery management center 410 has one digital content DB 411, but may have more. In this case, for example, a movie content file may be stored in a first DB and a music content file may be stored in a second DB. That is, different kinds of content files may be stored in DBs. The content files stored in the DBs may be the same to prevent access to the first DB from being concentrated at congestion. The same thing applies to the piece data DB 416. The delivery management center 410 has the digital content DB 411 and the piece data DB 416. The digital content DB 411 and the piece data DB 416 may be installed in locations different from the delivery management center 410. In this case, the delivery management center 410 authenticates the user to transmit the WEB address of the digital content DB

411 and the piece data DB 416 to the digital content playing device 420. The digital content playing device 420 may access the digital content DB 411 and the piece data DB 416 based on the WEB address to obtain the content file and piece data "D".

As for the digital content DB 411, the content file having the header information "A" and the data body "B" is recorded in a state of lacking the play information "A1" included in the header information a. It can be, of course, recorded in a state of adding other information. As for other information, there is a program or the like which decides whether the playing software is installed on the computer of the user or not, and when deciding that it is not installed, automatically accesses the HP of the delivery management center 410. When the program is recorded and the user executes the obtained content file on his/her own computer (computer corresponding to the digital content playing device 420 in a state that the playing software is not downloaded), the WEB address of the delivery management center 410 is read to automatically access the delivery management center 410 based on this. When obtaining the playing software by the above procedure, the content file on the memory section 424 can be played.

The content of the playing software are only an example. Changing timing at which user registration and user authentication are performed and changing the content or the like is arbitrary. When the content file is recorded on the

memory section 424 of the digital content playing device 420 and the rental period has elapsed, the content file may be deleted together with the piece data "D". Aside from the piece data "D", an elapsed period from the point of time at which the content file is received may be determined, and when the elapsed period reaches a predetermined period, the content file may be deleted.

The fourth embodiment can be design changed to a system preventing unauthorized use of the content file delivered for pay or for free, not rented. In this case, it has the same merit as above. The playing software used in this case may only delete processing when the delivered content file is not within the rental period. The digital content playing device 420, without downloading the playing software from the delivery management center 410, may download it via a recording medium such as a CD. As a matter of course, it may be an exclusive device, not a computer.

Embodiment 5

A third embodiment of the present invention will be described with reference to FIGS. 11 and 12. FIG. 11 is a block diagram of a system for preventing unauthorized play of digital content. FIG. 12 is a flowchart of playing software used for the system for preventing unauthorized use of digital content.

A system for preventing unauthorized use of digital content 500 shown in FIG. 11 has the same configuration as that of the

unauthorized use prevention system 400 except that the content of the playing software processed by a control section 512 of a digital content playing device 520 are different. The content of the playing software shown in FIG. 12 will be described below in detail and the description of the overlapped parts is omitted.

The playing software is recorded on a memory section 524 of the digital content playing device 520 by the same procedure as that of Embodiment 4.

When obtaining the content file, the digital content playing device 520 accesses a delivery management center 510 according to the operation via an operation section 523 of the user. The delivery management center 510 transmits data necessary for rental request processing via the communication line β to the digital content playing device 220. The digital content playing device 220 display outputs the rental requesting screen on the output section 222 based on the data.

Therefore, the user sequentially inputs or selects a rental period (by which a rental fee amount is automatically determined) via the operation section 523 as indicated on the rental requesting screen. Finally, when the user ID and password are inputted as a rental request of the content file via the operation section 523, the digital content playing device 520 switches the displayed output of the output section 522 to the authentication screen and transmits the inputted request data via the communication line β to the delivery management center

510. In this case, the player ID on the memory section 524 is read and transmitted to the delivery management center 210 together with the request data.

The delivery management center 510 then checks authentication of the user related to the request. That is, it refers to the transmitted user ID, player ID and the like of the user, and reads the user information of the user from the user information DB 514 to check whether the user is an authorized user or not. The delivery management center 510 prepares an inadequate persons list indicating persons having over predetermined nonpayment of rental fee in the user information DB 514 and checks whether the user is a person corresponding to the inadequate persons list or not together with the authentication (The check of the inadequate persons list is arbitrary.).

When the delivery management center 510 confirms that the user related to the request is an unauthorized user or a person corresponding to the inadequate persons list although he/she is an authorized user, a message to deny the request of the user is transmitted via the communication line β to the digital content playing device 520.

On the other hand, when the delivery management center 510 confirms that the user related to the request is an authorized user or a person not corresponding to the inadequate persons list, it refers to the player ID and the like of the user to

record a charge in the user information on the user information DB 514 of the user, and transmits the data of the content files list as a reply to approve the request of the user via the communication line β to the digital content playing device 520.

For charging, based on the user information DB 514 for each predetermined period, the rental fee is charged to a bank or credit card company 530 or is charged directly to the user to let him/her transfer it into an account or pay it at a convenience store and the like. When the delivery management center 510 has been still connected via the communication line β to the bank or credit card company 530, immediate payment can be, of course, made.

The digital content playing device 520 display outputs the content files list on the output section 522 based on the data. The delivery management center 510 may be accessed based on the WEB address recorded together with the software after executing the playing software, or may be accessed based on the WEB address registered by the user into the Internet browser.

Thereafter, the user selects the content file to be rented from the content files list via the operation section 523. Data of the request of the selected content file is transmitted to the delivery management center 510.

When the delivery management center 510 receives the data of the request, it refers to a content ID included in this to search for and read the content file corresponding to the content

ID from the digital content DB 511 and searches for and reads the piece data "D" and the decryption key corresponding to the content ID from the piece data DB 516 to sequentially transmit the content file, piece data "D" and decryption key to the digital content playing device 520.

When the digital content playing device 520 receives the content file, it records it on the registry of the memory section 524 or the recording medium set to the copy section 525. When it receives the piece data "D" and decryption key, it records them on a piece data registry different from the predetermined registry of the memory section 524 on which the content file is recorded. A predetermined flag is set.

Thereafter, when the playing software is executed by the user (When the content file is recorded on a recording medium, the playing software is executed and the recording medium is set.), the digital content playing device 520 display outputs the playing software on the output section 522. The content information "A2" of the content file recorded on the memory section 524 or the recording medium is read, and the content file is displayed on the play list on the screen of the playing software (sl). The play list displays the file name of the content file and the message that the content file is rented. It displays a message that the content file in which a predetermined flag is set is rented. Based on the play list, whether the rented content file is play operated via the operation

section 523 or not is decided (s2).

When it is decided that the play operation is not performed, whether a request to play an unrented content file is made via the operation section 523 or not based on the play list (s3). That is, whether a request to re-rent the content file whose rental period has ended is made or not is decided. When it is decided that the play request is made, the content information "A2" of the content file on the memory section 524 or recording medium is read to transmit the content ID based on the WEB address included in the content information "A2" and a message to perform play request processing via the communication line β to the delivery management center 510. The delivery management center 510 transmits data necessary for play request processing via the communication line β to the digital content playing device 520. The digital content playing device 520 display outputs the play requesting screen on the output section 522 based on the data (s4).

The user sequentially inputs or selects a rental period (by which a rental fee amount is automatically determined) via the operation section 523 as indicated on the play requesting screen. Finally, when the user ID and password are inputted as a play request of the content file via the operation section 523 (s5), the digital content playing device 520 switches the displayed output of the output section 522 to the authentication screen and transmits the inputted request data via the

communication line β to the delivery management center 510. In this case, the content ID of the content information "A2" on the memory section 524 or the recording medium and the player ID on the memory section 524 are read and transmitted to the delivery management center 510 together with the request data (s6).

The delivery management center 510 checks authentication of the user related to the request. It refers to the transmitted user ID, player ID and the like of the user, and reads the user information of the user from the user information DB 514 to check whether the user is an authorized user or not. The delivery management center 510 prepares an inadequate persons list indicating persons having over predetermined nonpayment of rental fee in the user information DB 514 and checks whether the user is a not person corresponding to the inadequate persons list together with the authentication (The check of the inadequate persons list is arbitrary.).

When the delivery management center 510 confirms that the user related to the request is an unauthorized user or a person corresponding to the inadequate persons list although he/she is an authorized user, a message to deny the request of the user is transmitted via the communication line β to the digital content playing device 520.

On the other hand, when the delivery management center 510 confirms that the user related to the request is an authorized

user and a person not corresponding to the inadequate persons list, it refers to the player ID and the like of the user to record a charge in the user information on the user information DB 514 of the user, searches the piece data DB 516 to read the piece data "D" and the decryption key corresponding to the content ID, and transmits them as a reply to approve the request of the user via the communication line β to the digital content playing device 520. Charging is performed as described above.

The digital content playing device 520, when the message to deny the request of the user is transmitted from the delivery management center 510 via the communication line β (s7), display outputs an error message on the output section 522 (s8).

When the piece data "D" and the decryption key are transmitted as the reply to approve the request of the user from the delivery management center 510 via the communication line β (a7), a predetermined flag is set, and the piece data "D" and the decryption key are recorded on the above-described piece data registry of the memory section 524 (s9). At the same time, the clock function of the computer is used to record the piece data transmission date on the memory section 524. The play list is display outputted on the output section 522 (s1).

The digital content playing device 520, when the rented content file is play operated via the operation section 523 based on the play list (s2), reads the decryption key from the memory section 524 to decrypt the piece data "D". Based on the piece

data "D", the data body d is read to read another decryption key from the memory section 524 to decrypt and play the data body d (s10). The program of the playing software is ended by performing ending processing by the user.

The playing software has the above basic function and a piece data management function resident in the digital content playing device 520 of managing the piece data "D" when the power of the digital content playing device 520 is turned on. By the piece data management function, the piece data "D" on the memory section 524 is managed, and the difference between the piece data transmission date and the current date is determined as an elapsed period from the point of time at which the piece data "D" is transmitted. When it reaches the rental period included in the rental information, it is decided that it is not within the rental period to delete the piece data "D" and the decryption key on the memory section 524 to unset a predetermined flag.

The unauthorized play prevention system 500 can obtain the content file and the piece data "D" at the same time. As compared with Embodiment 4, the authorized temporal use of the content file can be made easy. The piece data "D" of the content file whose rental period has elapsed is deleted to prevent secondary unauthorized use. When the content file is recorded by the user on the recording medium, the play information "A1" included in the header information "A" is lacked from the content file recorded on the recording medium. Therefore, unless the

piece data "D" is obtained as an authorized play requester, it cannot be played. Tertiary unauthorized use can be also prevented.

Not within the rental period of the digital content, the piece data "D" and the like on the memory section 224 is automatically deleted. The content file remains the same. Not within the rental period, the digital content playing device 520 can be used to copy the content file to another recording medium. To play the content file on the recording medium, the digital content playing device 520 can be used to reliably collect charges for secondary and tertiary uses since authentication and payment of the rental fee to the delivery management center 510 are necessary.

The unauthorized play prevention system 500 has: delivery management means which is a server in which a content file having header information and a data body is prepared in a state of lacking part of the header information and the part of the header information is prepared as piece data and delivers the content file via a communication line and manages use of the data body; and a digital content playing device capable of communicating via the communication line with the delivery management means and used for at least playing the content file delivered from the delivery management means, wherein when a request to download the content file is inputted by a user to the digital content playing device, the digital content playing device transmits

the request via the communication line to the delivery management means, the delivery management means transmits the content file related to the request via the communication line to the digital content playing device, thereafter, when a request to play the content file under an authentication condition is inputted by the user to the digital content playing device, the digital content playing device transmits the request via the communication line to the delivery management means, the delivery management means checks authentication of the user related to the request to transmit piece data of the content file related to the request via the communication line to the digital content playing device, and the digital content playing device uses the header information of the transmitted content file and the piece data in play operation to play the data body of the content file. Any design change can be made to the unauthorized play prevention system 500 of such configuration.

The delivery management center 510 has one digital content DB 511, but may have more. In this case, for example, a movie content file may be stored in a first DB and a music content file may be stored in a second DB. That is, different kinds of content files may be stored in DBs. The content files stored in the DBs may be the same to prevent access to the first DB from being concentrated at congestion. The same thing applies to the piece data DB 516. The delivery management center 510 has the digital content DB 511 and the piece data DB 516. The

digital content DB 511 and the piece data DB 516 may be installed in locations different from the delivery management center 510. In this case, the delivery management center 510 authenticates the user to transmit the WEB address of the digital content DB 511 and the piece data DB 516 to the digital content playing device 520. The digital content playing device 520 may access the digital content DB 511 and the piece data DB 516 based on the WEB address to obtain the content file and piece data "D".

As for the digital content DB 511, the content file having the header information "A" and the data body "B" is recorded in a state of lacking the play information "A1" included in the header information a. It can be, of course, recorded in a state of adding other information. As for other information, there is a program or the like which decides whether the playing software is installed on the computer of the user or not, and when deciding that it is not installed, automatically accesses the HP of the delivery management center 510. When the program is recorded and the user executes the obtained content file on his/her own computer (computer corresponding to the digital content playing device 520 in a state that the playing software is not downloaded), the WEB address of the delivery management center 510 is read to automatically access the delivery management center 510 based on this. When obtaining the playing software by the above procedure, the content file on the memory section 524 can be played.

The content of the playing software are only an example. Changing timing at which user registration and user authentication are performed and changing the content or the like is arbitrary. When the content file is recorded on the memory section 524 of the digital content playing device 520 and the rental period has elapsed, the content file may be deleted together with the piece data "D". Aside from the piece data "D", an elapsed period from the point of time at which the content file is received may be determined, and when the elapsed period reaches a predetermined period, the content file may be deleted.

The fifth embodiment can be design changed to a system preventing unauthorized use of the content file delivered for pay or for free, not rented. In this case, it has the same merit as above. The playing software used in this case may only delete processing when the delivered content file is not within the rental period. The digital content playing device 520, without downloading the playing software from the delivery management center 510, may download it via a recording medium such as a CD. As a matter of course, it may be an exclusive device, not a computer.

Needless to say, timing at which the piece data "D" can be obtained can be suitably design changed according to the content of the system.

CLAIMS

[Claim 1]

A system for preventing unauthorized play of digital content adapted to deliver a content file comprising a data body and header information from a delivery management means to a playing device via a communication line, the header information including:

playing information being data showing an address value of a sector necessary for the play of the data body or a size of the data body; and

content information relating to the data body,

the delivery management means being a server comprising a first database where the content file is recorded in a state of lacking the playing information included in the header information and a second database where the playing information is recorded,

the delivery management means, upon receiving a request to download the content file transmitted from the playing device, reading the content file relating to the request from the first database and transmitting the content file to the playing device via the communication line, and thereafter, upon receiving a request to play the content file transmitted from the playing device, reading the playing information of the content file

relating to the request from the second database and transmitting the playing information to the playing device via the communication line, and

the playing device being a device comprising a function capable of communicating with the delivery management means via the communication line,

the playing device, upon receiving an input of a request to download the content file, transmitting the request to the delivery management means via the communication line, and upon receiving the content file correspondingly transmitted from the delivery management means, recording the received content file onto a memory part,

thereafter, the playing device allowing the file name of the downloaded content file to be displayed in list form based on the content information of the content file on the memory part,

thereafter, the playing device, upon receiving an input of an application for the play of the content file, transmitting the application to the delivery management means via the communication line, and upon receiving the playing information correspondingly transmitted from the distribution management means, recording the received playing information onto the memory part, and

thereafter, the playing device, upon receiving an input of a play operation to play the content file, playing the data

body of the content file by means of the header information and the playing information of the content file stored on the memory part.

[Claim 2]

A system for preventing unauthorized play of digital content adapted to deliver a content file comprising a data body and header information from a delivery management means to a playing device via a communication line, the header information including:

playing information being data showing an address value of a sector necessary for the play of the data body or a size of the data body; and

content information relating to the data body,

the delivery management means being a server comprising a first database where the content file is recorded in a state of lacking the playing information included in the header information and a second database where the playing information is recorded,

the delivery management means, upon receiving a request to download the content file transmitted from the playing device, reading the content file relating to the request from the first database and the playing information of the content file from the second database, and transmitting the read content file and playing information to the playing device via the communication

line, and

the playing device being a device comprising a function capable of communicating with the delivery management means via the communication line,

the playing device, upon receiving an input of the request to download the content file, transmitting the request to the delivery management means via the communication line, and upon receiving the content file and the playing information correspondingly transmitted from the delivery management means, recording the received content file and playing information onto a memory part,

thereafter, the playing device allowing the file name of the downloaded content file to be displayed in list form based on the content information of the content file on the memory part, and

thereafter, the playing device, upon receiving an input of an operation for playing the content file, playing the data body of the content file by means of the header information and the playing information of the content file on the memory part.

[Claim 3]

The system for preventing the unauthorized play of the digital content as claimed in Claim 1 or 2, wherein

the playing device can record the content file on a recording medium in place of the memory part.

[Claim 4]

The system for preventing the unauthorized play of the digital content as claimed in Claim 1, 2 or 3, wherein

the playing device starts measurement of a length of elapsed time from a time point when the playing information is recorded on the memory part and sets a flag showing that the content file relating to the playing information is being rented, and when the elapsed time length has reached a predetermined period, the playing information is deleted from the memory part and the flag is reset, and

when the list is displayed based on the content information of the content file on the memory part, the playing device judges whether or not the flag relating to the content file is set, and upon judging that the flag is set, the playing device displays the file name of the content file and that the content file is being rented.

[Claim 5]

The system for preventing the unauthorized play of the digital content as claimed in Claim 1, wherein

upon receiving the application for the play of the content file, the playing device transmits a user ID and a password inputted by a user to the delivery management means, and

the delivery management means further comprises a third

database in which user information including the user ID and the password are recorded, and upon receiving the application for the play of the content file, the user ID and the password transmitted from the playing device , the delivery management means judges whether or not the received user ID and password match the user ID and the password on the third database and transmits the playing information to the playing device only when the match is judged.

[Claim 6]

The system for preventing the unauthorized play of the digital content as claimed in Claim 2, wherein

the playing device transmits to the delivery management means a user ID and a password inputted from a user who requests to download the content file when the request is made, and

the delivery management means further comprises a third database in which user information including the user ID and the password of the playing device are recorded, and upon receiving the request to download the content file, the user ID and the password transmitted from the playing device, the delivery management means judges whether or not the transmitted user ID and password match the user ID and the password on the third database and transmits the playing information to the playing device only when the match is judged.

[Claim 7]

The system for preventing the unauthorized play of the digital content as claimed in Claim 5 or 6, wherein

when the delivery management means judges that the user ID and the password transmitted from the playing device match the user ID and the password included in the user information on the third database, the delivery management means transmits the playing information to the playing device and records charging data in the user information on the third database .

[Claim 8]

A playing device for connection via a communication line to a delivery management means for delivering a content file comprising a data body and header information, the header information including:

playing information being data showing an address value of a sector necessary for the play of the data body or a size of the data body; and

content information relating to the data body, the playing device comprising:

a means for transmitting a request to download a content file to the delivery management device via the communication line upon receiving an input of the request;

a means for recording the content file transmitted from the delivery management means on a memory part upon receiving

the content file;

a means for displaying the file name of the downloaded content file in list form based on the content information of the content file recorded on the memory part;

a means for transmitting an application for play of the content file to the delivery management means via the communication line when the application is inputted;

a means for recording the playing information transmitted from the delivery management means on the memory part when the playing information is received; and

a means for playing the data body of the content file using the header information and the playing information of the content file on the memory part upon receiving an operation input for playing the content file inputted based on the list.

[Claim 9]

A playing device for connection via a communication line to a delivery management means for delivering a content file comprising a data body and header information, the header information including:

playing information being data showing an address value of a sector necessary for the play of the data body or a size of the data body; and

content information relating to the data body, the playing device comprising:

a means for transmitting a request to download a content file to the deliver management device via the communication line upon receiving an input of the request;

a means for recording the content file and the playing information transmitted from the deliver management means on a memory part upon receiving the content file and the playing information;

a means for displaying the file name of the downloaded content file in list form based on the content information of the content file recorded on the memory part; and

a means for playing the data body of the content file using the header information and the playing information of the content file on the memory part upon receiving an operation input for playing the content file inputted based on the list.

[Claim 10]

The playing device as claimed in Claim 8 or 9, comprising a means capable of recording the content file on a recording medium in place of the memory part.

[Claim 11]

The playing device as claimed in Claim 8 or 9, further comprising:

a means for measuring a length of elapsed time from a time point when the playing information is recorded on the memory

part and setting a flag showing that the content file relating to the playing information is being rented;

a means for deleting the playing information from the memory part and resetting the flag when the elapsed time length has reached a predetermined period; and

a means for judging whether or not the flag relating to the content file is set when the list is displayed based on the content information of the content file on the memory part, the means further displaying the file name of the content file and that the content file is being rented upon judging that the flag is set.

[Claim 12]

A method of preventing unauthorized play of digital content adapted to deliver a content file comprising a data body and header information from a delivery management means to a playing device via a communication line, the header information including:

playing information being data showing an address value of a sector necessary for the play of the data body or a size of the data body; and

content information relating to the data body,

the delivery management means being a server comprising a first database where the content file is recorded in a state of lacking the playing information included in the header

information and a second database where the playing information is recorded, and the playing device being adapted to communicate with the delivery management means via the communication line,

the playing device, upon receiving an input of a request to download the content file is inputted to the playing device, transmitting the request to the delivery management means via the communication line,

the delivery management means, upon receiving the request transmitted from the playing device, reading the content file relating to the request from the first database and transmitting the read content file to the playing device via the communication line,

the playing device, upon receiving the content file transmitted from the delivery management means, recording the content file onto the memory part, and allowing the file name of the downloaded content file to be displayed in list form based on the content information of the content file, and

thereafter, the playing device, upon receiving an input of the application for the play of the content file, transmitting the application to the delivery management means via the communication line,

the delivery management means, upon receiving the application for the play of the content file transmitted from the playing device, reading the playing information of the content file relating to the application from the second data

base and transmitting the read playing information to the playing device via the communication line,

the playing device, upon receiving the playing information transmitted from the delivery management means, recording the playing information onto the memory part , and

thereafter, the playing device, upon receiving a play operation input to play the content file, playing the data body of the content file using the header information and the playing information of the content file on the memory part.

[Claim 13]

A method of preventing unauthorized play of digital content adapted to deliver a content file comprising a data body and header information from a delivery management means to a playing device via a communication line, the header information including:

playing information being data showing an address value of a sector necessary for the play of the data body or a size of the data body; and

content information relating to the data body,

the delivery management means being a server comprising a first database where the content file is recorded in a state of lacking the playing information included in the header information and a second database where the playing information is recorded, and the playing device being adapted to communicate

with the delivery management means via the communication line,

the playing device, upon receiving an input of a request to download the content file, transmitting the request to the delivery management means via the communication line,

the delivery management means, upon receiving the request transmitted from the playing device, reading the content file relating to the request from the first database and the playing information of the content file from the second database, and transmitting the read content file and playing information to the playing device via the communication line,

the playing device, upon receiving the content file and playing information transmitted from the delivery management means, recording the content file and the playing information onto the memory part, and allowing the file name of the downloaded content file to be displayed in list form based on the content information of the content file, and

thereafter, the playing device, upon receiving a play operation input to play the content file, playing the data body of the content file using the header information and the playing information of the content file on the memory part.

[Claim 14]

The method of preventing the unauthorized play of the digital content as claimed in Claim 12 or 13, wherein

the playing device records the received content file on

a recording medium in place of the memory part.

[Claim 15]

The method of preventing the unauthorized play of the digital content as claimed in Claim 12, 13 or 14, wherein

the playing device starts measurement of a length of elapsed time from a time point when the playing information is recorded on the memory part and sets a flag showing that the content file relating to the playing information is being rented, the playing device further deleting the playing information from the memory part and reset the flag when the elapsed time length has reached a predetermined period, and

the playing device further judges whether or not the flag relating to the content file is set when the list is displayed based on the content information of the content file on the memory part, and, displays the file name of the content file and that the content file is being rented upon judging that the flag is set.