

DESCRIPTION
INFORMATION PROCESSING DEVICE AND INFORMATION PROCESSING
METHOD

5 TECHNICAL FIELD

[0001]

The present disclosure relates to information processing devices and information processing methods, and more particularly, to an information processing
10 device and an information processing method that are suitable in a case where an application program is executed in conjunction with reproduction of content such as a television program.

15 BACKGROUND ART

[0002]

Information (about the cast, the outline, the trailer, or the like) related to a TV (television) program being aired, and information (such as news,
20 weather forecasts, or traffic information) that is not related directly to the TV program (hereinafter referred to as the television program) but is useful for viewers can be displayed on the screens for the benefit of the viewers of the television program, for example.

25 [0003]

So as to realize this, a command for acquiring and executing a special-purpose application program (hereinafter referred to simply as the application) is transmitted to a TV receiver or the like in conjunction
30 with progress of the television program. In regions such as Japan and Europe, this has already been realized by

transmitting the command and the application using the band for data broadcasting with TV broadcast signals (see Patent Document 1, for example).

[0004]

5 In the United States, on the other hand, any data broadcast band has not been set for TV broadcast signals, and any substitute method has not been established. Therefore, an application cannot be executed in conjunction with progress of a television program.

10 [0005]

 In the United States, the number of households viewing television programs via CATV or IPTV or the like is larger than the number of households viewing television programs by directly receiving TV broadcast waves with a TV receiver. With CATV or IPTV, there are cases where only the signals of images and sound of a television program are extracted from TV broadcast signals and are distributed. Therefore, even if a data broadcast band is set for TV broadcast signals in the United States, there is no guarantee that data broadcast signals including the data of applications will be transmitted to receiving devices.

[0006]

 Furthermore, there is a demand these days for execution of an application in conjunction with desired content that is not necessarily a television program being aired in a case where content such as a recorded television program, a video reproduced from a packaged medium such as a DVD or a BD, or a moving image downloaded from the Internet is being viewed.

30 [0007]

To satisfy this demand, the content being viewed needs to be identified. As a method for realizing this, there are the ACR (Automatic Content Recognition) technology and ACR services using the ACR technology (see Patent Document 2, for example).

[0008]

An ACR service is realized by an ACR client and an ACR server. The ACR client mounted on a TV receiver or the like extracts signature data (such as a watermark or a fingerprint) from the currently-viewed content, notifies the ACR server of the signature data, and requests identification of the content. The ACR server compares the received signature data with the signature data of content registered beforehand in a database, and identifies the content being viewed with a TV receiver or the like. Further, the metadata related to the identified content and the application (hereinafter referred to simply as the linked application) to be executed in conjunction with the content is returned as an ACR response to the ACR client.

[0009]

The ACR client that has received the response acquires the linked application from a predetermined server, and executes the linked application.

25

CITATION LIST

PATENT DOCUMENT

[0010]

Patent Document 1: Japanese Patent Application
Laid-Open No. 2006-50237

30

Patent Document 2: Japanese Patent Application

Laid-Open No. 2012-168801

SUMMARY OF THE INVENTION

PROBLEMS TO BE SOLVED BY THE INVENTION

5 [0011]

In a case where the above described ACR service is realized, the ACR service needs to be managed while the rights of the respective holders of copyrights to the content and the linked application are respected. A
10 method of protecting copyrights has been set for television broadcast programs and content of packaged media or the like.

[0012]

However, any method has not been established to
15 protect copyrights to content related to ACR services and the corresponding linked applications in a forceful manner. Also, there are cases where the holders of copyrights to content and the corresponding linked application are different, and an ACR service that starts
20 the linked application in a manner unintended by the holder of the copyright to the content might be performed. In view of this, there is an urgent need to establish a method of protecting copyrights to content and the corresponding linked applications in a forceful manner
25 and rules for managing the linked applications in the market.

[0013]

Some content copyright holders have started
insisting copyrights not only to content but also to the
30 signature data extracted from the content. In an ACR service in this case, the signature data extracted from

content is used without permission from the holder of the copyright to the content, and the problem of infringement of the right of the content's copyright holder might be caused.

5 [0014]

The present disclosure is made in view of those circumstances, and aims to realize ACR services without any infringement of the rights of the respective holders of copyrights to content and linked applications.

10

SOLUTIONS TO PROBLEMS

[0015]

An information processing device as a first aspect of the present disclosure includes: a content managing
15 unit that manages first content viewable on the side of a content reproduction device that reproduces content; a database unit that generates reference data and turns the generated reference data into a database, the reference data being generated by associating first signature data
20 extracted from the first content with right management information about the first signature data and the content identifier representing the first content from which the first signature data is extracted, the first signature data indicating the features of the first
25 content; and an identifying unit that identifies the content and returns a response indicating an identification result by referring to the reference data of the database unit in reply to a query including second signature data extracted from second content being viewed
30 by the user of the content reproduction device, the query being transmitted from the side of the content

reproduction device, the second signature data indicating the features of the second content.

[0016]

5 The first signature data of the reference data may be encrypted, and the database unit may decrypt the encrypted first signature data through an authentication process with the content managing unit.

[0017]

10 The right management information about the first signature data may include an item for selecting an existing right management method for the first signature data.

[0018]

15 The right management information about the first signature data may further include an item for arbitrarily setting a right management method for the first signature data.

[0019]

20 An information processing method as the first aspect of the present disclosure is an information processing method implemented in an information processing device, and includes: a database forming step of generating reference data and turning the generated reference data into a database, the reference data being
25 generated by associating first signature data extracted from first content with right management information about the first signature data and the content identifier representing the first content from which the first signature data is extracted, the first content being
30 viewable on the side of a content reproduction device that reproduces content, the first signature data

indicating the features of the first content; and an
identifying step of identifying the content and returning
a response indicating an identification result by
referring to the reference data of the database in reply
5 to a query including second signature data extracted from
second content being viewed by the user of the content
reproduction device, the query being transmitted from the
side of the content reproduction device, the second
signature data indicating the features of the second
10 content,

the database forming step and the identifying step
being carried out by the information processing device.
[0020]

In the first aspect of the present disclosure, the
15 reference data is generated by associating the first
signature data extracted from the first content with the
right management information about the first signature
data and the content identifier representing the first
content from which the first signature data is extracted,
20 and the generated reference data is turned into a
database. The first content is viewable on the side of
the content reproduction device that reproduces content,
and the first signature data indicates the features of
the first content. Also, in reply to the query including
25 the second signature data extracted from the second
content being viewed by the user of the content
reproduction device, the content is identified by
referring to the reference data of the database, and a
response indicating an identification result is returned.
30 The query is transmitted from the side of the content
reproduction device, and the second signature data

indicates the features of the second content.

[0021]

A first information processing device in a second aspect of the present disclosure includes: a content
5 managing unit that manages first content viewable on the side of a content reproduction device that reproduces content; a database unit that generates reference data and turns the generated reference data into a database, the reference data being generated by associating first
10 signature data extracted from the first content with a content identifier, an application identifier, and rendering control information, the content identifier representing the first content from which the first signature data is extracted, the application identifier
15 representing the application to be executed on the side of the content reproduction device in conjunction with progress of the first content when the first content is being viewed on the side of the content reproduction device, the rendering control information being for
20 controlling rendering of the application, the first signature data indicating the features of the first content; and an identifying unit that identifies the content and returns a response indicating an identification result by referring to the reference data
25 of the database unit in reply to a query including second signature data extracted from second content being viewed by the user of the content reproduction device, the query being transmitted from the side of the content reproduction device, the second signature data indicating
30 the features of the second content.

[0022]

The rendering control information may include at least one of an item for limiting the device serving as the destination of output of an image from the application, and/or an item for restricting
5 superimposition of an image from the application and an image of the content.

[0023]

A first information processing method in the second aspect of the present disclosure is an information
10 processing method implemented in an information processing device, and includes: a database forming step of generating reference data and turning the generated reference data into a database, the reference data being generated by associating first signature data extracted
15 from first content with a content identifier, an application identifier, and rendering control information, the content identifier representing the first content from which the first signature data is extracted, the application identifier representing the application to be
20 executed on the side of a content reproduction device in conjunction with progress of the first content when the first content is being viewed on the side of the content reproduction device, the rendering control information being for controlling rendering of the application, the
25 first content being viewable on the side of the content reproduction device that reproduces content, the first signature data indicating the features of the first content; and an identifying step of identifying the content and returning a response indicating an
30 identification result by referring to the reference data of the database in reply to a query including second

signature data extracted from second content being viewed
by the user of the content reproduction device, the query
being transmitted from the side of the content
reproduction device, the second signature data indicating
5 a feature of the second content,

the database forming step and the identifying step
being carried out by the information processing device.

[0024]

A second information processing device in the
10 second aspect of the present disclosure includes: a query
generating unit that extracts signature data from the
content being reproduced, generates a query including the
signature data, transmits the query to an identification
server, and receives a response returned from the
15 identification server in reply to the query, the
signature data indicating the features of the content;
and an application executing unit that acquires and
executes an application based on the application
identifier included in the received response, and
20 controls rendering of the application based on rendering
control information about the application, the
application being designated to be executed in
conjunction with progress of the content being reproduced,
the rendering control information being included in the
25 response.

[0025]

Based on the rendering control information, the
application executing unit may perform at least one of a
process for limiting the device serving as the
30 destination of output of an image from the application,
and/or a process for restricting superimposition of an

image from the application and an image of the content.

[0026]

A second information processing method in the second aspect of the present disclosure is an information processing method implemented in an information processing device, and includes: a transmitting step of extracting signature data from the content being reproduced, generating a query including the signature data, and transmitting the query to an identification server, the signature data indicating the features of the content; a receiving step of receiving a response returned from the identification server in reply to the query; and a controlling step of acquiring and executing an application based on the application identifier included in the received response, and controlling rendering of the application based on rendering control information about the application, the application being designated to be executed in conjunction with progress of the content being reproduced, the rendering control information being included in the response,

the transmitting step, the receiving step, and the controlling step being carried out by the information processing device.

[0027]

In the second aspect of the present disclosure, the first information processing device generates reference data and turns the generated reference data into a database by associating the first signature data extracted from the first content with a content identifier, an application identifier, and rendering control information, the content identifier representing

the first content from which the first signature data is extracted, the application identifier representing the application to be executed on the side of the second information processing device in conjunction with
5 progress of the first content when the first content is being viewed on the side of the second information processing device, the rendering control information being for controlling rendering of the application, the first content being viewable on the side of the second
10 information processing device that reproduces content, the first signature data indicating the features of the first content. The first information processing device identifies the content and returns a response indicating an identification result by referring to the reference
15 data of the database unit in reply to a query including the second signature data extracted from the second content being viewed by the user of the second information processing device, the query being transmitted from the side of the second information
20 processing device, the second signature data indicating the features of the second content. Meanwhile, the second information processing device generates the query, transmits the query to the first information processing device, receives the response returned from the first
25 information processing device in reply to the query, acquires and executes the application based on the application identifier included in the received response, and controls rendering of the application based on the rendering control information about the application, the
30 application being designated to be executed in conjunction with progress of the content being reproduced,

the rendering control information being included in the response.

[0028]

A first information processing device in a third
5 aspect of the present disclosure includes: a content
managing unit that manages first content viewable on the
side of a content reproduction device that reproduces
content; a database unit that generates reference data
and turns the generated reference data into a database,
10 the reference data being generated by associating first
signature data extracted from the first content with a
content identifier, an application identifier, and right
management information about an application, the content
identifier representing the first content from which the
15 first signature data is extracted, the application
identifier representing the application to be executed on
the side of the content reproduction device in
conjunction with progress of the first content when the
first content is being viewed on the side of the content
20 reproduction device, the first signature data indicating
the features of the first content; and an identifying
unit that identifies the content and returns a response
indicating an identification result by referring to the
reference data of the database unit in reply to a query
25 including second signature data extracted from second
content being viewed by the user of the content
reproduction device, the query being transmitted from the
side of the content reproduction device, the second
signature data indicating the features of the second
30 content.

[0029]

The right management information about the application may include an item for selecting an existing right management method for the application and content cited by the application.

5 [0030]

The right management information about the application may further include an item for arbitrarily setting a right management method for the application and the content cited by the application.

10 [0031]

A first information processing method in the third aspect of the present disclosure is an information processing method implemented in an information processing device, and includes: a database forming step
15 of generating reference data and turning the generated reference data into a database, the reference data being generated by associating first signature data extracted from first content with a content identifier, an
application identifier, and right management information
20 about an application, the content identifier representing the first content from which the first signature data is extracted, the application identifier representing the application to be executed on the side of a content
reproduction device in conjunction with progress of the
25 first content when the first content is being viewed on the side of the content reproduction device, the first content being viewable on the side of the content reproduction device that reproduces content, the first signature data indicating the features of the first
30 content; and an identifying step of identifying the content and returning a response indicating an

identification result by referring to the reference data of the database unit in reply to a query including second signature data extracted from second content being viewed by the user of the content reproduction device, the query
5 being transmitted from the side of the content reproduction device, the second signature data indicating the features of the second content,

the database forming step and the identifying step being carried out by the information processing device.

10 [0032]

A second information processing device in the third aspect of the present disclosure includes: a query generating unit that extracts signature data from the content being reproduced, generates a query including the
15 signature data, transmits the query to an identification server, and receives a response returned from the identification server in reply to the query, the signature data indicating the features of the content; and an application executing unit that acquires and
20 executes an application based on the application identifier included in the received response, and manages the application and the content cited by the application based on right management information about the application, the application being designated to be
25 executed in conjunction with progress of the content being reproduced, the right management information being included in the response.

[0033]

The application executing unit may decrypt the
30 application based on the right management information, the application being encrypted.

[0034]

The application executing unit may manage copying of the application and the cited content based on the right management information.

5 [0035]

A second information processing method in the third aspect of the present disclosure is an information processing method implemented in an information processing device, and includes: a transmitting step of
10 extracting signature data from the content being reproduced, generating a query including the signature data, and transmitting the query to an identification server, the signature data indicating the features of the content; a receiving step of receiving a response
15 returned from the identification server in reply to the query; and a managing step of acquiring and executing an application based on the application identifier included in the received response, and managing the application and the content cited by the application based on right
20 management information about the application, the application being designated to be executed in conjunction with progress of the content being reproduced, the right management information being included in the response,
25 the transmitting step, the receiving step, and the managing step being carried out by the information processing device.

[0036]

In the third aspect of the present disclosure, the
30 first information processing device generates reference data and turns the generated reference data into a

database by associating the first signature data
extracted from the first content with a content
identifier, an application identifier, and the right
management information about the application, the content
5 identifier representing the first content from which the
first signature data is extracted, the application
identifier representing the application to be executed on
the side of the second information processing device in
conjunction with progress of the first content when the
10 first content is being viewed on the side of the second
information processing device, the first content being
viewable on the side of the second information processing
device that reproduces content, the first signature data
indicating the features of the first content. The first
15 information processing device identifies the content and
returns a response indicating an identification result by
referring to the reference data of the database unit in
reply to a query including the second signature data
extracted from the second content being viewed by the
20 user of the second information processing device, the
query being transmitted from the side of the second
information processing device, the second signature data
indicating the features of the second content. Meanwhile,
the second information processing device generates the
25 query, transmits the query to the first information
processing device, receives the response returned from
the first information processing device in reply to the
query, acquires and executes the application based on the
application identifier included in the received response,
30 and manages the application and the content cited by the
application based on the right management information

about the application, the application being designated to be executed in conjunction with progress of the content being reproduced, the right management information being included in the response.

5

EFFECTS OF THE INVENTION

[0037]

According to the first aspect of the present disclosure, ACR services using unauthorized signature data can be prevented.

10

[0038]

According to the second aspect of the present disclosure, rendering of the application to be executed in conjunction with progress of content can be restricted.

15

[0039]

According to the third aspect of the present disclosure, infringement of the right to the application to be executed in conjunction with progress of content and the right to the cited content can be prevented.

20

BRIEF DESCRIPTION OF DRAWINGS

[0040]

Fig. 1 is a block diagram showing an example configuration of an application linkage system as an embodiment of the present disclosure.

25

Fig. 2 is a block diagram showing an example structure of the ACR server.

Fig. 3 is a block diagram showing an example structure of the ACR client.

30

Fig. 4 is a diagram showing the data structure of ACR reference data.

Fig. 5 is a diagram showing the data structure of signature data copy control information (SCM).

Fig. 6 is a diagram showing the data structure of linked application rendering information (ARM).

5 Fig. 7 is a diagram showing the data structure of linked application copy control information (ACM).

Fig. 8 is a diagram showing the data structure of an ACR query.

10 Fig. 9 is a diagram showing the data structure of an ACR response.

Fig. 10 is a flowchart for explaining operation of the application linkage system.

Fig. 11 is a flowchart for explaining operation of the application linkage system.

15 Fig. 12 is a block diagram showing an example structure of a computer.

MODES FOR CARRYING OUT THE INVENTION

[0041]

20 The following is a detailed description of best modes for carrying out the present disclosure (hereinafter referred to as embodiments), with reference to the drawings.

[0042]

25 [Example Configuration of an Application Linkage System]

Fig. 1 shows an example configuration of an application linkage system as an embodiment of the present disclosure.

30 [0043]

This application linkage system 10 identifies the

content a user is viewing on the screen of a TV receiver or the like, and executes an application (hereinafter referred to as the linked application) in conjunction with progress of the content.

5 [0044]

Here, the content is not limited to a television program being aired and received by a TV receiver or the like. Examples of the content include various kinds of audio/visual content such as a television program
10 recorded by a video recorder or the like, a video such as a movie reproduced from a packaged medium, and a moving image downloaded via the Internet. The content may also include commercial messages (hereinafter referred to as CMs) inserted between television programs or into a
15 television program.

[0045]

The linked application can display the information related to the content being viewed, such as the summary of the content and the metadata of the cast, or introduce
20 a shopping site where the products shown in the images of the content (the clothes the cast members are wearing, or the items being used by the cast members) can be purchased. The linked application can also guide the user to downloading and viewing other content related to
25 the current content. The other content to which the user is guided by the linked application in this case is referred to as the cited content.

[0046]

In identifying content, the ACR technology is used.
30 By the ACR technology, the content being viewed is identified through a comparison between the signature

data (feature amount) periodically extracted from the content being viewed and the signature data of the content registered beforehand in a database.

[0047]

5 The application linkage system 10 is formed with a provider system 20 located on a side that supplies content and linked applications, and a home network system 30 located in the user's home or the like. The provider system 20 and the home network system 30 are
10 connected to each other via a broadcast network 11 and a bidirectional communication network 12.

[0048]

 The broadcast network 11 may be a TV broadcast network, a CATV network, an IPTV network, or the like.
15 The bidirectional communication network 12 indicates an IP communication network that is typically the Internet.

[0049]

 The home network system 30 is formed by connecting a primary screen device 30A and a second screen device
20 30B with a wireless LAN, for example. The primary screen device 30A is formed with a TV receiver or the like having a broadcast reception tuner function. The second screen device 30B is formed with a portable terminal device not having a broadcast reception tuner function,
25 such as a portable telephone device, a smartphone, a tablet computer, or a slate PC. A portable terminal device having a broadcast reception tuner function may be used as the second screen device 30B.

[0050]

30 [Description of the Provider System 20]

 The provider system 20 is formed with a content

server 21, an application server 22, and an ACR server 23.

[0051]

The content server 21 broadcasts content such as television programs and CMS via the broadcast network 11.

5 The content server 21 also supplies the broadcast content and the metadata corresponding to the broadcast content, to the ACR server 23.

[0052]

The metadata includes the signature data of the
10 content, signature data copy control information that is the copyright information about the signature data, the identifier of the corresponding linked application, linked application rendering information for restricting the rendering destinations of the linked application,
15 linked application copy control information that is the copyright information about the linked application, and the like.

[0053]

Hereinafter, the signature data copy control
20 information will be referred to simply as the SCM (Signature data Copy Management) information. The linked application rendering information will be referred to simply as the ARM (linked Application Rendering Management) information. The linked application copy
25 control information will be referred to simply as the ACM (linked Application Copy Management) information.

[0054]

In response to a request from the side of the home network system 30, the application server 22 supplies a
30 linked application and the data to be used by the linked application via the bidirectional communication network

12. Here, the linked application and the data to be used by the linked application may be encrypted by the DRM (Digital Rights Management) technology.

[0055]

5 The ACR server 23 holds a database that is prepared beforehand and contains ACR reference data that associates the signature data extracted at predetermined sampling intervals from various kinds of content to be viewed on the side of the home network system 30, with
10 content identifiers, application identifiers, signature data copy control information, linked application rendering information, linked application copy control information, and the like.

[0056]

15 Based on the database of the ACR reference data, the ACR server 23 generates and returns an ACR response in reply to an ACR query transmitted from an ACR client 32 on the side of the home network system 30.

[0057]

20 The content server 21, the application server 22, and the ACR server 23 constituting the provider system 20 may be placed at one location, or may be dispersed at different locations. The content server 21, the application server 22, and the ACR server 23 may be
25 combined as appropriate. Furthermore, there may be more than one content server 21, more than one application server 22, and more than one ACR server 23.

[0058]

[Description of the Home Network System 30]

30 The primary screen device 30A of the home network system 30 includes a content renderer 31, the ACR client

32, and an application manager 33. The second screen device 30B includes the same components as above.

[0059]

5 The content renderer 31 acquires and divides all the content to be displayed on the display of a TV receiver or the like serving as the primary screen device 30A, and supplies the content to the ACR client 32. That is, the content renderer 31 acquires and divides not only the content broadcast from the content server 21 but also
10 the content that is input via various input terminals (such as HDMI (registered trademark) terminals) of a TV receiver or the like, and supplies the content to the ACR client 32.

[0060]

15 The ACR client 32 extracts signature data indicating the features of content at predetermined sampling intervals from the content that is input from the content renderer 31. Here, the signature data extraction method is the same as the extraction method
20 (described later) used by the ACR server 23 of the provider system 20.

[0061]

 The ACR client 32 also generates an ACR query including the extracted signature data, and transmits the
25 ACR query to the ACR server 23 of the provider system 20 via the bidirectional communication network 12. The ACR client 32 also receives and holds an ACR response returned from the ACR server 23 in reply to the transmitted ACR query. The ACR client 32 further
30 analyzes the held ACR response, transfers the linked application rendering information and the linked

application copy control information corresponding to the content being viewed to the application manager 33, and causes the application manager 33 to execute the linked application in conjunction with the progress of the content.

[0062]

Based on related metadata, the linked application copy control information, the linked application rendering information, and the like supplied from the ACR client 32, the application manager 33 acquires the linked application corresponding to the content being viewed from the application server 22 via the bidirectional communication network 12, and executes the linked application.

[0063]

In accordance with the linked application rendering information, the application manager 33 can set not only the primary screen device 30A but also the second screen device 30B (as will be described later in detail) as the rendering destination of the linked application (or the destination of image display by the linked application).

[0064]

[Specific Example Structure of the ACR Server 23]

Fig. 2 shows a specific example structure of the ACR server 23 included in the provider system 20.

[0065]

The ACR server 23 is formed with a content acquiring unit 41, a reference signature extracting unit 42, an ACR database unit 43, an ACR response generating unit 44, a signature DRM encrypting unit 45, and a signature DRM decrypting unit 46.

[0066]

The content acquiring unit 41 acquires, from the content server 21, content to be broadcast by the content server 21 via the broadcast network 11 and the metadata (including related metadata, SCM information, ARM information, ACM information, and the like) corresponding to the content, and supplies the acquired content to the reference signature extracting unit 42. The content acquiring unit 41 also acquires, from outside, various kinds of content to be viewed on the side of the home network system 30 and the metadata corresponding to the content, and supplies the content and the metadata to the reference signature extracting unit 42.

[0067]

Using a predetermined extraction method, the reference signature extracting unit 42 extracts the signature data indicating the features of the content at predetermined sampling intervals from the content supplied from the content acquiring unit 41, and outputs the signature data to the ACR database unit 43. The reference signature extracting unit 42 also causes the signature DRM encrypting unit 45 to encrypt the extracted signature data through a predetermined DRM encryption process based on the SCM information included in the metadata corresponding to the input content. However, there are cases where the encryption is not performed depending on the contents of the SCM information.

[0068]

The signature data extraction method used at the reference signature extracting unit 42 may be an existing method. For example, the watermark embedded beforehand

in the content may be extracted and set as the signature data, or a fingerprint may be calculated and set as the signature data.

[0069]

5 Where a fingerprint is used as the signature data, identical signature data can be obtained before and after conversion of the resolution, the aspect ratio, the bit rate, the encoding format, or the like of the content. Accordingly, the identification accuracy in a case where
10 content identification is performed based on the signature data can be increased.

[0070]

 In a case where there is more than one ACR server 23, the same signature data extraction method is not
15 necessarily used at the reference signature extracting units 42, and a different extraction method may be employed for each ACR server 23.

[0071]

 The ACR database unit 43 generates and stores ACR
20 reference data that associates the respective pieces of signature data that has been extracted by the reference signature extracting unit 42 and been DRM-encrypted as necessary, with the content identifiers representing the content from which the signature data has been extracted.
25 With this, the signature data that has been extracted from the content and been DRM-encrypted is turned into a database.

[0072]

 In a case where more than one ACR server 23 exists,
30 and a different signature data extraction method is employed at the reference signature extracting unit 42 of

each ACR server 23, the ACR reference data having the signature data associated with the SCM information, the ARM information, and the ACM information integrated for each piece of content is turned into a database in each
5 corresponding ACR database unit 43. The data structure of the ACR reference data will be described later with reference to Fig. 4.

[0073]

By referring to the ACR database unit 43, the ACR
10 response generating unit 44 identifies the content from which the signature data included in the ACR query transmitted from the ACR client 32 has been extracted. In this identification, if the signature data is DRM-encrypted, the ACR database unit 43 causes the signature
15 DRM decrypting unit 46 to decrypt the signature data based on the SCM information included in the ACR reference data, and then compares the decrypted signature data with the signature data included in the ACR query.

[0074]

20 The ACR response generating unit 44 further generates an ACR response as an identification result including the content identifier, the related metadata, the ARM information, the ACM information, and the like. Under the control of a profile matching server 24, the
25 ACR response generating unit 44 further performs matching and filtering on the related metadata stored in the ACR response, and transmits the ACR response to the reception apparatus 30. The data structure of the ACR response will be described later with reference to Fig. 9.

30 [0075]

In accordance with a request from the reference

signature extracting unit 42, the signature DRM
encrypting unit 45 encrypts signature data extracted by
the reference signature extracting unit 42 through a
predetermined DRM encryption process. In doing so, the
5 signature DRM encrypting unit 45 performs an
authentication process with the content server 21, and
then performs a necessary key exchange with the content
server 21. Accordingly, the copyrights to both the
content and the signature data thereof can be protected
10 for the holder of the copyright to the content, and
unauthorized use of the signature not involving the
content server 21 can be prevented when an ACR service is
performed.

[0076]

15 In accordance with a request from the ACR database
unit 43, the signature DRM decrypting unit 46 decrypts
the DRM-encrypted signature data included in the ACR
reference data. In doing so, the signature DRM
decrypting unit 46 performs an authentication process
20 with the content server 21 based on the SCM information
included in the ACR reference data, and then performs the
key exchange necessary for the DRM decryption process
with the content server 21. Accordingly, the copyrights
to both the content and the signature data thereof can be
25 protected for the holder of the copyright to the content,
and unauthorized use of the signature not involving the
content server 21 can be prevented when an ACR service is
performed.

[0077]

30 Specifically, the signature data is extracted from
broadcast content (a television program), for example,

without permission from the broadcast station holding the copyright to the content. ACR reference data is then generated, an unauthorized ACR server 23 is activated, and an ACR service is performed. In this case, the
5 unauthorized ACR server 23 performs an authentication process with the content server 21, but is not authenticated as an authorized ACR server 23 by the content server 21. Accordingly, by analyzing the log of the content server 21, the holder of the copyright to the
10 content can detect the existence of the ACR server 23 performing the unauthorized ACR service, and eliminate the ACR server 23.

[0078]

[Specific Example Structure of the ACR Client 32]

15 Fig. 3 shows a specific example structure of the ACR client 32 in the primary screen device 30A.

[0079]

The ACR client 32 is formed with a signature extracting unit 51, an ACR query generating unit 52, a
20 communication unit 53, and an ACR response analyzing unit 54.

[0080]

The signature extracting unit 51 extracts the signature data indicating the features of content at
25 predetermined sampling intervals from the content that branches off and is supplied from the content renderer 31, and outputs the signature data to the ACR query generating unit 52. The signature data extraction method employed at the signature extracting unit 51 is the same
30 as that employed at the reference signature extracting unit 42 of the ACR server 23 being used.

[0081]

The ACR query generating unit 52 generates an ACR query that includes the signature data extracted by the signature extracting unit 51, and is to be used for
5 requesting the ACR server 23 to identify the content. The data structure of the ACR query will be described later with reference to Fig. 8.

[0082]

The communication unit 53 transmits the ACR query
10 generated by the ACR query generating unit 52 to the ACR server 23, receives an ACR response returned from the ACR server 23, and outputs the ACR response to the ACR response analyzing unit 54. The ACR response analyzing unit 54 analyzes the ACR response, and notifies the
15 application manager 33 of the related metadata, the linked application copy control information, the linked application rendering information, and the like, which are included in the ACR response. The application manager 33 acquires and executes the linked application
20 based on this notification.

[0083]

[Data Structure of the ACR Reference Data]

Fig. 4 shows the data structure of the ACR reference data turned into a database in the ACR database
25 unit 43 of the ACR server 23.

[0084]

In the ACR reference data 60, each piece of signature data 61 periodically extracted from content is associated with a content identifier 62, a reproduction
30 time 63, related metadata 64, SCM information 65, ARM information 66, and ACM information.

[0085]

The signature data 61 is extracted from content by the reference signature extracting unit 42, and is DRM-encrypted by the signature DRM encrypting unit 45 as
5 necessary. The content identifier 62 is the information for identifying the content from which the signature data 61 has been extracted. The reproduction time 63 indicates the progress of the content at the time when the signature data 61 is extracted from the content
10 represented by the content identifier 62, and is represented by the time that has elapsed from the top of the content.

[0086]

The related metadata 64 includes the metadata of
15 the content represented by the content identifier 62, the application identifier representing the linked application to be executed in conjunction with the progress of the content indicated by the reproduction time 63 and the supplier (the application server 22 in
20 this case) of the linked application, various kinds of data to be used by the linked application to be executed, and the like.

[0087]

The related metadata 64 may vary with the progress
25 of the content indicated by the reproduction time 63.

[0088]

The SCM information 65 indicates whether the signature data 61 needs to be protected by copyright like the content. If the signature data 61 needs to be
30 protected by copyright, the SCM information 65 is the information for defining the contents of an appropriate

copyright protection process. With the SCM information 65, copyright protection for each piece of the periodically-extracted signature data 61 can be realized.
[0089]

5 Fig. 5 shows an example data structure in a case where the SCM information 65 is defined in 16 bits.
[0090]

 The 16-bit SCM information 65 includes, from the MSB side, a flag (Bit 15) indicating whether DRM control
10 is to be performed, and flags (Bits 14 through 11) for selecting a DRM method from among three standardized methods and one unstandardized local method if DRM control is to be performed. The 16-bit SCM information 65 further includes flags (Bits 7 through 1) for defining
15 specific details (such as copy protection or copy permission only for one generation) of the DRM control for the signature data 61 in a case where the unstandardized local method is selected, and reserve flags (Bits 10 through 8, and Bit 0) reserved for future
20 expansion.
[0091]

 For example, in a case where the signature data 61 is extracted from content with DRM information indicating copy protection, and the holder of the copyright to the
25 content requests the same copyright management for the signature data 61 as the copyright management for the content while requesting management of the signature data 61 by DTCP/IP, which is a standardized DRM control method, the SCM information 65 is 1100 0000 1000 0000'b.
30 [0092]

 Referring back to Fig. 4, the ARM information 66 is

the information for defining execution and the destination of image display (the rendering destination) of the linked application determined to be executed in conjunction with the progress of the content from which the signature data 61 has been extracted.

[0093]

Fig. 6 shows an example data structure in a case where the ARM 66 is defined in 8 bits.

[0094]

The 8-bit ARM information 66 includes, from the MSB side, a flag (Bit 7) for allowing display anywhere on the primary screen device 30A, a flag (Bit 6) for allowing display on the primary screen device 30A but not allowing display superimposition on content, a flag (Bit 5) for allowing display anywhere on the second screen device 30B, and a flag (Bit 4) for allowing display on the second screen device 30B but not allowing display superimposition on content. The 8-bit ARM information 66 also includes a flag (Bit 3) for allowing display anywhere on the primary screen device 30A and second screen device 30B, a flag (Bit 2) for allowing display anywhere on the primary screen device 30A and the second screen device 30B but not allowing display superimposition on content, and a flag (Bit 1) for prohibiting display on any device. The 8-bit ARM information 66 further includes a reserve flag (Bit 0) reserved for future expansion.

[0095]

For example, in a case where the display relationship between content and the application is adjusted by the respective copyright holders, and as a

result, rendering of the linked application on the primary screen device 30A is allowed but display of the linked application on the content is prohibited, the ARM information 66 is 0100 0000'b.

5 [0096]

Referring back to Fig. 4, the ACM information 67 is for displaying copyright information about the linked application determined to be executed in conjunction with progress of the content from which the signature data 61 has been extracted, cited content, and the like. The copyright information is defined by the holder of the copyright to the linked application.

[0097]

Fig. 7 shows an example data structure in a case where the ACM information 67 is defined in 16 bits.

[0098]

The 16-bit ACM information 67 includes, from the MSB side, a flag (Bit 15) indicating whether DRM control is to be performed, and flags (Bits 14 through 11) for selecting a DRM method from among three standardized methods and one unstandardized local method if DRM control is to be performed. The 16-bit ACM information 67 further includes flags (Bits 7 through 1) for defining specific details (such as copy protection or copy permission only for one generation) of the linked application DRM control in a case where the unstandardized local method is selected, and reserve flags (Bits 10 through 8, and Bit 0) reserved for future expansion.

30 [0099]

For example, in a case where the holder of the

copyright to the linked application determines to manage the liked application and cited content by PlayReady (a trade name), which is a standardized DRM control method, and allows unlimited copying, the ACM information 67 is

5 1010 0000 0000 0100'b.

[0100]

[Data Structure of an ACR Query]

Fig. 8 shows the data structure of an ACR query generated by the ACR query generating unit 52 of the ACR client 32.

10

[0101]

The ACR query 70 includes an ACR query identifier 71, an extraction method identifier 72, a service identifier 73, signature data 74, a local time stamp 75, a sender address 76, and a signature 77.

15

[0102]

The ACR query identifier 71 is the information for uniquely identifying the ACR query 70. The extraction method identifier 72 is the information for identifying the extraction method used in extracting the signature data 74. The service identifier 73 is the information for selecting the ACR server 23 to obtain an ACR response in reply to transmission of the ACR query 70 in a case where more than one ACR server 23 exists.

20

25 [0103]

The signature data 74 is extracted from the content at the ACR client 32. The local time stamp 75 indicates the time at which the signature data 74 is extracted from the content, and is represented by the time indicated by the local system clock of the primary screen device 30A.

30

[0104]

The sender address 76 is the address of the ACR client 32 transmitting the ACR query 70 in the bidirectional communication network 12, and is to be used as the information indicating the address to which the ACR response generated at the ACR server 23 in reply to the ACR query 70 is to be returned. The signature 77 is for preventing falsification of the ACR query 70. The entire ACR query 70 may be encrypted and transmitted independently of the copyright to the content.

10 [0105]

[Data Structure of an ACR Response]

Fig. 9 shows the data structure of an ACR response generated by the ACR response generating unit 44 of the ACR server 23.

15 [0106]

The ACR response 80 has the data structure shown in A or B in the drawing. A in the drawing shows the data structure of the ACR response 80 in a case where the content from which the signature data 74 included in the ACR query 70 has been extracted is identified, or where the content being viewed with the primary screen device 30A is identified. B in the drawing shows the data structure of the ACR response 80 in a case where the content cannot be identified.

25 [0107]

The ACR response 80 in a case where the content being viewed with the primary screen device 30A can be identified (A in the drawing) includes an ACR query identifier 81, an extraction method identifier 82, a service identifier 83, a content identifier 84, ACM information 85, ARM information 86, a reproduction time

87, a local time stamp 88, related metadata 89, a sender address 90, and a signature 91.

[0108]

Meanwhile, the ACR response 80 in a case where the
5 content being viewed with the primary screen device 30A cannot be identified (B in the drawing) includes an ACR query identifier 81, a service identifier 83, a sender address 90, a signature 91, and a failed identification flag 92.

10 [0109]

The ACR query identifier 81, the extraction method identifier 82, the service identifier 83, and the local time stamp 88 are for identifying the ACR query 70 requesting a return of the ACR response 80, and are
15 written by citing the ACR query identifier 71, the extraction method identifier 72, the service identifier 73, and the local time stamp 75 of the ACR query 70.

[0110]

The content identifier 84, the ACM information 85,
20 the ARM information 86, the reproduction time 87, and the related metadata 89 are for indicating a result of content identification, and are written by citing the content identifier 62, the ARM information 66, the ACM information 67, the reproduction time 63, and the related
25 metadata 64 of the corresponding ACR reference data 60.

[0111]

The sender address 90 is the address of the ACR server 24 transmitting the ACR response 80 in the bidirectional communication network 12. The signature 91
30 is for preventing falsification of the ACR response 80. The entire ACR response 80 may be encrypted and

transmitted independently of the copyright to the content so that falsification of the ACR response 80 is prevented.

[0112]

The failed identification flag 92 is the flag
5 indicating that the content from which the signature data 74 included in the ACR query 70 from the ACR client 32 has been extracted, or the content being viewed with the primary screen device 30A, cannot be identified at the ACR server 23.

10 [0113]

[Operation of the Application Linkage System 10]

Fig. 10 is a flowchart for explaining operation of the application linkage system 10.

[0114]

15 In the provider system 20, in step S11 as the preprocessing for starting broadcasting of content via the broadcast network 11, the content to be broadcast thereafter and the related metadata 64 are supplied to the ACR server 23. The ACR server 23 extracts signature
20 data at predetermined intervals from the supplied content, performs DRM encryption as necessary, generates the ACR reference data 60 including the related metadata 64, the SCM information 65, the ARM information 66, and the ACM information 67 for each piece of the signature data, and
25 registers the ACR reference data 60 in the ACR database unit 43.

[0115]

The ACR server 23 generates the corresponding ACR reference data 60 not only for the content to be
30 broadcast but also for various kinds of content that can be viewed on the side of the home network system 30, and

turns the ACR reference data 60 into a database. After the ACR reference data 60 corresponding to various kinds of content is turned into a database in this manner, steps S12 through S15 described below are repeated.

5 [0116]

In step S12, the content server 21 of the provider system 20 starts broadcasting the content via the broadcast network 11.

[0117]

10 In the home network system 30, on the other hand, steps S21 through S24 described below are repeated while content (not limited to the broadcast content) is being viewed.

[0118]

15 In step S21, the content renderer 31 of the primary screen device 30A acquires the content being viewed, and outputs the content to the ACR client 32 in a branched manner. In step S22, the ACR client 32 extracts the signature data 74 at predetermined sampling intervals
20 from the currently-viewed content that is input from the content renderer 31 in a branched manner.

[0119]

In step S23, the ACR client 32 generates the ACR query 70 including the signature data 74 every time the signature data 74 is extracted, and transmits the ACR
25 query 70 to the ACR server 23.

[0120]

The ACR server 23 that has received the ACR query 70 identifies the content from which the signature data
30 74 included in the ACR query 70 has been extracted.

[0121]

Specifically, in step S13, the ACR database unit 43 acquires the key necessary in the DRM decryption process from the content server 21 and decrypts the DRM-encrypted signature data 61 in a case where the signature data 61 of the ACR reference data 60 turned into a database is
5 DRM-encrypted.

[0122]

In step S14, the ACR response generating unit 44 of the ACR server 23 refers to the ACR database unit 43 and
10 identifies the content from which the signature data 74 included in the received ACR query 70 has been extracted.

[0123]

In step S15, the ACR response generating unit 44 generates the ACR response 80 in accordance with a result
15 of the content identification, and returns the generated ACR response 80 to the ACR client 32 that has sent the ACR query 70.

[0124]

In step S24, the ACR client 32 that has received
20 the ACR response 80 analyzes the related metadata 89 included in the ACR response 80, and causes the application manager 33 to acquire and execute the linked application that should be executed in conjunction with progress of the content being viewed. Based on the
25 application identifier included in the related metadata 89, the application manager 33 acquires the linked application from the application server 22, and executes the linked application. In doing so, the application manager 33 analyzes the ACM information 85 and the ARM
30 information 86 included in the ACR response 80, decrypts the DRM-encrypted linked application, determines the

destination of the rendering of the linked application,
and performs cited content DRM control as well as
executing the linked application.

[0125]

5 The above described procedures in steps S12 through
S15 and the above described procedures in steps S21
through 24 are repeatedly carried out while the content
is being viewed on the side of the home network system 30.
Accordingly, the linked application can be executed in
10 conjunction with progress of the content being viewed.

[0126]

[Specific Operations in the Linked Application
Rendering Control and the DRM Decryption Process]

Fig. 11 is a flowchart for explaining in detail the
15 operations in the linked application rendering control
and the DRM decryption process to be performed between
the ACR server 23 and the application server 22 of the
provider system 20, and the ACR client 32 and the
application manager 33 of the primary screen device 30A.

20 [0127]

The procedures in steps S31 and S32 in the provider
system 20 described below are repeatedly carried out
while content is being viewed with the primary screen
device 30A.

25 [0128]

In step S31, the ACR server 23 identifies the
content in response to the ACR query 70 from the ACR
client 32, generates the ACR response 80 corresponding to
a result of the identification, and returns the ACR
30 response 80 to the ACR client 32.

[0129]

In step S41, the ACR client 32 that has received the ACR response 80 analyzes the ACR response 80. In step S42, the ACR client 32 determines whether the content being viewed has been successfully identified.

5 [0130]

Specifically, a check is made to determine whether the identification is successful based on whether the failed identification flag 92 is included in the ACR response 80. In a case where the failed identification
10 flag 92 is included in the ACR response 80, and the identification is determined to be unsuccessful, the process returns to step S41. In a case where the failed identification flag 92 is not included in the ACR response 80, and the identification is determined to be
15 successful, on the other hand, the process moves on to step S43. In this case, the data structure of the ACR response 80 is as shown in A in Fig. 9, and includes the ACM information 85 and the ARM information 86.

[0131]

20 In step S43, the ACR client 32 notifies the application manager 33 of the application identifier of the linked application in the related metadata 89, the ACM information 85, and the ARM information 86, which are included in the ACR response 80. Based on the
25 application identifier, the application manager 33 accesses the application server 22, and requests the linked application. The application manager 33 also analyzes the ACM information 85 and the ARM information 86.

30 [0132]

In step S44, based on a result of the analysis of

the ARM information 86, the application manager 33 sets the destination of the rendering of the linked application to be executed in conjunction with the content being viewed, and determines whether display is to be superimposed on the content. In step S45, based on the ACM information 85, the application manager 33 sets a decryption method (or sets the software module or the like for performing the DRM decryption process) in a case where the linked application to be executed in conjunction with the content being viewed is DRM-encrypted. In step S46, the application manager 33 further acquires the key necessary in the decryption process through a decryption authentication process in a case where the linked application is DRM-encrypted.

[0133]

Meanwhile, in step S32, the application server 22 of the provider system 20 supplies the linked application in a DRM-encrypted state (or in an unencrypted state) to the application manager 33 in response to the request that has been made by the application manager 33 in step S43. In step S47, the application manager 33 that has received the linked application uses the key acquired in step S46 and decrypts the received linked application in a DRM-encrypted state (or in an unencrypted state) according to the decryption method defined by the ACM information 85.

[0134]

In step S48, the application manager 33 executes the decrypted linked application, and controls the rendering by the linked application based on the setting performed in step S44.

[0135]

Through the above described operations, the rendering of the linked application and the DRM control can be performed, with the intentions of the respective
5 holders of the copyrights to the linked application and the content being reflected.

[0136]

As described above, in this embodiment, the copyright information about the signature data extracted
10 from content is defined as the SCM information 65. Accordingly, an unauthorized ACR service without permission from the holder of the copyright to the content can be prevented.

[0137]

15 Also, the ARM information 66 as the operation control information for the linked application to be executed in conjunction with progress of content can be set by the holder of the copyright to the content. Accordingly, the linked application can be executed,
20 while the rights and the intentions of both holders of the copyrights to the content and the linked application are reflected. Accordingly, the holder of the copyright to the content can prevent execution of a linked application that might infringe the copyright. Meanwhile,
25 the holder of the copyright to the linked application can prevent rendering in an unintended device.

[0138]

Furthermore, the ACM information 67 for copyright protection for the linked application and the content
30 cited by the linked application is defined in this embodiment. Accordingly, unauthorized copying of the

linked application and the cited content can be prevented.

[0139]

Meanwhile, each of the provider system 20 and the primary screen device 30A that perform the above

5 described series of processes may be formed with hardware, or may be realized by a computer executing software.

This computer may be a computer incorporated into special-purpose hardware, or may be a general-purpose personal computer that can execute various kinds of

10 functions as various kinds of programs are installed thereinto.

[0140]

Fig. 12 is a block diagram showing an example structure of the hardware of the above mentioned computer.

15 [0141]

In this computer 200, a CPU (Central Processing Unit) 201, a ROM (Read Only Memory) 202, and a RAM (Random Access Memory) 203 are connected to one another by a bus 204.

20 [0142]

An input/output interface 205 is further connected to the bus 204. An input unit 206, an output unit 207, a storage unit 208, a communication unit 209, and a drive 210 are connected to the input/output interface 205.

25 [0143]

The input unit 206 is formed with a keyboard, a mouse, a microphone, and the like. The output unit 207 is formed with a display, a speaker, and the like. The storage unit 208 is formed with a hard disk, a
30 nonvolatile memory, or the like. The communication unit 209 is formed with a network interface or the like. The

drive 210 drives a removable medium 211 such as a magnetic disk, an optical disk, a magnetooptical disk, or a semiconductor memory.

[0144]

5 In the computer 200 having the above described structure, the CPU 201 loads the programs stored in the storage unit 208 into the RAM 203 via the input/output interface 205 and the bus 204, and executes the programs, so that the above described series of processes are
10 performed.

[0145]

 The programs to be executed by the computer 200 (the CPU 201) may be recorded on the removable medium 211 as a package medium to be provided, for example.

15 Alternatively, the programs can be provided via a wired or wireless transmission medium such as a local area network, the Internet, or digital satellite broadcasting.

[0146]

 In the computer 200, the programs can be installed
20 into the storage unit 208 via the input/output interface 205 when the removable medium 211 is mounted on the drive 210. The program can also be received by the communication unit 209 via a wired or wireless transmission medium, and be installed into the storage
25 unit 208. Also, the program may be installed beforehand into the ROM 202 or the storage unit 208.

[0147]

 The programs to be executed by the computer 200 may be programs for performing processes in chronological
30 order in accordance with the sequence described in this specification, or may be programs for performing

processes in parallel or performing a process when necessary, such as when there is a call.

[0148]

It should be noted that embodiments of the present disclosure are not limited to the above described embodiments, and various modifications may be made to them without departing from the scope of the present disclosure.

10 REFERENCE SIGNS LIST

[0149]

- 10 Application linkage system
- 11 Broadcast network
- 12 Bidirectional communication network
- 15 20 Provider system
- 21 Content server
- 22 Application server
- 23 ACR server
- 30 Home network system
- 20 30A Primary screen device
- 30B Second screen device
- 31 Content renderer
- 32 ACR client
- 33 Application manager
- 25 41 Content acquiring unit
- 42 Reference signature extracting unit
- 43 ACR database unit
- 44 ACR response generating unit
- 45 Signature DRM encrypting unit
- 30 46 Signature DRM decrypting unit
- 51 Signature extracting unit

	52	ACR query generating unit
	53	Communication unit
	54	ACR response analyzing unit
	60	ACR reference data
5	65	SCM information
	66	ARM information
	67	ACM information
	70	ACR query
	80	ACR response
10	85	ACM information
	86	ARM information
	200	Computer
	201	CPU

CLAIMS

1. An information processing device comprising:

a content managing unit configured to manage first
5 content viewable on a side of a content reproduction
device that reproduces content;

a database unit configured to generate reference
data and turn the generated reference data into a
database, the reference data being generated by
10 associating first signature data extracted from the first
content with right management information about the first
signature data and a content identifier representing the
first content from which the first signature data is
extracted, the first signature data indicating a feature
15 of the first content; and

an identifying unit configured to identify the
content and return a response indicating an
identification result by referring to the reference data
of the database unit in reply to a query including second
20 signature data extracted from second content being viewed
by a user of the content reproduction device, the query
being transmitted from the side of the content
reproduction device, the second signature data indicating
a feature of the second content.

25
2. The information processing device according to
claim 1, wherein

the first signature data of the reference data is
encrypted, and

30 the database unit decrypts the encrypted first
signature data through an authentication process with the

content managing unit.

3. The information processing device according to claim 2, wherein the right management information about the first signature data includes an item for selecting an existing right management method for the first signature data.

4. The information processing device according to claim 3, wherein the right management information about the first signature data further includes an item for arbitrarily setting a right management method for the first signature data.

5. An information processing method implemented in an information processing device,
the information processing method comprising:
a database forming step of generating reference data and turning the generated reference data into a database, the reference data being generated by associating first signature data extracted from first content with right management information about the first signature data and a content identifier representing the first content from which the first signature data is extracted, the first content being viewable on a side of a content reproduction device that reproduces content, the first signature data indicating a feature of the first content; and
an identifying step of identifying the content and returning a response indicating an identification result by referring to the reference data of the database in

reply to a query including second signature data
extracted from second content being viewed by a user of
the content reproduction device, the query being
transmitted from the side of the content reproduction
5 device, the second signature data indicating a feature of
the second content,

the database forming step and the identifying step
being carried out by the information processing device.

- 10 6. An information processing device comprising:
a content managing unit configured to manage first
content viewable on a side of a content reproduction
device that reproduces content;
a database unit configured to generate reference
15 data and turn the generated reference data into a
database, the reference data being generated by
associating first signature data extracted from the first
content with a content identifier, an application
identifier, and rendering control information, the
20 content identifier representing the first content from
which the first signature data is extracted, the
application identifier representing an application to be
executed on the side of the content reproduction device
in conjunction with progress of the first content when
25 the first content is being viewed on the side of the
content reproduction device, the rendering control
information being for controlling rendering of the
application, the first signature data indicating a
feature of the first content; and
30 an identifying unit configured to identify the
content and return a response indicating an

identification result by referring to the reference data of the database unit in reply to a query including second signature data extracted from second content being viewed by a user of the content reproduction device, the query
5 being transmitted from the side of the content reproduction device, the second signature data indicating a feature of the second content.

7. The information processing device according to
10 claim 6, wherein the rendering control information includes at least one of an item for limiting a device serving as a destination of output of an image from the application, and an item for restricting superimposition of an image from the application and an image of the
15 content.

8. An information processing method implemented in an information processing device,
the information processing method comprising:
20 a database forming step of generating reference data and turning the generated reference data into a database, the reference data being generated by associating first signature data extracted from first content with a content identifier, an application
25 identifier, and rendering control information, the content identifier representing the first content from which the first signature data is extracted, the application identifier representing an application to be executed on a side of a content reproduction device in
30 conjunction with progress of the first content when the first content is being viewed on the side of the content

reproduction device, the rendering control information being for controlling rendering of the application, the first content being viewable on the side of the content reproduction device that reproduces content, the first
5 signature data indicating a feature of the first content;
and

an identifying step of identifying the content and returning a response indicating an identification result by referring to the reference data of the database in
10 reply to a query including second signature data extracted from second content being viewed by a user of the content reproduction device, the query being transmitted from the side of the content reproduction device, the second signature data indicating a feature of
15 the second content,

the database forming step and the identifying step being carried out by the information processing device.

9. An information processing device comprising:
20 a query generating unit configured to extract signature data from content being reproduced, generate a query including the signature data, transmit the query to an identification server, and receive a response returned from the identification server in reply to the query, the
25 signature data indicating a feature of the content; and
an application executing unit configured to acquire and execute an application based on an application identifier included in the received response, and control rendering of the application based on rendering control
30 information about the application, the application being designated to be executed in conjunction with progress of

the content being reproduced, the rendering control information being included in the response.

10. The information processing device according to
5 claim 9, wherein, based on the rendering control information, the application executing unit performs at least one of a process for limiting a device serving as a destination of output of an image from the application, and a process for restricting superimposition of an image
10 from the application and an image of the content.

11. An information processing method implemented in an information processing device,
the information processing method comprising:
15 a transmitting step of extracting signature data from content being reproduced, generating a query including the signature data, and transmitting the query to an identification server, the signature data indicating a feature of the content;
20 a receiving step of receiving a response returned from the identification server in reply to the query; and
a controlling step of acquiring and executing an application based on an application identifier included in the received response, and controlling rendering of
25 the application based on rendering control information about the application, the application being designated to be executed in conjunction with progress of the content being reproduced, the rendering control information being included in the response,
30 the transmitting step, the receiving step, and the controlling step being carried out by the information

processing device.

12. An information processing device comprising:

5 a content managing unit configured to manage first content viewable on a side of a content reproduction device that reproduces content;

a database unit configured to generate reference data and turn the generated reference data into a database, the reference data being generated by associating first signature data extracted from the first content with a content identifier, an application identifier, and right management information about an application, the content identifier representing the first content from which the first signature data is extracted, the application identifier representing the application to be executed on the side of the content reproduction device in conjunction with progress of the first content when the first content is being viewed on the side of the content reproduction device, the first signature data indicating a feature of the first content;

10 15 20 and

an identifying unit configured to identify the content and return a response indicating an identification result by referring to the reference data of the database unit in reply to a query including second signature data extracted from second content being viewed by a user of the content reproduction device, the query being transmitted from the side of the content reproduction device, the second signature data indicating a feature of the second content.

25 30

13. The information processing device according to claim 12, wherein the right management information about the application includes an item for selecting an existing right management method for the application and
5 content cited by the application.

14. The information processing device according to claim 13, wherein the right management information about the application further includes an item for arbitrarily
10 setting a right management method for the application and the content cited by the application.

15. An information processing method implemented in an information processing device,
15 the information processing method comprising:
a database forming step of generating reference data and turning the generated reference data into a database, the reference data being generated by associating first signature data extracted from first
20 content with a content identifier, an application identifier, and right management information about an application, the content identifier representing the first content from which the first signature data is extracted, the application identifier representing the
25 application to be executed on a side of a content reproduction device in conjunction with progress of the first content when the first content is being viewed on the side of the content reproduction device, the first content being viewable on the side of the content
30 reproduction device that reproduces content, the first signature data indicating a feature of the first content;

and

an identifying step of identifying the content and returning a response indicating an identification result by referring to the reference data of the database unit
5 in reply to a query including second signature data extracted from second content being viewed by a user of the content reproduction device, the query being transmitted from the side of the content reproduction device, the second signature data indicating a feature of
10 the second content,

the database forming step and the identifying step being carried out by the information processing device.

16. An information processing device comprising:
15 a query generating unit configured to extract signature data from content being reproduced, generate a query including the signature data, transmit the query to an identification server, and receive a response returned from the identification server in reply to the query, the
20 signature data indicating a feature of the content; and
an application executing unit configured to acquire and execute an application based on an application identifier included in the received response, and manage the application and content cited by the application
25 based on right management information about the application, the application being designated to be executed in conjunction with progress of the content being reproduced, the right management information being included in the response.

30

17. The information processing device according to

claim 16, wherein the application executing unit decrypts the application based on the right management information, the application being encrypted.

5 18. The information processing device according to claim 16, wherein the application executing unit manages copying of the application and the cited content based on the right management information.

10 19. An information processing method implemented in an information processing device,
the information processing method comprising:
a transmitting step of extracting signature data from content being reproduced, generating a query
15 including the signature data, and transmitting the query to an identification server, the signature data indicating a feature of the content;
a receiving step of receiving a response returned from the identification server in reply to the query; and
20 a managing step of acquiring and executing an application based on an application identifier included in the received response, and managing the application and content cited by the application based on right management information about the application, the
25 application being designated to be executed in conjunction with progress of the content being reproduced, the right management information being included in the response,
the transmitting step, the receiving step, and the
30 managing step being carried out by the information processing device.