

DIGITAL RIGHTS MANAGEMENT METHOD OF MEDIA CONTENT, DRM CLIENT AND SERVER SIDE

TECHNICAL FIELD

5 **[0001]** The present invention relates to digital rights management (DRM) technologies, and more particularly, to a DRM method of media content, a DRM client, a DRM server side, a terminal device and a DRM server.

BACKGROUND

10 **[0002]** Currently, smart devices such as smart televisions have entered thousands of households and are increasingly becoming an important way for users to acquire media content such as audio and video materials and document materials in daily life. International content providers, headed by Hollywood content providers, are actively deploying the operation of 4K ultra-high definition media content. Japan's NHK television station has
15 even achieved the industrialization of 8K content encoding and display devices. Domestic mainstream content providers such as CCTV and Jiangsu television are all actively deploying the production, broadcasting and operation of ultra-high definition media content. Jiangsu television has adopted an ultra-high definition mode to live-broadcast in the new year countdown party, which implies that the era of ultra-high definition media content
20 operation has arrived. Ultra-high definition media content is high in production cost and values, and is regarded as the next growth point of the media industry. The domestic mainstream content providers, Hollywood content providers and the like also pay special attention to the protection of ultra-high definition media content. The operation of ultra-high definition media content presents a high requirement on rights protection and it needs to
25 replace content protection algorithms frequently to improve security. Therefore, it is urgent to upgrade an existing content protection technology so as to provide the technical support and guarantee for building a healthy ultra-high definition media content ecosystem.

[0003] In an existing digital rights management (DRM) technology, digital media content is usually encrypted and encapsulated. According to business rules set by operators,
30 information such as a content encryption key and DRM authority (such as content authorization permission and restriction conditions) is encapsulated into a content authorization license in accordance with certain grammar. The content authorization license is sent to a DRM client through the interaction between the DRM client and a DRM server side of a terminal device, and the DRM client decrypts and plays the content according to

rules stipulated in the permission and restriction conditions in the content authorization license.

[0004] However, the existing DRM technology system cannot set a personalized content encryption algorithm, an authorization rule and the like for the media content, which results in low protection degree of the media content. In the existing DRM technology, if it needs to modify the content encryption algorithm, the authorization rule and the like, a DRM server side system and a DRM client system need to be upgraded at the same time, and the content encryption algorithm, the authorization rule and the like cannot be flexibly changed in real time according to commercial operation demands and security demands, which is not conducive to high-intensity security protection of media content.

[0005] In the case based on a trusted execution environment, core functions, such as decryption and decoding functions, of the DRM client all need to run in the trusted execution environment. If the DRM client is upgraded, it also needs to upgrade the overall trusted execution environment at the same time, which may affect the normal use of other non-DRM functions in the trusted execution environment.

[0006] In addition, the way to parse and execute the permission and restriction conditions of the existing content authorization license is poorly binding on the DRM client and execution loopholes appear easily. For example, the loophole that the DRM client does not decrypt and play the content in accordance with the requirements of permission and restriction conditions appears.

SUMMARY

[0007] One object of the present invention is to provide a new technical solution for digital rights management, which may at least solve one of the above technical problems.

[0008] According to a first aspect of the present invention, there is provided a digital rights management (DRM) method of media content implemented in a terminal device, in which a DRM client is installed. The method comprises the following steps:

[0009] step 1: receiving by the DRM client an invoking request of a media application of the terminal device, and acquiring by the DRM client a unique identifier of media content to be played from the invoking request;

[0010] step 2: sending, by the DRM client, a DRM authorization request to a DRM server side so as to acquire a content authorization execution unit, wherein the DRM authorization request contains an identifier of the media content and basic information of the DRM client, and

[0011] the content authorization execution unit is generated by the DRM server side in

the following way: the DRM server side obtains a content encryption algorithm and a content encryption key which are adopted by the media content, and DRM authority of the DRM client to the media content according to the DRM authorization request through query, and is then generated according to the identifier of the media content, the content encryption algorithm and the content encryption key which are adopted by the media content, the basic information of the DRM client, and the DRM authority of the DRM client to the media content; and

[0012] step 3, by the DRM client, running the content authorization execution unit in a DRM client running environment, verifying whether a terminal running environment conforms to the DRM authority of the DRM client to the media content through the content authorization execution unit, and if so, decrypting the media content according to the content encryption algorithm and the content encryption key.

[0013] Optionally, the content authorization execution unit is issued to the DRM client after being signed by the DRM server side. After acquiring the content authorization execution unit, the DRM client firstly checks the signature of the content authorization execution unit and then runs the content authorization execution unit after the checking succeeds.

[0014] Optionally, in the step 2, the DRM client runs a communication execution unit in the DRM client running environment and sends the DRM authorization request to the DRM server side through the communication execution unit.

[0015] Optionally, between the step 1 and the step 2, the method further comprises the step of acquiring the communication execution unit: sending, by the DRM client, a request for the communication execution unit to the DRM server side so as to acquire the communication execution unit. The request for the communication execution unit contains the basic information of the DRM client. The communication execution unit is generated by the DRM server side according to the basic information of the DRM client.

[0016] Optionally, the communication execution unit is issued to the DRM client after being signed by the DRM server side. After acquiring the communication execution unit, the DRM client firstly checks the signature of the communication execution unit and then runs the communication execution unit after the checking succeeds.

[0017] Optionally, the DRM authority of the DRM client to the media content comprises that the DRM client must check a digital watermark of the media content when playing the media content. The content authorization execution unit notifies the DRM client to run a digital watermark execution unit. The DRM client runs the digital watermark execution unit in the DRM client running environment, checks the digital watermark embedded into the media content in a playing process of the media content through the digital watermark execution unit and stops

playing the media content if the checking fails. The digital watermark execution unit is obtained by the DRM client requesting, according to the notification, a digital watermark execution unit corresponding to the media content, from the DRM server side.

[0018] Optionally, the digital watermark of the media content contains information of a restriction requirement of a content provider of the media content for a playing environment of the media content. The digital watermark execution unit determines whether the terminal running environment conforms to the restriction requirement of the content provider of the media content for the playing environment of the media content in the playing process of the media content, and if not, stops playing the media content.

[0019] Optionally, the DRM authority of the DRM client to the media content comprises that the DRM client must embed the digital watermark for tracking the media content when playing the media content. The content authorization execution unit notifies the DRM client to run the digital watermark execution unit. The DRM client runs the digital watermark execution unit in the DRM client running environment and embeds the digital watermark for tracking the media content in the playing process of the media content through the digital watermark execution unit. The digital watermark execution unit is obtained by the DRM client requesting, according to the notification, a digital watermark execution unit corresponding to the media content, from the DRM server side.

[0020] Optionally, the digital watermark execution unit is issued to the DRM client after being signed by the DRM server side. After acquiring the digital watermark execution unit, the DRM client firstly checks the signature of the digital watermark execution unit and then runs the digital watermark execution unit after the checking succeeds.

[0021] Optionally, the DRM client running environment comprises an execution unit engine and a terminal operating system adaptation module. The DRM client runs the execution unit through the execution unit engine and adapts the execution unit engine to a terminal operating system through the terminal operating system adaptation module.

[0022] Optionally, the execution unit engine provides a memory management interface, an external storage management interface, a network management interface, a cryptographic algorithm interface, a playing control interface and an output control interface for the running of the execution unit. The DRM client adapts the memory management interface, the external storage management interface, the network management interface, the cryptographic algorithm interface, the playing control interface and the output control interface of the execution unit engine to corresponding interfaces of the terminal operating system through the terminal operating system adaptation module.

[0023] Optionally, the DRM client running environment further comprises an execution unit scheduling and management module. The DRM client schedules and manages various execution units through the execution unit scheduling and management module, comprising scheduling the execution unit to the execution unit engine for running, and adding, deleting and
5 updating the execution unit.

[0024] According to a second aspect of the present invention, there is provided a digital rights management (DRM) method of media content implemented in a DRM server side. The method comprises the following steps:

[0025] step 1: receiving, by the DRM server side, a DRM authorization request sent by a
10 DRM client, wherein the DRM authorization request contains a unique identifier of the media content and basic information of the DRM client;

[0026] step 2: obtaining, by the DRM server side, a content encryption algorithm and a content encryption key which are adopted by the media content, and DRM authority of the DRM client to the media content according to the DRM authorization request through query;

[0027] step 3, generating, by the DRM server side, a content authorization execution unit according to an identifier of the media content, the content encryption algorithm and the content encryption key which are adopted by the media content, the basic information of the DRM client and the DRM authority of the DRM client to the media content, wherein the content authorization execution unit is configured to run in a DRM client running environment so as to verify whether
15 a terminal running environment of a terminal device where the DRM client is located conforms to the DRM authority of the DRM client to the media content and if so, decrypt the media content according to the content encryption algorithm and the content encryption key; and

[0028] step 4: issuing, by the DRM server side, the generated content authorization execution unit to the DRM client.

[0029] Optionally, between the step 3 and the step 4, the method further comprises the step of signing the generated content authorization execution unit by the DRM server side.

[0030] Optionally, in the step 3, the DRM server side searches for a content authorization execution unit template corresponding to the media content according to the identifier of the media content or the content encryption algorithm adopted by the media content; or the DRM authorization request further contains a DRM version number corresponding to the media content
30 and the DRM server side searches for the content authorization execution unit template corresponding to the media content according to the DRM version number corresponding to the media content. The DRM server side generates the content authorization execution unit in accordance with the content authorization execution unit template obtained through search.

[0031] Optionally, the step of scheduling a digital watermark execution unit is contained in the content authorization execution unit template corresponding to the media content. The DRM server side receives a request of the DRM client for the digital watermark execution unit corresponding to the media content. The request of the DRM client for the digital watermark execution unit corresponding to the media content is generated by the DRM client according to the step of scheduling the digital watermark execution unit by the content authorization execution unit. The DRM server side searches for a digital watermark execution unit template corresponding to the media content according to the identifier of the media content and generates the digital watermark execution unit according to the digital watermark execution unit template obtained through search. The DRM server side issues the generated digital watermark execution unit to the DRM client.

[0032] Optionally, in the step 2, the DRM server side obtains the encryption algorithm and the content encryption key, which are adopted by the media content, from a key management system through query according to the identifier of the media content.

[0033] Optionally, in the step 2, the DRM server side obtains the DRM authority of the DRM client to the media content from an operation support system through query according to the identifier of the media content and the basic information of the DRM client.

[0034] According to a third aspect of the present invention, there is provided a DRM client arranged in a terminal device in which an intelligent operating system is installed. The DRM client comprises a media application interface, an execution unit acquisition module and a content authorization execution unit, wherein

[0035] the media application interface is configured to receive an invoking request of a media application of the terminal device and acquire a unique identifier of media content to be played from the invoking request;

[0036] the execution unit acquisition module is configured to send a DRM authorization request to a DRM server side so as to acquire the content authorization execution unit, wherein the DRM authorization request contains an identifier of the media content and basic information of the DRM client; and

[0037] the content authorization execution unit is configured to verify whether a terminal running environment conforms to DRM authority of the DRM client to the media content and if so, decrypt the media content according to a content encryption algorithm and a content encryption key, wherein

[0038] the content authorization execution unit is generated by the DRM server side in the following way: the DRM server side obtains the content encryption algorithm and the content

encryption key which are adopted by the media content, and the DRM authority of the DRM client to the media content according to the DRM authorization request through query, and is then generated unit according to the identifier of the media content, the content encryption algorithm and the content encryption key which are adopted by the media content, the basic information of the DRM client, and the DRM authority of the DRM client to the media content.

[0039] Optionally, the DRM client further comprises an execution unit signature checking module configured to check the signature of the content authorization execution unit.

[0040] Optionally, the DRM authority of the DRM client to the media content comprises that the DRM client must check a digital watermark of the media content when playing the media content. The DRM client further comprises a digital watermark execution unit. The content authorization execution unit is further configured to notify the execution unit acquisition module to acquire the digital watermark execution unit. The execution unit acquisition module is further configured to request a digital watermark execution unit corresponding to the media content, from the DRM server side according to the notification. The digital watermark execution unit is configured to check the digital watermark embedded into the media content in a playing process of the media content and stop playing the media content if the checking fails.

[0041] Optionally, the digital watermark of the media content contains information of a restriction requirement of a content provider of the media content for a playing environment of the media content. The digital watermark execution unit is further configured to determine whether a terminal running environment conforms to the restriction requirement of the content provider of the media content for the playing environment of the media content in the playing process of the media content and if not, stop playing the media content.

[0042] Optionally, the DRM authority of the DRM client to the media content comprises that the DRM client must embed the digital watermark for tracking the media content when playing the media content. The DRM client further comprises a digital watermark execution unit. The content authorization execution unit is further configured to notify the execution unit acquisition module to acquire the digital watermark execution unit. The execution unit acquisition module is further configured to request a digital watermark execution unit corresponding to the media content, from the DRM server side according to the notification. The digital watermark execution unit is configured to embed the digital watermark for tracking the media content in the playing process of the media content.

[0043] Optionally, the DRM client further comprises an execution unit engine and a terminal operating system adaptation module. The execution unit engine is configured to run an execution unit. The terminal operating system adaptation module is configured to adapt the

execution unit engine to a terminal operating system.

[0044] Optionally, the execution unit engine is configured to provide a memory management interface, an external storage management interface, a network management interface, a cryptographic algorithm interface, a playing control interface and an output control interface for the running of the execution unit. The terminal operating system adaptation module is configured to adapt the memory management interface, the external storage management interface, the network management interface, the cryptographic algorithm interface, the playing control interface and the output control interface of the execution unit engine to corresponding interfaces of the terminal operating system.

[0045] Optionally, the DRM client further comprises an execution unit scheduling and management module. The execution unit scheduling and management module is configured to schedule and manage various execution units, comprising scheduling the execution unit to the execution unit engine for running, and adding, deleting and updating the execution unit.

[0046] According to a fourth aspect of the present invention, there is provided a DRM server side comprising a DRM message receiving module, a media content-related DRM information acquisition module, an execution unit generation module and an execution unit issuing module, wherein

[0047] the DRM message receiving module is configured to receive a DRM authorization request sent by a DRM client, wherein the DRM authorization request contains a unique identifier of media content and basic information of the DRM client;

[0048] the media content-related DRM information acquisition module is configured to obtain a content encryption algorithm and a content encryption key which are adopted by the media content, and DRM authority of the DRM client to the media content, according to the DRM authorization request through query;

[0049] the execution unit generation module is configured to generate a content authorization execution unit according to an identifier of the media content, the content encryption algorithm and the content encryption key which are adopted by the media content, the basic information of the DRM client and the DRM authority of the DRM client to the media content and in accordance with a content authorization execution unit template corresponding to the media content, wherein the content authorization execution unit is configured to run in a DRM client running environment so as to verify whether a terminal running environment of a terminal device where the DRM client is located conforms to the DRM authority of the DRM client to the media content and if so, decrypt the media content according to the content encryption algorithm and the content encryption key; and

[0050] the execution unit issuing module is configured to issue the content authorization execution unit to the DRM client.

[0051] Optionally, the DRM server side further comprises an execution unit signature module configured to sign the content authorization execution unit before the execution unit issuing module issues the content authorization execution unit.

[0052] Optionally, the DRM server side further comprises an execution unit template management module configured to manage a content authorization execution unit template, comprising adding, updating and deleting the content authorization execution template.

[0053] Optionally, the DRM server side further comprises a key management interface.

The media content DRM information acquisition module is configured to communicate with a key management system through the key management interface and obtain the content encryption algorithm and the content encryption key which are adopted by the media content, from the key management system according to the identifier of the media content through query.

[0054] Optionally, the DRM server side further comprises an operation support interface.

The media content DRM information acquisition module is further configured to communicate with an operation support system through the operation support interface and obtain the DRM authority of the DRM client to the media content from the operation support system according to the identifier of the media content and the basic information of the DRM client through query.

[0056] According to a fifth aspect of the present invention, there is provided a DRM client arranged in a terminal device in which an intelligent operating system is installed. The DRM client comprises a media application interface, an execution unit scheduling and management module, an execution unit engine and a terminal operating system adaptation module, wherein

[0057] the media application interface is configured to receive an invoking request of a media application of the terminal device and acquire a unique identifier of media content to be played from the invoking request;

[0058] the execution unit scheduling and management module is configured to search for an execution unit corresponding to the media content according to the invoking request and start the execution unit engine to run the execution unit so as to realize the DRM authorization to the media content; and send a DRM message to the DRM server side if no execution unit corresponding to the media content is found to acquire the execution unit corresponding to the media content, check the signature of the acquired execution unit to determine the legality of the execution unit and then start the DRM execution unit engine to run the execution unit so as to

realize the DRM authorization to the media content; and

[0059] the terminal operating system adaptation module is configured to realize the adaptation of the DRM execution unit engine and a terminal operating system.

[0060] Optionally, the execution unit engine is configured to provide a memory management interface, an external storage management interface, a network management interface, a cryptographic algorithm interface, a playing control interface and an output control interface for the running of the execution unit. The terminal operating system adaptation module is configured to adapt the memory management interface, the external storage management interface, the network management interface, the cryptographic algorithm interface, the playing control interface and the output control interface of the execution unit engine to corresponding interfaces of the terminal operating system.

[0061] According to a sixth aspect of the present invention, there is provided a DRM server side comprising a DRM message processing module, an execution unit template management module, an execution unit template and an execution unit generation module, wherein

[0062] the DRM message processing module is configured to receive a DRM message sent by a DRM client, wherein the DRM message comprises an identifier of media content and basic information of the DRM client; select a corresponding execution unit template according to the DRM message and invoke the execution unit generation module to generate an execution unit in accordance with the selected execution unit template, wherein the execution unit is configured to run in a DRM client running environment so as to realize DRM authorization to the media content; sign the execution unit generated by the execution unit generation module; and issue the signed execution unit to the DRM client; and

[0063] the execution unit template management module is configured to manage the execution unit template.

[0064] Optionally, the execution unit template comprises a content authorization execution unit template. The DRM message processing module is configured to invoke the execution unit generation module to generate a content authorization execution unit according to the identifier of the media content, a content encryption algorithm and a content encryption key which are adopted by the media content, the basic information of the DRM client, and the DRM authority of the DRM client to the media content and in accordance with the selected content authorization execution unit template. The content authorization execution unit is configured to run in a DRM client running environment so as to verify whether a terminal running environment of a terminal device where the DRM client is located conforms to the DRM authority of the DRM

client to the media content and if so, decrypt the media content according to the content encryption algorithm and the content encryption key.

[0065] Optionally, the DRM server side further comprises a key management interface and an operation support interface. The DRM message processing module is further configured to communicate with a key management system through the key management interface and obtain the encryption algorithm and the content encryption key which correspond to the media content from the key management system according to the identifier of the media content through query. The DRM message processing module is further configured to communicate with an operation support system through the operation support interface and obtain the DRM authority of the DRM client to the media content from the operation support system according to the identifier of the media content and the basic information of the DRM client through query.

[0066] According to a seventh aspect of the present invention, there is further provided a terminal device comprising the DRM client according to any of previous aspects.

[0067] Optionally, the DRM client runs in an intelligent operating system of the terminal device or runs in a trusted execution environment of the terminal device.

[0068] According to an eighth aspect of the present invention, there is further provided a DRM server comprising the DRM server side according to any of previous aspects.

[0069] In the present invention, the way of authorizing content through a content authorization license is changed, the DRM client requests the DRM authorization to the media content from the DRM server side after receiving the invoking request of the media application, the DRM server side generates the content authorization execution unit according to the encryption algorithm and the content encryption key of the media content, the DRM authority of the DRM client to the media content and the like and issues the content authorization execution unit to the DRM client, and the DRM client directly runs the content authorization execution unit in the DRM client running environment so as to decrypt the media content. By adopting the technical solution of the present invention, flexible protection may be provided for the media content, thereby improving the security degree of the media content.

[0070] Other features and advantages of the present invention will become clear by describing exemplary embodiments of the present invention in detail with reference to the accompanying drawings below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0071] The accompanying drawings, which are incorporated in and form a part of the description, illustrate embodiments of the present invention and, together with the

description, serve to explain the principles of the present invention.

[0072] Fig. 1 is a schematic block diagram of a media content operation-related system provided in an embodiment of the present invention;

[0073] Fig. 2 is a step diagram of a digital rights management method provided in a first embodiment of the present invention;

[0074] Fig. 3 is a block diagram of a DRM client and a DRM server side provided in the first embodiment of the present invention;

[0075] Fig. 4 is a block diagram of a DRM client and a DRM server side provided in second and third embodiments of the present invention;

[0076] Fig. 5 is a block diagram of a DRM client and a DRM server side provided in a fourth embodiment of the present invention; and

[0077] Fig. 6 is a schematic block diagram of a terminal device provided in an embodiment of the present invention.

DETAILED DESCRIPTION

[0078] Various exemplary embodiments of the present invention will now be described in detail with reference to the accompanying drawings. It should be noted that the relative arrangement of the components and steps, numerical expressions, and numerical values set forth in these embodiments do not limit the scope of the present invention unless it is specifically stated otherwise.

[0079] The following description of at least one exemplary embodiment is merely illustrative in nature and by no means is to be construed as any limitation on the invention and its application or use.

[0080] Techniques, methods, and apparatuses known to an ordinary person skilled in the relevant art may not be discussed in detail, but where appropriate, the techniques, methods, and apparatuses should be considered as part of the description.

[0081] In all of the examples shown and discussed herein, any specific value should be interpreted as exemplary merely and not as a limitation. Therefore, other examples of exemplary embodiments may have different values.

[0082] It should be noted that like reference numbers and letters designate similar terms in the following figures, and therefore, an item does not need to be further discussed in subsequent figures as soon as the item is defined in a figure.

[0083] The present invention provides a digital rights management solution of media content and relates to a DRM server side providing a DRM service and a DRM client of a

user terminal device.

[0084] The terminal device is an intelligent electronic device, such as a computer, a smart phone and a PAD, on which an intelligent operating system (such as Android, WINDOWS system and IOS) is installed.

5 **[0085]** The DRM client is composed of a DRM client running environment and an execution unit. The execution unit is an entity which is generated by the DRM server side according to a demand of the DRM client and may run in the DRM client running environment, such as a program, a statement, an instruction and a code. The DRM client running environment refers to an internal running environment provided by the DRM client
10 100 for the execution unit. The execution unit runs in the DRM client running environment and is not in direct contact with the DRM client externally, and the contact with a terminal operating system is provided by the DRM client running environment.

[0086] The DRM client realizes the reasonable authorization to the media content by running the execution unit in the DRM client running environment. The execution units
15 involved in the present invention comprise, but are not limited to, a communication execution unit, a content authorization execution unit, a digital watermark execution unit and the like.

[0087] A media content operation-related system of an embodiment of the present invention is illustrated with reference to Fig. 1, and the technical solution of the present
20 invention is described on the whole.

[0088] A content management system 4 sends media content to be played to a content encryption system 3 for encryption. The content encryption system 3 encrypts the media content, then sends the encrypted media content to an operation support system 6 for waiting for play on demand by a user, sends a content encryption key to a key management
25 system 5 for storage management, and sends basic information of the media content to a DRM server 2 for storage. The basic information of the media content at least should comprise a unique identifier of the media content and may also comprise other information of the media content, such as a document name, a size, duration and a corresponding DRM version number. The content encryption system 3 may further send an encryption algorithm
30 used for encrypting the media content to the key management system 5 and/or the DRM server 2 for storage. The content encryption key in the present invention refers to a key for encrypting a content key and the media content is encrypted using the content key.

[0089] The DRM server side 200 may generate a content authorization execution unit template by using the encryption algorithm of the media content or the content authorization

execution unit template in the DRM server side 200 may be issued to the DRM server 2 by the content encryption system 3 or the operation support system 6. The content authorization execution unit template is configured to generate a content authorization execution unit that may directly run in the DRM client running environment. The content authorization execution unit may carry authorization information of the DRM client, an IF statement that determines whether a terminal running environment conforms to a DRM authorization rule, for example, it needs to check a local certificate of the terminal device, and the media content may be decrypted and played only after the checking succeeds, and the like. The content authorization execution unit template may be set by a person skilled in the art in various ways, which will not be described herein. The DRM server side 200 may further comprise other types of execution unit templates, such as a communication execution unit template and a digital watermark execution unit template. New template types may be set according to operation needs.

[0090] An intelligent operating system 11, a media application 12 and a DRM client 100 run in the terminal device 1. The media application 11, for example, is a media player or a media APP. The user may play the media content on demand through the media application 11. Further, the user may also purchase and download the media content through the media application 11. The media application 11 acquires the media content through the operation support system 6 and presents the media content to the user.

[0091] When the user requests the media content from the operation support system 6 through the media application 11, the media application 11 will acquire the unique identifier of the media content from the operation support system 6 and may also acquire information such as the DRM version number corresponding to the media content and a DRM server side address. Subsequently, the media application 11 invokes the DRM client 100 for achieving operations such as DRM authorization to the media content so as to play the media content.

[0092] After being invoked by the media application 11, the DRM client 100 sends a DRM message to the DRM server side 200. After receiving the DRM message, the DRM server side 200 selects, according to the DRM message, a corresponding execution unit template to generate an execution unit and then issues the execution unit to the DRM client 100. The DRM client 100 runs the execution unit in the DRM client running environment and realizes the authorization to the media content through the running of the execution unit. The DRM message in the present invention comprises, but is not limited to, a DRM authorization request and may also be a request for the communication execution unit and

the like.

[0093] The DRM server side 200 may replace the execution unit template according to operation needs. The execution unit generated in accordance with the execution unit template may be directly executed in the DRM client running environment after being sent to the DRM client 100. If it needs to add a new DRM function or a new authorization rule, it only needs to add a new execution unit template in the DRM server side 2.

[0094] The DRM client 100 may run in the intelligent operating system of the terminal device 1 and may also run in the trusted execution environment of the terminal device 1. When the DRM client 100 runs in the trusted execution environment of a terminal, if the content encryption algorithm and the like need to be updated, it only needs to generate a new content authorization execution template at the DRM server side 200, and the DRM server side 200 generates a content authorization execution unit according to the new content authorization execution template and then sends the content authorization execution unit to the DRM client 100 for running, thereby avoiding the problem of frequently upgrading the DRM client 100.

[0095] <FIRST EMBODIMENT>

[0096] A digital rights management method, a DRM client 100 and a DRM server side 200 provided in a first embodiment of the present invention are illustrated with reference to Figs. 2 and 3. The DRM client 100 comprises a media application interface 101, an execution unit acquisition module 108, an execution unit signature checking module 109, an execution unit engine 106, a terminal operating system adaptation module 107 and an execution unit scheduling and management module (not shown in the figures). The DRM server side 200 comprises an operation support interface 205, a key management interface 206, a DRM message receiving module 207, a media content-related DRM information acquisition module 208, an execution unit generation module 204, an execution unit signature module 210, an execution unit issuing module 209 and an execution unit template management module 203.

[0097] S101 includes receiving by the DRM client 100 an invoking request of a media application of a terminal device through the media application interface 101, and acquiring by the DRM client 100 basic information of the media content to be played from the invoking request. The basic information of the media content at least should comprise a unique identifier of the media content and may also comprise other information of the media content, such as a document name, a size, duration and a corresponding DRM version

number.

[0098] S102 includes sending, by the DRM client 100, a DRM authorization request to the DRM server side 200 through the execution unit acquisition module 108, wherein the DRM authorization request at least should contain an identifier of the media content and
5 basic information of the DRM client 100 and may also comprise DRM version number information corresponding to the media content. The basic information of the DRM client 100 at least should comprise an ID of the DRM client 100 and may also comprise other information of the DRM client 100, such as address information, a version number and a certificate.

10 **[0099]** S103 includes receiving, by the DRM server side 200, the DRM authorization request through the DRM message receiving module 207; obtaining, by the media content-related DRM information acquisition module 208, a content encryption algorithm and a content encryption key which are adopted by the media content, and DRM authority of the DRM client 100 to the media content according to the DRM authorization request;
15 generating, by the execution unit generation module 204, a content authorization execution unit 104 according to the identifier of the media content, the content encryption algorithm and the content encryption key which are adopted by the media content, the basic information of the DRM client 100 and the DRM authority of the DRM client 100 to the media content; and finally, issuing, by the execution unit issuing module 209, the generated
20 content authorization execution unit 104 to the DRM client 100.

[00100] S104 includes, using the DRM client 100, receiving the content authorization execution unit 104 through the execution unit acquisition module 108, running the content authorization execution unit 104 in a DRM client running environment, verifying whether a terminal running environment conforms to the DRM authority of the DRM client 100 to the
25 media content through the content authorization execution unit 104, and if so, decrypting the media content according to the content encryption algorithm and the content encryption key and controlling the playing of the media content. For example, the DRM authority of the DRM client 100 to the media content is that the DRM client may only decrypt and play the media content at the time between 8:00 pm to 12:00 pm, the content authorization
30 execution unit 104 will determine whether the terminal running environment is between 8:00 pm to 12:00 pm, and if the terminal running environment conforms to the restriction condition that the time is between 8:00 pm to 12:00 pm, the content authorization execution unit 104 decrypts the media content and controls the playing of the media content.

[00101] In order to further improve the security of the media content, in the step S103,

after the execution unit generation module 204 generates the content authorization execution unit, the content authorization execution unit is firstly signed by the execution unit signature module 210 and then the signed content authorization execution unit is issued to the DRM client by the execution unit issuing module 209. In the step S104, after
5 acquiring the content authorization execution unit 104, the DRM client firstly checks the signature of the content authorization execution unit 104 and then runs the content authorization execution unit 104 in the DRM client running environment after the checking succeeds.

[00102] The execution unit generation module 204 may search for a content
10 authorization execution unit template corresponding to the media content according to the identifier of the media content and/or the content encryption algorithm adopted by the media content and/or the DRM version number corresponding to the media content, and generate the content authorization execution unit 104 in accordance with the content authorization execution unit template obtained through search.

[00103] The execution unit acquisition module 108 of the DRM client 100 may also be
15 a communication execution unit. After acquiring the invoking request of the media application, the DRM client 100 sends a request for the communication execution unit to the DRM server side 200. The request for the communication execution unit at least should contain the basic information of the DRM client 100 and may also contain the identifier of
20 the media content and DRM version number information corresponding to the media content. After the DRM message receiving module 207 receives the request of the DRM client 100 for the communication execution unit, the execution unit generation module 204 searches for a communication execution unit template according to the request for the communication execution unit, and generates the communication execution unit in
25 accordance with the communication execution unit template obtained through search. The execution unit signature module 210 signs the communication execution unit generated by the execution unit generation module 204. The execution unit issuing module 209 issues the signed communication execution unit to the DRM client 100. After acquiring the communication execution unit, the DRM client 100 firstly checks the signature of the
30 communication execution unit and then runs the communication execution unit in the DRM client running environment after the checking succeeds. The execution unit generation module 204 may search for the communication execution unit template according to the identifier of the media content and/or the DRM version number corresponding to the media content and/or the basic information of the DRM client.

[00104] The DRM server side 200 may further comprise an execution unit template management module 203 for managing the execution unit template, comprising downloading, adding, updating, deleting the execution unit template.

[00105] The media content-related DRM information acquisition module 208 is configured to communicate with a key management system through the key management interface 206, and obtain the encryption algorithm and the content encryption key which are adopted by the media content from the key management system according to the identifier of the media content through query, or the media content-related DRM information acquisition module 208 obtains the content encryption algorithm of the media content from a storage region of the DRM server 2.

[00106] The media content-related DRM information acquisition module 208 communicates with an operation support system through the operation support interface 205, and obtains the DRM authority of the DRM client to the media content from the operation support system according to the identifier of the media content and the basic information of the DRM client through query.

[00107] The DRM client running environment comprises an execution unit engine 106, a terminal operating system adaptation module 107 and an execution unit scheduling and management module. The DRM client 100 schedules and manages various execution units through the execution unit scheduling and management module, comprising scheduling the execution unit to the execution unit engine 106 for running, and adding, deleting and updating the execution unit. The DRM client 100 adapts the execution unit engine 106 to a terminal operating system through the terminal operating system adaptation module 107. The execution unit engine 106 further provides a memory management interface, an external storage management interface, a network management interface, a cryptographic algorithm interface, a playing control interface and an output control interface for the running of the execution unit. The terminal operating system adaptation module 107 adapts the memory management interface, the external storage management interface, the network management interface, the cryptographic algorithm interface, the playing control interface and the output control interface of the execution unit engine 106 to corresponding interfaces of the terminal operating system.

[00108] <SECOND EMBODIMENT>

[00109] A digital rights management method, a DRM client 100 and a DRM server side 200 provided in a second embodiment of the present invention are illustrated with

reference to Fig. 4. The second embodiment adds a digital watermark function on the basis of the first embodiment. To be specific:

[00110] if a digital watermark is embedded in media content to be played, the DRM authority of the DRM client 100 to the media content comprises that the DRM client 100 must check the digital watermark of the media content when playing the media content. The step of scheduling a digital watermark execution unit is contained in the content authorization execution unit template corresponding to the media content.

[00111] When the content authorization execution unit 104 runs in the DRM client running environment and notifies the DRM client 100 that the digital watermark execution unit needs to be started, the execution unit acquisition module 108 requests a digital watermark execution unit corresponding to the media content from the DRM server side 200 according to the notification. The request for the digital watermark execution unit may contain the identifier of the media content and the basic information of the DRM client 100.

[00112] After the DRM server side 200 receives the request of the DRM client 100 for the digital watermark execution unit corresponding to the media content, the execution unit generation module 204 searches for a digital watermark execution unit template corresponding to the media content according to the identifier of the media content, and generates the digital watermark execution unit according to the digital watermark execution unit template corresponding to the media content. Then the execution unit signature module 210 signs the digital watermark execution unit. The execution unit issuing module 209 issues the signed digital watermark execution unit 105 to the DRM client 100.

[00113] After the DRM client 100 receives the digital watermark execution unit 105, the execution unit signature checking module 109 firstly checks the signature of the digital watermark execution unit 105. The digital watermark execution unit 105 is run in the DRM client running environment after the checking succeeds. The digital watermark execution unit 105 checks the digital watermark embedded into the media content in the playing process of the media content and stops playing the media content if the checking fails.

[00114] Further, if the digital watermark of the media content contains information of a restriction requirement of a content provider of the media content for a playing environment of the media content, the digital watermark execution unit 105 determines whether the terminal running environment conforms to the restriction requirement of the content provider of the media content for the playing environment of the media content in the playing process of the media content and if not, stops playing the media content. The content provider involved in the present invention may be an original provider of the

content. For example, if a film company is responsible for shooting a film, the film company is the original provider of the content, and the film company may have special requirements for a playing environment of the film shot thereby. For example, if the film company requires that the film must be played on a smart TV rather than a smart phone, the film company may embed a digital watermark carrying restriction requirement information of the playing environment in the film. An operator provides the film for users after purchasing the operation authority of the film. When the film is to be watched, the users can decrypt and play the film only if they meet the requirements of the film company for the playing environment in addition to meeting DRM requirements of the operator for the film.

[00115] THIRD EMBODIMENT

[00116] A digital rights management method, a DRM client 100 and a DRM server side 200 provided in a third embodiment of the present invention are illustrated with reference to Fig. 4. The third embodiment adds a digital watermark function on the basis of the first embodiment. To be specific:

[00117] the DRM authority of the DRM client to the media content comprises that the DRM client must embed a digital watermark for tracking the media content when playing the media content. The step of scheduling the digital watermark execution unit is contained in the content authorization execution unit template corresponding to the media content.

[00118] When the content authorization execution unit 104 runs in the DRM client running environment and notifies the DRM client 100 that the digital watermark execution unit needs to be started, the execution unit acquisition module 108 requests a digital watermark execution unit corresponding to the media content from the DRM server side 200 according to the notification. The request for the digital watermark execution unit may contain the identifier of the media content and the basic information of the DRM client 100.

[00119] After the DRM server side 200 receives the request of the DRM client 100 for the digital watermark execution unit corresponding to the media content, the execution unit generation module 204 searches for a digital watermark execution unit template corresponding to the media content according to the identifier of the media content, and generates the digital watermark execution unit according to the digital watermark execution unit template corresponding to the media content. Then the execution unit signature module 210 signs the digital watermark execution unit. The execution unit issuing module 209 issues the signed digital watermark execution unit 105 to the DRM client 100.

[00120] After the DRM client 100 receives the digital watermark execution unit 105,

the execution unit signature checking module 109 firstly checks the signature of the digital watermark execution unit 105. Then the digital watermark execution unit 105 is run in the DRM client running environment after the checking succeeds. The digital watermark execution unit 105 embeds the digital watermark for tracking the media content in the playing process of the media content.

[00121] In other embodiments, when the content authorization execution unit 104 notifies the DRM client 100 that the digital watermark execution unit needs to be started, the notification may contain basic information of the digital watermark execution unit. The basic information of the digital watermark execution unit in the present invention at least comprises an ID of the digital watermark execution unit and may also comprise information such as a version number of the digital watermark. In this case, when the execution unit acquisition module 108 requests the digital watermark execution unit corresponding to the media content from the DRM server side 200, the request for the digital watermark execution unit may contain the basic information of the digital watermark execution unit and the basic information of the DRM client 100. After the DRM server side 200 receives the request of the DRM client 100 for the digital watermark execution unit corresponding to the media content, the execution unit generation module 204 searches for a digital watermark execution unit template according to the basic information of the digital watermark execution unit and generates the digital watermark execution unit in accordance with the found digital watermark execution unit template.

[00122] <FOURTH EEMBODIMENT>

[00123] A digital rights management method, a DRM client 100 and a DRM server side 200 provided in a fourth embodiment of the present invention are illustrated with reference to Fig. 5. The DRM client 100 comprises a media application interface 1001, an execution unit scheduling and management module 1002, an execution unit engine 1006 and a terminal operating system adaptation module 1007. The DRM server side 200 comprises an operation support interface 2005, a key management interface 2006, a DRM message scheduling module 2001, a DRM message processing module 2002, an execution unit generation module 2004 and an execution unit template management module 2003.

[00124] S201 includes receiving by the DRM client 100 an invoking request of a media application of a terminal device through the media application interface 101, and acquiring by the DRM client 100 basic information of the media content to be played from the invoking request. The basic information of the media content at least should comprise a

unique identifier of the media content and may also comprise other information of the media content, such as a document name, a size, duration and a corresponding DRM version number.

[00125] S202 includes querying, by the execution unit scheduling and management module 1002, whether there is an available communication execution unit 1003 according to an identifier of the media content and/or the DRM version number corresponding to the media content and if so, scheduling the DRM execution unit engine 1006 to run the communication execution unit 1003.

[00126] S203 induces sending, by the communication execution unit 1003, a DRM authorization request to the DRM server side 200, wherein the DRM authorization request at least should contain the identifier of the media content and basic information of the DRM client 100 and may also comprise DRM version number information corresponding to the media content. The basic information of the DRM client 100 at least should comprise an ID of the DRM client 100 and may also comprise other information of the DRM client 100, such as address information, a version number and a certificate.

[00127] S204 includes invoking, by the DRM message scheduling module 2001 of the DRM server side 200, certain DRM message processing module 2002 to process the DRM authorization request after receiving the DRM authorization request.

[00128] S205 includes, by the DRM message processing module 2002, querying an encryption algorithm and a content encryption key, which correspond to the media content, from a key management system according to the identifier of the media content through the key management interface 2006, querying the DRM authority of the DRM client 100 to the media content from an operation support system according to the identifier of the media content and the basic information of the DRM client 100 through the operation support interface 2005, and querying a corresponding content authorization execution unit template from the DRM execution unit template management module 2003 according to the identifier of the media content.

[00129] S206 includes sending, by the DRM message processing module 2002, the identifier of the media content, the content encryption algorithm and the content encryption key which are adopted by the media content, the basic information of the DRM client 100, the DRM authority of the DRM client 100 to the media content and the found content authorization execution unit template to the DRM execution unit generation module 2004.

[00130] S207 includes generating, by the DRM execution unit generation module 2004, a corresponding content authorization execution unit in accordance with the found

content authorization execution unit template and according to the identifier of the media content, the content encryption algorithm and the content encryption key which are adopted by the media content, the basic information of the DRM client 100, and the DRM authority of the DRM client 100 to the media content.

5 **[00131]** S208 includes signing, by the DRM message processing module 2002, the generated content authorization execution unit and issuing the signed content authorization execution unit to the DRM client 100.

10 **[00132]** S209 includes receiving, by the DRM client 100, the content authorization execution unit 1004 through the communication execution unit 1003 and notifying, by the communication execution unit 1003, the execution unit scheduling and management module 1002 after receiving the content authorization execution unit.

15 **[00133]** S210 includes, by the execution unit scheduling and management module 1002, firstly checking the legality of the signature of the content authorization execution unit 1004 and scheduling the content authorization execution unit 1004 to the execution unit engine 1006 for running after the checking succeeds.

20 **[00134]** S211 includes, using the content authorization execution unit 1004, determining and verifying whether the terminal running environment conforms to the DRM authority of the DRM client to the media content, if so, decrypting the content encryption key to obtain a content key, decrypting the media content according to the content key and the content encryption algorithm, and controlling the playing.

25 **[00135]** In the step S202, if the execution unit scheduling and management module 1002 does not find the corresponding communication execution unit, the execution unit scheduling and management module 1002 requests the communication execution unit from the DRM server side 200. After receiving the request, the DRM server side queries a communication execution unit template, generates the communication execution unit according to the basic information of the DRM client and in accordance with the communication execution unit template, signs the communication execution unit and sends the signed communication execution unit to the DRM client 100. After the DRM client 100 obtains the communication execution unit, the execution unit scheduling and management module 1002 firstly verifies the legality of the signature of the communication execution unit, stores the communication execution unit after the verification succeeds, and interacts with the DRM server side 200 by running the communication execution unit through the execution unit engine so as to acquire other execution units such as the content authorization execution unit.

30

[00136] It can be seen from Fig. 5 that the DRM client 100 further comprises a digital watermark execution unit 1005. The principle and function of the digital watermark execution unit 1005 may be similar to those of the second and third embodiments. The step of scheduling the digital watermark execution unit is contained in the content authorization execution unit template corresponding to the media content. The DRM client 100 generates a request for the digital watermark execution unit according to the running of the content authorization execution unit 1004. The DRM server side 200 searches for a digital watermark execution unit template corresponding to the media content, generates the digital watermark execution unit 1005 in accordance with the template, and issues the digital watermark execution unit 1005 to the DRM client 100.

[00137] The execution unit scheduling and management module 1002 is responsible for scheduling and managing the download, verification, installation, update, query, execution, and termination of the execution unit, and installs and runs the execution unit by starting the execution unit engine 1006.

[00138] With reference to the above embodiments, the present invention further provides a terminal device with the above DRM client, and a DRM server with the above DRM server side.

[00139] The terminal device 1 provided in the embodiments of the present invention is illustrated with reference to Fig. 6. The terminal device 1 comprises a memory 3020 and a processor 3010. The memory 3020 is configured to store an instruction for controlling the processor 3010 to perform a corresponding operation so as to implement the digital rights management method of the media content of the present invention.

[00140] The terminal device 1 further comprises an interface device 3030, a communication device 3040, a display device 3050, an input device 3060, a speaker 3070, a microphone 3080, and the like.

[00141] The processor 3010, for example, may be a central processing unit (CPU), a microprocessor (MCU), and the like. The memory 3020, for example, comprises an ROM (read only memory), an RAM (random access memory), a non-volatile memory such as a hard disk. The interface device 3030, for example, comprises a USB interface, an earphone jack or the like. The communication device 3040, for example, is capable of performing wired communication or wireless communication. The display device 3050, for example, is a liquid crystal display screen, a touch display screen or the like. The input device 3060, for example, may comprise a touch screen, a keyboard or the like. A user may input/output voice information through the speaker 3070 and the microphone 3080.

[00142] The terminal device shown in Fig. 6 is only explanatory and by no means intends to limit the present invention and its application or use. A person skilled in the art should understand that although a plurality of devices is shown in Fig. 6, part of devices in these devices may be involved only in the present invention. A person skilled in the art may design an instruction according to the solution disclosed in the present invention. How to control the processor to operate through the instruction is a known technique in the art and thus is not described in detail herein.

[00143] In the present invention, the way of authorizing content through a content authorization license is changed. The DRM client requests the DRM authorization to the media content from the DRM server side after receiving the invoking request of the media application. The DRM server side generates the content authorization execution unit according to the encryption algorithm and the content encryption key of the media content, the DRM authority of the DRM client to the media content and the like and issues the content authorization execution unit to the DRM client, and the DRM client directly runs the content authorization execution unit in the DRM client running environment so as to decrypt the media content.

[00144] In the technical solution of the present invention, since the execution unit generated by the DRM server side may directly run in the DRM client running environment after being sent to the DRM client, a personalized content encryption algorithm, the authorization rule and the like may be set for certain media content as long as a corresponding execution unit template is provided at the DRM server side.

[00145] By using the technical solution of the present invention, the content encryption algorithm may be upgraded or replaced frequently, which is particularly suitable for protecting ultra-high-definition content, thereby avoiding the problem of frequently upgrading the DRM client.

[00146] By using the technical solution of the present invention, a new DRM function or a new authorization rule may further be added as long as the corresponding execution unit template is provided at the DRM server side without upgrading the DRM client and the DRM server side on the whole, facilitating the commercial operation.

[00147] It can be seen that by using the technical solution of the present invention, the media content may be flexibly managed and protected, and thus the security of the media content is higher.

[00148] The DRM client of the present invention may run in the trusted execution environment of the terminal. In the case based on the trusted execution environment, the

update of a content protection algorithm and the like only requires the DRM server side to generate different execution units and send the same to the DRM client for running, which does not affect the normal use of the functions of other non-DRM clients in the trusted execution environment.

5 **[00149]** The DRM client runs the execution unit in the DRM client running environment and realizes the authorization to the media content by running the execution unit. The execution unit is issued by the DRM server side. Therefore, the situation that the DRM client does not decrypt and play the content in accordance with requirements of the permission and restriction conditions may be avoided, thereby solving loopholes and
10 disadvantages brought by an existing way of parsing a content authorization license.

[00150] The present invention may be a system, a method, and/or a computer program product. The computer program product may include a computer readable storage medium (or media) having computer readable program instructions thereon for causing a processor to carry out aspects of the present invention.

15 **[00151]** The computer readable storage medium can be a tangible device that can retain and store instructions for use by an instruction execution device. The computer readable storage medium may be, for example, but is not limited to, an electronic storage device, a magnetic storage device, an optical storage device, an electromagnetic storage device, a semiconductor storage device, or any suitable combination of the foregoing. A
20 non-exhaustive list of more specific examples of the computer readable storage medium includes the following: a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), a static random access memory (SRAM), a portable compact disc read-only memory (CD-ROM), a digital versatile disk (DVD), a memory stick, a floppy
25 disk, a mechanically encoded device such as punch-cards or raised structures in a groove having instructions recorded thereon, and any suitable combination of the foregoing. A computer readable storage medium, as used herein, is not to be construed as being transitory signals per se, such as radio waves or other freely propagating electromagnetic waves, electromagnetic waves propagating through a waveguide or other transmission media (e.g.,
30 light pulses passing through a fiber-optic cable), or electrical signals transmitted through a wire.

[00152] Computer readable program instructions described herein can be downloaded to respective computing/processing devices from a computer readable storage medium or to an external computer or external storage device via a network, for example, the Internet, a

local area network, a wide area network and/or a wireless network. The network may comprise copper transmission cables, optical transmission fibers, wireless transmission, routers, firewalls, switches, gateway computers and/or edge servers. A network adapter card or network interface in each computing/processing device receives computer readable
5 program instructions from the network and forwards the computer readable program instructions for storage in a computer readable storage medium within the respective computing/processing device.

[00153] Computer readable program instructions for carrying out operations of the present invention may be assembler instructions, instruction-set-architecture (ISA)
10 instructions, machine instructions, machine dependent instructions, microcode, firmware instructions, state-setting data, or either source code or object code written in any combination of one or more programming languages, including an object oriented programming language such as Smalltalk, C++ or the like, and conventional procedural programming languages, such as the "C" programming language or similar programming
15 languages. The computer readable program instructions may execute entirely on the user's computer, partly on the user's computer, as a stand-alone software package, partly on the user's computer and partly on a remote computer or entirely on the remote computer or server. In the latter scenario, the remote computer may be connected to the user's computer through any type of network, including a local area network (LAN) or a wide area network
20 (WAN), or the connection may be made to an external computer (for example, through the Internet using an Internet Service Provider). In some embodiments, electronic circuitry including, for example, programmable logic circuitry, field-programmable gate arrays (FPGA), or programmable logic arrays (PLA) may execute the computer readable program instructions by utilizing state information of the computer readable program instructions to
25 personalize the electronic circuitry, in order to perform aspects of the present invention.

[00154] Aspects of the present invention are described herein with reference to flowchart illustrations and/or block diagrams of methods, apparatus (systems), and computer program products according to embodiments of the invention. It will be understood that each block of the flowchart illustrations and/or block diagrams, and
30 combinations of blocks in the flowchart illustrations and/or block diagrams, can be implemented by computer readable program instructions.

[00155] These computer readable program instructions may be provided to a processor of a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions, which execute via the

processor of the computer or other programmable data processing apparatus, create means for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks. These computer readable program instructions may also be stored in a computer readable storage medium that can direct a computer, a programmable data processing apparatus, and/or other devices to function in a particular manner, such that the computer readable storage medium having instructions stored therein comprises an article of manufacture including instructions which implement aspects of the function/act specified in the flowchart and/or block diagram block or blocks.

[00156] The computer readable program instructions may also be loaded onto a computer, other programmable data processing apparatus, or other device to cause a series of operational steps to be performed on the computer, other programmable apparatus or other device to produce a computer implemented process, such that the instructions which execute on the computer, other programmable apparatus, or other device implement the functions/acts specified in the flowchart and/or block diagram block or blocks.

[00157] The flowchart and block diagrams in the Figures illustrate the architecture, functionality, and operation of possible implementations of systems, methods and computer program products according to various embodiments of the present invention. In this regard, each block in the flowchart or block diagrams may represent a module, segment, or portion of code, which comprises one or more executable instructions for implementing the specified logical function(s). It should also be noted that, in some alternative implementations, the functions noted in the block may occur out of the order noted in the figures. For example, two blocks shown in succession may, in fact, be executed substantially concurrently, or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved. It will also be noted that each block of the block diagrams and/or flowchart illustration, and combinations of blocks in the block diagrams and/or flowchart illustration, can be implemented by special purpose hardware-based systems that perform the specified functions or acts, or combinations of special purpose hardware and computer instructions. It is well-known to a person skilled in the art that the implementations of using hardware, using software or using the combination of software and hardware can be equivalent with each other.

[00158] The descriptions of the various embodiments of the present invention have been presented for purposes of illustration, but are not intended to be exhaustive or limited to the embodiments disclosed. Many modifications and variations will be apparent to those of ordinary skill in the art without departing from the scope and spirit of the described

embodiments. The terminology used herein was chosen to best explain the principles of the embodiments, the practical application or technical improvement over technologies found in the marketplace, or to enable others of ordinary skill in the art to understand the embodiments disclosed herein. The scope of the present invention is defined by the attached

5 claims.

CLAIMS

1. A digital rights management (DRM) method of media content implemented in a terminal device, on which a DRM client is installed, the method comprising:

5 step 1: receiving by the DRM client an invoking request of a media application of the terminal device, and acquiring by the DRM client a unique identifier of media content to be played from the invoking request;

 step 2: sending, by the DRM client, a DRM authorization request to a DRM server side so as to acquire a content authorization execution unit, wherein the DRM authorization request contains an identifier of the media content and basic information of the DRM client, wherein

10 the content authorization execution unit is generated by the DRM server side in the following way: the DRM server side obtains a content encryption algorithm and a content encryption key which are adopted by the media content, and DRM authority of the DRM client to the media content according to the DRM authorization request through query, and is then generated according to the identifier of the media content, the content encryption algorithm and the content encryption key which are adopted by the media content, the basic information of the DRM client, and the DRM authority of the DRM client to the media content; and

20 step 3, by the DRM client, running the content authorization execution unit in a DRM client running environment, verifying whether a terminal running environment conforms to the DRM authority of the DRM client to the media content through the content authorization execution unit, and if so, decrypting the media content according to the content encryption algorithm and the content encryption key.

25 2. A digital rights management (DRM) method of media content implemented in a DRM server side, the method comprising:

 step 1: receiving, by the DRM server side, a DRM authorization request sent by a DRM client, wherein the DRM authorization request contains a unique identifier of the media content and basic information of the DRM client;

30 step 2: obtaining, by the DRM server side, a content encryption algorithm and a content encryption key which are adopted by the media content, and DRM authority of the DRM client to the media content according to the DRM authorization request through query;

 step 3, generating, by the DRM server side, a content authorization execution unit

according to an identifier of the media content, the content encryption algorithm and the content encryption key which are adopted by the media content, the basic information of the DRM client, and the DRM authority of the DRM client to the media content, wherein the content authorization execution unit is configured to run in a DRM client running environment so as to verify whether a terminal running environment of a terminal device where the DRM client is located conforms to the DRM authority of the DRM client to the media content, and if so, decrypt the media content according to the content encryption algorithm and the content encryption key; and

step 4: issuing, by the DRM server side, the generated content authorization execution unit to the DRM client.

3. A DRM client arranged in a terminal device, in which an intelligent operating system is installed, the DRM client comprising a media application interface, an execution unit acquisition module and a content authorization execution unit, wherein

the media application interface is configured to receive an invoking request of a media application of the terminal device and acquire a unique identifier of media content to be played from the invoking request;

the execution unit acquisition module is configured to send a DRM authorization request to a DRM server side so as to acquire the content authorization execution unit, wherein the DRM authorization request contains an identifier of the media content and basic information of the DRM client; and

the content authorization execution unit is configured to verify whether a terminal running environment conforms to DRM authority of the DRM client to the media content, and if so, decrypt the media content according to a content encryption algorithm and a content encryption key, wherein

the content authorization execution unit is generated by the DRM server side in the following way: the DRM server side obtains the content encryption algorithm and the content encryption key which are adopted by the media content, and the DRM authority of the DRM client to the media content according to the DRM authorization request through query, and is then generated according to the identifier of the media content, the content encryption algorithm and the content encryption key which are adopted by the media content, the basic information of the DRM client, and the DRM authority of the DRM client to the media content.

4. The DRM client according to claim 3, further comprising an execution unit signature checking module configured to check the signature of the content authorization execution unit.

5. The DRM client according to claim 3 or 4, further comprising an execution unit engine and a terminal operating system adaptation module, wherein
the execution unit engine is configured to run an execution unit; and
the terminal operating system adaptation module is configured to adapt the execution unit engine to a terminal operating system.

6. The DRM client according to any of claims 3-5, wherein the execution unit engine is configured to provide a memory management interface, an external storage management interface, a network management interface, a cryptographic algorithm interface, a playing control interface and an output control interface for the running of the execution unit; and
the terminal operating system adaptation module is configured to adapt the memory management interface, the external storage management interface, the network management interface, the cryptographic algorithm interface, the playing control interface and the output control interface of the execution unit engine to corresponding interfaces of the terminal operating system.

7. The DRM client according to any of claims 3-6, further comprising an execution unit scheduling and management module, wherein
the execution unit scheduling and management module is configured to schedule and manage various execution units, comprising scheduling the execution unit to the execution unit engine for running, and adding, deleting and updating the execution unit.

8. A DRM server side comprising a DRM message receiving module, a media content-related DRM information acquisition module, an execution unit generation module, and an execution unit issuing module, wherein

the DRM message receiving module is configured to receive a DRM authorization request sent by a DRM client, wherein the DRM authorization request contains a unique identifier of media content and basic information of the DRM client;

the media content-related DRM information acquisition module is configured to obtain a content encryption algorithm and a content encryption key which are adopted by the media

content, and DRM authority of the DRM client to the media content according to the DRM authorization request through query;

5 the execution unit generation module is configured to generate a content authorization execution unit according to an identifier of the media content, the content encryption algorithm and the content encryption key which are adopted by the media content, the basic information of the DRM client, and the DRM authority of the DRM client to the media content and in accordance with a content authorization execution unit template corresponding to the media content, wherein the content authorization execution unit is configured to run in a DRM client running environment so as to verify whether a terminal
10 running environment of a terminal device where the DRM client is located conforms to the DRM authority of the DRM client to the media content and if so, decrypt the media content according to the content encryption algorithm and the content encryption key; and

the execution unit issuing module is configured to issue the content authorization execution unit to the DRM client.

15

9. The DRM server side according to claim 8, further comprising an execution unit signature module configured to sign the content authorization execution unit before the execution unit issuing module issues the content authorization execution unit.

20

10. The DRM server side according to claim 8 or 9, further comprising an execution unit template management module configured to manage the content authorization execution unit template, comprising adding, updating and deleting the content authorization execution unit template.