

METHOD AND SYSTEM FOR ADDING AND DETECTING WATERMARK

FIELD OF THE INVENTION

[0001] The present invention relates to the field of multimedia, and more particularly to a method and a system for adding or detecting a watermark in a multimedia file.

BACKGROUND OF THE INVENTION

[0002] Because of the rapid development of network and multimedia technologies, various multimedia data such as video files can be easily accessed through network. Although convenience of using the accessed multimedia data is undeniable, there are potential risks for security of the multimedia data. For example, pirates can spread huge multimedia data at low costs without authorization from creators or owners of the multimedia data, and such piracy impacts copyright and discourages creations. It is necessary to combine copyright information to the multimedia data to inhibit copyright infringement. A known method is to embed digital watermark in the multimedia data. Digital watermarking is a process of hiding digital information, which may include copyright information, in redundant data of the multimedia data according to a specific algorithm. Digital watermarks may be used to verify the authorization or integrity of the multimedia data so as to protect the intellectual property of legal owners of the multimedia data.

[0003] The digital watermark is usually embedded in the multimedia data before distribution or during playing. However, such action cannot effectively reduce piracy because the invisible digital watermark can be eliminated by non-contact image-capturing or recording. Even though an illegal copy is seized, the legal owner cannot trace the original distributor

of the illegal copy since the digital watermark is removed and cannot be restored for inspection.

SUMMARY OF THE INVENTION

[0004] The present invention provides a watermarking method and a client/server of a watermarking system for generating a watermark which can be traced and is not eliminated by non-contact copying.

[0005] The present invention further provides a watermark-detecting method and system for tracing a release source of the multimedia data by detecting the watermark.

[0006] According to an aspect of the present invention, the watermarking method is used with a client for watermarking multimedia data. The watermarking method includes: sending a login request to a server; receiving an identification code from the server; generating an on-screen watermark according to the identification code corresponding to the client; and adding the on-screen watermark onto the multimedia data. In response to the login request, the server authenticates an access right of the client to access the multimedia data and generates the identification code uniquely associated with the client according to the login request.

[0007] According to another aspect of the present invention, the watermarking method is used with a server for watermarking multimedia data. The watermarking method includes: receiving a login request from a client; authenticating an access right of the client to access the multimedia data in response to the login request; generating an identification code uniquely associated with the client according to the login request if the client is authenticated to have the access right to access the multimedia data; and sending the identification code to the client. Upon receiving the identification code, the client generates an on-screen watermark according to the identification code uniquely associated with

the client and adds the on-screen watermark onto the multimedia data.

[0008] According to a further aspect of the present invention, the watermarking method is used with a client for watermarking multimedia data. The watermarking method includes: sending a login request to a server; and receiving the multimedia data with an on-screen watermark from the server. In response to the login request, the server authenticates an access right of the client to access the multimedia data, generates an identification code uniquely associated with the client according to the login request, adds an on-screen watermark onto the multimedia data according to the identification code uniquely associated with the client, and sends the multimedia data with the on-screen watermark to the client.

[0009] According to a further aspect of the present invention, the watermarking method is used with a server for watermarking multimedia data. The watermarking method includes: receiving a login request from a client; authenticating an access right of the client to access the multimedia data; generating an identification code uniquely associated with the client according to the login request if the client is authenticated to have the access right to access the multimedia data; generating an on-screen watermark according to the identification code uniquely associated with the client; adding the on-screen watermark onto the multimedia data; and sending the multimedia data with the on-screen watermark to the client.

[0010] According to a further aspect of the present invention, a watermark-detecting method is used with a watermark-detecting system for detecting a watermark added onto multimedia data. The watermark-detecting method includes: retrieving the watermark from the multimedia data; analyzing the watermark to obtain an identification code; and looking the identification code up in an identification database to find out corresponding client information. The watermark is generated

according to the identification code and the identification code corresponds to one client. The identification database stores many identification codes and associated client information.

[0011] According to a further aspect of the present invention, a client of a watermarking system for watermarking multimedia data is provided. The client includes a login-requesting unit, a code-receiving unit and a superimposing unit. The login-requesting unit is used for sending a login request to a server of the watermarking system which authenticates an access right of the client to access the multimedia data and generates an identification code uniquely associated with the client according to the login request. The code-receiving unit is used for receiving the identification code from the server. The superimposing unit is used for generating an on-screen watermark according to the identification code uniquely associated with the client and superimposing the on-screen watermark on images of the multimedia data.

[0012] According to a further aspect of the present invention, a server of a watermarking system for watermarking multimedia data is provided. The server includes an authenticating unit, a code-generating unit and a code-sending unit. The authenticating unit is used for receiving a login request from a client of the watermarking system and authenticating an access right of the client to access the multimedia data in response to the login request. The code-generating unit is used for generating an identification code uniquely associated with the client according to the login request if the client is authenticated to have the access right to access the multimedia data. The code-sending unit is used for sending the identification code to the client which generates an on-screen watermark according to the identification code uniquely associated with the client and adding the on-screen watermark onto the multimedia data.

[0013] According to a further aspect of the present invention, a client

of a watermarking system for watermarking multimedia data is provided. The client includes a login-requesting unit and a data-receiving unit. The login-requesting unit is used for sending a login request to a server of the watermarking system which authenticates an access right of the client to the multimedia data, generates an identification code uniquely associated with the client according to the login request, adds an on-screen watermark onto the multimedia data according to the identification code uniquely associated with the client, and sends the multimedia data with the on-screen watermark to the client. The data-receiving unit is used for receiving the multimedia data with the on-screen watermark from the server.

[0014] According to a further aspect of the present invention, a server of a watermarking system for watermarking multimedia data is provided. The server includes an authenticating unit, a code-generating unit, a superimposing unit and a data-sending unit. The authenticating unit is used for receiving a login request from a client of the watermarking system and authenticating an access right of the client to access the multimedia data. The code-generating unit is used for generating an identification code uniquely associated with the client according to the login request if the client is authenticated to have the access right to access the multimedia data. The superimposing unit is used for generating an on-screen watermark according to the identification code uniquely associated with the client and superimposing the on-screen watermark on images of the multimedia data. The data-sending unit is used for sending the multimedia data with the on-screen watermark to the client.

[0015] According to a further aspect of the present invention, a watermark-detecting system can detect a watermark added onto multimedia data. The watermark-detecting system includes a retrieving unit, an analyzing unit and a look-up unit. The retrieving unit is used for

retrieving the watermark from the multimedia data. The analyzing unit is used for analyzing the watermark to obtain an identification code, wherein the watermark is generated according to the identification code and the identification code corresponds to one client. The look-up unit is used for looking the identification code up in an identification database to find out corresponding client information. The identification database stores many identification codes and associated client information.

BRIEF DESCRIPTION OF THE DRAWINGS

[0016] The present invention will become more readily apparent to those ordinarily skilled in the art after reviewing the following detailed description and accompanying drawings, in which:

[0017] FIG. 1 is a schematic diagram illustrating one embodiment of a watermarking system;

[0018] FIG. 2 is a flow chart illustrating one embodiment of a watermarking method for a client-side terminal;

[0019] FIG. 3 is a flow chart illustrating one embodiment of a watermarking method for a server-side terminal;

[0020] FIG. 4 is a flow chart illustrating another embodiment of a watermarking method for a client-side terminal;

[0021] FIG. 5 is a flow chart illustrating another embodiment of a watermarking method for a server-side terminal;

[0022] FIG. 6 is a flow chart illustrating one embodiment of a watermarking method for both of a client-side terminal and a server-side terminal;

[0023] FIG. 7 is a flow chart illustrating another embodiment of a watermarking method for both of a client-side terminal and a server-side terminal;

[0024] FIG. 8 is a flow chart illustrating one embodiment of a

watermark-detecting method;

[0025] FIGs. 9A and 9B are schematic block diagrams respectively illustrating structures of a client and a server of the watermarking system of FIG. 1;

[0026] FIGs. 10A and 10B are schematic block diagrams respectively illustrating another structures of a client and a server of the watermarking system of FIG. 1; and

[0027] FIG. 11 is a schematic block diagram illustrating a structure of a watermark-detecting system according to the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[0028] The present invention will now be described more specifically with reference to the following embodiments. It is to be noted that the following descriptions of preferred embodiments of this invention are presented herein for purpose of illustration and description only. It is not intended to be exhaustive or to be limited to the precise form disclosed.

[0029] Please refer to FIG. 1, a schematic diagram illustrating one embodiment of a watermarking system. The watermarking system 1 includes at least one client 11 and a server 12 in communication with each other. The client 11 registers one account in the server 12 so that the server 12 may identify the client 11 when the client 11 is logged in the server 12 with the account. If the server 12 confirms that the client 11 is allowed to access specific multimedia data, the server 12 generates an identification code associated with the client 11. Each client 11 has its own unique identification code. An on-screen watermark corresponding to the unique identification code will be added onto the multimedia data before playing or broadcasting the multimedia data. The on-screen watermark may be generated and attached to the multimedia data by the server 12 or the client 11 according to practical designs or requirements.

If the server 12 performs the watermarking, the multimedia data are shown on a screen of the client 11 after the client 11 receives the watermarked multimedia data sent from the server 12. Otherwise, the client 11 receives the multimedia data and the unique identification code respectively, generates an on-screen watermark according to the unique identification code, superimposes the on-screen watermark on the multimedia data, and shows the watermarked multimedia data on a screen of the client 11.

[0030] It is to be noted that the client 11 described in the present embodiment maybe computer hardware or software that can use a service provided by a server 12 through a network. For some servers, a computer device is considered as a single client; for other servers, a computer device may be associated with more than one client because several accounts are registered in the server 12 through the computer device. In the present invention, sometimes a web browser or video player software installed in a computer device capable of issuing access request to the server 12 is also considered as a client 11. Besides, any known authentication method can be used by the servers 12, if possible.

[0031] The above-mentioned multimedia data include a combination of text, audio, still images, animation, video, or interactive content. The client 11 may play or broadcast the multimedia data by means of any proper software or hardware.

Embodiment 1

[0032] One embodiment of a watermarking method performed by a client is described in detail with reference to a flow chart in FIG. 2. In step S201, the client 11 sends a login request to the server 12. The server 12 will authenticate an access right of the client 11 to access multimedia data and generate an identification code that is uniquely associated with the client 11 according to the login request. Before the login step, the

client 11 should register an account in the server 12. The register information of every client 11 is stored in the server 12. When the client 11 is required to show or play the multimedia data received from the server 12, the client 11 has to log in the server 12, and the server 12 can identify the client 11 based on the login request and the register information stored in the server 12. Therefore, the server 12 can check whether the client 11 is allowed to access or play the multimedia data. The client 11 may be video player software or a web browser.

[0033] In step S202, the client 11 receives the identification code sent from the server 12. The identification code of each client 11 is unique. Sometimes, one identification code is associated with only one client, but one client may have at least one unique identification code for trace purpose. The unique identification code may be encrypted by the server 12 to enhance security of on-screen watermark.

[0034] In step S203, the client 11 generates the on-screen watermark according to the identification code that is uniquely associated with the client 11 and adds the on-screen watermark onto the multimedia data. In the present embodiment, the on-screen watermark is superimposed on images of the multimedia data, and the multimedia data may be video data, animation data or text data. Furthermore, the client 11 receives a digital watermark from the server 12 and embeds the digital watermark in the multimedia data to be played. The server 12 generates the digital watermark associated with the client 11 according to the login request if the client 11 is authenticated to have the access right to access the multimedia data. The digital watermark associated to each client 11 may be, but is not limited to, unique digital watermark. Thus, the played multimedia data include the on-screen watermark and the digital watermark which can effectively reduce infringement intention.

Embodiment 2

[0035] One embodiment of a watermarking method performed by a server is described in detail with reference to a flow chart in FIG. 3. In step S301, the server 12 receives a login request from the client 11 and authenticates an access right of the client 11 accessing the multimedia data in response to the login request. Before the login step, the server 12 has stored register information of the client 11. Upon receiving the login request from the client 11, the server 12 can identify the client 11 based on the login request and the stored register information.

[0036] In step S302, the server 12 generates an identification code that is uniquely associated with the client 11 according to the login request if the client 11 is authenticated to have the access right to access the multimedia data. For increasing difficulty in attacking an on-screen watermark attached to the multimedia data, the unique identification code may be encrypted by the server 12.

[0037] In step S303, the server 12 sends the identification code to the client 11 to make the client 11 to generate the on-screen watermark according to the identification code that is uniquely associated with the client 11, and to add the on-screen watermark onto the multimedia data. Furthermore, the server 12 may generate a digital watermark associated with the client 11 according to the login request if the client is authenticated to have the access right to access the multimedia data. Then, the server 12 sends the digital watermark to the client 11 which will embed the digital watermark in the multimedia data. The digital watermark associated to each client 11 may be, but is not limited to, unique digital watermark. Thus, the played or broadcast multimedia data include the on-screen watermark and the digital watermark which can effectively reduce infringement intention.

Embodiment 3

[0038] Another embodiment of a watermarking method performed by

a client is described in detail with reference to a flow chart in FIG. 4. In step S401, the client 11 sends a login request to the server 12. The server 12 authenticates an access right of the client 11 to access the multimedia data, generates an identification code that is uniquely associated with the client 11 according to the login request, adds an on-screen watermark onto the multimedia data according to the identification code that is uniquely associated with the client 11, and sends the multimedia data with the on-screen watermark to the client 11.

[0039] In step S402, the client 11 receives the multimedia data with the on-screen watermark sent from the server 12. In addition to the on-screen watermark, the multimedia data received by the client 11 may be attached with a digital watermark to effectively reduce infringement intention.

[0040] Compared with the method as described with reference to FIG. 2, watermarks associated with different clients 11 in FIG. 4 are generated and attached to the multimedia data by the server 12 before the multimedia data are sent out. Thus, the method of FIG. 4 can prevent the multimedia data from being stolen during the transmission of the multimedia data before watermarking. Since the watermarking steps are performed by the server 12 rather than different clients 11, the overall efficiency of the watermarking system 1 increases because the efficiency of different clients 11 is not anticipatable or controllable sometimes, and the loading of the clients 11 is thus reduced.

Embodiment 4

[0041] Another embodiment of a watermarking method performed by a server is described in detail with reference to a flow chart in FIG. 5. In step S501, the server 12 receives a login request from the client 11 and authenticates an access right of the client 11 to access the multimedia data in response to the login request.

[0042] In step S502, the server 12 generates an identification code that is uniquely associated with the client 11 according to the login request if the client is authenticated to have the access right to access the multimedia data.

[0043] In step S503, the server 12 generates an on-screen watermark according to the identification code that is uniquely associated with the client 11 and adds the on-screen watermark onto the multimedia data. In the present embodiment, the on-screen watermark is superimposed on images of the multimedia data.

[0044] In step S504, the server 12 sends the multimedia data with the on-screen watermark to the client 11.

[0045] In the embodiment, the method may further include: generating a digital watermark associated with the client 11 according to the login request if the client is authenticated to have the access right to access the multimedia data; embedding the digital watermark in the multimedia data; sending the multimedia data with the on-screen watermark and the digital watermark to the client 11.

[0046] Compared with the method as described with reference to FIG. 3, watermarks associated with different clients 11 in FIG. 5 are generated and attached to the multimedia data by the server 12 before the multimedia data are sent out. Thus, the method of FIG. 5 can prevent the multimedia data from being stolen during the transmission of the multimedia data before watermarking. Since the watermarking steps are performed by the server 12 rather than different clients 11, the overall efficiency of the watermarking system 1 increases, and the loading of the clients 11 is thus reduced.

Embodiment 5

[0047] Please refer to FIG. 6, a flow chart illustrating one embodiment of a watermarking method performed by both of a client and

a server. At first, the client 11 sends a login request to the server 12 for authentication (step S601). The authentication may be an identity authentication or an access right authentication, and is detected in step S602. Upon the condition that the server 12 does not authenticate the client 11 to access the multimedia data, the flow returns to step S601. Otherwise, if the server 12 authenticates that the client 11 has an access right to access the multimedia data, the server 12 generates an identification code corresponding to the client 11 (step S603). In the embodiment, each client 11 corresponds to a unique identification code. In other words, different clients 11 correspond to different identification codes. The server 12 sends the identification code to the login client 11 (step S604). The identification code is also stored in an identification database, which records many identification codes and associated client information. For example, the associated client information may include, but not limited to, an IP address, a media access control address (MAC address) of a network interface installed in the client 11, and client's register information or user information. In one embodiment, the identification code is encrypted by the server 12 before the step S604, so that it is difficult to capture and tamper the identification code and the security of accessing the multimedia data is enhanced. After the client 11 receives the identification code (step S605), the client 11 generates an on-screen watermark according to the identification code, and adds the on-screen watermark onto the multimedia data for display, playing, or broadcasting (step S606). The multimedia data and the identification code may be sent from the server 12 during the same login or different logins. The on-screen watermark may be a pattern, a word string, a barcode or a dynamic image which is not recognized by subscribers or viewers. The on-screen watermark may be kept on the same position of images of the multimedia data or dynamically moved to different positions

to increase the difficulty of illegal modification. The on-screen watermark should not affect the image context so that it is usually located at corners of the images.

[0048] Furthermore, upon authenticating the client 11, the server 12 also generates a digital watermark that is associated with the client 11. Similarly, each client 11 corresponds to a unique digital watermark. Then, the digital watermark is sent to the client 11. Before playing or displaying the multimedia data, the client 11 adds the on-screen watermark on the multimedia data and embeds the digital watermark in the multimedia data. The digital watermark is usually imperceptible and only perceptible under certain conditions, e.g. after some algorithm. Therefore, it is hard to attack or modify the digital watermark. It offers the multimedia data double security regardless of contact or non-contact copying. The on-screen watermark inhibits the pirate from capturing the multimedia data by non-contact image-capturing or recording, while the digital watermark inhibits the pirate from cloning the original multimedia data and spreading the cloned multimedia data. The multimedia data shown on a screen of the client 11 includes the on-screen watermark and the digital watermark, and the watermarks can effectively reduce the intention of arbitrarily spreading the watermarked multimedia data to avoid copyright infringement.

[0049] In the embodiment, the client 11 receives the unique identification code generated by the sever 12, and the client 11 can be identified according to the identification code. The multimedia data are shown together with the on-screen watermark which indicates the unique identification code. It means that the client 11 can be identified by inspecting the on-screen watermark superimposed on the multimedia data. Even though the illegal copy is generated by non-contact manner such as non-contact image-capturing, the release source still can be traced

according to the on-screen watermark.

Embodiment 6

[0050] Please refer to FIG. 7, a flow chart illustrating one embodiment of a watermarking method performed by both of a client and a server. At first, the client 11 sends a login request to the server 12 for authentication (step S701). The authentication may be an identity authentication or an access right authentication, and is detected in step S702. Upon the condition that the server 12 does not authenticate the client 11 to access the multimedia data, the flow returns to step S701. Otherwise, if the server 12 authenticates that the client 11 has an access right to access the multimedia data, the server 12 generates an identification code corresponding to the client 11 (step S703). In the embodiment, the identification code of each client 11 is unique. The identification code is also stored in an identification database, which records many identification codes and associated client information. The server 12 generates an on-screen watermark according to the identification code, and adds the on-screen watermark onto the multimedia data by superimposition (step 704). The on-screen watermark may be kept on the same position of images of the multimedia data or dynamically moved to different positions to increase the difficulty of illegal modification. Then, the server 12 sends the multimedia data with the on-screen watermark to the login client 11 (step S705). At last, the client 11 receives the multimedia data with the on-screen watermark to be viewed (step S706).

[0051] Before the login step, there is a register step for the server 12 to record the register information of the client 11, and the register information is used for later authentication. The register step is similar to that described above and repetitious details are not given here.

[0052] Upon authenticating the client 11, the server 12 may further

generate a digital watermark associated with the client 11 and embed the digital watermark in the multimedia data. Similarly, the digital watermark of each client 11 is unique. Therefore, the watermarked multimedia data received by the client 11 has included the one-screen watermark and the digital watermark. The on-screen watermark inhibits the pirate from capturing the multimedia data by non-contact image-capturing or recording, while the digital watermark inhibits the pirate from cloning the original multimedia data and spreading the cloned multimedia data.

Embodiment 7

[0053] The watermark added according to the above-described methods will be detected if infringement occurs. A method for detecting the watermark superimposed on the multimedia data is described in detail with reference to a flow chart in FIG. 8. At first, the watermark added onto the multimedia data is retrieved from the multimedia data to be inspected (step S801). The watermark is analyzed to obtain the identification code (step S802). The watermark is previously generated according to the identification code which corresponds to one client 11. If the identification code is ever encrypted, the encrypted identification code should be decrypted to obtain the unique identification code. There is an identification database stored in the server 12. The identification database records information of every client 11 and corresponding identification code of the every client 11. Thus, the server 12 looks up the identification code obtained in step S802 in the identification database to find out the corresponding client information (step 803).

[0054] In the embodiment, if pirated multimedia data or suspicious multimedia data are seized, the present watermark-detecting method can be used to trace the piracy source. The watermark added onto the multimedia data is retrieved and analyzed to obtain the unique

identification code associated with the exact client. Thus, the owner or author of the multimedia data can take necessary actions to stop the infringement and minimize the damage. It is easy and convenient to implement the watermark-detecting method with low costs.

[0055] Please refer to FIGs. 9A and 9B, schematic block diagrams respectively illustrating structures of the client 11 and the server 12 of the watermarking system 1 illustrated in FIG. 1. It is to be noted that only a relative portion of the system is shown in the schematic block diagrams, but it is not intended to limit the real structure thereof. The client 11 includes a login-requesting unit 111, a code-receiving unit 112, and a superimposing unit 113; and the server 12 includes an authenticating unit 121, a code-generating unit 122, and a code-sending unit 123.

[0056] With regard to functions of the components of the client 11, the login-requesting unit 111 sends a login request to the server 12 which authenticates an access right of the client 11 to access the multimedia data and generates an identification code that is uniquely associated with the client 11 according to the login request. The code-receiving unit 112 receives the identification code sent from the server 12. The superimposing unit 113 generates an on-screen watermark according to the identification code that is uniquely associated with the client 11 and then superimposes the on-screen watermark on images of the multimedia data. A digital watermark may be further provided in the multimedia data. Thus, the code-receiving unit 112 receives the digital watermark from the server 12 which generates the digital watermark associated with the client 11 according to the login request if the client is authenticated to have the access right to access the multimedia data. Thus, the superimposing unit 113 embeds the digital watermark in the multimedia data. This client 11 may be used with the method as described in Embodiment 1, and the detailed operation is not repeated here.

[0057] With regard to functions of the components of the server 12, the authenticating unit 121 receives a login request from the client 11 and authenticates an access right of the client 11 to access the multimedia data in response to the login request. Concretely, the authenticating unit 121 confirms whether the client 11 is allowed to access or play the multimedia data. The code-generating unit 122 generates an identification code that is uniquely associated with the client 11 according to the login request if the client is authenticated to have the access right to access the multimedia data. The code-sending unit 123 sends the identification code to the client 11 which generates an on-screen watermark according to the identification code that is uniquely associated with the client 11 and adds the on-screen watermark onto the multimedia data. In addition to the on-screen watermark, a digital watermark may be optionally inserted into the multimedia data. Under this condition, the code-generating unit 122 generates the digital watermark associated with the client 11 according to the login request if the client is authenticated to have the access right to access the multimedia data. Then, the code-sending unit 123 sends the digital watermark to the client 11 so that the client 11 can embed the digital watermark in the multimedia data. This server 12 may be used with the method as described in Embodiment 2, and the detailed operation is not repeated here. In addition, the client 11 and the server 12 of FIGs. 9A and 9B may be cooperated with each other to perform the method as described in Embodiment 5.

[0058] Please refer to FIGs. 10A and 10B, schematic block diagrams respectively illustrating another structures of the client 11 and the server 12 of the watermarking system 1 illustrated in FIG. 1. It is to be noted that only a relative portion of the system is shown in the schematic block diagrams, but it is not intended to limit the real structure thereof. The client 11 includes a login-requesting unit 111 and a data-receiving unit 114;

and the server 12 includes an authenticating unit 121, a code-generating unit 122, a superimposing unit 124, and a data-sending unit 125.

[0059] With regard to functions of the components of the client 11, the login-requesting unit 111 sends a login request to the server 12 which generates an identification code that is uniquely associated with the client 11 according to the login request, adds an on-screen watermark onto the multimedia data according to the identification code that is uniquely associated with the client 11, and sends the multimedia data with the on-screen watermark to the client 11. The data-receiving unit 114 receives the multimedia data with the on-screen watermark to be viewed from the server 12. A digital watermark may be further provided in the multimedia data. Thus, the data-receiving unit 114 receives the multimedia data with the on-screen watermark and the digital watermark sent from the server 12. The digital watermark is generated and embedded in the multimedia data if the client is authenticated to have the access right to access the multimedia data. This client 11 may be used with the method as described in Embodiment 3, and the detailed operation is not repeated here.

[0060] With regard to functions of the components of the server 12, the authenticating unit 121 receives a login request from the client 11 and authenticates an access right of the client 11 to access the multimedia data. Concretely, the authenticating unit 121 confirms whether the client 11 is allowed to access or play the multimedia data. The code-generating unit 122 generates an identification code that is uniquely associated with the client 11 according to the login request if the client is authenticated to have the access right to access the multimedia data. Different clients 11 correspond to different identification codes. The superimposing unit 124 generates an on-screen watermark according to the identification code that is uniquely associated with the client 11 and superimposes the on-screen

watermark on images of the multimedia data. The data-sending unit 125 sends the watermarked multimedia data to the client 11. In addition to the on-screen watermark, a digital watermark may be optionally inserted in the multimedia data. Under this condition, the code-generating unit 122 generates the digital watermark associated with the client 11 if the client is authenticated to have the access right to access the multimedia data. The superimposing unit 124 embeds the digital watermark in the multimedia data, and the data-sending unit 125 sends the multimedia data with the on-screen watermark and the digital watermark to the client 11. This server 12 may be used with the method as described in Embodiment 4, and the detailed operation is not repeated here. In addition, the client 11 and the server 12 of FIGs. 10A and 10B may be cooperated with each other to perform the method as described in Embodiment 6.

[0061] The watermark superimposed on or embedded in the multimedia data according to the above-described methods will be detected if infringement occurs. Please refer to FIG. 11, a schematic block diagram illustrating a structure of a watermark-detecting system. It is to be noted that only a relative portion of the system is shown in the schematic block diagram, but it is not intended to limit the real structure thereof. The watermark-detecting system 9 may be integrated to the server 12 of the watermarking system 1 or separately provided. The watermark-detecting system 9 includes a retrieving unit 91, an analyzing unit 92, and a look-up unit 93. The retrieving unit 91 retrieves the on-screen watermark from the multimedia data to be inspected. The analyzing unit 92 analyzes the on-screen watermark to obtain the identification code. The watermark superimposed on or embedded in the multimedia data is generated according to the identification code which corresponds to one client 11. There is an identification database stored in the server 12. The identification database records information of every client 11 and corresponding identification code of the every client 11.

The identification database may be also set up in the look-up unit 73 and updated with the server 12. The look-up unit 93 looks the identification code up in the identification database to find out the corresponding client information. This watermark-detecting system 9 may be used with the method as described in Embodiment 7, and the detailed operation is not repeated here.

[0062] It is to be noted in the above-described embodiments, all units, elements and devices are described and denominated based on their functionality. Other units, elements or devices capable of performing at least one of the steps described above are included in the modifications of the embodiments and encompassed in the invention. In addition, the steps of the methods according to the present invention can be implemented by hardware or software. The scope of the present invention is not limited thereto.

[0063] For those having ordinary skill in the art, it is understood that all or part of the steps in the various embodiments described above can be executed by a program instructing relevant hardware or implemented by one or more sequences of computer-executable instructions. The corresponding program or instructions for causing one or more processing units to perform the methods may be stored in a computer-readable medium. The so-called medium can be, for example, a ROM / RAM, disk or optical disk, etc.

[0064] While the invention has been described in terms of what is presently considered to be the most practical and preferred embodiments, it is to be understood that the invention needs not be limited to the disclosed embodiment. On the contrary, it is intended to cover various modifications and similar arrangements included within the spirit and scope of the appended claims which are to be accorded with the broadest interpretation so as to encompass all such modifications and similar structures.

WHAT IS CLAIMED IS:

1. A watermarking method adapted to be used with a client for watermarking multimedia data, the watermarking method comprising:

 sending a login request to a server which authenticates an access right of the client to access the multimedia data and generates an identification code uniquely associated with the client according to the login request;

 receiving the identification code from the server;

 generating an on-screen watermark according to the identification code uniquely associated with the client; and

 adding the on-screen watermark onto the multimedia data.

2. The watermarking method according to claim 1, further comprising:

 receiving a digital watermark from the server which generates the digital watermark associated with the client according to the login request if the client is authenticated to have the access right to access the multimedia data; and

 embedding the digital watermark in the multimedia data.

3. The watermarking method according to claim 2, wherein the digital watermark corresponding to each client is unique.

4. The watermarking method according to claim 2, wherein the digital watermark is an invisible digital watermark.

5. The watermarking method according to claim 1, wherein the on-screen watermark is added onto the multimedia data by superimposing the on-screen watermark on images of the multimedia data.

6. A watermarking method adapted to be used with a server for

watermarking multimedia data, the watermarking method comprising:

receiving a login request from a client;

authenticating an access right of the client to access the multimedia data in response to the login request;

generating an identification code uniquely associated with the client according to the login request if the client is authenticated to have the access right to access the multimedia data; and

sending the identification code to the client which generates an on-screen watermark according to the identification code uniquely associated with the client and adds the on-screen watermark onto the multimedia data.

7. The watermarking method according to claim 6, further comprising:

generating a digital watermark associated with the client according to the login request if the client is authenticated to have the access right to access the multimedia data; and

sending the digital watermark to the client which embeds the digital watermark in the multimedia data.

8. The watermarking method according to claim 6, further comprising:

recording the identification code in an identification database that stores a plurality of identification codes and associated client information.

9. A watermarking method adapted to be used with a client for watermarking multimedia data, the watermarking method comprising:

sending a login request to a server which authenticates an access right of the client to access the multimedia data, generates an identification code uniquely associated with the client according to the login request, adds an on-screen watermark onto the multimedia data according to the identification code uniquely associated with the client, and sends the

multimedia data with the on-screen watermark to the client; and

receiving the multimedia data with the on-screen watermark from the server.

10. The watermarking method according to claim 9, wherein the received multimedia data comprise a digital watermark associated with the client according to the login request, the digital watermark being generated and embedded in the multimedia data if the client is authenticated to have the access right to access the multimedia data.

11. A watermarking method adapted to be used with a server for watermarking multimedia data, the watermarking method comprising:

receiving a login request from a client;

authenticating an access right of the client to access the multimedia data in response to the login request;

generating an identification code uniquely associated with the client according to the login request if the client is authenticated to have the access right to access the multimedia data;

generating an on-screen watermark according to the identification code uniquely associated with the client;

adding the on-screen watermark onto the multimedia data; and

sending the multimedia data with the on-screen watermark to the client.

12. The watermarking method according to claim 11, wherein the multimedia data sent to the client comprise a digital watermark, and the watermarking method further comprises:

generating a digital watermark associated with the client according to the login request if the client is authenticated to have the access right to access the multimedia data; and

embedding the digital watermark in the multimedia data.

13. The watermarking method according to claim 11, wherein the on-screen watermark is added onto the multimedia data by superimposing the on-screen watermark on images of the multimedia data.

14. The watermarking method according to claim 11, further comprising:

recording the identification code in an identification database that stores a plurality of identification codes and associated client information.

15. A watermark-detecting method adapted to be used with a watermark-detecting system for detecting a watermark added onto multimedia data, the watermark-detecting method comprising:

retrieving the watermark from the multimedia data;

analyzing the watermark to obtain an identification code, wherein the watermark is generated according to the identification code and the identification code corresponds to one client; and

looking the identification code up in an identification database to find out corresponding client information, the identification database storing a plurality of identification codes and associated client information.

16. A client of a watermarking system for watermarking multimedia data, the client comprising:

a login-requesting unit for sending a login request to a server of the watermarking system which authenticates an access right of the client to access the multimedia data and generates an identification code uniquely associated with the client according to the login request;

a code-receiving unit for receiving the identification code from the server; and

a superimposing unit for generating an on-screen watermark

according to the identification code uniquely associated with the client and superimposing the on-screen watermark on images of the multimedia data.

17. The client according to claim 16, wherein the code-receiving unit receives a digital watermark from the server which generates the digital watermark associated with the client according to the login request if the client is authenticated to have the access right to access the multimedia data, and the superimposing unit embeds the digital watermark in the multimedia data.

18. A server of a watermarking system for watermarking multimedia data, the server comprising:

an authenticating unit for receiving a login request from a client of the watermarking system and authenticating an access right of the client to access the multimedia data in response to the login request;

a code-generating unit for generating an identification code uniquely associated with the client according to the login request if the client is authenticated to have the access right to access the multimedia data; and

a code-sending unit for sending the identification code to the client which generates an on-screen watermark according to the identification code uniquely associated with the client and adding the on-screen watermark onto the multimedia data.

19. The server according to claim 18, wherein the code-generating unit generates a digital watermark associated with the client according to the login request if the client is authenticated to have the access right to access the multimedia data, and the code-sending unit sends the digital watermark to the client which embeds the digital watermark in the multimedia data.

20. A client of a watermarking system for watermarking multimedia data,

the client comprising:

a login-requesting unit for sending a login request to a server of the watermarking system which authenticates an access right of the client to access the multimedia data, generates an identification code uniquely associated with the client according to the login request, adds an on-screen watermark onto the multimedia data according to the identification code uniquely associated with the client, and sends the multimedia data with the on-screen watermark to the client; and

a data-receiving unit for receiving the multimedia data with the on-screen watermark from the server.

21. The client according to claim 20, wherein the multimedia data received by the data-receiving unit comprise a digital watermark associated with the client according to the login request, the digital watermark being generated and embedded in the multimedia data if the client is authenticated to have the access right to access the multimedia data.

22. A server of a watermarking system for watermarking multimedia data, the server comprising:

an authenticating unit for receiving a login request from a client of the watermarking system and authenticating an access right of the client to access the multimedia data;

a code-generating unit for generating an identification code uniquely associated with the client according to the login request if the client is authenticated to have the access right to access the multimedia data;

a superimposing unit for generating an on-screen watermark according to the identification code uniquely associated with the client and superimposing the on-screen watermark on images of the multimedia data; and

a data-sending unit for sending the multimedia data with the on-screen watermark to the client.

23. The server according to claim 22, wherein the code-generating unit generates a digital watermark associated with the client according to the login request if the client is authenticated to have the access right to access the multimedia data, and the superimposing unit embeds the digital watermark in the multimedia data.

24. A watermark-detecting system for detecting a watermark added onto multimedia data, comprising:

a retrieving unit for retrieving the watermark from the multimedia data;

an analyzing unit for analyzing the watermark to obtain an identification code, wherein the watermark is generated according to the identification code and the identification code corresponds to one client; and

a look-up unit for looking the identification code up in an identification database to find out corresponding client information, the identification database storing a plurality of identification codes and associated client information.

25. A computer-readable medium carrying one or more sequences of computer-executable instructions for causing one or more processing units to perform the method according to any one of claims 1-15.