Screen Watermark Creation and Decipher System and Process

Field of Invention

[001] The present invention relates to a system and a process for creating a screen watermark and an associated watermark decipher process. Generally, creation of a screen watermark is to deter a third party from capturing information, with a camera or video camera, on a screen display, which may include presentation data, game, or a video, and sharing the captured information.

Background

[002] With pervasive uses of computers and internet, distribution of digital content will require some forms of proprietary protection or deterrence from copying. For example, copyright warnings are not effective enough to stop illegal sharing of proprietary information; digital watermarking is possibly an additional approach to stop or deter such illegal or restricted sharing.

[003] US Patent 9,454,790, issued to Fasoo.com, describes a method for displaying a screen watermark. Screen watermark display policy is received from an administrator terminal and the display policy is tailored for each user. A watermark display determining unit is configured to determine whether a watermark is displayed on a screen; when no important or confidential content is displayed on the screen, the watermark disappears from the screen.

[004] In another approach, US Patent 9,367,885, issued to Tencent Technology, describes a method for adding or detecting a watermark. A client registers at a server of a rights owner to request rights to access multimedia data, and, in response, is given a unique identification code. A screen watermark is generated according to the client's unique identification code. In a reverse process, a watermark detects a watermark embedded in a multimedia data and then analyses the unique identification code by looking up in the identification database to identify a client, who may be a source of the watermark violation.

[005] When digital contents are not embedded with watermarks, such digital contents can still be copied by capturing a screen displaying restricted digital contents with a camera or

video camera. Capturing of digital contents on a screen with a camera/video camera is made possible because the camera/video camera is often equipped with high resolutions, and even a faint watermark can be captured by the camera/video camera. Despite the above approaches, it can thus be seen that there exists a need to provide another method to generate a screen watermark to deter copying of restricted digital contents via screen captures. Preferably, the watermark is of a low transparency or contrast and does not visually obstruct a screen display. A reverse process of deciphering an identity of a user sharing or distributing such restricted digital contents is also desired.

Summary

[006] The following presents a simplified summary to provide a basic understanding of the present invention. This summary is not an extensive overview of the present invention, and is not intended to identify key features of the invention. Rather, it is to present some of the inventive concepts of this invention in a generalised form as a prelude to the detailed description that is to follow.

[007] The present invention seeks to provide a system and a process for creating a screen watermark and an associated watermark decipher process.

[008] In one embodiment, the present invention provides a screen watermark system comprising: a server hosting a watermark agent code, and a graphic algorithm; and a user communication device that is configured to access the server, which host proprietary information and the watermark agent code and graphic algorithm are provided to create a screen watermark on a display screen of the user communication device. Preferably, the server is configured for access to a web or a cloud system associated with a host having rights to the screen watermark system.

[009] Preferably, the screen watermark comprises a cipher code pattern. Preferably, a user identity, a user communication device identity, and a user device location are encrypted into a pattern, an arrangement or an orientation of a line or lines forming the cipher code pattern.

[0010] Preferably, the screen watermark further comprises an encrypted cipher string. Preferably, a user identity, a user device identity and a user device location are encrypted into the cipher string. The cipher code pattern may comprise a predetermined number of

matrix cells, and the cipher string with a predetermined length may be inserted into the matrix cells of the cipher code pattern.

[0011] Preferably, the watermark agent code is operable to capture a display screen setting or a screen zoom parameter, so that the graphic algorithm is operable to position the screen watermark, one or two screen watermarks or more in an array, on the display screen according to a predetermined location, size, orientation or rotation, transparency, or contrast level with respect to a background of the display screen.

[0012] Preferably, when a screen capture containing a screen watermark is discovered, the graphic algorithm is operable in reverse to retrieve the cipher code pattern, the cipher string or the combination of the cipher code pattern and cipher string, and decodes the captured screen watermark to reveal an identity of the user, and an identity and location of the user communication device.

[0013] In other embodiments, the present invention includes a data processing device or a computer readable storage media comprising a watermark agent code and a graphic algorithm for generating the above screen watermark.

[0014] In another embodiment, the present invention provides a method for creating a screen watermark comprises: downloading a watermark agent code and a graphic algorithm into a user communication device; the watermark agent code extracting a user communication device identity, a user device location, a user identity and an associated screen display setting or zoom parameter, and creating a screen watermark comprising a cipher code pattern. Alternatively, this method creates a screen watermark comprising into a cipher string of a predetermined length, or a combination of a cipher code pattern and a cipher string.

[0015] Preferably, the method further comprises executing the graphic algorithm to position the screen watermark according to the screen display setting or zoom parameters; and reducing transparency and contrast of the screen watermark with respect to a background of the screen display, so that the screen watermark remains visible and without visually interfering with information presented on the screen display.

[0016] In yet another embodiment, the present invention provides a method for deciphering the above screen watermark comprises: sending a captured screen containing a screen

watermark to an administrative station of a rights owner; operating the graphic algorithm to restore contrasts of the screen watermark; decoding the encryption algorithm to extract the cipher code pattern and/or the cipher string constituting the screen watermark to reveal the use identity, the user device identity and the user device location; and determining whether the user identified has violated restricted permissions of the rights owner.

Brief Description of the Drawings

[0017] This invention will be described by way of non-limiting embodiments of the present invention, with reference to the accompanying drawings, in which:

[0018] FIG. 1 illustrates a system in which a user device is configured for creating a screen watermark according to an embodiment of the present invention;

[0019] FIG. 2 illustrates a screen watermark according to another embodiment;

[0020] FIG. 3 illustrates a process for starting a screen watermark agent code in the user device according to another embodiment of the present invention;

[0021] FIG. 4 illustrates the above screen watermark creation process in the user device;

[0022] FIG. 5 illustrates a display showing position, layout, transparency and contrast level of the above screen watermark on a screen with a white or a dark background; and

[0023] FIG. 6 illustrates a reverse process of deciphering the above screen watermark to reveal a source of screen watermark violation.

Detailed Description

[0024] One or more specific and alternative embodiments of the present invention will now be described with reference to the attached drawings. It shall be apparent to one skilled in the art, however, that this invention may be practised without such specific details. Some of the details may not be described at length so as not to obscure the present invention. For ease

of reference, common reference numerals or series of numerals will be used throughout the figures when referring to the same or similar features common to the figures.

[0025] FIG. 1 shows a data communication system **100** in which a user device **150** equipped with a display screen **151** is configured to display a screen watermark **130**. The data communication system **100** may include a computer, a data processing, a metauniverse simulator, a virtual reality system, digital gaming, or similar electronic implementations. As shown in FIG. 1, the data communication system **100** includes a rights owner hosting an application through a server **110** which the user device **150** is linked directly thereto; in another embodiment, the server **110** is configured as a web server **110**, which is connected to a cloud or internet system **120**; in the following description, the server or the web server **110** is now referred to generally as a server **110**. The user using the device **150** may find the application interesting, and clicks to access the server **110** belonging to the rights owner. The server **110** stores at least a watermark agent code **112** and a graphic algorithm **116**. In one embodiment, once the user permits installation of the watermark agent code **112** into the user device **150**, a watermark **130** is installed and appears onto the screen **151** of the user device **150**; in an alternative embodiment, by accessing the server **110**, implied permission is given to install the watermark agent code **112** into the user device **150**.

[0026] In one embodiment, the system **100** encrypts the watermark **130** according to an encryption algorithm **114** (such as, an Advanced Encryption System, AES); preferably, an encryption performed by the encryption algorithm **114** is reversible, so that an administrator performing a reverse encryption can identify the user device **150** and user identity, as will be described with FIG. 6. It is possible that the rights owner may provide a database, a photograph, a video, a digital game, a simulation or any presentation, instead of an application, which contains proprietary or restricted information, and the user is notified of restricted permissions from distributing or sharing such proprietary information. In yet another alternative embodiment, the user may access the server **110** or the database/video/game directly or indirectly through another web application.

[0027] In FIG. 1, the screen display **151** shows the watermark **130** is made up of a cipher code pattern **135** containing a cipher string xxxxxx according to an embodiment of the watermark **130**. In another embodiment, a watermark **130a** is shown in FIG. 2, to comprise of a cipher code pattern **135a** without a cipher string; the cipher code pattern **135a** is uniquely

identified by the patterns, arrangements, orientation, and so on, of a line or lines forming the cipher code pattern **135a**. A process **300** for generating the watermark **130**,**130a** will be described below with reference to FIG. 4.

[0028] FIG. 3 shows a process **200** for initiating the screen watermark **130**,**130a** on the user device **150**,**150a**. After finding an interesting web application, database, photograph, video, game, simulator or presentation, the user clicks, in step 210, on a link to the server **110**; a window pops up and notifies the user, in step 220, of permission required for accessing restricted or proprietary information located in the server **110**. The notice gives the user a choice whether to proceed with connection to the server **110**, in decision step 230; if the user chooses not to continue accessing the server, the process reverts back to step 220 and, preferably, after the user declines, iterates a confirmation loop before ending the process **200**; if the user chooses to continue accessing the server **110**, and consents to downloading the screen watermark agent code **112**, in step 240. Depending on the encryption algorithm of the watermark **130**,**130a**, the encryption algorithm **114** and a graphic algorithm **116** are downloaded into the user device **150**,**150a** together with the watermark agent code **112**, and the process **200** proceeds to the process **300** for generating the screen watermark **130**,**130a**.

[0029] In the event that the user device **150**,**150a** has been used to access the server **110** at an earlier time, at least, the watermark agent code **112** and the graphic algorithm **116** are already resident in the user device **150**,**150a**, and the process **200** proceeds directly to the process **300** for generating the screen watermark **130**,**130a**.

[0030] FIG. 4 shows the process **300** for generating the above screen watermark **130**,**130a**. Once the watermark agent code **112** is downloaded into the user device **150**,**150a**, together, where necessary, with the encryption algorithm **114**, the watermark agent code **112** retrieves, in step 310, the user identity and the user device identity; the user identity may include the user's login name; the user device identity may include the user's device name, MAC address, IP address, and so on; the user identity and the user device identity are useful for tracing and locating the user, in the event of unauthorized sharing of information from the user device **150**,**150a**. Following this, in step 320, the watermark agent code **112** and the encryption algorithm **114**,**114a** encrypts or encodes the user identity and the user device identity to generate a unique cipher string **xxxxxx**; preferably, the unique cipher string

xxxxxx is alphanumeric; also preferably, the unique cipher string **xxxxxx** comprises between 6 and 12 characters, or more.

[0031] The process **300** continues further, and in step 330, the watermark agent code **112** generates the above unique cipher code pattern **135**,**135a**. In one embodiment, the cipher code pattern **135** is arranged in a matrix format; preferably, the cipher code pattern **135** comprises 3 rows and 3 columns, and cells of the cipher code pattern **135** store the cipher string **xxxxxx** in a consecutive order. When the cipher string **xxxxxx** is shorter than the number of cells in the cipher code pattern, the trailing cells of the cipher code pattern **135** do not store any alphanumeric character. It is also possible that the cipher code pattern **135** comprises more than 3 rows or 3 columns. In the embodiment where the cipher string xxxxxx is not encoded with the user identity and the user device identity, the cipher code pattern **135a** is uniquely encrypted or encoded with the user identity and the user device identity.

[0032] In one embodiment of the watermark agent code **112**, an administrator of the watermark agent has access to the watermark agent code **112** in the server **110** to configure a predetermined length of the cipher string xxxxxx and/or the cipher code pattern **135** or to configure the cipher code pattern **135a** according to a need or for a customer. Following step 330, the process **300** executes the graphic algorithm **116**. The graphic algorithm **116** extracts the screen background brightness, colour, display size, zoom size, for example, by reading from the screen display settings or parameters, and in response, dynamically adjusts transparency, contrast and size of the cipher code pattern **135**,**135a** suitable for the screen **151**; for example, the graphic algorithm **116** reduces transparency and contrast of both the cipher code pattern **135**,**135a** and the cipher string **xxxxxx**, so that the cipher code pattern **135**,**135a** and the cipher string **xxxxxx** remain visible and is shown in the background of the screen **151** without visually interfering with information presented on the screen **151**. In addition, the watermark agent code **112** allows an administrator to customise the watermark **130**,**130a** on the screen **151** according to a position, size, layout or in an array, orientation or rotation, and so on, in relation to the screen size or zoom parameter. When a camera or video camera is used to capture the screen **151**, resolution of the camera is high enough to capture the lowly transparent or contrasted screen watermark **130**,**130a**; the captured watermark **130b** can be deciphered to extract or reveal the user's identity, in a reverse deciphering process **400**, for forensic purposes.

[0033] In the above description, both the user identity and the user device identity determine the cipher string xxxxxx; in the alternative embodiment of the process **300**, both the user identity and the user device identity are used to generate the cipher code pattern **135a**. In these ways, the cipher code pattern **135**,**135a** and the cipher string xxxxxx can either, both or in combination be used to identify the user and the user device **150**,**150a** in the reverse deciphering process **400**.

[0034] In one embodiment, a sub-routine **113**, residing in the watermark agent code **112**, captures the user device identity, current date and time, screen display size and settings, network connection, and so on; the user device information thus captured allows the administrator to configure the position, size, layout or array, orientation/rotation, transparency, contrast level, and so on, of the watermark **130**,**130a** with respect to background of the screen display. FIG. 5 shows a display of the user device **150**,**150a** shown examples of the positioning, sizing, transparency and contrast of the screen watermark **130**,**130a**; as shown in FIG. 5, half of the display on the left-hand side illustrates a screen **151** with a white background and an array of cipher strings xxxxxx arranged in a matrix format as described above, whilst half of the display on the right-hand side illustrates a screen **151** with a dark background and an array of cipher strings xxxxxx.

[0035] By knowing the network connection, it is also possible that the administrator can determine the location of the user device **150**,**150a**, whether the user is in the office, at home or at a public location. Information on location of the user and user device **150**,**150a** from the network connection may be useful for forensic purposes.

[0036] FIG. 6 shows the reverse deciphering process **400**. As shown in FIG. 6, step 410 involves discovering the captured screen watermark **130b**. At an administrative station of the rights owner, the captured screen watermark **130b** is scanned into a computing device in which the graphic algorithm **116** is executed to restore contrast of the screen watermark **130b**; the restored screen watermark is then deciphered by decoding the encryption algorithm **114** to extract the cipher code pattern **135** and the cipher string **xxxxxx**. Results of deciphering the cipher code pattern **135**,**135a** and/or the cipher string **xxxxxx** would reveal the user identity and the user device **150**,**150a**. With the use identity and/or user device identity being identified, follow on actions can then be conducted if the owner's rights are exploited.

[0037] In the above description, the watermark agent code **112** and the graphic algorithm **116** and associated subroutines are software codes that can be stored or distributed in storage media; these software codes can be installed, for example as drivers, into the operating system of the user device **150**,**150a**; in this way, these software codes can then be un-installed by the user. In another embodiment, these software codes are configured to reside as firmware in electronic chips, such as, field-programmable gate arrays (FPGA); a user device **150**,**150a** with such an electronic chip and associated firmware will inherently generate the above screen watermark functionality built there into.

[0038] While specific embodiments have been described and illustrated, it is understood that many changes, modifications, variations and combinations of variations disclosed in the text description and drawings thereof could be made to the present invention without departing from the scope of the present invention. For example, the above watermark system **100** is compatible with window-based communication devices, such as, computers, Macintosh machines, servers, tablets, ebook readers, smart phones, and so on, that are supported by various operating systems. In addition, drivers of the screen **151** are electronically linked to output drivers in the user device **150**,**150a**, and the screen watermarks **130**,**130a** appear in printouts and or file prints from the user device **150**,**150a**.

CLAIMS:

1. A screen watermark system comprising:

a server hosting a watermark agent code, and a graphic algorithm; and

a user communication device that is configured to access the server, wherein host proprietary information and the watermark agent code and the graphic algorithm are provided in the server to create a screen watermark on a display screen of the user communication device.

2. The system according to claim 1, wherein the server is configured for access to a web or cloud system associated with a host having rights to the screen watermark system.

3. The system according to claim 1 or 2, wherein the screen watermark comprises a cipher code pattern.

4. The system according to claim 3, wherein the cipher code pattern further comprises a predetermined number of matrix cells.

5. The system according to claim 4, wherein the screen watermark further comprises an encrypted cipher string, wherein the encrypted cipher string is insertable into the cipher code pattern.

6. The system according to claim 4, wherein a user identity, a user device identity and a user device location are encrypted into the cipher string.

7. The system according to claim 3, wherein a user identity, a user communication device identity, and a user device location are encrypted into a pattern, an arrangement or an orientation of a line or lines forming the cipher code pattern.

8. The system according to any one of the preceding claims, wherein the watermark agent code is operable to capture a display screen setting or a screen zoom parameter, so that the graphic algorithm is operable to position the screen watermark, one or two screen watermarks or more in an array, on the display screen according to a predetermined location, size, orientation or rotation, transparency, or contrast level with respect to a background of the display screen.

9. The system according to any one of the preceding claims, wherein, when a screen capture containing a screen watermark is discovered, the graphic algorithm is operable in reverse to retrieve the cipher code pattern, the cipher string or the combination of the cipher code pattern and the cipher string, and decodes the captured screen watermark to reveal an identity of the user, and an identity and location of the user communication device.

10. A data processing device comprising a watermark agent code and a graphic algorithm for generating a screen watermark, wherein the screen watermark comprises a cipher code pattern and/or a cipher string, wherein the cipher code pattern and the cipher string are encrypted with a user identity, a user device identity and a user device location.

11. A computer readable storage media comprising a watermark agent code and a graphic algorithm for generating a screen watermark, wherein the screen watermark comprises a cipher code pattern and/or a cipher string, wherein the cipher code pattern and the cipher string are encrypted with a user identity, a user device identity and a user device location.

12. A method of creating a screen watermark comprising:

downloading a watermark agent code and a graphic algorithm into a user communication device; and

the watermark agent code extracting a user communication device identity, a user device location, a user identity and an associated screen display setting or zoom parameter, and creating a screen watermark comprising a cipher code pattern.

13. The method according to claim 12, wherein the watermark agent code further comprises encrypting the user communication device identity, the user device location, the user identity and an associated screen display setting or zoom parameter, and creating a screen watermark comprising into a cipher string of a predetermined length.

14. The method according to claim 13, wherein creating the screen watermark further comprises inserting or merging the cipher string into the cipher code pattern.

15. The method according to any one of claims 12-14, further comprises executing the graphic algorithm to position the screen watermark according to the screen display setting or zoom parameter; and

reducing transparency and contrast of the screen watermark with respect to a background of the screen display, so that the screen watermark remains visible and without visually interfering with information presented on the screen display.

16. The method according to any one of claims 13-15, further comprises encrypting the cipher string or the cipher code pattern with an encryption algorithm.

17. The method according to claim 15 or 16, wherein an administrator accesses the watermark agent code at an administrative station to customise a position, size, layout, or orientation/rotation of the screen watermark in relation to the screen display setting or screen zoom parameter.

18. A method of deciphering the screen watermark recited in claims 12-17, comprises:

sending a captured screen containing a screen watermark to an administrative station of a rights owner;

operating the graphic algorithm to restore contrast of the screen watermark;

decoding the encryption algorithm to extract the cipher code pattern and/or the cipher string constituting the screen watermark to reveal the use identity, the user device identity and the user device location; and

determining whether the user identified has violated restricted permissions of the rights owner.