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, wherein host proprietary information and the watermark agent code and graphic algorithm are provided in the server to create a screen watermark in a cipher code pattern on a display screen of the user communication device; wherein the cipher code pattern comprises a predetermined number of matrix cells or a pattern /arrangement formed by a line or lines. 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, a user identity, a user communication device identity, and a user device location are encrypted into 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 which is inserted into the predetermined number of the matrix cells of the

cipher code pattern. Preferably, the pattern or arrangement formed by the line or lines has a predetermined orientation.

[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, 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, which is made up of a predetermined number of matrix cells or a pattern /arrangement formed by a line or lines.

[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, which is made up of a predetermined number of matrix cells or a pattern /arrangement formed by a line or lines. 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 a user identity, a user device identity and a 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