

A SYSTEM FOR PROVIDING AN UNOBTRUSIVE WATERMARK IN A SECURE DOCUMENT

Field of Invention

The invention relates generally to secure document authentication and protection. In particular, the invention relates to authentication and protection of a secure document using a watermark.

Background

Since the early 90s, watermarking techniques that can create, embed, and/or reveal watermarks such as signatures, identifying marks or other images have been used for document protection and authentication. A document can exist either as an electronic copy or in digital form, such as an image and/or text file, or on a physical medium or in physical form such as a printed hardcopy.

In general, there are two kinds of watermarks: visible and invisible watermarks. Visible watermarking is typically applied to documents such as those found in the public domain so that the visible appearance of the visible watermarks present or issue a warning to the public that visibly watermarked documents are authentic documents and alteration and/or forgery of these documents is prohibited. However, visible watermarking techniques involve minimal consideration for the security of visible watermarks when such are applied on or embedded in documents. As a result, visible watermarks can be easily attacked by being altered or removed from documents. Furthermore, visible watermarks may be deemed as obtrusive to viewers of visibly watermarked documents because in the process of imbuing documents with the visual effects of the visible watermarks, visible watermarking techniques sometimes unavoidably change or alter the original appearance or content of these documents.

Unlike visible watermarks, invisible watermarks when applied on documents must firstly be revealed or extracted and then checked for consistency in order for the

authenticity of invisibly watermarked documents to be determined. During such checks or inspection, revealed watermarks are compared with originally embedded watermarks. For example, if an invisibly watermarked document is processed to reveal a watermark and such a watermark is inconsistent with a watermark originally embedded in an original document, the authenticity of the invisibly watermarked document is questionable.

Invisible watermarks are also not obtrusive to viewers of invisibly watermarked documents, as little or no change or alteration to the original appearance or content of such documents is introduced. However, in applying invisible watermarks on documents for authentication purposes, a number of issues need to be addressed for practicality and feasibility purposes and cost considerations.

One issue that needs to be addressed relates to the difficulty in balancing between the robustness of invisible watermarks that is embedded in documents, and the sensitivity of invisible watermark extraction processes. This means there has to be a compromise or trade-off between the propensity of invisible watermarks to remain unchanged or unaltered under normal processing or handling, and the ability of the same invisible watermarks to allow the detection of forgery, respectively.

Another issue that needs to be addressed relates to the security of the invisible watermarks embedded in documents. It is desirable that invisible watermarks are non-invertible so that invisible watermarks are secured and the probability of inadvertent attacks on the invisible watermarks succeeding is minimized. Currently to this end, other security protocols have to be employed and special or extra tools, for example software applications or tools, are typically required for the extraction of the invisible watermarks.

Several techniques for anti-alteration/forgery or authentication of documents have been proposed. One such technique proposes applying a transparent visible watermark on a document for providing a warning message to the public accessing the document. The visible watermark is embedded in the document in such a way that the content of the document remains viewable and because of the presence of the visible watermark, unauthorized use of the image is discouraged. There is, however,

no security mechanism built into the process for the visible watermarking of the document, and thus authentication can only be carried by visual inspection and forgery is not prevented.

Another technique proposes the generation of a watermark in a digitally reproducible document. Although the authentication of such a watermark can be done either in the digital domain or in the physical domain, there still remain several problems. One problem relates to the security of the watermark because where there exist hints as to how the watermarking technique works, the watermark may be easily forged and the forger may therefore claim that the forged watermark comes from the original owner. The other problem relates to the inflexible extraction of the watermark generated by such a watermarking technique. If the watermark extraction is done in the physical domain, a special scheme has to be adopted, for example, involving scanning and/or extracting. Or, the viewer may find the appearance of the watermark obtrusive because the watermark is actually an array of noise. Another similar technique proposes verifying the originality of a document to be authenticated by hashing the highest significant bit of the image pixels in the document and putting the hashed results back in the least significant bit of the image pixels. This watermarking technique works for documents in the digital domain but does not work as well in the physical domain because the printing and/or re-scanning of the image can cause noise to be introduced to the document.

Another yet technique proposes protecting secure documents by means of special physical or chemical processes. A typical way to do so is to increase the difficulty for attackers in re-creating or reproducing the processes of making the original document. Other similar watermarking techniques propose incorporating anti-copy elements in the process of forming the documents, for example, based on multi-layer printing or printing indicia so that the formed documents cannot be photocopied. However, such watermarking techniques require complicated processes, and sometimes require special equipment, which undesirably lead to high costs.

Several further techniques propose the protection of original documents from photocopying by adopting color, gradient, or line screen modulation. After photocopying such documents, messages such as "void", "not valid" appear on the

copies. However, these watermarking techniques merely prevent copying and do not allow verification that the original document comes from the supposed owner. This is because a forgery of a document with such messages can be easily made.

Other even further techniques propose embedding microdots into original documents that are detectable by photocopy machines to prevent illegal photocopying of the original documents. Once these photocopying machines detect the microdots, the photocopy machines are automatically stopped from photocopying the original documents. However, such technology requires that all photocopy machines to be installed with a component for detecting the microdots, which again may lead to undesirable high costs.

Therefore, there is an apparent need for a solution for protecting and authenticating documents that ameliorates the inadequacy of at least one foregoing proposal.

Summary

A system, method and computer product for providing authentication and protection of a document embedded with an unobtrusive and secure watermark is provided.

In accordance with a first aspect of the invention, a method of providing an unobtrusive watermark for securing a document is provided. The method includes the steps of generating at least one visual key, wherein the generation of the at least one visual key depends on the watermark, and embedding unobtrusively one of the at least one visual key in the document by modulating the values of pixels of said document, wherein the modulation of said values is dependent on said at least one visual key.

In accordance with a second aspect of the invention, a system for providing an unobtrusive watermark for securing a document is provided. The system includes means for generating at least one visual key, wherein the generation of the at least one visual key depends on the watermark, and means for embedding unobtrusively one of the at least one visual key in the document, including means for modulating the values of pixels of said document, wherein the modulation of said values is dependent on said at least one visual key.

30

Brief Description of the Drawings

Embodiments of the invention is described hereinafter with reference to the drawings, in which:

Figure 1 is a block diagram for illustrating a scenario involving a user and an authenticator in which a watermarking technique is applied to a document resulting in an unobtrusive and secure watermark being embedded in a secure document for authentication and protection purposes in accordance with an embodiment of the invention;

Figure 2 is a block diagram for illustrating a process for embedding a visual watermark in the document of Figure 1;

Figure 3 is a block diagram for illustrating the details of forming the secure document of Figure 1;

Figure 4 is a block diagram for illustrating processes for verifying the secure document of Figure 1 in both digital and physical domains;

Figure 5 is a block diagram for illustrating the details of a process of forming visual keys for the embedding process in Figure 2;

Figure 6 is an example of an image for embedding in the document of Figure 1;

Figure 7 is an example of a first visual key derived from the process shown in Figure 5 on the image shown in Figure 6 that is embedded in the secure document of Figure 1;

Figure 8 is an example of a second visual key derived from the process shown in Figure 5 on the image shown in Figure 6 that the user of Figure 1 can hold;

Figure 9 is an example of a third visual key derived from the process shown in Figure 5 on the image shown in Figure 6 that the authenticator of Figure 1 can hold;

Figure 10 is an example of a generated watermark after modulation of the first visual key during the formation of the secure document as illustrated in Figure 3 in which the generated watermark is visually not obtrusive;

Figure 11 is an example of the interim result after directional filtering in the digital domain for verifying the image shown in Figure 6;

Figure 12 is an example of the interim result after photocopying in the physical domain for verifying the image shown in Figure 6;

Figure 13 is an example of the verification result after overlaying the interim result shown in Figure 12 with the second or third visual key in the physical domain, where the verification result is consistent with the image shown in Figure 6;

Figure 14 is an example of the verification result after overlaying the interim result shown in Figure 11 with the second or third visual key in the digital domain, where the verification result is consistent with the image shown in Figure 6; and

Figure 15 is an example of the verification result after overlaying any interim result with the second or third visual key, where the verification result is inconsistent with the image shown in Figure 6.

Detailed Description

It is apparent from the foregoing that the existing proposals for document protection and authentication in relation to the originality and integrity of secure documents have a number of identifiable inadequacies. One such inadequacy relates to the security of the protected document. Operatively, anyone can remove and add protective devices such as watermarks easily. That means such proposals cannot adequately address issues such as non-repudiation by owners of the secure documents and forgery of the secure documents by forgers, such omissions or acts being common attacks on the originality and integrity of the document.

Another such inadequacy relates to the visibility of the protective devices used such as watermarks. It is desirable that the watermarks embedded in the secure documents are non-obtrusive to viewers of the secure documents.

A further such inadequacy relates to the ease with which the secure document is checked or verified in relation to the protective devices. It is desirable the verification should be easily achieved through means that are commonly available.

A system for providing an unobtrusive watermark in a secure document is therefore provided as a response to ameliorating at least one of such inadequacies whereby the

purposes of protecting and authenticating the secure document is easily yet effectively achievable by cost effectively applying simple visual verification means.

Figure 1 illustrates in block diagram form a scenario in which a watermarking technique in accordance with a first embodiment of the invention is applied to a document resulting in an unobtrusive watermark being embedded in a secure document for protection and authentication purposes. A secure and trusted service center (generally known hereinafter as service center) 1 preferably provides the service for notarizing the secure document. In a typical case, an authorized user 2 communicates with a computer system, for example a server, at the service center 1 to request for the secure document that can be verified or authenticated by an authorized authenticator 3. To request for the secure document, the authorized user 2 sends a request for service 4 to the service center 1 by specifying, for example, a request logon, key information, and plain content of the document to be embedded with the watermark. Preferably, the authorized user 2 is provided with an option which if selected renders adaptive the visual information that is to be embedded into the formatted secure document for later verification by the authorized authenticator 3. Upon receiving the request for service 4, the service center 1 processes the same and sends the authorized user 2 a set of information 5. The set of information 5 contains the formatted secure document with the embedded watermark and (optionally) one of a number of visual keys created at the service center 2. This visual key is useful in case the authorized user 2 needs to prove the originality and integrity of the formatted secure document to others. Alternatively, the authorized user 2 can present an authorized document 6 (either electronic or print version of the formatted secure document) to the authorized authenticator 3 for verification. After receiving the authorized document 6, the authorized authenticator 3 sends an authorization request 7 to the service center 1. In response, the service center 1 sends the authorized authenticator 3 a visual key 8 that is distinct from the visual key the authorized user 2 may hold, if any. With the visual key 8 the authorized authenticator 3 can verify the originality and integrity of the authorized document 6.

Figure 2 illustrates a process for embedding the watermark, an example of which is shown in Figure 6, in the document 9 provided by the authorized user 2. The

document 9 to be protected is firstly pre-processed in region detection and selection process 10 for achieving a better visual effect when the formatted secure document is viewed. In the example shown in Figure 6 where the visual image 12 to be embedded in the document 9 is a logo, the visual image 12 is provided as input to a visual key generator module 14. Additional visual information may be embedded in the document 9 using the key information 13 by providing the same as input to the visual key generator module 14. The key information may include certification and/or notarization information provided by the service center 1, the name of authorized user 2 provided by the authorized user 2, and/or the digest of the content in the document 9 extracted from the document 9. All relevant visual information for protection and authentication purposes is thus provided to the visual key generator module 14. The visual key generator module 14 then processes all the visual information and generates a number of visual keys 15, 16, and 17, each of which is unique. The first visual key 15 is provided as input to a pixel modulation module 11 together with the document 9 which had been pre-processed in the region detection and selection process 10. To achieve a better unobtrusive visual effect when merging the visual information with the content of the document 9, the pixel modulation module 11 preferably includes a flexible modulation function where the specific modulation method carried out in the pixel modulation module 11 depends on the content of the document 9. The output of the pixel modulation module 11 is a formatted secure document 18 whose content is protected by the embedded visual information. The formatted secure document 18 is verifiable by the authorized user 2 or authorized authenticator 3 using any combination of the first visual key 15 with one of the second or third visual key 16 or 17. Examples of the first, second and third visual keys 15, 16 and 17 are shown in Figures 7, 8, and 9 respectively, all of which are derived from the processing of the watermark shown in Figure 6 by the visual key generator module 14. Examples of the combinations therefore include the first visual key 15 and the second visual key 16, and the first visual key 15 and the third visual key 17.

Figure 5 is a block diagram for illustrating the details of a process of forming visual keys for the embedding process in Figure 2. Such a process is carried out or caused

by the visual key generator module 14. The key information (K) 13 forms the additional visual information, which can be provided by service center 1 and/or the authorized user 2, and/or any feature extracted from the document 9, that is to be embedded into the formatted secure document together with the watermark. There are a number of ways to provide as input the key information 13 to the process and therefor embed the same in the formatted secure document. A first way is to embed the key information 13 into the Adaptive Visual Image (AVI), and therefore the Adaptive Visual Image AVI is an integration of the watermark and the key information 13. A second way is to embed the key information into the first visual key (VK_0) 15. The watermark or Visual Image (x', y') 34 is provided as input to the process and is the main image which is used for generating all the visual keys and can be revealed by overlapping or overlaying the first visual key 15 and any other visual key 16 or 17. Parameter n 35 is also provided as input to the process and represents the number of visual keys to be generated, where $n \geq 2$.

With the Visual Image (x', y') 34 as input, the process begins by generating the Adaptive Visual Image AVI to be embedded in the formatted secure document in a module 36. This is an optional module as there are a number of ways to embed the key information K 13. To integrate the key information K 13 into the Adaptive Visual Image AVI , direct methods such as displaying the key information K 13 value in the Visual Image VI or non-direct ways such as putting the hash value of the key information K 13 into the Visual Image VI can be used.

After generating the Adaptive Visual Image AVI , the process takes the parameter n 35 input and finds two $n \times m^2$ matrices W and B over the general field $GF(2)$ in a module 37. The W and B matrices must be qualified in order to be used for generating the visual keys. Let W and B be denoted by:

$$W = \begin{pmatrix} w_0 \\ \cdot \\ \cdot \\ \cdot \\ w_{n-1} \end{pmatrix} \quad B = \begin{pmatrix} b_0 \\ \cdot \\ \cdot \\ \cdot \\ b_{n-1} \end{pmatrix}$$

where $w_0, \dots, w_{n-1}, b_0, \dots, b_{n-1}$ are all m^2 -tuples in a relational database by which W and B are preferably manipulated and computed, and $n < m^2$. Also, let Ω and Ψ be two collections of $n \times m^2$ matrices obtained by randomly column permuting W and B , respectively. To be qualified for producing the visual keys, W and B are to satisfy several conditions.

A first such condition relates to the security of the embedded watermark, where for any $1 \leq p \leq n - 1$ condition, two collections of $p \times m^2$ matrices Ω' and Ψ' obtained by restricting each $n \times m^2$ matrix in the two collections of Ω and Ψ to rows $i_1, \dots, i_p$ are indistinguishable to the extent that the Ω' and Ψ' collections contain the same matrices with the same frequencies.

A second such condition relates to the verifiability of the embedded watermark, where for any $1 \leq j \leq n - 1$ condition, the result of the Boolean operation $(b_0 \text{ OR } b_j)$ contains more elements with value 1 than the result of the Boolean operation $(w_0 \text{ OR } w_j)$.

A third such condition is where all rows or m^2 -tuples of W or B are different from each other.

There are many qualified pairs of matrices W and B for each parameter $n \geq 2$ input to the process. An example of a pair of $n \times m^2$ matrices W and B which satisfy the foregoing conditions and therefore can be used for generating the visual keys are:

$$\begin{aligned} w_0 &= (1, 0, \dots, 0) \\ b_0 &= (0, \dots, 0, 1) \\ w_j = b_j &= (\underbrace{1, \dots, 1}_{j+1}, \underbrace{0, \dots, 0}_{m^2-j-1}) \text{ for } j = 1, \dots, n-1. \end{aligned}$$

If the size of the Adaptive Visual Image AVI obtained in module 36 step one is (x, y) and the process finds a pair of qualified $n \times m^2$ matrices W and B , then all n visual

keys are of the same size (mx, my) . The process subsequently initializes n number of (mx, my) matrices, $VK_0, VK_1, \dots, VK_{n-1}$ representing the first, second, and third visual keys 15, 16, and 17 respectively, in a module 38.

If however the option is taken to embed the key information K 13 into the first visual key VK_0 15 in a module 39, the hash result of the key information K 13 can be used as the random seed for producing the visual keys. Otherwise, an arbitrary random seed can be used. The random seed is used to decide the random column permutation operation

$$P_{ij} \ (i = 0, \dots, x - 1; j = 0, \dots, y - 1)$$

performed on W and B to obtain the two collections of $n \times m^2$ matrices Ω and Ψ .

Let any pixel of any image I with a size (w, h) be labeled as pixel (i, j) with the condition that $i = 0, \dots, w - 1; j = 0, \dots, h - 1$. The value of $I(i, j)$ is defined as following:

$$I(i, j) = \begin{cases} 0 & \text{if and only if pixel } (i, j) \text{ is white} \\ 1 & \text{if and only if pixel } (i, j) \text{ is black} \end{cases}$$

The process produces n visual keys based on AVI , W , and B in a module 40. Let $W_{ij} = WP_{ij}$ and $B_{ij} = BP_{ij}$. Then for $l = 0, \dots, n-1$,

$$VK_l(mi + i', mj + j') = \begin{cases} W_{ij}(l, mi' + j') & \text{if } AVI(i, j) = 0 \\ B_{ij}(l, mi' + j') & \text{if } AVI(i, j) = 1 \end{cases}$$

where $0 \leq i', j' \leq m-1$. Thus the process outputs n visual keys $VK_0, VK_1, \dots, VK_{n-1}$ in a module 41.

The first visual key VK_0 15 is the visual key to be embedded in the document 9, and the second and third visual keys VK_1 and VK_2 16 and 17 are provided to the authorized user 2 and authorized authenticator 3 respectively. In the process of generating these visual keys, the three conditions on W and B must be satisfied. When the condition that relates to the security of the embedded watermark is satisfied, it is guaranteed that any subset of the visual keys $VK_1, \dots, VK_{n-1}$ does not reveal the watermark or Visual Image VI . Similarly, when the condition that relates to the verifiability of the embedded watermark is satisfied, it is guaranteed that VK_0 and any other visual key can reveal the watermark or visual image VI if any combination of VK_0 with any other visual key is overlapped or overlaid. When the last condition is satisfied, $VK_0, VK_1, \dots, VK_{n-1}$ are all unique or different from each other and so no two identical visual keys exist.

After the generation of the visual keys, the formatting of the secure document is carried out with reference to a block diagram shown in Figure 3. The document 9 to be protected is pre-processed in the region detection and selection module 10. In the meantime, the first visual key 15 generated in a module 19 in accordance with the process described with reference to Figure 5 is provided as input to control the specific pixel modulation method to be carried out in the pixel modulation module 11. The first visual key 15 is provided as input to a module 20 and mapped to the image domain (dot matrix) therein for controlling the corresponding positions in the document 9 to be modulated. The document 9 is also zoomed out n times or resized in a module 21 to facilitate the modulation function. Within the detected and selected region of the document 9, all pixels are carefully checked in the module 21 to ensure that a good visual effect can be obtained after embedding the watermark by calculating the distance matrix between the document 9 and the desirous formatted secure document. This matrix is used for controlling the strength of modulation carried out in the pixel modulation module 11. One or a combination of three main kinds of pixel modulation methods can be employed in a module 22: color modulation; gradient modulation; or line/curve modulation. The underlying

principles behind these pixel modulation methods are re-sampling and quantization so that when the formatted secure document is photocopied, photo-scanned, or digitally filtered, the formatted secure document is demodulated for revealing the watermark.

Let the pixel value of any position $p: (x, y)$ on the document 9 be (R_p, G_p, B_p) . The luminance value is therefore:

$$L_p = 0.299R_p + 0.578G_p + 0.114B_p$$

In a testing region R within the detected and selected region of the document 9, the size of the region R is equal to the size of the first visual key 15 to be embedded where the mean values and variances are E_R, E_G, E_B and $\sigma_R, \sigma_G, \sigma_B$ respectively. The region R is regarded as a potential embeddable region if

$$E_L \leq T_1, \text{ and } \sigma_L \leq T_2$$

where T_1 and T_2 are two thresholds for controlling the quality of the visual effect of the document 9 after being embedded with the watermark. These two thresholds can be derived using well known techniques such as Maximize Entropy. Typical ranges of T_1 and T_2 values are $[0.65, 0.95]$ and $[0.0, 0.2]$, respectively assuming that the luminance value has been normalized to $[0, 1]$. Pixels which do not satisfy these requirements are skipped in the embedding process. The corresponding color should be some light colors such as aquamarine, faded brown, yellow, goldenrod, spring green, plum, silver, light wood, medium turquoise, new tan, quartz, green yellow, light blue, old gold, pale green, wheat, etc.

If the size of the first visual key 15 is $[V_m, V_n]$ before embedding, then the region to be embedded is zoomed out or resized to $[nV_m, nV_n]$. The three modulation methods of color modulation, gradient modulation and line/curve modulation, which are

modulation methods well known to those skilled in the art, are described in greater details hereinafter.

If color modulation is used, the color space of the document 9 is initially converted from the R-G-B color space (red value, green value, and blue value) to the L-a-b color space (brightness value, red-green value, and yellow-blue value) to appropriately match the human color perceptual system. In this case, n is usually set to 3. This means that each pixel is split into 3 X 3 pixels. The average value of these 3 X 3 pixels should be set equal to the value of the pixel of the document 9 before the split. After modulation, the value of the central pixel of the 3 X 3 pixels is assigned the nearest pure color but the brightness value of the same is to be adjusted so that the central pixel is blackened if the control value of the corresponding pixel from the first visual key 15 is 0. Otherwise, the value of central pixel is to be also assigned the nearest pure color but the brightness value of the same is to be adjusted so that the central pixel is whitened. The values of other pixels surrounding the central pixel is to be decided both by the central pixel and other neighbor central pixels according to the Gaussian low-filter model under the condition that the color difference is within a predefined threshold T_3 . The purpose is to obtain a smooth visual effect and the color difference can be obtained by calculating:

$$(\Delta s)^2 = (\Delta L)^2 + (\Delta a)^2 + (\Delta b)^2$$

Typically, $T_3 \leq 0.2$ assuming the normalized range of Δs is $[0,1]$. If gradient modulation is used, n is usually set to 4. There are two directions of gradients: horizontal and vertical. In a manner similar to the color modulation method, the average value within a 4 X 4 block of pixels should be set equal the value of the original pixel of the document 9. The highest values are found at the central portion of the block and the direction is decided by the control value of the corresponding pixel from the first visual key 15. If the control value of the corresponding pixel from the first visual key 15 is 1, the direction of gradient modulation is horizontal. Otherwise, the direction of gradient modulation is vertical. The pixel value of other

portions of the document 9 is set in a descending manner to form gradients along the decided direction.

If line/curve modulation is used, in a manner similar to gradient modulation, the directions of lines are decided by the values of the corresponding pixels from the first visual key 15. In this case, n is usually set between 4 and 8. Line/curve modulation works in a discrete way, which means that within a block of pixels, there are only two kinds of pixel values, i.e. 0 or 1.

After modulation according to any of the foregoing modulation methods, the formatted secure document is either directly sent to printer for making a hardcopy of the formatted secure document or saved as a standard format such as a PDF file in a module 23. Typically, the visual effect of the detected and selected region after modulation is a little transparent as shown in Figure 10.

During the embedding process, it is important that all zooming out or resizing operations are performed so as to keep the printing size of the formatted secure document unchanged from the printing size of the document 9. To this end, it is required that the resolution of the printer used for making a hardcopy of the formatted secure document is at least 300 dpi.

When the authorized user 2 wishes to prove the originality or integrity of the formatted secure document to others or to the authorized authenticator 3, the authorized user 2 can do so using any of the two verification methods. With reference to Figure 4, the verification of the embedded watermark can be done either in the electronic domain or in the physical domain.

In the electronic domain, a formatted secure document 24 to be verified is first processed by directional filtering and then subjected to a thresholding operation in a module 26 to recover the first visual key 15. The result is shown in Figure 11. The recovered first visual key 15 and another visual key 28 (16 or 17) that is used for verification are then provided as input to a module 30, where there is digital overlaying of the two input images by Boolean exclusive or multiple operations. The embedded visual image shown in Figure 6 then appears and can be visually verified by human eyes in a module 32. If the combination of the recovered visual key 15 and

the verifying visual key 28 is consistent and the formatted secure document 24 has not been altered or forged, the result of the digital overlaying is shown in Figure 13 where there is resemblance of the visual image shown in Figure 6.

In the physical domain, a hardcopy of the formatted secure document 25 to be verified is first photocopied in a module 27 where the modulated first visual key 15 can be recovered. The resolution at which the hardcopy is printed must be higher than the resolution at which the photocopy of printed hardcopy is made. The resulting photocopy of the embedded region of the formatted secure document 25 is shown in Figure 12. One condition for properly recovering the modulated first visual key 15 is that the printer resolution must be higher than the photocopier resolution. Another visual key 29 (16 or 17) that is used for verification is printed on a transparency. The transparent hardcopy of the visual key 29 is then overlaid on the photocopy of the formatted secure document in a module 31. The embedded visual image shown in Figure 6 then appears and can be visually verified by human eyes in a module 33. If the combination of the recovered visual key 15 and the verifying visual key 29 is consistent and the hardcopy of the formatted secure document 25 has not been altered or forged, the result of the physical overlaying is shown in Figure 14 where there is resemblance of the visual image shown in Figure 6.

Otherwise, if the formatted secure document has been altered or forged, the result of digitally or physically overlaying the recovered first visual key 15 and the verifying visual key 28 or 29 is shown in Figure 15. What is shown is merely noise and there isn't any resemblance of the visual image shown in Figure 6.

When the hardcopy of the formatted secure document 25 is photocopied, there are two reasons that the photocopied document differs from the original printed document. The first reason is that normally the resolution of photocopier is less than resolution of the printer. The second reason is that normally the colors of photocopier are less than the colors of printer. These two effects result in the difference between the original printed document and the photocopied document based on the principles of re-sampling and quantization, which is well known to those skilled in the art. As described in the foregoing, the visual keys have been linked to the content of the document 9 during the formation of the formatted secure document. Therefore, any

modification to the formatted secure document such as alteration results in an inconsistent visual effect when visual verification is carried out, i.e. the embedded visual image shown in Figure 6 does not appear anymore.

The system for providing an unobtrusive watermark in a secure document disclosed in the foregoing can be applied to many applications to protect the originality of any secure document or prevent any manipulations such as alterations on the secure document. With reference to Figure 1, the service center 1 may be a third party or commercial entity providing the services of notarizing documents submitted by the authorized user 2. When requested by a party such as the authorized authenticator 3 who may wish to have documents submitted to the same by an alleged party claiming to be the authorized user 2 validated by an independent party, the service center 1 sends a verifying visual key to the authorized authenticator 3. Alternatively, the authorized user 2 may provide a visual key which the authorized user 2 may hold to the authorized authenticator 3 to serve the same purpose of verifying the originality and integrity of the secure document.

Claims

1. A method of providing an unobtrusive watermark for securing a document, said method including the steps of:
 - 5 generating at least one visual key, wherein the generation of said at least one visual key depends on said watermark; and
 - embedding unobtrusively one of said at least one visual key in said document by modulating the values of pixels of said document, wherein the modulation of said values is dependent on said at least one visual key.
- 10 2. The method as in claim 1, further including the step of detecting and selecting a region on said document for embedding unobtrusively said one of said at least one visual key.
- 15 3. The method as in claim 1, wherein said step of embedding unobtrusively said one of said at least one visual key in said document includes detecting and selecting a portion of said document for embedding unobtrusively said one of said at least one visual key.
- 20 4. The method as in claim 1, wherein said step of modulating the values of pixels of said document includes modulating the values of pixels of said document using at least one of color modulation, gradient modulation, and line or curve modulation methods.
- 25 5. The method as in claim 1, wherein said step of generating said at least one visual key includes generating said at least one visual key, wherein generation of said at least one visual key depends on information extracted from said document.
- 30 6. The method as in claim 5, wherein said step of generating said at least one visual key further includes generating said at least one visual key, wherein generation of said at least one visual key depends on information based on the content of said document

7. The method as in claim 1,
wherein the generating step generates at least two different visual keys,
the generation of which depends on the watermark; and
further including the steps of:
5 extracting the unobtrusively embedded one of the at least two visual
keys; and
revealing said watermark using the extracted one of the at least two
visual keys and another of said at least two visual keys.
- 10 8. The method as in claim 7, wherein said step of extracting the unobtrusively
embedded one of said at least two visual keys includes re-sampling and quantizing the
unobtrusively embedded one of said at least two visual keys.
9. The method as in claim 8, wherein said step of revealing said watermark
15 includes overlaying said extracted one of said at least two visual keys and said another
of said at least two visual keys.
10. The method as in claim 1, wherein modulating the values of the pixels of the
document further depends on the content of the document.
- 20 11. A system for providing an unobtrusive watermark for securing a document,
said system including:
means for generating at least one visual key, wherein the generation of
said at least one visual key depends on said watermark; and
25 means for embedding unobtrusively one of said at least one visual key
in said document, including means for modulating the values of pixels of said
document, wherein the modulation of said values is dependent on said at least
one visual key.
- 30 12. The system as in claim 11, further including means for detecting and selecting
a region on said document for embedding unobtrusively said one of said at least one
visual key.

13. The system as in claim 11, wherein said means for embedding unobtrusively said one of said at least one visual key in said document includes means for detecting and selecting a portion of said document for embedding unobtrusively said visual key.
- 5 14. The system as in claim 11, wherein said means for modulating the values of pixels of said document includes means for modulating the values of pixels of said document using at least one of color modulation, gradient modulation, and line or curve modulation methods.
- 10 15. The system as in claim 11, wherein said means for generating said at least one visual key includes means for generating said at least one visual key, wherein generation of said at least one visual key depends on information extracted from said document.
- 15 16. The system as in claim 15, wherein said means for generating said at least one visual key further includes means for generating said at least one visual key, wherein generation of said at least one visual key depends on information based on the content of said document
- 20 17. The system as in claim 11,
wherein the means for generating at least one visual key generates at least two different visual keys, the generation of which depends on the watermark; and
further including:
25 means for extracting the unobtrusively embedded one of the at least two visual keys; and
means for revealing said watermark using said extracted one of said at least two visual keys and another of said at least two visual keys.
- 30 18. The system as in claim 17, wherein said means for extracting the unobtrusively embedded one of said at least two visual keys includes means for re-sampling and quantizing the unobtrusively embedded one of said at least two visual keys.

19. The system as in claim 18, wherein said means for revealing said watermark includes means for overlaying said extracted one of said at least two visual keys and said another of said at least two visual keys.

5

20. The system as in claim 11, wherein the modulation of the values of the pixels of the document further depends on the content of the document.

A SYSTEM FOR PROVIDING AN UNOBTRUSIVE WATERMARK IN A SECURE DOCUMENT

Abstract

A method and system of providing an unobtrusive watermark for securing a document is disclosed. At least one visual key is generated, wherein the generation of the at least one visual key depends on the watermark. Further, one of the at least one visual key is embedded unobtrusively in the document.

Figure 1

