An Optical Watermarking Solution for Authenticating Printed Documents*

Q.B. Sun, P.R. Feng and R. Deng

Kent Ridge Digital Labs
21 Hui Meng Keng Terrace, Singapore 119613

ABSTRACT

In this paper, we present a novel and simple optical watermarking system aiming at overriding some practical problems when the state-of-the-art digital watermarking techniques are applied to authenticat[*]*e the printed documents. We name our technique as optical watermarking differing from traditional digital watermarking in a sense that the watermark extraction is done by some optical and visual means like photocopier while no any digitization is required. The system security is guaranteed by adopting content-based key share scheme originated from visual cryptography. The non-obtrusiveness effect of watermarked document is achieved by modulating the watermark into a higher resolution gratings level. Experimental results demonstrate the availability and practibility of the proposed approach.*

Keywords: watermarking, document authentication, integrity verification, secret share.

1. Introduction

Authenticating valuable documents has been becoming a research topic since a long time because of its potential market. Typical solutions are based on either physical means or chemical means such as specious printer (>4000dpi) that cannot appear in the common market, special inks that are very sensitive to re-produce, and hologram, etc. The typical applications are cash, check or ID. However, there are also a lot of other valuable documents like certificate, contract in which the protection on its integrity is still desired. Especially in this digital age, making a fake copy is trivial by some digital ways. In this case, the above-mentioned approaches will not be practical due to their high costs. Previous work on protecting the content integrity can be categorized into two classes: watermarking-based and digital signature-based.

Originated from tradition cryptography, some robust digital signature-based approaches [1,2] intend to tackle the problems of incidental distortions introduced by some acceptable manipulations like compression or other format conversion. In [1], the authors proposed a solution to generate the robust signature that is invariant to JPEG compression. However, the invariant conditions will not satisfy anymore during the printing and re-scanning procedure because its distortion model is different from JPEG compression. In [2], the author proposed a public key based solution. They use owner's private key to encrypt the compressed document content while using owner's public key to decrypt the compressed content. The authentication is done by directly comparing the content to be authenticated and the content from decryption and de-compression. They suffer from two problems that obstacle their approach to practice. The first one is infeasible computation of the method because encrypting the content with high volume will be a time-consuming task [3]. The second one is that their final authentication result is comparison-based or correlation-based globally. Thus it will cause serious false acceptance and false rejection problems.

Some watermarking-based solutions can be found in [4,5,6]. Generally speaking, there are two kinds of watermarks: visible watermark and invisible watermark. Visible watermarking usually is used for public warning as no any security considerations were involved, embedding and removing are both easy. Furthermore, visible watermark seems a little obtrusive to viewer as visible watermarking embedding unavoidably needs to change the original content to generate a visual effect. Unlike visible watermark, invisible watermarking achieves the target of authentication by checking the consistence of embedded invisible watermark. It is not obtrusive, and visually no any difference between original content and watermarked content. For example, in [4] the authors proposed an invisible watermarking solution for authenticating the images. In [5], the authors presented a compression-compatible watermarking scheme and in [6], the authors proposed a text watermarking solution. But state-of-art of invisible watermarking for authenticating printed documents still has to solve two difficult problems. The first is to find out a trade-off between robustness of watermark embedding (survival under normal processing) and sensitivity of watermark extracting (able to detect the forgery parts). For instance, how to override the noise introduced by printing and re-scanning procedure, the

- The first author now is with Dept of E.E. of Columbia University. Emails: qibin@ee.columbia.edu, {pfeng, deng}@krdl.org.sg

0-7695-1062-0/01 $10.00 © 2001 IEEE

misalignment during the document registration, etc. The second one is the system security problem. Non-invertible watermarking scheme is desired and public key infrastructure based security protocols may need to be employed. Furthermore, the document must be digitized again for watermark extraction and content authentication. This may also cause some inconvenience for the users.

In this paper, We present a novel solution for authenticating printed document based on optical watermarking. We name our technique as optical watermarking differing from traditional digital watermarking in a sense that the watermark extraction is done by some optical and visual means like photocopier while no any digitization (re-scanning) is required. The system security is guaranteed by adopting content-based key share scheme originated from visual cryptography. The non-obtrusiveness effect of watermarked document is achieved by modulating the noise-like watermark into a higher resolution gratings level. In summary, our system has the following advantages:

- Secure: By adopting content-based key sharing scheme (visual cryptography), the security of whole embedding and authentication procedure is guaranteed by theoretic analysis.
- Robust: The authentication is based on global visual effect, any local defect will not affect the final decision.
- Convenient: Since no digitalization is required for watermark extraction, it will reduce system cost and bring the convenience to users. Furthermore, the whole authentication comprises of two steps: firstly checking the originality of the document by xeroxing it and secondly verifying the authenticity of the document by superimposing a transparency with secure key onto the xeroxed document.

The paper is organized as follows. In Section 2, we'll give a brief review on some backgrounds, followed by system description and security analysis. In Section 3, some implementation details are discussed such as visual key formation, watermark embedding and verification. Some experimental results are given in Section 4, and followed by some conclusions and the outline of future work that are given in Section 5.

2. System overview and security analysis

Our proposed solution mainly originates from two different research fields: visual cryptography [7,8] and frequency modulation [9,10,11].

2.1 Review of visual cryptography

The idea of visual cryptography was independently invented by G.R. Blakley and A. Schamir [7] which originated from traditional topic in cryptography: secret sharing. In general, a *n*-out-of-*m* threshold scheme is a method of sharing a *secret K* among a set of *m* participants in such a way that

- Any *n* participants can compute the value of *K*, and
- No group of *n*-1 (or fewer) participants can compute and information about the value of *K*.

The form of given secret can be a binary image *I*, comprises of black (1) and white (0) pixels. [7] gives an illustration on how it works based on 2-out-of-2 visual threshold scheme. Refer to Figure 1. Consider one pixel *P* in the image *I*. If *P* is black, then we get two black subpixels when we superimpose the two shares; if *P* is white, then we get one black subpixel and one white subpixel when we superimpose the two shares. Therefore, we can see that the final reconstructed pixel has a gray level of 1 if *P* is black and a gray level of 0.5 if *P* is white. Although for white pixel, the final value is not 0, it is still visible.

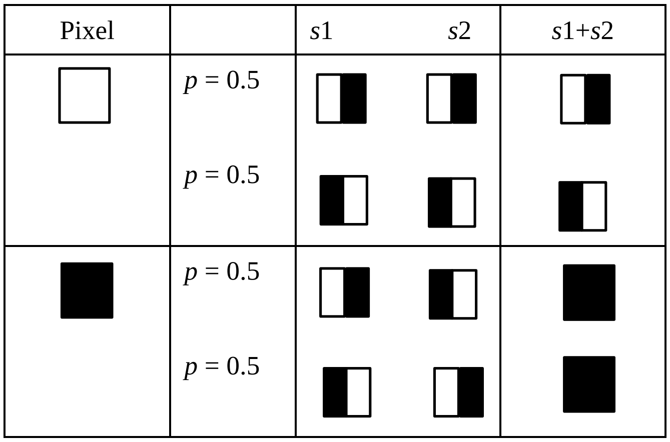


Figure 1. A 2-out-of-2 visual threshold scheme

However, directly applying the technique of visual cryptography to document authentication will cause serious visual degradation of document and therefore is not feasible because most of documents are also binary. In our application, we adopt visual cryptography as the engine of watermark generation. Once the watermark is generated, we will utilize frequency modulation to embed the watermark into printed document to achieve the non-obtrusive effect.

2.2 Frequency modulation of printed pattern

Differing from the state-of-the-art of watermarking techniques such as spread spectrum or quantization, we adopt the principle of frequency modulation for our watermark embedding. It is well-known that, for images with a limited bandwidth, it is possible to completely reconstruct the original image if the sampling frequency $W_s > 2W_m$, where W_m is the highest frequency present in the image. $2W_m$ is the Nyquist frequency. However, if the sampling frequency is less than the Nyquist frequency, it causes under-sampling that will lead to “alias” frequencies. The alias effect is also called Moire phenomena in some industries such as printing. The embedding and extracting can be illustrated as Figure 2. The frequency of watermark image is lower than the host image. Hence watermark can be done extracted by down-sampling (alias effect).

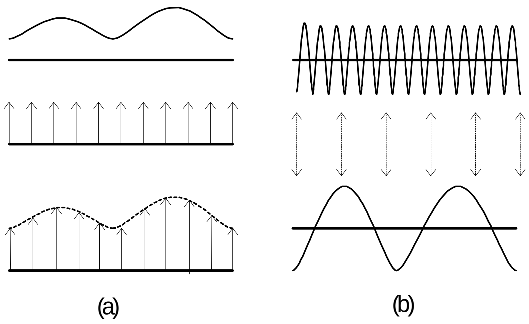


Figure.2 Watermark embedding and extracting
(a) embedding (b) extracting

In our application, the elements used to modulate the watermark are directional lines and dots with different sizes.

2.3 System description

Refer to Figure 3, the whole embedding procedure is as follows.

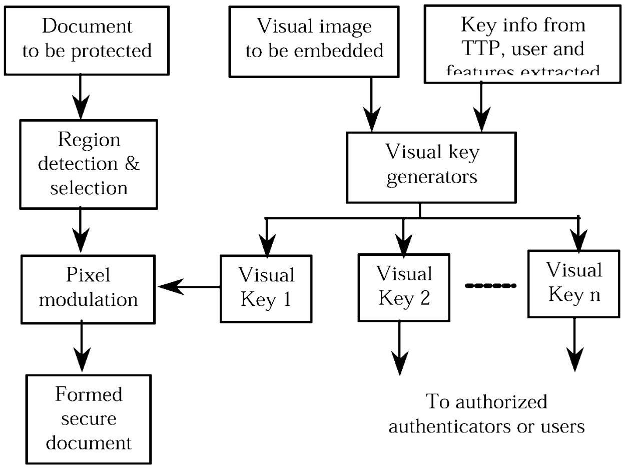

Document to be protected
Visual image to be embedded
Key info from TTP, user and features extracted
Region detection & selection
Visual key generators
Pixel modulation
Visual Key 1
Visual Key 2
Visual Key n
Formed secure document
To authorized authenticators or users

Fig.3. System diagram (embedding)

Given the document to be protected, we select the smooth areas to embed the watermark (for the cases that the text in the document are sparse, we can embed the watermark into whole background of the printed document) to obtain a good visual quality when authentication. In the mean time, the visual image (*VI*) such as a logo image is selected as the watermark image. The watermark image associated with other relevant information from Third Trusted Party (TTP), user and the features from the content of the document are fed into visual key generators to produce a set of secure keys that are under *n*-out-of-*m* threshold scheme and *n*>1. Taking one key, let’s say key 1, as watermark seed and embed it into the document by frequency modulation to achieve a non-obtrusive effect. The other keys are assigned to either authorized authenticators or users to verify the authenticity of the document to be protected. For example, in the case of 2-out-of-3 scheme, if key 1 is taken as watermark seed, the relationship among keys is: superimposing key 1 upon either key 2 or key 3 could produce the watermark image, while superimposing key 2 upon key 3 only results in a noise-like appearance.

The authentication procedure is very simple. The watermark extraction (key 1) is done by photocopying the document assuming that the document is printed in a higher resolution than that of photocopiers. By superimposing other authentication keys such as key 2 or key 3, the watermark image will appear if the content is authentic. Otherwise, key 2 or key 3 can be re-produced by extracting the features from the content done by automatically (OCR) or manually (inputting key text) and the document can be re-verified. If there are any malicious modifications on the content of the document, the superimposition either by key 1 and key 2 or key 1 and key 3 will result in a noise-like visual appearance.

2.4 Analysis on system security

Based on the description on the system, we can see that the system security is actually guaranteed by the module of key formation originated from visual cryptography. Differing from other watermarking methods that remain some disputable security issues, here our watermark embedding is a one-to-one linear modulation that is seamlessly connected to the generated watermark seed (key 1). Therefore, if key generation module is secure, the whole system should be secure. To analyze the security of key generation, let’s go back to Figure 1.

Refer to Figure 1, suppose we turn our attention to a pixel *P* in the share *s*1. One of the two subpixels in *P* is black and the other is white. Moreover, each of the two possibilities black-white and white-black is equally likely to occur, independent of whether the corresponding pixel in the secret image *I* is black or white. Thus the share *s*1 gives no clue as to whether the pixel is black or white. The same argument applies to the share *s*2. Since all the pixels in *I* were decrypted using independent random “coin flips”, there is no information to be gained by looking at any group of pixels on a share, either. For a formal security analysis, please refer to [7][8].

3. Some detailed implementation issues

3.1 Key formation

Refer to Figure 4, the whole procedure of producing visual keys is described as follows. Key information K is the information that can be from service center, user, and some features extracted from the document, which is to be embedded into final verifiable document. Here visual Image *VI*: (x', y') is the main image, which is used to produce all visual keys and can be disclosed by overlapping the first visual key and any other keys. Parameter n is the number of visual keys to be generated, and $n \geq 2$. Given VI, we need to find 2 base $(n \times m^2)$-matrices over $GF(2)$. Two qualified $(n \times m^2)$-matrices, say W and B, are required to produce the visual keys. From now on, we denote W and B by

$$W = \begin{bmatrix} w_0 \\ \vdots \\ w_{n-1} \end{bmatrix}, \quad B = \begin{bmatrix} b_0 \\ \vdots \\ b_{n-1} \end{bmatrix}$$

where $w_0, \cdots, w_{n-1}, b_0, \cdots, b_{n-1}$ are all m^2-tuples ($n < m^2$). And let in 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 visual keys, W and B must satisfy the following conditions:

Security: For any $1 \leq i_1, \cdots, i_p \leq n-1$, the two collections of $(p \times m^2)$ matrices Ω' and Ψ', obtained by restricting each $(n \times m^2)$ matrix in Ω and Ψ to rows $i_1, \cdots, i_p$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.

Verifiability: For any $1 \leq j \leq n-1$, (b_0 OR b_j) has more elements with value 1 than (w_0 OR w_j).

Difference: All rows of W or B are different to each other.

There are many qualified pairs of matrices (W and B) for each parameter $n \geq 2$. Here we give one example pair of $(n \times m^2)$-matrices W and B satisfying the requirements and can be used to generate visual keys:

$$w_0 = (1,0,\cdots,0), \; b_0 = (0,\cdots,0,1)$$

$$w_j = b_j = (\underbrace{1,\cdots,1}_{j+1} \quad \underbrace{0,\cdots,0}_{m^2-j-1}) \text{ for } j = 1,\cdots,n-1.$$

If the size of VI we get at step one is (x, y) and we find a pair of qualified $(n \times m^2)$-matrices W and B, then all n visual keys are of the same size (mx, my). We first initialize n (mx, my)-matrices, $VK_0, VK_1, \cdots, VK_{n-1}$.

The random seed is used to decide the random column permutations P_{ij} ($i = 0,\cdots,x-1$; $j = 0,\cdots,y-1$) on W and B.

Let the pixels of any document image I with size (w,h) be labeled as (i, j), $i = 0,\cdots,w-1$, $j = 0,\cdots,h-1$. And we define the value of $I(i, j)$ as the following:

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

We now produce n visual keys based on VI, W and B. Let $W_{ij} = WP_{ij}$, $B_{ij} = BP_{ij}$. Then for $l = 0,\cdots,n-1$,

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

where $0 \leq i', j' \leq m-1$. Thus we get n visual keys: $VK_0, VK_1, \cdots, VK_{n-1}$.

Here VK_0 is the visual key to be placed in the document. Notice that we have three requirements on W and B. Security guarantees that any set of $VK_1, \cdots, VK_{n-1}$ will not disclose the visual image VI, and Verifiability guarantees that VK_0 and any other visual key can disclose the visual image VI if we stack their transparencies together. We can see from the last requirement that $VK_0, VK_1, \cdots, VK_{n-1}$ will be different to each other and so no identical keys exist.

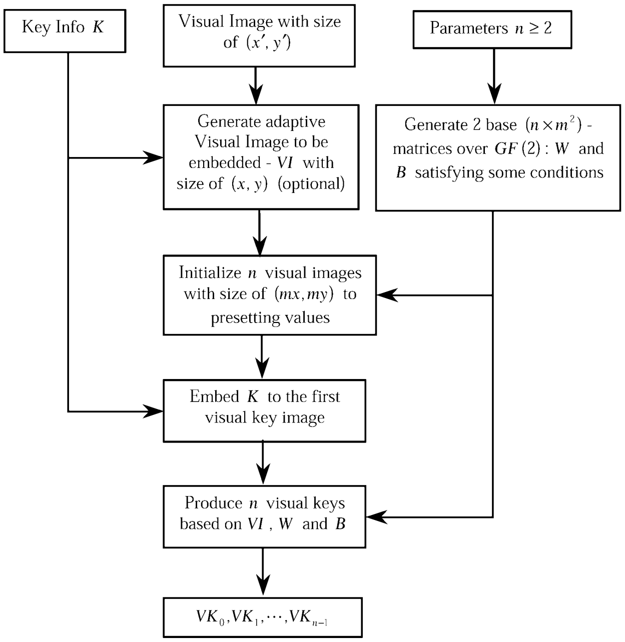

Key Info K
Visual Image with size of (x', y')
Parameters $n \geq 2$
Generate adaptive Visual Image to be embedded - VI with size of (x, y) (optional)
Generate 2 base $(n \times m^2)$-matrices over $GF(2)$: W and B satisfying some conditions
Initialize n visual images with size of (mx, my) to presetting values
Embed K to the first visual key image
Produce n visual keys based on VI, W and B
$VK_0, VK_1, \cdots, VK_{n-1}$

Figure 4. Key formation

3.2 Watermark embedding

Before watermark embedding, the document image will be zoomed in d times to accomplish the modulation function. Within the selected region, all pixels will be carefully checked to ensure that a good visual effect can be obtained after embedding by calculating the distance matrix between original document and the document after embedding. This matrix will be used for controlling the strength of modulation (embedding). Two main kinds of modulation methods are employed here: line modulation or dot modulation. Hence controlling the strength of modulation is actually controlling the line width or doc size. Refer to Figure 5. If the value of watermark seed is 1 (black), after zooming in, the corresponding block pixel values should be all 1s. Thus we can modify these 1s by replacing some of them with 0s to form a thin directional line or to form a large dot. If the value of watermark seed is 0 (white), we can modify all those 0s by replacing some of them with 1 to form a thin line with another direction or to form a small dot. By carefully selecting the zoom-in resolution and the direction of the line or the size of the dot, a good visual quality can be still kept after watermark embedding.

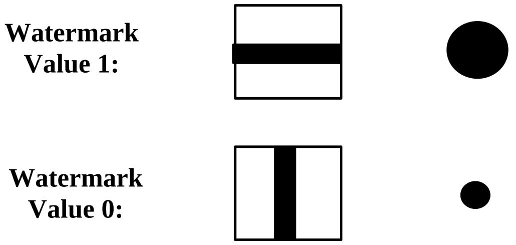


Figure 5. Watermark modulation

3.3 Watermark (document) integrity verification

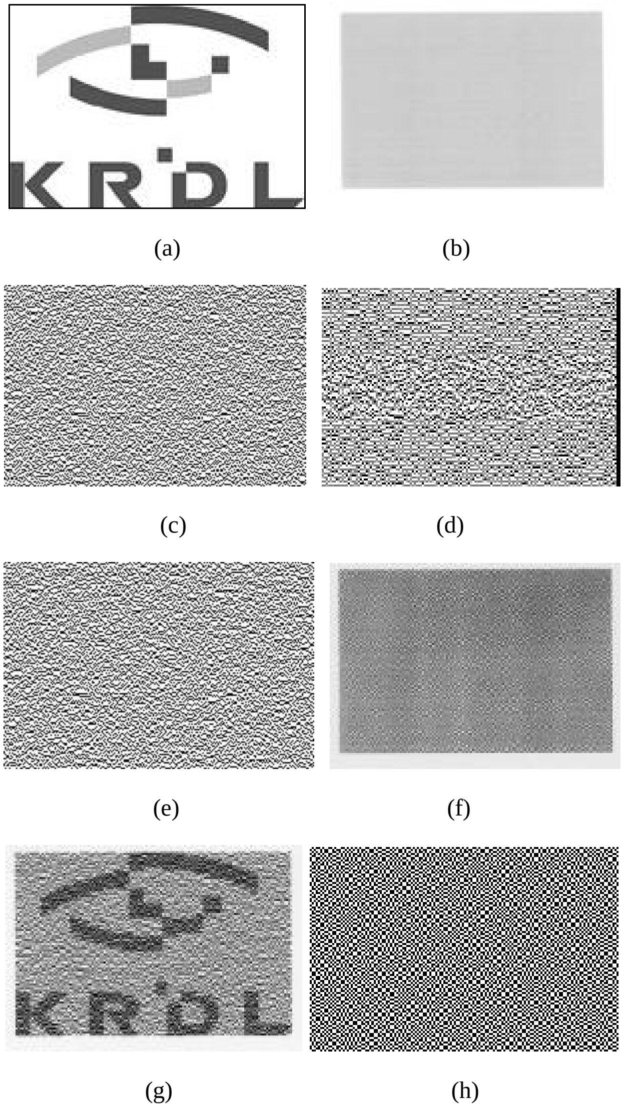
As we mentioned before, the principles behind wateramrk modulation are re-sampling and alias quantization. Therefore, watermark extraction can be easily done by put the printed document onto photocopier. The key 1 image will appear on the photocopied document. Then by overlapping another key (usually it is a transparency) onto it, the logo image (secret) will appear and be verifiable by human eyes. If the authenticator suspects the authenticity of the document, simply, he could re-produce the key he is owning and check again. If there is a malicious modification, the overlapping will result in a noise-like appearance.

4. Experimental results

In this section, we'll present some experimental results to demonstrate the feasibility of our proposed solution for document authentication.

Figure 6(a) is the watermark image we'd like to embed into the document to be protected. Figure 6(b) is the final watermarked image, the text can then be printed onto it. Figure 6(c), (d) and (e) are 3 keys we generated: Overlapping (a) and either (b) or (c) will make Figure (a) appear, while overlapping (b) and (c) will only result in a noise-like image (h). The extracted watermark is shown in Figure 6(f). Note that due to rescanned quality, it looks not so clear here. We will try to give an on-site demo at the conference. Figure 6(g) is the superimposition result done by overlapping Figure 6(f) and 6(d). The watermark image can be clearly verified by human eyes. For comparison, Figure 6(h) shows the superimposition result by overlapping Figure 6(d) (key 2) and Figure 6(e) (key 3).

Some experimental parameters used in our tests are given here. The size of original watermark image is 200x300. A 2-out-of 3 visual threshold scheme was adopted in our test that results in the size of keys being 600x900. The watermark embedding is done in the resolution of 3600x5400 which is the typical resolution for the document being printed in either 300dpi or 600 dpi. It is worthy of mentioning that due to the fact that the final key size is zoomed in a large times, the distortions caused by printing or photocopying can be improved. The document image is printed out in 600dpi resolution. Due to the resolution of most common photocopiers is 150-400dpi, the watermark can be correctly extracted by alias effect of these photocopiers.



(a) (b)

(c) (d)

(e) (f)

(g) (h)

Figure 6. Some experimental results

5. Summary and future work

In this paper, an optical watermarking solution for document authentication has been given. We introduced a concept of optical watermarking by conducting document authenticity verification with human eyes. The system security is guaranteed by adopting visual cryptography in key set generation. The non-obtrusiveness of watermarked document is obtained by frequency modulation. Since no any special means needed for watermark extraction, our proposed method will bring great convenience for users and also reduce the system costs.

Our future work is to establish a unified framework for document authentication that can be achieved both in electronic domain and in physical (after document printed out) domain. Of course, we still need to work on improving the robustness of the system to make it more practical in terms of system computation.

References

[1] C.-Y. Lin and S.-F. Chang, Generating robust digital signature for image/video authentication, *Proc. Multimedia and Security Workshop at ACM Multimedia'98*, Bristol, U.K., Sep. 1998.

[2] L. O'Gorman and I. Rabinovich, Secure identification document via pattern recognition and public-key cryptography, *IEEE Trans. PAMI*, Vol.20, No.10, pp.1097-1102, 1998.

[3] A. Menezes, V. Oorschot and S. Vanstone, Handbook of applied cryptography, CRC Press, 1998.

[4] M. Yeung and F. Mintzer, An invisible watermarking techniques for image verification, *IEEE ICIP'97*, Santa Barbara, USA, Oct., 1997.

[5] L. M. Marvel, G. Hartwig and C. G. Boncelet Jr., Compression compatible fragile and semi-fragile tamper detection, *SPIE Vol. 3971*, *EI'00*, SanJose, USA, Jan 2000.

[6] S. H. Low, N. F. Maxemchuk, J. T. Brassil and L.O'Gorman, Document marking and identification using both line and word shifting, *Infocom'95*, April, 1995.

[7] Doug Stinson, Visual cryptography and threshold scheme, *IEEE Potential*, pp.13-19, Feb./Mar., 1998.

[8] M. Naor and Benny Pinkas, Visual Authentication and identification, in "Advances in Cryptology - CRYPTO '97", B. Kaliski Jr. Ed., Vol. 1294 of *"Lecture Notes in Computer Science"* Springer-Verlag, Berlin, pp. 322-336, 1997.

[9] S. Spannenburg, (Frequency) Modulation of printed gratings as a protection against copying, *SPIE Vol.1509 Holographic Optical Security Systems*, pp.88-104, 1991.

[10] Copy restrictive system using microdots to restrict copying of color-reversal documents, *US Patent* No. 5864742.

[11] Security documents with multi-angled voids, *US Patent* No. 5707083.