A Visual Cryptography Based Watermark Technology for Individual and Group Images

Azzam SLEIT (Previously, Azzam IBRAHIM)
King Abdullah II School for Information Technology, University of Jordan,
Amman, Jordan

and

Adel ABUSITTA
King Abdullah II School for Information Technology, University of Jordan,
Amman, Jordan

ABSTRACT

The ease by which digital information can be duplicated and distributed has led to the need for effective copyright protection tools. Various techniques including watermarking have been introduced in attempt to address these growing concerns. Most watermarking algorithms call for a piece of information to be hidden directly in media content, in such a way that it is imperceptible to a human observer, but detectable by a computer. This paper presents an improved cryptographic watermark method based on Hwang and Naor-Shamir [1, 2] approaches. The technique does not require that the watermark pattern to be embedded in to the original digital image. Verification information is generated and used to validate the ownership of the image or a group of images. The watermark pattern can be any bitmap image. Experimental results show that the proposed method can recover the watermark pattern from the marked image (or group of images) even if major changes are reflected on the original digital image or any member of the image group such as rotation, scaling and distortion.

Keywords: Image Watermark, Group of Images, Pattern, Visual Cryptography, Rotation, Scaling, Copyright.

1. INTRODUCTION

Digital watermarking is the practice of hiding a message in an image, audio, video or other digital media element. Since the late 1990s, there has been a massive production for digital watermarking algorithms [3–17]. The sudden increase is mostly attributed to the increase in concern over copyright protection of content. Because new devices store content in digital form, there is no degradation in quality of data after a copy is made.

Traditionally, the owner of an image registers the image with the Copyright Office by sending a copy to them. The Copyright Office archives the image, together with information about the rightful owner. When dispute occurs, the real owner contacts the Copyright Office to obtain proof that he is the rightful owner. If he did not register the image, then he should at least be able to show the film negative. However, with the rapid acceptance of digital photography, there might never have been a negative. In theory, it is possible for the owner to use a watermark embedded in the image to prove that he/she owns it. Digital watermarking describes methods and technologies that allow hiding information, for example a number or text, in digital media, such as images, video and audio. The embedding takes place by manipulating the contents of the digital data. The modifications of the pixel values have to be invisible. Furthermore, the watermark has to be robust or fragile, depending on the application. With robustness we refer to the capability of the watermark to resist to manipulations of the media, such as loss compression, scaling, and cropping, just to enumerate some. Figure 1 shows the standard digital watermark schema. An image watermark method must satisfy the following two properties:

- Transparency: the embedded watermark pattern does not visually spoil the original image fidelity and should be perceptually invisible.

- Robustness: the watermark pattern is hard to detect and remove illegally.

This paper proposes a solution for watermarking digital images. Marking images will be conducted without embedding patterns into images. This leaves marked images unchanged with sizes exactly equal to the original ones. The new solution will retrieve the watermark pattern from rotated and / or resized image as is without any noise in the watermark pattern. As will be demonstrated in the coming sections, retrieving the watermark pattern from the marked image will be reasonably fast. The next section of this paper briefly outlines existing watermarking methods. Section 3 explains the proposed watermark method. Then, we discuss experimental results to demonstrate the merits of the proposed method.

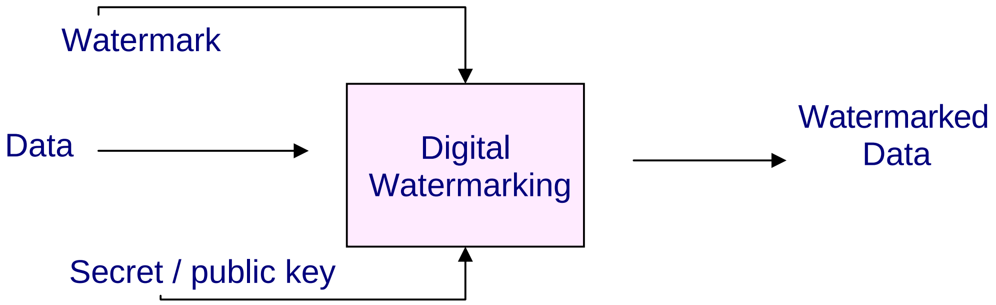


Figure 1: Digital watermark schema

2. WATERMARKING AND INVARIANT IMAGE SIZE

This section focuses on the works the watermarking methods that do not directly embed watermarks into the original digital images. Instead, verification information is generated which is used to verify the ownership of the image. The visual cryptography is a new concept defined by Naor-Shamir [2]. It is an extended type of (*t*, *n*)-threshold scheme which is also named the (*t*, *n*)-visual threshold scheme. In [2], the shadow of each participant is a transparency showing random dots. The shared secret is an image composed of black and white pixels. Any *t* out of these *n* shadows can make the shared secret recognized through the human visual system when they are stacked together. Any *t*-1 (or less) shadows stacked together can generate no knowledge about the shared secret. The image stored in the computer system can be considered a composition of pixels. Let each pixel be stored in *d* bits. Then, a 2^d gray-leveled image can be shown by using a set of pixels. It only uses one bit to express each pixel. Table 1 illustrates a simple (2, 2)-threshold scheme based on Naor-Shamir’s idea [2]. It also specifies the algorithm to encode each pixel in the shared image. This algorithm is applied to each pixel in the shared image in order to generate the corresponding subpixels in its corresponding two shadows. Each pixel *P* in the shared image is divided into two subpixels in each of these two shadows. If *P* is black, then the dealer randomly selects one of the first two rows in Table 1. If *P* is white, then the dealer randomly selects one of the last two rows in Table 1. Then, the dealer puts two two-subpixel blocks from Columns 2 and 3 to the corresponding positions in shadows 1 and 2, respectively. Let’s consider the result when these two shadows are stacked together. For each pixel *P* in the shared image, if *P* is black, then it generates a block with two black subpixels when these two shadows are stacked together. If *P* is white, then it generates a block with one black subpixel and one white subpixel when these two shadows are stacked together. The result is a collection of two black/white subpixels, which are printed in close proximity to each other so that the human visual system averages their individual black/white contributions. Through the human visual system, the block with two black subpixels will be recognized as a black dot while the block with one black subpixel and one white subpixel will be recognized as a white dot. Obviously, we can readily recognize if an image is the shared image with our visual system when these two shadows are stacked together.

Pixel	**Block 1**	**Block 2**	**Block1 superimposes on Block 2**
Black	(1, 0)	(0, 1)	(1, 1)
Black	(0, 1)	(1, 0)	(1, 1)
White	(1, 0)	(1, 0)	(1, 0)
White	(0, 1)	(0, 1)	(0, 1)

Table 1: A (2, 2)- visual threshold scheme; Note: bit "1" denotes black and bit "0" denotes white.

Hwang's method [1] is based on the simple (2, 2) visual threshold scheme presented by Naor-Shamir [2]. According to Hwang, the owner should select h*n black/white image as his/her watermark pattern P and a key S which must be kept securely. Then, verification information V is generated from the original k*1 image M and the watermark pattern P using the key S; as follows:

1. Use the secret key S as the seed to generate h*n different random numbers over the interval [0, k*1]. (R_i represents the i-th random number).

2. Assign the i-th pair (V_{i1}, V_{i2}) of the verification information V based on the following table:

The color of the with pixel in watermark pattern is	**The left most bit of the R_i-th pixel of image *M* is**	**Assign the i-th pair (v_{i1}, v_{i2}), of verification information *V* to be**
Black	"1"	(0,1)
Black	"0"	(1,0)
White	"1"	(1,0)
White	"0"	(0,1)

Table 2: Rules to assign values of verification information.

3. Assemble all the (V_{i1}, V_{i2}) pairs to construct the verification information V. This verification information must be kept by neutral organization.

When the owner want to claim the ownership of an image F as a copy of the original image M, he/she provides the secret key S, and the watermark pattern is restored using the image F and verification information V as follows:

1. Use S as the seed to generate h*n different random numbers over the interval [0, k*1]. (Ri represents the i-th random number).

2. Assign the color of the i-th pixel of the watermark pattern P' based on the image F as follows:

   a. Get the left-most bit, b, of the Ri-th pixel of image F, and if b is 1 then, assign *fi* = (1,0); otherwise assign *fi* = (0,1).
   b. If *fi* is equal to i-th pair of V then assigns the color of the i-th pixel of P' to be white; otherwise, assign it to be black.

3. If P' can be recognized as P through the human, the neutral organization shall adjudge that the image F is a copy of M.

The previous method has deficiencies in that it does not give consideration to the rotation, and scaling of images. Moreover, the watermark pattern must be a black and white image which does not offer flexibility to the owner [17]. The following section provides solutions for the above mentioned deficiencies.

3. PROPOSED WATERMARK METHOD

This paper offers a solution for the previously mentioned shortcomings. Let M_g represent a group of images to be marked. This group contain The following images {M_1, M_2, … M_n }. The proposed method generates verification information V from a group image M_g as shown bellow.

First, the owner must select a secret key S of length 8...128 byte. The key must be a multiple of 8 bytes and will be expanded to PK, where PK is the length of the watermark pattern as we will see later. The expanding algorithm is as follows:

1. Let S[i] be the i-th byte of the original key, Se[i] the i-th byte of the expanded key, and K the length of S.
2. Load the key S without change into the first K bytes of Se.
3. For i = K+1 to PK

```
        Se[i] = (Se[i-8]  XOR Se[i-4] XOR
                     Se[i-3]  XOR Se[i-1]) <<< 3
```

Then, the owner should select a watermark pattern P which can be any significant bitmap image. Consequently, the owner can typify a group image M_g using the watermark pattern and the expanded key Se according to the following steps for each M_i where i = 1, 2, ….n.

1. Let PK be the length of the watermark pattern P, MK_i the length of the image M_i, and MK_i' the length of the image M_i' which will be equal to MK_i/8 as we will see below.
2. Sort in-place all the pixel values of the original image M_i in ascending order. For example if the original image M_i has the following gray values (12 1 6 1 2 7 18 12 6 9), then M_i will receive the following values (1 1 2 6 6 7 9 12 12 18). The size of M_i is equal to that of MK_i.
3. Generate M_i' from M_i. Each pixel in M_i' represents 8 pixels of M_i. Bit 0 in pixel 0 of M_i' represents the most significant bit from pixel 0 of M_i, bit 1 in pixel 0 of M_i' represents the most significant bit from pixel 1 of M_i, and so on. For example, if the first 8 pixels of M_i are: **1**1111101 **1**1110111 **1**1101000 **1**1101000 **1**0100100 **0**1100001 **0**1001101 **0**0010010, then bit 0 of M_i' will receive1, and bit 1 of M_i' will be 1 as well and so on. The first pixel in M_i' will be 11111000.
4. Divide M_i' into g groups of pixels, in which g = MK_i'/PK rounded to the largest integer. MK_i' represents the length of the image M_i'. The grouping is performed without any manipulation.
5. Create array X_i which has the same length as P (i.e. PK). X_i is assigned the exclusive-or of all the pixels in each group of the groups generated from M_i'. If there is still space in X_i while M_i' pixels are finished (this happened when PK > MK_i') then X_i will repeat itself until all PK pixels in X_i have been filled.
6. Steps from 1 to 5 are repeated n times with different value of i where i = {1, 2,…n}
7. Finally, After generating X_i for each M_i, where i = 1, 2, ….n, verification information V is generated according to the following segment:

```
    For i = 1   to  PK
            V[i] = (P[i] XOR Se[i] XOR X_1[i] XOR
                          X_2[i] XOR ….. XOR X_n[i])
```

The verification information V is given to a neutral organization. In case the owner needs to claim ownership of some data F, and F seems to be one of the group's images M_i ,where i = {1, 2, …., n}. A watermark pattern P' is generated from the verification information V and key Se according to the following steps:

1. Replace F with its similar image in M_g and Repeat steps from 1 to 5 of the embedding process (use VK which is the length of the verification information instead of PK and generation information of the key as VK instead of PK). Then create array X from F to be used along with the extended key Se.
2. Generate the watermark pattern P' according to the following:

```
For i = 1   to  VK
        P'[i] = (V[i] XOR Se[i] XOR X_1[i] XOR X_2[i]
                      XOR ….. XOR X_n[i])
```

3. If P' is equal to the original watermark pattern P, then F is a copy of M_i (in case F is a copy of M_i with minor changes then the changes will appear on P' as some distortions).

In summary, the proposed method calls for sorting the input group images. The algorithm takes the sorted image as input to generate verification information instead of the original image. Also, it is obvious that the watermark pattern is restored successfully if no change occurs to any member in the group. This is because the embedding and verification processes are the same except for the final step (i.e. the exclusive-or operation). Mathematically,

$$(X\ \ \mathbf{XOR}\ \ Y)\ \mathbf{XOR}\ \ Y\ \ =\ \ X$$

Then, it can be concluded that P'[i] = (V[i] **XOR** X[i]) **XOR** S[i]) = ((P[i] **XOR** X[i]) **XOR** Se[i] **XOR** X'[i]) **XOR** Se[i] = P[i] only if X[i] is the same as X'[i]. Also it can be seen that if there is change in X[i] which represents a change in the image, then this change will reflect on the restored watermark pattern P'. Therefore, if the image M_i undergoes minor changes to become image F, the watermark pattern will still be recognized but it will have some distortions.

4. EXPERIMENTAL RESULTS

The proposed algorithms are studied on 24-bitmap *bean* and *moon* groups of images in Figure 2. Two watermark patterns are used; namely: Cheng and Tiger. Several types of distortions are experimentally investigated including rotation and scaling. Table 3 demonstrates that the watermark pattern can be recognized after rotating and/or scaling the images. Also, the proposed method works for significant patterns on groups of images unlike most of the existing techniques which work only on black and white patterns for individual images.

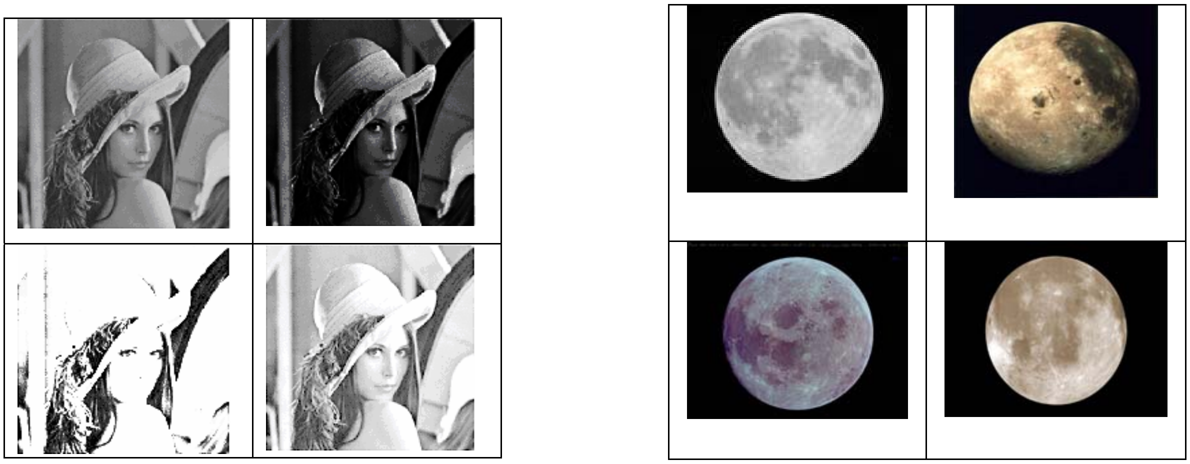
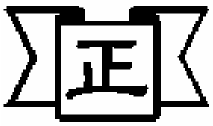
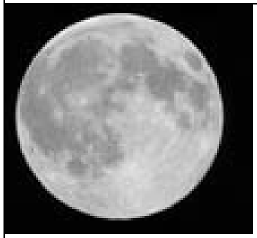
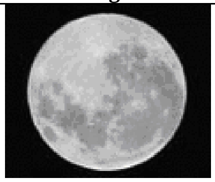
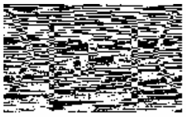
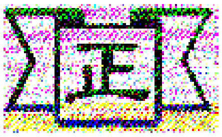
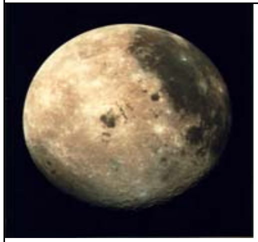
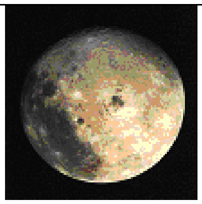
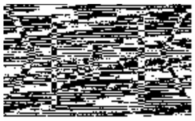
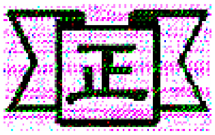
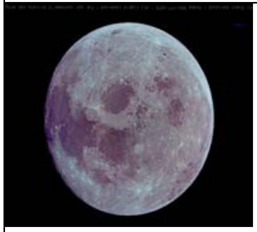
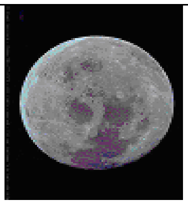
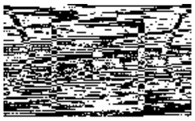
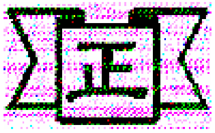
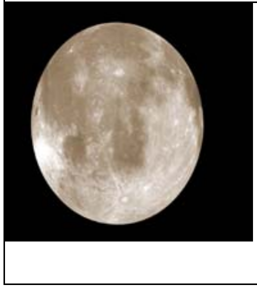
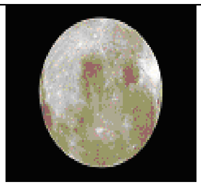
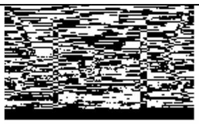
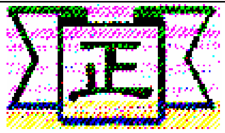
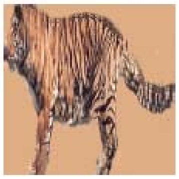
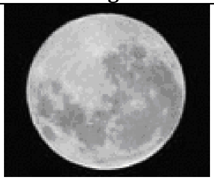
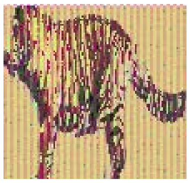
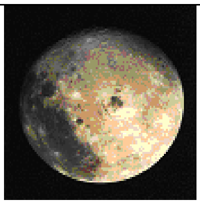
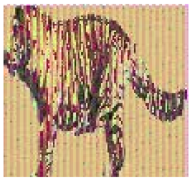
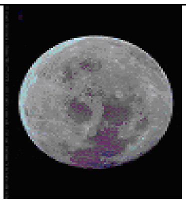
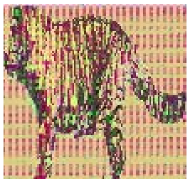
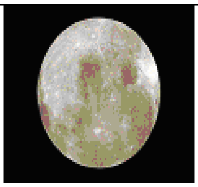
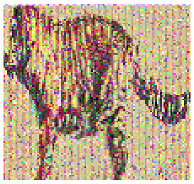


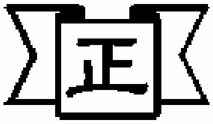
Figure 2: Lina and moon image groups

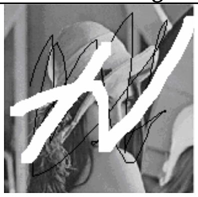
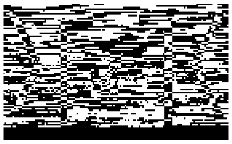
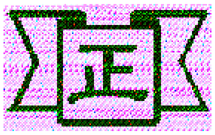
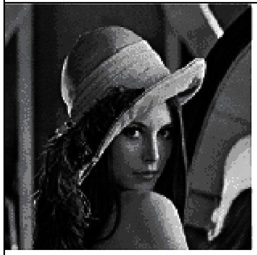
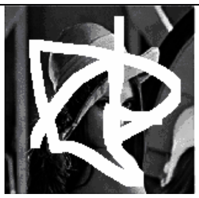
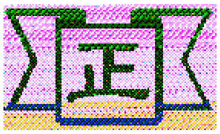
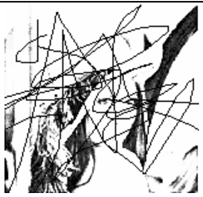
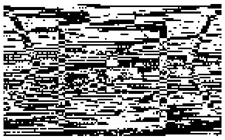
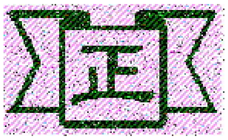
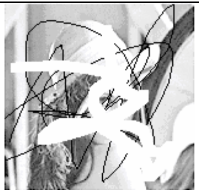
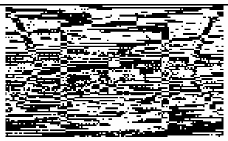
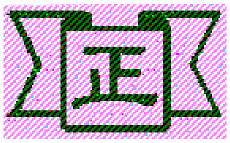
Pattern Used (Cheng)	Problem
 Black and white pattern	Image Scaling and Rotation

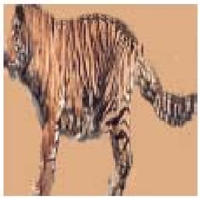
Original Image	Scaled and Rotated Image	Hwang Result	Our Result
			
			
			
			

Pattern Used (Tiger)	Problem
 Colored pattern	Image Scaling and Rotation

Original Image	Scaled and Rotated Image	Hwang Result	Our Result
		Hwang method works only on black and white Pattern	
		Hwang method works only on black and white Pattern	
		Hwang method works only on black and white Pattern	
		Hwang method works only on black and white Pattern	

Pattern Used (Cheng)	Problem
 Black and white pattern	Image Scaling and Distortion

Original Image	Scaled and Distorted Image	Hwang Result	Our Result
			
			
			
			

Pattern Used (Tiger)	Problem
 Colored Pattern	Image Scaling and Distortion

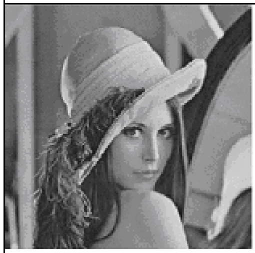
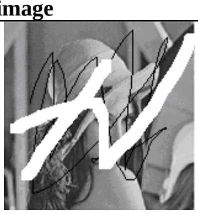
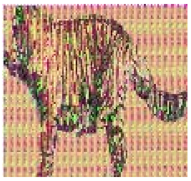
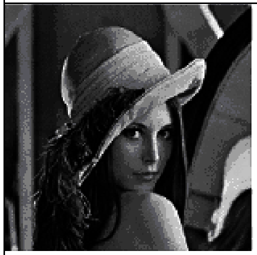
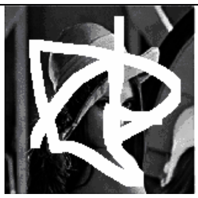
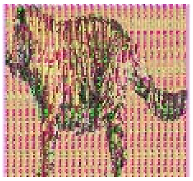
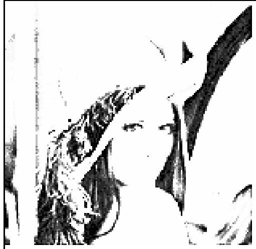
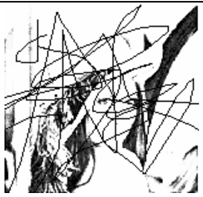
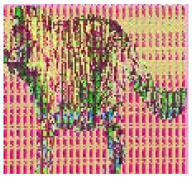
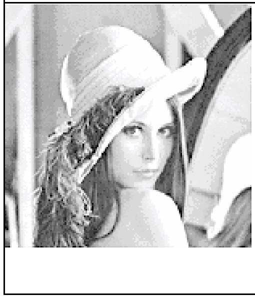
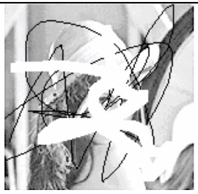
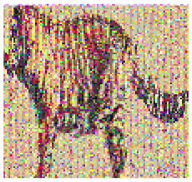
Original Image	Scaled and distort image	Hwang Result	Our Result
		Hwang method works only on black and white Patterns	
		Hwang method works only on black and white Patterns	
		Hwang method works only on black and white Pattern	
		Hwang method works only on black and white Patterns	

Table 3: Experimental results outlining the superiority of the proposed algorithms.

5. CONCLUTION

This paper presented a digital image copyright protection method which does not require that the watermark pattern to be embedded in to the original image which leaves the marked image equal to the original image. The watermark pattern is retrieved as is for rotated and resized images or group of images. The proposed technique is capable of protecting a group of images and demonstrated superiority when compared to other techniques. The watermark pattern cannot be retrieved from the marked image unless the key is given. Also the key cannot be retrieved even if all the algorithm components are known. Security of the method can be controlled by the length of the given key. For very long keys, the method is secure while for shorter keys the method obviously becomes less secure.

6. REFERENCES

[1] R. J. Hwang, "A Digital Copyright Protection Scheme Based on Visual Cryptography", **Tamkang Journal of science and Engineering**, Vol. 3, No. 3, 2000, pp. 97-106.

[2] N. Naor and A. Shamir, "Visual Cryptography", **Advances in Cryptology: Eurocrypt'94, Springer-Verlag, Berlin**, 1995, pp.1-12.

[3] R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp, “Perceptual watermarks for digital images and video”, **Proceedings of the IEEE**, Vol. 87, No. 7, Jul. 1999, pp. 1108–1126.

[4] E. T. Lin, A. M. Eskicioglu, R. L. Lagendijk, and E. J. Delp, “Advances in digital video content protection”, **Proceedings of the IEEE**, Vol. 93, No. 1, January 2005, pp. 171–183.

[5] I. Cox, J. Kilian, T. Leighton, and T. Shamoon, “Secure spread spectrum watermarking for multimedia”, **IEEE Transactions on Image Processing**, Vol. 6, No. 12, 1997, pp. 1673–1687.

[6] J. Fridrich and M. Goljan, “Comparing robustness of watermarking techniques”, **Proceedings of the SPIE/IS&T Conference on Security and Watermarking of Multimedia Contents**, Vol. 3657, San Jose, CA, Jan. 1999, pp. 214–225.

[7] C. I. Podilchuk and E. J. Delp, “Digital watermarking: Algorithms and applications”, **IEEE Signal Processing Magazine**, Vol. 18, No. 4, Jul. 2001, pp. 33–46.

[8] I. Cox, M. Miller, and J. Bloom, **Digital Watermarking**, Morgan Kaufmann, 2001.

[9] W. Stallings, **Cryptography and Network Security**, Third Edition, Prentice Hall, 2003.

[10] C. Rafael and E. Richard, **Digital Image Processing**, Second Edition, Prentice Hall, 2002.

[11] M. Swanson, B. Zhu and A. H. Tewfik, “Transparent Robust Image Watermarking”, **The Proceedings of IEEE International Conference on Image Processing**, Vol. 3, 1996, pp. 211-214.

[12] G. Voyatzis and I. Pitas, “Applications of Total Automorphisms in Image Watermarking”, **The Proceedings of IEEE International Conference on Image Processing**, Vol. 2, 1996, pp. 237-240.

[13] Xia X. G., Boncelet C. G. and Arce G. R., “A Multiresolution Watermark for Digital Images”, **The Proceedings of IEEE International Conference on Image Processing**, Vol. 1, 1997, pp. 548-551.

[14] W. Bender, D. Gruhl, N. Morimotoand, “Techniques for Data Hiding”, **IBM System Journal**, Vol. 35, No. 3, 1996, pp. 313-336.

[15] K. Matsui, J. Ohnishi, and Y. Nakamura, “Embedding a Signature to Pictures under Wavelet Transform”, **IEICE Transactions**, Vol. J79-D-II, No. 6, 1996, pp. 1017-1024.

[16] Hwang M. S., Chang C. C., and Hwang K. F., “A Watermarking Technique Based on One-way Hash Functions”, **IEEE Transactions on Consumer Electronics**, Vol. 45, No. 2, 1999, pp. 286-294.

[17] A. Sleit, and A. Abusitta, “A Watermark Technology Based on Visual Cryptography”, **in the Proceedings of the 10th World Multi-Conference on Systemics, Cybernetics and Informatics**, Vol. 1, 2006, pp. 227-238.