International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:1, No:8, 2007

Self Watermarking based on Visual Cryptography

Mahmoud A. Hassan, and Mohammed A. Khalili

***Abstract*—**We are proposing a simple watermarking method based on visual cryptography. The method is based on selection of specific pixels from the original image instead of random selection of pixels as per Hwang [1] paper. Verification information is generated which will be used to verify the ownership of the image without the need to embed the watermark pattern into the original digital data.

Experimental results show the proposed method can recover the watermark pattern from the marked data even if some changes are made to the original digital data.

***Keywords*—**Watermarking, visual cryptography, visual threshold.

I. Introduction

THE accelerating achievements in computers/internet need a range of security systems to prevent information (images, video, audio…) from being accessed, modified or used illegally by unauthorized people. Visual cryptography is a simple and powerful method which can provide privacy protection when transmitting sensitive shared information.

Naor and Shamir [2] introduced the concept of visual cryptography during EUROCRYPT 94. A simple version of visual cryptography is shown in Fig. 3 [3].

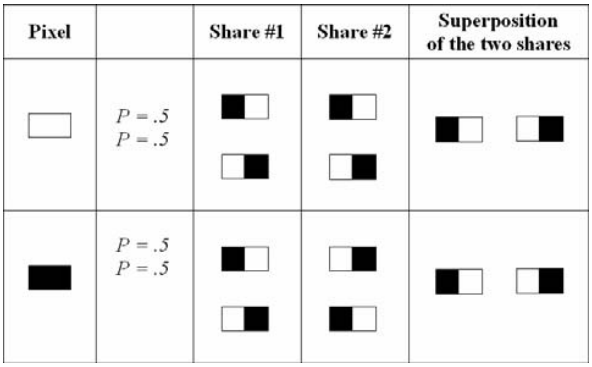

Fig. 1 A (2,2) visual cryptography scheme

It is assumed that the image to be encrypted consists of black and white pixels. Each pixel is split separately. An image is divided into several transparencies or slides. Each pixel will appear n times each time with different format called a share. Each share has m black and white subpixels.

That is, one pixel in an encrypted image is split m times and exists in n slides. To decrypt the secret image, the shares must be simply stacked or superimposed to produce the original image. More detailed information about visual cryptography can be found in [4, 5, 6, 7].

Hwang [1] watermark method is based on the simple (2, 2) visual threshold scheme presented by Naor and Shamir [2]. In Hwang method, the owner should select h x n black/white images as his watermark pattern P and a key S which must be kept securely. Verification information V is generated from the original kx1 image M and the watermark pattern P using the key S according to the following steps:

- Use the secret key S as the seed to generate h x n different random numbers over the interval [0, kx1]. Allow R_i to represent the i-th random number.
- Assign the pair (v_{i1}, v_{i2}) of the verification information V based on Table I.

TABLE I
The Rules to Assign the Value of Verification Information

The color of the *i*-th 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)

- Assemble all the (v_{i1}, v_{i2}) pairs to construct the verification information V.

Above information must be kept by neutral organization. When the owner wants to claim the ownership of an image F as a copy of the original image M, he just provides the secret key S, and the watermark pattern are restored using the image F and verification information V as follows:

- Use S as the seed to generate hxn different random numbers over the interval [0, kx1], allow R_i to represent the i-th random number.
- Assign the color of the i-th pixel of the watermark pattern P' based on the image F as follows:

Mahmoud A. Hassan is with the Electronics Engineering Department of Princess Sumaya University, Amman, Jordan (e-mail: m.hassan@psut.edu.jo).
Mohammed A. Khalili is with the Computer Science Department of Jordan University, Amman, Jordan.

1. Get the left-most bit, b, of the R_i-th pixel of image F, and if b is 1 then assign $f_i = (1, 0)$, otherwise assign $f_i = (0, 1)$.
2. If f_i is equal to the i-th pair of V then assign the color of the i-th pixel of P′ to be white; otherwise assign it to be black.

- If P′ can be recognized as P through the human visual system, the neutral organization shall adjudge that the image F is a copy of M.

According to Hwang [1] method, the random pixels are derived from the original image. This method generates the following problems:

- Since the selection of pixels is random, for the case of a restored watermark pattern from image F which is a copy of image M, and this watermark pattern be distorted in such a way that it cannot make sure that the image F is a copy of the original image M, especially if the image F goes into minor charges.
- If we have an image F with some similarities with the original image M. The watermark pattern P may be restored successfully, although the image F is not the same as the image M.

II. The Proposed Watermark Method

This method is based on selection of specific pixels from the original image instead of random selection of pixels. Initially, the owner must select a secret key S of length 8….128 byte, the key must be multiple of 8 bytes and it will be expanded to P_k bytes where P_k is the length of the watermark pattern as will be shown later. Expanding is done as follows:

1. Let S[i] represents the i-th byte of the expanded key, k represents the length of S.
2. The key S is loaded without change into the first k bytes of S_e.
3. The following format is applied to the expanded key S_e for I = k+1 to P_k:

$$S_e[i] = (S_e[i-8] \wedge S_e[i-4] \wedge S_e[i-3] \wedge S_e[i-1] <<<] \qquad (1)$$

(Symbol ^: exclusive-or, symbol <<<: left shift).

Then, the owner has to select a watermark pattern P which can be any significant bitmap image, now the owner can typify an image M using the watermark pattern and the expanded key S_e according to the following steps:

1. Let P_k represents the length of the watermark pattern P, M_k represents the length of the image M and M'_k represents the length of the image M′ (will show later that $M' = M_k/8$).
2. Image M' is generated from image M in which every pixel in M^- represents 8 pixels in M, so bit "0 in pixel 0 in M' represents the most significant bit from pixel 0 in M, and bit 1 in pixel 0 in M' represents the most significant bit from pixel 1 in M and so on.
3. The generated image M' is divided into g groups of pixels, in which
   $g = M'_k/P_k$ rounded to the largest integer, so if $(M'_k/P_k) = 3.2$, then g = 4. The grouping is done from the beginning to the end without any manipulation.
4. Create array X which has the same length $P(P_k)$, X is assigned from the XOR of all the pixels in each group of the group, generated from M′, pixels are taken from the beginning to the end, if there is still space in X which M' pixels are finished (this happened when $P_k > M'_k$) then X will read itself until all P_k pixels in X are filled.
5. Finally, verification information V is generated according to the following formula for S = 1 to P_k:

$$V[i] = (P[i] \wedge X[i] \wedge S_e[i]) \qquad (2)$$

The verification information V is given to a neutral organization, when the owner wants to claim the ownership of some data F, watermark pattern P' is generated from the verification information V and the key S (which will be given by the owner) according to the following steps:

1. Previous embedding steps from 1-4 are repeated except that V_k which is the length of the verification information replaces P_k. Also generation of the key is the same using V_k instead P_k. Array X from image F will be used along the extended key S_e.
2. Watermark pattern P' is generated according to the following formula for S= 1 to V_k:

$$P'[i] = (V[i] \wedge X[i] \wedge S_e[i]) \qquad (3)$$

3. If P' equals original watermark pattern P_o or can be recognized as it, then we conclude that F is a copy of M, also if F is a copy of M which goes into minor changes then changes will appear on P′ as some distortion.

It is very obvious that the watermark pattern is restored successfully if there is no change on the image, this is because that the embedding and verification process is the same, the only difference is the final step, which is simple exclusive-or operation and from the fact that X^Y^Y=X then we can show that :

$$P'[i] = (V[i] \wedge X[i]) \wedge S_e[i]$$
$$= (P[i] \wedge X[i] \wedge S_e[i] \wedge X'[i]) \wedge S_e[i] = P[i] \qquad (4)$$

only if X[i] is the same as X′[i].

Also it can be concluded that if there is a change in X[i] which represents a change on the image, then this change will be reflected on the restored watermark pattern P′, so if the image M goes into minor changes to become image F, the watermark pattern will still be recognized but it will have some distortion.

The security in the proposed method is based on the

generation of the extended key S_e which as long as the data, so the algorithm security can be adjusted as needed, for optimum security a long random key can be provided which was proven that if the given key is totally random and provides no regular patterns, then the method will survive all cryptanalysis attacks and will be completely secure [8]. Shorter keys will provide security as needed but the key length of 64-bits (8 bytes) is the minimum length.

III. Experimental Results

The proposed method is tested using Lina, Baboon and Earth 24-bitmap images. Two watermarks are used, Tiger and Cheng. The proposed method is repeated on distorted images Lina1, Lina2 (Fig. 3), Baboon1, Baboon2 (Fig. 4), Earth1 and Earth2 (Fig. 5).

Fig. 2 Watermark patterns: Tiger and Cheng

Fig. 3 Test images: Lina, Lina1 (distorted), Lina2 (distorted)

Fig. 4 Test images: Baboon, Baboon1 (distorted), Baboon2 (distorted)

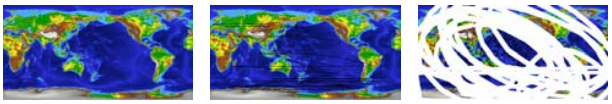

Fig. 5 Test images: Earth, Earth1 (distorted), Earth2 (distorted)

The distortions are reflected on the restored watermark patterns.

Figures 6, 7, and 8 show results using images: Lina, Baboon, and Earth respectively.

Fig. 6 Watermark patterns resulting from Lina, Lina1, Lina2

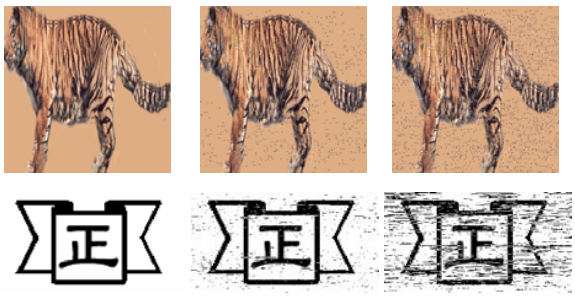

Fig. 7 Watermark patterns resulting from Baboon, Baboon1, Baboon2

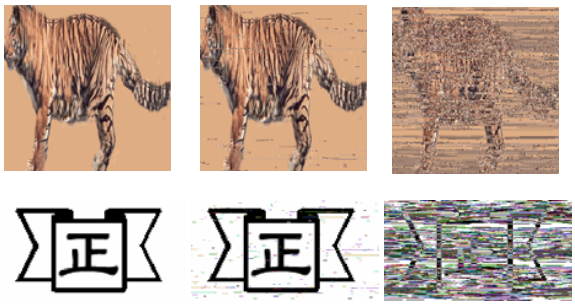

Fig. 8 Watermark patterns resulting from Earth, Earth1, Earth2

IV. Conclusion

In this paper we present a simple and efficient method for any valuable digital data that need to be protected. The main features of the proposed method are as follows:

- The watermark pattern is not embedded into the original image, which leaves the marked image equal to the original image.
- Any minor changes will not affect the success of the algorithm, and the restored watermark pattern will still be recognized.
- The watermark pattern cannot be retrieved from the marked image or verification information unless the key is given.
- Security of the proposal method can be controlled by the length of the given key, for very long keys the method is very secure.

REFERENCES

[1] R. Hwang, A digital Image Copyright Protection Scheme Based on Visual Cryptography, Tambang Journal of science and Engineering, vol.3, No.2, pp. 97-106 (2000).
[2] N.Naor and A. Shamir, Visual Cryptography, Advances in Cryptology: Eurocrypt'94, Springer - Verleg, Berlin, pp l-129 (1995).
[3] D. Stinson, http://www.cacr.math.uwaterloo.ca/~dstinson/visual.html (2003).
[4] L. Hawkes, A.Yasinsac and C. Cline, An Application of Visual Cryptography to Financial Documents; technical report TR001001, Florida State University (2000).
[5] A. Bonnis and A. Santis, Randomness in secret sharing and visual cryptography schemes, Theor. Comput. Sci, 314, pp 351-374 (2004).
[6] N. Paul, D. Evans, A. Rubin and D. Wallach, Authentication for remote voting, workshop on human-computer interaction and security systems, Fort Lauderdale, Florida, April (2003).
[7] C. Yang, A note on Efficient Color Visual Encryption, vol.18, pp 367-372 (2002).
[8] W. Stallings, Cryptography and Security, third edition, Prentice Hall, (2003).