An (3, 3)-Visual Secret Sharing Scheme for Hiding Three Secret Data

Pei-Fang Tsai, Ming-Shi Wang[1]

[1] Department of Engineering Science,
National Cheng Kung University,
Tainan 701, Taiwan
*E-mail: mswang@mail.ncku.edu.tw

Abstract

Visual cryptography is one kind of image encrypting. It is different from traditional cryptography, because it does not need complex computation to decrypt. In current technology, most of visual cryptography are embedded a secret using two shares is limited. This paper proposes a new approach of (3, 3)- visual secret sharing scheme to embed more information and have more secure than traditional visual cryptography.

Keywords: Visual cryptography; Halftone.

1. Introduction

With the network is more and more popular, the hackers utilize leak of the Internet to steal information that they want. Therefore, secure data transmitting becomes very important. In the recent years, generally using the traditional cryptology to avoid the data to be altered, but it needs complex computation to decode.

In order to reduce the computation and furthermore secure the data, Naor and Shamir[1] proposed a new cryptology called visual cryptography in 1994. Without huge calculation, it can restore encrypted messages by stacking two shares via human visual system to identify. The first visual cryptography scheme is used for the black-and-white image in disorder to embed the confidential message. These disordered images are called "shares" that one of them may regard as the cipher text and the other treats as the key. Hackers cannot decrypt the secret message from one share. Later on this theory, visual cryptography can extend as (k, n) – threshold visual secret sharing scheme that divides n transparencies into secret information. When be decoded, the owner must have k or more shares to stack. In 1998, Chen and Wu proposed a new visual cryptography scheme. It improves the drawback of the conventional visual cryptography that two share images only can embed one confidential message. It applies to rotate shares that encrypt two messages into two shares.

This paper proposes an improved (3, 3)-visual secret sharing scheme, which can be used to embed three secret messages into three shares and improve security. First of all, the fist main share image is resulted randomly and other two share images are based on the first share image and the two coding tables designed in this paper.

The rest of this paper is organized as follows. Section 2 reviews some conventional visual cryptography. In Section 3, the proposed technique is described in detail. Next in Section 4 shows the experimental results of the proposed method. Finally, the conclusions are given in Section 5.

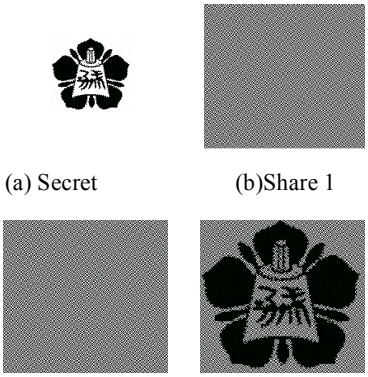
2. Previous schemes

In 1994, visual cryptography that uses stacking shares to recover confidential messages is proposed by Noar and Shamir. The secret owner encrypts the secret message into more than one share image. Each pixel in the secret image is expanded to four subpixels in each share that consist of white and black according to the patterns shown in Table.1.

secret image	Share 1	Share 2	stack image
□	▚	▚	▚
	▚	▚	▚
■	▚	▚	■
	▚	▚	■

Table.1: Naor and Shamir 's visual cryptography model

Fig. 1 shows an example to illustrate the above scheme. Fig. 1(a) shows the secret. The two corresponding shares of the secret are shown in Fig. 1(b) and Fig. 1(c), respectively. Then stacking the two shares, it can get the secret information via human's eyes and the result is shown in Fig. 1(d).



(a) Secret (b)Share 1

(c) Share 2 (d) Recovered secret

Fig. 1: An example of traditional visual cryptography.

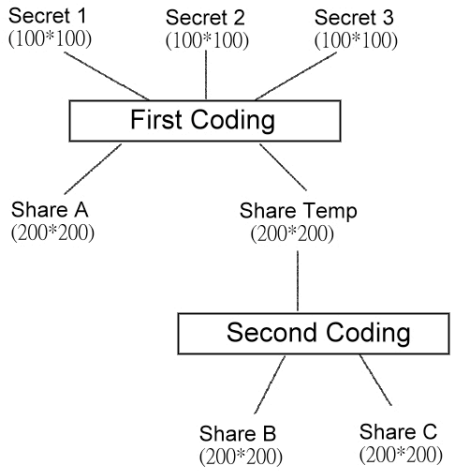
In 1998, Chen and Wu [3][4] proposed a novel visual cryptography scheme that rotating the share image and then stacking them can embed two messages into the two shares. The share A and share B can be created through the encoding process as shown in Table 2. Assume an extended block in share A is ▀, the pixel at the corresponding position of the first secret message is white, and the pixel at the corresponding position of the second secret message is also white, then at the position of the extended block for the share B is . As decrypting, to obtain the first confidential image can be implemented by stacking share A and share B together. Then, by rotating the share A counterclockwise 90^{o} and stack it with share B, the second secret image can be obtained.

Pixel of the first confidential image	W	W	B	B	W	W	B	B	W	W	B	B	W	W	B	B
Pixel of the second confidential image	W	B	B	W	W	B	B	W	W	B	B	W	W	B	B	W
2×2 block of share *A*	▚	▞	▚	▞	▚	▞	▚	▞	▚	▞	▚	▞	▚	▞	▚	▞
2×2 block of share *B*	▙	▟	▙	▟	▙	▟	▟	▙	▙	▟	▙	▙	▟	▙	▙	▙
Stacked block	▙	▙	■	■	▙	▙	■	■	▙	▙	■	■	▙	▙	■	■

Table.2: Chen and Wu's visual secret sharing scheme.

3. The proposed method

In conventional (3, 3) - visual secret sharing scheme, three share images can only be encrypted one secret message. In this paper, the same philosophy proposed by [3] is also used but more confidential messages are encrypted. The proposed scheme includes two steps,



the first s

Then share Ten

Fig.2 The

Fig. 3 The

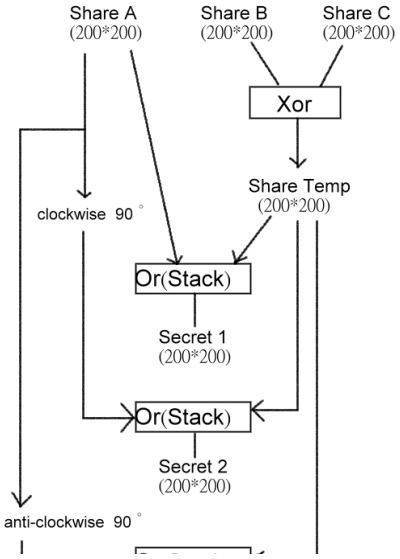


Fig.4: Four patterns of the extended block in share A

Pixel of the first secret image	W	W	W	W	B	B	B	B	W	W	W	W	B	B	B	B
Pixel of the second secret image	W	W	B	B	W	W	B	B	W	W	B	B	W	W	B	B
Pixel of the third secret image	W	B	W	B	W	B	W	B	W	B	W	B	W	B	W	B
2×2 block of Share *A*																
2×2 block of Share *Temp*																
Stacked block by Shares *A* and *Temp*																
Share *A'*																
Stacked block by Shares *A'* and *Temp*																
Share *A"*																
Stacked block by Shares *A"* and *Temp*																

Table.3: The proposed of the part in first coding processing.

Figure 2 shows the proposed encoding process. The three secret messages are passed through the first coding process to generate the share A and share Temp. The second coding process is used to generate share B and share C from the share Temp. Share A, share B, and share C are transmitted. For decoding process, after getting the three shares, share B and share C are logic XORed to create a temporal image-share Temp. The first secret image can be obtained by stacking the share A and the share Temp. Then the second secret information can be obtained by stacking the clockwise 90^o rotation of the share A and share Temp. The third secret information is obtained by stacking the counterclockwise 90^o rotation of the share A and the share Temp. Figure 3 gives the flow chart of the decoding procedures

3.1. Process for generating share A and share Temp

For the extended block of share A, one of the patterns is selected randomly from the patterns shown in Figure 4. Put the selected pattern in the pixel located at (i, j)、(j, N-i-1)、(N-j-1, i)、(N-i-1, N-j-1), where i, j, and N represent the pixel coordinates and the size of the original image, respectively. After the extension, the size of share A is become four times of the original one. Share Temp can be generated according to the three secret data and the generated share A. The generating rules are shown in Table 3.

For example, if the extended block of the share A is , and the first, second, and third secrets are white, black, and white, respectively, then the extended block of share Temp is corresponding to according to the rule shown in Table.3. According the rules designed in Table 3, it is shown that if share A and share Temp are stacked together, and assume the extended block is filled with two white pixels and two black pixels, and then it means there is a white pixel in the secret image. On the other hand, if the stacked extended block is filled with one white pixel and three black pixels, it means that the confidential image is a black pixel. In Table 3, the share A' and share A" represent the results of share A rotated 90^o clockwise and 90^o counterclockwise, respectively.

3.2. Process for generating share B and share C

To split the share Temp into two share B and share C, the coding rules are designed carefully. The idea is to consider the problem reversed. Assume to do logic exclusive-or share B and share C will generate the share Temp Then the code book for the second encoding process can be designed. For example, if the extended block of the share Temp is , then Table 4 shows all the possible cases of share B and share C. So to split the share Temp into two shares can be selected one of the ten solutions randomly. This encoding process also increases the security.

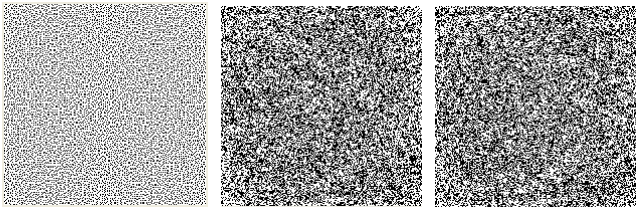
	1	2	3	4	5	6	7	8	9	10
Share *B*										
Share *C*										
Shares *Temp*										

Table.4: The partial rules of the second encoding process.

4. Experimental results

Fig. 5: Three secret images of the experiment.

Three secret images shown in Fig. 5 each with 100 * 100 pixels are encrypted into three shares. After performed the encoding processes described above, the three shares each with 200 * 200 pixels are shown in Fig. 6(a)-(c), respectively.



(a) Share A (b) Share B (c) Share C

Fig, 6: Three shares after two coding process.

When the receiver gets the three disordered share images, it needs to choose two correct images, which are share B and share C, to decrypt the share Temp as shown in Fig. 7 via logic exclusive-or operation. While obtaining the correct share Temp, it can be stacked with the other share to get the first confidential image as shown in Fig. 8 (a).

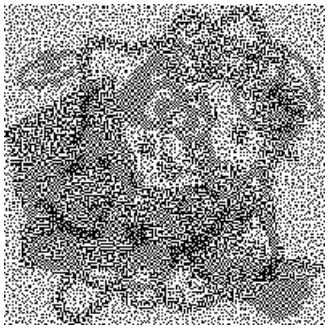
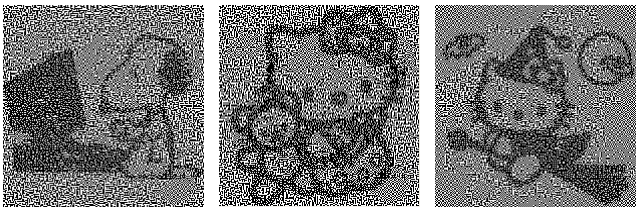


Fig. 7: Share Temp after decrypting share B and share C.



(a) Restored secret1 (b) Restored secret2 (c) Restored secret3

Fig. 8: The three decrypted confidential images.

In Fig. 8(b), rotating the share A clockwise 90^o and stacks it with the share Temp to identify the second secret image. Finally, rotating the share A counterclockwise 90^o and stacks it with the share Temp to obtain the third secret image as shown in Fig. 8 (c).

5. Conclusions

In the conventional (3, 3)-visual secret sharing scheme, it is usually to embed one confidential messages. In this paper, the conventional (3, 3)-visual secret sharing scheme has been extended to encrypt three secret images. It is also increased security.

6. References

[1] M. Naor and A. Shamir, “Visual Cryptography”, *Advances in Cryptology: Eurpocrypt’94,* Springer-Verlag, Berlin, pp. 1-12, 1994.

[2] Ateniese, G., C. Blundo, A. De Santis, and D. R. Stinson, “Extended Schemes for Visual Cryptography”*, Theoretical Computer Science*, 1996.

[3] L.H. Chen, and C.C. Wu, “A Study on Visual Cryptography,” *Master thesis, Institute of Computer and Information Science*, National Chiao Tung University, Taiwan, R.O.C.,1998.

[4] C.S. Tsai, C.C. Chang, and T.S. Chen, “Sharing multiple secrets in digital images”, *Journal of Systems and Software*, Vol. 64 ,pp. 163–170,2002.

[5] Wu, HC and Chang, CC, "Sharing Visual Multi-secrets Using Circle Shares," *Computer Standards & Interfaces*, Vol. 28, pp. 123-135. 373, 2005.

[6] Ming-Shi, Wang and Pei-Fang, Tsai, “The Implement of Visual Cryptography via Two Shares Embed Three Messages,” *The 3th Digital Content, Digital Education, and Management Policy*, pp. 69-77, 2005. (in Chinese)