Maximizing the Secret Hiding Ratio in Visual Secret Sharing with Reversible Property

Wen-Pinn Fang , Chiu-Jian Hsu and Mei-Ling Lin

Yuanpei University, Taiwan, R.O.C

Summary

This paper proposed a new visual secret sharing method. The property of visual secret sharing in reversible style is that it can be applied without depending on any computing If one stacks two transparencies together straightforwardly, a secret image will appear. Stacking two transparencies after reversing one of the transparencies, another secret image will unveil. Different from the traditional visual secret sharing with reversible property as previously proposed by Fang in 2007 and 2009, the method not only can fast decode while causing no pixel expansion but also increase the secret-hiding ratio. Based on the probabilistic method ,the experimental results showed that applying the technique proposed in this paper, it was possible to make the size of secret equal to that of the share.

Key words:

Visual cryptography; probabilistic; reversible, non-expansion

1. Introduction

Visual cryptography was first proposed by Shamir in 1995 [1]. The simplest format is (2, 2) threshold visual secret sharing. In (2,2) threshold visual secret sharing, there are two transparencies, the so-called shares. Both are noise-like, as shown in Figure 1(b) and (c). Since the probability of black pixel in every transparency is 50%, nobody can obtain secret image with one single transparency. However, if we stacks the two transparencies, as shown in Fig.1(b) and (c), the binary secret image will appear as in Fig.1(d). In the decrypting phase, instead of depending on any computing device, human eye alone can perform the function. The method used to generate shares is first defined in the table as shown in Fig.2. The next step is to scan all pixels of original image, as presented in Fig.1 (a). On the other hand, if the pixel value is white, then certain block of shares needs to be painted as exhibited by the corresponding blocks in Fig.2, column 2 and 3.

Shamir also designed visual cryptography with fault-tolerance property, named (n, r) threshold scheme. The method is used to first create basis matrix, and then look up the table to generate transparencies. In the beginning, most of studies only focused on handling single secret image. Recently, there were a lot of studies handling multi secret images. Ateniese, *et al*.[2] discussed access structure. Wu and Chang[3] proposed a method that can be applied for obtaining two secret images by modifying the stacking angles. Fang and Lin[4] proposed shift style visual cryptography method in 2006 which are able to get two secret images through different aligning location. Fang[5] proposed reversible visual cryptography scheme in 2007 that simultaneously embeds two secret images; one secret image will appear just by stacking two shares while the other secret image will appear only when one of the stacked shares being reversed. The advantage of such a scheme is that since there are two secret images, it is more difficult to create a fake share.

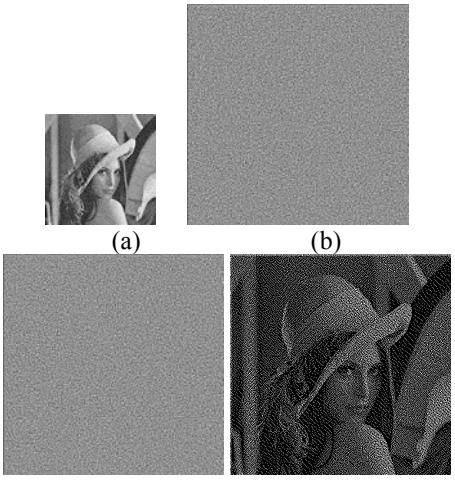


Fig.1 An example of traditional visual cryptography.

However, for all of these methods there is a pixel expansion step that needs to be conducted. For now one of the visual secret sharing approaches that do not need to go through pixel expansion is the random-grid method [6-8]. Such a method also does not require extra code book for generating shares.

In 2009, Fang[11] proposed a non-expansion visual secret sharing method with reversible property. The properties of this proposed method include security, fast decrypting and small share size. Nevertheless, there is a limit in applying this method: the total size of secret image

Manuscript received July 5, 2009
Manuscript revised July 20, 2009

is 3/2 of one share. Therefore, a new method has been explored, aiming to enlarge the ratio of secret images and shares, that is, trying to equalize the sizes of both the secret images and the shares.

The rest of this paper is organized as follows: the traditional Visual Cryptography in reversible style is introduced in Section 2; Non-expansion Visual Secret Sharing in reversible style is described in the section 3; the proposed method is demonstrated in Section 4; and the experimental results are presented in Section 5; the conclusions are given in Section 6.

2. Visual Cryptography in Reversible Style

Fang [5] proposed a brand new type of visual cryptography (VC), namely, the VC in reversible style. An example is shown in Fig.3. For any two given secret images (JET and MONKEY), two corresponding transparencies S_1 and S_2, also known as shares, can be produced. Both transparencies look noisy. However, if we stack the front views of both transparencies, then the first secret image will be unveiled. On the other hand, if we stack the front view of S_1 with the back-view (the turn-over) of S_2, then the second secret image will be unveiled. The block size of this method is 3×3 pixels. The share size is 9 times the original image. Fig.4 (a) and (b) represent the original images. Fig.4 (c) and (d) stand for the shares. Fig. 4(e) and (f) envisage the recovery images. The reasons to expand corresponding pixel to 3×3 block are (1) fit the relationship of turn-over property and (2) make the ratio (width and height) of the recovery image be the same as that of the secret image.

A pixel in secret image	Corresponding blocks		Resulting bloc from stacking the two shares
	Share 1	Share 2	
□			
			
■			
			

Fig. 2 Some sharing blocks found in Ref. 1 (not used here in the paper).

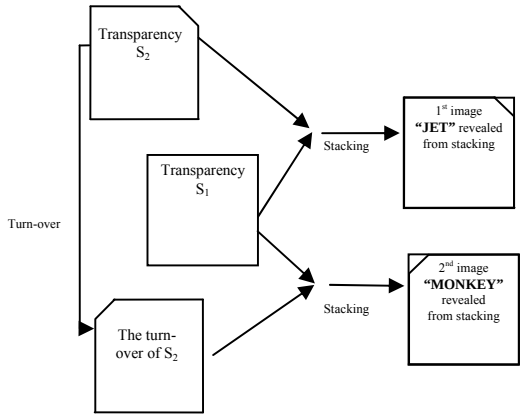
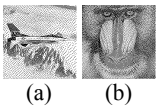
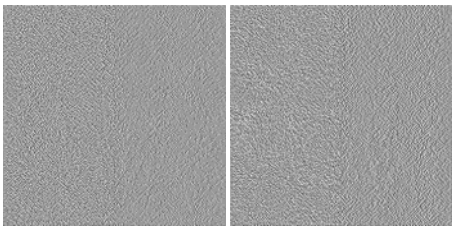


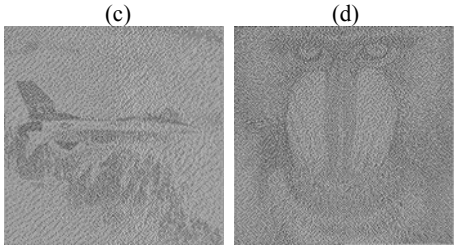
Fig.3. Visual cryptography in reversible style.



(a) (b)



(c) (d)

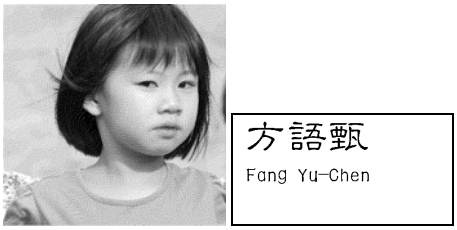


(e) (f)

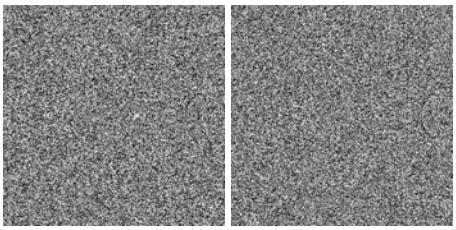
Fig. 4 the result of [5] (not this paper) (a) and (b) are the two original images; (c) and (d) are the two generated transparencies S1 and S2; whereas (e) and (f) are the stack results.

3. Non-expansion Visual Secret Sharing in Reversible Style

Kafri and Keren [6] presented three similar algorithms for image encryption applying random grids method. Precisely, the binary secret image I with the size of $h \times w$ will be encrypted into two cipher-grids S_1 and S_2 with the same size as that of I. First, the cipher-grid S_1 is created by randomly assigning each pixel the color 0 or 1, i.e., white and black. Secondly, the other cipher-grid S_2 will be created by referring to both the secret image I and the cipher-grid S_1 using one of Kafri and Keren's three algorithms. Afterwards in 2008, Chen and Tsao[8] proposed an extension principle that the algorithms mainly consist of three properties: (1) randomization, (2) complement, and (3) equivalence for general operation.
An example result is shown in Fig.6. Fig.6(a) is the first original image. It is a pretty girl's photograph. Fig.6(b) is another original image. The content of the second original image is the girl's name. Fig. 6(c) and (d) are the two shares. Fig. 6(e) is the stack result of Fig.6 (c) and (d). Fig. 6 (f) is the stack result obtained after Fig.6 (d) being overturned.



(a) (b)



(c) (d)

(e) (f)

Fig. 5 The experiment result in [11] (a) and (b) are original images, (c) and (d) are shares, (e) is the result that stack (c) and (d), (f) is stack (c) and reveries (d)

4. Proposed Method

In this paper, a non-expansion secret image sharing method is proposed, which enables the size of secret images created to be equal to that of the shares. The relationship of shares is shown as equation (1) to (4),

$$\alpha_1 \oplus \alpha_2 = \alpha_L, \tag{1}$$

$$\beta_1 \oplus \beta_2 = \beta_L, \tag{2}$$

$$\alpha_1 \oplus (\beta_2^{turn-over}) = \alpha_p \tag{3}$$

and

$$\beta_1 \oplus (\alpha_2^{turn-over}) = \beta_P \tag{4}$$

Here, "$\oplus$" means the stacking operation; α_i means the block (x,y) of the transparency S_i (i=1 and 2); while $\alpha_L$and α_p mean the block (x,y) of the recovered image, respectively. Similarly, β_i means the block (512-x,y) of the transparency S_i (i=1 and 2); while β_L and β_p mean the block (512-x,y) of the recovered images, respectively. The above four equations (1)-(4) provide us the rules to design our transparencies.

Set the size of images as W × H

There are two stages in encrypting phase, generating codebook and creating shares.

Input: original images I_1 and I_2 which are two binary images (half-toned images)

Output: shares S_1 and S_2 which are two noisy –like transparencies.

Step 1. Generate candidate lists

Step 1.1 Decide the number of candidate list c.

Step 1.2.Decide the patterns which meet Equation (1) to (4), Fig.6 is one example. The simplest method is brute force search

Step 2. Create Shares

Step 2.1 Divide every image into two equal size groups $G1_L$ and $G1_R$, $G2_L$ and $G2_R$ by middle axis. That is, $G1_L(x,y)=I1(x,y)$, $G1_R(x,y)=I1(x+W/2,y)$,

$G2_L(x,y)=I2(x,y)$,
$G2_R(x,y)=I2(x+W/2,y)$, here x=1~W/2, y=1~H.

Step 2.2 Scan G_L and G_R line by line and repeat step 2.2.1 to step 2.2.3 until all pixels have been process

Step 2.2.1 Look up the candidate list as shown in table 1.

Step 2.2.2 Randomly set the value of r where 0<r<c+1

Step 2.23 Assign the value of corresponding position of shares by the r^{th} element in the corresponding candidate list in table 1.

For example, if the size of all images are 512×512, the middle will be x=256. The pixel value of original images in position (10,3)and (512-10,3) are (B,W,B,B). The randomly selected number from 1 to 9 is 4,

Then, look up the table 1, the candidate lists will be

(B,B,B,**B**,B,W,W,W,W)
(B,B,W,**B**,B,W,B,W,W)
(B,B,W,**W**,W,B,B,B,W)
(B,B,W,**B**,W,W,B,B,W)

The pixel value of share in (10,3) and (502,3) will be B,B,W,B.

goal for the stacked results	Design of the two transparencies		Stacked results really meet our goal
	Transparency S_1	Transparency S_2	
(W,W,W,W)			
(W,W,W,B)			
(W,W,B,W)			
(W,W,B,B)			
(W,B,W,W)			
(W,B,W,B)			
(W,B,B,W)			
(W,B,B,B)			
(B,W,W,W)			
(B,W,W,B)			
(B,W,B,W)			
(B,W,B,B)			
(B,B,W,W)			
(B,B,W,B)			
(B,B,B,W)			
(B,B,B,B)			

Fig. 6. The pattern blocks $\{\alpha_1, \beta_1, \alpha_2, \beta_2\}$ used in [5] to paint the two transparencies. Columns (α_1) and (β_1) are, respectively, the pattern blocks in position α=(x,y) and position β=(256-x,y), for transparency S_1. Analogously, columns (α_2) and (β_2) are for transparency S_2; (α_L) and (β_L) are for the stacked result; (α_P) and (β_P) are for the stacked result. Note that the stacked result are $\alpha_1 \oplus \alpha_2 = \alpha_L$, $\beta_1 \oplus \beta_2 = \beta_L$, $\alpha_1 \oplus \beta_2^{turn-over} = \alpha_p$, and $\beta_1 \oplus \alpha_2^{turn-over} = \beta_P$ (to understand, see Fig.6, which corresponds to the last row (B,B,B,B) here).

Table 1: Candidate list

$G1_L(x,y)$, $G2_L(x,y)$, $G1_R(x,y)$, $G2_R(x,y)$	$S_1(x,y)$ $S_2(x,y)$ $S_1(x+W/2,y)$ $S_2(x+W/2,y)$
(W,W,W,W)	(B,B,B,B,B,W,W,W,W) (B,B,B,B,B,W,W,W,W) (B,B,B,B,W,B,W,W,W) (B,B,B,B,W,B,W,W,W)
(W,W,W,B)	(B,B,B,B,B,W,W,W,W) (B,B,W,W,B,W,B,B,W) (B,B,B,B,W,B,W,W,W) (B,B,B,W,B,W,B,W,W)
(W,W,B,W)	(B,B,B,B,B,W,W,W,W) (B,B,B,B,W,W,B,W,W) (B,B,B,B,W,B,W,W,W) (B,B,W,B,W,W,B,B,W)
(W,W,B,B)	(B,B,B,B,B,W,W,W,W) (B,B,W,W,B,W,B,B,W) (B,B,B,B,W,B,W,W,W) (B,B,W,B,W,W,B,B,W)
(W,B,W,W)	(B,B,B,B,B,W,W,W,W) (B,B,B,B,W,W,B,W,W) (B,B,B,B,W,B,W,W,W) (B,B,W,W,B,B,W,B,W)
(W,B,W,B)	(B,B,B,B,B,W,W,W,W) (B,B,W,W,B,W,B,B,W) (B,B,B,B,W,B,W,W,W) (B,B,B,B,W,B,W,W,W)
(W,B,B,W)	(B,B,B,B,B,W,W,W,W) (B,B,B,B,B,W,W,W,W) (B,B,B,B,W,B,W,W,W) (B,W,W,B,W,B,B,B,W)
(W,B,B,B)	(B,B,B,B,B,W,W,W,W) (B,B,W,W,B,W,B,B,W) (B,B,B,B,W,B,W,W,W) (W,W,B,B,W,B,B,B,W)
(B,W,W,W)	(B,B,B,B,B,W,W,W,W) (B,B,B,B,W,W,B,W,W) (B,B,W,W,W,B,B,B,W) (B,B,B,B,B,W,W,W,W)
(B,W,W,B)	(B,B,B,B,B,W,W,W,W) (B,B,B,W,B,B,W,W,W) (B,B,W,W,W,B,B,B,W) (B,B,B,B,B,W,W,W,W)
(B,W,B,W)	(B,B,B,B,B,W,W,W,W) (B,B,B,B,W,W,B,W,W) (B,B,W,W,W,B,B,B,W) (B,B,W,B,W,W,B,B,W)

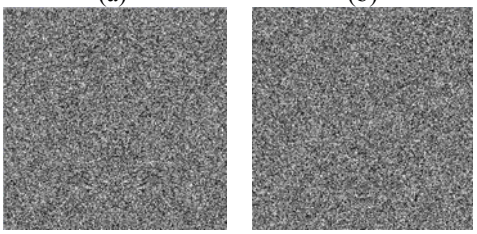
	(B,B,W,B,W,W,B,B,W)
(B,W,B,B)	(B,B,B,B,B,W,W,W,W) (B,B,W,B,B,W,B,W,W) (B,B,W,W,W,B,B,B,W) (B,B,W,B,W,W,B,B,W)\
(B,B,W,W)	(B,B,B,B,B,W,W,W,W) (B,B,B,B,W,W,W,B,W) (B,B,W,W,W,B,B,B,W) (B,B,W,W,B,B,B,B,W)
(B,B,W,B)	(B,B,B,B,B,W,W,W,W) (B,B,W,B,B,W,B,W,W) (B,B,W,W,W,B,B,B,W) (B,B,B,W,W,B,W,B,W)
(B,B,B,W)	(B,B,B,B,B,W,W,W,W) (B,B,B,B,W,W,W,B,W) (B,B,W,W,W,B,B,B,W) (W,W,W,B,B,B,B,B,W)
(B,B,B,B)	(B,B,B,B,B,W,W,W,W) (B,B,B,B,B,W,W,W,W) (B,B,B,W,B,B,W,W,W) (B,B,W,W,W,B,B,B,W) (B,B,W,B,W,W,B,B,W)

5. Experimental Results

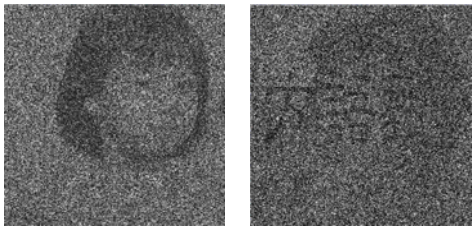
One of the experimental results from the proposed method is shown in Fig.7. Fig.7(a) is the first original image. It is a pretty girl's photograph. Fig.7(b) is another original image. The content of the second original image is the girl's name. Fig. 7(c) and (d) are the two shares. Fig. 7(e) is the stack result of Fig.7 (c) and (d). Fig. 7 (f) is the stack result obtained after overturning Fig.7 (d). Therefore, it is different from Fig.6 as presented in Ref.11. The size of the secret image (Fig.7 (b)) is twice that of the result secret image demonstrated in ref .11.(Fig.6(b)).

.

(a) (b)



(b) (d)



(e) (f)

Fig. 7 The experimental results (a) and (b) are original images, (c) and (d) are shares, (e) is the result from stacking (c) and (d), (f) is stack (c) and reverse (d)

6. Conclusion

Recently, visual secret sharing has been investigated more and more frequently. The main differences between the original design[1] and visual secret sharing include multi-secret approaches[3-5][11], general access structure property[2], application[9-10] and size expansion discussion[7-8][11-12]. This paper focused on multi-secret and size–non-expansion. To investigate the multi-secret property, this paper proposed a two-secret approach. There are two secrets hidden in two noisy-like shares. One of the secrets will appear just after two shares being stacked. The other secret will appear only when one of the shares being first reversed and then stacked together again. Different from ref.11, this paper increased the ratio of hidden secret. The reason that this paper can achieve the non-expansion goal is primarily because it adopted the probabilistic method[12] and at the same time added more constrains (Eq.1-Eq.4). Even though this paper adopted the same pattern as that in [11], it is possible to change the probability by redesigning candidate list as shown in table 1. Compared with the existing methods as shown in table 2, the approach employed in this paper not only has all the advantages of [11] and [12] but also can ensure more security in preserving secret. The method is suitable for fast transmission rather than for the most top secret. For the future work, how the probability can be best controlled and how security in preserving secret can be more enhanced are worth further investigation.

Table 2: compare with relative reports

paper	size expansion	Hide rate
Ref.[5]	Yes	1/9
Ref.[8]	No	3/4
This paper	no	1

References

[1] M. Naor and A. Shamir, "Visual Cryptography," Advances in Cryptogoly --- Eurocrypt '94, Lecture Notes in Computer Science, vol. 950, pp. 1-12,Springer-Verlag, Berlin,1995

[2] G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson, "Visual Cryptography for General Access Structure", *Information and Computing*, Vol. 129, 1996, pp. 86-106

[3] H.C. Wu and C.C. Chang, "Sharing Visual Multi-secrets Using Circle Shares," *Computer Standards & Interfaces*, Vol. 28, pp.123-135, 2005

[4] W.P. Fang, J.C. Lin, 2006, 4, "Visual Cryptography with Extra Ability of Hiding Confidential Data" *Journal of Electronic Imaging*, 15, pp.023020

[5] W.P. Fang, "Visual Cryptography in Reversible Style, "IEEE Proceeding on the Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing(IIHMSP2007), Kaohsiung, Taiwan, R.O.C, 2007, 11, 26～2007, 11, 28.

[6] O. Kafri and E. Keren, "Encryption of Pictures and Shapes by Random Grids," *Optics Letters*, Vol. 12, No. 6, pp. 377 - 379, 1987.

[7] S. J. Shyu, "Image Encryption by Random Grids," Pattern Recognition, Vol. 40, Issue 3, pp. 1014 - 1031, 2007.

[8] T. H. Chen and K.H. Tsao, "Visual Secret Sharing by Random Grids Revisited", *Pattern Recognition*, 2008, online(http://www.sciencedirect.com/science?_ob=MImg&_imagekey=B6V14-4V1TXMJ-1-1&_cdi=5664&_user=2414342&_orig=mlkt&_coverDate=11%2F30%2F2008&_sk=999999999&view=c&wchp=dGLzVtz-zSkzV&md5=0f9b092b81e841ed86e4a8c6eadd4a22&ie=/sdarticle.pdf)

[9] R.Lukac and K.N. Plataniotis , "Bi-level Based Secret Sharing for Image Encryption", Pattern Recognition Vol. 38, 2005, pp. 767–772.

[10] W.P. Fang and J. C. Lin, "Multi-channel Secret Image Transmission with Fast Decoding: by using Bit-level Sharing and Economic-size Shares" International Journal of Computer and Network Security, 6, 2006, 6, pp.228-234.

[11] W.P. Fang, "Non-expansion Visual Secret Sharing in Reversible Style, "*International Journal of Computer and Network Security*, Vol. 9, No. 2, 2009, 2, pp. 204-208

[12] C. N. Yang, "New Visual Secret Sharing Schemes Using Probabilistic Method," Pattern Recognition Letter, Vol. 25 2004, pp. 481‐494

Wen-pinn Fang received his BS degree in Mechanical Engineering in 1994 from National Sun Yat-sen University and his MS degree in Mechanical Engineering in 1998 from National Chiao Tung University, where he also got his PhD degree in Computer Science in 2006. His recent research interests include image sharing, pattern recognition, image processing and e-learning.

Chieu-jian Hsu received his M.A. degree in the Department of Foreign Languages & Literature from National Taiwan University in 1989. He is teaching in Yuanpei University in Hsinchu. In recent years, his academic interest shifted to translation and scientific English writing.

Mei-ling Lin received her M.A. degree in the Department of Foreign Languages & Literature from National Sun Yat-sen University in 1991. She is teaching in Yuanpei University now.