Non-expansion Visual Secret Sharing in Reversible Style

Wen-Pinn Fang

Yuanpei University, Hsinchu, Taiwan

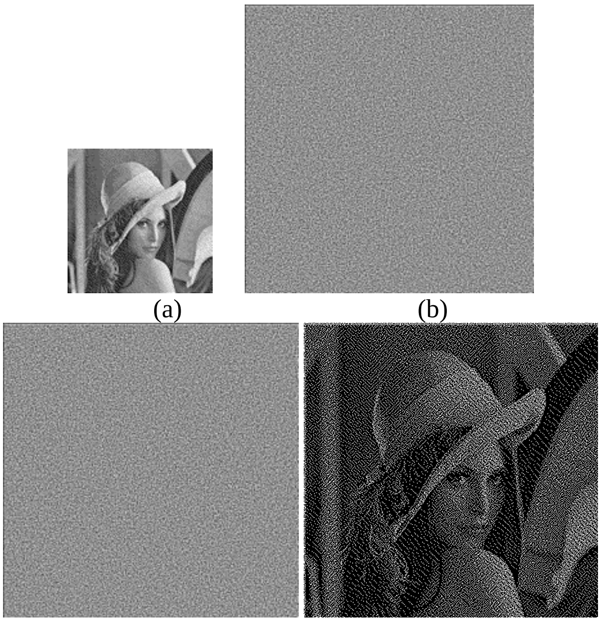
Summary
This paper proposed a novel reversible visual secret sharing method. Without any computing, if we stack two transparencies directly, a secret image will appear. Stacking two transparencies after reversing one of transparencies, another secret image will unveil. Different from traditional reversible visual cryptography, the method not only has advantages but also will not have pixel expansion and code-book. Besides, the same idea can be extended to complex style visual cryptography.

Key words:
Visual Cryptography; Random grid; Reversible; Non-expansion

1. Introduction

Visual cryptography is proposed by Shamir[1]. The simplest format is (2, 2) threshold visual secret sharing. In (2,2) threshold visual secret sharing, there are two transparencies, said shares. Both are noise-like as shown in Figure 1(a) and (b). Nobody can get secret image with one transparency. The probability of black pixel is 50%. If he stacks the two transparencies, that is Fig.1(b) and (c), the binary secret image will appear as Fig.1(d). In the decoding phase, computing device is unnecessary. Only naked eye is needed. The method to generate shares is predefined in the table as shown in Fig.2 first. Then scan all pixels of original image, such as Fig.1 (a). If the pixel value is white, then paint corresponding block of shares by looking up 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 to create basis matrix, and then look up the table to generate transparencies. In the beginning, most of studies handle with single secret. Recently, there are a lot of studies handling multi secret images. For example, Ateniese, *et al*.[2] discuss access structure. Wu and Chang[3] proposed a method that someone can get two secret images with different stack angles. Fang and Lin[4]proposed shift style visual cryptography method in 2006 which has two secret images with different align location. Fang[5] proposed reversible visual cryptography scheme in 2007, which has two secret images; one secret image appears with just stacking two shares and the other secret image appears with stack two shares after reversing one of them. Because there are two secret images, it is more difficult to create a fake share.


(a) (b)

(c) (d)

Fig.1 An example of traditional visual cryptography.

However, there is a pixel expansion step in all of the methods. There is another visual secret sharing approach without expanding method, named random-grid method [6-8]. The method also does not need extra code book in generating shares.

In this paper, a non-expansion visual secret sharing method with reversible property is proposed. The properties of the proposed method include security, fast decoding and small share size. The idea of the proposed method also can extend to complex visual cryptography.

The rest of this paper is organized as follows: the traditional Visual Cryptography in reversible style is given in Section 2; the review of the basic visual secret sharing scheme by random grids is given in the section 3; the proposed method is presented in Section 4; and the experimental results are demonstrated in Section 5; the conclusions are given in Section 6.

Manuscript received February 5, 2009
Manuscript revised February 20, 2009

A pixel i 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).

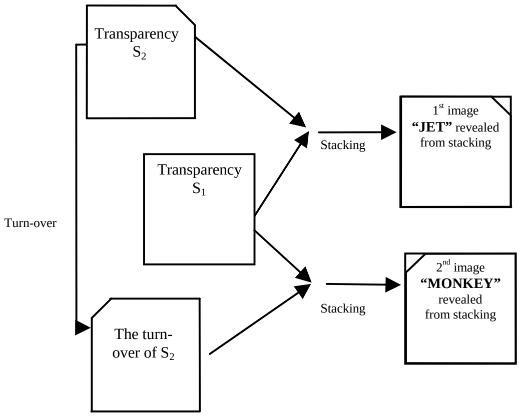

Transparency S2
Transparency S1
The turn-over of S2
Turn-over
Stacking
Stacking
1st image "JET" revealed from stacking
2nd image "MONKEY" revealed from stacking

Fig.3. Visual cryptography in reversible style.

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 is 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 is unveiled. The block size of this method is 3x3 pixels. The shares size is 9 times original image. Fig.4 (a) and (b) are the original images. Fig.4 (c) and (d) are the shares. Fig. 4(e) and (f) are the recovery images. The reasons to expand corresponding pixel to 3x3 block are (1) fit the relationship of turn-over property and (2) let the ratio (width and height) of recovery image be the same as secret image.

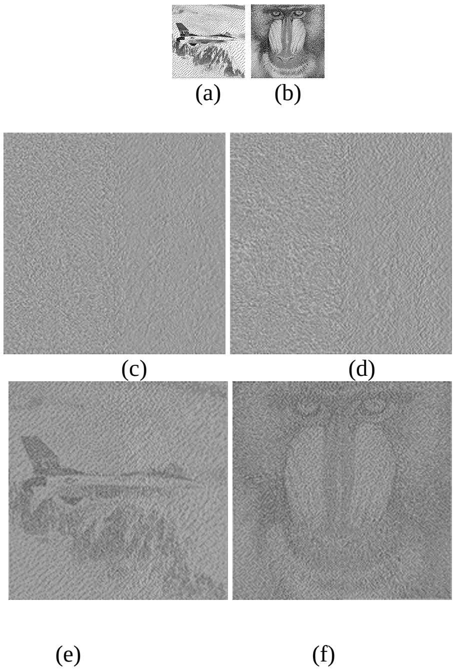


Fig. 4 the result of[5](not this paper) (a) and (b) are the two original images; (c) and (d) are the two generated transparencies S1 and S2; whereas (e) and (f) are the stack results.

2. Visual secret sharing by random grids

Kafri and Keren [6] presented three similar algorithms for image encryption by random grids. Precisely, the binary secret image I with the size of h×w will be encrypted into two cipher-grids S_1 and S_2 with the same size as that of I. Firstly, 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 both the secret image I and the cipher-grid S_1 according to one of Kafri and Keren' s three algorithms. Chen and Tsao[8] proposed an extension method that the algorithms mainly consist of three operations: (1) randomization, (2) complement, and (3) equivalence for general operation. Without losing generality, the method is shown as below:

Random grid method

input :original image I, where I is a halftone image and the image size is 512 by 512 pixels

```
output : shares $S_1$ and $S_2$.

for(i=0;i<512;i++)
    for(j=0;j<512;j++)
        Random assign $S_1$[i][j] as white or black
        If I[i][j] is white then
            $S_2$[i][j]=$S_1$[i][j];
        else
            $S_2$[i][j]=complement of $S_1$[i][j];
        endif
    end for
end for
                                        --- end of method
```

Fig.4 is an example of random grid method. Fig.4(a) is the original image. Fig.4(b) and (c) are the shares, Fig.4 (d) is the stack result. We can see that the size of original and shares are the same.

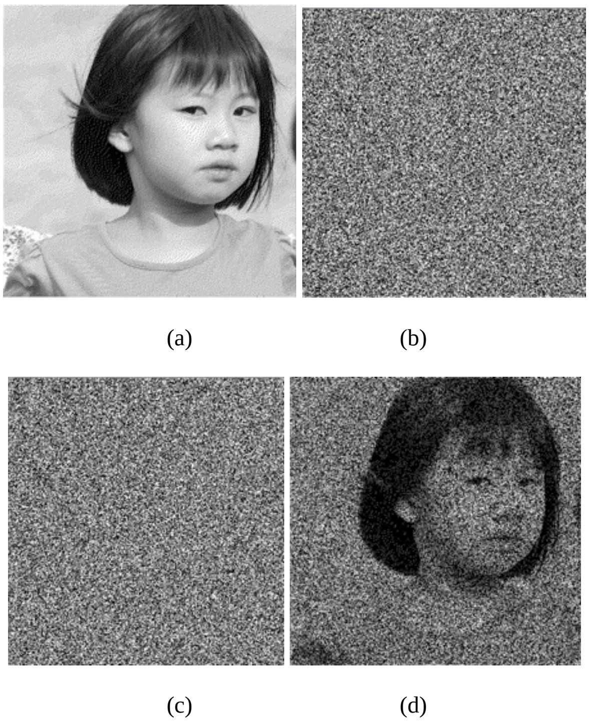


Fig. 4 An example of Random grid visual cryptography method (a) is original image, (b) and (c) are shares, (d) is the stack result.

3. Proposed method

There are four steps to generate the shares. Before starting to generate shares, divide original image and shares into two same size parts, upper part and lower part as shown in Fig.5. named I_1^U,I_1^L,S_2^U , I_2^L ,I_1^U,S_1^L,S_2^U and S_2^L. The algorithm is shown as below.

Random grid method in reversible style

```
input :original image $I_1$ and $I_2$, both are halftone images
  and the image size is 512 by 512 pixels
output : shares $S_1$ and $S_2$.

Step. 1 Assign the pixel values of $S_1^U$ randomly.
Step. 2 Assign the pixel value of $S_2^U$.
        if $I_1$[x][y]=white then
            $S_2^U$[x][y]= $S_1^U$[x][y].
        else
            $S_2^U$[x][y]=complement of $S_1^U$[x][y].
        end if
Step 3. Reverse $S_2^U$, that is Temp[x][y]= $S_2^U$ [512-x][y].
Step 4. Assign the pixel value of $S_2^L$.
        if I2[x][y]=white, then
            $S_1^L$[x][y]= temp[x][y].
        else,
            $S_1^L$ [x][y]=complement of temp[x][y].
        end if
Step 5. Assign the pixel value of $S_2^L$,
        if $I_1$[x][y]=white then
            $S_2^L$[x][y]= $S_1^L$[x][y].
        else
            $S_2^L$[x][y]=complement of $S_1^L$[x][y].
        end if
                                        --- end of method
```

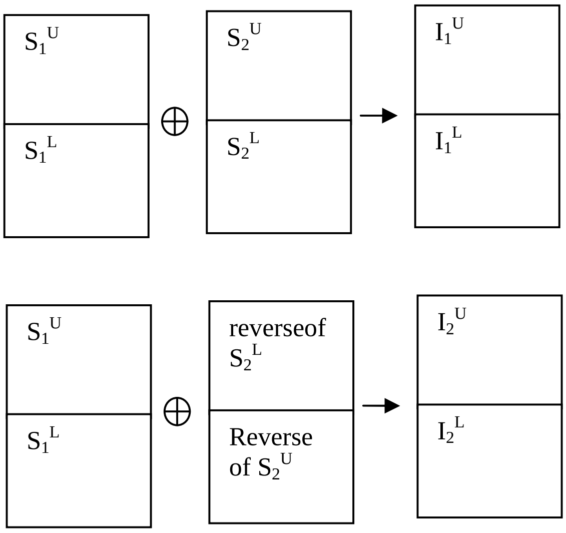


Fig. 5 the shares and stack result

4. Experiment Result

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 after turnover fig.6 (d).

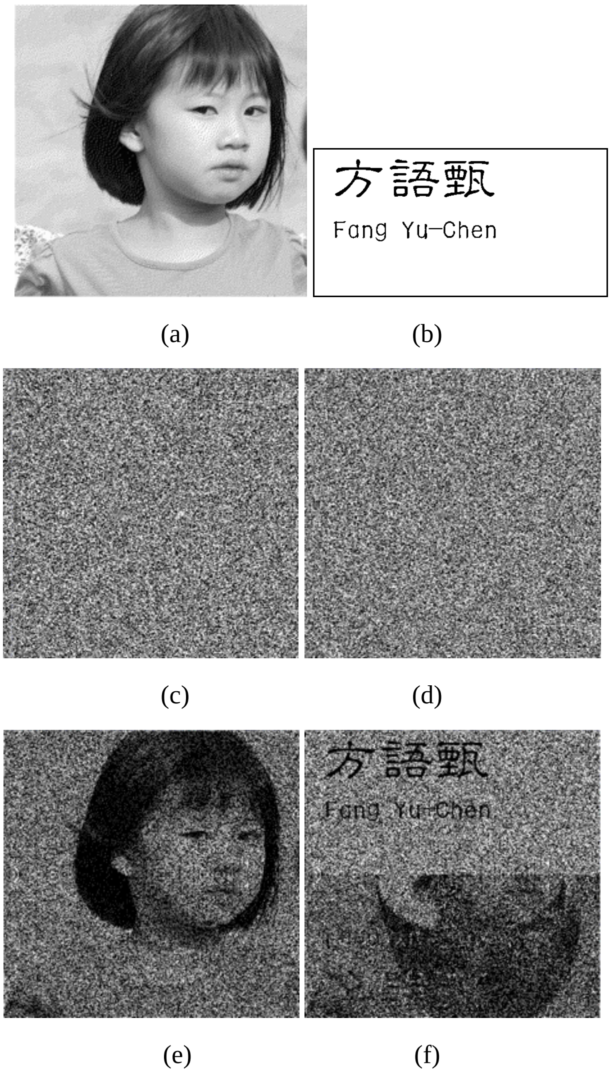


Fig. 6 The experiment result(a) and (b) are original images, (c) and (d) are shares, (e) is the result that stack (c) and (d), (f) is stack (c) and reveries (d)

5. Conclusion and remark

This paper proposed a visual secret sharing method in reversible style without size expansion. The differences between traditional visual secret sharing in reversible style and the proposed method are shown in table.1. Based on the study of Chen and Tsao[8], it is safe and extendable. Compared with the method of Fang[5], there are three important differences. First, the proposed method of this paper does not need to define look-up table. Second, the size of shares and original image is the same. Third, in the method of Ref.5, for the sake of satisfying the property of reversible, the number of basic block pattern are not the same in different stack result case. Although it is impossible to see secret by naked eyes, or guess the secret image with computing device, there still exist probability biases. However, there is no such problem in the proposed method.

Recently, there are some reports that study how to combine visual secret sharing method and digital devices. The reports of, Lukac and Plataniotis[9] and Fang and Lin[10] are good examples. For further study, how to extend the random gird idea in digital multimedia transmission is an interesting topic.

Table.1 Comp arson with exist method

	Block style (Ref.5)	Random grid style (proposed method)
Pixel expanding	yes	No need
Code book	yes	No need

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, 023020

[5] Wen-Pinn 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] Tzung-Her Chen and Kai-Hsiang 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 38 (2005) 767–772.

[10] Wen-Pinn Fang and Ja-Chen 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, 228-234.

Wen-Pinn Fang received his BS degree in mechanical engineering in 1994 from National Sun-Yet-Sen University and his MS degree in mechanical engineering in 1998 from National Chiao Tung University, where he get his PhD degree in Computer Science in 2006 from National Chiao Tung University. His recent research interests include image sharing, pattern recognition,, image processing and e-learning.