ISBN 978-981-11-3671-9
Proceedings of 2017 the 7th International Workshop on Computer Science and Engineering (WCSE 2017)
Beijing, 25-27 June, 2017, pp. 517-525
doi: 10.18178/wcse.2017.06.089

Fault-Tolerant Visual 2-Secrets Sharing Scheme*

Jen-Yu Lin [1], Justie Su-Tzu Juan [2 +]

[1] National Chi Nan University, Master Student, Taiwan.
[2] National Chi Nan University, Professor, Taiwan.

Abstract. In 1994, Noar and Shamir proposed the basic visual secret sharing scheme (also called visual cryptography) to solve a part of the security problem. Visual cryptography is to encrypt a secret image into two meaningless random images, called shares, such that it can be decrypted by stacking these two shares without any calculations. In practice, there would be problems in alignment when staking these two shares by hand. Besides, share two secret images in the same time will enhance the functionality of the scheme. Therefore, this study proposed a new visual secret sharing scheme which encrypt two secret images into two shares in the same time, and it is not necessary to align the shares precisely. Both theoretical analysis and simulation results demonstrate the effectiveness and practicality of the proposed scheme.

Keywords: visual cryptography (VC), tolerant, multi-secret, pixel expansion

1. Introduction

A *secret sharing scheme* (*SSS*) is a method for distributing a secret among several participants in such a way that only qualified subsets of the participants can reconstruct it and unqualified subsets receive no information about the secret. *Visual secret sharing*, *VSS* for short (also called *Visual cryptography*, *VC* for short) was proposed by Noar and Shamir in 1994 [1], which is a kind of secret sharing scheme. The concept of VC is that the secret image S has been encrypted into two random meaningless images G_1 and G_2, called *shares*, and the secret image S can be restored by stacking G_1 and G_2 directly. Different with previous secret sharing scheme technique, when the shares are stacked, the confidential content can be interpreted with human vision directly. That is, a VSS scheme can restore the secret image without additional computation. The technique of the VSS scheme can be applied in many way for the real world, such as lottery. One shared image was posted on the website of the manufacturer, and the customer will get one "random shared image" from the commodity. Every customer can stack their shared image with the posted one, only the special shared image can recover the secret image (such as the words "You Win!" or some special meaningful image) and win the lottery. That will be a good promotion method for the manufacturer.

However, in the Noar and Shamir's method [1], there are two major drawbacks in visual cryptography approach. (1) There is a great pixel expansion between the secret image and the shared images. (2) It needs a storage space to record codebook to cause the cost increased. Kafri and Keren had proposed a *random grid visual secret sharing* (*RG-based VSS*) scheme [2], which regards each pixel on image as a grid and encrypt image by the concept of random variables. So that their scheme will causes no pixel expansion after the encryption, and it needs no codebook. In recent years, more and more researches about VC by using random grids has been proposed, such as references [2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12].

Inspired by the RG-based VSS, Chen et al. proposed a *RG-based multiple visual secret image sharing* (*MVSS* for short) scheme which encrypts more than one secret images into two shares in 2008 [7]. However, Chen et al.'s scheme will restrict the secret images must be square. In order to allow the rectangle images can

+ Corresponding author. Tel.: + 886-492910960#4875; fax: +886-492915226.
E-mail address: jsjuan@ncnu.edu.tw.

be encrypted and still avoid the problems of pixel expansion and codebook redesign, Chang and Juan proposed one RG-based MVSS scheme by shifting random grids, called *OSRG scheme* [3, 4]. In OSRG scheme, two secret images can be encrypted into two shares based on random grads. In the decryption phase, the users reconstruct the secret images by superimposing one of these two shares with the image which obtained by shifting the other share with specific width.

For VC, the secret image can be visually reconstructed with shares, printed on transparencies, and stacked precisely on an overhead projector. A slight misalignment between the shares could dramatically degrade the visual quality of the reconstructed image. If the size of shares is small, the alignment will be difficult. Therefore, some literatures study in this *fault-tolerant* problem (also called *misalignment*). Nakajima and Yamaguchi proposed an extended VSS scheme which enhanced registration tolerance when stacked shares are not aligned perfectly in 2004 [13]. After grey level of a secret image is converted to black and white by using a Half-tone technique, it was encrypted into two random images. The difference is that the encryption pattern of the code book is modified so that there are some space for fault tolerance when reconstructed the secret image. According to the idea of [13], Chen and Juan proposed a new fault-tolerant VSS scheme with no pixel expansion in 2016 [2]. In this paper, we will refer to the ideas of [2] and [4], then design a new visual 2-secret sharing scheme with no pixel expansion, and to achieve the fault-tolerant mechanisms.

The remainder of this paper is organized as follows. In section 2, we will describe above mentioned definitions and technologies in detail. The main proposed scheme, including three steps, was been proposed in Section 3. Section 4 will shows some computer simulation results. Finally, the conclusion has been given in Section 5.

2. Definitions and Related Works

In this section, we will give some basic definition about visual cryptography, and some useful algorithms that will be used in the following section.

2.1. Definitions

The most important purpose of a VSS scheme is to identify hidden secrets directly with the naked-eye. Besides, different with the previous cryptography technology, encryption process of a VSS scheme does not require complex algorithms. That is, a VSS scheme can restore the secret without additional computation. Fig.1 shows the encryption and decryption process model of a VSS scheme.

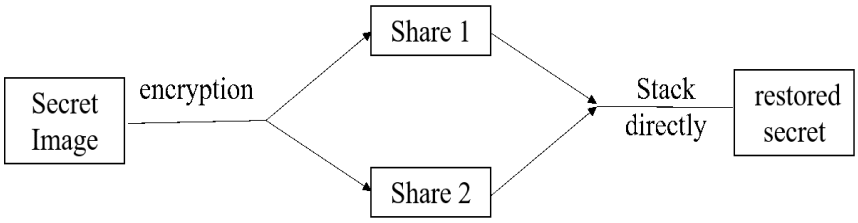
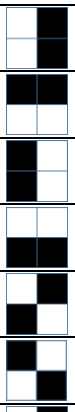
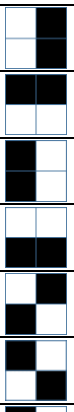
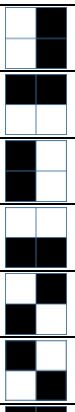
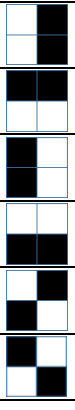


Fig. 1: The encryption and decryption process model of a VSS scheme.

The encryption method of the visual cryptography is to generate two random images G_1 and G_2 from secret image S through the encryption process, and then restore the image by stacking G_1 and G_2. The visual cryptography construction model proposed by Noar and Shamir [1] can be seen as Table 1. Each black or white small grid in a secret image represents the color of the pixel. When encrypting, each pixel in the secret image is sequentially encrypted into a 2×2 matrix. For example, if the pixel of secret image is white, an encryption method is selected from the white code book. The far right column is the result of stack. In the results, we can clearly find that if the secret pixel is superimposed on white, there will be half white and the black is completely black. This can be used to achieve the effect that human's naked eye can identify directly. Also, from the table, we can find that if only getting a random image, the secret of the original image cannot be found. The reason is that half of the pixels of any random image are black and the other are white.

Table 1: The Code Book of Noar and Shamir's scheme

Secret Image	Share1	Share2	Restored Secret
			
			

2.2. Kafri and Keren's Scheme

In 1987, Kafri and Keren proposed three random grid visual secret sharing (RG-based VSS) schemes for black and white image [8]. For understanding the following statement, we have to understand some important notations about random grid listed in this paper in advance. In general, we define S is a secret image with size of $w \times h$ pixels, where w and h are positive integers. Let $S(i, j)$ denote a pixel value of the image S at position (i, j), defined as $S(i, j) = 0$ if $S(i, j)$ is white; 1 if $S(i, j)$ is black. Actually, 0 is *transparent* and 1 is *opaque* when S is printed on a transparency. The opposite value of $S(i, j)$ is denoted as follows.

$$\overline{S(i, j)} = \begin{cases} 0, & \text{if } S(i, j) = 1; \\ 1, & \text{if } S(i, j) = 0, \end{cases} = 1 - S(i, j).$$

Those schemes form the first encrypted image randomly. That is, the probability of the black or white pixels of the generated image is the same. This idea solved the image expansion problem. Define the *transmittance* ($\mathcal{T}$) as the ratio of the number of white pixels to the total number of pixels. Therefore, it is known from the above that the transmittance of the random image is 1/2. A secret image S is encrypted into two shares G_1 and G_2. Let r_i be a pixel in G_i for i = 1, 2. The resulting value of the overlapped pixels $r_1$and r_2 will be $r_1 \oplus r_2$, where $\oplus$ stands for the Boolean "OR" operation. All results when stacking any two pixels together are shown in Table 2.

Table 2: Results for Stacking Two Different Pixels Together

r_1	r_2	$r_1 \oplus r_2$
0	0	0
0	1	1
1	0	1
1	1	1

The following algorithm is one of those three encryption algorithms proposed by Kafri and Keren [8]. Table 3 shows the transmittance of Algorithm KK1.

Algorithm KK1

Input: S // the secret image.

Output: (G_1 , G_2) // two shares.

Generate a $w \times h$ random grid G_1

for ($i = 0$; $i < w$; i ++)

for ($j = 0$; $j < h$; j ++)

if ($S(i, j) == 0$)

$G_2(i, j) = G_1(i, j)$;

else

$G_2(i, j) = \overline{G_1(i, j)}$;

output (G_1 , G_2).

Table 3: The Transmittance of the Algorithm KK1

Secret	Probability	r_1	r_2	$r_1 \oplus r_2$	$\mathcal{T}(r_1 \oplus r_2)$
□	1/2	□	□	□	1/2
	1/2	■	■	■	
■	1/2	■	□	■	0
	1/2	□	■	■	

2.3. Chen and Juan's Scheme

In 2004, Nakajima and Yamaguchi proposed a visual secret sharing scheme to achieve fault tolerant mechanism [13]. They expanded the secret image, and make random image of Noar and Shamir's code book become the diamond pattern, one large and one small. As a result, if there is a little deviation when stacking, one can still recognize the original color (black/white) of the secret image. This method will makes secret image can still be identified under the condition of a little deviation when stacking.

In 2016, Chen and Juan proposed a new fault-tolerant VSS scheme with no pixel expansion [2]. The main concept of that algorithm is as follows. First, taking $n \times n$ pixels as a unit, the image is divided into several units. In the first generated share, each unit is randomly chosen from the patterns they designed. For the generation of the second share, the number of black and white pixels in each unit on the original secret image needs to be counted individually. This will be used to select the suitable pattern according to the pattern of the first share for the same unit. Run the steps sequentially and repeatedly until the second share is generated. Taking the idea of Nakajima and Yamaguchi's scheme as a reference [13], they design the special patterns for the main encryption scheme and apply them to the Algorithm KK1 [8]. Chen and Juan design the fault-tolerant VSS schemes by taking $n \times n$ pixels as a unit, for n = 3, 4, 5 or 6. In this paper, we will set n = 6 and use their designed patterns for encryption scheme, which is shown in Tables 4.

Chen and Juan also analyze the transmittance when two shares are not stacked correctly. Because the pattern of each unit is symmetric, the analysis results are all equal when two units are stacked by shifting one pixel to the right, left, up or down. Table 5 gives the transmittance analysis for stacking two units when n = 6 in [2].

2.4. Multiple-Secret Sharing Scheme

Chen et al. propose an algorithm that encrypts two images simultaneously to obtain two shares of confidential images, when superimpose directly can obtain the first secret image [7]. The second segment will rotate 90 °, 180 °, or 270 ° and then superimpose the first fragment, will receive the second secret image.

Table 4: The Designed Patterns for n = 6 in [2]

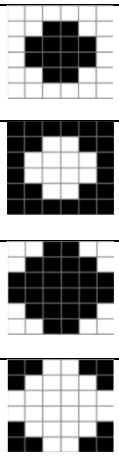
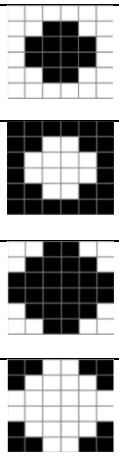
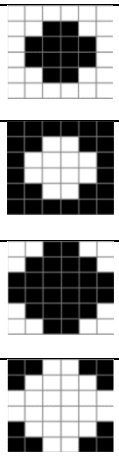
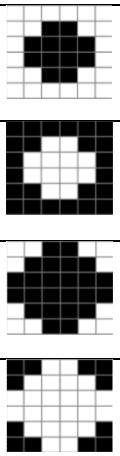
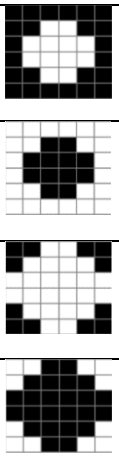
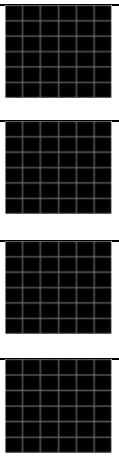
Image	G_1	G_2	Stack	Image	G_1	G_2	Stack
□				■			

Table 5: The Transmittance Analysis for n = 6 in [2]

6 × 6	Stack	Shift 1 pixel	Shift 2 pixel	Shift 3 pixel	Diagonal Shift 1 pixel
□	1/2	50/144	42/144	38/144	1189/4608
■	0	25/144	36/144	33/144	422/4608

Although Chen et al.'s scheme [7] can securely encrypt two secrete images, but the size of the encrypted image must be limited as a square (such can be superimposed by rotating one share). Besides, the second restored secrete image has distortion 1/4 in their scheme, where *distortion* means the number of pixels which not be encrypted over the number of all pixels of the secret images. Therefore, Chang and Juan proposed some new schemes to improve it, such as Algorithm 6 in [4], we called RSRG scheme in this paper. Their schemes uses the concept of moving horizontally to substitute for rotation. The motion of moving horizontally does not need to fix the size of the secret image to be square, so that the first restrictions question will be direct solved. This method can also decide the rate of the pixel which need be randomly selected by user. Hence, the second question also can be improved.

In the RSRG scheme, the input are two images S_A, S_B with the size of $m \times n$ pixels, and integer k is selected according to the width of user want to move. G_1 will be moved 1 / k pixels horizontally to recover the second image. The quantity of distortion on restored images is defined as $D(M)$. The authors show that D(RSRG) is 1 / (2k). Before describing the details of the encoding process, the related functions are defined as follows:

Definition 1: *Random*( ): $X \leftarrow$ *Random*(.), X is the output of the function *Random*(.), which randomly assigns a pixel value 0 or 1.

Definition 2: $f_{RSP}(.)$: $Y \leftarrow f_{RSP}(Z)$, the position Y of a pixel is the output of the function $f_{RSP}(.)$ with the inputs image Z, where $f_{RSP}(.)$ is that randomly select a pixel of Z, and output the position of this pixel.

Definition 3: $\overline{f}_{RG}(.) : X \leftarrow \overline{f}_{RG}(Y, Z)$, the pixel value X is the output of the function $\overline{f}_{RG}(.)$ with the input pixel values Y and Z, where $\overline{f}_{RG}(.)$is the function based on the Algorithm KK1, which inputs a pixel value Z of share at some position (i, j) and a pixel value Y of the secret image at the same position (i, j), then outputs the other pixel value X of the other share at the same position (i, j).

The detail of the RSRG scheme shows as follows.

Algorithm f_{RG}:

Input: The pixel of secret image $S_t(i, j)$. // $t = A$ or B

Output: The pixel of share $G_1(i, j)$ and $G_2(i, j)$.

$G_1(i, j)$ = *Random*(0, 1) // Randomly assign a pixel value 0 or 1

If ($S_t(i, j)$ == 0) then

$G_2(i, j) = G_1(i, j)$;

else

$G_2(i, j) = \overline{G_1(i, j)}$.

Procedure OSRG($S_A(i, j)$, $S_B(i, j)$, p)

$G_1(i, j) || G_2(i, j) \leftarrow f_{RG}(S_A(i, j))$

for (int $k = 1$; $k <= p - 1$; k ++)

$G_2((i + m*k/p), j) \leftarrow \overline{f}_{RG}(S_B((i + m*(k - 1)/p), j), G_1((i + m*(k - 1)/p), j))$;

$G_1((i + m*k/p), j) \leftarrow \overline{f}_{RG}(S_A((i + m*k/p), j), G_2((i + m*k/p), j))$.

Algorithm RSRG

Input: The secret images S_A and S_B and the positive integer p is according to the distortion one want.

Output: The shares G_1 and G_2.

Repeat

Randomly select $A' = A$ or B, $B' = \{A, B\} \setminus \{A'\}$;

$(i, j) \leftarrow f_{RSP}(S_{A'})$;

Procedure **OSRG**($S_{A'}(i, j)$, $S_{B'}(i, j)$, p);

Until all the pixels of G_1 and G_2 are generated.

3. Main Ideal and Algorithm

We propose a scheme to encrypt two secret images by shifting random grids, which also can solve the problems about the fault-tolerant when decrypting the secret images. This study is divided into three parts: scale-down, encryption, and tolerance. S is secret image with the size of $m \times n$ pixels. First, the original image S is partitioned into $m/6 \times n/6$ units, where the size of each unit is 6×6 pixels. Then, we forms a resized image S' with size of $m/6 \times n/6$ pixels. We count the numbers of white and black pixels in each unit of the original secret image S separately, then the larger one will determine the color of the corresponding pixel of S'. Note that, if m or n is not the multiple of 6, we can add some white pixels in the most right and/or the most down of the secret image S.

As the RSRG scheme [3, 4], the input of our scheme are two images S_A, S_B with the size of $m \times n$ pixels, and integer k is selected according to the width of user want to move. By the Algorithm Scale-Down, we will get two resized images S'_A, S'_B with the size of $m/6 \times n/6$ pixels. According to the RSRG scheme, we will get two shares G'_1 and G'_2 with the size of $m/6 \times n/6$ pixels. Because of expecting to extend the ability of tolerance, we use the idea of the encryption method proposed by Chen and Juan [2], to converse each pixel of G'_1 and G'_2 into the corresponding unit of [2] for $n = 6$. Then two shares G_1 and G_2 with the size of $m \times n$ pixels without any pixel expansion will be get. The following is our algorithm.

Encryption phase:

Algorithm Scale-Down

Input: The original secret image S with size $m \times n$ pixels.

Output: The scaled down image S' with size $m/6 \times n/6$ pixels.

```
for (int a = 0; a < m/6; i ++)
    for (int b = 0; b < n/6; j ++)
        count = 0;
        for (int i = 6a; i < 6(a + 1); i ++)
            for (int j = 6b; j < 6(b + 1); j ++)
                if (S(i, j) == 0) then count ++;
        if (count >= 18) then
            S'(a, b) = 0;
        else
```

$S'(a, b) = 1$.

Procedure FTOSRG($S_A(i, j)$, $S_B(i, j)$, p)

$G_1'(i, j) \| G_2'(i, j) \leftarrow f_{RG}(S_A(i, j))$

According to $G_1'(i, j)$, $G_2'(i, j)$, randomly choose one corresponding pair of units in Table 4 to $G_1(a, b)$ and $G_2(a, b)$ for $6i \le a < 6(i + 1)$, $6j \le b < 6(j + 1)$.

for (int $k = 1$; $k <= p - 1$; k ++)

$G_2'((i + m*k/p), j) \leftarrow \overline{f}_{RG}(S_B((i + m*(k - 1)/p), j),\ G_1'((i + m*(k - 1)/p), j))$;

$G_1'((i + m*k/p), j) \leftarrow \overline{f}_{RG}(S_A((i + m*k/p), j),\ G_2'((i + m*k/p), j))$;

According to $G_1'((i + m*k/p), j)$, $G_2'((i + m*k/p), j)$, assign corresponding unit to $G_1(a, b)$ and $G_2(a, b)$ for $6(i + m*k/p) \le a < 6((i + m*k/p) + 1)$, $6j \le b < 6(j + 1)$.

Algorithm Fault-Tolerant Visual 2-Secret Sharing Scheme

Input: The secret images S_A and S_B and the positive integer p is according to the distortion one want.

Output: The shares G_1 and G_2.

$S_A' =$ **Scale-Down**(S_A);

$S_B' =$ **Scale-Down**(S_B);

Repeat

Randomly select $A' = A$ or B, $B' = \{A, B\} \setminus \{A'\}$;

$(i, j) \leftarrow f_{RSP}(S_{A'})$;

Procedure **FTOSRG**($S_{A'}'(i, j)$, $S_{B'}'(i, j)$, p);

Until all the pixels of G_1 and G_2 are generated.

Decryption phase:

Upon collecting these two share images G_1 and G_2, the users can easily restore the first secret image S_A by directly superposing G_1 and G_2. The second secret image S_B can be restored by superposing G_1 and G_3, where G_3 is obtained from G_2 by moving horizontally $1/p$ width.

4. Experimental Results

The secret images used in this experiment are binary images, and we use the method proposed in the previous section to conduct three simulations in this section. For the first two similations, the size is 600×600 pixels and $p = 4$ or 20, respectively. The experimental results are shown in Table 6 and 7. In both cases, these two resulting share G_1 and G_2 have no any pixel expansion. The first secret is restored by directly superposing G_1 and G_2. The second secret is restored by superposing G_1 and G_3, where G_3 is obtained from G_2 by moving horizontally $1/p$ ($p = 4$ in Table 6, and $p = 20$ in Table 7) width. The first restored secret shift right 1 pixel means G_1 shift right 1 pixel before superposing G_1 and G_2. The second restored secret shift right 1 pixel means G_1 shift right 1 pixel before superposing G_1 and G_3. The first restored secret shift upper right 1 pixel means G_1 diagonal shift (upper 1 pixel and right 1 pixel) before superposing G_1 and G_2. The second restored secret shift upper right 1 pixel means G_1 diagonal shift (upper 1 pixel and right 1 pixel) before superposing G_1 and G_3.

Table 8 is the xeperimental resul for the secret images with size 600×960 pixels and $p = 20$. Those two resulting share G_1 and G_2 have the same size with the original secret images, without any pixel expansion. The first secret is restored by directly superposing G_1 and G_2. The second secret is restored by superposing G_1 and G_3, where G_3 is obtained from G_2 by moving horizontally $1/p = 1/20$ width. As the previous Tables, the first restored secret shift right 1 pixel means G_1 shift right 1 pixel before superposing G_1 and G_2. The second restored secret shift right 1 pixel means G_1 shift right 1 pixel before superposing G_1 and G_3. The first restored secret shift upper right 1 pixel means G_1 diagonal shift (upper 1 pixel and right 1 pixel) before superposing G_1 and G_2. The second restored secret shift upper right 1 pixel means G_1 diagonal shift (upper 1 pixel and right 1 pixel) before superposing G_1 and G_3.

Table 6: p = 4, the size of secret images is 600 × 600 pixels

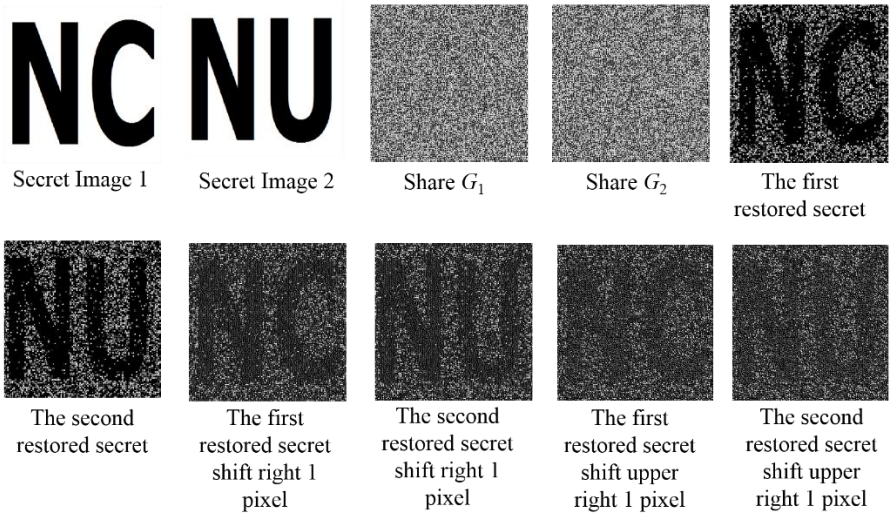


Table 7: p = 20, the size of secret images is 600 × 600 pixels

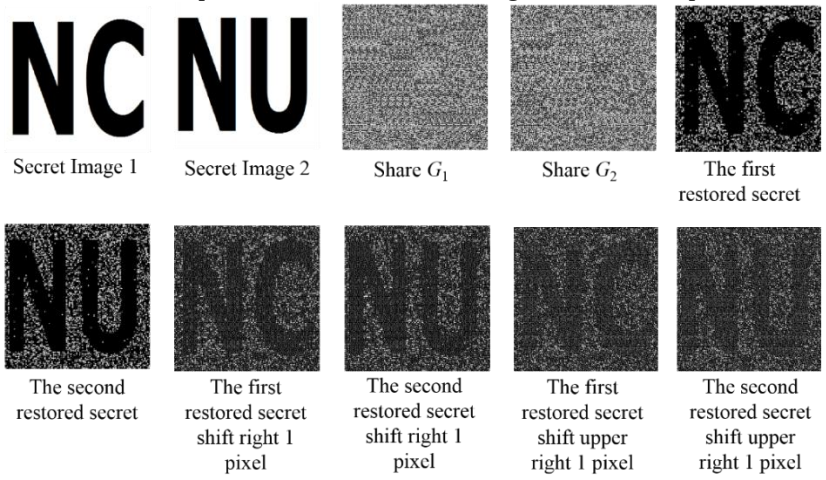
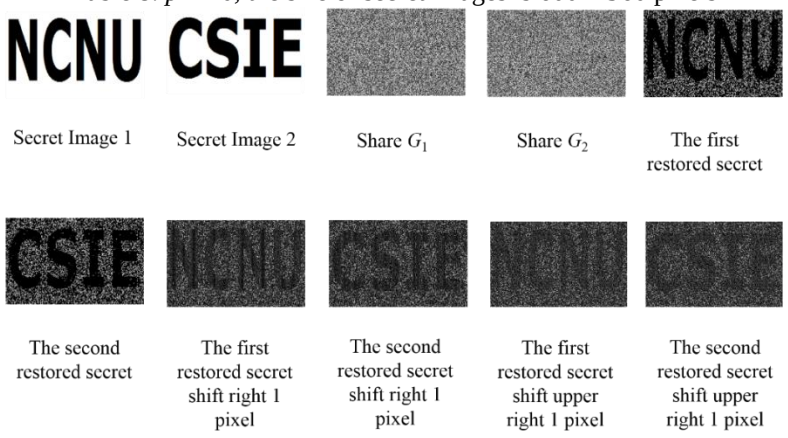


Table 8: p = 20, the size of secret images is 600 × 960 pixels



From above experimental results, we can believe that the information in the secret images can also be understand even if those two shares are not superposing exactly. The distortion of these two restored image is 1/(2p) according to [3, 4], so one can choose suitable p by themselves. It shows that the proposed schemes are effective and our analysis is valid.

5. Conclusion and Expect

In this paper, we successfully propose a fault-tolerant visual secret sharing scheme for sharing two secret images. Two secrets can be hidden into two shares, the distortion spread to those two shares evenly and those two secrets can be recovered successfully. When stacked shares are not aligned perfectly at the time of

reduction, we still can recover the original information and achieve the fault-tolerant of visual cryptography mechanism that make it more practical. In the future, we want to design a VSS scheme which can hide more than two secret images into two shares, and also achieve the fault-tolerant mechanism.

6. Acknowledgment

This research was supported in part by the Ministry of Science and Technology of the Republic of China under grant MOST 105-2115-M-260-001.

7. References

[1] M. Naor and A. Shamir. Visual cryptography. In: *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer Berlin Heidelberg, 1994. pp. 1-12.

[2] J. S.-T. Juan, Y.-C. Chen, and S. Guo, Fault-tolerant visual secret sharing schemes without pixel expansion. *Applied Sciences*. 2016, **6** (1): Article 18. doi: 10.3390/app6010018

[3] J. J.-Y. Chang. *Visual Multi-Secret Image Sharing Schemes by Shifting Random Grids*. Master Thesis, National Chi Nan University, 2012

[4] J. J.-Y. Chang and J. S.-T. Juan. Multi-VSS Scheme by Shifting Random Grids. *Proc. of World Academy of Science, Engineering and Technology*. Tokyo, Japan: International Journal of Computer, Electrical, Automation, Control and Information Engineering. 2012, pp. 1277-1283.

[5] L.-C. Chen. *A Study on Quality-Enhanced Visual Multi-Secret Images Sharing Schemes*. Master Thesis, National Chi Nan University, 2014.

[6] T.-H. Chen, K.-H. Tsao and Y.-S. Lee. Yet another multiple-image encryption by rotating random grids. *Signal Processing*. 2012, **92** (9): 2229-2237.

[7] T.-H. Chen, K.-H. Tsao, and K.-C. Wei. Multiple-Image Encryption by Rotating Random Grids. In: *Eighth International Conference on Intelligent Systems Design and Applications*. 2008, pp. 252-256.

[8] O. Kafri and E. Keren. Encryption of pictures and shapes by random grids. *Optics letters*. 1987, **12** (6): 377-379.

[9] C.-L. Liu, W.-J. Tsai, T.-Y. Chang, C.-C. Peng, and P.-S. Wong. Meaningful share generation for (2, 2)-multiple visual secret sharing scheme without pixel expansion. *The Computer Journal*. 2015, **58** (7): 1598-1606.

[10] S. J. Shyu. Image encryption by random grids. *Pattern Recognition*. 2007, **40** (3): 1014-1031.

[11] D. Wang, L. Dong, and X. Li. Towards shift tolerant visual secret sharing schemes. *IEEE Transactions on Information Forensics and Security*. 2011, **6** (2): 323-337.

[12] M. Nakajima and Y. Yamaguchi. Extended visual cryptography for natural images. *Journal of WSCG*. 2002, **10** (1-2): 303-310.7

[13] M. Nakajima and Y. Yamaguchi. Enhancing registration tolerance of extended visual cryptography for natural images. *Journal of Electronic Imaging*. 2004, **13** (3): 654-662.