Towards Shift Tolerant Visual Secret Sharing Schemes without Pixel Expansion

Justie Su-Tzu Juan[1, a], Yung-Chang Chen[1] and Song Guo[2]

[1]*Department of Computer Science & Information Engineering, National Chi Nan University, 54561 Nantou, Taiwan*
[2]*School of Computer Science and Engineering, The University of Aizu, 965-8580 Fukushima, Japan.*

Abstract: Naor and Shamir proposed the visual cryptography in 1995, they encrypted secret image into two meaningless random images, called shares, and it can be decrypted by human vision without any calculations. However, there would be problems in alignment when these two shares are staked by hand in practical. Therefore, this paper presents the fault-tolerant schemes of stacking two shares which are acquired from secret image encryption without pixel expansion. The main idea of these schemes is combining several pixels to be a unit, then encrypting every unit into a specific combination of pixels. It makes visual secret sharing scheme more practical.

1 Introduction

In 1995, Noar and Shamir proposed *visual cryptography* (VC for short), which is a way to encrypt one secret image and it can decoded by human vision without any calculation [11]. The concept is encrypting secret image S into two meaningless random images, called *share* (also called *sheet* or *random grid*), G_1 and G_2, one can be seen as a cipher text and the other is key to it. Stacking them is the only way to restore the hidden secret. *Random grid visual secret sharing* (VSS for short) which is made by [6] receives more attention in recent years, such as references [3, 4, 5, 9, 12, 14] are visual cryptography algorithms, designed on the basis of random grid. In the method proposed by Kafri and Keren, taking each *pixel* as a grid on the image and apply the concept of random variables to encrypt images.

For VSS, 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 are small, the alignment will be difficult. Therefore, some literatures study in this problem, such as [1, 2, 6, 8, 11, 13, 15]. Nakajima and Yamaguchi propose proposed an extended VSS scheme which enhanced registration tolerance when stacked shares are not aligned perfectly in 2004 [10]. Transfer the secret image into black and white values with half-tone technique, and then encrypt into two random images, the difference with other methods is that one of the random images becomes large diamond pattern and the other one is smaller so there will be some space for fault tolerance when stacking the shares. However, their scheme will make the pixel expansion. We will refer to their ideas to design the visual secret sharing scheme to achieve fault tolerance mechanism without pixel expansion.

The rest of this paper is organized as follows. Section 2 will detail techniques mentioned above. Section 3 discuss the major findings, we have designed three VSS schemes that achieve better fault tolerance. In Section 4, the fault tolerance result acquired from computer simulation of various schemes are mentioned in previous section will be presented. Finally, our conclusions and references.

2 Related works

2.1 Visual cryptography concepts

Difference with previous secret sharing scheme technique, when the shares are stacked, the confidential content can be interpreted with human vision directly. That is, a VC scheme can restore the secret without additional computational calculation. Figure 1 shows the encryption and decryption process model of a VC scheme.

[a] Corresponding author: jsjuan@ncnu.edu.tw

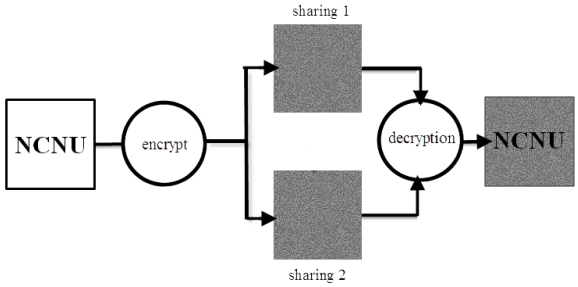


Figure 1. VC encryption and decryption process model.

For understanding the following sections, we have to understand some important notations about random grid which listed in this section in advance. In general, we define S is a secret image with size w pixels by h pixels for positive integers w and h.

Definition 1: Let $S(i, j)$ denote a *pixel value* of the secret image S at the position (i, j), where

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

Actually, 1 is opaque and 0 is transparent when S is printed on transparencies.

Definition 2: Let $S(i, j)$ denote a pixel value of the secret image S at the position (i ,j), then

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

Definition 3: *Transmittance* (T) is defined as proportion of white pixels to total pixels.

A secret image S is encrypted into two shares, one is G_1 and the other is G_2. r_i is a pixel in G_i; $\oplus$ stands for Boolean "OR" operation, so the output of $r_1 \oplus r_2$ means the result pixel of pixel r_1 overlap pixel r_2. All results when stacking any two pixels together are shown as Table 1.

Table 1: 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

2.2 Random grid encryption algorithm

In 1987, Kafri and Keren proposed three encryption algorithms for halftone images. Transparent (white) is defined as 0 and opaque (black) is 1, the *random grid* obtained from determining each pixel by flipping a coin, it means that the probability of getting black or white pixel is the same. Therefore, the transmittance of random image is 1/2. Kafri and Keren [6] proposed three different algorithms to encrypt a secret image S with the size $w \times h$ pixels for some positive integers w and h into two shares, G_1 and G_2 with the same size. We list the most important one as follow:

Algorithm KK:
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
      $G_2[i][j] = 1 - G_1[i][j]$;
Output (G_1, G_2)

Table 2. The Transmittance of KK Algorithm

S	Probability	G_1	G_2	$G_1 \oplus G_2$	$T(G_1 \oplus G_2)$
□	1/2	□	□	□	1/2
	1/2	■	■	■	
■	1/2	□	■	■	0
	1/2	■	□	■	

2.3 The concept of fault tolerance

Naor and Shamir proposed an extended visual secret sharing scheme in 1995 [11]. When they encrypt the secret image, each pixel on the secret image will be expand into m subpixels. Nakajima and Yamaguchi proposed an extended visual secret sharing scheme to show that the fault tolerance mechanism can be achieved in 2004 [10]. They encrypted the secret image into two expand shares. Each pixel in the secret image will produce a 7 × 7 subpixels which become a diamond-like pattern, one is small and the other is big, as shown in Figure 2. Even though there are slight deviation when stacking, primary color (black or white) still can be restore. Their design will allow some space for fault tolerance. However, due to the expansion, the size of the restored image will be 49 times of the original secret image. Hence, this paper will focus on halftone secret image, designing the VSS scheme using the idea of the method mentioned above, for towards shift tolerance without pixel expansion.

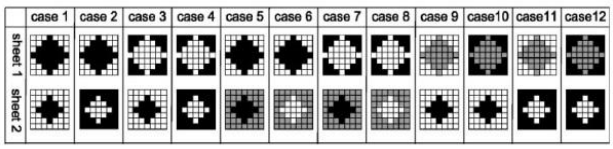


Figure 2. The patterns in Nakajima and Yamaguchi's scheme. This figure come from [10].

3 Main result

The main concept of our algorithm is as follows. First, taking $n \times n$ pixels as a unit, the image is divided into several units. Next, basis on the pattern we designed,

randomly choose one pattern for each unit, and generate the first share as combine those patterns. For the generation of second share, the amount of black and white pixel in each unit on original secret image need to be counted individually. Then identify which one is more than the other, selecting the suitable pattern according to the pattern of first share for the same unit. Run the steps sequentially and repeatedly, and second share will be generated.

Take the idea of Nakajima and Yamaguchi's scheme as a reference [10], we design the special patterns for the main encryption scheme and apply the KK algorithm [6]. With $n \times n$ pixels as a unit, we design the fault-tolerant VSS schemes n is 3, 4 or 5. After computing, analysis and screening, the final design of the patterns for encryption schemes as shown in Tables 3, 4 and 5, for n is 3, 4 and 5, respectively.

Table 3. The Designed Patterns for $n = 3$

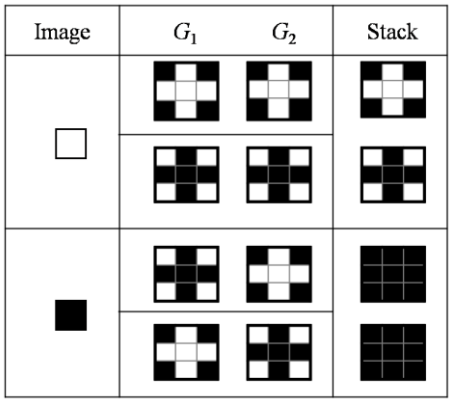


Table 4. The Designed Patterns for $n = 4$

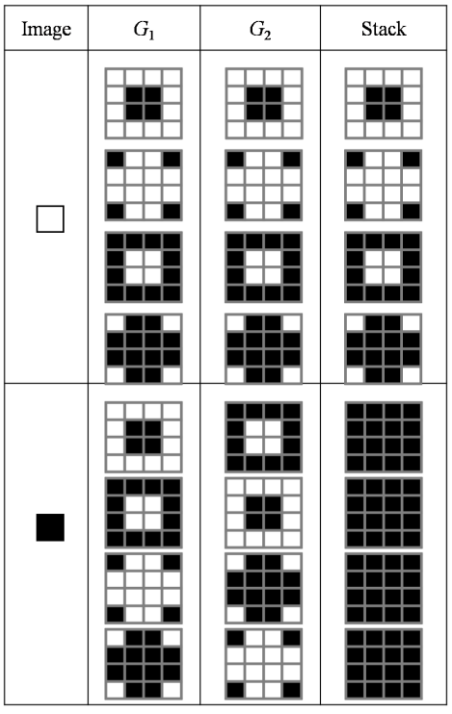
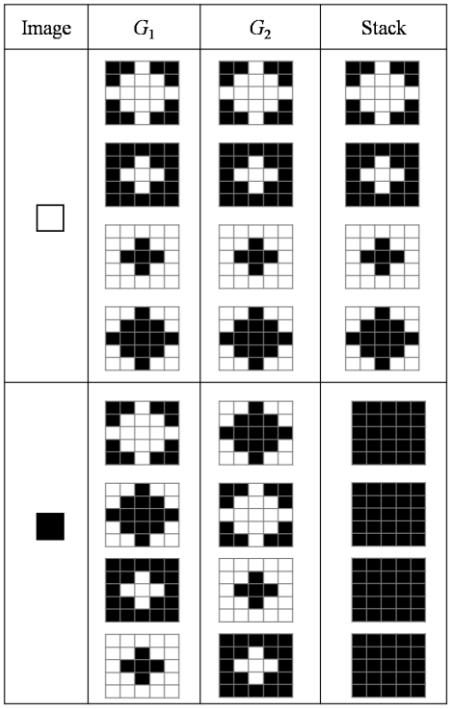


Table 5. The Designed Patterns for $n = 5$



4 Experimental results

In this section, we use the scheme proposed in previous section to perform the simulation, the experimental results are shown as Figures 3-5 for n is 3, 4, or 5, respectively. The secret image we used in the experiment is 300 × 300 pixels halftone image. Because there is no pixel expansion, the size of two shares are also 300 × 300 pixel after encryption. Information on the restored image can be identified clearly after stacking the resulting two shares directly, or one of the share with 1 or 2 pixel shift. It shows that the effectiveness that we analysis in last section is correct as we expect.

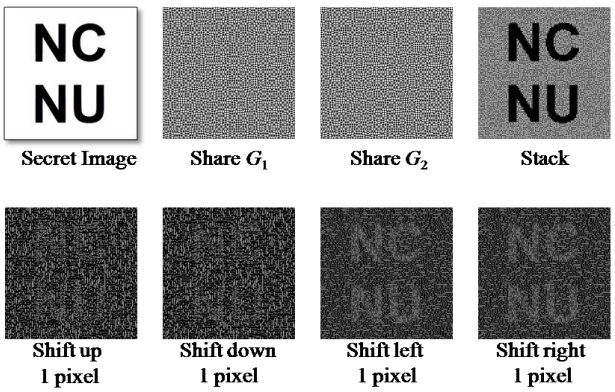


Figure 3. The experimental results for $n = 3$.

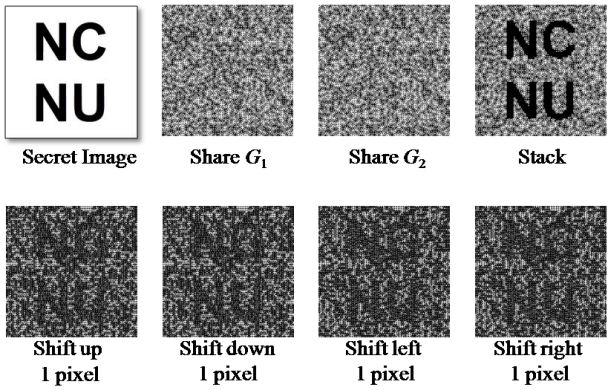


Figure 4. The experimental results for $n = 4$.

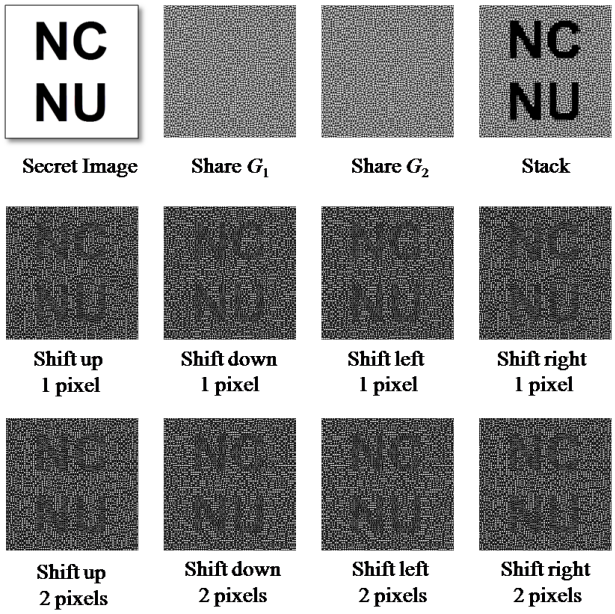


Figure 5. The experimental results for $n = 5$.

5 Conclusion

This paper presents that a visual secret sharing scheme can be designed with fault tolerance mechanism and without pixel expansion; the original information can be identified even if we stack the two resulting shares not perfectly. We expect further study for designing the encryption scheme with n is 6 or more. However, due to along the value of n is greater, the distortion of the graph will be much more. So the value of n has its upper limitation. Besides, improve the current algorithms for increasing the difference of the transmittance between black and white areas and reducing the distortion. So that the restored image could be more clearly. That is our goal as well.

Acknowledgments

The authors would like to thank the Ministry of Science and Technology of the Republic of China for financially supporting this research under Contract No. MOST 104-2918-I-260-004.

References

1. C. Blundo, A. Santis, Visual cryptography schemes with perfect reconstruction of black pixels. *Computer Graph* **22**(4): 449-455 (1998).
2. C. Blundo, A. Bonis, A. Santis, Improved schemes for visual cryptography. *Designs, Codes and Cryptograph* **24**: 255-278 (2001).
3. J. J.-Y. Chang, J. S.-T. Juan, Multi-VSS scheme by shifting random grids. In *Proc. World Academy of Science, Engineering and Technology*, **65**, Tokyo, Japan, 29-30 May 2012: 1277-1283 (2012).
4. L.-C. Chen, *Multi-Secret Images Sharing Schemes*, Master Thesis: National Chi Nan University (2014).
5. T.-H. Chen, K.-H. Tsao, K.-C. Wei, Multiple-image encryption by rotating random grids. In *Intelligent Systems Design and Applications, 2008. ISDA'08. Eighth International Conference on* **3**: 252-256 (2008): IEEE.
6. O. Kafri, E. Keren, Encryption of pictures and shapes by random grids. *Optics Letters* **12**(6): 377-379 (1987).
7. K. Kobara, H. Imai, Limiting the visible space visual secret sharing schemes and their application to human identification. In *Advances in Cryptology—ASIACRYPT'96* 185-195 (1996): Springer Berlin Heidelberg.
8. F. Liu, C. K. Wu, X. J. Lin, The alignment problem of visual cryptography schemes. *Designs, Codes and Cryptography* **50**(2): 215–227 (2009).
9. M. Nakajima, Y. Yamaguchi, Extended visual cryptography for natural images. *Journal of WSCG* **10**(2): 303-310 (2002).
10. M. Nakajima, Y. Yamaguchi, Enhancing registration tolerance of extended visual cryptography for natural images. *Journal of Electronic Imaging* **13**(3): 654-662 (2004).
11. M. Naor, A. Shamir, Visual cryptography. In *Advances in Cryptology—EUROCRYPT'94* 1-12 (1995): Springer Berlin Heidelberg.
12. S. J. Shyu, Image encryption by random grids. *Pattern Recognition* **40**: 1014- 1031(2007).
13. E. R.Verheul, H. C. Van Tilborg, Constructions and properties of k out of n visual secret sharing schemes. *Designs, Codes and Cryptography* **11**(2): 179-19(1997).
14. D. S. Wang, L. Dong, X. Li, Towards shift tolerant visual secret sharing schemes. *IEEE Transactions on Information Forensics and Security* **6**(2): 323-337 (2011).
15. C. N. Yang, A. G. Peng, T. S. Chen, MTVSS: Misalignment tolerant visual secret sharing on resolving alignment difficulty. *Signal Process* **89**: 1602-1624 (2009).