GCEAS-0059
A Meaningful Visual Multi-Secret Sharing Scheme by Random Grids

Bo-Yuan Hunag, Justie Su-Tzu Juan *
Department of Computer Science and Information Engineering, National Chi Nan University, Puli, Nantou, Taiwan
* E-mail: jsjuan@nucn.edu.tw

Abstract

Recently, the development of network technology was very soon. In order to ensure the secret images are not been stolen when transmitting, it must be encrypted. Visual secret sharing (VSS) is a kind of the secure communication technology which main concept is that the secret image can be encrypted into some shares, and restore it by human vision through superimposing those shares. Random grid is an important technique for VSS. Without any computation in decrypting phase and pixel expansion, many scholars consider it as the better skill for the VSS and put into research. Some scholars proposed high-capacity multi-secret sharing schemes that can achieve encrypting many images in the same time, whereas the problem of shares management has arisen. Others proposed meaningful visual multi-secret sharing schemes still have the restrictions on number of secret images. Therefore, this paper proposed a new meaningful visual multi-secret sharing scheme able to solve the problem arose from the previous two schemes.

Keywords: Visual Secret Sharing, random grids, pixel expansion, meaningful

1. Introduction

There are many researches about the visual secret sharing (VSS, for short) have been proposed, that means secret images can be restored directly by human vision through superimposing the shares. The main technologies are visual cryptography (VC) and random grid (RG). In 1987, Keren and Kafri [10] proposed the method of random grid which 0 represents white and 1 represents black. With this scheme, binary images can be encrypted into two same sizes of random grids. The study of visual cryptography proposed by Naor and Shamir [12] in 1995; however, it need to construct codebook and has problems of pixel expansion. Therefore, the shares will be bigger than the original secret images, and be associated with the increased cost for transmitting the image and the waste of storage space.

In order to overcome the two major shortcomings of visual cryptography, the technologies of random grid have developed in recent years [1-9] [13-14]. In 2008, Chen et al. [9] proposed a multi-VSS scheme used random grid that encrypts two secret images into two shares. In 2010, Chen et al. [5] proposed a method that can encrypt more than two secret images. An extended random grid VSS scheme proposed by Chen et al. [7] that achieves to encrypt four secret images

into two shares. Although these studies mentioned above have their own unique encryption ideas, they all have the problem of distortion.

In 2010, Chang et al. [3] proposed another multi-VSS used random grid which the skill of the encryption and decryption phases are similar to [9], and additionally, can adjust the distortion by users. [3] can encrypt two secret images in the same time. First, it divides encryption process into p part, and randomly selects one of the images before each encryption phase. Next, a pixel of that secret image is randomly selected, and it encrypts into two shares. Finally, the steps as above are repeated until all the pixels of two cipher-grids are generated. According to this encryption process, it can reduce the distortion to $1 / 2p$, and improve on the problem of distortion. In 2012, Chang and Juan [4] proposed four schemes which are based on the idea of [3]. One of them can encrypt three secret images in the same time. In 2017, the number of secret images be encrypted can be increased into 6 or even more [2].

In 2014, Liu et al. [11] proposed a method which can encrypt three secret images and two camouflaged images into two shares, and reconstruct the images by directly stacking and rotating one of two shares at 0°, 90°, and 270°, respectively. With the symbols on two shares, it can easily distinguish one from the other.

It can be seen from those literatures that each scheme has its own advantages; however, there are still have the restrictions on the distortion and the number of the secret images in different considerations. Moreover, to improve the drawback of meaningless shares, this paper adapts to encrypt more than two secret images and two camouflaged images into two shares. With this method, not only can overcome the problems as mentioned above, but also increase the efficiency when managing shares.

This paper is organized as follows. Section 2 presents the related work. Section 3 presents the detail of the algorithm. The experimental results are presented in Section 4. Section 5 presents the analysis between the related work and the proposed scheme. Conclusions are given in the final section.

2. Preliminary

The purpose of this paper is to design a new algorithm to overcome the restriction of the number of secret images, reduce the significant distortion, and generate meaningful shares for image management. Section 2.1 reviews the basic random grid algorithms proposed by Kafri and Keren [10]. VMSS scheme and meaningful share generation are described in Section 2.2 and Section 2.3, respectively.

(2.1) Kafri and Keren's Random Grids

In 1987, Kafri and Keren [10] define the random grid of each pixel as either black or white, where 1 presents black and 0 presents white (transparence). Since each pixel is generated by random numbers, the amount of black pixels and white pixels in a random grid can be seen as equal. The results of stacking any two pixels are shown in Table 1. Based on the stacking rules, Kafri et al. propose three different algorithms to encrypt a binary secret image G into two shares R_1 and R_2, as listed following.

Table 1: All the results of stacking two pixels

R_1	R_2	$R_1 \| R_2$
0	0	0
0	1	1
1	0	1
1	1	1

Algorithm: KK1

Generate an $m \times n$ random grid R_1

```
for( int i = 0; i < m; i++)
    for( int j = 0; j < n; j++)
        if( G[i][j] == 0)
            R2[i][j] = R1[i][j];
        else
            R2[i][j] = ¬R1[i][j];
output(R1, R2)
```

Algorithm: KK2

Generate an $m \times n$ random grid R_1

```
for( int i = 0; i < m; i++)
    for( int j = 0; j < n; j++)
        if( G[i][j] == 0)
            R2[i][j] = R1[i][j];
        else
            R2[i][j] = Random(0, 1);
output(R1, R2)
```

Algorithm: KK3

Generate an $m \times n$ random grid R_1

```
for( int i = 0; i < m; i++)
    for( int j = 0; j < n; j++)
        if( G[i][j] == 0)
            R2[i][j] = Random(0, 1);
        else
            R2[i][j] = ¬R1[i][j];
output(R1, R2)
```

(2.2) VMSS Scheme

Visual Multi-Secret Sharing (VMSS) scheme based on the concept of VSS is proposed by Chang et al. [2], it can encrypt N secret images in the same time into two shares. According to their encryption process, it can reduce the distortion to $((N-2)p+1) / Np$. It is approximate to $(N-2) / N$ for big p. Therefore, it can be found that the bigger p is, the lower the distortion will be, and extending this concept to encrypt multiple images. In [2], it numbers images from 0 to $N-1$ and then selects a random pair in (0, 1), (1, 2),…, ($N-2$, $N-1$), ($N-1$, 0) to encrypt until all the shares are generated. The results of shares vary with three algorithms proposed by Kafri and Keren [10] where size 800 × 600 pixels and p = 100, though those algorithms can correctly restore the secret images. On the premise of ensuring the correctness of reconstructed images, it must guarantee that there is no risk to reveal secret messages when generating shares. According to the results in Chang et al. [2], we therefore select the third algorithm (KK3) proposed by Kafri et al. [10] to be the basis of the encryption phase.

(2.3) Meaningful Share Generation

Having more disadvantages on meaningless shares in the aspects of image management and being suspicious, some scholars put the concept of meaningful shares into research. In 2014, Liu et al. [11] proposed a method which not only are the secret images participated in the encryption phase, but also the camouflaged images do. With the square images, they achieve the rotating encryption mechanism. Not encrypting the forth secret image, the marks will appear on the shares. Therefore, in the decryption phase, users can easily restore the first image by stacking two shares directly, and the second (respectively, third) can be recovered by stacking the second share and the first share with rotating clockwise at 90° (respectively, 270°). In the consideration of secret security, the meaningful share will be a better choice compared to meaningless one.

3. Main Results

In this Section, with three basic functions and one procedure, we present the proposed meaningful visual multi-secret sharing scheme (MVMSS scheme) in detail.

Function f_{pixel}

Input: One of the secret images S with size $m \times n$ pixels

Output: The pixel $S(i, j)$ of input secret image

i = Random(0, $m - 1$)

j = Random(0, $n - 1$)

Return $S(i, j)$

Function f_{RG}

Input: The pixel of secret image $S(i, j)$

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

$G_1(i, j)$ = Random(0, 1)

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

$G_2(i, j)$ = Random(0, 1)

else

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

Return $G_1(i, j)$ and $G_2(i, j)$

Function $\bar{f}_{RG}$

Input: The pixel of one share $G_1(i, j)$ and the pixel of secret image $S(i, j)$

Output: The pixel of the other share $G_2(i, j)$

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

$G_2(i, j)$ = Random(0, 1)

else

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

Return $G_2(i, j)$

Procedure $M2RG(S_A(i, j), S_B(i, j), p, b)$

$G_1(i, j) || G_2\left(i + b \times \frac{m}{p}, j\right) \leftarrow f_{RG}(S_A(i, j))$

for (int $k = 0$; $k < p - 1$; k++)

int $b' = (b + k + 1) \bmod N$

if ($k == p - 2$)

$G_2\left(i + b' \times \frac{m}{p}, j\right) = C_2\left(i + b' \times \frac{m}{p}, j\right)$

$G_1\left(i + (k + 1) \times \frac{m}{p}, j\right) = C_1\left(i + (k + 1) \times \frac{m}{p}, j\right)$

else

$$G_2\left(i + b' \times \frac{m}{p}, j\right) \leftarrow \bar{f}_{RG}(S_B\left(i + k \times \frac{m}{p}, j\right), G_1\left(i + k \times \frac{m}{p}, j\right))$$

$$G_1\left(i + (k+1) \times \frac{m}{p}, j\right) \leftarrow \bar{f}_{RG}(S_A\left(i + (k+1) \times \frac{m}{p}, j\right), G_2\left(i + b' \times \frac{m}{p}, j\right))$$

Algorithm MVMSSS

Input: The secret images $S_0, S_1, \ldots, S_{N-1}$ and the camouflaged images C_1, C_2 with size $m \times n$ pixels

Output: The meaningful shares G_1, G_2

Repeat

Randomly select S_A = one of secret images.

$S_A(i, j) \leftarrow f_{\text{pixel}}(S_A)$

Procedure $M2RG(S_A(i, j), S_{A+1}(i, j), p, A)$

Until all the cipher-pixels of two shares are generated

4. Experimental Results

The platform for this experience is Intel(R) Pentium(R) CPU 2117U at 1.80 GHz, Window 10 Professional OS, DEV C++ for programming tool and image processing. There are six experiments using words and images as shown in Fig. 1 and Fig. 5, respectively. By using the proposed scheme, the entire input secret images with size 540 × 540 pixels are used in the first five (respectively, the last one) experiments for p = 10 (respectively, p = 20). In the first and second experiments, the experiment results are shown in Fig. 2 and Fig. 6, respectively. We performed the similar experiments of [11] as shown in Fig. 3, 4 and Fig. 7, 8. In the third and the fourth experiments, we achieved to encrypt four secret images and two camouflaged images into two meaningful shares as shown in Fig. 9 and Fig. 10. In the last two experiments, we apply algorithm KK1 to be the basis of the encryption phase and use the same images of the first and the third images and the complementary images of the second and fourth images in experiment 3, and experiment 4. Additionally, in the last experiment , we replace $p = k - 2$ with $p \geq k - 3$ in procedure *M2RG*, that means it sacrifices two encryption phases for the sake of more clear share images. The results are shown in Fig. 11 and Fig. 12, respectively.

5. Comparison with the Related Schemes

Compare the Fig. 2 (respectively, Fig. 6) with Fig. 4 (respectively, Fig. 8), not only the restored images are more clear than Liu et al.'s [11], but also the shares do. Additionally, our scheme can encrypt more than three secret images, and we can find that the clarity of images in Fig. 2 (respectively, Fig. 6) and Fig. 9 (respectively, Fig. 10) are almost the same. In consideration of input images like experiment 5 and experiment 6, we can adjust the basis of the encryption phase from algorithm KK3 to KK1. Moreover, for the sake of the quality of shares, we can sacrifice more than one encryption phase as presented in experiment 6.

With no code books required, no pixel expansion generated, multiple shares encrypted, and meaningful shares, the algorithm has more security on shares, flexibility on the number of the secret images, and efficiency on image management. Moreover, our scheme encrypts images by shifting rather than rotating random grids so that any rectangle images can be the input images. The comparison between the related schemes and the proposed scheme is given in Table 2.

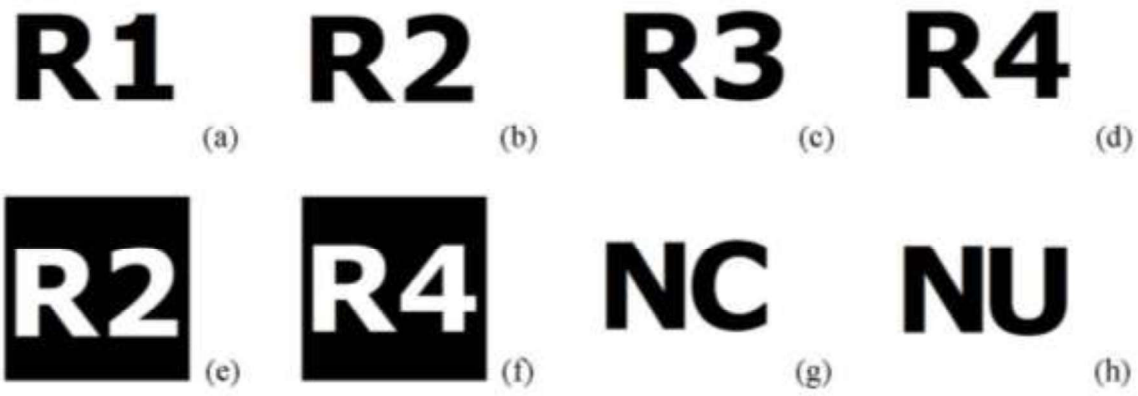

Fig. 1: Original images of experiment 1 (without (d) ~ (f)), experiment 3 (without (e), (f)) and experiment 5 (without (b), (d)). (a) Secret image S_1. (b) Secret image S_2. (c) Secret image S_3. (d) Secret image S_4. (e) Secret image S_5. (f) Secret image S_6. (g) Camouflaged image C_1. (h) Camouflaged image C_2.

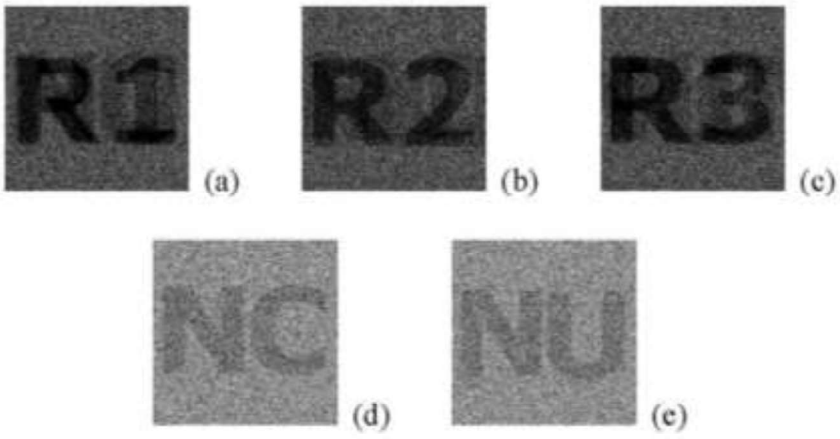

Fig. 2: Results of experiment 1. (a) Restored image S_1. (b) Restored image S_2. (c) Restored image S_3. (d) Share image G_1. (e) Share image G_2.

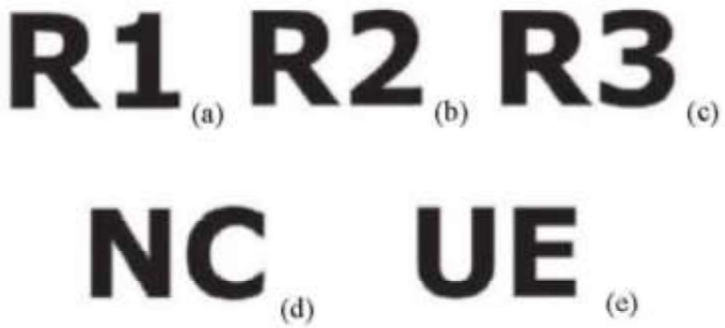

Fig. 3: Original images of similar experiment 1 by [11]. (a) Secret image S_1. (b) Secret image S_2. (c) Secret image S_3. (d) Camouflaged image C_1 (e) Camouflaged image C_2.

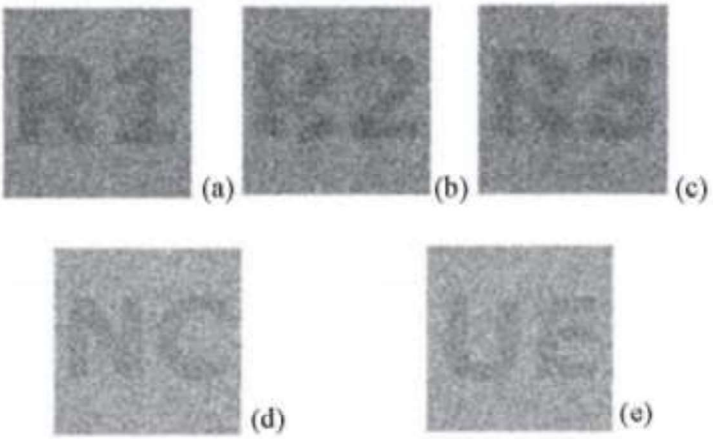

Fig. 4: Results of similar experiment 1 by [11]. (a) Restored image S_1. (b) Restored image S_2 (c) Restored image S_3. (d) Share image G_1. (e) Share image G_2

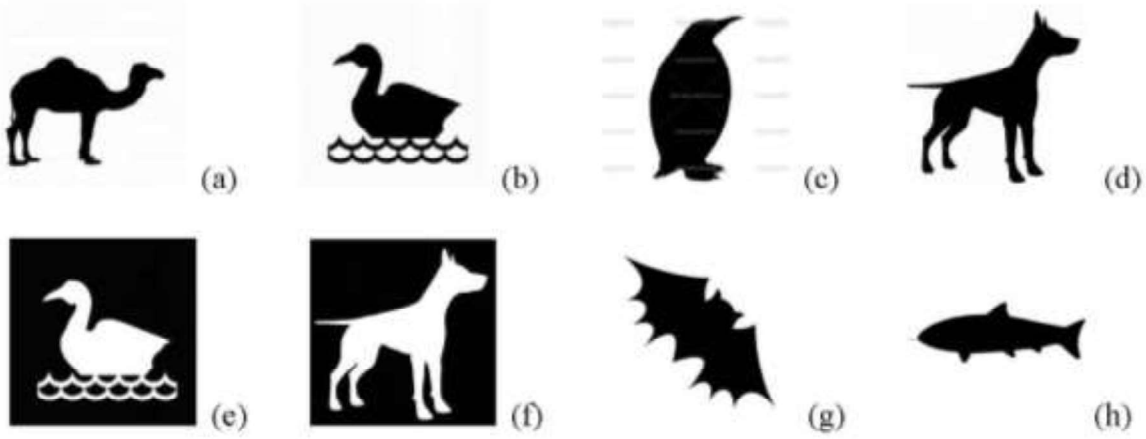

Fig. 5: Original images of experiment 2 (without (d) ~ (f)), experiment 4 (without (e), (f)) and experiment 6 (without (b), (d)). (a) Secret image S_1. (b) Secret image S_2 (c) Secret image S_3. (d) Secret image S_4. (e) Secret image S_5. (f) Secret image S_6. (g) Camouflaged image C_1. (h) Camouflaged image C_2.

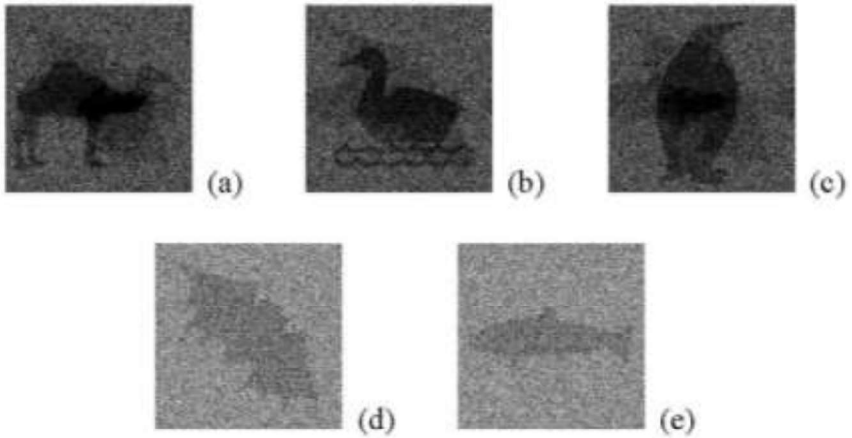

Fig. 6: Results of experiment 2. (a) Restored image S_1. (b) Restored image S_2. (c) Restored image S_3. (d) Share image C_1. (e) Share image C_2

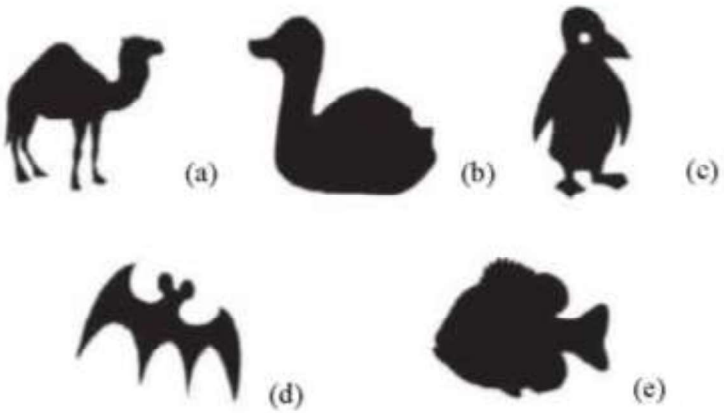

Fig. 7: Original images of similar experiment 2 by [11]. (a) Secret image S_1. (b) Secret image S_2. (c) Secret image S_3. (d) Camouflaged image C_1. (e) Camouflaged image C_2.

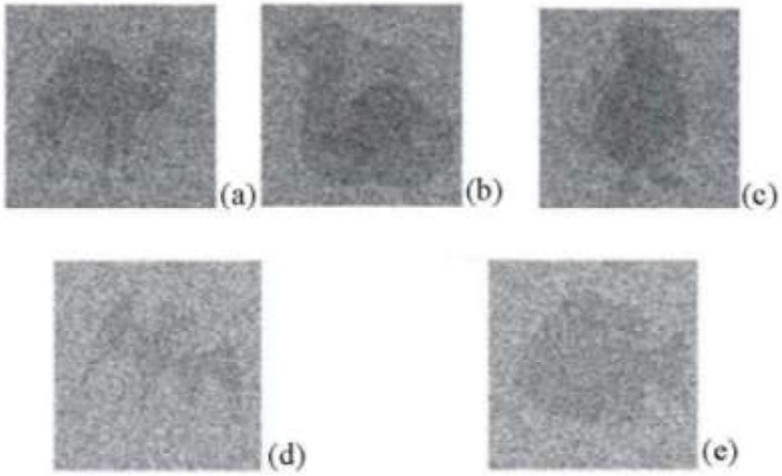

Fig. 8: Results of similar experiment 2 by [11]. (a) Restored image S_1. (b) Restored image S_2. (c) Restored image S_3. (d) Share image C_1. (e) Share image C_2.

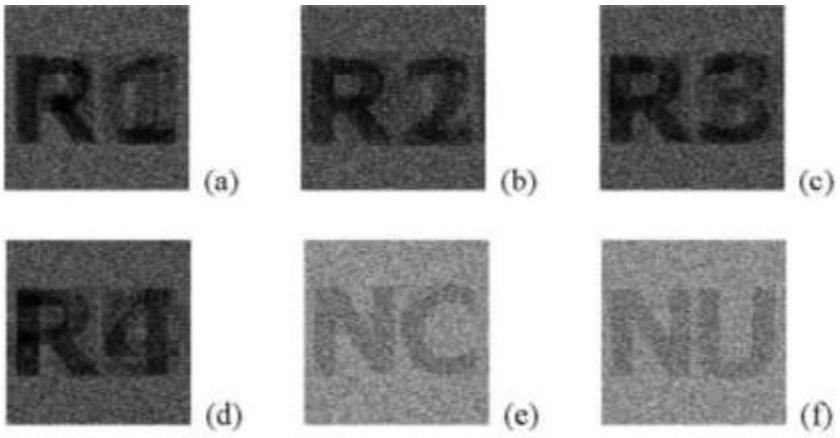

Fig. 9: Results of experiment 3. (a) Restored image S_1. (b) Restored image S_2. (c) Restored image S_3. (d) Restored image S_4. (e) Share image C_1. (f) Share image C_2.

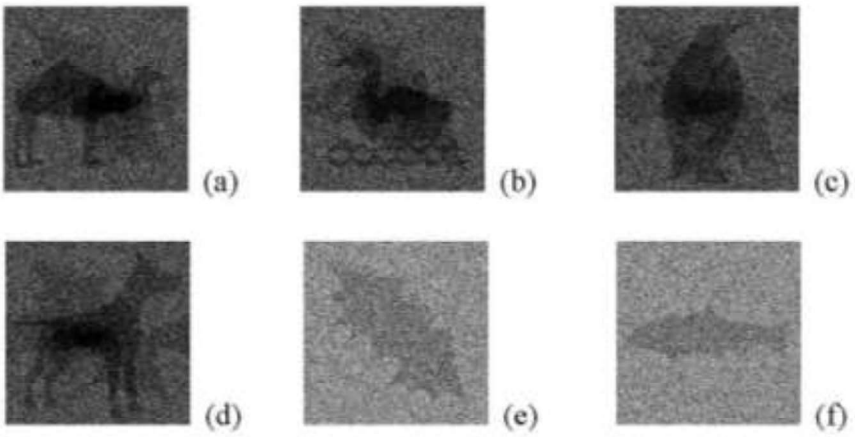

Fig. 10: Results of experiment 4. (a) Restored image S_1. (b) Restored image S_2. (c) Restored image S_3. (d) Restored image S_4. (e) Share image C_1. (f) Share image C_2.

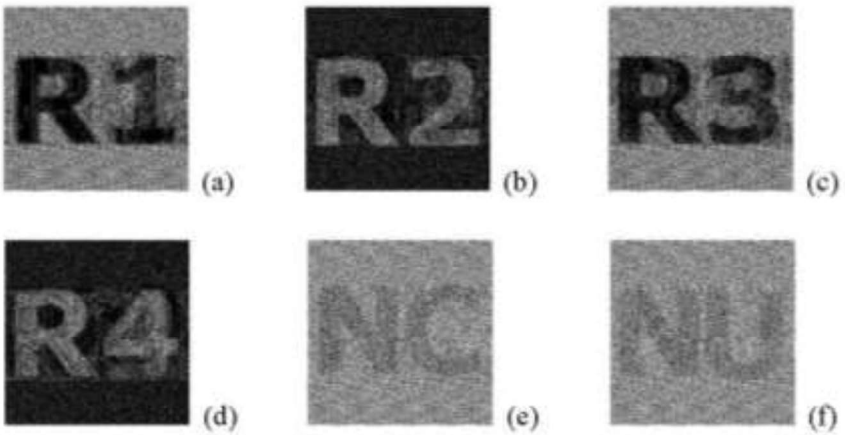

Fig. 11: Results of experiment 5. (a) Restored image S_1. (b) Restored image S_2. (c) Restored image S_3. (d) Restored image S_4. (e) Share image C_1. (f) Share image C_2.

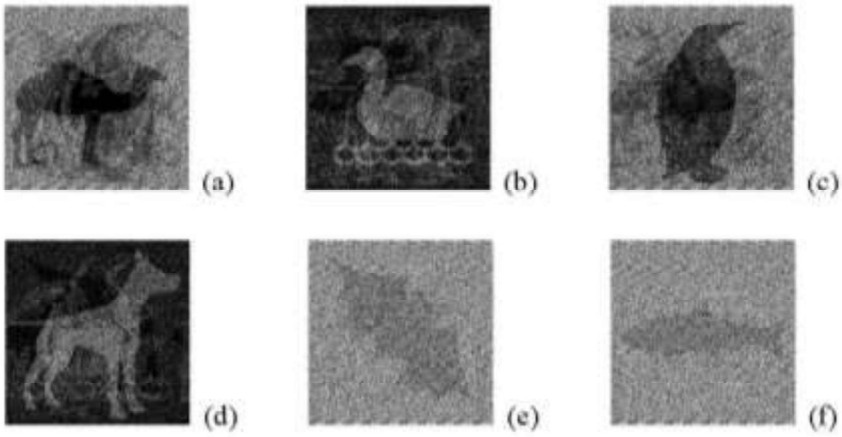

Fig. 12: Results of experiment 6. (a) Restored image S_1. (b) Restored image S_2. (c) Restored image S_3. (d) Restored image S_4. (e) Share image C_1. (f) Share image C_2.

Table 2: Comparison between the related schemes and the proposed scheme

	Number of secret images	Meaningful shares	Quality of shares	Any secret rectangle images
Chang et al. [2]	More than 2	No	High	Yes
Chen et al. [7]	4	No	Low	No
Liu et al. [11]	3	Yes	Low	No
The proposed scheme	More than 2	Yes	High	Yes

6. Conclusion

In this paper, we proposed an advanced visual multi-VSS scheme. When restoring secret images, the first image can be got by stacking two shares directly, and the others can be recovered by stacking the second share with shifting horizontally and the first share. Compare the experimental results with previous results, we not only can hold the high capacity of secret images, but also guarantee the quality of shares.

7. Acknowledgments and Legal Responsibility

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 -.

8. References

[1] J.-L. Bai, "*Random-based secret image sharing scheme*," Master's Thesis, Computer Science and Information Engineering, Ming Chuan University, 2005.

[2] J. J.-Y. Chang, B.-Y. Huang, J. S.-T. Juan, "*Visual Multi-Secret Sharing Scheme by Random Grids*", manuscript.

[3] J. J.-Y. Chang, M.-J. Li, Y.-C. Wang, J. S.-T. Juan, *"Two-Image Encryption by Random Grids*,'' Prof. of 10th International Symposium on Communications and Information

Technologies (ISCIT2010), Meiji University, Tokyo, Japan, pp. 458-463, 2010.

[4] J. J.-Y. Chang, J. S.-T. Juan, "*Multi-VSS Scheme by Shifting Random Grids*", World Academy of Science, Engineering and Technology, pp. 1277-1283, 2012.

[5] T.-H. Chen, Y.-S. Lee and C.-L. Li, "*High-capacity multi-secret sharing by random grid*," International Conference on Broadband, Wireless Computing, Communication and Applications, pp. 459-462, 2010.

[6] T.-H. Chen, and K.-H. Tsao, "*Image encryption by* (*n*, *n*) *Random Grids*," in Proceedings of 18th Information Security Conference, Hualien, 2008.

[7] T.-H. Chen, K.-H. Tsao, and Y.-S. Lee, "*Yet another multiple-image encryption by rotating random grids*." Signal Processing, vol. 92, Iss. 9, pp. 2229-2237, 2012.

[8] T.-H. Chen, K.-H. Taso, and G.-Z. Wei, "*A multi-secret image scheme by using random grids*," in Proceedings of 18th Information Security Conference, pp. 29-30, 2008.

[9] T.-H. Chen, K.-H. Tsao, and K.-C. Wei, "*Multiple-image encryption by rotating random grids*," in Proceedings of The 8th International Conference on Intelligent System Design and Applications (ISDA 2008), vol. 3, pp. 252-256, 2008.

[10] O. Kafri, and E. Keren, "*Encryption of pictures and shapes by random grids*," Optics Letters, vol. 12, no. 6, pp. 377-37, 19879.

[11] 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*," *Computer Journal*, vol. 58, no. 7, pp.1598-1606, 2015.

[12] M. Naor, and A. Shamir, "*Visual cryptography*," in Proceedings of Advances in Cryptology – Eurocrypt' 94, Lecture Notes in Computer Science, vol. 950, pp. 1-12, 1995.

[13] S.-J. Shyu, "*Image encryption by random grids*," Pattern Recognition, vol. 40, no. 3, pp. 1014-1031, 2007.

[14] S.-J. Shyu, "*Image encryption by multiple random grids*," Pattern Recognition, vol. 42, no. 7, pp. 1582-1596, 2009.