Multi-VSS Scheme by Shifting Random Grids

Joy Jo-Yi Chang, Justie Su-Tzu Juan

Abstract**—**Visual secret sharing (VSS) was proposed by Naor and Shamir in 1995. Visual secret sharing schemes encode a secret image into two or more share images, and single share image can't obtain any information about the secret image. When superimposes the shares, it can restore the secret by human vision. Due to the traditional VSS have some problems like pixel expansion and the cost of sophisticated. And this method only can encode one secret image. The schemes of encrypting more secret images by random grids into two shares were proposed by Chen et al. in 2008. But when those restored secret images have much distortion, those schemes are almost limited in decoding. In the other words, if there is too much distortion, we can't encrypt too much information. So, if we can adjust distortion to very small, we can encrypt more secret images. In this paper, four new algorithms which based on Chang et al.'s scheme be held in 2010 are proposed. First algorithm can adjust distortion to very small. Second algorithm distributes the distortion into two restored secret images. Third algorithm achieves no distortion for special secret images. Fourth algorithm encrypts three secret images, which not only retain the advantage of VSS but also improve on the problems of decoding.

Keywords**—**Visual cryptography, visual secret sharing, random grids, multiple, secret image sharing

I. Introduction

RECENTLY, the development of network technology was very soon. In order to guarantee the secret image that transmits through the network will not be stolen, the secret images must be encrypted, the concept of this process is called secret image encryption. There are many research [9][11] about secret image encryption have been proposed. The studies of visual cryptography (VC) are one of the method of secret image encryption which be proposed by Naor and Shamir [11] in 1995. VC can encrypt a secret image into two shares. The secret information can be decrypted by directly stacking two share images without any computation in computer. However, these methods need to construct codebook and they have problem of pixel expansion. So, many researches began to use the random grid [2-6], [9] and [13] algorithm to encrypt the secret image.

In 1987, Kafri and Keren proposed the encryption of a secret image by random grids. A binary secret image can turn into two meaningless shares by random grids with same size of the original secret image. The decryption process is the same as that of VC. Therefore, more researches used random grids were proposed. Chen et al. [4] (2008) proposed a multi-VSS used random grids which encrypts two secret images into two shares. However, Chen et al.'s scheme has the restriction on distortion when decrypting. So, Chang et al. [2] (2010) proposed another multi-VSS used random grids which not only encrypts two secret images as Chen et al.'s but also can adjust distortion with users. But this scheme still has sensibly distortion. Moreover, these multi-VSS scheme cannot encrypt more than two secret images.

In 2010, Chen et al. [8] proposed a method which can encrypt more than two secret images, but this method also has sensibly distortion.

Hence, this paper proposes three algorithms by shifting random grids at first. The first algorithm can adjust distortion to very small. Second algorithm can distribute the distortion over two restored secret images. Third algorithm can achieve no distortion for special secret images. Secondly, this paper proposes a scheme to encrypt three secret images into two shares. This scheme not only kept the advantage of the proposed scheme by Chang at al. but also improve on the problems of decoding.

II. Related Work

First of all, Table I defines all results when overlapping any two pixels, where 1 represent black, 0 represent white pixel.

TABLE I
ALL RESULTS WHEN OVERLAP TWO DIFFERENT PIXELS

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

In 1987, Kafri and Keren define the random grid of each pixel is only classified into transparent (white) or opaque (black) [9]. And each pixel is generated by the random number, so the amount of the transparent and opaque pixels is equal. Therefore the average light transmission ($\Im$) of a random grid is 1/2. In which light transmission is defined as the percentage of incident light that passes through an image, that is the number of white pixels over all pixels of an image. Kafri et al. propose three different algorithms to encrypt a binary secret image. The input of the algorithm is the image B which want to encrypt, the output are two random grids, R_1 and R_2. The following are these three algorithms in [9]:

Algorithm 1*:*

```
Generate a $w \times h$ random grid $R_1$// $\Im(R_1)$ =1/2
    for ($i = 0$; $i < w$; $i$ ++)
        for ($j = 0$; $j < h$; $j$ ++)
          if ($B[i][j] == 0$)
                    $R_2[i][j]\underline{= R_1[i][j]}$;
          else  $R_2[i][j] = R_1[i][j]$;
    output ($R_1$, $R_2$)
```

Algorithm 2*:*

```
Generate a $w \times h$ random grid $R_1$// $\Im(R_1)$ =1/2
    for ($i = 0$; $i < w$; $i$ ++)
        for ($j = 0$; $j < h$; $j$ ++)
          if ($B[i][j] == 0$)
                    $R_2[i][j] = R_1[i][j]$;
          else  $R_2[i][j]$ = random(0 ,1);
    output ($R_1$, $R_2$)
```

Joy Jo-Yi Chang and Justie Su-Tzu Juan are with Department of Computer Science and Information Engineering National Chi Nan University Puli, Nantou, 54561, Taiwan, R.O.C. *Corresponding author. Email: jsjuan@ncnu.edu.tw.

```
Algorithm 3:
Generate a $w \times h$ random grid $R_1$// $\Im(R_1) = 1/2$
  for ($i = 0$; $i < w$; $i$ ++)
    for ($j = 0$; $j < h$; $j$ ++)
      if ( $B[i][j] == 0$)
            $R_2[i][j] = \text{random}(0, 1)$;
      else  $R_2[i][j] = R_1[i][j]$ ;
  output ($R_1$, $R_2$)
```

Next, this paper discusses Chang et al.'s Algorithms 4 that be held in 2010 [2]. In order to explain clearly, this paper gives an example by using the Algorithm 1 to carry out the encryption in the proposed scheme. Also, we can use Algorithm 2 and 3 substituted for Algorithm 1. The inputs of Algorithms 4 are two images S_A, S_B which want to be encrypted, and the output of Algorithms 4 are two encrypted images G_1 and G_2.

Subsequently, some definitions in Chang et al.'s algorithm will be defined as follows.

Definition 1*:* $f_{RSP}(.)$: $Y \leftarrow f_{RSP}(X)$, Y is the output of the function $f_{RSP}(.)$ with the inputs X, where $f_{RSP}(.)$ is that randomly select a pixel of X.

Definition 2*:* $f_{RG}(.)$: $Y||Z \leftarrow f_{RG}(X)$, Y and Z are the outputs of the function $f_{RG}(.)$ with the input X, where $f_{RG}(.)$ is one of the three random grids algorithm in [8] which inputs a pixel of the secret image, then outputs two cipher-pixels for two shares.

Definition 3*:* $\overline{f}_{RG}(.)$: $Z \leftarrow \overline{f}_{RG}(X, Y)$, Z is the output of the function $\overline{f}_{RG}(.)$ with the inputs X and Y, where $\overline{f}_{RG}(.)$ is the function according to $f_{RG}(.)$ (as in Definition 2) which inputs a cipher-pixel of one share Y and a pixel of the secret image X, then outputs the other cipher-pixel.

As stated above, Chang 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. The second segment will move horizontally and then superimpose the first fragment, will receive the second secret image. The following is the method that the second share moves horizontally 1/4 width when restored the second image. The idea of that scheme is presented in Figure 1.

Algorithm 4*:*
Step 1: $S_A(i, j) \leftarrow f_{RSP}(S_A)$.
Step 2: $G_1(i, j)||G_2(i, j) \leftarrow f_{RG}(S_A(i, j))$.
Step 3: $G_2((i + m/4), j) \leftarrow \overline{f}_{RG}(S_B(i, j), G_1(i, j))$.
Step 4: $G_1((i + m/4), j) \leftarrow \overline{f}_{RG}(S_A((i + m/4), j), G_2((i + m/4), j))$.
Step 5: $G_2((i + m/2), j) \leftarrow \overline{f}_{RG}(S_B((i + m/4), j), G_1((i + m/4), j))$.
Step 6: $G_1((i + m/2), j) \leftarrow \overline{f}_{RG}(S_A((i + m/2), j), G_2((i + m/2), j))$.
Step 7: $G_2((i + 3m/4), j) \leftarrow \overline{f}_{RG}(S_B((i + m/2), j), G_1((i + m/2), j))$.
Step 8: $G_1((i + 3m/4), j) \leftarrow \overline{f}_{RG}(S_A((i + 3m/4), j), G_2((i + 3m/4), j))$.
Step 9: Repeating Step 1 to 8 until all the cipher-pixels of two cipher-grids are generated.

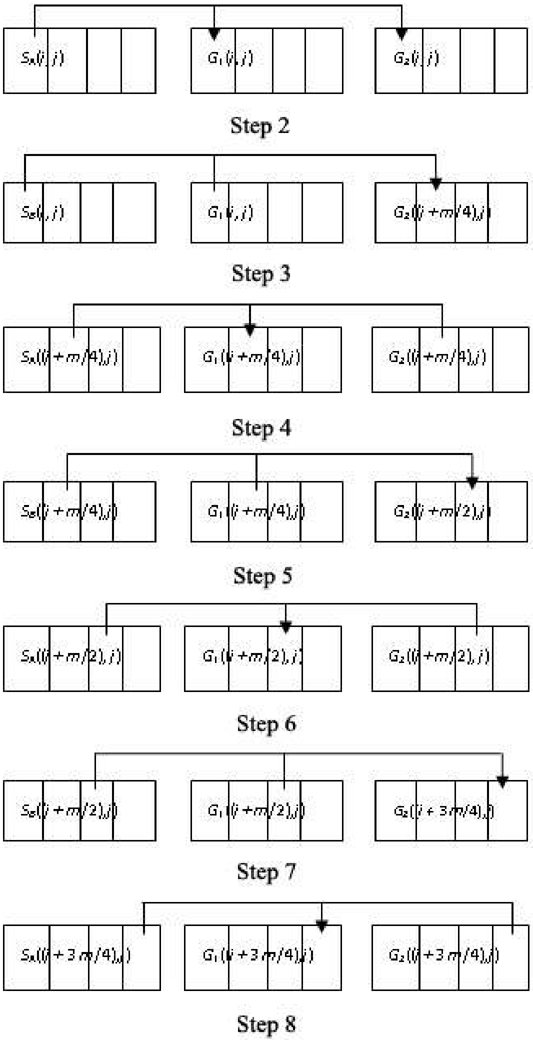


Fig. 1 The diagram of the processes in the encryption phase of the proposed scheme with respected to moving horizontally 1/4 width

III. Main Result

In Section A, this paper proposes three algorithms which are based on Algorithm 4 also can encrypt two secret images into two shares. The Algorithm 5 can reduce the distortion to $1/p$. And Algorithm 6 let distortion distribute over two restored secret images. Algorithm 7 does even achieve no distortion.

In Section B, this paper proposes a new scheme to encrypt three secret images into two shares, which also can adjust distortion. So, we can get the other algorithms Algorithm 8.

A. Encrypt two secret images

i. Encryption phase

According to the proposed method, the distortion 1/4 can be reduced to smaller. The distortion of the second restored image can be chose by users. The amount of distortion is related to the degree of moving when we restored the second image. For example, if the distortion was 1/4, we can set the degree of moving to be quarter, half or three quarters of the width of the second share.

For the same reason, if we want to reduce the distortion to 1/10, we can set the degree of moving to be p tenth, for p = 1, 2, … , 9. This way can get more clearly restored secrete image.

The inputs of the Algorithm 5 are two images S_A, S_B with the size of m x m be encrypted into two share images G_1 and G_2 with the size of m x m without any pixel expansion. And the input p is the degree of we want to move. That is to say, we can reduce the distortion to $1/p$. The idea has been stated in [2], here we give the detail of the algorithm as follows:

```
Procedure URG ($S_A(i, j)$, $S_B(i, j)$, $p$)

$G_1(i, j)||G_2(i, j) \leftarrow f_{RG}(S_A(i, j))$
int $a = 0$, $b = 1$;
for (int $i = 3$; $i <= p * 2$; $i$ ++)
  if (i % 2 == 1)
    $G_2((i + m*b/p), j) \leftarrow \overline{f}_{RG}(S_B((i + m*a/p), j), G_1((i + m*a/p), j))$
  else
    $G_1((i + m*b/p), j) \leftarrow \overline{f}_{RG}(S_A((i + m*b/p), j), G_2((i + m*b/p), j))$
    $a$ ++;
    $b$ ++;
```

Algorithm 5:

```
Repeat
    $S_A(i, j) \leftarrow f_{RSP}(S_A)$
    Procedure URG ($S_A(i, j)$, $S_B(i, j)$, $p$)
Until all the cipher-pixels of two cipher-grids are generated
```

Next, Algorithm 6 make that distortion be distributed over two restored secret images as following:

Algorithm 6:

```
Repeat
    Randomly select $A' = A$ or $B$, $B' = \{A, B\} \setminus \{A'\}$
    $S_{A'}(i, j) \leftarrow f_{RSP}(S_{A'})$
    Procedure URG ($S_{A'}(i, j)$, $S_{B'}(i, j)$, $p$)
Until all the cipher-pixels of two cipher-grids are generated
```

Algorithm 7 does even achieve no distortion for special secret images. The $1/p$ segment of the second secret image is meaningless, so we don't select that segment for encryption. The detail of the algorithm as following:

Algorithm 7:

```
for ($i = 0$; $i < w$; $i$ ++)
  for ($j = 0$; $j < h$; $j$ ++)
    $G_1(i, j)||G_2(i, j) \leftarrow f_{RG}(S_A(i, j))$
    int $a = 0$, $b = 1$;
    for (int $i = 3$; $i <= p * 2 - 1$; $i$ ++)
      if (i % 2 == 1)
        $G_2((i + m*b/p), j) \leftarrow \overline{f}_{RG}(S_B(( + m*a/p), j), G_1((i + m*a/p), j))$
      else
        $G_1((i + m*b/p), j) \leftarrow \overline{f}_{RG}(S_A((i + m*b/p), j), G_2((i + m*b/p), j))$
        $a$ ++;
        $b$ ++;
```

ii. Decryption phase

Upon collecting these two cipher-grids 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_1 by moving horizontally m/p width.

B. Encrypt three secret images

i. Encryption phase

From the idea of above subsection, we can propose a new secret sharing scheme by random grids which can encrypt three secret images. The following is the method that the second share moves horizontally 1/10 width when restored the second image. And the second share moves horizontally 1/5 width when restored the third image. The details of the encryption processes are illustrated as follows.

The inputs of Algorithms 8 are three images S_A, S_B and S_C which want to be encrypted, and the output of Algorithms 8 are two encrypted images G_1 and G_2.

Algorithm 8:

```
Step 1: $S_A(i, j) \leftarrow f_{RSP}(S_A)$.
Step 2: $G_1(i, j)||G_2(i, j) \leftarrow f_{RG}(S_A(i, j))$.
Step 3: $G_2((i + m/10), j) \leftarrow \overline{f}_{RG}(S_B(i, j), G_1(i, j))$.
Step 4: $G_2((i + m/5), j) \leftarrow \overline{f}_{RG}(S_C(i, j), G_1(i, j))$.
Step 5: $G_1((i + m/10), j) \leftarrow \overline{f}_{RG}(S_A((i + m/10), j), G_2((i + m/10), j))$.
Step 6: $G_1((i + 9m/10), j) \leftarrow \overline{f}_{RG}(S_B((i + 9m/10), j), G_2(i, j))$.
Step 7: $G_2((i + 2m/5), j) \leftarrow \overline{f}_{RG}(S_C(i + m/5, j), G_1(i + m/5, j))$.
Step 8: $G_1((i + 2m/5), j) \leftarrow \overline{f}_{RG}(S_A((i + 2m/5), j), G_2((i + 2m/5), j))$.
Step 9: $G_1((i + 3m/10), j) \leftarrow \overline{f}_{RG}(S_B((i + 3m/10), j), G_2(i + 2m/5, j))$.
Step 10: $G_2((i + 3m/10), j) \leftarrow \overline{f}_{RG}(S_C(i + m/10, j), G_1(i + m/10, j))$.
Step 11:$G_2((i + 9m/10), j) \leftarrow \overline{f}_{RG}(S_A((i + 9m/10), j), G_1((i + 9m/10), j))$.
Step 12: $G_2((i + m/2), j) \leftarrow \overline{f}_{RG}(S_B((i + 2m/5), j), G_1(i + 2m/5, j))$.
Step 13: $G_2((i + 3m/5), j) \leftarrow \overline{f}_{RG}(S_C(i + 2m/5, j), G_1(i + 2m/5, j))$.
Step          $(i + m/2), j) \leftarrow \overline{f}_{RG}(S_A((i + m/2), j), G_2((i + m/2), j))$.
```

Step 15: $G_1((i + 4m/5), j) \leftarrow \overline{f}_{RG}(S_B((i + 4m/5), j), G_2(i + 9m/10, j))$.
Step 16: $G_2((i + 7m/10), j) \leftarrow \overline{f}_{RG}(S_C(i + m/2, j), G_1(i + m/2, j))$.
Step 17: $G_1((i + 7m/10), j) \leftarrow \overline{f}_{RG}(S_A((i + 7m/10), j), G_2((i + 7m/10), j))$.
Step 18: $G_2((i + 4m/5), j) \leftarrow \overline{f}_{RG}(S_B((i + 7m/10), j), G_1(i + 7m/10, j))$.
Step 19: $G_1((i + 3m/5), j) \leftarrow \overline{f}_{RG}(S_C(i + 3m/5, j), G_2(i + 4m/5, j))$.
Step 20: Repeating Step 1 to 19 until all the cipher-pixels of two cipher-grids are generated.

ii. Decryption phase

Upon collecting these two cipher-grids 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_1 by moving horizontally 1/10 width. The third secret image S_C can obtain by superposing G_1 and G_4, where G_4 is obtained from G_1 by moving horizontally 1/5 width.

IV. Experiments

In this section, we present some results to show that the distortion of the restored images can be reduced as one want, which is better than Chen et al.'s scheme [4]. And we also present the three-secret image sharing scheme by shifting random grids.

A. Encrypt two secret images

Simulation 1: Execute Algorithm 5

The input images are binary secrets, moving horizontally by $1/p$ width can recover the second image. Take $p = 10$ for example as following:

Two secret images S_A and S_B with the size of 400 × 300 are stored some simple English alphabets, Figure 2(a) and 2(b), which are encrypted into two cipher-grids shares G_1 and G_2 with the size of 400 × 300 as shown in Figure 2(c) and 2(d). The first secret image S_A with the size of 400 × 300 is decrypted by superposing G_1 with G_2 directly as shown in Figure 2(e). Upon moving 1/4 width for G_2 horizontally, the second secret image S_B with the size of 400 × 300 is decrypted by superposing G_1 and the moved G_2, as shown in Figure 2(f).

Simulation 2: Execute Algorithm 6

The input images are binary secrets, moving horizontally 1/50 width can recover the second image and the distortion can be spread for all restored images.

Simulation 3: Execute Algorithm 7

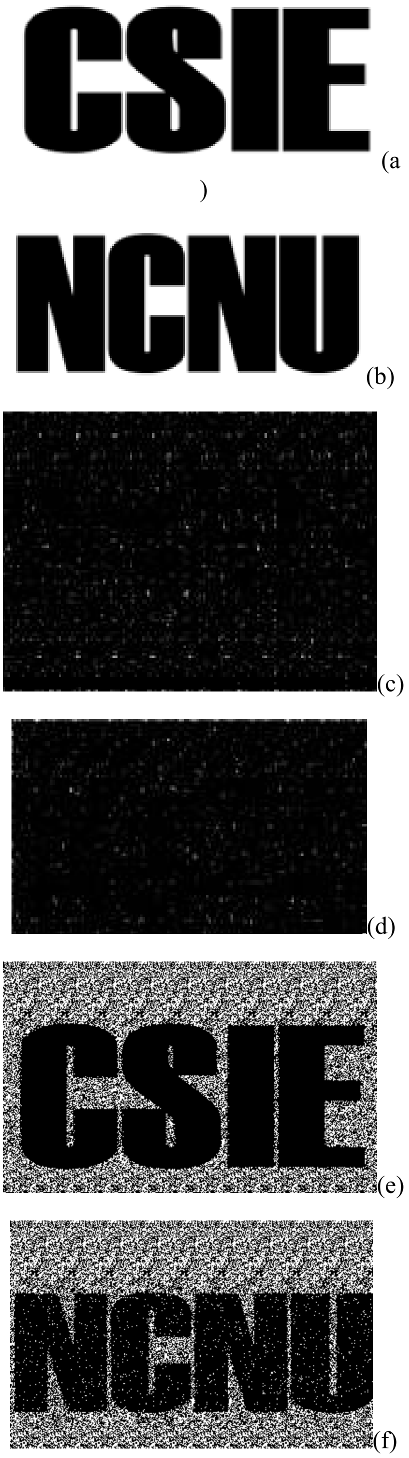


Fig. 2 Results of *Simulation* 1: (a) the first secret image S_A, (b) the second secret image S_B, (c) share G_1, (d) share G_2, (e) the first restored secret S_A, (f) the second restored secret S_B.

The input images are binary secrets, moving horizontally 1/50 width can recover the second image with no any distortion for special secret images.

Likewise, *Simulation* 2 and 3 show the cases of moving horizontally by 1/50 width when restore the second secret image. The experimental results are given in Figure 3 and 4, respectively.

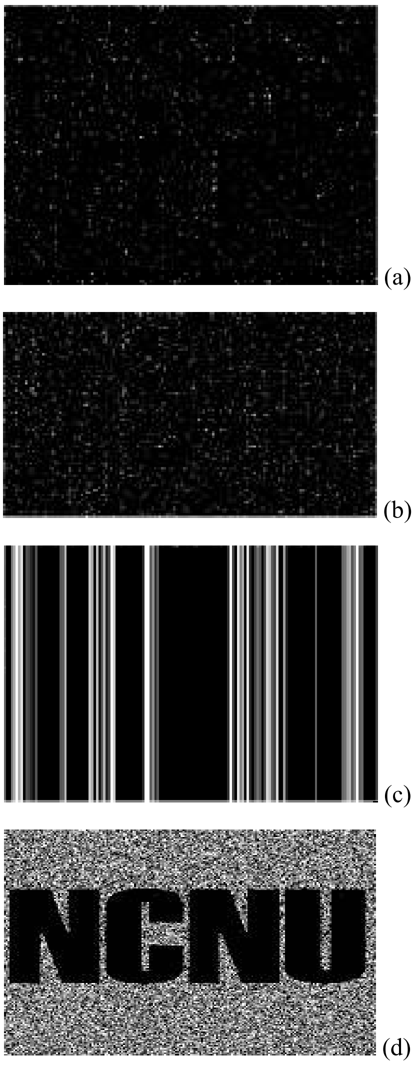


Fig. 3 Results of *Simulation* 2: the first secret image S_A is the same as *Simulation* 1, the second secret image S_B is the same as *Simulation* 1, (a) share G_1, (b) share G_2, (c) the first restore secret S_A, (d) the second restored secret S

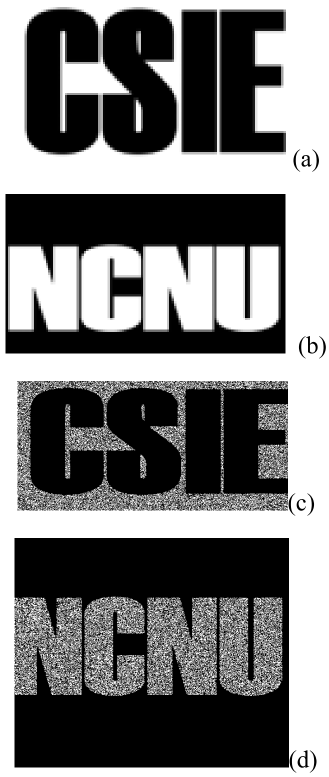


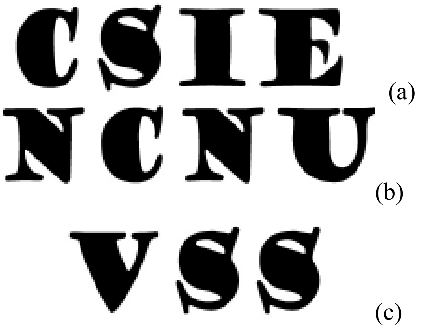
Fig. 4 Results of *Simulation* 3: (a) the first secret image S_A, (b) the first restored secret S_A, (c) the second secret image S_B, (d) the second restored secret S_B.

B. Encrypt three secret images

Simulation 4: Execute Algorithm 8

The input images are binary secrets, moving horizontally by 1/10 width can recover the second image, moving horizontally by 1/5 width can recover the third image.

Two secret images S_A and S_B with the size of 400 × 300 are stored some simple English alphabets, Figure 5(a) ,5(b) and 5(c), which are encrypted into two cipher-grids shares G_1 and G_2 with the size of 400 × 300 as shown in Figure 5(d) and 5(e).



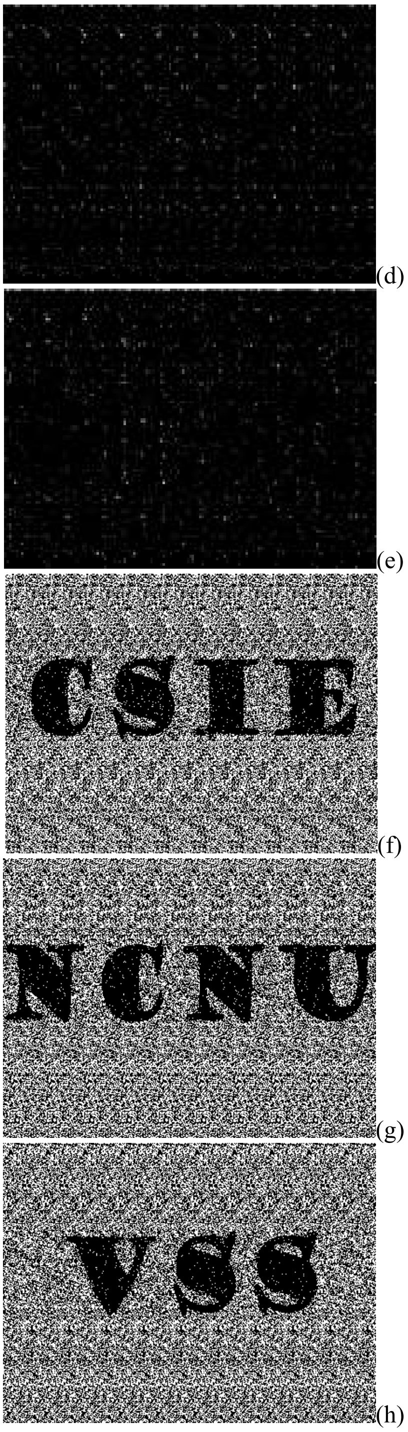


Fig. 5 Results of *Simulation* 4: (a) the first secret image S_A, (b) the second secret image S_B, (c) the third secret image S_C, (d) share G_1, (e) share G_2, (f) the first restored secret S_A, (g) the second restored secret $S_{B,}$ (h) the third restored secret S_c.

V. Conclusion

In this paper, three algorithms for encrypting two secret images and a visual secret sharing (VSS) scheme uses random grids for encrypting three secret images are proposed.

At first, the first algorithm can adjust distortion to very small. And the second algorithm can distribute the distortion over two restored secret images. The third algorithm can achieve no distortion for special secret images. These three algorithms not only retain the advantage of VSS but also improve on the problems of decoding.

Secondly, we propose a visual secret sharing scheme uses random grids which can encrypt three secret images at once into two shares. When restored the secret images, first secret image can be got by overlap these two shares directly, while the second and the third secret image can be got by overlap the first share with the shifted second share, where shift means moving horizontally. The simulate results of superposing these two shares are displaying on the computer.

Compared with the traditional VSS methods such as VC and random grids, the proposed scheme needs not to redesign any codebook and without any pixel expansion. Moreover, the proposed scheme can carry more information than traditional VSS schemes and saves the cost of transmission bandwidth and storage. Compared with Chen et al.'s scheme in 2010 for encrypting three secret images, this proposed scheme can reduce the distortion too very small.

Compared with the VSS methods which are proposed by Chang-Chou Lin and Wen-Hsiang Tsai in 2002. This scheme used image processing to transform gray-level images into an approximate binary image, but when encrypting the secret images, it has a problem which is pixel expansion.

In the near future, we will try to encrypt *n* secret images into two shares by using the idea of the proposed Algorithm 5 to Algorithm 8 for any positive integer *n*. Hence, the proposed scheme can be widely applied.

Acknowledgment

This research was supported in part by the National Science Council of the Republic of China under grant NSC 100-2221-E-260-024- .

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, M.-J. Li, Y.-C. Wang, J. S.-T. Juan*, Oct 2010, "Two-Image Encryption by Random Grids," Prof. of 10th International Symposium on Communications and Information Technologies (ISCIT2010), Meiji University, Tokyo, Japan, Oct. 26-29, 2010, pp. 458-463. (NSC98-2221-E-260-013-) (EI)

[3] T.-H. Chen, G.-Z. Wei, and K.-X. Taso, "An multi-secret image scheme by using random grids," in Proceedings of 18th Information Security Conference, Hualien, May 29-30, 2008.

[4] 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, 2008, pp. 252-256.

[5] T.-H. Chen, and K.-H. Tsao, "Image encryption by (n, n) Random Grids," in Proceedings of 18th Information Security Conference, Hualien, May 29-30, 2008.

[-H. Chen, K.-H. Taso, and Y.-T. Yang, "Friendly color visual secret sharing by random grids," Fundamenta Informaticae, vol. 96, 2009, pp. 61-70.

[-Y. Chen, J. S.-T. Juan, and M.-J. Li, "A random grid-based visual cr ography to adjust light transmission and the number of shares," i

Proceeding of 2009 National Computer Symposium, National Taipei University, Taiwan, Nov. 27-28, 2009, pp. 184-192.

[8] T.-H. Chen, Y.-S. Lee and C.-L. Li, "High-capacity multi-secret sharing by random grid," Proceedings of The First International Workshop on Cloud, Wireless and e-Commerce Security (CWECS 2010), Fukuoka, Japan, November 4-6, 2010.(NSC 99-2221-E-415-017)

[9] O. Kafri, and E. Keren, “Encryption of pictures and shapes by random grids,” Optics Letters, vol. 12, no. 6, 1987, pp. 377-379.

[10] R. Lukac, and K. N. Plataniotis, “Bit-level based secret sharing for image encryption,” Pattern Recognition, vol. 38, no. 5, 2005, pp. 767-772.

[11] M. Naor, and A. Shamir, “Visual cryptography,” in Proceedings of Advances in Cryptology – Eurocrypt’ 94, Lecture Notes in Computer Science, vol. 950, Springer Berlin, 1995, pp. 1-12.

[12] S.-J. Shyu, “Image encryption by random grids,” Pattern Recognition, vol. 40, no. 3, 2007, pp. 1014-1031.

-J. Shyu, “Image encryption by multiple random grids,” Pattern Recognition, vol. 42, no. 7, 2009, pp. 1582-1596.