International Journal of Innovative Computing, Information and Control
Volume **9**, Number **4**, April **2013**

ICIC International ©2013 ISSN 1349-4198
pp. 1691–1701

REVERSIBLE VISUAL SECRET SHARING BASED ON RANDOM-GRIDS FOR TWO-IMAGE ENCRYPTION

Zhi-Hui Wang[1], Marcos Segalla Pizzolatti[2] and Chin-Chen Chang[2,3,*]

[1]School of Software
Dalian University of Technology
Economy and Technology Development Area, Dalian 116620, P. R. China
Wangzhihui1017@gmail.com

[2]Department of Information Engineering and Computer Science
Feng Chia University
No. 100, Wenhwa Road, Seatwen, Taichung 40724, Taiwan
segall.pizzo@gmail.com; *Corresponding author: alan3c@gmail.com

[3]Department of Computer Science and Information Engineering
Asia University
No. 500, Lioufeng Road, Wufeng, Taichung 41354, Taiwan

Received January 2012; revised June 2012

Abstract. *Based on the random-grids technique proposed by Kafri and Keren, Chang et al. presented a visual secret-sharing (VSS) scheme in order to encrypt two secret images simultaneously. Such a scheme stacks two generated shadows together to recover the first secret image and shifts the second shadow horizontally to reveal the second secret image, but the visual quality of the recovered image is not satisfactory. In this paper, two visual secret-sharing schemes are proposed to improve the visual quality in different ways to satisfy the requirements of applying VSS in the visual authentication field and in the highly-sensitive, information-hiding field, respectively. The first scheme utilizes the exclusive OR operation to recover the first secret image completely and to achieve much better contrast quality in the second secret image when it is recovered. The second scheme can achieve reversibility for both recovered secret images at the cost of losing the shifted part of the second recovered image. Our experimental results showed the effectiveness of the proposed schemes.*

Keywords: Secret sharing, Random grids, Two-image encryption, Reversibility

1. **Introduction.** The secret-sharing technique, first proposed by Shamir in 1979 [1], aims to protect secret data by dividing them into n parts. The key idea of secret sharing is that it is only possible to reconstruct the original secret by using at least k parts; no useful information about the original secret can be revealed with less than k parts. Also in 1979, Blakley proposed another secret-sharing scheme in order to safeguard cryptographic keys [2]. To implement the secret-sharing scheme into the image-processing field, traditional, visual secret sharing (VSS), first proposed by Naor and Shamir [3], is designed to share one binary, secret image hidden among some meaningless shadow images, and, then, the secret image could be recovered without any computational cost. VSS has been applied to many applications, such as image encryption [4], visual authentication, copyright protection, watermarking [5], and, especially, information hiding [6]. Many researchers have been active in the VSS field in the past several years, and their research usually is based on the requirements of the applications of interest. Some research that has been reported in the literature extended binary image-sharing schemes, making them suitable for grayscale and color images [7-12]. The major drawback of traditional VSS schemes is that two or

more sub-pixels are required to represent each secret image pixel in each shadow image. Therefore, these schemes have the pixel-expansion problem, which leads to burdening the communication channels when the shadows are being transmitted.

Many schemes have been proposed in recent years with the goal of solving the pixel-expansion problem [13-18]. Blundo and Santis managed to generate a perfect reconstruction of black pixels, while achieving a minimum pixel expansion [13]. Yang proposed a probabilistic method that took the frequency of white pixels into account [14]. This method is non-expandable, and the contrast quality is the same as that of the traditional VSS schemes. Wang *et al.* improved the scheme in [14] to achieve a better contrast of the recovered image [15]. Shyu and Chen proposed an optimal pixel-expansion method that achieved the optimum solution by using an integer linear program [16]. Pai *et al.* proposed a multiple, graylevel, visual-cryptography scheme that simultaneously achieved meaningful shadows and no pixel expansion [17]. Totally different from the aforementioned visual cryptography-based, visual secret sharing methods (VCVSS), Kafri and Keren proposed three visual secret sharing algorithms based on the random cypher-grids (RGVSS) [18]. In these algorithms, one shadow, named a random grid, was produced randomly using the bits 0 and 1. Then, the other shadow can be generated using the binary secret image and the random grid. As a result, the RGVSS has two shadows that have secret images of identical size, meaning that it does not introduce any pixel expansion, but it provides the advantages of VCVSS at a lower computation cost and without the requirement that the user has extensive knowledge of cryptography. Inspired by [18], many studies began to use the random-grids technique to deal with the undesirable pixel expansion problem of traditional VSS schemes [19-22]. Shyu's schemes utilized random grids to generate shadows from binary, grayscale, and color images [19,20]. Chen and Tsao proposed two general (k, n), user-friendly schemes based on random grids [21,22], which are also suitable for both binary and color images. Furthermore, meaningful shadows can be obtained based on the logo images in [22].

Because the aforementioned schemes can only encrypt one secret image at a time, two schemes were proposed in [23,24] to encrypt two secret images simultaneously, based on the random-grids technique. In the scheme proposed by Chen *et al.* [23], the first secret image was disclosed by stacking the two generated shadows together, after which the second secret image can be revealed by rotating the second shadow by 90, 180, or 270 degrees. Chang *et al.*'s scheme shifted the second shadow horizontally to reveal the second secret image, and the first secret image can be disclosed by superimposing the two shadows without any shifting [24]. The contrast quality of the method in [24] was better than that of the recovered secret images in [23].

Knowing that VSS can be applied more effectively in visual authentication and watermarking when its visual quality is better, we proposed a scheme to improve the visual quality of both recovered secrets in [24]. Further, in the research reported in this paper, we designed another scheme based on the first scheme to achieve reversibility in order to satisfy the lossless recovery of secret data for applying VSS in the information-hiding area. The main idea of the first scheme was to use the exclusive OR operation instead of the OR operation in the decryption phase, because the exclusive OR operation can recover the first secret image completely and achieve better visual quality for the second, recovered secret image. And the second scheme can achieve reversibility for both recovered secret images at the cost of losing some of the information in the second, recovered secret image.

The remainder of this paper is organized as follows. Section 2 introduces related work. Section 3 describes two proposed, visual secret sharing schemes based on random grids. Experimental results and analysis are presented in Section 4, and Section 5 provides our conclusions based on the experimental results.

2. Related Work.

2.1. Random-grids technique.

The random-grids technique can encrypt one binary image into two shadows, called random cypher-grids, without expanding the number of pixels necessary and without designing a codebook [18]. In [18], each image pixel can be represented as either transparent (white) or opaque (black), and the choice between them is made randomly. Therefore, each shadow has an average light transmission that equals 1/2. The transparent pixel lets the light through, while the opaque pixel stops it. Thus, three cases can exist as determined by the characteristics of the shadows in the random grids, i.e., 1) two identical shadows, 2) two independent shadows, and 3) two complementary shadows. Based on the above cases, Kafri *et al.* proposed three visual secret sharing algorithms using random grids that differ from each other in their contrast quality as follows:

Algorithm 1: The first shadow G_1 is generated randomly by the bits 0 or 1. Then, if the secret binary pixel $S(i,j)$ is equal to 0, the binary pixel of the second shadow $G_2(i,j)$ at the same position will be the same as in $G_1(i,j)$; otherwise, the binary pixel in $G_2(i,j)$ will be the complement of $G_1(i,j)$.

$$G_2(i,j) = \begin{cases} G_1(i,j) & \text{if } S(i,j) = 0 \\ \overline{G_1(i,j)} & \text{otherwise.} \end{cases} \tag{1}$$

Algorithm 2: The first shadow G_1 is generated randomly by the bits 0 or 1. Then, if the secret binary pixel $S(i,j)$ is equal to 0, the binary pixel of the second shadow $G_2(i,j)$ at the same position will be the same as in $G_1(i,j)$; otherwise, the binary pixel in $G_2(i,j)$ will be generated randomly by the function $f_c(0,1)$.

$$G_2(i,j) = \begin{cases} G_1(i,j) & \text{if } S(i,j) = 0 \\ f_c(0,\ 1) & \text{otherwise} \end{cases} \tag{2}$$

Algorithm 3: The first shadow G_1 is generated randomly by the bits 0 or 1. Then, if the secret binary pixel $S(i,j)$ is equal to 0, the binary pixel in $G_2(i,j)$ will be generated randomly by the function $f_c(0,1)$; otherwise, the binary pixel in $G_2(i,j)$ will be the complement of $G_1(i,j)$.

$$G_2(i,j) = \begin{cases} f_c(0,1) & \text{if } S(i,j) = 0 \\ \overline{G_1(i,j)} & \text{otherwise} \end{cases} \tag{3}$$

2.2. Chang *et al.*'s scheme.

Chang *et al.*'s scheme stacks two shadows together and shifts the second generated shadow horizontally by a certain width to disclose the second secret image, while the first secret image can be disclosed easily by stacking the two shadows directly without any shift [24]. In Chang *et al.*'s scheme, the width of the shift can be determined by the user. The smaller the width is, the clearer the second recovered secret image will be. Therefore, the visual distortion of the second recovered image is related to the width of the shift. Compared with Chen *et al.*'s scheme [23] in which the visual distortion of the second recovered secret image is fixed at 1/4, Chang *et al.*'s scheme [24] can produce better visual quality by setting a smaller value of visual distortion during the recovery of the second secret image. In order to introduce Chang *et al.*'s scheme clearly, three definitions, as stated in [23], are described below:

Definition 2.1. *$f_{RSP}(\cdot)$: $Y \leftarrow f_{RSP}(X)$, where Y is the output of the function $f_{RSP}(\cdot)$ with the input X, and the pixel of X is selected randomly by $f_{RSP}(\cdot)$.*

Definition 2.2. *$f_{RG}(\cdot)$: $Y\|Z \leftarrow f_{RG}(X)$, where $f_{RG}(\cdot)$ is one of the three random-grid algorithms [14], which inputs one pixel of the secret image X and outputs two cipher-pixels, i.e., Y and Z, for two shadows.*

Definition 2.3. *$F_{RG}(\cdot)$: $Z \leftarrow F_{RG}(X,Y)$, where the function $F_{RG}(\cdot)$ inputs a pixel of the secret image and a cipher-pixel of one shadow, i.e., X and Y, and outputs the other cipher-pixel Z.*

The following subsections, which are based on the above three definitions, are the detailed descriptions of encryption and decryption phases for Chang *et al.*'s scheme.

Encryption Phase of Chang et al.'s Scheme: In the method proposed by Chang *et al.*, the visual distortion value of the second recovered secret image is set to be $1/p$. Therefore, the shifting quantity of the second generated shadow should be $x \times n/p$, only if $\gcd(x,p) = 1$, where x/p is the shifting quantity, and n is the width of the secret image. In other words, if the visual distortion of the second recovered secret image is set to 1/4, we must simplify the correspondent fractions as follows: 1/4 (quarter), 2/4 simplified to 1/2 (half), and 3/4 (three quarters). In addition, the modular operation % must be included in the calculations in order to correct the range of the index position of j when sharing a binary pixel from the first secret image. The detailed steps of Chang *et al.*'s scheme, with 1/4-width, horizontal shifting, are given as follows:

Input: two secret images, S_A and S_B, sized $m\times n$.

Output: two shadow images, G_1 and G_2, sized $m\times n$.

Step 1: $S_A(i,j) \leftarrow f_{RSP}(S_A)$. Select a binary pixel, $S_A(i,j)$, randomly from the first secret image, S_A, where $i = 0, 1, \ldots, m-1$, and $j = 0, 1, \ldots, n-1$.

Step 2: $G_1(i,j)\|G_2(i,j) \leftarrow f_{RG}(S_A(i,j))$. Generate the binary pixels, $G_1(i,j)$ and $G_2(i,j)$, for the shadows, G_1 and G_2, according to the selected binary pixel $S_A(i,j)$.

Step 3: $G_2(i,(j+n/4)\%n) \leftarrow F_{RG}(S_B(i,j), G_1(i,j))$. Generate the binary pixel, $G_2(i,(j+n/4)\%n)$, for the shadow, G_2, according to the generated binary pixel, $G_1(i,j)$, and the binary pixel, $S_B(i,j)$, of the second secret image, S_B.

Step 4: $G_1(i,(j+n/4)\%n) \leftarrow F_{RG}(S_A(i,(j+n/4)\%n), G_2(i,(j+n/4)\%n))$. Generate the binary pixel, $G_1(i,(j+n/4)\%n)$, for the shadow, G_1, according to the generated binary pixel, $G_2(i,(j+n/4)\%n)$, and the binary pixel, $S_A(i,(j+n/4)\%n)$, of the first secret image S_A. Steps 5 through 8 are implemented by using the same structures as used in Steps 3 and 4.

Step 5: $G_2(i,(j+n/2)\%n) \leftarrow F_{RG}(S_B(i,(j+n/4)\%n), G_1(i,(j+n/4)\%n))$.

Step 6: $G_1(i,(j+n/2)\%n) \leftarrow F_{RG}(S_A(i,(j+n/2)\%n), G_2(i,(j+n/2)\%n))$.

Step 7: $G_2(i,(j+3n/4)\%n) \leftarrow F_{RG}(S_B(i,(j+n/2)\%n), G_1(i,(j+n/2)\%n))$.

Step 8: $G_1(i,(j+3n/4)\%n) \leftarrow F_{RG}(S_A(i,(j+3n/4)\%n), G_2(i,(j+3n/4)\%n))$.

Step 9: Repeat Steps 1 through 8 until the two shadow images, G_1 and G_2, are generated completely.

It can be observed that the shifting width in this algorithm is set to be one quarter, one half, or three quarters of the width of the second shadow when the visual distortion value is 1/4. If the distortion value is changed to 1/8, the shifting width should be set as one eighth, one quarter, three eighths, one half, five eighths, three quarters, or seven eighths, because the rule $\gcd(x,p) = 1$ must be satisfied. In such a case, the encryption phase has 17 steps.

Decryption Phase of Chang et al.'s Scheme: In order to decrypt the first secret image, the two generated shadows, G_1 and G_2, are stacked together without any shifting. To recover the second secret image, the first shadow, G_1, should be kept stationary, while the second shadow, G_2, is shifted horizontally from the right to the left. Chang *et al.* used the OR operation to stack the shadows, which can be printed on transparencies to make them visible to the human eye.

3. **Proposed Schemes.**

In this section, we propose two schemes with the aim of improving the visual quality of both recovered secret images and achieving reversibility. When stacking the two generated shadows to reveal the secrets, the OR operation is used in Chang *et al.*'s scheme, which requires no computational cost. However, the procedure of stacking the shadows may be difficult to align during the stacking procedure, and the visual quality of the recovered secret images cannot be completely equal to that of the original secrets. Therefore, we focused on reversibility and designed two schemes, each of which is described in the following subsection.

3.1. **Scheme I.**

In the encryption phase of proposed Scheme I, we used the same algorithm that Chang *et al.* used to encrypt the two secret images and to generate the same shadows, G_1 and G_2. But, for the decryption phase, we used the exclusive OR operation rather than the OR operation to recover the first secret image completely and to achieve much better quality of the contrast in the second recovered secret image. The exclusive OR operation can be implemented simply, and it has the advantage of making the recovered secret images clearer.

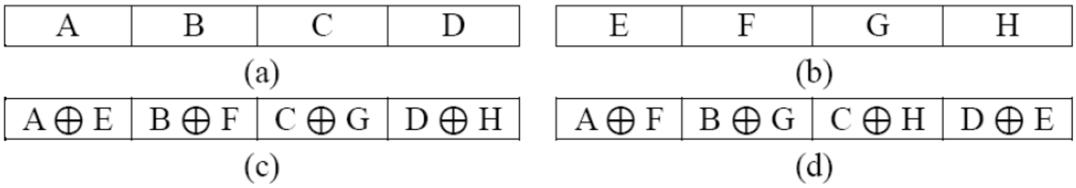

FIGURE 1. Scheme 1 partition illustration: (a) the first shadow image, (b) the second shadow image, (c) the first recovered secret by stacking the two shadows without shifting and (d) the second recovered secret by shifting 1/4 of the width of the image horizontally from the right to the left of the second shadow

By analyzing the OR and the exclusive OR operations in the decryption phase, we found that: 1) when using the OR operation, it has a probability of 1/4 to have the bit 0 as the stacking result, and it has a probability of 3/4 to have the bit 1 as the stacking result; 2) when using the exclusive OR operation, it has an equal probability to have bit 0 or bit 1 as the stacking result. Therefore, the exclusive OR operation can achieve a better visual quality than the OR operation. The results of stacking the two shadows by using the exclusive OR operation during the recovery of the first and second secret images are shown in Figure 1. We used a partition illustration to show the decryption phase of our Scheme I with 1/4 visual distortion. The shadow images were divided into four partitions, i.e., A, B, C, and D for the first shadow shown in Figure 1(a), and E, F, G, and H for the second shadow shown in Figure 1(b). After stacking the two shadows by using the exclusive OR operation, the first secret image was revealed, as shown in Figure 1(c). By shifting the partitions of the second shadow from the right to the left and stacking the two shadows, the second secret image was revealed, as shown in Figure 1(d).

3.2. **Scheme II.**

Scheme II can achieve reversibility for both recovered secret images, which is an improved version of Chang *et al.*'s scheme. The rule $\gcd(x, p) = 1$ is no longer followed in our improved scheme. In other words, we do not need to simplify the fractions of the shifting width. Therefore, if the visual distortion value is set to 1/4, the shifting width in Scheme II is set to one quarter (1/4), two quarters (2/4), or three quarters (3/4). In our Scheme II, we modified Step 1 of Chang *et al.*'s scheme to make the modular operation % unnecessary, since the range of the index position j no longer has to be corrected. Because of this modification, for the second recovered secret, we lost an area of visual information equal to the shifting quantity. However, by modifying Step 1 and using the exclusive OR operation instead, we can recover completely all of the visual information of the area that can be seen. The detailed steps of Scheme II with the horizontal shifting of 1/4 width are given in the paragraphs that follow, and the definitions of the functions $f_{RG}(\cdot)$ and $F_{RG}(\cdot)$ are the same as those in Subsection 2.2.

Step 1: Rather than choose a random binary pixel from the first secret, S_A, we chose the binary pixel, $S_A(i,j)$, where $i = 0, 1, \ldots, m-1$, and $j = 0, 1, \ldots, n/p - 1$. It means that a binary pixel of S_A was chosen from the position $i = 0$ to $i = m - 1$ and $j = 0$ to $j = n/p - 1$, because only the binary pixels of the first quarter of the image (if the visual distortion value is set to 1/4) are needed to generate the two shadows. Here, we define a new function $f_B(\cdot)$: $Y \leftarrow f_B(X)$, where Y is the output of the function $f_B(\cdot)$ with the input X, and the pixel of X is selected from the position $i = 0$ to $i = m - 1$ and $j = 0$ to $j = n/p - 1$ by $f_B(\cdot)$.

$$S_A(i,j) \leftarrow f_B(S_A). \tag{4}$$

Step 2: Generate the binary pixels, $G_1(i,j)$ and $G_2(i,j)$, for the shadows, G_1 and G_2, according to the selected binary pixel, $S_A(i,j)$, by using the random-grids algorithm [18].

$$G_1(i,j)\|G_2(i,j) \leftarrow f_{RG}(S_A(i,j)). \tag{5}$$

Step 3: Generate the binary pixel, $G_2(i, j + n/4)$, for the shadow, G_2, according to the generated binary pixel, $G_1(i,j)$, and the binary pixel, $S_B(i,j)$, of the second secret image, S_B.

$$G_2(i, j + n/4) \leftarrow F_{RG}(S_B(i,j), G_1(i,j)). \tag{6}$$

Step 4: Generate the binary pixel, $G_1(i, j + n/4)$, for the shadow, G_1, according to the generated binary pixel, $G_2(i, j + n/4)$, and the binary pixel, $S_A(i, j + n/4)$, of the first secret image, S_A.

$$G_1(i, j + n/4) \leftarrow F_{RG}(S_A(i, j + n/4), G_2(i, j + n/4)). \tag{7}$$

Step 5: Generate the binary pixel, $G_2(i, j + 2n/4)$, for the shadow, G_2, according to the generated binary pixel, $G_1(i, j + n/4)$, and the binary pixel, $S_B(i, j + n/4)$ of the second secret image, S_B.

$$G_2(i, j + 2n/4) \leftarrow F_{RG}(S_B(i, j + n/4), G_1(i, j + n/4)). \tag{8}$$

Step 6: Generate the binary pixel, $G_1(i, j + 2n/4)$, for the shadow, G_1, according to the generated binary pixel, $G_2(i, j + 2n/4)$, and the binary pixel, $S_A(i, j + 2n/4)$ of the first secret image, S_A.

$$G_1(i, j + 2n/4) \leftarrow F_{RG}(S_A(i, j + 2n/4), G_2(i, j + 2n/4)). \tag{9}$$

Step 7: Generate the binary pixel, $G_2(i, j + 3n/4)$, for the shadow, G_2, according to the generated binary pixel, $G_1(i, j + 2n/4)$, and the binary pixel, $S_B(i, j + 2n/4)$, of the second secret image, S_B.

$$G_2(i, j + 3n/4) \leftarrow F_{RG}(S_B(i, j + 2n/4), G_1(i, j + 2n/4)). \tag{10}$$

Step 8: Generate the binary pixel, $G_1(i, j + 3n/4)$, for the shadow, G_1, according to the generated binary pixel, $G_2(i, j + 3n/4)$, and the binary pixel, $S_A(i, j + 3n/4)$, of the first secret image, S_A.

$$G_1(i, j + 3n/4) \leftarrow F_{RG}(S_A(i, j + 3n/4), G_2(i, j + 3n/4)). \tag{11}$$

Step 9: Repeat Steps 1 through 8 until the two shadow images, G_1 and G_2, are generated fully.

If the visual distortion value is set to 1/8, then the shifting width should be set to one eighth, two eighths, three eighths, four eighths, five eighths, six eighths, or seven eighths since the rule $\gcd(x, p) = 1$ is no longer satisfied.

4. Experimental Results.

In the experiments, four secret images were used for testing, as shown in Figure 2. Figures 2(a) and 2(b) display two binary images of size 256×256, and Figures 2(c) and 2(d) display two halftone images transformed from standard grayscale images, i.e., Lena and Peppers, which are sized 512 × 512. The first algorithm of random grids in [18] was utilized in our proposed schemes, since it can achieve a better contrast quality.

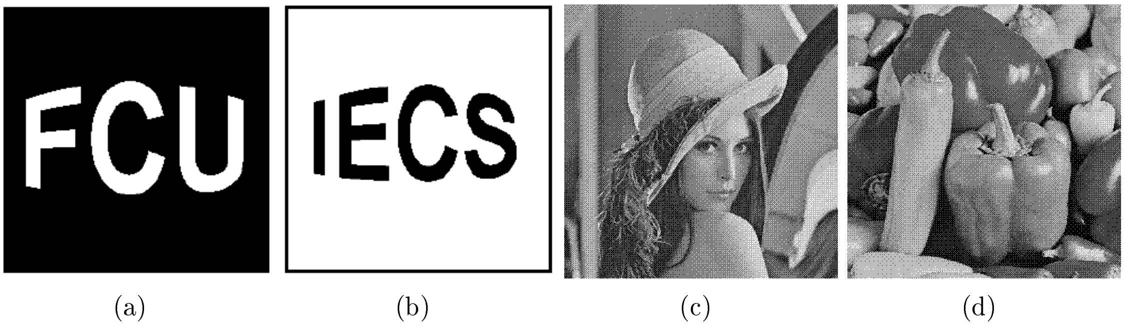

Figure 2. Four secret images tested: (a) binary secret image FCU, (b) binary secret image IECS, (c) halftone secret image Lena and (d) halftone secret image Peppers

First, we compared Chang *et al.*'s method [24] with the proposed Scheme I using the binary secret images in Figures 2(a) and 2(b). It can be seen from Figure 3 that, when the visual distortion value was 1/4, the proposed Scheme I achieved reversibility for the first recovered secret image and a much better visual quality for the second recovered secret image than those achieved by Chang *et al.*'s scheme. To evaluate the influence of the value of visual distortion on proposed Scheme I, another experiment was conducted by setting the value to 1/16. Figure 4 shows the results of the experiment. Apparently, the visual quality of the first recovered image was the same irrespective of the distortion value, while the visual quality of the second image in Figure 4 was much better than that in Figure 3 because a smaller number was assigned to the value of visual distortion. However, the execution time of the latter experiment was almost four times greater than it was in the experiment when the visual distortion was 1/4.

We also compared the results of proposed Scheme II by using both the OR and exclusive OR operations to demonstrate why proposed Scheme II used the exclusive OR operation rather than the OR operation when the value of visual distortion was set to 1/16. The results are shown in Figure 5. By comparing Figure 3 and Figure 4 with Figure 5, it can be seen that Scheme II with exclusive OR operation achieved better visual quality than by using the OR operation, since reversibility for both revealed secret images was achieved by using the exclusive OR operation. In Figure 5, it is obvious that 1/16 of the second secret image was lost in the second recovered image.

Next, we used the halftone images of Lena and Peppers in Figures 2(c) and 2(d) to test the effectiveness of proposed Scheme II, in which the value of visual distortion was set to 1/32. It can be observed from Figure 6 that the proposed Scheme II works well for

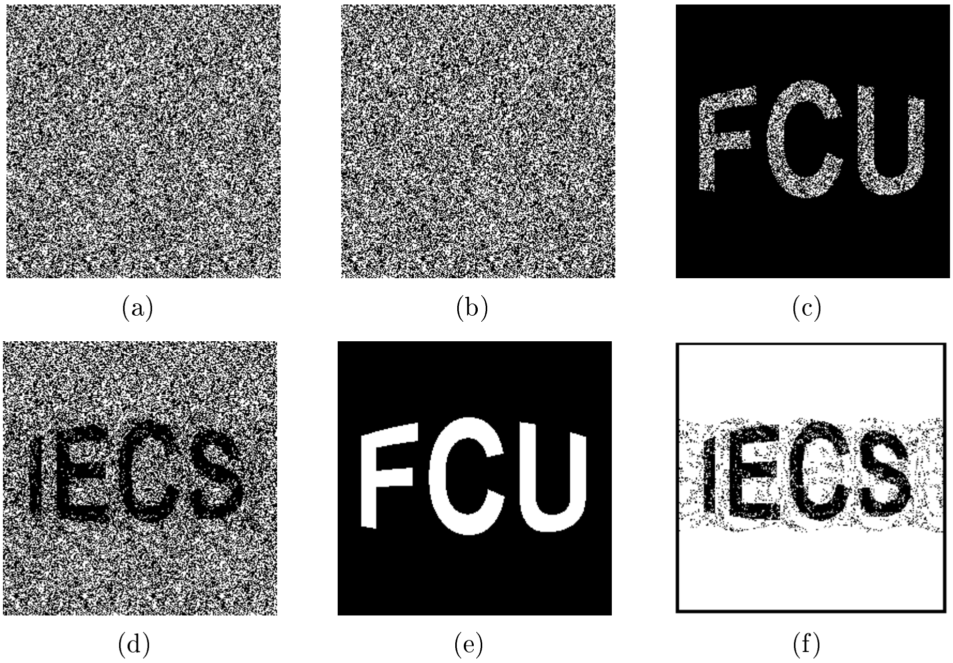

Figure 3. Comparison of the visual quality provided by proposed Scheme I and the scheme in [24] using a shifting width of 1/4; (a) the first shadow, (b) the second shadow, (c) the first recovered secret of [24], (d) the second recovered secret of [24], (e) the first recovered secret of Scheme I and (f) the second recovered secret of Scheme I

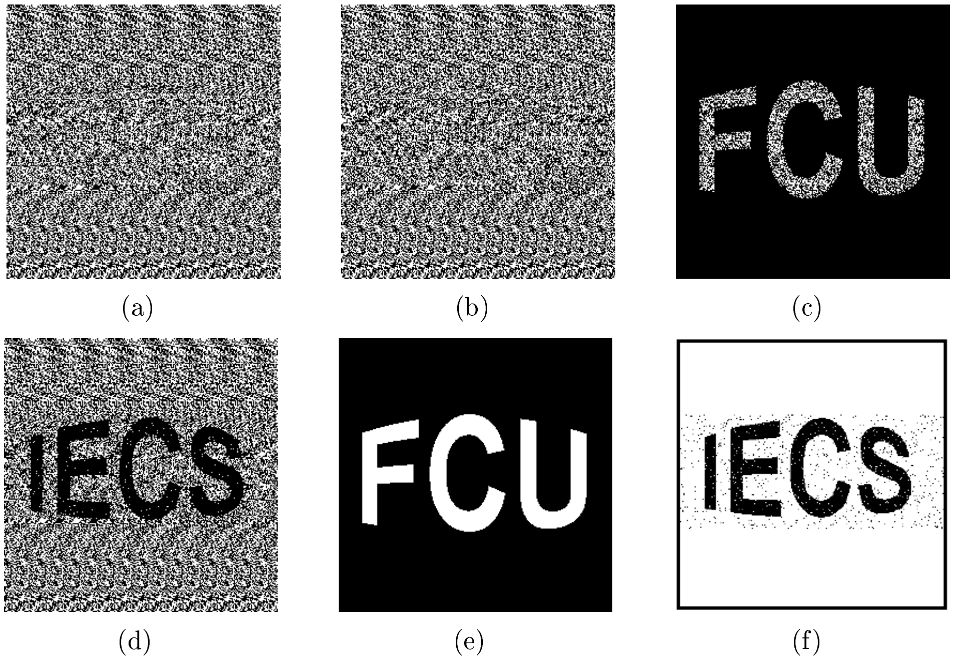

Figure 4. Comparison of the visual quality of proposed Scheme I and the scheme proposed in [24] using a shifting width of 1/16; (a) the first shadow, (b) the second shadow, (c) the first recovered secret of [24], (d) the second recovered secret of [24], (e) the first recovered secret of Scheme I, and (f) the second recovered secret of Scheme I

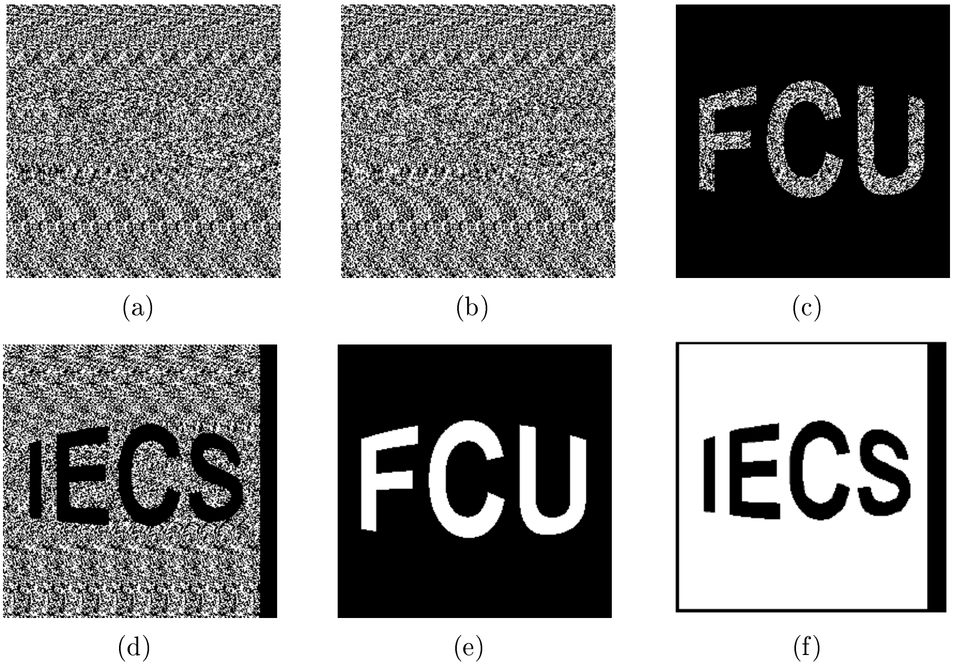

Figure 5. Comparison of visual quality between proposed Scheme II using OR and XOR with width shifting of 1/16; (a) the first shadow, (b) the second shadow, (c) the first recovered secret of Scheme II (OR), (d) the second recovered secret of Scheme II (OR), (e) the first recovered secret of Scheme II (XOR) and (f) the second recovered secret of Scheme II (XOR)

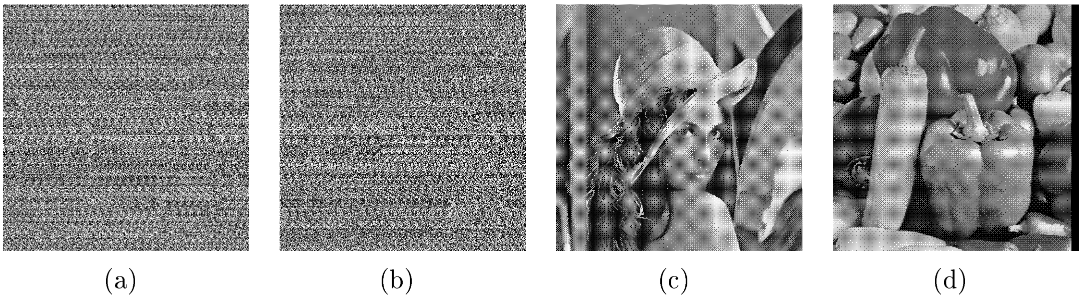

Figure 6. Test of effectiveness of proposed Scheme II with width shifting of 1/32 on halftone images; (a) the first shadow, (b) the second shadow, (c) the first recovered secret of Scheme II, and (d) the second recovered secret of Scheme II

halftone images. In addition, it is obvious that 1/32 of the second secret image was lost in the second recovered image.

From the experimental results shown in Figures 5 and 6, the influence of the value of visual distortion on proposed Scheme II is apparent, i.e., the value of visual distortion determines the size of the lost part of the second secret image in the second recovered secret image. The smaller the value of visual distortion is, the smaller the area of the second secret image that will be lost in the second recovered secret image. However, the value of visual distortion had the same influence on the execution time for proposed Scheme II as it had for proposed Scheme I. Therefore, the value of visual distortion makes our proposed schemes more flexible, which means the user can adjust the value of visual distortion depending on the requirements of different applications.

5. **Conclusions.** In this work, we proposed two schemes for improving the visual quality of the two decrypted secret images of Chang *et al.*'s schme [24]. The proposed Scheme I achieved lossless recovery of the first secret image and high visual quality for the second recovered secret image, which means that the visual quality of both of the recovered secret images is much better than that with Chang *et al.*'s scheme, so Scheme I is more applicable in visual authentication and identification applications. Proposed Scheme II can recover the entire content of the first secret image, but it lost some of the information in the second secret image based on the initial setting of the value of visual distortion. The greatest strength of proposed Scheme II is that it can achieve lossless recovery for all of the recovered content of the secret images, which is very useful in information hiding, especially when the hiding information is too important to allow any distortion, such as military information and medical information. Concerning the lost-content problem, the user could minimize the loss by setting the value of visual distortion to a smaller value or by moving the region of interest out of the shifting area to avoid any loss. In conclusion, the two schemes proposed in this paper achieved better visual quality for the extracted secret images than did Chang *et al.*'s scheme [24], and the user could use the extracted secret images in different applications according to their characteristics.

Acknowledgment. This work is supported by the Fundamental Research Funds for the Central Universities (No. 1600-852013) and the Postdoctoral Science Foundation of China (No. 20110491529).

REFERENCES

[1] A. Shamir, How to share a secret, *Communications of the ACM*, vol.22, no.11, pp.612-613, 1979.

[2] G. R. Blakley, Safeguarding cryptography keys, *Proc. of AFIPS 1979 National Computer Conference*, vol.48, pp.313-317, New York, USA, 1979.

[3] M. Naor and A. Shamir, Visual cryptography, *Proc. of the Advances in Cryptology-Eurocrypt, LNCS*, vol.950, pp.1-12, 1995.

[4] C.-C. Chen and C.-C. Chang, A digital image and secret messages sharing scheme using two stego images, *International Journal of Innovative Computing, Information and Control*, vol.6, no.4, pp.5797-5807, 2010.

[5] T. D. Kieu, and C.-C. Chang, A reversible watermarking scheme with high payload and good visual quality for watermarked images, *International Journal of Innovative Computing, Information and Control*, vol.7, no.11, pp.6203-6218, 2011.

[6] C. Guo, C.-C. Chang and Z.-H. Wang, A new data hiding scheme based on DNA sequence, *International Journal of Innovative Computing, Information and Control*, vol.8, no.1(A), pp.139-149, 2012.

[7] C. Blundo, A. D. Santis and M. Naor, Visual cryptography for grey level images, *Information Processing Letters*, vol.75, no.6, pp.255-259, 2000.

[8] M. Iwamoto and H. Yamamoto, The optimal n-out-of-n visual secret sharing scheme for gray-scale images, *IEICE Transactions Fundamentals*, vol.E86–A, no.10, pp.2238-2247, 2003.

[9] C. C. Lin and W. H. Tsai, Visual cryptography for gray-level images by dithering techniques, *Information Processing Letters*, vol.110, no.7, pp.241-246, 2010.

[10] Y. C. Hou, Visual cryptography for color images, *Pattern Recognition*, vol.36, no.7, pp.1619-1629, 2003.

[11] S. J. Shyu, Efficient visual secret sharing scheme for color images, *Pattern Recognition*, vol.39, no.5, pp.866-880, 2006.

[12] F. Liu, C. K. Wu and X. J. Lin, Colour visual cryptography schemes, *IEEE Transactions on Image Processing*, vol.5, no.8, pp.2441-2453, 2008.

[13] C. Blundo and A. D. Santis, Visual cryptography schemes with perfect reconstruction of black pixels, *Computers & Graphics*, vol.22, no.4, pp.449-455, 1998.

[14] C. N. Yang, New visual secret sharing schemes using probabilistic method, *Pattern Recognition Letters*, vol.25, no.4, pp.481-494, 2004.

[15] D. Wang, L. Zhang, N. Ma and X. Li, Two secret sharing schemes based on Boolean operations, *Pattern Recognition*, vol.40, no.10, pp.2776-2785, 2007.

[16] S. J. Shyu and M. C. Chen, Optimum pixel expansions for threshold visual secret sharing schemes, *IEEE Transactions on Information Forensics and Security*, vol.6, no.3, pp.960-969, 2011.

[17] P.-Y. Pai, C.-C. Chang, Y.-K. Chan and C.-C. Liao, Meaningful shadow based multiple gray level visual cryptography without size expansion, *International Journal of Innovative Computing, Information and Control*, vol.7, no.3, pp.1457-1465, 2011.

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

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

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

[21] T. H. Chen and K. H. Tsao, Threshold visual secret sharing by random grids, *Journal of Systems and Software*, vol.84, no.7, pp.1197-1208, 2011.

[22] T. H. Chen and K. H. Tsao, User-friendly random grid-based visual secret sharing, *IEEE Transactions on Circuits and Systems for Video Technology*, vol.21, no.11, pp.1693-1703, 2011.

[23] T. H. Chen, K. H. Tsao and K. C. Wei, Multiple-image encryption by rotating random grids, *Proc. of the 8th International Conference on Intelligent System Design and Applications*, vol.3, pp.252-256, 2008.

[24] J. Y. Chang, M. J. Li, Y. C. Wang and S. T. Juan, Two-image encryption by random grids, *Proc. of International Symposium on Communications and Information Technologies*, pp.458-463, 2010.