Image Sharing Method Using Somewhat Homomorphic Encryption and Random Grid

Hao-Kuan Tso

Department of Computer Science and Communication Engineering, Army Academy R.O.C.

Taoyuan 320, Taiwan, ROC

haokuantso@gmail.com

Received 26 August 2013; Revised 13 January 2014; Accepted 18 January 2014

Abstract. In recent years, image sharing method has become a popular technique due to the characteristics of security and simplicity. However, pixel expansion and bad image contrast are two common disadvantages that must be improved. This paper proposes an image sharing method to improve the problems mentioned above. First, the homomorphic encryption is utilized to enhance the security of digital images. Then the algorithm of random grid is utilized to construct the non-expanded shares. Furthermore, performing XOR and modular operations can completely recover the original secret images. Experimental results show the effectiveness of the proposed method.

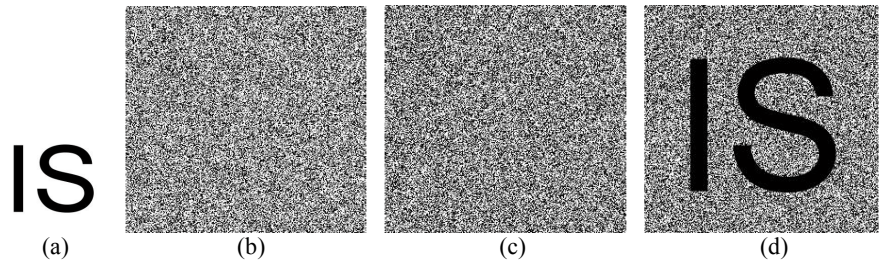
Keywords: image sharing, homomorphic encryption, random grid, pixel expansion, image contrast.

1 Introduction

With the development of computer network, digital information can be rapidly transmitted and received among businesses and organizations so that they can save much time and cost. However, unprotected information transmitted through networks can be easily attacked by unauthorized people. Once the important information is illegally utilized, the benefit of businesses and organizations can cause great damage. Therefore, protecting the security of digital information has become an important work.

In recent years, image sharing technique, firstly proposed by Naor and Shamir [1], has been eagerly discussed due to the characteristics of security and simplicity. The basic principle is encoding an image into several noise-like shares and assigning to different participators. Any participator cannot obtain the original image from one of the shares unless superimposing all of the shares. Table 1 shows a 2-out-of-2 codebook of image sharing, where white and black pixels represent 0 and 1 respectively. If a pixel of an image is white, one of four pairs can be randomly selected from the upper side of the codebook to construct into share 1 and share 2. On the other hand, if a pixel of an image is black, one of four pairs can be randomly selected from the lower side of the codebook. After consecutively processing all pixels, two noise-like shares can be constructed.

An example of image sharing is shown in Fig 1. First an image with size of 256×256 (as shown in Fig. 1(a)) is encoded into two shares with size of 512×512 (as shown in Fig. 1(b) and Fig. 1(c)) by using the codebook of Table 1. Then two shares are distributed to different participators. The original image can be recovered by collecting and superimposing two shares (shown as Fig. 1(d)). The main disadvantage is that the constructed shares are four times the size of the original image, which thus increases the storage space for protectors. Furthermore, the image contrast of retrieved result is not ideal and may result in fault judgment by authenticators.



(a) (b) (c) (d)

Fig. 1. (a) The secret image with size of 256×256, (b)-(c) the shares with size of 512 ×512 (d) the recovered image with size of 512×512

Table 1. The codebook of 2-out-of-2 sharing method

Pixel	Share 1	Share 2	Stacked results
□	■■ / □□	■■ / □□	■■ / □□
	□■ / ■□	□■ / ■□	□■ / ■□
	■□ / □■	■□ / □■	■□ / □■
	□□ / ■■	□□ / ■■	□□ / ■■
■	□■ / ■□	■□ / □■	■■ / ■■
	■■ / □□	□□ / ■■	■■ / ■■
	■□ / □■	□■ / ■□	■■ / ■■
	□□ / ■■	■■ / □□	■■ / ■■

In recent years, the image sharing techniques based on random grid [2-9] have been proposed to improve the disadvantage of pixel expansion. The algorithms of random grid can be described as follows.

[Algorithm 1]

1. Generate a random grid $R1$, where $R1$ consists of random value of 0 or 1.
2. For every pixel of the image S:

```
for i = 1 to m;
    for j = 1 to n;
        if S(i, j) == 0;
            R2(i, j) = R1(i, j) ;
        else
            R2(i, j) = R1(i, j) ;
        end
    end
end
```

where m and n represent the length and width of an image respectively, $\overline{R1}$ represents the complement of $R1$.

3. Output random grids $R1$ and $R2$.

[Algorithm 2]

1. Generate a random grid $R1$, where $R1$ consists of random value of 0 or 1.
2. For every pixel of the image S:

```
for i = 1 to m;
    for j = 1 to n;
        if S(i, j) == 0;
            R2(i, j) = R1(i, j) ;
        else
            R2(i, j) = Random _ pixel(0, 1) ;
        end
    end
end
```

where *m* and *n* represent the length and width of an image respectively, *Random_pixel*(0, 1) represents the function that consists of random value of 0 or 1.

3. Output random grids *R*1 and *R*2.

[Algorithm 3]

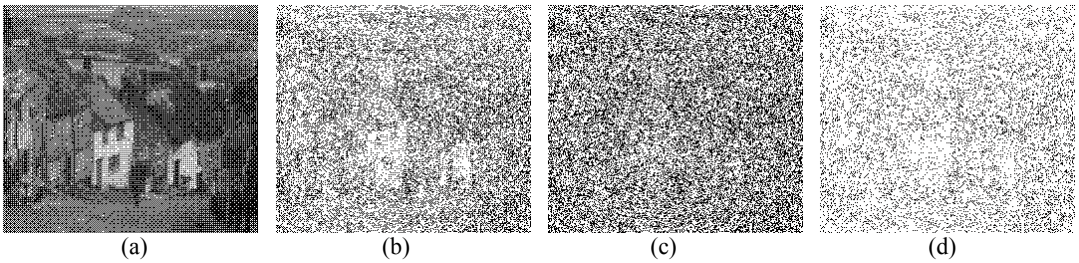
1. Generate a random grid *R*1, where *R*1 consists of random value of 0 or 1.
2. For every pixel of the image *S*:

```
for i = 1 to m;
    for j = 1 to n;
        if S(i, j) == 0;
            R2(i, j) = Random _ pixel(0, 1);
        else
            R2(i, j) = R1(i, j);
        end
    end
end
```

where *m* and *n* represent the length and width of an image respectively, *Random_pixel*(0, 1) represents the function that consists of random value of 0 or 1.

3. Output random grids *R*1 and *R*2.

Furthermore, by performing OR operation between the shares, the secret image can be recovered shown in Fig 2. As you can see, the recovered images cannot be identified clearly. The results will cause the fault judgment for authenticators.



(a) (b) (c) (d)

Fig. 2. (a) The secret image with size of 256×256, (b)-(d) the recovered images with size of 256×256 by using algorithms 1, 2 and 3

In 2007, Shyu [3] utilized the algorithms of random grid to construct the non-expanded shares. First a gray-scale image is transformed into halftone image. Then the halftone image is encoded into two shares by utilizing the algorithms of the random grid. In 2011, Chen and Tsao [4] proposed a threshold image sharing method where the algorithms of random grid are utilized to encode a binary image into *n* shares. Less than *k* ($k \le n$) shares cannot recover the secret image unless greater than or equal to *k* shares are superimposed. The common disadvantage of the two methods is that the contrast of the recovered image is not ideal and may result in fault judgment by authenticators.

In 2013, Guo et al. [7] proposed a threshold sharing method with improved contrast to improve the disadvantage of Chen and Tsao [4]. Although the experimental results show that the proposed method improves the contrast of Chen and Tsao's method, the quality of the recovered image is not ideal. Wu and Sun [8] also proposed a random grid-based sharing method with abilities of OR and XOR decryptions to improve the contrast of the recovered image. When the computational devices are not available, the original image can be recovered by superimposing the shares. On the other hand, when the computational devices are available, the original image with better contrast can be recovered by performing XOR operation. Although the image contrast has been improved, the original images cannot be completely recovered.

As one can see, the contrast of image recovery should be improved for avoiding the fault judgement. Furthermore, the security of secret image should be enhanced for preventing unauthorized access. This paper proposes an image sharing method by utilizing homomorphic encryption and the algorithm of random grid to overcome the problem. First the homomorphic encryption is applied to the secret image to generate an encrypted

image. Then the algorithm of random grid is utilized to construct the non-expanded shares. Furthermore, by performing XOR and modular operations, the secret image can be completely recovered.

The rest of the paper is organized as follows. Section 2 describes the somewhat homomorphic encryption method. Section 3 describes the proposed scheme. The experimental results are shown in Section 4. Finally, the conclusions are drawn in Section 5.

2 Somewhat Homomorphic Encryption

Homomorphic encryption is a form of encryption that can allow users without the decryption key to compute any result of the data and keep data confidential. Due to the characteristic of security, the homomorphic encryption has been used in the applications of electronic voting and cloud computing. A simple encryption method called "somewhat homomorphic encryption" is described as follows [10-11].

To encrypt a bit m, first an odd number p is generated as the sharing key. Then we randomly choose two parameters q and r, where r is sufficiently smaller than the key p. Finally by using Eq. (1), the ciphertext c can be outputted.

$$c = p * q + 2 * r + m. \tag{1}$$

Furthermore, the original bit m can be recovered by using Eq. (2).

$$m = (c \bmod p) \bmod 2. \tag{2}$$

For example, we set p, q, r, and m equal to 11, 3, 2, and 1 respectively. After taking the parameters into Eq. (1), we can obtain the ciphertext c=38. To recover the plaintext, we take the parameters c=38 and p=11 into Eq. (2) and obtain m=1. The recovered and original plaintexts are equal. Therefore, the method can be utilized to completely recover the original information.

3 The Proposed Method

3.1 Image Sharing

First, the somewhat homomorphic encryption is utilized to enhance the security of secret image. Then the algorithm of random grid is utilized to construct the non-expanded shares. The detailed steps are illustrated as follows.

Step 1. Generate an odd number p as the sharing key as follows

```
do
p = n * Int(rand( ))
loop until p mod 2 <> 0
```

where n represents an integer and *rand* represents a random number between 0 and 1.

Step 2. Generate two random images q and r with size of $m \times n$, where q and r consists of random value of 0 or 1 respectively.

Step 3. Consecutively take the related parameters and pixel of the secret image S with size of $m \times n$ into Eq. (3) and obtain the encrypted image E.

$$E(i, j) = p * q(i, j) + 2 * r(i, j) + S(i, j). \tag{3}$$

Step 4. Generate a random grid RG_1 that is same size as the secret image, where RG_1 consists of random value of 0 or 1.

Step 5. Decompose the encrypted image into bit planes and take every bit plane and random grid RG_1 into the algorithm of random grid respectively as follows.

```
if E^L(i, j) == 0;
    RG_2^L(i, j) = RG_1(i, j) ;
else
    RG_2^L(i, j) = ¬RG_1(i, j) ;
```

where E^L represents the bit plane of the encrypted image E, L represents the range from 1 to $\lceil \log_2 c \rceil$, c represents the largest value in the encrypted image E. For example, if c is equal to 255, we will obtain L=8 by performing the above operation.

Step 6. Superimpose the result of step 5 to obtain L-bit random image RG_2.

3.2 Image Recovery

The recovery process is quite simple. By performing XOR and modular operations, the secret image can be recovered. The detailed steps are illustrated as follows.

Step 1. Decompose random grid RG_2 into bit planes and consecutively perform XOR operation between RG_1 and RG_2 as Eq. (4).

$$E^L(i,j) = RG_1(i,j) \oplus RG_2^L(i,j). \tag{4}$$

Step 2. Superimpose the result of step 1 to obtain the encrypted image.

Step 3. Perform modular operation as Eq. (5) to recover the secret image.

$$S(i,j) = (E(i,j) \bmod p) \bmod 2. \tag{5}$$

4 The Experimental Results

In the first experiment, the binary image "Lena" with size of 256×256 is utilized to be the secret image shown as Fig. 3(a). First we encrypt the secret image by utilized the algorithm of somewhat homomorphic encryption and obtain the encrypted image (Fig. 3(b)), where the parameters p is set 13, q and r are two random image with the size of 256×256. From the appearance of the encrypted image, we cannot obtain any information about the secret image. The following work is to construct the shares. We utilize a pseudo random number generator to generate the random grid RG_1 (Fig. 3(c)). Furthermore, by using the algorithm of random grid and superimposing all of bit planes, the random grid RG_2 can be constructed (Fig. 3(d)). As you can see, the constructed random grid is of no pixel expansion and cannot reveal any information about the secret image.

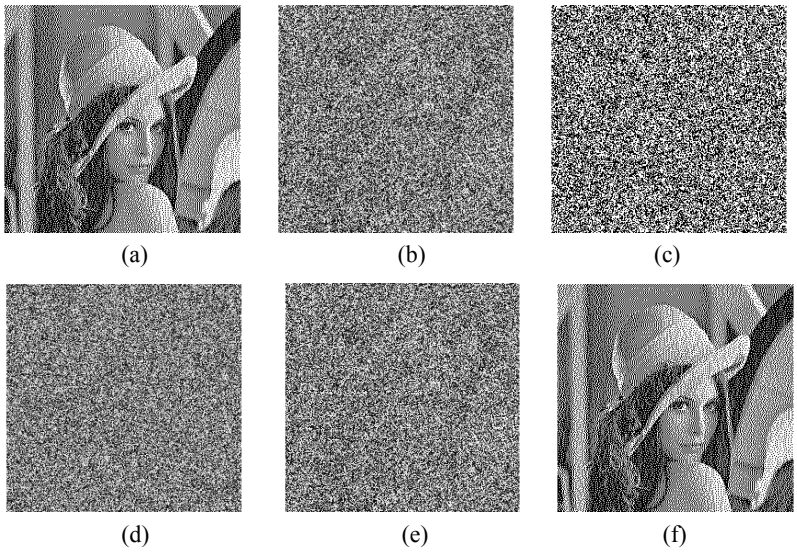


Fig. 3. (a) The secret image with size of 256×256, (b) the encrypted image, (c)-(d) the shares RG_1 and RG_2 with size of 256×256, (e)-(f) the recovered encrypted image and secret image

To recover the secret image, we first decompose the random grid RG_2 into bit plains and perform XOR operation between the random grids RG_1 and RG_2 to obtain the encrypted image as Fig. 3(e). By performing modular operation, the secret image can be completely recovered without distortion (Fig. 3(f)).

In the second experiment, the binary image "Bird" with size of 256×256 is utilized to be the secret image shown as Fig. 4(a). Fig 4(b) represents the encrypted image, where the parameters p is set 11. Fig 4(c) and Fig.

4(d) represent the constructed random grids RG_1 and RG_2. Fig 4(e) and Fig. 4(f) represent the recovered encrypted image and secret image respectively.

Traditional image sharing method has the problem of pixel expansion. Some published methods based on random grid have been proposed to improve the disadvantage. However, bad recovery quality is the common disadvantage [4-5], [7-8] that must be improved. From the above experiments, the constructed shares are of no pixel expansion and the secret image can be completely recovered. Therefore, the proposed method improves the disadvantages of pixel expansion and bad image quality. Table 2 shows the results compared with some published methods. As you can see, the proposed method outperforms some published methods.

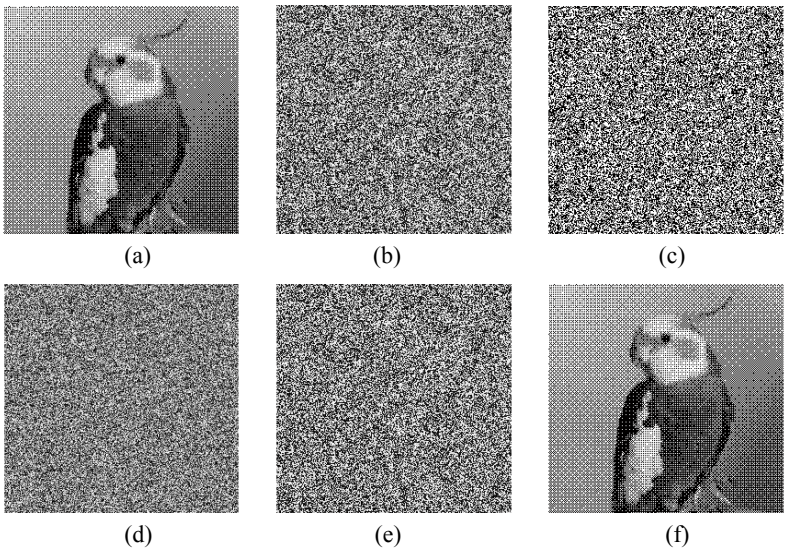
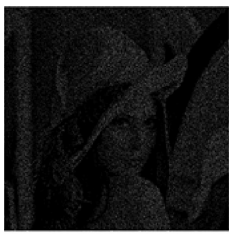


Fig. 4. (a) The secret image with size of 256×256, (b) the encrypted image, (c)-(d) the shares RG_1 and RG_2 with size of 256×256, (e)-(f) the recovered encrypted image and secret image

Table 2. The results compared with some published methods

Method	Chen-Tsao' method (2011)	Guo et al's method	The proposed method
Base	Random grid	Random grid	Random grid
Recovered results			

5 Conclusions

Image sharing method can be used to protect the security of secret images. However, pixel expansion and bad image contrast are two main disadvantages that must be improved. Furthermore, the security of secret image should be enhanced for preventing unauthorized access. The paper first utilizes somewhat homomorphic encryption to enhance the security of secret image. Then the algorithm of random grid is utilized to construct the non-expanded shares. Furthermore, by performing XOR and modular operations, the secret image can be completely recovered. In the future, the threshold sharing method and meaningful shares will be the main research topics.

Acknowledgment

The authors would like to thank the anonymous referees and the editor for their valuable opinions. This work was supported in part by National Science Council of the Republic of China under grants NSC 101-2221-E-539-005-.

References

[1] N. Naor and A Shamir, "Visual Cryptography," *Advances in Cryptology*, Vol. 950, pp. 1-12, 1995.

[2] O. Kafri and E. Keren, "Encryption of Pictures and Shapes by Random Grids," *Optics Letters*, Vol. 12, pp. 377-379, 1987.

[3] S.J. Shyu, "Image Encryption by Random Grids," *Pattern Recognition*, Vol. 40, pp. 1014-1031, 2007.

[4] T.H. Chen and K.H. Tsao, "Threshold Visual Secret Sharing by Random Grids," *The Journal of Systems and Software*, Vol. 84, pp. 1197-2008, 2011.

[5] T.H. Chen and K.H. Tsao, "Visual Secret Sharing by Random Grids Revisited," *Pattern Recognition*, Vol. 42, pp. 2203-2217, 2009.

[6] H.K. Tso and D.C. Lou, "Sharing Secret Image Based on Random Grids," *Proceedings of The Second International* Workshop *on Multimedia, Information Privacy and Intelligent Computing Systems*, Vol. 2, pp. 399-403, 2009.

[7] T. Guo, F. Liu, C.K. Wu, "Threshold Visual Secret Sharing by Random Grids with Improved Contrast," *The Journal of Systems and Software*, Vol. 86, No. 8, pp. 2094-2109, 2013.

[8] X.T. Wu and W. Sun, "Random Grid-Based Sharing Method with Abilities of OR and XOR Decryptions," *Journal of Visual Communication and Image Representation*, Vol. 24, No. 1, pp. 48-62, 2013.

[9] S.K. Chen, "A 2 out of 3 Visual Multiple Secret Sharing Method Using Generalized Random Grids," *Journal of Computers*, Vol. 22, pp. 48-56, 2011.

[10] M.V. Dijk, C. Gentry, S. Halevi, V. Vaikuntanathan, "Fully Homomorphic Encryption Over The Integers," *Advances in Cryptology*, Vol. 6110, pp. 24-43, 2010.

[11] C. Gentry, "Computing Arbitrary Functions of Encrypted Data," *Communications of the ACM*, Vol. 53, pp. 97-105, 2010.