Journal of Network Intelligence ©2016 ISSN 2414-8105 (Online)
Taiwan Ubiquitous Information Volume **1**, Number **1**, February **2016**

A Friendly and Verifiable Image Sharing Method

Wei-Kuei Chen, Hsin-Pei Chen, and Hao-Kuan Tso

Department of Computer Science and Information Engineering
Chien Hsin University of Science and Technology
Chungli, Taoyuan 320, Taiwan
wkchen@uch.edu.tw, hpchen@uch.edu.tw, haokuantso@uch.edu.tw

Received October, 2015; revised November, 2015

Abstract. *Image sharing is a secure technique to protect the security of the secret image by dividing an image into different shares. In 2011, Wang et al. proposed an image sharing method with verification which uses two equations to divide the secret image and watermark image into two shares to achieve the goal of image sharing. The above method can be used to verify the validity of the secret image. Besides, the method also removes the disadvantages of pixel expansion and lossy reconstruction. However, meaningless shares are the main disadvantage of the above method, which has improved in this paper. Furthermore, how to accelerate the computation speed of sharing image is also the goal of the paper. Experimental results show the efficiency of the proposed method.*

Keywords: Image sharing, friendly shares, verification, pixel expansion, lossless reconstruction

1. **Introduction.** With the rapid development of computer and network, transmitting data to a far country is more and more convenient. However, intruders can easily steal the information of the computers and networks. How to protect the security of the secret information has become an important work. Lots of cryptography algorithms have been proposed to prevent the attack of intruders. A well-known technique is called secret sharing proposed by Shamir [1] and Blakley [2]. The main concept is to divide the secret into m shares and transmit to m protectors. Collecting n or more than n shares $(0 < n \leq m)$ can recover the original secret. Furthermore, image sharing is also a secure technique proposed by Naor and Shamir [3] that can be used to protect the security of secret image. By dividing the secret into different shares, no one can recognize the information of the original image from any one of the shares. Only if superimposing the enough shares, the secret image can be recovered and recognized directly by human eyes.

Fig. 1 shows the example of the (2, 2) image sharing. By utilizing the codebook (Table 1), the secret image (Fig. 1(a)) can be encoded into two shares (Fig. 1(b) and Fig. 1(c)). No one can recover the original secret image from any one of the shares. By superimposing two shares, the information of the secret image can be revealed and recognized by human eyes (Fig. 1(d)). However, the disadvantages of the method are that the constructed shares are four times as large as the original secret image and the shares are meaningless images that are difficult to manage.

Lukac and Plataniotis [4] proposed a grayscale image sharing method based on the codebook. The grayscale image is firstly decomposed into different bit planes and every bit plane is encoded into two shares by using the codebook of Naor and Shamir method. The constructed shares are then stacked into two grayscale shares respectively. However, the constructed shares inherit the disadvantage of Naor and Shamir method that are still four times as large as the secret image. Although the method can recover the original

Table 1. The codebook of (2, 2) image sharing

Pixel	Share1	Share2	Stacking results
□	□□ ■■	□□ ■■	□□ ■■
	■■ □□	■■ □□	■■ □□
	■□ □■	■□ □■	■□ □■
	□■ ■□	□■ ■□	□■ ■□
■	□□ ■■	■■ □□	■■ ■■
	■■ □□	□□ ■■	■■ ■■
	■□ □■	□■ ■□	■■ ■■
	□■ ■□	■□ □■	■■ ■■

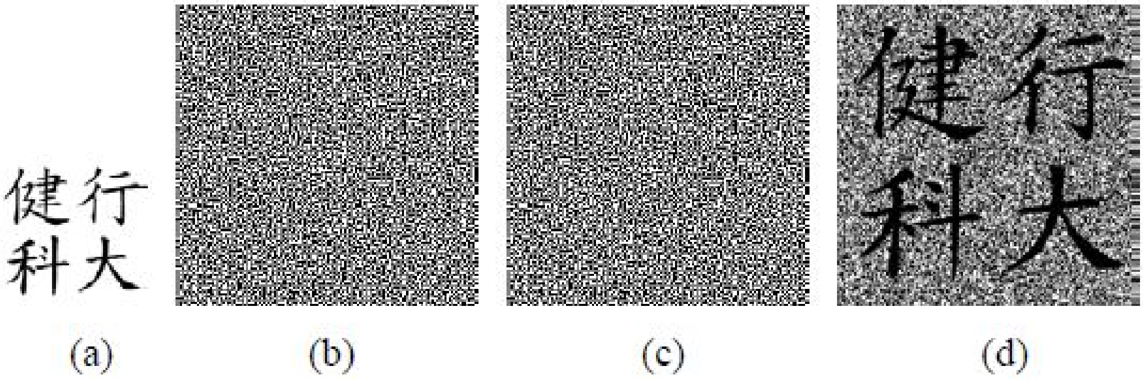

Figure 1. The sharing process, (a) the secret image, (b)-(c) the shares, (d) the recovered image

secret image without distortion, meaningless shares are another urgent problem that must be improved. Lin et al. [5] proposed a friendly image sharing method based on random grid. Friendly shares means that the constructed shares are meaningful that can be identified and managed conveniently. As you can see, the conventional method encodes the secret image into several meaningless shares. The more the shares are, the more difficult the management is. To easily manage the shares, the method firstly uses random grid algorithm to construct the meaningless images. Then the meaningful images are taken into the proposed algorithm to construct the meaningful shares. To recover the secret image, the proposed method can progressively reveal the information of the secret image by stacking the shares. The more the shares are stacked, the better the image quality is. Another advantage is that random-grid-based method has no the phenomenon of pixel expansion, which cannot cause a waste of storage space. However, the method cannot recover the original image without distortion. Wei et al. [6] proposed a new image sharing method based on the codebook and exclusive-or operation. The method uses different algorithms to construct the noise-like shares and meaningful shares by expanding the block size from 33 to 55, respectively. The recovered image can be recovered without distortion. However, the constructed shares are at least 9 times as large as the original image that cause a waste of storage space and transmission time.

The above-mentioned methods cannot prevent cheating problem. Hence, how to verify the validity of the image has become a popular issue in recent year. Wang et al. [7] proposed an image sharing method with verification. The method can recover the original secret image without distortion. First the watermark is embedded into the secret image to construct two noise-like shares by using two equations. The size of the constructed shares is the same as the secret image. Then the torus automorphism operation is used to enhance the security of the shares. In the recovering process, the torus automorphism operation is firstly used to permute two shares. Then two equations are used to recover the secret image and the watermark. Furthermore, the watermark can be used to identify the validity of the shares. By comparing the mean square error (MSE) between the recovered watermark and the original watermark, the participants can identify whether the cheating has occurred. If the MSE is equal to zero, it shows that the secret image is reliable. On the other hand, if the MSE is not equal to zero, it shows that the secret image is unreliable. However, meaningless shares are the main disadvantage of the method.

A and Thampi [8] applied Wang et al. method and proposed a secure verifiable sharing method. First a verifiable image and a secret image are taken into two equations as Wang et al. method to construct two shares. Due to the fact that the constructed shares can reveal the information of the original image. In order to scramble the information of the shares, authors use Arnold transform to construct two noise-like shares. Finally the noise-like shares are embedded into two cover images by using bit-plane complexity steganography (BPCS) technique. To verify the validity of the secret image, the method use MSE and structural similarity (SSIM) to verify whether the cheating problem has occurred. If the MSE is equal to zero or SSIM is equal to one, it shows that the secret image is reliable. On the other hand, if the MSE is not equal to zero or SSIM is not equal to one, it shows that the secret image is unreliable. However, the processes of image sharing consume much time. Based on the above discussions, the paper proposed a friendly and verifiable image sharing method. The rest of the paper is organized as follows. The proposed sharing method is described in Section 2. Experimental results are shown in Section 3. Conclusions are given in Section 4.

2. **The proposed method.** The proposed method consists of two processes: sharing and revealing and verification processes. The detailed processes are described as follows.

2.1. Sharing process.

- ***Input***: A secret image I, a verifiable image V and two cover images C^1 and C^2 with size of m by n.
- ***Output***: Two friendly shares F^1 and F^2 with size of m by n.
- *Step 1*: Take the first pixel of the secret image and the verifiable image into Eq. (1) and Eq. (2) respectively to obtain first pixel of two shares S^1 and S^2

$$S^1_{i,j} = (V_{i,j} + I_{i,j}) \bmod 2, \tag{1}$$

$$S^2_{i,j} = (1 + I_{i,j}) \bmod 2. \tag{2}$$

- *Step 2*: Repeat Step 1 until all pixels are processed
- *Step 3*: Perform torus automorphism operation to two shares and obtain two scrambled shares $\tilde{S}^1$ and $\tilde{S}^2$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ a & a+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod n \ , \tag{3}$$

- *Step 4*: Take the first pixel of two scrambled shares $\tilde{S}^1$ and $\tilde{S}^2$ and two cover image C^1 and C^2 into Eq. (4) and Eq. (5) respectively to obtain the first pixel of two friendly shares F^1 and F^2.

$$F^1_{i,j} = 2 \times C^1_{i,j} + \tilde{S}^1_{i,j}, \tag{4}$$

$$F^2_{i,j} = 2 \times C^2_{i,j} + \tilde{S}^2_{i,j}. \tag{5}$$

- *Step 5*: Repeat Step 4 until all pixels are processed.

2.2. **Revealing and verifivation process.**

- ***Input***: Two shares F^1 and F^2 with size of m by n
- ***Output***: The recovered secret image and the verifiable image with size of m by n
- Step 1: Decompose the shares F^1 and F^2 by using Eq. (4) and Eq. (5) to obtain two scrambled shares $\tilde{S}^1$ and $\tilde{S}^2$.
- *Step 2*: Perform torus automorphism operation to two scrambled shares and obtain two shares S^1 and S^2.
- *Step 3*: Take the first pixel of two shares into Eq. (6) and Eq. (7) respectively to obtain the first pixel of the verifiable image V and the secret image I.

$$V_{i,j} = (1 + S^1_{i,j} + S^2_{i,j}) \bmod 2, \tag{6}$$

$$I_{i,j} = (1 + S^2_{i,j}) \bmod 2. \tag{7}$$

- *Step 4*: Repeat Step 3 until all pixels are processed.
- *Step 5*: Compute the MSE between the original verifiable image and the reconstructed verifiable image.

$$\text{MSE} = \frac{1}{m \times n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (X_{ij} - X'_{ij})^{2} \ , \tag{8}$$

where X_{ij} and ${X_{ij}}'$ represent the original image and the reconstructed image respectively.

2.3. **The experimental results.** In the first experiment, the images "Lena" and "uch" with size 256 × 256 is utilized as the secret image and the verifiable image shown as Fig. 2(a) and Fig. 2(b). The images "1" and "2" with size 256 × 256 is utilized as the cover images shown as Fig. 2(c) and Fig. 2(d). First the images "Lena" and "uch" are taken into Eq. (1) and Eq. (2) to obtain two noise-like shares with size 256 × 256. To enhance the security, two noise-like shares are then performed the torus automoprism operation respectively to obtain the scrambled shares shown as Fig. 3(a) and Fig. 3(b). Finally, two cover images are respectively superimposed on the two scrambled shares by using Eq. (4) and Eq. (5) to obtain two friendly shares shown as Fig. 3(c) and Fig. 3(d). As you can see, the friendly shares are more convenient to manage and identify.

To recover the secret image, two friendly shares are firstly decomposed to obtain two scrambled shares. Then two scrambled shares are respectively performed the torus automoprism operation to obtain the two shares. Finally, two shares are taken into Eq. (6) and Eq. (7) to obtain the verifiable image and the secret image shown as Fig. 3(e) and Fig. 3(f). To verify the validity of the secret image, MSE is computed between the original verifiable image and the reconstructed verifiable image. If the MSE is equal to zero, it shows that the secret image is reliable. On the other hand, if the MSE is not

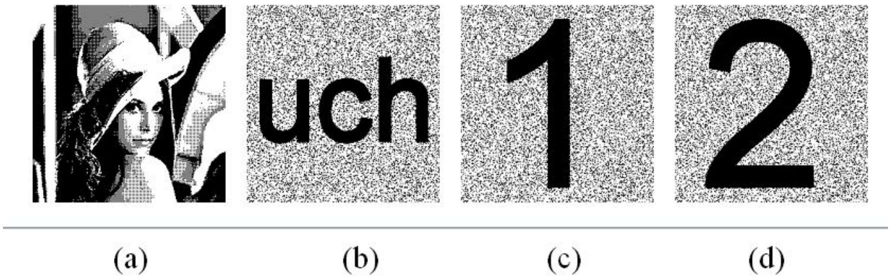

Figure 2. The experimental images, (a) the secret image, (b) the verifiable image, (c)-(d) the cover images

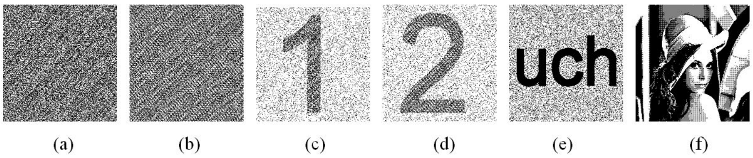

Figure 3. The experimental results, (a)-(b) the scramble images, (c)-(d) the friendly shares, (e) the recovered verifiable image, (f) the recovered secret image

equal to zero, it shows that the secret image is unreliable. In the first experiment, the computed result of MSE is zero that shows the recovered secret image is reliable.

In the second experiment, the images "peppers" and "csie" with size 256256 is utilized as the secret image and the verifiable image shown as Fig. 4(a) and Fig. 4(b). The images "5" and "6" with size 256256 is utilized as the cover images shown as Fig. 4(c) and Fig. 4(d). The same process is performed as the first experiment. The experimental results are shown as Fig. 5. In the second experiment, the computed result of MSE is zero.

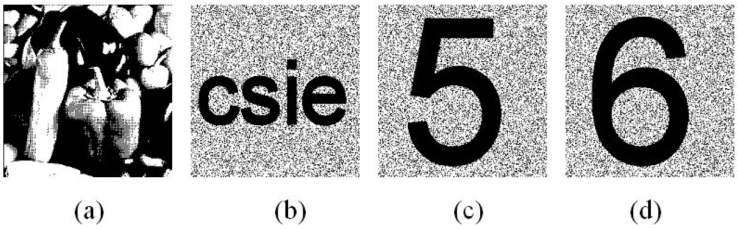

Figure 4. The experimental images, (a) the secret image, (b) the verifiable image, (c)-(d) the cover images

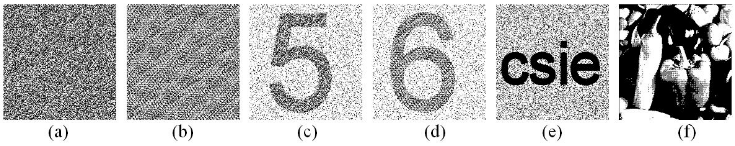

Figure 5. The experimental results, (a)-(b) the scramble images, (c)-(d) the friendly shares, (e) the recovered verifiable image, (f) the recovered secret image

Table 2. The comparison between Wang et al and the proposed method

Methods	Speed		Pixel	Verifiable	Friendly	Lossless
	Lena	Peppers	expansion	ability	shares	reconstruction
Wang et al. [7]	0.547s	0.546s	No	Yes	No	Yes
The proposed method	0.311s	0.297s	No	Yes	Yes	Yes

The comparison results between Wang et al. and the proposed method are shown as Table 2. The results show the proposed method outperforms Wang et al. method.

3. **Conclusions.** Image sharing method can protect the security of digital images by constructing different shares. However, the constructed shares should prevent cheating problem and are meaningful images so that the shares can be manage conveniently. Based on the above descriptions, the paper proposes a friendly and verifiable image sharing method to satisfy the above requirements. Table 2 shows the advantages of the proposed method.

Acknowledgments. The authors gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation

REFERENCES

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

[2] G. R. Blakley, Safeguarding cryptographic keys, *Proceedings of AFIPS Conference*, vol. 48, pp. 313-317, 1979.

[3] N. Naor and A Shamir, Visual cryptography, *Advanced in Cryptology*, vol. 950, pp. 1-12, 1995.

[4] R. Lukac and K. N. Plataniotis, Bit-level based secret sharing for image encryption, *Pattern Recognition*, vol. 38, pp. 767-772, 2005.

[5] C. H. Lin, Y. S. Lee, and T. H. Chen, Friendly progressive random-grid-based visual secret sharing with adaptive contrast, *Journal of Visual Communication and Image Representation*, vol. 33, pp. 31-41, 2015.

[6] S. C. Wei, Y. C. Hou, and Y. C. Lu, A technique for sharing a digital image, *Computer Standards & Interfaces*, vol. 40, pp. 53-61, 2015.

[7] Z. H. Wang, C. C. Chang, H. N. Tu, and M. C. Li, Sharing a secret image in binary images with verification, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 2, pp. 78-90, 2011.

[8] A. R. A and S. M Thampi, A secure verifiable scheme for secret image sharing, *Procedia Computer Science*, vol. 58, pp. 140150, 2015.