Secret Sharing Using Meaningful Images

Hao-Kuan Tso
Department of Computer Science and Communication Engineering, Army Academy R.O.C., Chungli, Taoyuan 320, Taiwan
E-mail: haokuantso@gmail.com

***Abstract*—In recent years, image sharing method has attracted much attention for protecting the security of secret images. Pixel expansion, meaningless sharing, and bad recovering quality are the important issues that need to be improved. The paper proposes a new image sharing method to remove the above problems. First a secret image is decomposed and encoded into *n* encoded images. Then the encoded images are embedded into the cover images to construct the meaningful sharing images. The size of the sharing images is the same with that of the secret image. When the sharing images are collected more, the recovered image is more and more clear. After collecting all sharing images, the secret image can be completely recovered without distortion. Experimental results show the feasibility of the proposed method.**

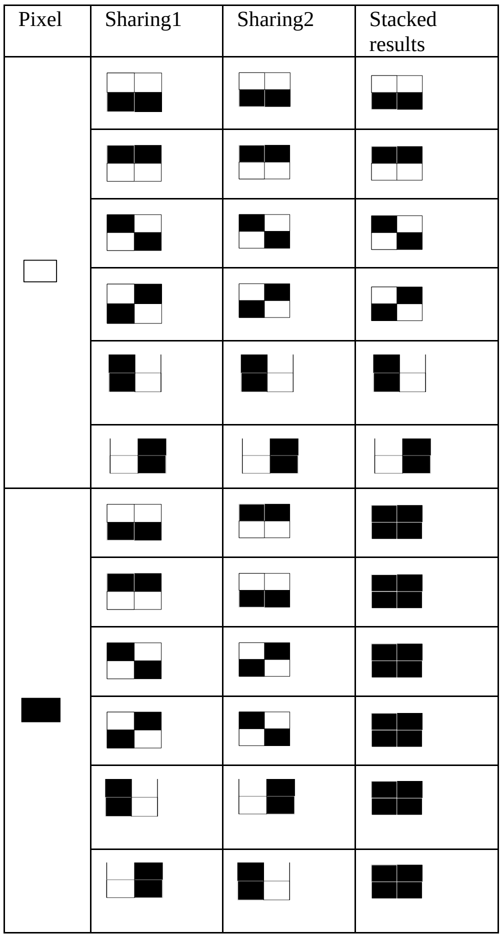
***Index Terms*—image sharing, data hiding, pixel expansion, meaningful sharing.**

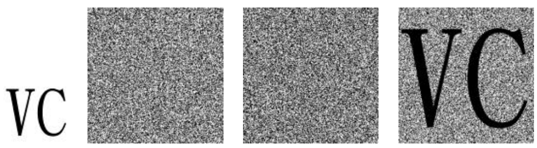
I. INTRODUCTION

The rapid development of Internet has caused the change of lifestyle. People can go shopping in virtual shop or transmit their message to distance friends by Internet, which has greatly saved their precious time. To prevent the sensitive message being stolen, many protection methods have been proposed, such as cryptography, data hiding and visual sharing. Cryptography is an ancient technique that has been used in daily life for a long time such as data encryption and E-commerce. By disordering process, the plaintext can be changed to meaningless cipher. No one can understand the real meaning unless the authorized users. Data hiding is to embed the important information into meaningful cover media (such as audio, image, video or text) which has become a popular technique due to the characteristics of transparency and security etc.

The two techniques have a common problem. If the information is once stolen, it will be very difficult to retrieve. To avoid causing the situation, the information should be protected among users. One of the emerging techniques is visual sharing firstly proposed by Naor and Shamir [1]. The main concept of visual sharing is to divide an image into different sharing images and transmit to different participant. From one of the sharing images, no one can obtain the information of the original image. When all sharing images are collected and superimposed, the information of the original image can be recovered and perceived by human eyes.

TABLE I. THE CODEBOOK OF THE (2, 2) SHARING METHOD.





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

Figure 1. (a) The secret image with size $m\times n$, (b)-(c) the sharing images with size $2m\times 2n$ (d) the recovered image with size $2m\times 2n$.

The example of the (2, 2) visual sharing method is illustrated as follows. First a codebook consisting of black and white is constructed (shown in Table I). Then the

Manuscript received September 15, 2012; revised December 28, 2012.
This work was supported in part by the National Science Council of the Republic of China under grants NSC 101-2221-E-539-005-.

©2013 Engineering and Technology Publishing
doi: 10.12720/joams.1.1.35-38

secret image can be encoded by the following rule. If a pixel of an image is white, two blocks with size 2×2 can be randomly selected from the top rows of Table I. On the other hand, if a pixel of an image is black, two blocks with size 2×2 can be randomly selected from the bottom rows of Table I. After encoding all pixels, two expanded sharing images can be constructed. No one can recover the original image from one of the shared images unless superimposing two sharing images. The sharing and superimposing process are shown as Fig. 1. As you see, the recovered image can be directly recognized by human eyes. However, the problem of pixel expansion is necessary to be improved.

Due to the characteristics of simpleness and easy implement, many researchers successively propose many improved methods [2]-[10]. Shyu [2] proposed the random grid based sharing method [11] to improve the problem of pixel expansion in 2003. Firstly a random grid that consists of 0 and 1 is randomly generated by using a random generator. Then the random grid and the secret image are used to construct the nonexpanded sharing images by using the random grid algorithm. Furthermore, superimposing the sharing images can recover the information of the secret image. Although Shyu's scheme can deal with binary, gray-level, and color images, the quality of the retrieved image must be improved.

After that, many extended methods are successively proposed. Wang et al. proposed the *n*-level incrementing sharing method by using the concept of random grid in 2010 [6]. The method firstly divides an image into multiple regions and then encodes them into *n*+1 sharing images, where each region belongs to one of the *n* secret levels. The *n* levels of the secret image can be recovered incrementally by superimposing the *n*+1 sharing images. The main advantage of the method is that the constructed sharing images have the same size with the secret image. However, the secret image cannot be completely recovered.

In recent years, progressive sharing method has attracted much attention. Fang proposed a friendly progressive sharing method in 2008 [7]. First a secret image is expanded from 256 ×256 to 512×512 pixels. Then the expanded secret image and the cover image are encoded into *n* meaningful sharing images by using the designed codebook. The secret image can be recovered incrementally by superimposing the sharing images. When *n* sharing images are superimposed, the secret image can be completely recovered. Wang and Shyu proposed the scalable image sharing method with multisecret, priority, and progressive modes [9]. The secret image can be partitioned according to users' demand and the information of the secret image can be recovered by combining different sharing images.

Wang et al. proposed a visual sharing method with verification ability in 2011 [10]. The method firstly utilizes the equations to encode a watermark image and a secret image into two nonexpanded sharing image. Then the torus automorphism is utilized to scramble the two sharing images. Furthermore, the reverse process can be performed to recover the original watermark image and secret image. The disadvantage of the above method is that the constructed sharing images can appear the rough information of the original image. Although the torus automorphism can be utilized to increase the security of the sharing images, it will consume much time to scramble the images. Furthermore, the constructed sharing images are meaningless which are difficult to manage. To remove the disadvantages, the paper proposes a new sharing method using meaningful images.

The rest of the paper is organized as follows. Section Ⅱ describes the proposed scheme. The experimental results are shown in Section Ⅲ. Finally, the conclusions are given in Section Ⅳ.

II. Proposed Method

A. Image Sharing

The problems of pixel expansion, meaningless sharing and bad recovering quality are necessary to be improved. The proposed image sharing method can remove the above disadvantages simultaneously. The detailed processes are described as follows.

1) Decompose the 8-bit gray-level image into eight bit-planes.

2) Utilize a seed to generate the random numbers R with the length of m×n.

3) Take the bit-plane B, the authorized image A and the random numbers R into (1) and obtained the encoded image.

$$E_{i,j} = (2 \times B_{i,j} + A_{i,j} + R_k) \bmod 2 \tag{1}$$

where k=0…m×n.

4) Embed the encoded image E into the cover image C by using (2) and obtain the meaningful sharing image M.

$$M_{i,j} = 2 \times C_{i,j} + E_{i,j}. \tag{2}$$

5) Repeat Step 3 to Step 4 to obtain the other sharing images.

Note that the seed and authorized image must be kept secret.

B. Image Recovery

The secret image can be incrementally recovered when superimposing more encoded images. The image recovery process is described as follows.

1) Collect the meaningful sharing images.

2) Extract the encoded image E from the meaningful sharing image M by using (3).

$$E_{i,j} = M_{i,j} \bmod 2. \tag{3}$$

3) Utilize the seed to generate the random numbers R with the length of m×n.

4) Take the encoded image E, the authorized image A and the random numbers R *into (4) and obtain the bit-plane B.*

$$B_{i,j} = (2 \times A_{i,j} + E_{i,j} + R_k) \bmod 2. \tag{4}$$

5) Repeat Step 2 to Step 4 to recover the other encoded images.

6) Superimpose the bit-planes to recover the information of the secret image.

III. Experimental Results

The experimental results of the proposed method are described in the section. The gray-level image and binary image with size 256×256 pixels are utilized to be the secret image and the authorized image. Furthermore, eight cover images with size 256×256 pixels are utilized to embed the encoded images shown as Fig. 2(a) to Fig. 2(j) respectively. The gray-level image is firstly decomposed into eight bit-planes (as shown in Fig. 3). Then the bit-planes, the authorized image and the random numbers are successively taken into (1). Finally the encoded images can be obtained shown as Fig. 4. To conveniently manage the sharing images and avoid attracting the attackers' attention, the encoded images are successively embedded into the cover images to construct the meaningful sharing images shown as Fig. 5.

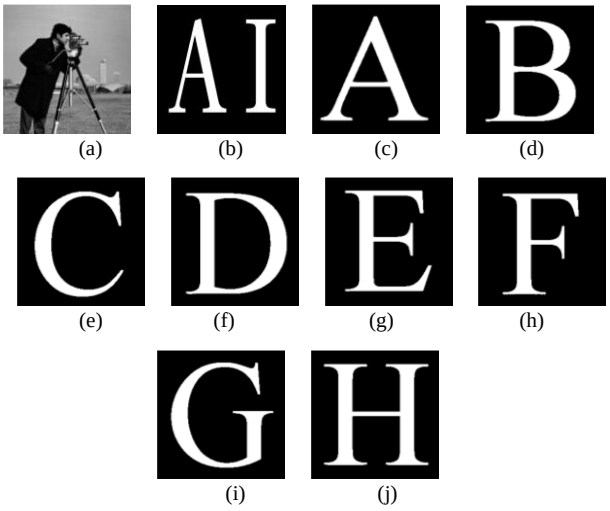


Figure 2. (a) The secret image, (b) the authorized image, (c) to (j) the cover images.

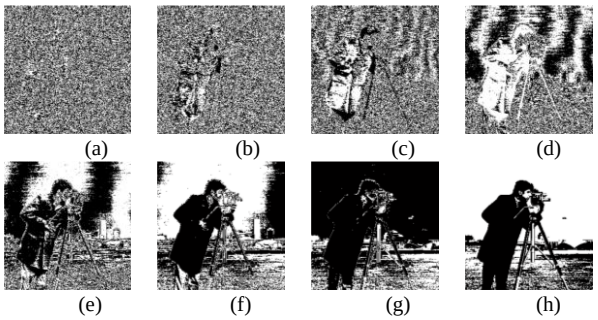


Figure 3. (a) to (h) The decomposed bit-plans (bit-plane 1 to 8).

To recover the information of the secret image, first the encoded images must be extracted from the meaningful sharing images according to users' demand. Then the encoded image, the authorized image and the random numbers are taken into (4) to obtained different bit-plane. Fig. 7 shows the recovered image by superimposing different bit-plane. Fig. 6 to Fig. 8 show the different resolution of the secret image respectively. When all bit-planes are superimposed, the original secret image can be completely recovered without distortion.

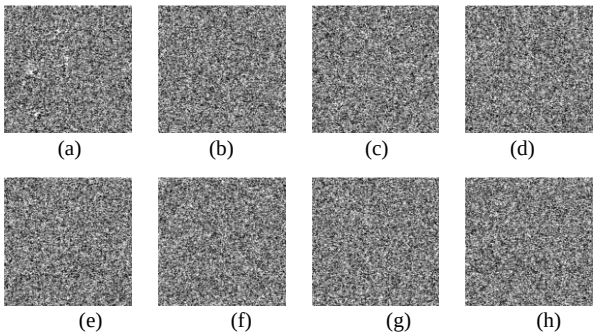


Figure 4. (a) to (h) The encoded bit-plans (bit-plane 1 to 8).

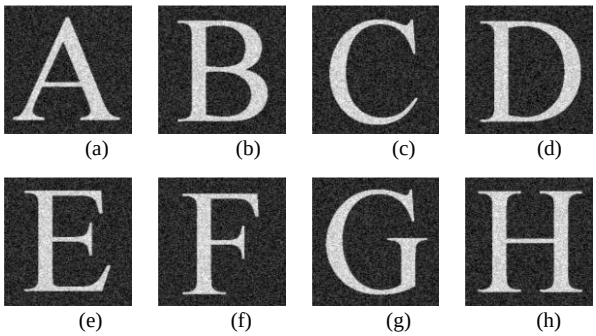


Figure 5. (a) to (h) The results of embedding the encoded images into the cover images.

Figure 6. The retrieved results by superimposing different bit-plane, (a) bit-planes 7 and 8, (b) bit-planes 6 and 7, (c) bit-planes 5 and 6, (d) bit-planes 4 and 5.

Figure 7. The retrieved results by superimposing different bit-plane, (a) bit-planes 4 to 7, (b) bit-planes 5 to 7, (c) bit-planes 6 to 8, (d) bit-planes 5 to 8.

Figure 8. The retrieved results by superimposing different bit-plane, (a) bit-planes 1 to 5, (b) bit-planes 1 to 6, (c) bit-planes 1 to 7, (d) bit-planes 1 to 8.

IV. Conclusions

Image sharing method can protect the security of the sensitive images. Furthermore, one of the sharing images

cannot reveal any information of the original images. When the enough sharing images are obtained, the original information can be revealed. Traditional visual sharing method has the disadvantages of pixel expansion, meaningless sharing, and bad recovering quality. The paper proposes an image sharing method by using meaningful images to remove the above problems. The experimental results show the feasibility of the proposed method.

ACKNOWLEDGMENT

The author would like to thank the anonymous Referees for their valuable suggestions and many constructive comments that resulted in the improvement and readability of this paper. This research was partially supported 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," *Advance in Cryptology*, no. 950, pp. 1-12, 1994.

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

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

[4] T. H. Chen and K. H. Tsao, "Visual secret sharing by random grids revisited," *Pattern Recognition*, vol. 42, no. 9, pp. 2203-2217, 2009.

[5] 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, July 2011.

[6] R. Z. Wang, Y. C. Lan, Y. K. Lee, S. Y. Huang, S. J. Shyu, and T. L. Chia, "Incrementing visual cryptography using random grids," *Optics Communications*, vol. 283, no. 21, pp. 4242-4249, Dec. 2010.

[7] W. P. Fang, "Friendly progressive visual secret sharing," *Pattern Recognition*, vol. 41, no. 4, pp. 1410-1414, 2008.

[8] D. Jin, W. Q. Yan, and M. S. Kankanhalli, "Progressive color visual cryptography," *Journal of Electronic Imaging*, vol. 14, no. 3, pp. 033019, Aug. 2005.

[9] R. Z. Wang, Y. F. Chien, and Y. Y. Lin, "Scalable user-friendly image sharing," *Journal of Visual Communication and Image Representation*, vol. 21, no. 7, pp. 751-761, Oct. 2010

[10] 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, no. 1, pp. 78-90, Jan. 2011.

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

Hao-Kuan Tso received the PhD degree from Department of Electrical Engineering at Institute of Technology, National Defense University, Taiwan, R.O.C. He is currently an associate professor in the Department of Computer Science and Communication Engineering at Army Academy R.O.C. His research interests include visual cryptography, information hiding, and information security.