

Sharing Secret Image Based on Bit Plane

Hao-Kuan Tso

Department of Electronic Engineering
Army Academy R.O.C.
E-mail: haokuantso@gmail.com

Der-Chyuan Lou

Department of Computer Science and
Information Engineering
Chang Gung University
E-mail: dclouprof@gmail.com

Chia-Long Wu

Department of Aeronotic Communication Elec-
tronics, Air Force Institute of Technology
E-mail: chialongwu@gmail.com

Abstract—Most secret sharing schemes transform the gray-level images into the halftone images so that the original images cannot be recovered completely. In 2005, Lukac and Plataniotis proposed a bit-level based secret sharing scheme to improve the disadvantage. However, the above-mentioned method exists the problem of pixel expansion. The paper proposes an improved secret sharing scheme based on bit plane. Experimental results will show the feasibility of the proposed scheme.

Index Terms—Secret sharing, bit plane, pixel expansion, meaningful sharing.

I. INTRODUCTION

The rapid development of network and computer technologies makes us more convenient to transmit data to worldwide parties, which greatly save much precious time. Furthermore, many merchant also gain great benefits by using information technologies on business. Due to the fact that most people lack for the concept of information security, some problems follow it. Unauthorized parties can intrude network or personal computer easily and intercept the important information. The behaviors have caused largely damages for business or personal benefits.

To protect the security of personal privacy, cryptography technique has been extensively used in many applications of daily life, for example certificate, E-commerce, identity authentication etc. By encrypting the information into disordering codes, unauthorized parties cannot recover the original content so that the important information can be protected. One of cryptography technologies is secret sharing technique, which is firstly proposed by Shamir [1] and Blakley [2] and has been extensively discussed in recent years. By dividing the data into n parts, unauthorized parties cannot recognize the original content of the data from any

$m-1$ ($m \leq n$) or less than m parts. Only if collecting any m or more than m parts, the original data can be revealed.

A secret sharing technique applied to secret image is firstly proposed by Naor and Shamir [3] in 1995. Due to the contrast difference of black and white, a binary image can be divided into several noise-like images by using predefined codebook and then protected among parties. Even though one of the sharing images is intercepted by unauthorized parties, the original image still cannot be revealed. Furthermore, performing a simple superimposing operation among the sharing images can reveal the original image.

A simple (2, 2) secret sharing technique is illustrated as follows. To construct the sharing images, a codebook is designed firstly. Due to the fact that people can recognize the content of an image according to the contrast of black and white, the codebook can be designed that consists of black and white. Hence, the method first generates two basic matrices as follows.

$$S_1 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, S_2 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}.$$

where every pixel will be expanded into a block with the size of 2 by 2. By permuting the pixels of the above block, finally a codebook can be designed as Table 1. The following work is to construct the sharing images. If a pixel of an image is white, two blocks with the size of 2 by 2 can randomly be chosen from the left columns of Table 1. On the contrast, if a pixel of an image is black, two blocks with the size of 2 by 2 can randomly be chosen from the right columns of Table 1. After finishing encoding, a binary image with the size of m by n will be expanded into two sharing images with

the size of $2m$ by $2n$. Furthermore, superimposing two sharing images can reveal the original image. The characteristic of the method is that the superimposed image can be recognized by human eyes directly. However, the constructed sharing images exist the problem of pixel expansion.

In recent years, many secret sharing methods based on Naor and Shamir's concept have been proposed [4-8]. However, most secret sharing methods have the disadvantage of pixel expansion, which will cause enlarged sharing images and distorted reconstructed image. In 2004, Hou and Tu [6] proposed a secret sharing technique by encrypting m successively pixels to remove the problem of pixel expansion. Due to the halftoning is a technique that transforms a continuous-tone image into a binary image and can generate the similar effect as the gray-level images, hence a halftone image by using the density of the net dots to simulate a gray-level image is introduced into their method. In the encoding phase, a halftone secret image is firstly divided into non-overlapping sections, in which every section consists of two pixels. Then two pixels of every section are encoded successively according to two basic matrices. When all sections are processed, two non-expanded sharing images will be constructed. Furthermore, superimposing two sharing images can reveal the secret image. Experimental results show that the proposed method totally removes the disadvantage of pixel expansion. However, the constructed sharing images are meaningless.

Most methods transform a gray-level image into a halftone one, which will limit the applicability of secret sharing technique [7]. In 2005, Lukac and Plataniotis [7] proposed a new secret sharing method based on bit-level decomposition. The concept of the method is to decompose an image with B -bit into B bit planes, in which every plane can be viewed as a binary image. By superimposing B encrypted bit planes, several B -bit sharing images are constructed. To recover the original image, the similar decomposition process is utilized to decompose B -bit sharing images first. After that, by performing the decrypting algorithm, the original image can be revealed without any loss of information. However, the problem of pixel expansion is still existed.

To improve the disadvantage of Lukac and Plataniotis method, an improved secret sharing method based on bit plane is proposed in the paper. The concept of multi-point encoding and the meaningful sharing will be introduced into the proposed method. Experimental results confirm that the proposed method can meet the above-mentioned requirements.

The rest of the paper is organized as follows. A brief review of Lukac and Plataniotis method is introduced in Section 2. The secret sharing method based on bit plane is proposed in Section 3. Experimental results are shown in Section 4. Conclusions are given in Section 5.

II. RELATED WORK

Due to the characteristic of conventional secret sharing method, most methods introduce a halftone image into their method. However, the recovered image has the bad quality of reconstruction. Hence, Lukac and Plataniotis proposed a new secret sharing method based on bit-level decomposition. The detail of the method is illustrated as follows.

A. Secret sharing phase:

1. Decompose a gray-level image with the size of k by k into 8 bit planes.
2. Encrypt each bit plane into the sharing images with the size of $2k$ by $2k$ by using conventional sharing method as Table 1.
3. Construct the 8-bit sharing images with the size of $2k$ by $2k$ by bit-level superimposing.

B. The reconstructed phase:

1. Decompose the 8-bit sharing images with the size of $2k$ by $2k$ into 8 bit planes.
2. Obtain the original pixels of bit planes by the following rule:

$$\text{If } s_{1(2i-1,2j-1)}^b = s_{2(2i-1,2j-1)}^b \quad \text{Then}$$

$$o_{(i,j)}^b = 1$$

Else

$$o_{(i,j)}^b = 0$$

End If

where s_1^b denotes the b th bit plane of the sharing image s_1 . o^b denotes the pixel of the b th bit plane.

3. Reveal the original image by bit-level superimposing.

The advantage of the method is that the recovered image satisfies the perfect reconstruction. However, meaningless and enlarged sharing images are two unsolved problems.

III. THE PROPOSED METHOD

The method is divided into two phase. One is the sharing phase, the other is the reconstruction phase.

A. The sharing phase

Input: a gray-level image with the size of m by n and a halftone image with the size of m by n

Output: two meaningful gray-level sharing images with the size of m by n

1. Scramble the gray-level image by using a scrambled function.
2. Decompose the scrambled version of the gray-level image into 8 bit planes.
3. Divide each bit plane and the halftone image into non-overlapping sequence.
4. Encode the results of Step 3 into the sharing images with m by n size by using the designed sharing method as Table 2.
5. Construct the 8-bit sharing images with the size of m by n size by the following equation.

$$S_1 = s_1^8 \cdot 2^7 + s_1^7 \cdot 2^6 + s_1^6 \cdot 2^5 + s_1^5 \cdot 2^4 + s_1^4 \cdot 2^3 + s_1^3 \cdot 2^2 + s_1^2 \cdot 2^1 + s_1^1 \cdot 2^0 \quad (1)$$

$$S_2 = s_2^8 \cdot 2^7 + s_2^7 \cdot 2^6 + s_2^6 \cdot 2^5 + s_2^5 \cdot 2^4 + s_2^4 \cdot 2^3 + s_2^3 \cdot 2^2 + s_2^2 \cdot 2^1 + s_2^1 \cdot 2^0 \quad (2)$$

where $s_1^1 \dots s_1^8$ and $s_2^1 \dots s_2^8$ denote the bit planes of the sharing images S_1 and S_2 respectively.

B. The construction phase

Input: two meaningful gray-level sharing images with the size of m by n

Output: The original gray-level image with the size of m by n

1. Decompose the two sharing images into 8 bit planes.

2. Perform the Exclusive-OR (XOR) operation between the same bit planes of the two sharing images. For example, the operation between the first bit planes of the two sharing images can be represented as follows.

$$S^1 = s_1^1 \oplus s_2^1. \quad (3)$$

3. Reveal a scrambled version of the gray-level image with the size of m by n by using bit-plane superimposing operation as Eq. (1).

4. Unscramble the result of Step 3 and obtain the original image.

IV. THE EXPERIMENTAL RESULTS

In this experiment, the gray-level image “Lena” with the size of 256 by 256 and the halftone image “Barb” with the size of 256 by 256 are used as the input images (shown in Fig. 1(a) and Fig. 1(b)). According to the proposed algorithm, the gray-level image “Lena” is firstly scrambled by using a scrambled function. The scrambled version of the image is shown as Fig. 1(c). Then the scrambled version is decomposed into 8 bit planes and encoded with the halftone image into two sharing images with the size of 256 by 256 (shown as Fig. 1(d) and Fig. 1(e)). As you see, the two sharing images are meaningful and non-expanded images. Furthermore, from one of the sharing images, it is very difficult to reveal the information of the original image.

In the reconstruction phase, the similar process as the sharing phase can be implemented to reveal the original gray-level image. First the two sharing images are decomposed into 8 bit planes respectively. Then the XOR operation is performed between the bit planes of the sharing images. Finally by bit-plane superimposing operation, the original gray-level image can be revealed without any loss of information (shown in Fig. 1(f)).

Fig. 2 show the another experimental results. the gray-level image “Bridge” with the size of 256 by 256 and the halftone image “Camera” with the size of 256 by 256 are used as the input images (shown in Fig. 2(a) and Fig. 2(b)). The scrambled version

of the image “Bridge” is shown as Fig. 2(c). Fig 2(d) and Fig. 2(e) show the meaningful sharing images. The recovered image is shown in Fig. 2(f). The above experimental results show the effectiveness of the proposed method.

V. CONCLUSIONS

In the paper, a secret sharing method based on bit plane is proposed. To improve the disadvantage of Lukac and Plataniotis method, the concept of multi-point encoding and meaningful sharing is introduced into the proposed method. Experimental results show that the proposed method has the following advantages: (1) the sharing images are non-expanded and meaningful images, (2) the reconstructed image is lossless.

ACKNOWLEDGE

This research was partially supported by National Science Council of the Republic of China under grants NSC 98-2221-E-539-002-. The authors also thank the anonymous reviewers for their valuable opinions.

REFERENCE

- [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,” *AFIPS conference proceedings*, vol. 48, pp. 313-317, 1979.
- [3] N. Naor and A. Shamir, “Visual cryptography,” *Advances in Cryptology: Eurocrypt’94*, LNCS, vol. 950, pp. 1-12, 1995.
- [4] W. P. Fang, “Friendly progressive visual secret sharing,” *Pattern Recognition*, vol. 41, no. 4, pp. 1410-1414, April 2008.
- [5] J.-B. Feng, H.-C. Wu, C.-S. Tsai, Y.-F. Chang, and Y.-P. Chu, “Visual secret sharing for mul-

tiple secrets,” *Pattern Recognition*, vol. 41, pp. 3572-3581, 2008.

- [6] Y. C. Hou and S. F. Tu, “Visual cryptography techniques for color images without pixel expansion”, *Journal of Information, Technology and Society*, vol. 1, pp. 95-110, 2004.
- [7] R. Lukac and K. N. Plataniotis, “Bit-level based secret sharing for image encryption,” *Pattern Recognition*, vol. 38, no. 5, pp. 767-772, May 2005.
- [8] J.-C. Hou, “Visual cryptography for color images,” *Pattern Recognition*, vol. 36, no. 7, pp. 1619-1629, 2003.

Table 1 The codebook of the (2, 2) secret sharing method.














































































Pixel								
Share1								
Share2								
Stacking results								

Table 2 The codebook of the proposed method.

The pixels of bit plane of the gray-level image	The pixels of the halftone image	Sharing image 1	Sharing image 2	The results of the XOR operation
				
				
				
				
				
				
				
				
				
				
				
				

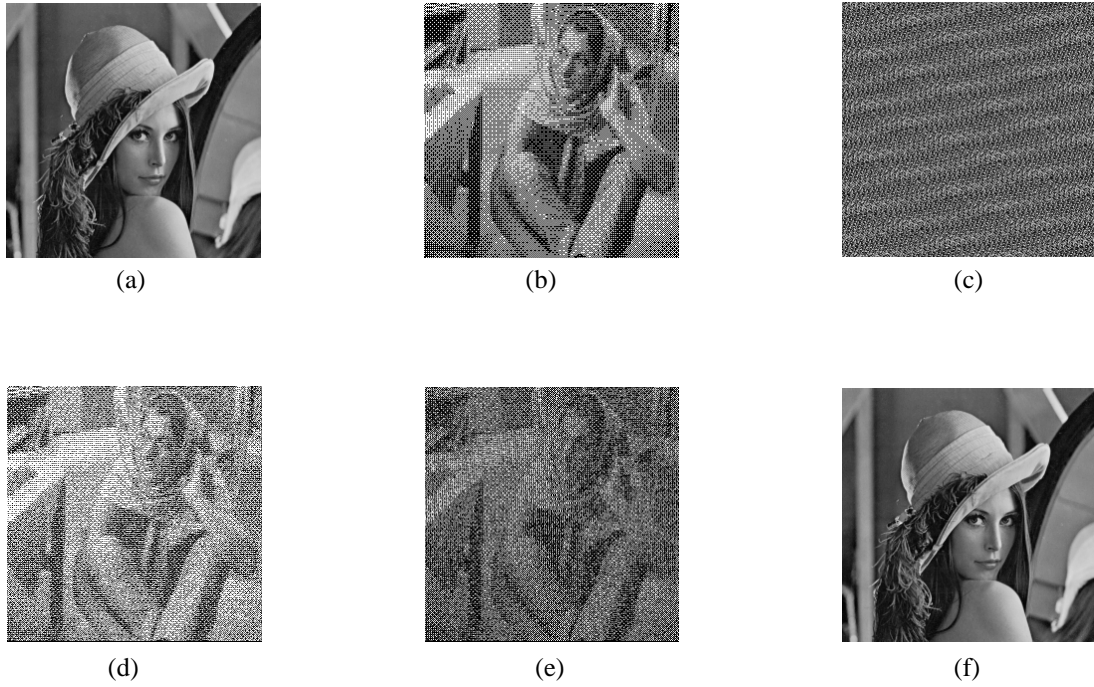


Fig. 1 The experimental results: (a) the gray-level image “Lena”, (b) the scrambled version of the gray-level image, (c) the halftone image “Barb”, (d) and (e) the sharing images, (f) the reconstructed image.

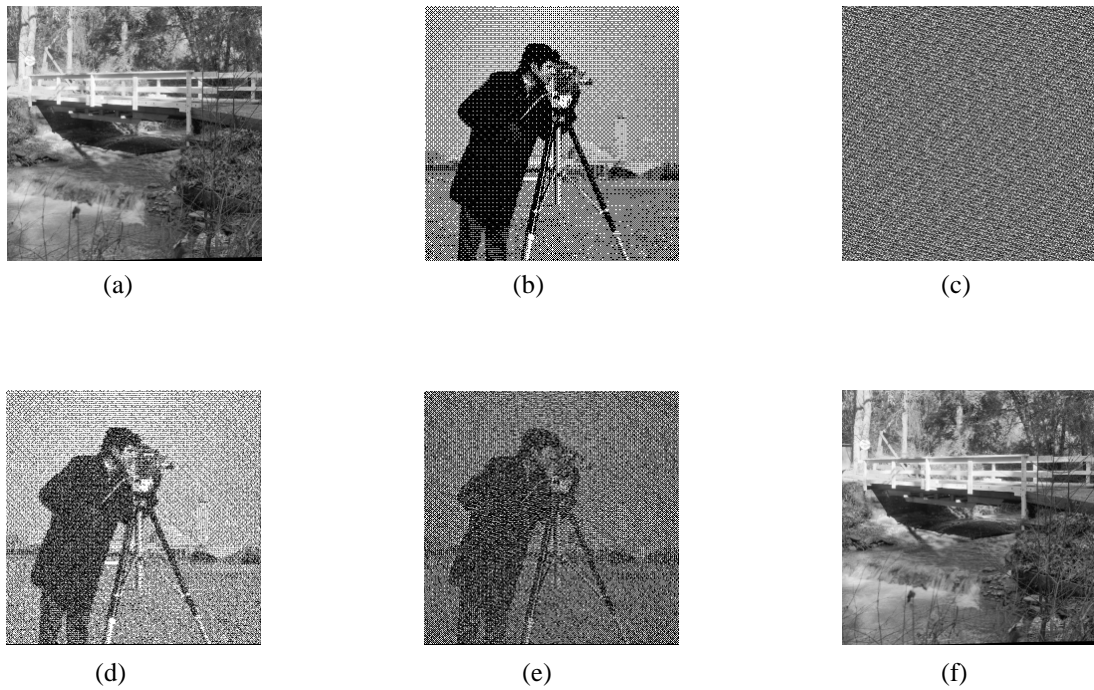


Fig. 2 The experimental results: (a) the gray-level image “Bridge”, (b) the scrambled version of the gray-level image, (c) the halftone image “Camera”, (d) and (e) the sharing images, (f) the reconstructed image.