A Meaningful Scheme for Sharing Secret Images Using Mosaic Images

Shengyun Zhai[1], Fan Li[1], Chin-Chen Chang[2,3] and Qian Mao[1]
(Corresponding author: Chin-Chen Chang)
School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology[1]
516, Jungong Road, Yangpu, Shanghai 200093, P. R. China
Department of Computer Science and Information Engineering, Asia University[2]
500, Lioufeng Road, Wufeng, Taichung 41354, Taiwan
Department of Information Engineering and Computer Science, Feng Chia University[3]
100, Wenhwa Road, Seatwen, Taichung, 40724, Taiwan
(Email: alan3c@gmail.com)
(Received Dec. 2, 2014; revised and accepted Feb. 8 & Mar. 7, 2015)

Abstract

Secret image sharing (SIS) technique protects an image by sharing it among many users. Most existing SIS schemes produce meaningless shadow images, which tends to cause attackers' suspicion. In this paper, a meaningful secret image sharing scheme is proposed that, for the first time, uses mosaic images as the shadow images. The secret image is divided into several parts, and each part is transformed into a mosaic image according to a host image. The indices of the secret tiles of the mosaic image are permuted according to the secret key, and they are hidden in the mosaic images to provide security for the SIS scheme. The experimental results showed that the proposed SIS scheme can reconstruct the original secret image and provide high security.

Keywords: Indices hiding, mosaic image, random numbers, secret image sharing

1 Introduction

Secret image sharing (SIS) is a technique that ensures the security of a secret image by sharing it with several users. The secret image can be reconstructed only when a certain number of users cooperate together. The principle of secret sharing, which is based on the (r, n) threshold, was proposed by Shamir [13] and Blakley [1] independently in 1979. The secret is divided into n shadow images $W_i(i = 1, 2, ..., n)$, and any r or more than r shadow images can reconstruct the secret image cooperatively; none of the secret information can be obtained unless at least r shadow images cooperate together. Many secret image sharing (SIS) methods have been proposed based on this principle. Lee and Chiu [5] obtained $n - 1$ meaningful natural shadow images and one noise-like shadow image after sharing the secret image into $n - 1$ natural images. Then, the noise-like shadow image was hidden through steganography and quick-response code (QR code) techniques, which can reduce the risk of transmission. Using steganographic method, Lin and Chan [6] obtained the lossless secret image and the original host image from the shadow images. A $(2, n)$ matrix-based SIS scheme was proposed by Rey [12]. However, Elsheh *et al.* [4] pointed out that the threshold property of Rey's scheme was compromised, which means that the secret information could be reconstructed from only one shadow. To solve this problem, Yang *et al.* [20] presented a new method using random binary matrices. On the basis of pixel division and XOR operation, Bhattacharjee *et al.* [2] proposed a $(2, n)$ secret image sharing scheme to reconstruct the secret image correctly. In order to improve the security of the secret image and the quality of the reconstructed secret image, Chen [3] proposed a new sharing scheme using linear equations of Hill cipher and random grid. Wang *et al.* [17] proposed a creative scheme, which can share more than one secret images, using matrix transformation. Latif *et al.* [7] utilized random grids, error diffusion, and chaotic encryption to propose a new sharing scheme that can generate meaningful shadow images. Lin and Wang [8] presented a (t, n) scalable secret image sharing method, in which the size of the shadow image is $(2n - t)/n^2$ times that of the original secret image. Based on block truncation coding (BTC), discrete wavelet transform (DWT) and vector quantization (VQ), Le *et al.* [9] proposed an SIS scheme that also can generate small shadow images. However, the shadow images of [8] and [9] are noise-like images, which can increase the risk associated with the transmission of the shadow images.

Recently, many algorithms associated with hiding images have been proposed. According to vector quanti-

zation, Shie *et al*. [14] proposed a visually-imperceptible image hiding scheme. Through this method, multiple secret images can be hidden into the cover image. Based on phase-truncation and phase retrieval in the fractional Fourier domain, a method of hiding the color image into the host image was proposed by Wang *et al*. [18]. A data hiding algorithm was proposed in [19] that uses block patterns to hide a large amount of data into a binary image without attracting the attention of a hacker. Based on LSB substitution and pixel difference, Tsai *et al*. [15] proposed a new scheme to realize information hiding.

In [10], a scheme for hiding secret images was proposed, in which the meaningful cover image can be obtained by assembling the tiny fragments of the secret image. Lee and Tsai [11] used pixel color transformation to improve the quality of the mosaic image provided by the scheme proposed in [10]. Based on color, a scheme of reassembling the fragments of the image rapidly and efficiently was proposed by Tsamoura [16]. In [21], it was shown that potential matching can be generated according to the geometry and color of the fragments. However, if the two aspects of the fragments are similar, this scheme cannot achieve an accurate match.

In the previous research, the generated shadow images are not ideal for most of them are noise-like images, which may arouse the attention of hackers. In this paper, a new SIS scheme is proposed that improves the security and visualization of the shadow images by combining the benefits of traditional secret image sharing and the image mosaicing technique. The contributions of the proposed scheme are that:

1) For the first time, it uses the image mosaicing technique to share the secret image, achieving high-quality shadow images.

2) The sequence of the indices is encrypted by seed key K, which improves the security of the scheme.

3) The shadow images are meaningful, so they do not attract the hacker's attention.

The rest of this paper is organized as follows. The proposed scheme is introduced in Section 2. The experimental results and analyzes are presented in Section 3. The conclusions are discussed in Section 4.

2 Proposed SIS Scheme Based on Image Mosaicing

The proposed SIS scheme is comprised of three phases, i.e., secret image sharing, tile-indexes sharing, and secret image restoration.

2.1 Secret Image Sharing

The size of the secret image is $m_S \times n_S$. First, the secret image is divided into n blocks, each of which has the size of $\frac{m_S}{n} \times n_S$. Here, the parameter n is chosen so that m_S is divisible by it. Then, each block is divided into many adjacent tiles. All of the tiles have the same shape and the same size, i.e., $a \times b$. a, b and n are fixed, which are known to both sender and receiver. Figure 1 shows the process for generating the tiles.

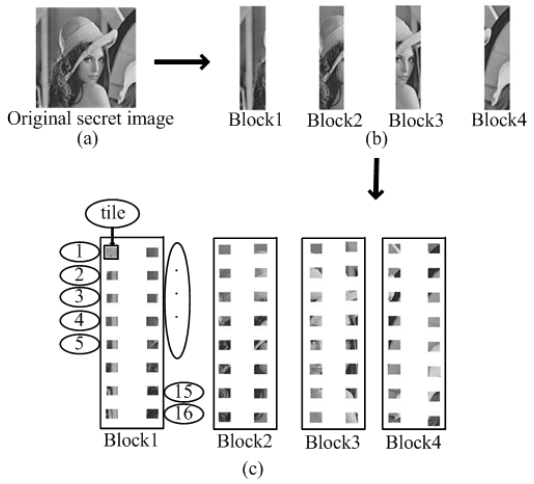

Figure 1: Tiles generation

Following that, the n host images with sizes of $m_H \times n_H$ are chosen, in which $m_H = k_1 m_S$ and $n_H = k_2 n_S (k_1, k_2 = 1, 2, ..., l)$($l$ is an integer). In the phase in which the shadow images are generated, the ith secret block will be hidden in the ith host image, where $i = 1, 2, ..., n$. Each host image is divided into adjacent tiles with the same shape and size, i.e., $a \times b$. The number of tiles, L_H, in each host image is:

$$L_H = \frac{m_H \times n_H}{a \times b}. \tag{1}$$

Similarly, the number of tiles in the secret image block is $L_S = \frac{m_S \times n_S}{n \times a \times b}$. For the ith tile ($i = 1, 2, ..., L_S or L_H$)($L_H \geqslant L_S$) of either the secret image block or the host image, the feature value is computed by the following function:

$$f_i = p \times m_i + q \times d_i, \tag{2}$$

$$s_{ij} = |f_i^S - f_j^H|, \tag{3}$$

where m_i is the average of the pixels' gray values in the ith tile, d_i is the standard deviation, $i \in \{1, 2, 3, ..., L_S\}$, $j \in \{1, 2, 3, ..., L_H\}$. The symbols p and q are the weighting factor of m_i and d_i, respectively. The mosaic image changes as the weighting factor changes. In the experiment, p equals to 0.99 and q equals to 0.01, which are the empirical values. In this case, the quality of the mosaic image was acceptable. For the ith tile in a secret image block and in a host image, the feature value f_i can be obtained by Equation (2). The secret tile's feature value f_i was called f_i^S and the host tile's feature value f_i was called f_i^H.

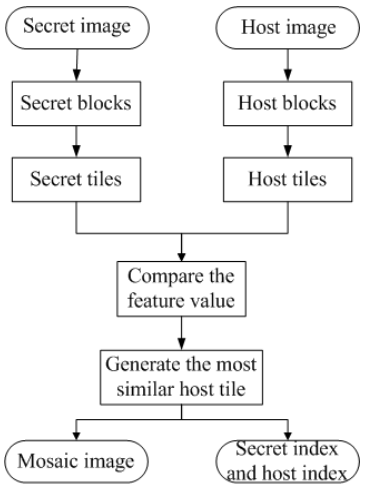

Figure 2: Process of the secret image sharing

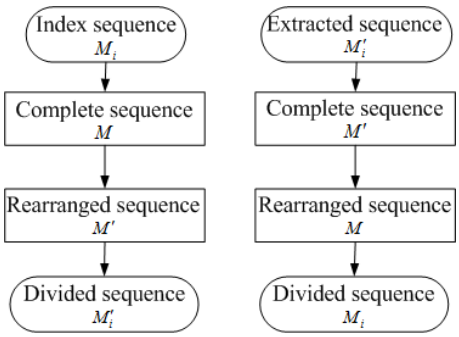

Figure 3: Process of indices sequence

Conducting the operation as shown in Equation (2) for the entire secret image and the entire host image, the feature sequences, $F^S = f_1^S, f_2^S, ..., f_{L_S}^S$ and $F^H = f_1^H, f_2^H, ..., f_{L_H}^H$, can be obtained. The order of scanning the secret tile increases monotonically. Then, according to the Equation (3), the similarity value between the secret tile and the host tile can be obtained. The first secret block and the first host image are considered for the image mosaicing. The first feature value of secret tile f_1^S and all of the whole feature values of the host tiles are scanned. And the similarity value, s_{1j}, between the feature of the first secret tile and the feature of the jth host tile, is obtained, where $j = 1, 2, ..., L_H$. The smaller s_{ij} is, the more similar between the ith secret tile and the jth host tile will be. So, the smallest similarity value, s_{1,j_1}, is chosen among the L_H similarity values. That is to say, the host tile H_{j_1} is the tile that is the most similar to the first secret tile. After that, for the second feature value of the secret tile f_2^S, all of the host feature values, except for $f_{j_1}^H$, are scanned. The similarity values between f_2^S and each of the rest of the feature values of the host tile are created and referred to as called s_{2j}. The smallest value s_{2,j_2}, among the $L_H - 1$ similarity values indicates that the host tile, H_{j_2}, is the most similar to the second secret tile. Similarly, for the ith secret feature value and the remaining $L_H - i + 1$ host tiles, the $L_H - i + 1$ similarity values are created and the smallest one is obtained. Thus, the host tile, H_{j_i}, which is the most similar to the ith secret tile is identified.

After that, for all of the tiles $S_1, S_2, ..., S_i, ...$, in the first secret block, the most similar tiles $H_{j_1}, H_{j_2}, ..., H_{j_i}, ...$, in the first host image are chosen. Thus, the indices sequence M, including $M_S = 1, 2, ...$(the order of secret tiles in one block) and $M_H = j_1, j_2, ...$(the order of the chosen host tiles), is constructed. Moving the secret tiles $S_1, S_2, ...$to the corresponding position of the host tiles $H_{j_1}, H_{j_2}, ...$, respectively, the preliminary shadow image is obtained, i.e., the mosaic image. The vector M_H is restored as the indices to be used in reconstructing the secret. The same operation is conducted for all of the secret blocks and host images. Figure 2 shows the flowchart that is used to generate shadow images.

2.2 Index Sharing

After generating the shadow images, n indices sequences $M_i (i = 1, 2, ..., n)$ are obtained. Based on the order of the secret blocks, the indices sequences M_i are connected to form a complete indices map, called M, $M = M_1||M_2||...||M_n$. Now, indices sequence M is encrypted by seed key K and a permutated sequence, M_r, is obtained. The key K is fixed, which is known to both sender and receiver. Divide M_r into n segments and transform them into a binary string. Using the least significant bit (LSB) method, the binary string of the ith segment is hidden into the ith mosaic image. Therefore, the shadow images are obtained. Figure 3 shows the flowchart that is used to generate indices sequence.

2.3 Secret Image Restoration

When reconstructing the secret image, first, the binary indices sequence is extracted from the shadow images and transformed into decimal numbers, $M_i^{'}$. In the order of the host images, the components of the sequence $M_i^{'}$ are connected with each other to construct the complete indices sequence $M^{'} = M_1^{'}||M_2^{'}||...||M_n^{'}$. The original order of the indices sequence $M^{'}$ has been rearranged by the seed key K, then the sequence M is divided into n segments, called $M_i (i = 1, 2, ..., n)$. An empty image is defined, which size is identical to the size of the original secret image. The empty image and the shadow images are divided, respectively, as the division of original secret image and host image. The tiles of the shadow images are moved to the corresponding positions of tiles of the empty image according to indices sequence M_i. Thus, the original secret image is reconstructed.

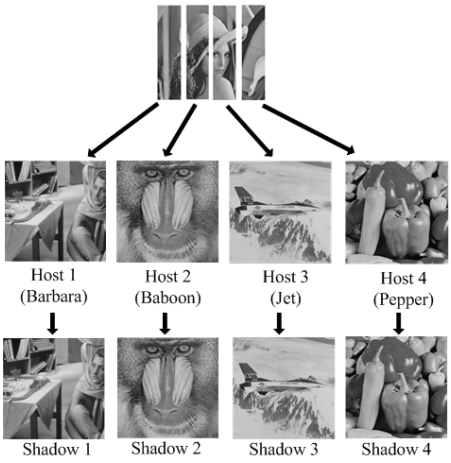

Figure 4: Secret image sharing

Figure 5: Secret images

Table 1: PSNR between host images and shadow images

Images (384×384)	PSNR of shadow images (dB)
Barbara	39.52
Baboon	37.26
Jet	37.41
Pepper	39.64

3 Experimental Results and Analyzes

3.1 Experimental Results

An example of sharing a secret image by this scheme is shown in Figure 1 and Figure 4. In Figure 1, the original secret image is divided into four blocks, and each block is divided into many tiles. The *ith* block is hidden into the *ith* host image as shown in Figure 4, where $i = 1, 2, 3, 4$. In the following, the secret image, Lena, as shown in Figure 1, is hidden in four host images, as shown in Figure 4. For the sake of convenience, the size of the secret image is 128×128. The secret image is divided into four blocks. The size of each host image is 384×384. The secret blocks and host images are divided into 2×2 tiles. The experimental results are shown in Figure 4 and Table 1. The reconstructed secret image is shown in Figure 5. The experimental results indicated that the shadow images were meaningful and that their quality was acceptable, which proved the usefulness of the proposed visualization scheme in the field of secret image sharing.

3.2 Performance Analyzes

The relationship between the quality of the shadow image and the size of the host image was analyzed first. The sizes of the host images were varied from 128×128 to 256×256 and to 384×384. The size of the secret image was 128×128, and the size of tile was 2×2. It is obvious that the quality of the shadow image improved as the size of the host image increased, as shown in Figures 6 and 7.

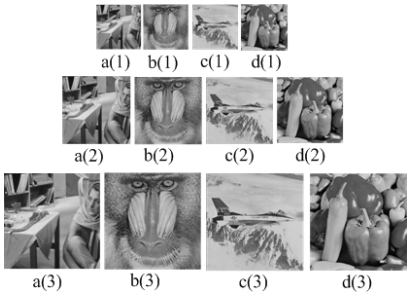

Figure 6: Different sizes of shadow images: a(1)∼d(1): 128×128, a(2)∼d(2): 256×256, a(3)∼ d(3): 384×384.

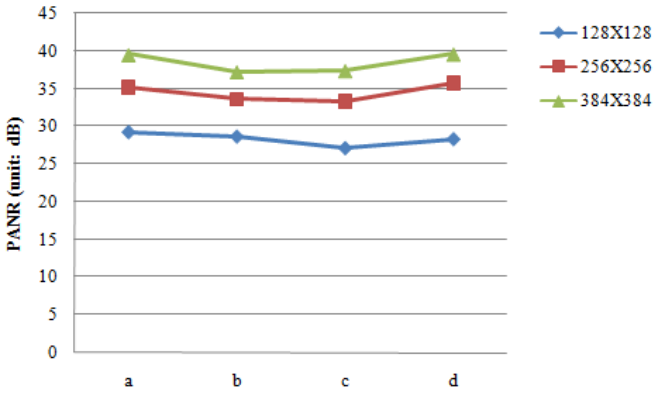

Figure 7: PSNR between host images and shadow images with different sizes

The general images are chose as the secret images and host images, as shown in Figure 8. In the experiments, PSNR between general host images and shadow images with different size are shown in Figure 9. For the same size secret image, the larger the size of the host image is, the better the quality of the shadow image will be. This is because a larger host image provides more choices for identifying the similarity value for each tile of the secret image. PSNR between mosaic images and host images with different sizes of tiles are shown in Table 2, while PSNR between shadow images and host images with different sizes of tiles are shown in Table 3. It can be seen

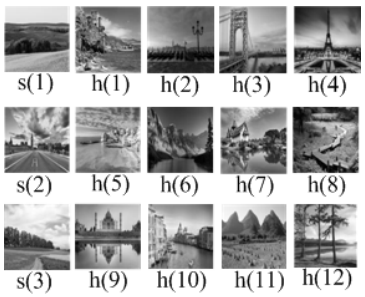

Figure 8: s(3)∼s(3) the three secret images, h(1)∼h(4) the host images to s(1), h(5)∼h(8) the host images to s(2), h(9)∼h(12) the host images to s(3)

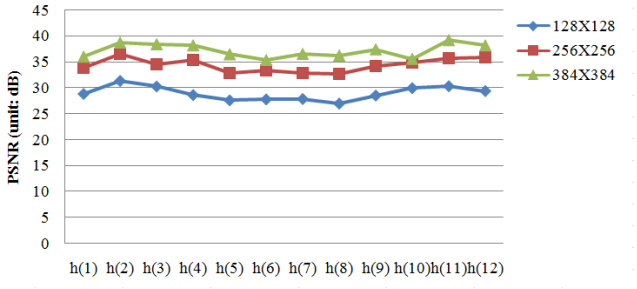

Figure 9: PSNR between general host images and shadow images with different sizes

from Table 2, the PSNR values decrease as the sizes of tiles increase, that is to say, the size of tile have an important impact on the image quality. By the comparison between Table 2 and Table 3, for the same size of tiles, the PSNR values decrease slightly, i.e., the impact of the data hiding to the image quality is tiny. The PSNR values between secret images and restored secret images are shown in Figure 10, which illustrates that the PSNR values increase as the sizes of tiles increase. Meanwhile, the quality of restored secret image is also acceptable when the size of tile is the smallest, i.e., 2×2. In practice applications, users can adapt the sizes of tiles to obtain suitable shadows according to the requirement. It can be seen from the Table 4 that the computational time is increased when the size of tile is decreased. Especially when the size of tile is 2×2, the computational time is increased sharply.

The experimental results of this method and other three methods are shown in Table 5. The shadow images created by Lin and Wang's scheme [8] and Bhattacharjee *et al.*'s method [2] are meaningless, so they likely to attract the attention of hackers. The algorithm proposed by Latif *et al.* [7] can produce meaningful shadow images by encoding the secret image into natural host images. However, this encryption technology changes the pixels of original image, so the shadow images can be identified during transmission. In this study, the shadow images are meaningful and the pixels of the original image are

Table 2: PSNR between mosaic images and host images with different sizes of tiles (unit: dB)

Mosaic images	Size			
	2×2	4×4	8×8	16×16
h(1)	36.04	30.87	27.79	25.90
h(2)	38.77	36.14	31.88	28.82
h(3)	38.46	33.14	30.90	28.75
h(4)	38.24	33.74	29.88	30.00
h(5)	36.52	32.10	29.73	27.73
h(6)	35.40	30.60	28.89	27.66
h(7)	36.58	32.39	29.60	28.24
h(8)	36.28	31.63	28.87	25.89
h(9)	37.48	32.70	30.22	29.71
h(10)	35.61	29.78	28.23	28.67
h(11)	39.27	34.43	31.68	29.54
h(12)	38.23	34.95	31.84	31.23

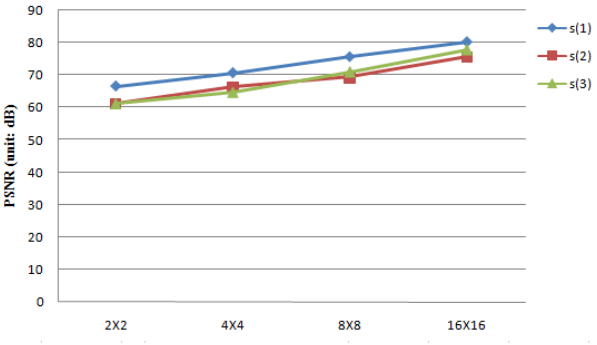

Figure 10: PSNR between general secret images and restored secret images with different sizes of tiles

Table 3: PSNR between shadow images and host images with different sizes of tiles (unit: dB)

Shadow images	Size			
	2×2	4×4	8×8	16×16
h(1)	36.03	30.87	27.80	25.91
h(2)	38.74	36.13	31.88	28.82
h(3)	38.43	33.14	30.90	28.75
h(4)	38.21	33.74	29.88	30.00
h(5)	36.50	32.10	29.73	27.73
h(6)	35.39	30.60	28.89	27.66
h(7)	36.56	32.38	29.60	28.24
h(8)	36.27	31.63	28.87	25.89
h(9)	37.46	32.70	30.22	29.71
h(10)	35.60	29.78	28.22	28.67
h(11)	39.24	34.43	31.68	29.54
h(12)	38.20	34.95	31.83	31.23

Table 4: Computational time of the general secret image sharing (unit:second)

Secret images	Size			
	2×2	4×4	8×8	16×16
s(1)	66.6	8.4	4.0	3.3
s(2)	63.0	8.4	3.9	3.4
s(3)	55.3	8.2	4.0	3.4

Table 5: The thresholds and shadow images descriptions

Schemes	(t,n)	Description
Bhattacharjee *et al.*'s scheme [2]	$t = 2$	Meaningless shadow images
Latif *et al.*'s scheme [7]	$t < n$	Meaningful shadow images
Lin and Wang's scheme [8]	$t < n$	Meaningless shadow images
Proposed scheme	$t = n$	Meaningful shadow images

unchanged. In addition, this scheme can be used to share other forms of secret images, such as color images, texture images.

4 Future Work

In this paper, the reconstructed secret image is lossy because the irreversible hiding method was used in the embedding of the indices sequence. In the future, the research work is directed to developing a reversible hiding method to hide the indices sequence and reconstruct the lossless secret image. In addition, a more accurate method of calculating the similarity of the tiles is necessary, which can improve the quality and security of the shadow images.

5 Conclusions

A new kind of sharing scheme, called meaningful secret image sharing with a mosaic image, was proposed in this work. In the scheme, it is the first time that the mosaic technique has been used in sharing secret images, and a good quality of the shadow images is achieved. And also, the generated shadow images are meaningful. Furthermore, a seed key K is used to generate the rearranged order, which is the order of the indices, to ensure the security of the algorithm. The comparisons between the proposed scheme and other existing secret image sharing techniques demonstrate a good performance of the proposed algorithm.

References

[1] G. R. Blakley, "Safeguarding cryptographic keys," *AFIPS Conference Proceedings*, vol. 48, pp. 313–317, 1979.

[2] T. Bhattacharjee, J. P. Singh and A. Nag, "A novel $(2, n)$ secret image sharing scheme," *Procedia Technology*, vol. 4, pp. 619–623, 2012.

[3] W. K. Chen, "Image sharing method for gray-level images," *Journal of Systems and Software*, vol. 86, no. 2, pp. 581–585, 2013.

[4] E. Elsheh and A. B. Hamza, "Comments on matrix-based secret sharing scheme for images," in *Progress in Pattern Recognition, Image Analysis and Applications*, LNCS 6419, pp. 169–175, 2010.

[5] K. H. Lee and P. L. Chiu, "Digital image sharing by diverse image media," *IEEE Transactions on Information Forensics and Security*, vol. 9, no, 1, pp. 88–98, 2014.

[6] P. Y. Lin and C. S. Chan, "Invertible secret image sharing with steganography," *Pattern Recognition Letters*, vol. 31, no. 13, pp. 1887–1893, 2010.

[7] A. A. E. Latif, X. H. Yan, L. Li, N. Wang, J. L. Peng and X. M. Niu, "A new meaningful secret sharing scheme based on random grids, error diffusion and chaotic encryption," *Optics and Laser Technology*, vol. 54, pp. 389–400, 2013.

[8] Y. Y. Lin and R. Z. Wang, "Scalable secret image sharing with smaller shadow images," *IEEE Signal Processing Letters*, vol. 17, no. 3, pp. 316–319, 2010.

[9] T. H. N. Le, C. C. Lin, C. C. Chang and H.B. Le, "A high quality and small shadow size visual secret sharing scheme based on hybrid strategy for grayscale images," *Digital Signal Processing*, vol. 21, no. 6, pp. 734–745, 2011.

[10] I. J. Lai and W. H. Tsai, "Secret-fragment-visible mosaic image-a new computer art and its application to information hiding," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 936–945, 2011.

[11] Y. L. Lee and W. H. Tsai, "A new secret image transmission technique via secret-fragment-visible mosaic images by nearly reversible color transformations," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 24, no. 4, pp. 695–703, 2014.

[12] A. M. Rey, "A matrix-based secret sharing scheme for images," in *Progress in Pattern Recognition, Image Analysis and Applications*, LNCS 5197, pp. 635–642, 2008.

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

[14] S. C. Shie, S. D. Lin and J. H. Jiang, "Visually imperceptible image hiding scheme based on vector quantization," *Information Processing and Management*, vol. 46, no. 5, pp. 495–501, 2010.

[15] Y. Y. Tsai, J. T. Chen and C. S. Chan, "Exploring LSB substitution and pixel-value differencing for block-based adaptive data hiding," *International*

Journal of Network Security, vol. 16, no. 5, pp. 363–368, 2014.

[16] E. Tsamoura and I. Pitas, "Automatic color based reassembly of fragmented images and paintings," *IEEE Transactions on Image Processing*, vol. 19, no. 3, pp. 680–690, 2010.

[17] Z. H. Wang, H. B. Jin, X. B. Wang and C. C. Chang, "An adaptable (n, n) secret image sharing mechanism based on boonlean operation," *International Journal of Network Security*, vol. 16, no. 6, pp. 487–493, 2014.

[18] Q. Wang, Q. Guo and J.Y. Zhou, "Color image hiding based on phase-truncation and phase retrieval technique in the fractional Fourier domain," *Optik-International Journal for Light and Electrics Optics*, vol. 124, no. 12, pp. 1224–1229, 2013.

[19] C. C. Wang, Y. F. Chang, C. C. Chang, J. K. Jan and C. C. Lin, "A high capacity data hiding scheme for binary images based on block patterns," *Journal of Systems and Software*, vol. 93, pp. 152–162, 2014.

[20] C. N. Yang, C. C. Wu, Y. C. Lin and C. Kim, "Enhanced matrix-based secret image sharing scheme," *IEEE Signal Processing Letters*, vol. 19, no. 12, pp. 789–792, 2012.

[21] K. Zhang and X. Li, "A graph-based optimization algorithm for fragmented image reassembly," *Graphical Models*, vol. 76, no. 5, pp. 484–495, 2014.

Shengyun Zhai was born in Henan Province, China, in 1990. She received the B.S. degree in Mechanical and Automotive Engineering from Nanyang Institute of Technology, Henan, China, in 2013. She is currently working toward the M.S. degree in Instrumentation Engineering from University of Shanghai for Science and Technology, Shanghai, China. Her research interests include information sharing and image processing.

Fan Li was born in Shandong Province, China, in 1990. She received the B.S. degree in Electronic and Information Engineering from Shandong Institute of Business and Technology, Shandong, China, in 2012. She is currently working toward the M.S. degree in Signal and Information Processing from University of Shanghai for Science and Technology, Shanghai, China. Her research interests include information hiding and image processing.

Chin-Chen Chang received the B.S. degrees in Science in Applied Mathematics and M.S. degree in Science in computer and decision sciences. Both were awarded in National Tsing Hua University, Taiwan. He received his Ph.D. degree in computer engineering from National Chiao Tung University, Taiwan.

His current title is Chair Professor in Department of Information Engineering and Computer Science, Feng Chia University, from Feb. 2005. He is currently a Fellow of IEEE and a Fellow of IEE, UK. His current research interests include database design, computer cryptography, image compression and data structures.

Since his early years of career development, he consecutively won Outstanding Talent in Information Sciences of the R. O. C., AceR Dragon Award of the Ten Most Outstanding Talents, Outstanding Scholar Award of the R. O. C., Outstanding Engineering Professor Award of the R. O. C., Distinguished Research Awards of National Science Council of the R. O. C., Top Fifteen Scholars in Systems and Software Engineering of the Journal of Systems and Software, and so on. On numerous occasions, he was invited to serve as Visiting Professor, Chair Professor, Honorary Professor, Honorary Director, Honorary Chairman, Distinguished Alumnus, Distinguished Researcher, Research Fellow by universities and research institutes.

Qian Mao was born in Shanxi Province, China, in 1978. She received the B.S. degree in Mechanical Engineering and Automation Science from Nanjing University of Aeronautics and Astronautics, Jiangsu, China, in 2000, the M.S. degrees in Traffic Information Engineering and Control from Shanghai Ship and Shipping Research Institute, Shanghai, China, in 2003, and the Ph.D. degree in Traffic Information Engineering and Control from Tongji University, Shanghai, China, in 2006.

Since 2006, she has been with the faculty of the School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai, China, where she is currently a lecturer. She is also a post-doctoral researcher of Asia University, Taiwan. Her research interests include information security, image processing, and information theory and coding.