Journal of Information Hiding and Multimedia Signal Processing ©2014 ISSN 2073-4212
Ubiquitous International Volume **5**, Number **1**, January **2014**

Efficient and Meaningful Multisecret Image Sharing Based on Block Imitation

Zhi-Hui Wang
Department of Software
Dalian University of Technology
DaLian, China
wangzhihui1017@gmail.com

Marcos Segalla Pizzolatti
Department of Information Engineering and Computer Science
Feng Chia University
Taichung City 40724 Taiwan
segall.pizzo@gmail.com

Chin-Chen Chang
Department of Information Engineering and Computer Science
Feng Chia University
Taichung City 40724 Taiwan
alan3c@gmail.com

Received December, 2012; revised February, 2013

Abstract. *Chen et al. proposed a deterministic algorithm to create a new secret sharing scheme for multiple secret images (n+1, n+1), by Boolean-based visual secret sharing. This algorithm achieves no pixel expansion, reversibility, and no codebook required. However, this scheme has the disadvantage that the shared images are all meaningless shares, becoming very suspicious in the attackers' eyes. To solve the above problem, this paper proposes a new multi-secret image sharing algorithm to share n secret images into n meaningful shared images using halftone images. The proposed scheme can encode multiple secrets in fewer shares than Chen et al.'s scheme, and also achieves a reversible secret construction. Most important this technique can avoid attracting the attention of attackers by using meaningful shared images rather than showing meaningless shares to attackers.*

Keywords: Secret sharing, Image sharing, Meaningful shared images, Halftone images

1. Introduction.

Shamir [1] proposed a secret sharing scheme to divide a data D into n parts where only all needed parts put together are allowed in reconstructing the original secret and with fewer parts put together revealing no information of the original secret. In the same year, Blakley [2] proposed a secret sharing scheme in order to safeguard cryptographical keys. This paper focuses on a new branch of sharing-visual secret sharing.

The traditional visual secret sharing (VSS), first proposed by Naor and Shamir [3], provides a human visual system to decrypt the binary secret image from shared images without any computational cost. Based on sharing binary images, many schemes [8, 14-16] extended the VSS scheme to be suitable for gray level and color images. In Naor and Shamir's scheme, the secret image quality degrades to a very low constraint quality at the end of the decoding process, and the participants who have the shares must carefully overlap them to see the secret. Most of the time, this procedure of overlapping the shares can be difficult to align. Another problem of traditional VSS schemes is that since each pixel of the secret image is encoded into two or more sub-pixels, these schemes have a pixel expansion problem, which provides a greater information burden in transferring the images through the Internet. Many secret sharing schemes [4-13, 17-18] have been proposed to improve the traditional VSS's sharing capacity, contrast quality, and to solve the pixel expansion problem.

Wang et al. [7] proposed a method to provide shadow images that are smaller than the secret images. This scheme provides a better image quality of the secret images during the sharing process, and achieves 40% less of the overall shadow size than [4]. Chang et al. [10] also achieves small shadow images based on the technology of [7] and they can use color images as the secret in their scheme. Shyu et al. [9] and Feng et al. [11] proposed schemes to encode multiple secrets into two shared images, using circle and cylinder shares, respectively. However, while sharing more secrets, the pixel expansion increases and the contrast quality decreases. Lin et al. [12] improved Shyu et al.'s scheme [9] and Feng et al.'s scheme [11], archiving no pixel expansion for secrets, but have the limitation to share only two secrets at a time. Lin et al. [12] generated shared images without a predefined pattern book to achieve no pixel expansion, and the encrypting process is divided into three processes, including a camouflaging algorithm that allows the construction of shares without pixel expansion and also achieves a good contrast quality in the decoded image. Recently, Wang et al.'s scheme [8] and Chen et al.'s scheme [13] achieved lossless secret construction, no pixel expansion, easy alignment, and no codebook required by using the Boolean operations. Chen et al.'s scheme [13] has better sharing capacity than Wang et al.'s scheme [8], which uses $n+1$ shared images to conceal n secret images. The big problem of Chen et al.'s scheme is that meaningless shares may cause attackers' suspicions.

In general, all schemes mentioned above have some disadvantages to be improved. Some of them have a pixel expansion problem; some of them have the limitation of sharing one secret image at a time, and especially, all of them use meaningless shares. Thus, a new visual secret sharing scheme is proposed in this paper. The proposed scheme improves the sharing capacity of Chen et al.'s scheme to achieve sharing n secret images by n shares at a time. Furthermore, the proposed scheme constructs meaningful shares for participants without a pixel expansion problem through imitating to a reference image.

The remainder of this paper is organized as follows: in Section 2, the related work is reviewed; the proposed scheme is explained in Section 3; in Section 4, the experimental results are shown; finally, the last section gives the conclusions of this paper.

2. Related Work.

Chen et al. [13] extended the deterministic algorithm (n, n) of Wang et al.'s [8] scheme, creating a new secret sharing scheme for multiple secret images $(n+1, n+1)$, by Boolean-based VSS. Chen et al. implemented an XOR Boolean operation for the encoding and decoding processes. This algorithm has no pixel expansion; no extra information is needed to send to the receiver, and for n secrets has created $n+1$ meaningless shared images. Sections 2.1 and 2.2 show the encoding and decoding processes in detail, respectively.

2.1. The encoding process of Chen et al.'s scheme.

The encoding process is divided into three steps as follows:
Input: n secret images $G_i, i = 0, ..., n-1$.
Output: $n+1$ shared images $S_m, m = 0, ..., n$.
Step 1: Generate a random integer matrix S_0 as the first shared image.

Step 2: Generate $n-1$ random matrices B_k by the following equation:

$$B_k = G_k \oplus S_0, where\ k = 1, 2, ..., n-1. \tag{1}$$

Step 3: Compute the other shared images S$_k$'s by the following equation:

$$S_k = \begin{cases} B_k & if\ k = 1, \\ B_k \oplus B_{k-1} & if\ k = 2, \dots, n-1, \\ G_0 \oplus B_{k-1} & if\ k - n. \end{cases} \tag{2}$$

Encoding example of Chen et al.'s scheme

The secret binary matrices are taken as an example to show the encoding process as below. We assume that n is equal to two, which means two secrets as input and three shares as output.

Input: G_0, G_1Output: S_0, S_1, S_2.

The secret binary matrices G_0 and G_1 are given, as following:

$$G_0 = \begin{array}{|c|c|c|}\hline 1 & 0 & 1 \\ \hline 1 & 0 & 0 \\ \hline 1 & 1 & 0 \\ \hline \end{array} \qquad G_1 = \begin{array}{|c|c|c|}\hline 0 & 1 & 0 \\ \hline 0 & 0 & 1 \\ \hline 0 & 0 & 1 \\ \hline \end{array}$$

Step 1: Generate a random matrix S_0 as the first shared image, as following:

$$S_0 = \begin{array}{|c|c|c|}\hline 1 & 1 & 0 \\ \hline 0 & 1 & 1 \\ \hline 1 & 1 & 0 \\ \hline \end{array}$$

Step 2: Create the random matrix B_1 by Equation (1).

$$B_1 = G_1: \begin{array}{|c|c|c|}\hline 0 & 1 & 0 \\ \hline 0 & 0 & 1 \\ \hline 0 & 0 & 1 \\ \hline \end{array} \oplus S_0: \begin{array}{|c|c|c|}\hline 1 & 1 & 0 \\ \hline 0 & 1 & 1 \\ \hline 1 & 1 & 0 \\ \hline \end{array} = \begin{array}{|c|c|c|}\hline 1 & 0 & 0 \\ \hline 0 & 1 & 0 \\ \hline 1 & 1 & 1 \\ \hline \end{array}$$

Step 3: Compute the shared images S1 and S2 Equation (2).

$$S_1 = B_1: \begin{array}{|c|c|c|}\hline 1 & 0 & 0 \\ \hline 0 & 1 & 0 \\ \hline 1 & 1 & 1 \\ \hline \end{array} \qquad S_2 = G_0: \begin{array}{|c|c|c|}\hline 1 & 0 & 1 \\ \hline 1 & 0 & 0 \\ \hline 1 & 1 & 0 \\ \hline \end{array} \oplus B_1: \begin{array}{|c|c|c|}\hline 1 & 0 & 0 \\ \hline 0 & 1 & 0 \\ \hline 1 & 1 & 1 \\ \hline \end{array} = \begin{array}{|c|c|c|}\hline 0 & 0 & 1 \\ \hline 1 & 1 & 0 \\ \hline 0 & 0 & 1 \\ \hline \end{array}$$

2.2. **The decoding process of Chen et al.'s scheme.** The decoding process is divided into three steps as following:

Step 1: Use all $n+1$ shared images together to reconstruct the first secret image G'_0 by the following equation:

$$G'_0 = \psi_{i=1}^{n} S_i. \tag{3}$$

Step 2: Generate $n-1$ random matrices B_k by the following equation:

$$S_k = \begin{cases} B_k & if\ k = 1, \\ B_k \oplus B_{k-1} & if\ k = 2, \dots, n-1. \end{cases} \tag{4}$$

Step 3: Reconstruct the other $n-1$ secret images G'_k' s by the follow equation:

$$G'_k = B_k \oplus S_0,\ if\ k = 1, \ldots, n-1. \tag{5}$$

Decoding example of Chen et al.'s scheme

Step 1: Reconstruct the first secret image G'_k by using the shared images $S_1$and $S_2$by Equation (3), as following:

$$G'_0 = S_1\text{:}\ \begin{array}{|c|c|c|}\hline 1 & 0 & 0 \\ \hline 0 & 1 & 0 \\ \hline 1 & 1 & 1 \\ \hline\end{array} \oplus S_2\text{:}\ \begin{array}{|c|c|c|}\hline 0 & 0 & 1 \\ \hline 1 & 1 & 0 \\ \hline 0 & 0 & 1 \\ \hline\end{array} = \begin{array}{|c|c|c|}\hline 1 & 0 & 1 \\ \hline 1 & 0 & 0 \\ \hline 1 & 1 & 0 \\ \hline\end{array}$$

Step 2: Generate the random matrix B_1 by Equation (4), as following:

$$B_1 = S_1\text{:}\ \begin{array}{|c|c|c|}\hline 1 & 0 & 0 \\ \hline 0 & 1 & 0 \\ \hline 1 & 1 & 1 \\ \hline\end{array}$$

Step 3: Reconstruct the second secret image G'_1 by the Equation (5), as following:

$$G'_1 = B_1\text{:}\ \begin{array}{|c|c|c|}\hline 1 & 0 & 0 \\ \hline 0 & 1 & 0 \\ \hline 1 & 1 & 1 \\ \hline\end{array} \oplus S_0\text{:}\ \begin{array}{|c|c|c|}\hline 1 & 1 & 0 \\ \hline 0 & 1 & 1 \\ \hline 1 & 1 & 0 \\ \hline\end{array} = \begin{array}{|c|c|c|}\hline 0 & 1 & 0 \\ \hline 0 & 0 & 1 \\ \hline 0 & 0 & 1 \\ \hline\end{array}$$

3. **Proposed Scheme.** In this section, a new multi-secret image-sharing algorithm is proposed to share n secret images into n meaningful shared images, where $n \geq 2$. This algorithm is reversible and uses halftone images as secret images, cover images, and shares. To convert grey-level/color images into halftone images, the graphic software Photoshop was used. To achieve the capacity to share the same number of secrets into the same number of shares, we use an algorithm based on block imitation. The secret images are encoded into shared images by using cover images as the reference, which can make the shares meaningful.

3.1. **The encoding procedure.** The encoding procedure consists of six steps as follows: Step 1: Given n secret images, the bits of the reference shares' blocks are calculated, by the following equation:

$$R_x^s = (G + x) \bmod (y) \tag{6}$$

where R_x^s is reference shared image's bit, G is secret image's bit, s is number of secrets; where $1 \leq s \leq n$ and $n \geq 2$, x is a reference number starting from 1 until $(y-1)$ and y is a geometric sequence (starting from 4) with the common ratio equal to 2

The variables x and y depend on the number of secrets (n) to be embedded each time; if $n = 2$ Equation (6) will be:
R_1^s=(G + 1)mod4 for the first reference,
R_2^s=(G + 2)mod4 for the second reference,
R_3^s=(G + 3)mod4 for the third reference.

In Equation (6), the secret images are divided into blocks. For each secret image block, one reference block of the same size is created, where the secret bits are embedded. From the blocks of the secret images, the bits are embedded into the first reference block. When the first reference block is completely filled, then the secret bits are embedded into the next reference block, and so on, until all the reference blocks are filled.

Step 2: Given n cover images, count the number of bits equal to 1 for each cover block.

Step 3: Count the number of bits equal to 1 for each reference shared block and calculated the absolute difference (dif) between the number of bits equal to 1 of the first shared reference block and the number of bits equal to 1 of the first cover block, and so on, until the last reference shared and cover blocks are calculated. The dif operation is given below:

$$dif_s^x = \left| S_x^s - C_s \right|, \tag{7}$$

where S_x^s is the number of bits equal to 1 for the reference shared blocks, C_s is the number of bits equal to 1 for the cover blocks, s is the number of secrets, where $1 \leq s \leq n$ and $n \geq 2$, and x is the reference number.

Step 4: Calculate the addition (sum) between the absolute differences (dif) of the shared blocks of the same reference and the result nearest to 0 shows the best reference. Thus, it is saved into a reference sequence (ref) as a decimal number. The sum operation is given, as below:

$$sum = \sum_{s=1}^{n} dif_s^x, \tag{8}$$

where s = number of secrets, where $\sum_{s=1}^{n}$ and $n \geq 2$, x = reference number.

Step 5: After choosing the best reference, which means the reference shared blocks more similar to the cover blocks, these reference shared blocks are embedded into the original shared image.

Step 6: Repeat Steps 1 to 5 until the last secret image blocks and the complete construction of the original shared images.

Encoding Example

The secret binary matrices are taken as an example to show the encoding process We assume that n is equal to two, which means two secrets as input and two shares as output as below:

Input: G1, G2.

Output: O1, O2.

The secret binary matrices G_1 and G_2 are given as following:

G_1

0	1
1	0

G_2

0	1
0	0

In Step 1, the proposed scheme calculates the three reference shares for two secrets, by Equation (6), as following:

$(G+\mathbf{1})mod4$	=	R_1^s
00		01
01		10
10		11
11		00

R_1^1

0	1
0	0

R_1^2

1	1
0	1

$(G+\mathbf{2})mod4$	=	R_2^s
00		10
01		11
10		00
11		01

R_2^1

1	0
0	1

R_2^2

0	0
1	0

$(G+\mathbf{3})mod4$	=	R_3^s
00		11
01		00
10		01

R_3^1

1	1
1	0

R_3^2

0	1
1	1

In Step 2, for given two cover images, each one are counted the bits equal to 1, as following:

C_1

1	**1**
1	0

C_2

0	**1**
0	**1**

C_1 = **3 bits** equal to1 C_2 = **2 bits** equal to 1

In Step 3, count the bits equal to 1 for each reference shared block. Thus, the absolute difference is calculated by Equation (7), for the corresponding shared and cover blocks, as following:

$$\begin{array}{llllll}
S_1^1 = 1 & C1 = 3 & dif_1^1 = |1-3| = 2 & S_1^2 = 3 & C_2 = 2 & dif_2^1 = |3-2| = 1 \\
S_2^1 = 2 & C1 = 3 & dif_1^2 = |2-3| = 1 & S_2^2 = 1 & C_2 = 2 & dif_2^2 = |1-2| = 1 \\
S_3^1 = 3 & C1 = 3 & dif_1^3 = |3-3| = 0 & S_3^2 = 3 & C_2 = 2 & dif_2^3 = |3-2| = 1
\end{array}$$

In Step 4, calculate the *sum*, by Equation (8), of the same reference shared blocks, and also save the corresponding decimal number of the reference number into an array *ref*, as following:

Reference 1: $dif_1^1 + dif_2^1 = 3$
Reference 2: $dif_1^2 + dif_2^2 = 2$
Reference 3: $dif_1^3 + dif_2^3 = 1$ => **best reference (nearest to 0)** => $ref[3, \ldots]$

In Step 5, the bits of the chosen reference blocks are embedded into the original shared blocks $O_1$and O_2, as following:

O_1

1	1
1	0

O_2

0	1
1	1

In Step 6, repeat Steps 1 to 5, until all blocks are encoded.

3.2. **The decoding procedure.** The decoding procedure consists of two steps as follows: Step 1: From n original shared images the bits of the original shared blocks are used to calculate the bits of the recovery secret blocks by the following equation:

$$G'_s = (O + x) \bmod (y) \tag{9}$$

where G'_s is recovered secret image's bit, O is original shared image's bit, s is number of secrets; where $\sum_{s=1}^{n}$ and $n \geq 2$, x is the extracted reference number, and y is the geometric sequence (starting from 4) with the common ratio equal to 2.

Firstly, extract the reference number from the reference sequence. Thus, we can discover which x in Equation (9) is used to recover the original secret bits. When the bits of the first original shared block are finished, the bits of the next original shared block are used to recover the secret bits, and so on, until the bits of last original shared block are used.
Step 2: Repeat Step 1 until the original secret images are totally recovered.

Decoding Example

The original shared image blocks O_1 and O_2 are given, as below:

O_1

1	1
1	0

O_2

0	1
1	1

In Step 1: extract the reference number from the array *ref* to recover the original secret bits G'_1 and G'_2 as shown below:

ref = 3

$(O+\mathbf{3})mod4$ =	G'_s
11	00
00	01
01	10
10	11

G'_1

0	1
1	0

G'_2

0	1
0	0

Step 2: Repeat Step 1 until the original secret images are completely recovered.

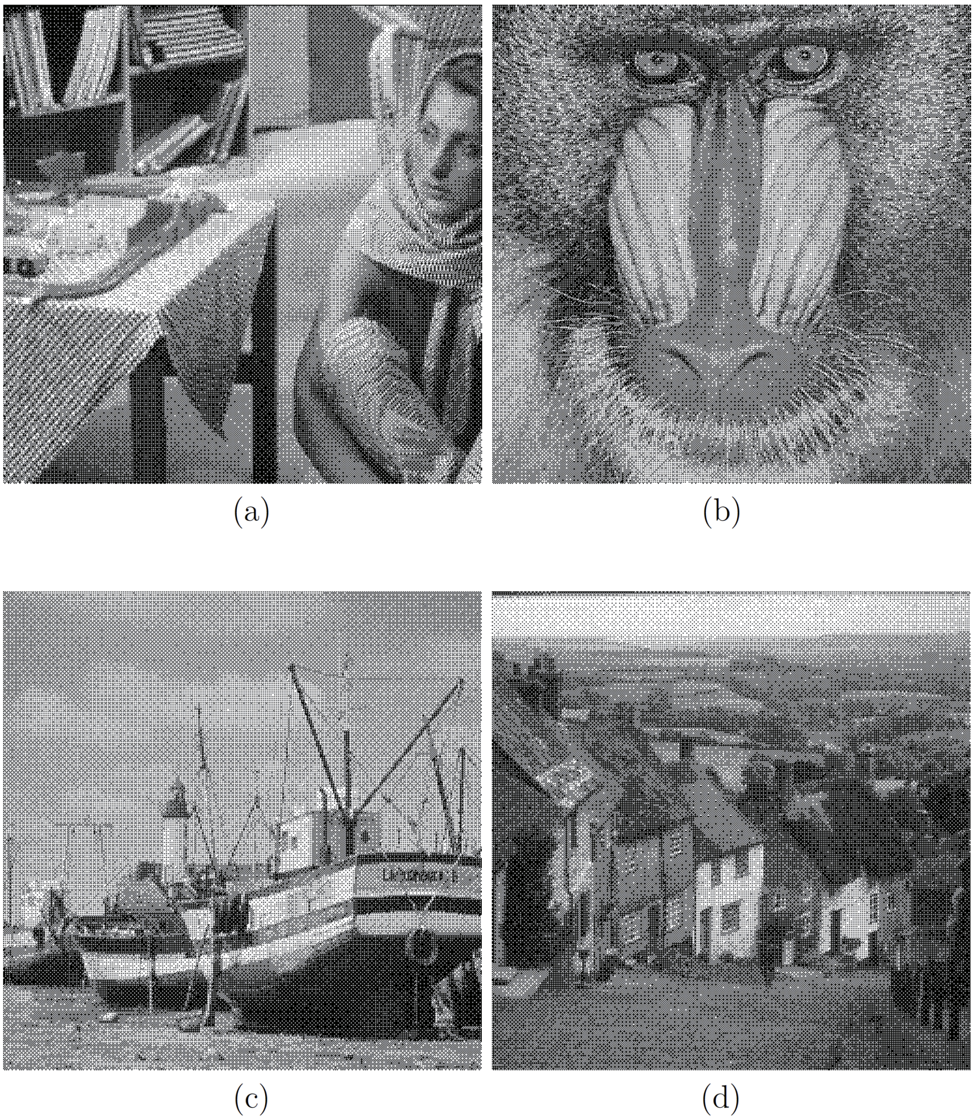
4. **Experimental Results.** All images used in the experiments are halftone images sized 512 × 512. The experiments include three parts: two, three, and four secret images with blocks sized 2 × 2 and 4 × 4, respectively. We use Barbara, baboon, boat, and gold hill as the secret images as shown in Figure 1. As to the cover images we use peppers, Lena, airplane, and sailboat, as shown in Figure 2, to construct the meaningful shared images. The results of the shared images for two, three, and four secrets using blocks of size 2 × 2 and 4 × 4 are shown in Figures 3, 4, 5, 6, 7, and 8. The recovered images are shown in Figure 9.

To embed two secret images, we use the secret images of Figures 1(a) and (b) and the cover images of Figures 2(a) and (b), to construct the shared images of Figures 3 and 6. To embed three secret images, we use the secret images of Figures 1(a), (b) and (c) and the cover images of Figures 2(a), (b) and (c), to construct the shared images of Figures 4 and 7. Finally, in the last experiment all secret images of Figure 1, and all the cover images of Figure 2, are used to construct the shared images of Figures 5 and 8.

We compare our proposed scheme with Wang et al.'s scheme [8] and Chen et al.'s scheme [13] in Table 1. As can be observed in Table 1, Wang et al.'s scheme requires n shared images to embed only one secret. Chen et al.'s scheme [13] is a multi-secret image scheme, and requires $n+1$ shared images to embed n secrets. The proposed scheme achieves the highest sharing capacity, where the number of secrets is the same as the number of shared images.

The sharing capacity is defined as: $\frac{\text{the number of secret images}}{\text{the number of share images}}$.

From Fig. 3, Fig. 4 and Fig. 5, it is obvious that the new generated shares are meaningful. So the proposed scheme can solve the security problem of meaningless shares. Our experimental results show only the quality of binary test images. For the gray level image and color image, also the proposed scheme is suitable by transforming them into



(a) (b)

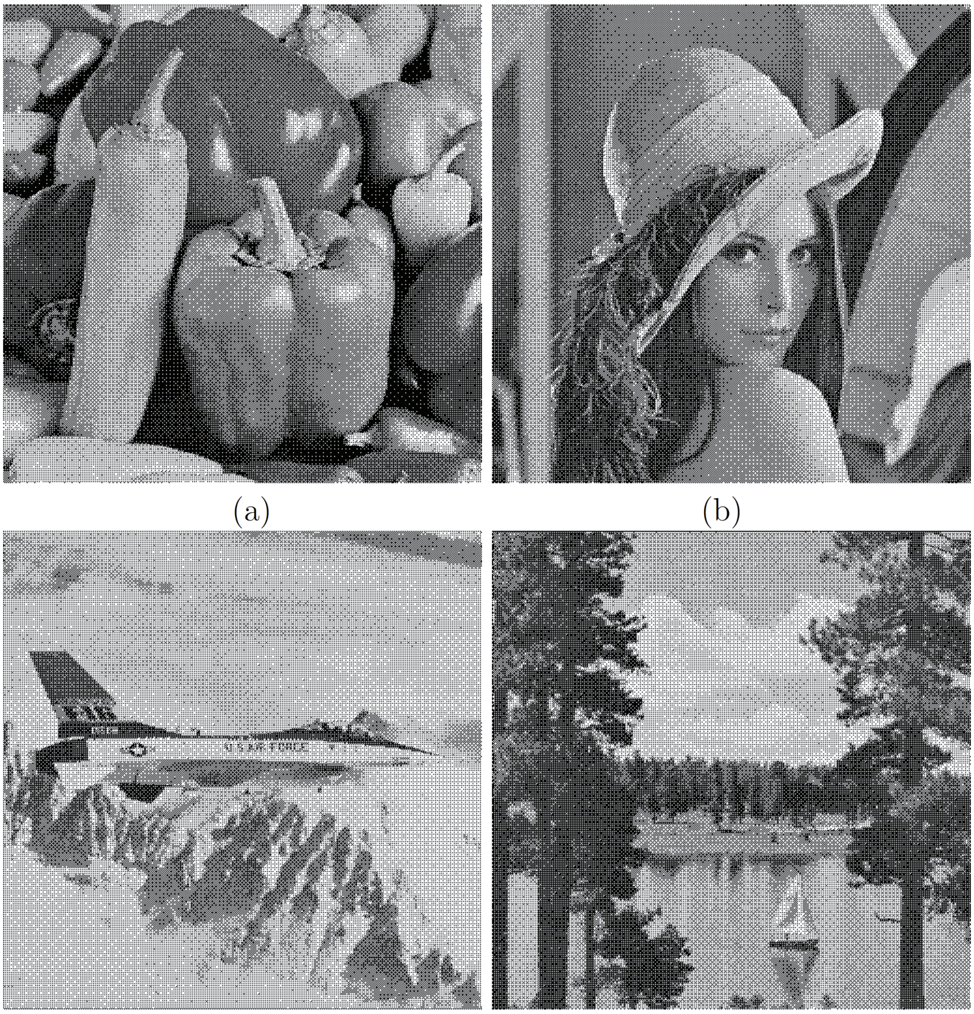
(c) (d)

Figure 1. (a) Secret image of Barbara, (b) secret image of baboon, (c) secret image of boat, and (d) secret image of gold hill

Table 1. Performance comparisons

	Wang et al. [8]	Chen et al. [13]	The proposed
Reversible	Yes	Yes	Yes
Pixel expansion	No	No	No
Image format	Binary grey-level color	Binary grey-level color	Binary grey-level color
Need extra information	No	No	Yes
Sharing capacity	1/n	n/(n+1)	n/n
Significance of shared images	Meaningless	Meaningless	Meaningful

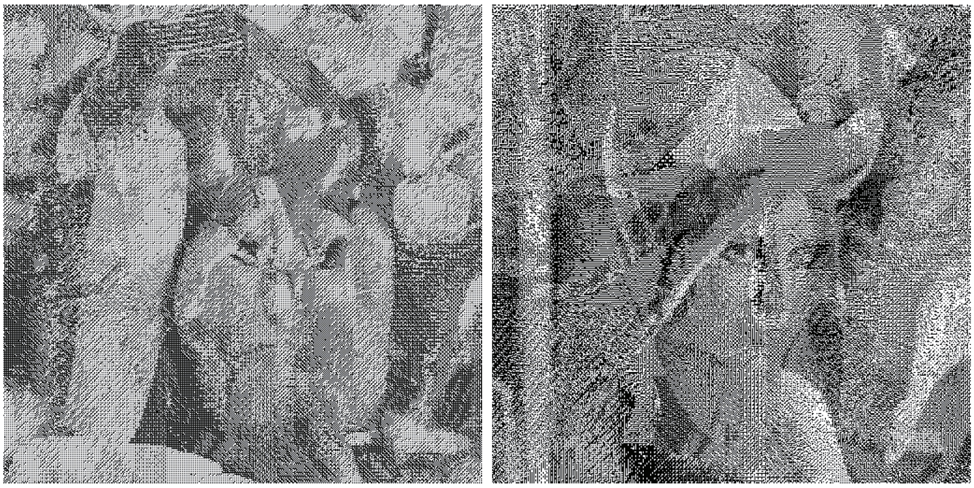
halftone images. The extra information needed to decode the shared images can be compressed by the JBIG lossless compressing algorithm. The experimental result shows



(a) (b)

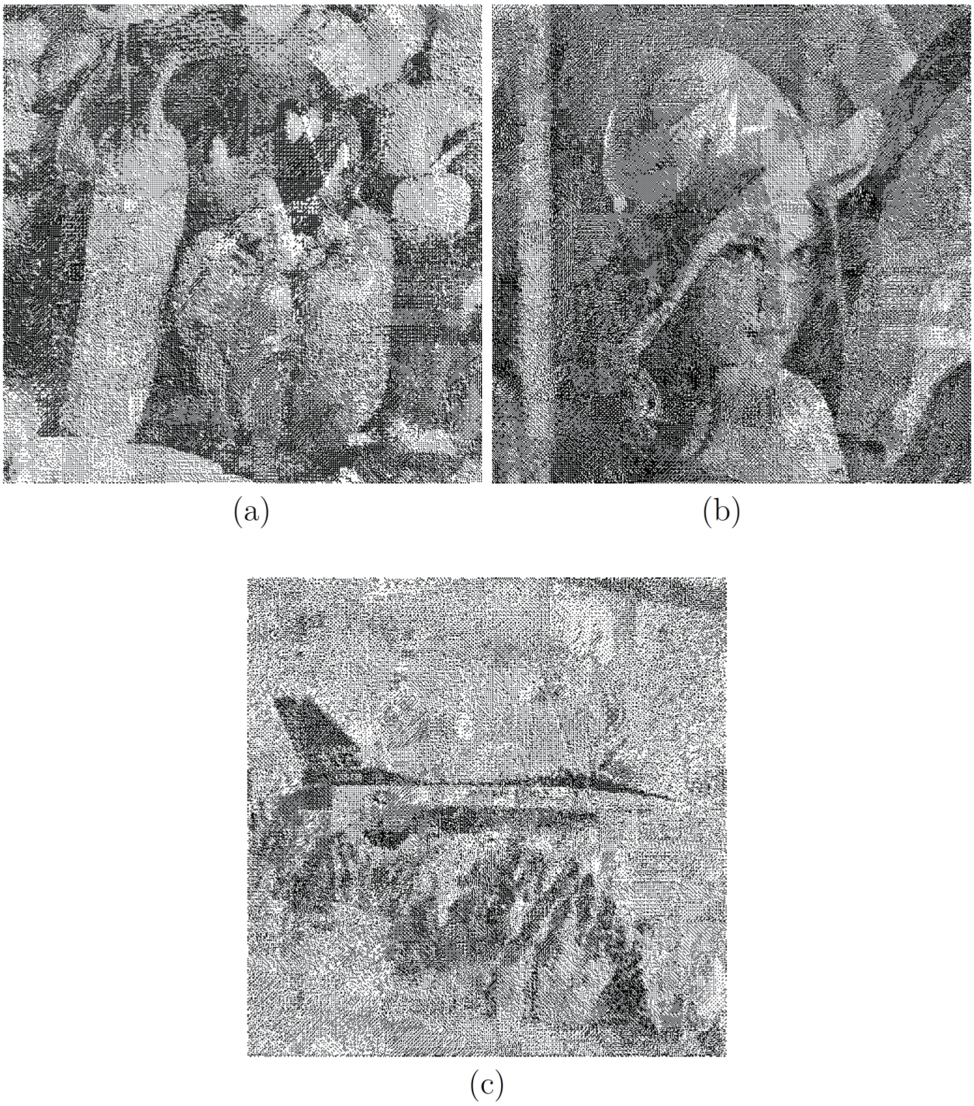
(c) (d)

Figure 2. (a) Cover image of peppers, (b) cover image of Lena, (c) cover image of airplane, and (d) cover image of sailboat



(a) (b)

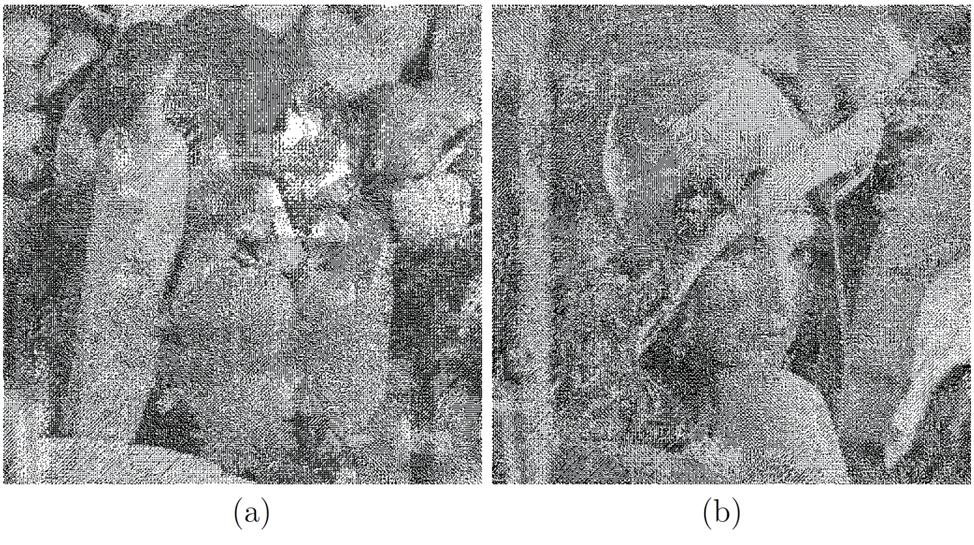
Figure 3. Shared images for two secrets using blocks of size 2 × 2



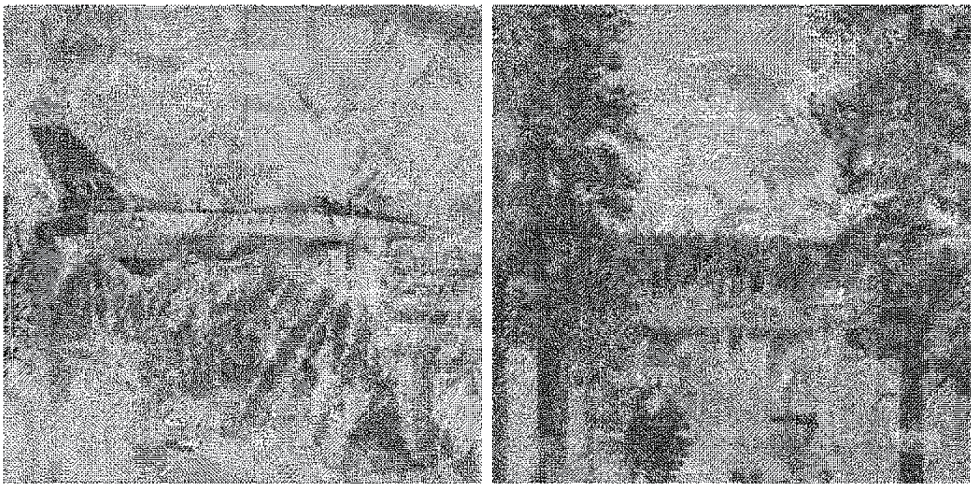
(a) (b)

(c)

Figure 4. Shared images for three secrets using blocks of size 2 × 2

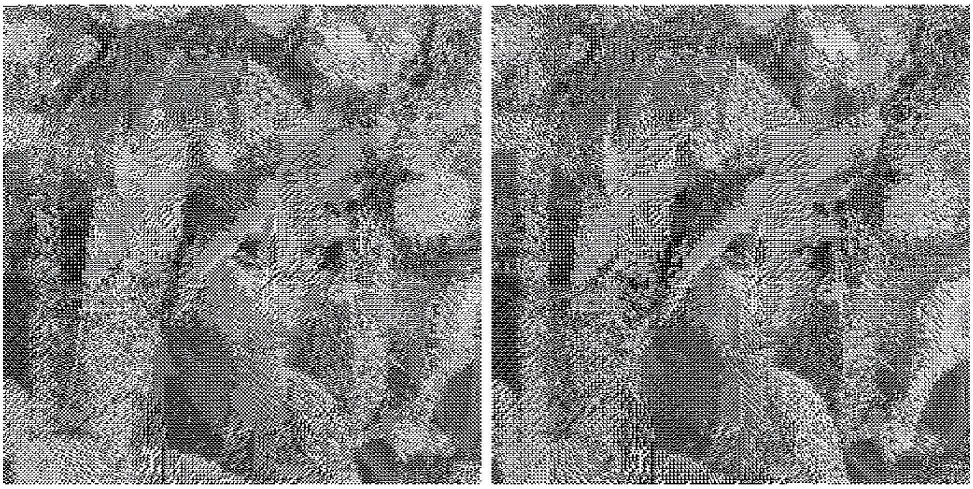


(a) (b)



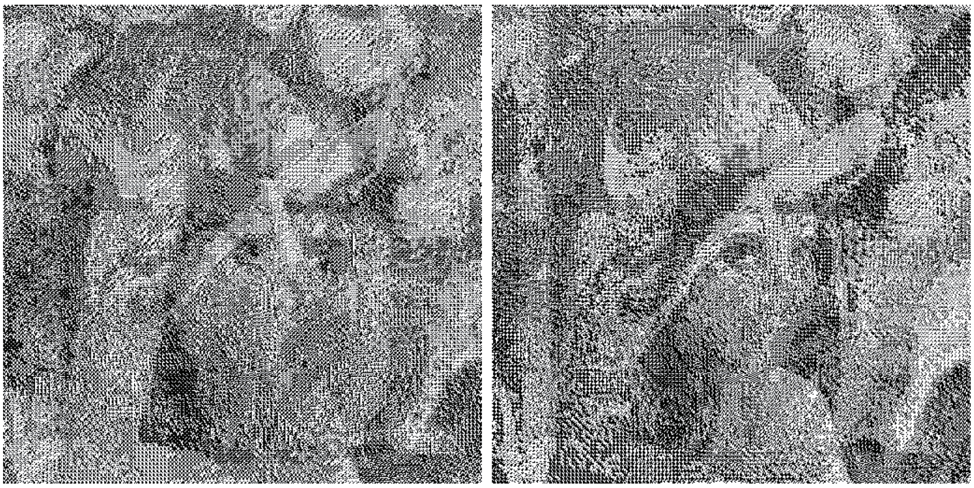
(c) (d)

Figure 5. Shared images for four secrets using blocks of size 2 × 2

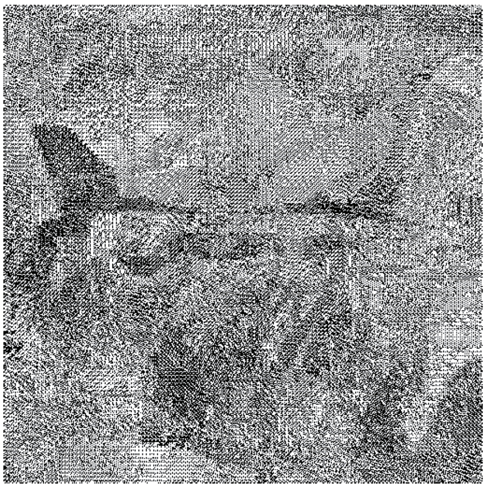


(a) (b)

Figure 6. Shared images for two secrets using blocks of size 4 × 4

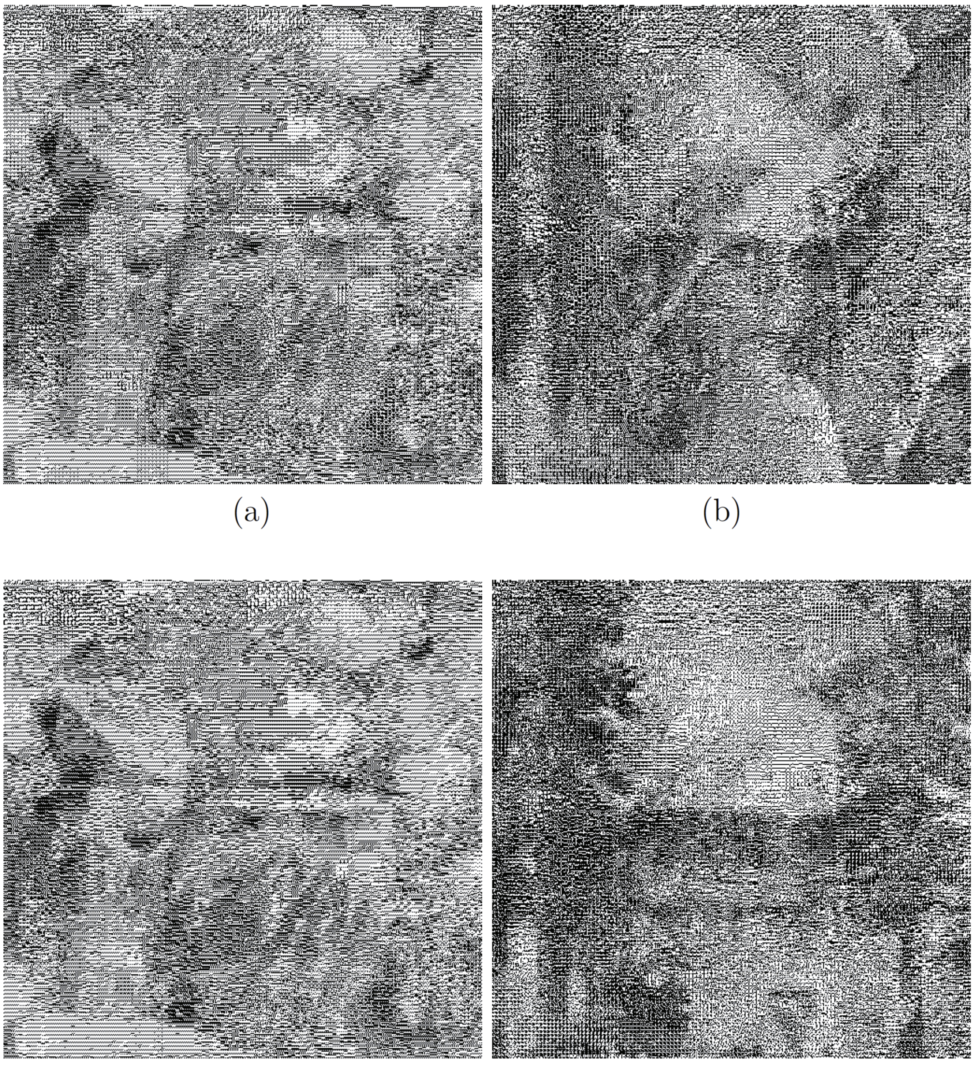


(a) (b)



(c)

Figure 7. Shared images for three secrets using blocks of size 4 × 4



(a) (b)

(c) (d)

Figure 8. Shared images for four secrets using blocks of size 4 × 4

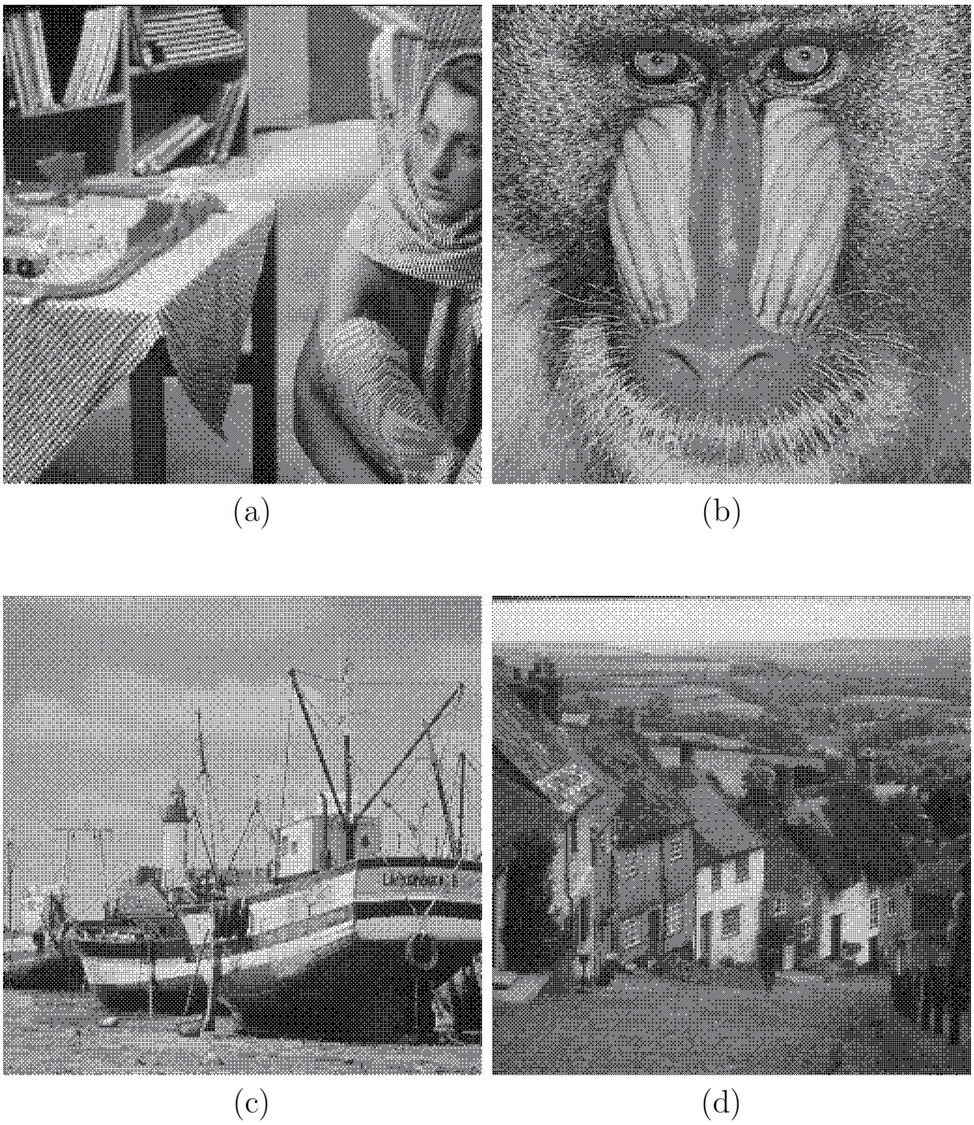

(a) (b) (c) (d)

FIGURE 9. Recovery images of Barbara baboon, boat, and gold hill

the compression ratio of JBIG can achieve lower than 1%; therefore, there is no problem in transmitting it to the receiver side.

After experimenting for blocks of size 2 × 2 and 4 × 4 by using many different kinds of images, it is suggested that the secret images should be chosen as complex images and the cover images should be chosen as smooth images. And the block size of 2 × 2 can achieve better results.

5. **Conclusion.** The proposed secret image scheme is a multi-secret image sharing that can encode the secret images using less shared images than [13], and also have the advantage that the shared images can be recognized as meaningful images, having no information of the secret images. In the proposed algorithm, when using blocks of size 2 × 2, the more secrets it has, the better the quality that the shared images get. Thus, this paper clearly shows that the proposed method is better than the other schemes mentioned previously since it could diminish the number of the shared images required to encode the secrets, improving the sharing capacity, and, in addition, the shared images

are meaningful. Therefore, we can say that the proposed method can make the system friendlier.

REFERENCES

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

[2] G. R. Blakley, Safeguarding cryptography keys, *Proc. of AFIPS National Computer Conference*, pp. 313-317, 1979.

[3] M. Naor, and A. Shamir, Visual cryptography, *Proc. of the Advances in Cryptology-Eurocrypt*, LNCS 950, pp. 1-12, 1995.

[4] C. C. Thien, and J. C. Lin, Secret image sharing, *Journal of Computers & Graphics*, vol. 26, no. 5, pp. 765-770, 2002.

[5] C. S. Tsai, C. C. Chang, and T. S. Chen, Sharing multiple secrets in digital images, *Journal of Systems and Software*, vol. 64, no. 2, pp. 163-170, 2002.

[6] J. B. Feng, H. C. Wu, C. S. Tsai, and Y. P. Chu, A new multi-secret images sharing scheme using Largrange's interpolation, *Journal of Systems and Software*, vol. 76, no. 3, pp. 327-339, 2005.

[7] R. Z. Wang, and C. H. Su, Secret image sharing with smaller shadow images, *Journal of Pattern Recognition Letters*, vol. 27, no. 6, pp. 551-555, 2006.

[8] D. Wang, L. Zhang, N. Ma, and X. Li, Two secret sharing schemes based on Boolean operations, *Journal of Pattern Recognition*, vol. 40, no. 10, pp. 2776-2785, 2007.

[9] S. J. Shyu, S. Y. Huang, Y. K. Lee, R. Z. Wang, and K. Chen, Sharing multiple secrets in visual cryptography, *Journal of Pattern Recognition*, vol. 40, no. 12, pp. 3633-3651, 2007.

[10] C. C. Chang, C. C. Lin, C. H. Lin, and Y. H. Chen, A novel secret image sharing scheme in color images using small shadow images, *Journal of Information Sciences*, vol. 178, no. 11, pp. 2433-2447, 2008.

[11] J. B. Feng, H. C. Wu, C. S. Tsai, Y. F. Chang, and Y. P. Chu, Visual secret sharing for multiple secrets, *Journal of Pattern Recognition*, vol. 41, no. 12, pp. 3572-3581, 2008.

[12] T. L. Lin, S. J. Horng, K. H. Lee, P. L. Chiu, T. W. Kao, Y. H. Chen, R. S. Run, J. L. Lai, and R. J. Chen, A novel visual secret sharing scheme for multiple secrets without pixel expansion, *Journal of Expert Systems with Applications*, vol. 37, no. 12, pp. 7858-7869, 2010.

[13] T. H. Chen, and C. S. Wu, Efficient multi-secret image sharing based on Boolean operations, *Journal of Signal Processing*, vol. 91, no. 1, pp. 90-97, 2011.

[14] Y. C. Hou, Visual cryptography for color images, *Journal of Pattern Recognition*, vol. 36, no. 7, pp. 1619-1629, 2003.

[15] S. J. Shyu, Efficient visual secret sharing scheme for color images, *Journal of Pattern Recognition*, vol. 39, no. 5, pp. 866-880, 2006.

[16] M. Iwamoto, and H. Yamamoto, The optimal n-out-of-n visual secret sharing scheme for gray-scale images, *IEICE trans. fundamentals of electronics, communications and computer sciences* vol. E85-A, no. 10, pp. 2238-2247, 2002.

[17] C. Guo, and C. C. Chang, A construction for cecret sharing scheme with general access structure, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 4, no. 1, pp. 1-8, 2013.

[18] C. S. Chan, C. C. Chang, and H. P. Vo, A user-friendly image sharing scheme using JPEG-LS median edge predictor, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 3, no. 4, pp. 340-351, 2012.