# An Adaptable (n, n) Secret Image Sharing Mechanism Based on Boolean Operation

Zhi-Hui Wang[1], Haibo Jin [2], Xuebo Wang [3], and Chin-Chen Chang[4,5]
*(Corresponding author: Chin-Chen Chang)*

School of Software, Dalian University of Technology, Dalian, Liaoning, China[1]
Department of Computer Science, University of Helsinki, P.O. 68, FI-00014, Finland[2]
Chalmers University of Technology, SE-412 96 Gothenburg, Sweden[3]
Department of Information Engineering and Computer Science, Feng Chia University[4]
Taichung City 40724, Taiwan
Department of Computer Science and Information Engineering, Asia University[5]
Taichung 41354, Taiwan
(Email: alan3c@gmail.com)

*(Received Apr. 20, 2012; revised and accepted July 5, 2012)*

## Abstract

Secret image sharing, as an extension of secret sharing, has attracted the attention of many scholars in recent years. Multi-secret image sharing is an extension of traditional secret image sharing in which only one secret image can be shared among one group. In order to extend the utility of the mechanism, we propose an innovative (*n*, *n*) secret image sharing scheme based on matrix transformation. Due to the skillful design of the matrix operation used in matrix transformation, the proposed scheme is applicable to more than one secret image. Further, more secret images and participants can be included in this sharing system even after the secret image sharing procedure has been constructed. Also, the proposed scheme produces high-quality shadow images, and it can reconstruct the secret images losslessly. Moreover, the computational complexity of the proposed scheme is minimized by only using the XOR operation, which stands for exclusive or and is a logical operation that outputs true whenever both inputs differ. The experimental results demonstrated that the proposed scheme provides the aforementioned advantages.

*Keywords: secret image sharing, secret sharing, information hiding, adaptable secret sharing*

## 1 Introduction

Recently, due to the prevalent use of Internet applications and the rapid growth of network bandwidth, more and more multi-media information, such as radio, images, and videos, is being transmitted through the Internet. Since the Internet is not a secure environment, we must deal with the major issue of providing secure transmission and storage of sensitive, multi-media information, especially multi-media documents that are classified as top secret documents.

A secret sharing mechanism was proposed for the first time in 1979 by Blakely[1] and Shamir[10]. In their (*t*, *n*)-threshold secret sharing scheme, the secret data can be divided into *n* independent parts and then distributed to *n* involved participants. However, the secret data can be retrieved only when only *t* or more than *t* of the *n* participants cooperate. Any *t*-1 or less than *t*-1 of the *n* participants cannot retrieve any of the secret data. For decades, the studies and complementary work based on this scheme have made many prominent achievements [2, 3, 11]. In 1995, Naor and Shamir[9] first introduced a new secret image sharing method based on the (*t*, *n*)-threshold scheme, and it is known as visual secret sharing (VSS) and could share a secret image using several images called shadows. This method can reduce the computation complexity effectively because it utilizes the human visual system to recover the secret image and requires little computation in the shadow-generation phase. However, it often leads to some other problems, such as image expansion, contrast, and meaningless shadows[4, 15, 17]. Since a meaningless image easily can arouse the suspicion of a malicious attacker when it is transmitted through the Internet, the steganographic approach is utilized to hide the shadows in meaningful cover images, called meaningful shadow images[8, 12, 13, 16]. As long as the shadow images have high quality from the standpoint of visual perception, they are protected from attacks and are easy to store. However, this approach may lead to distortion of the secret image[8, 16] or expansion of the pixels of the shadow image [5, 12, 17]. To solve these shortcomings, Tuyls[14] proposed an (*n*, *n*) scheme based on the XOR operation for binary images that has no pixel expansion and precisely reconstructs the image. Also, the computational complexity of the bit-wise operation that is used is low. It is worth mentioning that all of the secret image sharing schemes listed above focus on the one-secret image sharing scheme. In other words, only one secret image can be hidden in one sharing scheme. Actually, with the rapid development of the Internet, the

amount of information transmitted over the Internet has become very large, and sometimes we need to share more than one secret image at a time. In order to meet this need, a novel, adaptable, secret image sharing scheme is required that can share n secret images at a time. Since ($t$, $n$)-threshold is difficult to construct to fulfill this special need, we decide to start with ($n$, $n$)-threshold, which is a special case of ($t$, $n$). Afterwards, an ($n$, $n$) scheme can be extended to a ($t$, $n$) scheme. Based on this, we proposed a novel ($n$, $n$) secret image sharing scheme in this paper. The scheme meets the four essential requirements of an ideal scheme, i.e., security, precision, low computational complexity, and no pixel expansion, and also can be extended. In addition, first, more than one image can be hidden in one sharing system, and the number of shared images depends on the number of participants. Second, more participants with new secret images conveniently can be included in this sharing system, even after it has already been constructed. Furthermore, it can be applied directly to binary images and easily be extended to grayscale images and color images.

The remainder of this paper is organized as follows. Section 2 contains the preliminaries of secret image sharing. Our proposed scheme is presented in Section 3. Section 4 shows the experimental results and compares the results with those of other schemes. Finally, our conclusions are presented in Section 5.

## 2 Preliminaries

In this section, first, we briefly introduce the concept of secret image sharing. Second, we list some necessary notations and facts about our scheme.

Consider a binary secret image S with a size of $H \times W$. Image $S$ can be represented by an integer matrix $S$, i.e., $S = [S_{ij}]_{H \times W}$, where $i = 1, 2, \cdots, H$; $j = 1, 2, \cdots, W$; and $S_{ij} \in \{0, 1\}$. For a grayscale image, each pixel is represented by one byte. We can extract every bit of the byte respectively, transforming the grayscale image into eight binary images. Then, it can be represented by an integer matrix, as mentioned above. The RGB color model can be used in a color image, and the RGB color model is an additive color model in which red, green and blue are added together in various ways to reproduce a broad array of colors. After pre-conditioning, a color image first can be changed into three grayscale images and then into 24 binary images. In other words, eventually, three different types of secret images could be expressed in the same representation, which is binary image. Since the proposed scheme is focused on processing a binary image, it can be extended easily to process a grayscale image or a color image.

Assume that $A$ is the secret image that we want to hide and that $R$ is a random matrix that has the same size as $A$. Compute $B = A \oplus R$. It is obvious that $B$ is a random-like matrix and that nothing about $A$ could be revealed from $B$.

The definition of a secret image sharing scheme is shown as below.

Definition: In a ($t$, $n$) secret image sharing scheme, a secret image $S$ is transformed into $n$ shares, i.e., $S_1, S_2 \ldots, S_n$, and the following conditions must be satisfied:

Condition 1: The secret $S$ is recoverable from any $t$ shares.

Condition 2: Knowledge of $t$-1 or fewer shares does not provide any information about $S$.

The first condition is called precision, and the second condition is called security.

## 3 Proposed Scheme

In the proposed secret image sharing mechanism, assume that an image dealer $D$ holds the cover image $C$, which has a size of $H \times W$ pixels, where $H$ and $W$ stand for the height and width of the cover image, respectively, both are positive integers., and there are $N$ ($2 \leqslant N \leqslant 2^W$-1) secret images to be shared and $S_i$($i$ = 1, 2, …, $N$). $N$ participants $P_j$ ($j$ = 1, 2, …, $N$) are involved to share the secret images. The dealer is in charge of generating a set of shadow images $C_q'$ ($q$ = 1, 2, …, $N$) from the secret images for all of the involved participants. In the proposed method, each of the participants carries one secret image. Next, we will use the matrix transformation method based on the XOR operation to complete the secret sharing and retrieval procedures.

Subsection 3.1 provides a detailed description of the secret image sharing procedure, and Subsection 3.2 presents the the secret image retrieval procedure. A brief example of the proposed scheme is discussed in Subsection 3.3.

### 3.1 Secret Image Sharing Procedure

Assume that the grayscale cover image $C$ and all the secret image $S_i$ have $H \times W$ pixels and that all secret images are binary images. The steps presented below provide a detailed description of the proposed secret image sharing procedure.

Step 1: Generate $N$ copies of $C$, each of which can be used to initialize the shadow image $C_q'$ ($q$=1,2, …, $N$).

Step 2: Select the third to the last bit of each pixel from the first row of $C_q'$, which forms a binary sequence $B_q$. (Note that we choose the third to the last bit here because the last bit and the the second to the last bit will be occupied, and changing the last several bits of a pixel produces less damage to an image.) Translate every decimal number $(q)_{10}$ ($q$ = 1, 2, …, $N$) into its binary format $(q)_2$, and then use $(q)_2$ to replace each $B_q$ in each shadow image $C_q'$ as a sequence tag $T_q$ to present the sequence number of $C_q'$. (A certain sequence of the shadow images is required when retrieving the secret images, so we embed the sequence number in advance.)

Step 3: Generate $N$ random matrices $R_r$ ($r$ = 1, 2, …, $N$), each of which has $H \times W$ elements, and the value of each

element belongs to {0, 1}. Then, calculate $R_k'$ ($k$ = 2, 3,…, $N$) using the equation below:

$$R_k' = R_{k-1} \oplus R_k \ . \quad (1)$$

Step 4: Use $R_1$ to replace the last bit of each pixel of $C_1'$.

Step 5: Use $R_k'$ ( $k$ = 2, 3, …, $N$) to replace the last bit of each pixel of the shadow image $C_p'$ ( $p$ = 2, 3, …, $N$) according to its sequence number $B_q$, respectively.

Step 6: Calculate $S_i'$ ( $I$ = 1, 2, …, $N$) using the equation below:

$$S_i' = R_N \oplus S_i \ . \quad (2)$$

Step 7: Use $S_i'$ to replace the second to the last bit of each pixel of $C_q'$ in sequence.

Step8: Distribute $C_q'$ randomly to all of the participants.

In addition, this method can be applied to the condition in which a new participant who has a new secret image intends to enroll in the sharing procedure after the construction already has been completed. Assuming that the new participant is to be added into a completed sharing system that has $N$ participants, the most efficient way to do so is to locate the new participant, who has a new $R_1$, $S_1$, and $C_1'$, at the first place. An example is given in Subsection 3.3.3.

### 3.2 Secret Image Retrieving Procedure

In the proposed ($n$, $n$) secret image scheme, $N$ participants are provided with $N$ shadow images, and all of them must cooperate to retrieve all of the secret images. Notably, the definitions of all of the variables and characters used in this subsection remain the same as those in Subsection 3.1.

The steps presented below describe in detail the proposed procedure for retrieving the secret image.

Step 1: By searching $B_q$ of each shadow image among all of the participants, we can retrieve each shadow image's sequence number $T_q$. Thus, by transferring $T_q$ to its decimal number, the order of shadow images is determined as 1, 2, …, $N$, and each participant is named as $P_q$ according to her or his sequence number.

Step 2: Participant $P_1$ extracts the last bit of each pixel of $C_1'$ to get $R_1$.

Step 3: Participant $P_k$ ($k$ = 2, 3, …, $N$) extracts the last bit of each pixel of $C_k'$ to get $R_k'$.

Step 4: Based on Equation(1), we can obtain a new equation as shown below:

$$R_k = R_k' \oplus R_{k-1} \ . \quad (3)$$

We can extract $R_N$ using Equation(3).

Step 5: Extract the second to the last bit of each pixel of $C_q'$, and we can get $S_i'$.

Step 6: Based on Equation(2), we can obtain a new equation as shown below:

$$S_i = S_i' \oplus R_N \ . \quad (4)$$

Then, we can extract the secret image $S_i$ using Equation(4). Finally, all of the secret images are retrieved.

### 3.3 Example of Sharing and Retrieving

In this subsection, an example is given to describe more clearly the procedures for sharing a secret image, retrieving a secret image, and enrolling a new participant.

#### 3.3.1 Example of Sharing a Secret Image

Assume that $N$ is 3 and that $C$, $S_i$, and $R_r$ each have 4×4 pixels. $S_1$, $S_2$, $S_3$, $R_1$, $R_2$, and $R_3$ are listed below. Generate three copies of $C$, which are $C_1'$, $C_2'$, and $C_3'$.

$$S_1 = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \quad S_2 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

$$S_3 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}, \quad R_1 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

$$R_2 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \quad R_3 = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

Using Equation(1), we can calculate $R_2'$ and $R_3'$, as shown below:

$$R_2' = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix} \quad \text{and} \quad R_3' = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

Embed the sequence tags $T_1$, $T_2$, and $T_3$ into $C_1'$, $C_2'$, and $C_3'$, respectively, according to Step 3 of Subsection 3.1. Then, use $R_1$, $R_2'$, and $R_3'$ to replace the last bit of each pixel of $C_1'$, $C_2'$, and $C_3'$ in sequence, respectively. Using Equation(2), we can calculate $S_1'$, $S_2'$, and $S_3'$, as shown below:

$$S_1' = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}, \quad S_2' = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

$$S_3' = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}.$$

Use $S_1'$, $S_2'$, and $S_3'$ to replace the second to the last bit of each pixel of $C_1'$, $C_2'$, and $C_3'$ in sequence, respectively. Then, distribute $C_1'$, $C_2'$, and $C_3'$ randomly to all of the participants, and the procedure for sharing a secret image is completed.

3.3.2 Example of Retrieving a Secret Image

By searching $B_1$, $B_2$, and $B_3$ of each shadow image among all of the participants, we can retrieve sequence tags $T_1$, $T_2$, and $T_3$. Then, the corresponding participants are $P_1$, $P_2$, and $P_3$, according to their sequence numbers.

Participants $P_1$, $P_2$, and $P_3$ extract the last bit of each pixel of $C_1'$, $C_2'$, and $C_3'$, and we can obtain $R_1$, $R_2'$, and $R_3'$, as shown below:

$$R_1=\begin{pmatrix}0&0&0&1\\1&1&1&0\\0&1&0&0\\0&0&1&0\end{pmatrix},\quad R_2'=\begin{pmatrix}1&0&1&1\\1&0&0&0\\0&0&1&0\\1&0&1&1\end{pmatrix},$$

$$R_3'=\begin{pmatrix}1&1&0&1\\1&0&0&0\\0&1&0&0\\1&1&1&1\end{pmatrix}.$$

Using Equation(3), we can retrieve $R_2$ and $R_3$, as shown below:

$$R_2=\begin{pmatrix}1&0&1&0\\0&1&1&0\\0&1&1&0\\1&0&0&1\end{pmatrix}\quad\text{and}\quad R_3=\begin{pmatrix}0&1&1&1\\1&1&1&0\\0&0&1&0\\0&1&1&0\end{pmatrix}.$$

$$S_1=\begin{pmatrix}0&1&0&1\\1&1&1&0\\1&0&0&0\\1&0&0&1\end{pmatrix},\quad S_2=\begin{pmatrix}1&0&0&1\\0&0&1&0\\1&0&0&0\\0&0&1&0\end{pmatrix},$$

$$S_3=\begin{pmatrix}1&0&1&0\\0&0&1&0\\0&1&0&0\\1&0&1&1\end{pmatrix}.$$

Extract the second to the last bit of each pixel of $C_1'$, $C_2'$, and $C_3'$, and we can obtain $S_1'$, $S_2'$, and $S_3'$. Using Equation (4), we can retrieve secret images $S_1$, $S_2$, and $S_3$, as shown below, and the procedure for retrieving a secret image is completed.

3.3.3 Example of Enrolling a New Participant

When a new participant who has a new secret image $S_1$ intends to enroll after the procedure for sharing a secret image has been completed, as stated above, he or she should be added at the first place, and 1 should be added to all of the original subscripts of each character in order to fulfill a procedure for sharing a secret image. An example is given below.

Now, $N$ becomes 4, and we generate a new $R_1$ and a new $C_1$ according to the rules of the procedure for sharing a secret image. $R_1$ and $S_1$ can be obtained, as shown below:

$$R_1=\begin{pmatrix}1&1&1&1\\0&1&0&1\\1&0&1&0\\0&1&0&0\end{pmatrix}\quad\text{and}\quad S_1=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&1\\0&1&0&0\end{pmatrix}.$$

$P_2$ can reveal $R_2$ by selecting the last bit of each pixel of $C_2'$, and all of the original participants, i.e., $P_2$, $P_3$, and $P_4$, must cooperate to retrieve $R_4$. An example of this is presented in Subsection 3.3.2. Then, calculate $S_1' = R_4 \oplus S_1$ and $R_2' = R_1 \oplus R_2$. Thus, $R_2$, $R_4$, $S_1'$, and $R_2'$ are obtained, as shown below:

$$R_2=\begin{pmatrix}0&0&0&1\\1&1&1&0\\0&1&0&0\\0&0&1&0\end{pmatrix},\quad R_4=\begin{pmatrix}0&1&1&1\\1&1&1&0\\0&0&1&0\\0&1&1&0\end{pmatrix},$$

$$S_1'=\begin{pmatrix}1&1&1&1\\1&0&1&0\\0&0&0&1\\0&0&1&0\end{pmatrix},\quad R_2'=\begin{pmatrix}1&1&1&0\\1&0&1&1\\1&1&1&0\\0&1&1&0\end{pmatrix}.$$

Use $R_2'$ to replace the last bit of each pixel of $C_2'$; use $R_1$ to replace the last bit of each pixel of $C_1'$; and use $S_1'$ to replace the second last bit of each pixel of $C_1'$.

In this way, the new participant who has a new secret image can be added successfully to the sharing system. The procedure for retrieving the secret image remains the same as stated in Subsection 3.2.

## 4 Experimental Results and Comparison

In this section, we show the experimental results that demonstrate the performance of our proposed scheme. Also, we provide a comparison of our proposed scheme and the previous scheme.

### 4.1 Experimental Results

The experiments were conducted on an Intel Core2 Duo T6600 computer at 2.2 GHz, and implemented in C using visual c++ 6.0. It was implemented in the case of a (4, 4) secret image sharing scheme.

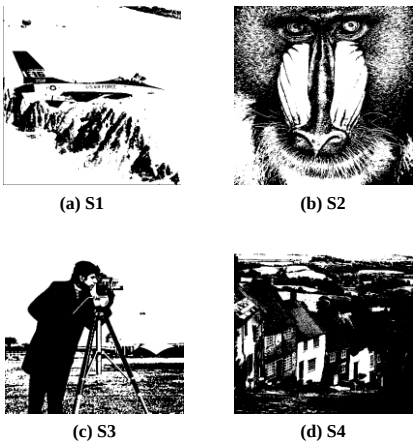


Figure 1: Binary secret images

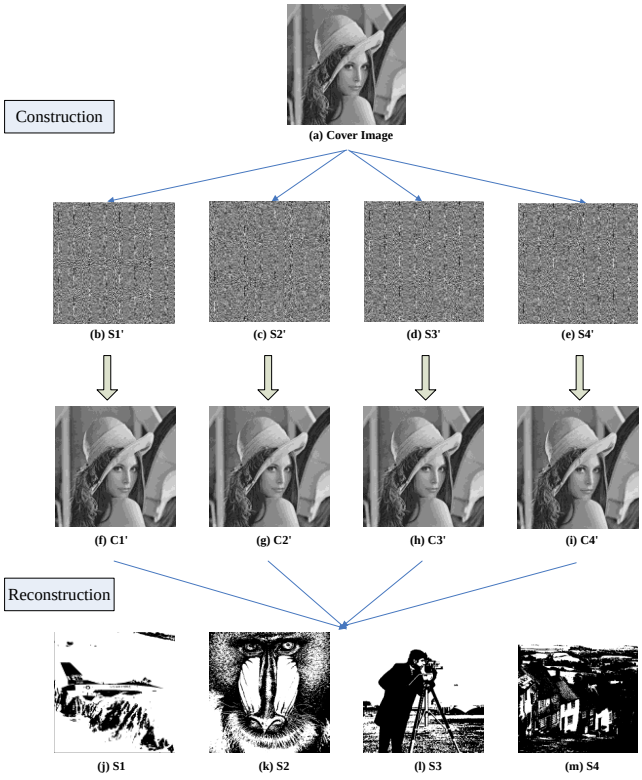


Figure 2: Overview of construction and reconstruction

Figures 1(a) - (d) are binary secret images, $S_1$, $S_2$, $S_3$, and $S_4$, respectively, with sizes of 512 x 512 pixels. Figure 2 shows the images that were obtained during the procedures for sharing and retrieving secret images in the experiment. Figure 2(a) is the grayscale cover image "Lena.jpg", with a size 512 x 512 pixels. Figure 2(b) - (e) are meaningless shadow images that were computed from the secret images. Figure 2(f) - (i) are meaningful shadow images, each of which includes an original meaningless shadow image. In terms of visual perception, the four shadow images can successfully camouflage shadows from attackers. The *PSNR* values of the shadow images are listed in Table 1. *PSNR* stands for peak signal to noise ratio and it is a important criteria to evaluate the quality of pictures. The definition is listed in Equation(5) and (6).

Table 1. *PSNR* values of shadow images

| Shadow images | *PSNR*(dB) |
|---|---|
| C1' | 44.18 |
| C2' | 44.13 |
| C3' | 44.17 |
| C4' | 44.16 |
| Average | 44.16 |

Table 2. Running times of procedures for sharing and retrieving images

| No. | Sharing (s) | Retrieving (s) |
|---|---|---|
| 1 | 0.320 | 0.065 |
| 2 | 0.342 | 0.083 |
| 3 | 0.381 | 0.114 |
| 4 | 0.390 | 0.085 |
| 5 | 0.330 | 0.117 |
| 6 | 0.381 | 0.083 |
| Average | 0.357 | 0.091 |

*PSNR* is an objective criterion to evaluate the visual quality of an image. The definition of *PSNR* is:

$$PSNR = 10\log_{10}\left(\frac{MAX_I^2}{MSE}\right). \qquad (5)$$

$MAX_I$ is the maximum possible value of the pixels of the image. In this paper, since we use eight bits to represent every pixel, $MAX_I$ here is 255. Mean squared error (*MSE*) is defined by Equation(6). I' is the noisy approximation of a noise-free m×n image I.

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left[I(i,j) - I'(i,j)\right]^2. \qquad (6)$$

Basically, the larger the value of *PSNR* is, the better the quality of the image is. From Table 1, we can see that the average value of *PSNR* for the shadow images was 44.16, which indicates very good quality of the image.

Figures 2 (j) - (m) show the reconstructed secret images. They are exactly the same as the original secret images, which proved that the scheme was effective. The average running time of sharing and retrieving images were 0.357 s and 0.091 s, respectively, which proved the scheme had low computational complexity. The specific running times are listed in Table 2. However, since a part of the cover image is used to hide the secret, the original cover image cannot be recovered losslessly.

### 4.2 Comparison

To clearly describe the characteristics of our scheme, we compared our scheme with two previously proposed schemes, one of which was presented by Chang, Lin, and Chan[6], also used cover images to hide secret image. Another one was presented by Dong and Ku[7], which also used boolean operations in the sharing and retrieving procedure. The comparison is based on four criterion, i.e., security, precision, capacity, and visual quality.

Security: Our scheme, Dong et al.'s and Chang et al.'s scheme all satisfied the security condition and can share secret images successfully. However, our scheme and Dong et al.'s used the (*n*, *n*) scheme, Chang et al.[6] used the (*t*, *n*) scheme.

Precision: Our scheme, Dong et al.'s and Chang et al.'s scheme all retrieved the secret image precisely.

Capacity: To some extent, our scheme and Chang et al.'s scheme have the same capacity. For example, for a $512\times512$ grayscale image in both schemes, the image has $512\times512$ bytes, and $512\times512$ bits of it can be used to hide secrets. As for Dong et al.'s scheme, it has a larger capacity when *n* is small because they don't use cover images, but when *n* is large, the capacity of our scheme is much larger because of the expansibility.

Visual Quality: The average *PSNR* value of our shadow images was 44.16 while the value for Chang et al.'s scheme was 40.37, which means that the visual quality of our scheme was much better than that of Chang et al's. Although we embed *n* secret sharings into *n* shares, the *PSNR* value of our scheme is still high, that is because we make use of every share legitimately so that information stored in the share does not overlap. As for Dong et al.'s scheme, they don't use cover images, so PSNR is not applicable for it.

## 5 Conclusions

In the development of our scheme, we used the matrix transformation method based on XOR operation to design a procedure for sharing a secret image, and it proved to be lossless and secure, it had low computational complexity, and no pixel expansion occurred from our experiments. In addition, this innovative method allows more than one secret image to be shared, and the images were successfully camouflaged in shadow images. The extensibility of the novel sharing scheme is of great importance to the contemporary information society, which has a large demand for information storage in sharing secret images.

## Acknowledgments

This work was supported by the National Nature Science Foundation of China under Grant No. 61272374.

## References

[1] G. R. Blakley, "Safeguarding cryptographic keys," in *Proceedings of AFIPS National Computer Conference*, vol.48, pp. 313-317, 1979.

[2] C. C. Chang and R. J. Hwang. "Sharing secret images using shadow codebooks," *Information Sciences*, vol. 111, no. 1, pp. 335-345, 1998.

[3] C. C. Chang, C. Y. Lin, and C. S. Tseng, "Secret image hiding and sharing based on the (t, n)-threshold," *Fundamenta Informaticae*, vol. 76, no. 4, pp. 399-411, 2007.

[4] 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," *Information Sciences*, vol. 178, no. 11, pp. 2433-2447, 2008.

[5] C. C. Chang, Y. P. Hsieh, and C. H. Lin, "Sharing secrets in stego images with authentication," *Pattern Recognition*, vol. 41, no. 10, pp. 3130-3137, 2008.

[6] C. C. Chang, P. Y. Lin, and C. S. Chan, "Secret image sharing with reversible steganography," *Computational Intelligence and Natural Computing*, pp. 253-256, 2009.

[7] L. Dong and M. Ku, "Novel (n, n) secret image sharing scheme based on addition," in *The Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, pp.583-586, 2010.

[8] C. C. Lin and W. H. Tsai, "Secret image sharing with steganography and authentication," *The Journal of Systems and Software*, vol. 73, no. 3, pp. 405-414, 2004.

[9] M. Naor and A. Shamir, "Visual cryptography," *Advances in Cryptology: Eurocrypt '94*, pp. 1-12, Spring-Verlag, Berlin, 1995.

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

[11] H. M. Sun, and S. P. Shieh, "Construction of dynamic threshold schemes," *Electronics Letters*, vol. 30, no. 24, pp. 2023-2024, 1994.

[12] C. C. Thien and J. C. Lin, "Secret image sharing," *Computer & Graphics*, vol. 26, no. 1, pp. 765-770, 2002.

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

[14] P. Tuyls, H. D. L. Hollmann, J. H. van Lint, and L. Tolhuizen, "Xor-based visual cryptography Schemes," *Designs Codes and Cryptography*, vol. 37, pp. 169-186, 2005.

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

[16] Y. S. Wu, C. C. Thien, and J. C. Lin, "Sharing and hiding secret images with size constraint," *Pattern Recognition*, vol. 37, no. 7, pp. 1377-1385, 2004.

[17] R. Zhao, J. J. Zhao, F. Dai, and F. Q. Zhao, "A new image secret sharing scheme to identify cheaters," *Computer Standards & Interfaces*, vol. 31 no. 1, pp. 252-257, 2009.

**Zhi-Hui Wang** received the BS degree in software engineering in 2004 from the North Eastern University, Shenyang, China. She received her MS degree in software engineering in 2007 and the PhD degree in software and theory of computer in 2010, both from the Dalian University of Technology, Dalian, China. Since November 2011, she has been a visiting scholar of University of Washington. Her current research interests include information hiding and image compression.

**Haibo Jin** received his B.E. degree in software engineering from Dalian University of Technology in 2013. He is going to finish his M.S. degree in computer science from University of Helsinki in the next two years. His current research interests include algorithms and machine learning.

**Xuebo Wang** received B.E.degree in Software Engineering (Intensive Japanese) from Dalian University of Technology in 2013. Now he is studying master science program of Management and Economics of Innovation at Chalmers University of Technology in Sweden.

**Chin-Chen Chang** received his Ph.D. degree in computer engineering from National Chiao Tung University. His first degree is Bachelor of Science in Applied Mathematics and master degree is Master of Science in computer and decision sciences. Both were awarded in National Tsing Hua University. Dr. Chang served in National Chung Cheng University from 1989 to 2005. His title is Chair Professor in Department of Information Engineering and Computer Science, Feng Chia University, from Feb. 2005. He is a Fellow of IEEE and a Fellow of IEE, UK. His research interests include database design, computer cryptography, image compression and data structures.