Role-Balance Based Multi-Secret Images Sharing using Boolean Operations

Chi-Shiang Chan[1], Yung-Chen Chou[2], Yi-Hui Chen[1], and Yuan-Yu Tsai[1]*
[1]Department of Applied Informatics and Multimedia,
Asia University,
[2]Department of Computer Science and Information Engineering,
Asia University,

Wufeng, Taichung 41354, Taiwan, R. O. C.
[e-mail: {CSChan, yungchen, chenyh, yytsai}@asia.edu.tw]
*Corresponding author: Yuan-Yu Tsai

Received December 8, 2013; revised March 21, 2014; revised April 21, 2014; accepted April 24, 2014; published May 29, 2014

Abstract

In 2011, Chen and Wu proposed their method of sharing *n* secret images to *n*+1 shadow images through the concept of a Boolean-based Visual Secret Sharing (VSS) method. However, the shadow images produced by this method are not equally important. If the participant who owns an important shadow image does not want to cooperate with other participants, most secret images can not be reconstructed. In the proposed method, the relationship between the shadows images and secret images are designed in a circular way mostly. Each shadow image only relates to two secret images. This means that if one participant refuses to cooperate with other participants, there are only two secret images which can not be reconstructed. Moreover, our proposed method only needs to produce *n* shadow images and *n* secret images can be shared to them.

Keywords: Boolean-based VSS, Multi-secret image sharing, Visual secret sharing

This work was supported by Asia University, Taiwan under Grant No. 102-ASIA-43 and the National Science Council of Taiwan under Grant No. NSC 101-2221-E-468-026. The authors also gratefully acknowledge the helpful comments and suggestions of the revewers, which have improved the presentation.

http://dx.doi.org/10.3837/tiis.2014.05.016

1. Introduction

Digital secret data are transferred across the Internet every day, and it is important to protect this secret data from being accessed by unauthorized users. The simplest way to achieve this goal is to encrypt the secret data with a secret key. However, if the secret key is lost or stolen from a careless key holder, an unauthorized user who obtains the secret key can freely access the secret data. In order to prevent this situation Shamir [10] proposed the (t, n) threshold scheme that divides a secret key into n key shadows. Each participant owns a key shadow and any t of n authorized participants can reconstruct the secret key through their key shadows.

Following this development many applications have been proposed using the (t, n) threshold scheme [3, 7, 8, 9, 12, 15, 16, 18]. In 1995 Naor and Shamir [9] applied a (t, n) threshold scheme to design a secret image sharing technique known as Visual Secret Sharing (VSS). Through VSS a secret image is shared to n shadow images and the shadow images are delivered to authorized participants. Those shadow images appear to be random images. When t shadow images are stacked, the secret image is revealed to visual perception without computation.

Several multiple-secret sharing schemes have been proposed [2, 11, 13, 14] to achieve the goal of sharing more secret images via the VSS technique. For example, Wu and Chen's method [13] shared two secret images to two shadow images. The first secret image can be revealed by stacking two shadow images. The second secret image can be revealed by stacking two shadow images where one of the two shadow images needs to be rotated 90° counter-clockwise. The following researches [2, 11, 14] has extended Wu and Chen's idea to multi-secret image sharing.

However, the VSS technique is applied to binary images and the reconstructed secret image comes from stacking two shadow images manually. This causes three problems when using the concept of the VSS technique to develop the schemes. The first problem is one of alignments. Two shadow images have to be aligned in exactly the right position otherwise the secret image can not be revealed; this is more appropriately achieved by computers rather than manually. The second problem is pixel expansion. To perform the VSS technique the pixels need to be expanded. Therefore, the size of the shadow image becomes larger than that of the secret image. The third problem is contrast. Because of the stacking property, the constructed secret image usually has low contrast. This means the image quality of the constructed secret image is very low.

Since there are problems in the traditional VSS technique, some improvement methods [1, 4, 6, 17] derived from the traditional VSS technique are developed. On of them is Boolean-based VSS [4, 17]. In fact, the stacking operator in the traditional VSS technique can be treated as an AND operator. On the other hand, the stacking operator in Boolean-based VSS is usually replaced with an Exclusive-OR (XOR) operator. Owing to the usage of an XOR operator, the secret images can be in the form of binary, gray-level, or color images. Similarly, the produced shadow images can also be in the form of binary, gray-level, or color images without expanding pixels.

For example, Wang et al. [17] proposed a Boolean-based VSS method by sharing a secret image to n shadow images. More precisely, Wang et al.'s method first generates n-1 random matrices, and the n shadow images are subsequently produced by performing an XOR operator on n-1 random matrices and the secret image. In order to share more secret images, Chen and

Wu [4] developed their method by modifying Wang et al.'s method. To begin with, a random matrix is produced as the first shadow image. Then, *n* secret images are subsequently encoded into the other *n* shadow images. Finally, Chen and Wu's method shared *n* secret images to *n*+1 shadow images.

There are some drawbacks in Chen and Wu's method. The most important one is that not all shadow images are equally important. This means that if the participant with the important shadow image does not want to cooperate with other participants, all secret images can not be reconstructed. Although Guo et al.'s method [6] can achieve equally important shadow images totally, the computation complexity becomes larger in both sides of producing and stacking shares. Moreover, the size of the shares becomes larger than the original secret image.

In this paper the proposed method only needs to produce *n* shadow images and *n* secret images can be shared to them. Moreover, the relationship between the shadow image and secret image are modified in a circular way. Each shadow image only relates to two secret images. This means once one participant refuses to cooperate with other participants, only two secret images can not be reconstructed.

The rest of this paper is organized as follows: Chen and Wu's method is introduced in Section 2. In Section 3 we give detailed descriptions of the proposed method. Section 4 presents the experimental results. Finally, conclusions are drawn in Section 5.

2. Related Work

In this section, Chen and Wu's method [4] is reviewed. First of all, Chen and Wu assumed that all secret images were high entropy images, such as natural images photographed by a digital camera. Chen and Wu's sharing and the reconstructing phases are described under this assumption in Subsection 2.1. However, in the case of secret images with low entropy Chen and Wu proposed a modified version of their method; as described in Subsection 2.2.

2.1 Chen and Wu's Method

To begin with we define some variables for further use. Assume the variable *n* represents the number of secret images that we want to encode. The *i*-th secret image is denoted as G_i, where *i* is in the range from 0 to *n*-1. After performing the sharing phase, the *i*-th shadow image is represented as S_i, where *i* is in the range from 0 to *n*. Note that Chen and Wu's method shared *n* secret images to *n*+1 shadow images.

There are three steps in the sharing phase. The flow chart of Chen and Wu's method is shown in Fig. 1. In the first step, the sharing phase generates a random integer matrix as the first shadow image S_0. The size of the random integer matrix is the same as that of the secret image. The value of each element in the random integer matrix is in the range from 0 to 255. In the second step, the *i*-th temporary matrix B_i is produced according to Formula (1), where *i* is in the range from 1 to n-1.

$$B_i = G_i \oplus S_0, \tag{1}$$

where $\oplus$ stands for the XOR operator.

In the third step, the other shadow images are produced according to Formula (2):

$$S_i = \begin{cases} B_i & \text{if } i = 1, \\ B_i \oplus B_{i-1} & \text{if } i = 2 \text{ to } n\text{-}1, \\ G_0 \oplus B_{i-1} & \text{if } i = n. \end{cases} \tag{2}$$

Note that the first shadow image S_0 is a random integer matrix while the other shadow images are produced according to Formula (2). Finally, n+1 shadow images can be obtained in the sharing phase. From Step 3 in Fig. 1, the shadow image S_i ($2 \leqq i \leqq n$-1) is equal to $G_i \oplus G_{i-1}$. The reason is that the shadow image S_i comes from performing the XOR operator on B_i and B_{i-1} according to Formula (2). Since B_i and B_{i-1} come from $G_i \oplus S_0$ and $G_{i-1} \oplus S_0$, the shadow image S_i is equal to $B_i \oplus B_{i-1} = (G_i \oplus S_0) \oplus (G_{i-1} \oplus S_0) = G_i \oplus G_{i-1}$.

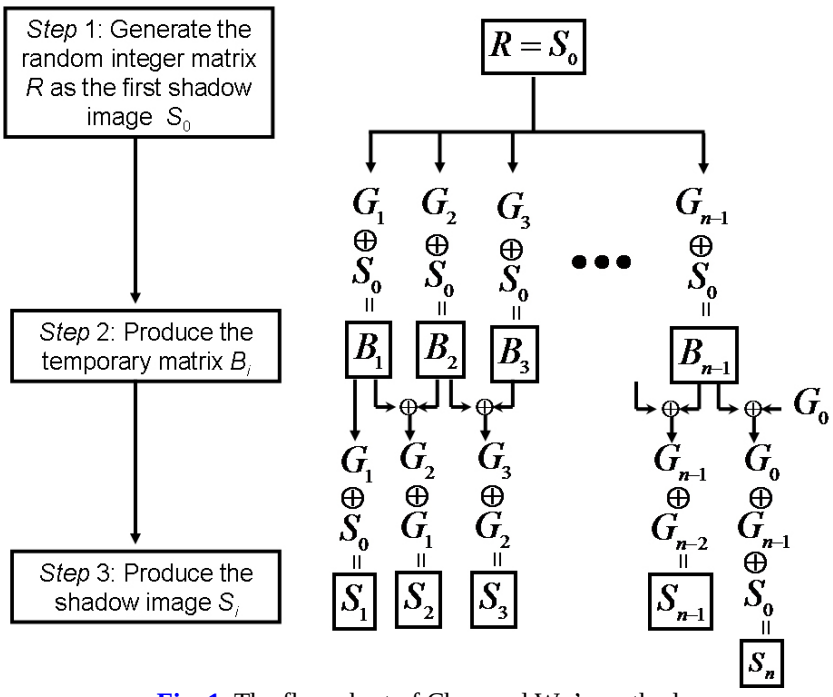


Fig. 1. The flow chart of Chen and Wu's method

In the reconstruction phase, the i-th secret image can be obtained from shadow images according to Formula (3):

$$G_i = \begin{cases} \Psi_{k=1}^{n} S_k & \text{if } i = 0, \\ \Psi_{k=0}^{i} S_k & \text{otherwise.} \end{cases} \tag{3}$$

where $\Psi_{k=1}^{i} S_k$ is $S_1 \oplus S_2 \oplus \ldots \oplus S_i$.

2.2 The Modified Version of Chen and Wu's Method

According to the descriptions in Subsection 2.1, the shadow image S_i is equal to $G_i \oplus G_{i-1}$ as shown in Fig. 1. It can be seen that the random matrix S_0 has been eliminated. Therefore, if two secret images, G_i and G_{i-1}, are not high entropy images, a partial secret image may be revealed.

To overcome this problem, Chen and Wu's method modified the method of producing the shadow image S_i as follows:

$$S_i = \begin{cases} G_i \oplus S_0 & \text{if } i = 1, \\ G_i \oplus G_{i-1} \oplus S_0 & \text{if } i = 2 \text{ to } n\text{-}1, \\ G_0 \oplus G_{i-1} \oplus S_0 & \text{if } i = n. \end{cases} \tag{4}$$

The flow chart of the modified version of Chen and Wu's method is shown in Fig. 2. The shadow image S_i ($2 \leqq i \leqq n$-1) of the modified version of Chen and Wu's method can be seen as performing the XOR operator on the random integer matrix S_0 and the shadow image S_i which comes from Step 3 in Fig. 1. Note that because S_0 is a random matrix, the shadow image S_i also becomes a random matrix after performing the XOR operator on S_i and S_0.

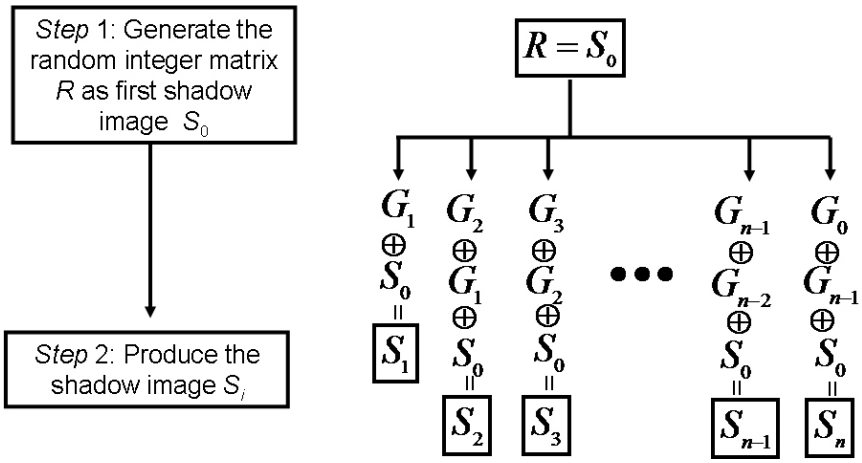


Fig. 2. The flow chart of the modified version of Chen and Wu's method

Since the method of producing shadow image S_i has been modified, the reconstructing formula, Formula (3), should also be modified simultaneously as follow:

$$G_i = \begin{cases} \Psi^{n}_{k=(n+1) \bmod 2} S_k & \text{if } i = 0, \\ \Psi^{i}_{k=(i+1) \bmod 2} S_k & \text{otherwise.} \end{cases} \tag{5}$$

Briefly, if the value of i is odd (odd number state), the secret image G_i is reconstructed from $S_0 \oplus S_1 \oplus \ldots \oplus S_i$. On the other hand, if the value of i is even (even number state), the secret image G_i is reconstructed from $S_1 \oplus S_2 \oplus \ldots \oplus S_i$.

3. The Proposed Method

In this section, we first introduce the drawbacks of Chen and Wu's Method in Subsection 3.1. Then, the sharing and reconstruction phases of the proposed method are described in Subsection 3.2.

3.1 The Drawback of Chen and Wu's Method

The first drawback of Chen and Wu's method is that not all shadow images are equally important. From Formula (3) it can be seen that the role of the shadow image S_i is more

important than the other shadow image S_j, where j is larger than i. The relationship between secret images and shadow images is shown in Fig. 3. In Fig. 3, G_1 can be reconstructed through S_0 and S_1, and G_2 can be reconstructed through S_0, S_1 and S_2, and so on. From this it can be seen that if the shadow image S_i is not handed over, the secret image G_j ($j \geq i$) can not be reconstructed. For example, if the participant who owns the shadow image S_1 does not want to cooperate with other participants, none of the secret images can be reconstructed. Of course this kind of mechanism may be useful in some conditions. However, in the secret sharing mechanism, all shadow images should be as equally important as possible.

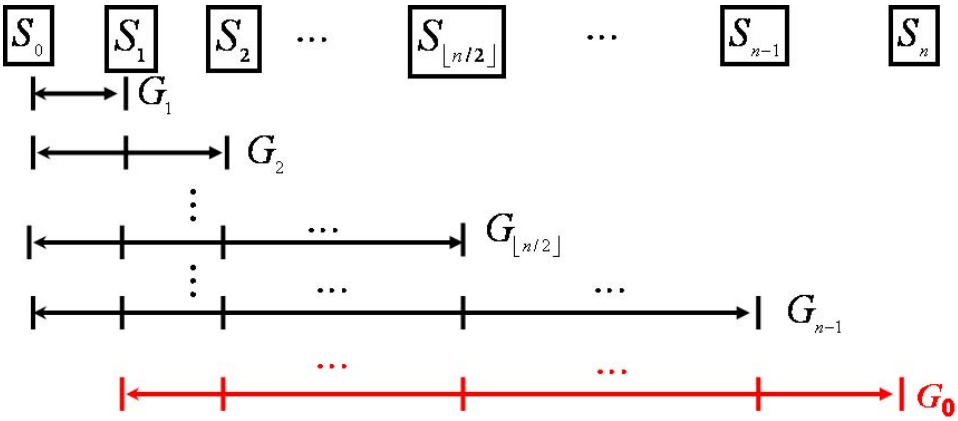


Fig. 3. The relationship between secret images and shadow images in Chen and Wu's method

The second drawback is that the shadow image S_i is equal to $G_i \oplus G_{i-1}$. If two secret images G_i and G_{i-1} are not high entropy images, the partial secret images may be revealed. Although Chen and Wu have proposed a revised version, the reconstruction formula, Formula (5), of the revised version, this becomes a little complex. That is, the odd or even number state that the secret image belongs to should be checked before it is reconstructed. However, our proposed method does not need to perform this additional check.

The third drawback is related to the number of shared secret images. In Chen and Wu's method, n secret images are shared into n+1 shadow images. However, our proposed method only needs to produce n shadow images, and n secret images can be shared to them. Therefore, the proposed method can share more secret images under the same number of shadow images.

3.2 The Sharing and Reconstruction Phases

In this subsection, the sharing and reconstruction phases are introduced. We use the same definitions of variables as Chen and Wu's method to illustrate our proposed method. That is the variables G_i and S_i are used to represent the i-th secret image and the i-th shadow image, respectively.

In order to make all shadow images as equally important as possible, the relationship between secret images and shadow images is modified in a circular way in our proposed method; as shown in Fig. 4. Through Fig. 4, it can be seen that the secret image G_i is reconstructed from performing an XOR operator on shadow images S_{i-1} and S_i. Moreover, each shadow image is related to two secret images. Therefore, under this kind of topology, if the shadow image S_i is not handed over, only two secret images can not be reconstructed. Note that this kind of topology is the aim of the proposed method. The proposed method achieves all

parts in Fig. 4, except for the producing of G_0. A small modification is needed, and the details are of this described in the following paragraphs.

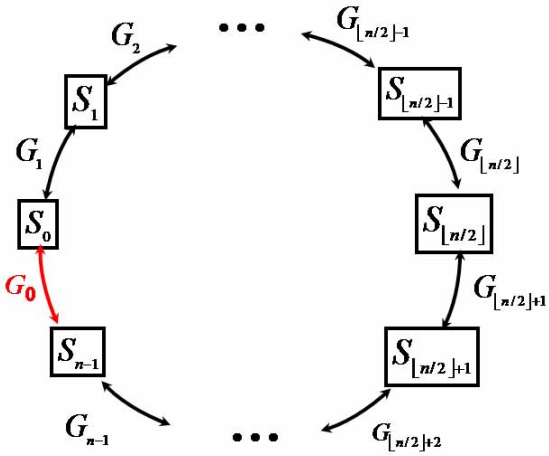


Fig. 4. The aim of the proposed method

We now start to introduce our proposed method. There are four steps in the sharing phase of the proposed method. The flow chart of the proposed method is shown in Fig. 5.

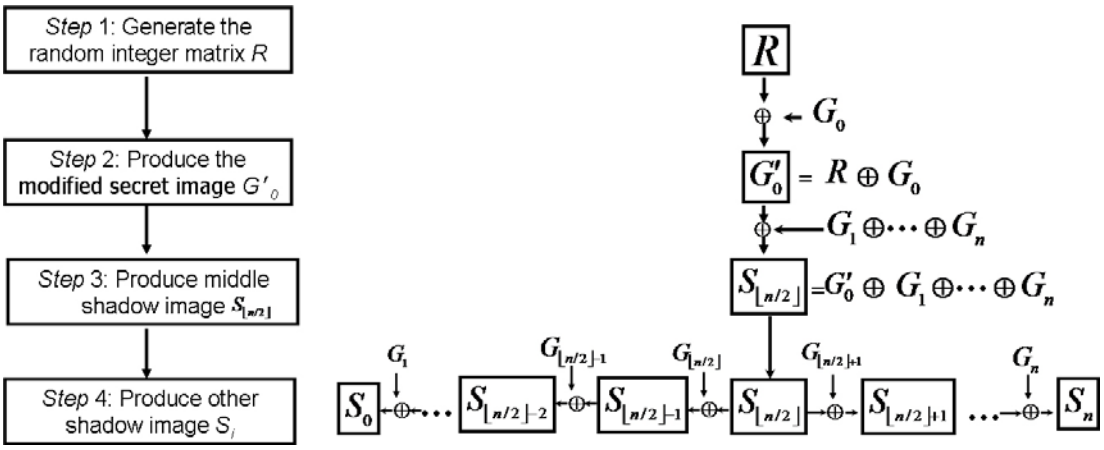


Fig. 5. The flow chart of the proposed method

In the first step, a random integer matrix is produced. The way to generate the random integer matrix is shown in Fig. 6. More precisely, the proposed method takes the pixel at the center position of the first secret image as a seed to generate eight random integer numbers. These eight pixels of the first secret image are extracted by treating eight random integer numbers as position indicators. The eight pixels are concatenated as a 64-bit key (a seed of random number generator). This key is fed into the random number generator, called ''Linear Feedback Shift Register,'' to generate a sequence of bit stream. Assume the produced bit stream is the same as the result shown in the top-right corner of Fig. 6. The bit stream is then partitioned into segments with eight bits in each segment. For example, the first eight bits $(10111010)_2$ are treated as the first segment and the second eight bits $(10110101)_2$ are treated as the second segment and so on. The number of segments produced by the random number generator is equal to the number of pixels in the secret images. Since each segment contains

eight bits, its value is an integer value in the range from 0 to 255. The segments are filled into a matrix R sequentially as its elements. Finally, the random integer matrix R can be obtained.

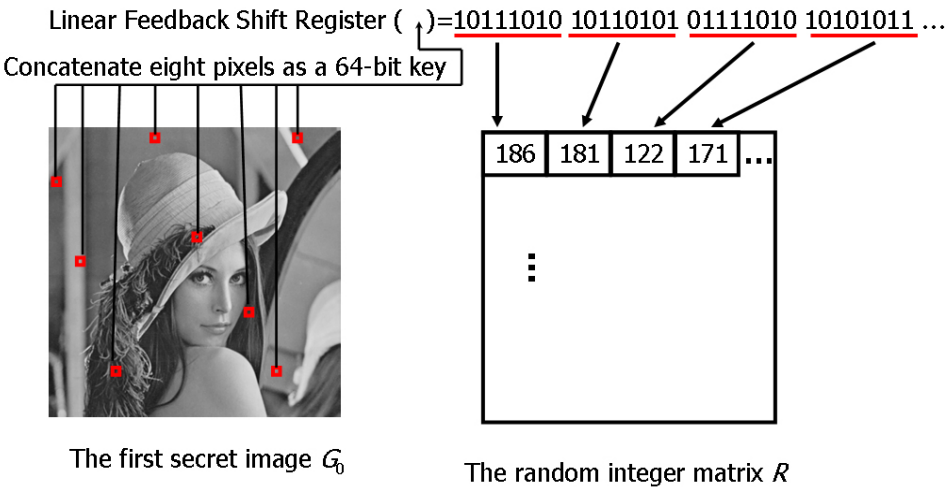


Fig. 6. The way to generate the random integer matrix R

In the second step, the modified secret image G'_0 is produced. Except for the nine pixels (the center pixel and the eight pixels), the XOR operator is performed on the elements of matrix R and the pixels of the first secret image G_0. The modified secret image G'_0 can then be obtained. The procedure for producing the modified secret image G'_0 is shown below:

$$G'_0 = R \oplus G_0 . \tag{6}$$

In the third step, the middle shadow image $S_{\lfloor n/2 \rfloor}$ is produced according to Formula (7).

$$S_{\lfloor n/2 \rfloor} = G'_0 \oplus \Psi_{k=1}^{n-1} G_k , \tag{7}$$

where variable n is the total number of secret images.

The other shadow images are produced in the fourth step. The shadow images can be divided into front and rear parts according to the middle shadow image $S_{\lfloor n/2 \rfloor}$. The process for producing the front part of the shadow images is not the same as the process for producing the rear part of the shadow images. The formula for producing those shadow images is shown in Formula (8).

$$S_i = \begin{cases} G_{i+1} \oplus S_{i+1} & \text{if } 0 \le i < \lfloor n/2 \rfloor, \\ G_i \oplus S_{i-1} & \text{if } \lfloor n/2 \rfloor < i \le n-1. \end{cases} \tag{8}$$

Note that the middle shadow image has been produced in Formula (7). Therefore, the variable i in Formula (8) does not contain value $\lfloor n/2 \rfloor$. Finally, n shadow images can be obtained.

Through Formula (6)-(8), it can be seen that each shadow image contains the modified secret image G'_0, and G'_0 has become a random-like image after performing the XOR operator on the secret image G_0 and the matrix R. According to the proof in [4], if a well-defined random number generator, such as a ‘‘Linear Feedback Shift Register’’[5], is adopted, the produced integers in the random integer matrix R will be random enough that each generated

share image S_i dose not contain any information. Therefore, all generated share image S_i will become distinct and random-like image.

Here, the mechanism of ‘‘Linear Feedback Shift Register’’ is introduced roughly. At first, a seed is put into a register as an initial state. Each time, bits in the register are right shifted to produce one random bit. Moreover, the state in the register is changed simultaneously. More precisely, the right-most bit in the register is right shifted out as a produced random bit. For the state in the register, because the bits in the register are right shifted and the left-most bit becomes empty, the left-most bit should be reassigned to a new bit value. The new bit value comes from performing XOR on some bits in the predetermined positions in the register (referring to the polynomials of ‘‘Linear Feedback Shift Register’’). Then, the register with new state can be reached and it will be used to produce the next random bit next time.

We give a simple example to demonstrate our proposed method. Assume the variable n is equal to 5. That means there are five secret images, G_0, G_2, …, and G_4. In the first step, the first secret image G_0 is modified according to Formula (6) to obtain the modified secret image G'_0. The second step is to produce the middle shadow image. Because the variable n is equal to 5, the middle shadow image represents the $\lfloor n/2 \rfloor$-th shadow image, that is, the shadow image S_2. Therefore, the shadow image S_2 is equal to $G'_0 \oplus G_1 \oplus G_2 \oplus G_3 \oplus G_4$. The third step is to produce other shadow images. The shadow image S_1 is derived from $G_2 \oplus S_2$ according to Formula (8). Because S_2 contains G_2, if we perform $G_2 \oplus S_2$ to get S_1, the secret image G_2 in S_2 is eliminated. Therefore the shadow image S_1 becomes $G'_0 \oplus G_1 \oplus G_3 \oplus G_4$. Similarly, S_1 contains G_1, and if we perform $G_1 \oplus S_1$ to get S_0, the secret image G_1 in S_1 is eliminated. Therefore, the shadow image S_0 becomes $G'_0 \oplus G_3 \oplus G_4$. The shadow image S_3 and S_4 can also be derived according the induction described above. Finally, four shadow images S_0, S_1,…, and S_4 can be produced as shown in Fig. 7.

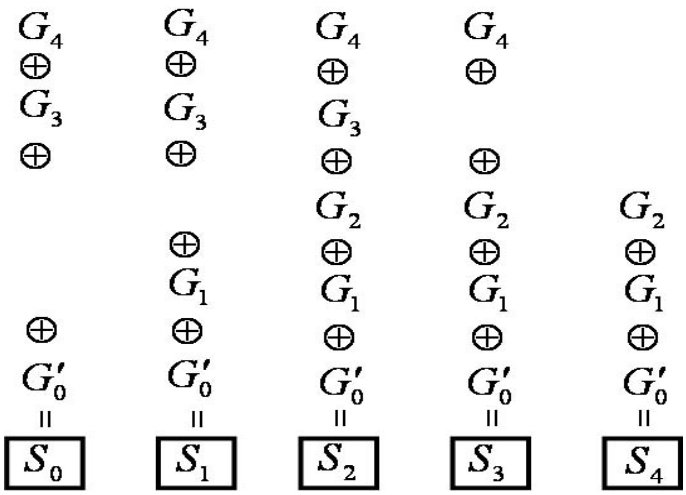


Fig. 7. An example of the proposed method

The methods of reconstructing the secret images in the reconstruction phase are all the same except for the modified secret image G'_0. The secret image and the modified secret image G'_0 are reconstructed according to Formula (9) and Formula (10), respectively.

$$G_i = S_{i-1} \oplus S_i \,, \tag{9}$$

where the value i in Formula (9) is in the range of 1 to n-1.

$$G_0' = S_0 \oplus S_{n-1} \oplus S_{\lfloor n/2 \rfloor}. \tag{10}$$

After obtaining G'_0 from Formula (10), the pixel at the center position of G'_0 is extracted and taken as a seed to generate eight random integer numbers. The eight pixels of G'_0 are extracted according to eight random integer numbers. The eight pixels are concatenated as a 64-bit key (a seed of a random number generator) to generate a random integer matrix R. Except for the nine pixels, the XOR operator is performed on the elements of matrix R and the pixels of G'_0 to reconstruced the secret image G_0 as shown below:

$$G_0 = G_0' \oplus R, \tag{11}$$

Finally, all secret images can be reconstructed according to the reconstruction phase of the proposed method.

There are two important points for the above reconstruction phase of the proposed method. The first one is that our aim is to reconstruct G_0 from S_0 and S_{n-1} recalling the descriptions in Fig. 4. However, in our proposed method, we still need a little help from an additional shadow image $S_{\lfloor n/2 \rfloor}$. It is a minor flaw in our proposed method. However, with this exception the proposed method achieves the aim of Fig. 4. The second point is how the i-th secret image G_i and modified secret image G'_0 can be reconstructed through Formula (9) and Formula (10), respectively. We prove them in **Theorem 1** and **Theorem 2**, respectively.

Theorem 1. The i-th secret image G_i can be reconstructed by $S_{i-1} \oplus S_i$.

Proof. According to Formula (8) where G_i orginates, we divide this problem into two cases. In the first case, if $0 \le i < \lfloor n/2 \rfloor$, then $S_i = G_{i+1} \oplus S_{i+1}$ through Formula (8). It can be shown that $G_{i+1} = S_i \oplus S_{i+1}$. We reassign the value i+1 to y. The statement becomes; if $1 \le y < \lfloor n/2 \rfloor + 1$, then $G_y = S_{y-1} \oplus S_y$. Through the first case, it can be shown that G_1, G_2, …, and $G_{\lfloor n/2 \rfloor}$ satisfy Formula (9). In the second case, if $\lfloor n/2 \rfloor < i \le n$-1, then $S_i = G_i \oplus S_{i-1}$ through Formula (8). It can be shown that $G_i = S_{i-1} \oplus S_i$. Through the second case, it can be shown that $G_{\lfloor n/2 \rfloor+1}$, $G_{\lfloor n/2 \rfloor+2}$, …, and G_{n-1} satisfy the Formula (9). Combining two cases, it can be proved that $G_i = S_{i-1} \oplus S_i$, when i is in the range from 1 to n-1.

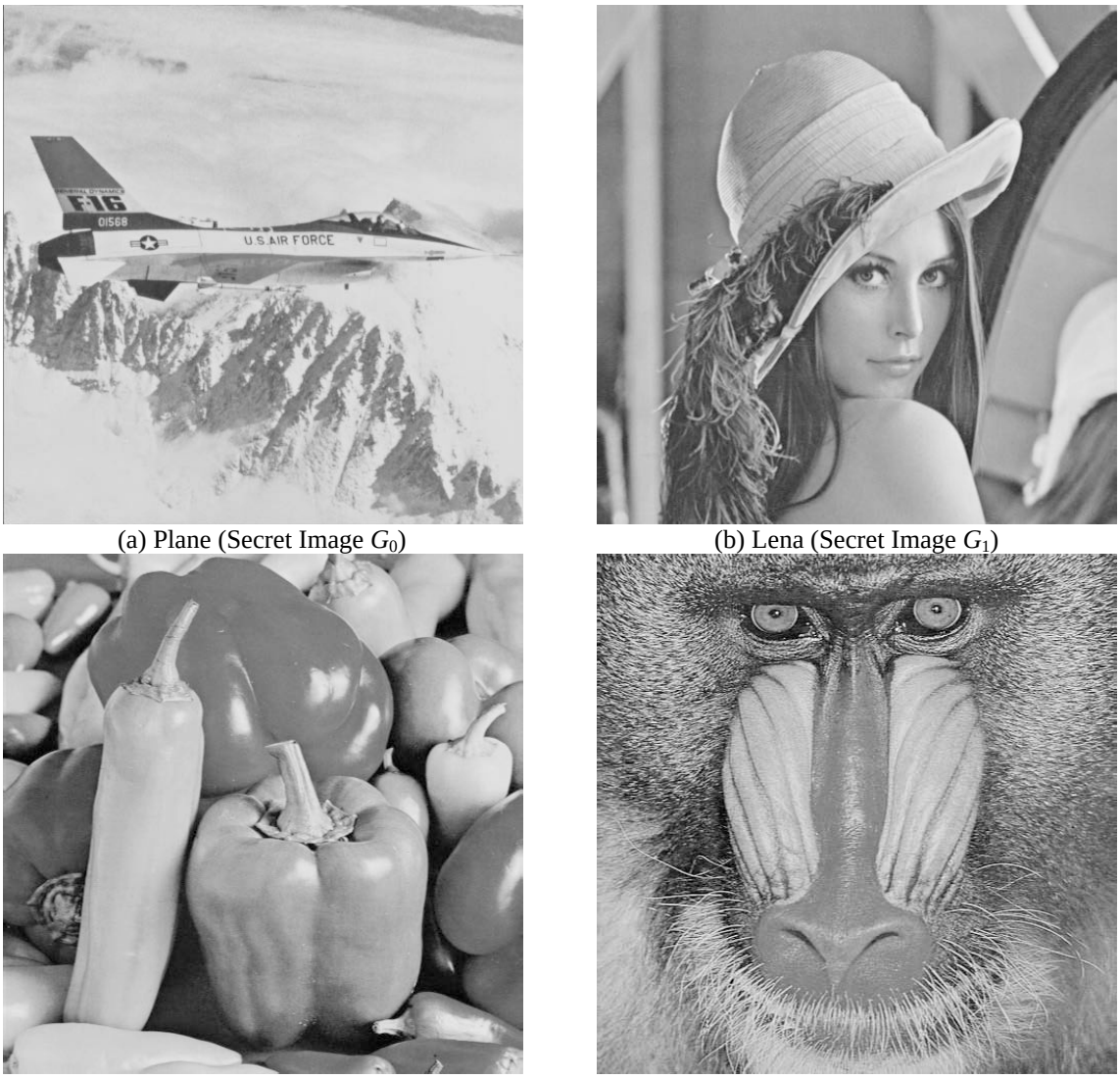
Theorem 2. The modified secret image G'_0 can be reconstructed by $S_0 \oplus S_{n-1} \oplus S_{\lfloor n/2 \rfloor}$.

Proof. Based on Formula (7), the shadow image $S_{\lfloor n/2 \rfloor}$ is equal to $G'_0 \oplus G_1 \oplus G_2 \oplus \ldots \oplus G_{n-1}$. Moreover, based on **Theorem 1**, the secret image G_i can be substituted by $S_{i-1} \oplus S_i$. This means the shadow image $S_{\lfloor n/2 \rfloor}$ is equal to $G'_0 \oplus G_1 \oplus G_2 \oplus \ldots \oplus G_{n-1} = G'_0 \oplus (S_0 \oplus S_1) \oplus (S_1 \oplus S_2) \oplus \ldots \oplus (S_{n-2} \oplus S_{n-1})$, that is, $S_{\lfloor n/2 \rfloor} = G'_0 \oplus S_0 \oplus S_{n-1}$. Finally, it can be proved that $G'_0 = S_0 \oplus S_{n-1} \oplus S_{\lfloor n/2 \rfloor}$.

4. Experimental Results

The experimental results are demonstrated in this section. Real images were used to perform the proposed method. Four grayscale images were selected as secret images, including Plane, Lena, Pepper, and Baboon as shown in Fig. 8. The size of each cover image was 512×512 pixels. They were used to represent the secret images G_0, G_1, G_2 and G_3. The four shadow images are shown in Fig. 9.

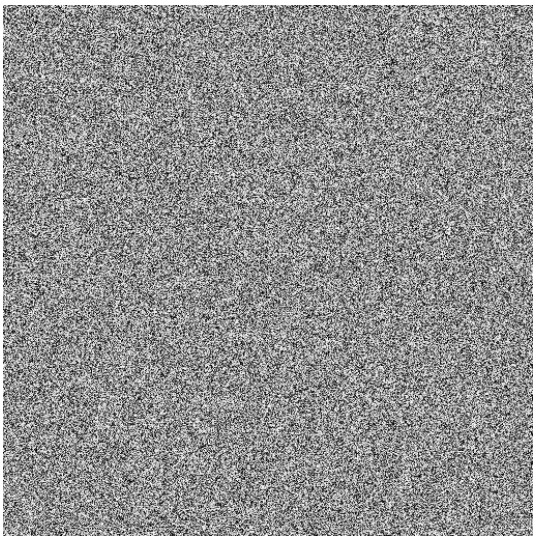
From Fig. 9, it can be seen that no partial secret information is revealed. All four shadow images are random-like images. The reason is that each shadow image contains the modified secret image G'_0, and G'_0 is a random-like image. Therefore, all shadow images become random-like images. This means we do not need to worry about whether the secret images are low entropy images or not. The reconstructed images, because they are exactly the same as the original secret images shown in Fig. 8, are not shown in this manuscript.



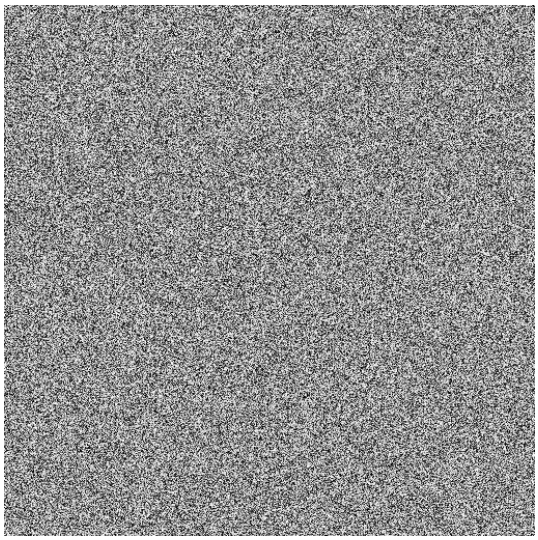
(a) Plane (Secret Image G_0) (b) Lena (Secret Image G_1)

(c) Pepper (Secret Image G_2) (d) Baboon (Secret Image G_3)

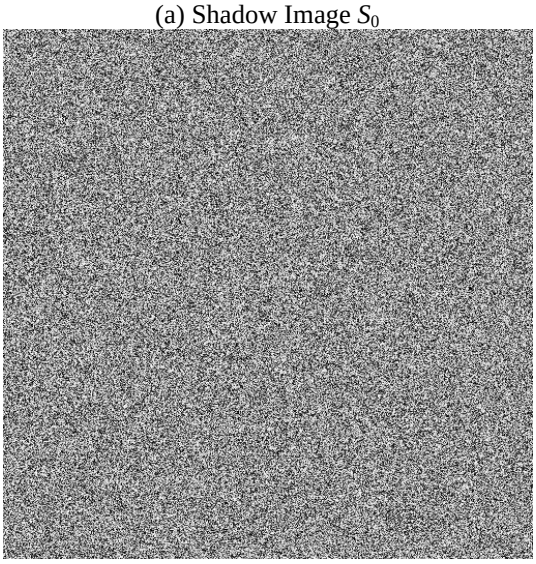
Fig. 8. The secret images



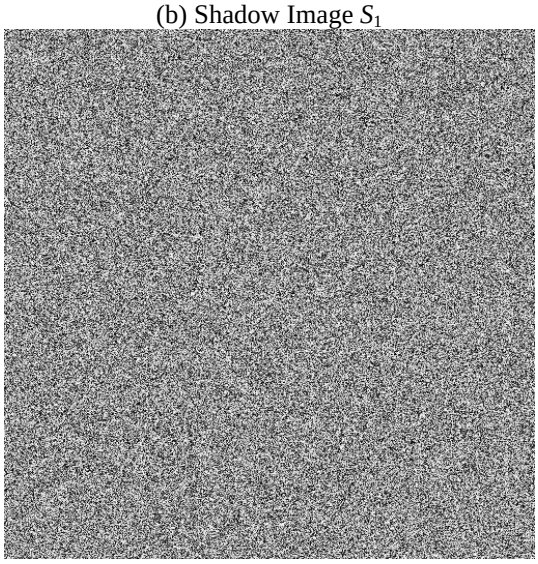
(a) Shadow Image S_0



(b) Shadow Image S_1



(c) Shadow Image S_3



(d) Shadow Image S_4

Fig. 9. The shadow images

The comparisons among different methods are in Table 1. Among those comparisons, "*Sharing Capacity*" defined by Chen and Wu [4] are shown as follows:

$$Sharing\ \ Capacity = \frac{\text{the number of secret images}}{\text{the number of the shadow images} \times \text{pixel expansion}}. \quad (12)$$

The larger the value of the *sharing capacity*, the better is the sharing method. In Chen and Wu's method [4], n secret images are shared into n+1 shadow images and their method dose not expand the pixels. Therefore, the *Sharing Capacity* of Chen and Wu's method [4] is $n/(n+1)$. Moreover, in Guo et al.'s method [6] each share value derived from one secret pixel is encoded by fifteen bits. Therefore, its "Pixel Expansion" is 15/8. As for Chen's method [1], the size of shadows related to the number of shadows. If the number of shadows is n, the size of shadows becomes 1/n. That is why we mark '*' in the "Pixel Expansion" field. Finally, the

method proposed here shares *n* secret images into *n* shadow images and does not need to expand pixels either. Therefore, the *sharing capacity* of the proposed method is *n*/*n*, that is, 1.

Table 1. Comparisons among different methods

	Wang et al.'s method[17]	**Chen and Wu's method[4]**	**Chen's method [1]**	**Guo et al.'s method [6]**	**The proposed method**
Lossless Secret Construction	**YES**	**YES**	**YES**	**YES**	**YES**
Pixel Expansion	**NO**	**NO**	**NO***	**YES**	**NO**
Operators	**Boolean**	**Boolean**	**Add, Multiply**	**Add, Multiply**	**Boolean**
Image Format	**Binary, Gray-Level, Color**	**Binary, Gray-Level, Color**	**Binary, Gray-Level, Color**	**Binary, Gray-Level, Color**	**Binary, Gray-Level, Color**
Sharing Capacity	$\frac{1}{n\times 1}$	$\frac{n}{(n+1)\times 1}$	$\frac{1}{(n)\times(1/n)}=1$	$\frac{n}{(n)\times(15/8)}=\frac{8}{15}$	$\frac{n}{(n)\times 1}=1$

In the following paragraphs we demonstrate the importance of the role of all shadow images in the related method and the proposed method. The values in Table 2 represent the total number of secret images that are affected by the corresponding shadow images. For example, in Chen and Wu's method, there are *n* secret images that are affected by the shadow image S_1. This means that if the participant who owns the shadow image S_1 does not want to cooperate with other participants, all *n* secret images can not be reconstructed. In Wang et al.'s method [17] and Wu's method [4], their values are marked as '*' because both two methods produce shares from only "one" secret image. Under this situation, this secret image is affected by all shares. Therefore, their values in Table 2 are all 1 with star symbol '*'. Moreover, the value of $S_{\lfloor n/2 \rfloor}$ for our proposed method in Table 2 is equal to 3. This is because the proposed method needed S_0, S_{n-1} and $S_{\lfloor n/2 \rfloor}$ to reconstruct the modified secret image G'_0, which means the modified secret image G'_0 is also affected by $S_{\lfloor n/2 \rfloor}$. Therefore, there are three secret images that are affected by the shadow image $S_{\lfloor n/2 \rfloor}$.

Another point is that the total number of shadow images that are used to share *n* secret images is *n*+1 in Chen and Wu's method. This number is *n* in Guo et al.'s method and the proposed method. Therefore, Guo et al.'s method and the proposed method do not produce shadow image S_n. That is why there is no value in shadow image S_n for Guo et al.'s method and the proposed method in Table 2. And, we mark 'X' at the corresponding positions in Table 2 to indicate this situation.

Just as we discussed in Subsection 3.1, all shadow images should be as equally important as possible in the aspect of secret sharing. Thus it is better when the values in Table 2 are as equal as possible. Through the values in Table 2 it can be seen that almost all values in the proposed method are equal to 2. Therefore, the shadow images produced by our proposed method are more equally important than those produced by other methods. Although Guo et al.'s method [6] achieves equally important shadow images totally, the method causes pixel expansion and the computation complexity is larger than the proposed method by referring Table 1.

Table 2. The number of secret images that are affected by the shadow images

	The shadow images									
	S_0	S_1	S_2	$\cdots$	$S_{\lfloor n/2 \rfloor -1}$	$S_{\lfloor n/2 \rfloor}$	$S_{\lfloor n/2 \rfloor +1}$	$\cdots$	S_{n-1}	S_n
Wang et al.'s method[17]	1^*	1^*	1^*	$\cdots$	1^*	1^*	1^*	$\cdots$	1^*	X
Chen and Wu's method[4]	n-1	n	n-1	$\cdots$	$\lfloor n/2 \rfloor -2$	$\lfloor n/2 \rfloor -1$	$\lfloor n/2 \rfloor$	$\cdots$	2	1
Chen's method [1]	1^*	1^*	1^*	$\cdots$	1^*	1^*	1^*	$\cdots$	1^*	X
Guo et al.'s method [6]	2	2	2	$\cdots$	2	2	2	$\cdots$	2	X
The proposed method	2	2	2	$\cdots$	2	3	2	$\cdots$	2	X

5. Conclusion

In this paper the drawbacks of Chen and Wu's method are addressed. The first drawback is that the produced shadow images are not equally important. To overcome this, the proposed method modifies Chen and Wu's approach so that the relationship between the shadows images and secret images are modified in a circular way. Each shadow image only relates to two secret images. Therefore, the shadow images produced by the proposed method are equally important. The second drawback of Chen and Wu's method is that if the secret images are low entropy images, the reconstruction phase should check whether the reconstructed secret image belongs to the odd or even number state. However, in the proposed method, the reconstruction phase is consistent no matter what number state the secret image belongs to. The third drawback is that the *Sharing Capacity* of Chen and Wu's method is n/(n+1). However, that of the proposed method is *n*/*n*, that is, 1. This means the proposed method can share more secret images compared to Chen and Wu's method under the same number of shadow images. Moreover, through the comparisons between our proposed method and other related methods in Table 1 and 2, it can be concluded that the proposed method is better than other related methods.

References

[1] W. K. Chen, "Image Sharing Method for Gray-level Images," *Journal of Systems and Software*, vol. 86, no. 2, pp. 581-585, 2013. Article (CrossRef Link)

[2] J. Chen, Y. S. Chen, H. C. Hsu, and H. W. Chen, "New Visual Cryptography System Based on Circular Shadow Image and Fixed Angle Segmentation," *Journal of Electronic Imaging*, vol. 14, no. 3, pp. 0330181 - 033018-5, 2005. Article (CrossRef Link)

[3] D. Catalano and R. Gennaro, "New Efficient and Secure Protocols for Verifiable Signature Sharing and Other Applications," *Journal of Computer and System Sciences*, vol. 61, no. 1, pp. 51-80, 2000. Article (CrossRef Link)

[4] T. H. Chen and C. S. Wu, "Efficient Multi-secret Image Sharing based on Boolean Operations," *Signal Processing*, vol. 91, pp. 90-97, 2011. Article (CrossRef Link)

[5] D. W. Clark and L. J. Weng, "Maximal and Near-Maximal Shift Register Sequences: Efficient Event Counters and Easy Discrete Logarithms," *IEEE Transactions on Computers*, vol. 43, no. 5,

pp. 560-568, 1994. Article (CrossRef Link)

[6] C. Guo, C. C. Chang, N. Ma, and C. Qin, "A Multi-threshold Secret Image Sharing Scheme Based on MSP," *Pattern Recognition Letters*, vol. 33, pp. 1594-1600, 2012. Article (CrossRef Link)

[7] C. C. Lin and W. H. Tsai, "Secret Image Sharing with Steganography and Authentication," *Journal of Systems and Software*, vol. 73, vol. 3, pp. 405-414, 2004. Article (CrossRef Link)

[8] J. Nam, M. Kim, J. Paik, and D. Won, "Security weaknesses in Harn-Lin and Dutta-Barua Protocols for Group Key Establishment," *KSII Transactions on Internet and Information Systems*, vol. 6, no. 2, pp. 751-765, 2012. Article (CrossRef Link)

[9] M. Naor and A. Shamir, "Visual Cryptography," *Lecture Notes in Computer Science*, vol. 950, pp. 1-12, 1994. Article (CrossRef Link)

[10] A. Shamir, "How to Share a Secret," *Communication of the ACM*, vol. 22, no. 11, pp. 612-613, 1979. Article (CrossRef Link)

[11] S. J. Shyu, S. Y. Huang, Y. K. Lee, and R. Z. Wang, "Sharing Multiple Secrets in Visual Cryptography," *Pattern Recognition*, vol. 40, no. 12, pp. 3633-3651, 2007. Article (CrossRef Link)

[12] C. C. Thien, and J. C. Lin, "Secret Image Sharing," *Computer & Graphics*, vol. 26, pp. 765-770, 2002. Article (CrossRef Link)

[13] C. C. Wu and L. H. Chen, "A Study on Visual Cryptography," *Master Thesis*, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, 1998.

H. C. Wu and C. C. Chang, "Sharing Visual Multi-secrets using Circle Shares," *Computer Standards & Interfaces*, vol. 134, no. 28, pp. 123-135, 2005. Article (CrossRef Link)

[14] C. H. Wang, and T. Hwang, "*(t,m)* Threshold and Generalized ID-based Conference Key Distribution System," *Applied Mathematics and Computation*, vol. 112, no. 2-3, pp. 181-191, 2000. Article (CrossRef Link)

[15] G. Wei, X. Yang, and J. Shao, "Efficient Certificateless Authenticated Asymmetric Group Key Agreement Protocol," *KSII Transactions on Internet and Information Systems*, vol. 6, no. 12, pp. 3352-3365, 2012. Article (CrossRef Link)

[16] D. Wang, L. Zhang N. Ma, and X. Li, "Two Secret Sharing Schemes Based on Boolean Operations," *Pattern Recognition*, vol. 40, no. 10, pp. 2776-2785, 2007. Article (CrossRef Link)

[17] W. J. Zhang, "Robust Multiparty Quantum Secret Key Sharing over Two Collective-noise Channels," *Physical A: Statistical Mechanics and its Applications*, vol. 361, no. 1, pp. 233-238, 2006. Article (CrossRef Link)

Chi-Shiang Chan was born in Taiwan in 1975. He received the B.S. degree in computer science in 1999 from the National Cheng-Chi University and the M.S. degree in computer science and information engineering in 2001 from the National Chung Cheng University. He received his Ph.D. degree in computer engineering in 2005 also from the National Chung Cheng University. From 2007 to 2010, he has worked as an assistant professor with the Department of Information Science and Applications, Asia University. He is currently an associate professor with the Department of Applied Informatics and Multimedia, Asia University. His research interests include image and signal processing, image compression, information hiding, and data engineering.

Yung-Chen Chou received the BS degree in Management Information Systems from National National Pingtung University of Science & Technology, Pingtung, Taiwan, in 1998, and the MS degree in Information Management from Chaoyang University of Technology, Taichung, Taiwan, in 2002. He received Ph.D degree in Computer Science and Information Engineering in 2008 from the National Chung Cheng University, Chiayi, Taiwan. Since February 2009, he has been an Assistant Professor of Asia University, Taichung, Taiwan. His current research interests include steganography, watermarking, and image processing.

Yi-Hui Chen was born in Taiwan in 1979. She received the B.S. and M.S. degrees in information management from Chaoyang University of Technology, in 2001 and 2004, respectively. Afterward, she got her Ph.D. degree in computer science and information engineering from the National Chung Cheng University, in 2009. From 2009 to 2010, she worked with Academia Sinica as a postdoctoral fellow. Later on, she served for IBM Taiwan Collaboratory Research Center as a research scientist. She is now an assistant professor with the Department of Applied Informatics and Multimedia, Asia University. Her research interests include image processing, watermarking, steganography, and XML techniques.

Yuan-Yu Tsai was born in Taichung, Taiwan, in 1978. He received the B.S. degree in Department of Computer Science and Information Engineering from National Central University, Taiwan, in 2000, and the Ph.D. degree in Institute of Computer Science from National Chung Hsing University, Taiwan, in 2006. He is currently an assistant professor at the Department of Applied Informatics and Multimedia, Asia University, Taiwan. His research interests include computer graphics and information hiding algorithms for three-dimensional models and images. He is a member of the ACM and the IEEE Computer Society.