Multimed Tools Appl (2016) 75:11577–11594
DOI 10.1007/s11042-015-2885-x

A multi-threshold secret image sharing scheme based on the generalized Chinese reminder theorem

Cheng Guo[1] · **Huan Zhang**[1] · **Qiongqiong Song**[1] · **Mingchu Li**[1]

Received: 28 October 2014 / Revised: 25 June 2015 / Accepted: 12 August 2015 /
Published online: 20 August 2015

Abstract In a multi-secret image sharing scheme, participants are able to share multiple secret images such the way that each secret image can be reconstructed according to the corresponding access structure. In this paper, employing Chan and Chang's multi-secret sharing, we propose a new multi-threshold secret image sharing scheme. In the secret image sharing process, based on the generalized CRT, secret values are produced according to the associated access structures. The shadow images can be generated by embedding the secret values into a cover image using the quantization operation. The new scheme allows a qualified subset of participants to retrieve the related secret image. Moreover, any monotone access structure can be realized with a deletion procedure. The experiments demonstrate that secret images can be recovered without distortion. Besides, the quality of the shadow images is satisfactory and the capacity of embedded secret values is acceptable especially under binary images.

Keywords Access structure · Multi-threshold secret sharing · Secret image sharing · Chinese remainder theorem

1 Introduction

A secret sharing (SS) scheme, aiming at sharing a secret among a group of participants, is a method that each participant owns a share of the secret, and only the authorized participants

✉ Cheng Guo
guo8016@gmail.com

Huan Zhang
zhanghuan0211@126.com

Qiongqiong Song
qiongq.song@gmail.com

Mingchu Li
li_minqchu@yahoo.com

[1] School of Software Technology, Dalian University of Technology, No. 8 Road, Jinzhou District, Dalian 116620, People's Republic of China

with sufficient shares can cooperate to reconstruct the secret. In 1979, Shamir [14] and Blakley [3] proposed the first (*t, n*) threshold secret sharing schemes independently, wherein a dealer divides a secret into *n* different secret shares, and distributes them to the involved participants. Any *t* out of *n* authorized participants can cooperatively recover the secret, while fewer than *t* participants cannot retrieve any information about it.

In 1995, based on the concept of the secret sharing, visual secret sharing (VSS) scheme was developed by Naor and Shamir [11]. Subsequently, more schemes (Wu and Sun.[17]; Kumar and Sharma [8]; Sasaki and Watanabe [13]; Yan et al.[18]) were proposed. Compared with a secret sharing scheme, the secret of a (*t, n*) threshold VSS scheme is a binary image which is encrypted into *n* shadows such that the secret image can be visually revealed by stacking *t* out of *n* shadows without computation. Nevertheless, in these schemes, the generated shadows are meaningless, which tend to attract attention to malicious attackers. In 2004, utilizing the steganography and authentication approach, Lin and Tsai [10] implemented a novel sharing scheme, in which the secret image is embedded into an ordinary-looking image (cover image) to generate meaningful shadow images. However, there exists distortion of the retrieved secret image, and their method causes size expansion of the secret image. In 2007, Yang et al. [19] improved the approach of Lin and Tsai [10] to a distortion-free scheme by using Galois Field GF (2^8). In addition, the scheme allows authorized participants to verify the validity of the shadow images. Unfortunately, the maximum secret capacity is limited to a quarter of the size of the cover image. In 2009, the modulus operator was employed by Lin et al. [9] such that the shadow images are meaningful with satisfactory quality and both the retrieved secret image and the reconstructed cover image are lossless. In 2013, Ulutas et al. [16] utilized Exploiting Modification Direction (EMD) and modulus operator to design an invertible secret image sharing scheme, where the quality of the shadow images is highly improved for both gray level and binary cover images. In 2014, a novel hierarchical threshold secret image sharing scheme was proposed by Pakniat et al. [12]. In their scheme, any authorized subset of participants is able to reveal the secret and cover image losslessly while a non-authorized subset of participants gains no information about the secret image. Furthermore, their scheme allows participants to check whether the retrieved secret image is valid or not.

However, one of the common drawbacks in the schemes mentioned above is that they consider little about the access structure, which refers to the family of all qualified subsets of participants that can cooperate to reconstruct the secret image. For instance, three bank officials, one of whom is the financial manager, the other two of whom are staffs of the financial department, want to recover a bank check image. According to the regulation of the bank, the check image can be retrieved only if the financial manager and at least one of the staffs are on spot. Then these schemes fail to deal with this situation.

In 1989, Ito et al. [7] designed the first multiple assignment scheme for any given access structure whereby any qualified subset of the participants can reconstruct the secret while any unqualified subset cannot gain any information. In the same year, Benaloh and Leichter [2] presented a general method for building perfect secret sharing schemes for any access structure, provided it is monotone (that is, any set containing an authorized subset can also recover the secret). However, their scheme can't be applied efficiently in many cases. In 1994, a novel decomposition construction was utilized by Stinson [15] for perfect secret sharing schemes for any graph-based access structure. In their scheme, the information rate for any graph G can be $2/(d+1)$, where d is the maximum degree of graph G. In 2005, Barwick and Jackson [1] described an optimal (2, 3, *n*)-multi-threshold scheme to share multiple secrets among a group of *n* participants such that a secret s_K related to each subset K of three participants can be recovered by any two participants in K. Nevertheless, the scheme can't be

used in other situations. In the same year, based on the similarity between the Chinese remainder theorem and the uniqueness theorem of interpolating theorem, Chan and Chang [4] proposed a perfect threshold multi-secret sharing scheme where each secret is associated with an access structure. In the scheme, a dealer generates one master secret share for each participant such that participants are able to recover different secrets according to the corresponding threshold access structures. Besides, with a deletion procedure, any participant can be removed from a qualified subset and the secret can be reconstructed by the remaining participants of the qualified subset. Hence, their scheme has the ability to achieve any monotone access structure.

In 2005, using Largrange's interpolation, Feng et al. [5] proposed a scheme which is able to distribute multiple secret images according to any access structure. Nonetheless, in their scheme, any pixel value larger than 250 is truncated to 250, which causes the distortion of the retrieved secret images. Besides, the scheme is not a perfect one wherefore there exists chances for attackers to obtain a correct secret image from an unauthorized subset of the shadow images. In 2012, Guo et al. [6] presented a multi-threshold secret image sharing scheme based on monotone span programs (MSP). Their scheme realizes the function of sharing several secret images according to the corresponding threshold access structures. However, it can't be applied to general access structures.

And, in some situations, there are several secret images need to be protected, and according to the different security requirements, maybe each secret image is associated with different access structure. For example, there are several secret images that must be shared among a group of people in such a way that different subsets of the group can cooperate to reconstruct the related secret image. Due to the difficulty of finding efficient secret sharing schemes with multi-threshold access structures, and being suitable for image camouflage technology, it is worthwhile to find an efficient secret image sharing scheme with multi-threshold access structure.

To the best of our knowledge, there are few secret image sharing schemes dealing with a general access structure. Inspired by Chan and Chang's work, we propose a new multi-threshold secret image sharing scheme based on the generalized Chinese Remainder Theorem in this paper. With a deletion procedure, our scheme can also realize any monotone access structure. The proposed scheme allows the involved participants to share multiple secret images such that each secret image can be reconstructed without distortion by a qualified subset of the shadow images according to the corresponding threshold access structure while any unauthorized subset of the shadow images gets no information about it.

The contribution of this paper is the design of a multi-threshold secret image sharing scheme based on the generalized CRT, and our scheme has the following characteristics:

1. Multiple secret images can be shared according to the corresponding threshold access structures.
2. The scheme is able to deal with any monotone access structure with a deletion procedure.
3. The secret images can be retrieved without distortion.
4. The visual quality of the shadow images is acceptable and the capacity under binary images is quite satisfactory.

The rest of this paper is organized as follows: Section 2 will briefly describe Chan and Chang's threshold multi-secret sharing scheme. The proposed scheme is elaborated in Section 3. Section 4 discusses experimental results and analysis and finally, conclusions are presented in Section 5.

2 Preliminaries

In this section, we first describe Chinese Remainder Theorem (CRT), and then, we briefly introduce the multi-threshold secret sharing scheme proposed by Chan and Chang (2005), which is the major foundation of our method.

2.1 Chinese remainder theorem

Chinese remainder theorem is a theorem of packing a finite set of integers into one integer. We will state CRT and the related corollaries. The interested readers can find the proof in [4].

Theorem 1. Let m positive integers $p_1,p_2,\ldots,p_m$ be relatively prime in pairs. Given any m integers $K_1,K_2,\ldots,K_m$, there exists a unique integer $K\in Z_{p_1,p_2,\ldots,p_m}$ such that

$$\begin{aligned} K&\equiv K_1 (\mathrm{mod} p_1),\\ K&\equiv K_2 (\mathrm{mod} p_2),\\ &\vdots\\ K&\equiv K_m (\mathrm{mod} p_m). \end{aligned}$$

Theorem 2. Let P be a prime number and let $p_1,p_2,\ldots,p_m\in Z_P$ be m distinct integers. Given any m integers $K_1,K_2,\ldots,K_m\in Z_P$, there exists a unique polynomial $K(X)\in Z_P[X]$ with deg $(K)\leq m$-1 such that

$$\begin{aligned} K(p_1)&\equiv K_1 (\mathrm{mod} P),\\ K(p_2)&\equiv K_2 (\mathrm{mod} P),\\ &\vdots\\ K(p_m)&\equiv K_m (\mathrm{mod} P). \end{aligned}$$

Corollary 1. Let $M=\prod_{i=1}^{n} p_i^{r_i}$ where $p_1<p_2<\ldots<p_n$ are n distinct primes, and let $x_0,x_1,\ldots,x_{t-1}$ be distinct integers in Z_{p_1}. Given any t integers $y_0,y_1,\ldots,y_{t-1}$, there exists a unique polynomial $f(X)\in Z_M[X]$ with deg $(f)\leq t$ such that

$$\begin{aligned} f(x_0)&\equiv y_0 \left(\mathrm{mod} p_1^{r_1}\right),\\ f(x_1)&\equiv y_1 \left(\mathrm{mod} p_2^{r_2}\right),\\ &\vdots\\ f(x_{t-1})&\equiv y_{t-1} \left(\mathrm{mod} p_t^{r_t}\right). \end{aligned}$$

2.2 Review of Chan and Chang's scheme

Chan and Chang (2005)'s scheme is a generalization of Shamir's (t, n) threshold secret sharing scheme, which realizes multi-threshold access structures.

Given an access structure Γ, we call $A\in\Gamma$ a minimal authorized subset if any set B which is a subset of A and not equal to A is not a member of Γ. The family of all minimal authorized subsets of Γ is called the basis of Γ. Suppose that m secrets $K_1,K_2,\ldots,K_m$ are shared among a set of participants P according to the threshold bases $\Gamma_1,\Gamma_2,\ldots,\Gamma_m$, respectively, where $|\mathrm{P}|=n$ and $\Gamma_i=\{A\subset \mathrm{P}:|A|=t_i\}$. In this case, K_i is shared among P according to the (t_i,n) threshold access structure such that any t_i or more participants have the ability to collaboratively recover the secret K_i. Distinct primes $p_1,p_2,\ldots,p_m$ are selected by the dealer where $p_1<p_2<\ldots<p_m$ and $K_i<p_i$. Furthermore, we assume that n

numbers $x_0, x_1, \ldots, x_{n-1}$ are distinct in Z_{p_1}, which denote the public identification numbers of P, and that $t_1 \le t_2 \le \ldots \le t_m$.

1. The result of the simultaneous congruences below is denoted as a_0:

$$\begin{aligned} X &\equiv K_1 (\mathrm{mod} p_1), \\ X &\equiv K_2 (\mathrm{mod} p_2), \\ &\vdots \\ X &\equiv K_m (\mathrm{mod} p_m). \end{aligned}$$

2. Let $M = \prod_{i=1}^{m} p_i$ and the dealer randomly chooses $(t_1 - 1)$ integers $a_1, a_2, \ldots, a_{t_1 - 1} \in Z_M$
3. Compute the coefficients $a_{t_i}, a_{t_i+1}, \ldots, a_{t_{i+1}-1}$ for each $i = 1, 2, \ldots, m-1$, as follows:for each $j = t_i, t_i + 1, \ldots, t_{i+1} - 1, a_j \equiv b_j \times r_j \times \prod_{k=1}^{i-1} p_k (\mathrm{mod} M)$where b_j is a random number in $\{0, 1, 2, \ldots, p_i - 1\}$ and r_j is a random integer.
4. Construct a polynomial $f(X)$ of degree $(t_m - 1)$, as

$$f(X) = a_0 + a_1 X + \cdots + a_{t_m - 1} X^{t_m - 1}$$

5. Computer $y_i = f(x_i) (\mathrm{mod} M)$ as the ith master shadow. Then the dealer distributes it together with the prime factorization of M to the related participant via a secure channel.

In the deletion procedure, by calculating the shadow y_j' instead of y_j for the participant whose public identification number is x_j, the dealer is possible to prevent the participant from recovering the secret K_i, where y_j' is the solution of the simultaneous congruences below:

$$\begin{aligned} X &\equiv \left(y_j \mathrm{mod} \frac{M}{p_i} \right) \left(\mathrm{mod} \frac{M}{p_i} \right), \\ X &\equiv R_i \left(\mathrm{mod} p_i \right)_i, \end{aligned}$$

where

$$R_i \in Z_{p_i}$$

3 The proposed scheme

In the proposed scheme, multiple secret images can be shared among a set of participants according to the corresponding threshold access structures. By modifying the generated secret image shadows with a deletion procedure, the scheme is possible to realize any monotone access structure. Meanwhile, each secret image can be losslessly reconstructed by the qualified participants. In subsection 3.1, we discuss how to generate shadow images for different secret images and the corresponding access structures. Subsection 3.2 describes the method of revealing the secret images. To begin with, we give a definition for a multi-threshold secret image sharing scheme.

Definition 1. Given a set P of n involved participants $P_1, P_2, \ldots, P_n$ and a set S of m possible secret images $s_1, s_2, \ldots, s_m$. Threshold bases $\Gamma_1, \Gamma_2, \ldots, \Gamma_m$ are supposed to be associated with m

secret images where $\Gamma_i=\{A\subset \mathrm{P}:|A|=t_i\}$, respectively. A multi-threshold secret image sharing scheme is a method of generating n secret image shadows $I_1,I_2,\ldots,I_n$ for S, such that

1. For each $i=1,2,\ldots,m$, given any t_i out of n secret image shadows, the related secret image s_i can be easily reconstructed by the authorized participants.
2. For each $i=1,2,\ldots,m$, given fewer than t_i secret image shadows, the related secret image s_i is completely undetermined.

3.1 Secret image sharing procedure

Based on Chan and Chang (2005)'s threshold multi-secret sharing scheme, we introduce the image sharing process, which include two phases: the derivation phase and the camouflage phase. In the former phase, secret values are produced according to different access structures. In the latter phase, the dealer generates n meaningful shadow images by embedding the secret values in a cover image. Figure 1 shows the flowchart of the sharing procedure.

Assume that a set of $\mathrm{S}=\{s_1,s_2,\ldots,s_m\}$ contains m grayscale secret images each of which has $M_S\times M_S$ pixels, where $s_i=\{s_{ij}|1\le i\le m,1\le j\le M_S\times M_S\}$. O is a cover image with $H\times W$ pixels. In addition, all the n involved participants $P_1,P_2,\ldots,P_n$ belong to a set signed as P, and a set of $\mathrm{I}=\{I_k|k=1,2,\ldots,n\}$ denotes the generated shadow images. The secret images are supposed to be shared according to the threshold bases $\Gamma_1,\Gamma_2,\ldots,\Gamma_m$, respectively, where $\Gamma_i=\{A\subset \mathsf{P}:|A|=t_i\}$ and $t_1\le t_2\le\ldots\le t_m$.

3.1.1 Preliminaries

Step 1 The dealer obtains all pixels of m secret images and determines the maximum pixel value for each secret image.

Step 2 The dealer chooses m distinct primes $p_1,p_2,\ldots,p_m$ where $p_1<p_2<\ldots<p_m$ and the maximum pixel value of the ith secret image is less than p_i

Step 3 Distinct $x_1,x_2,\ldots,x_n\in {}^nZ_{p_1}$ are selected as the public identification numbers of n participants $P_1,P_2,\ldots,P_n$, respectively.

3.1.2 Derivation phase

The dealer can perform the following steps to generate the secret values for multi-threshold access structures:

Step 1 The dealer computers $M=\prod_{i=1}^{m}p_i$

Step 2 For the group of the jth pixel values of all secret images, the dealer constructs t_1 coefficients $a_0,a_1,\ldots,a_{t_1-1}$, where a_0 is the solution of the following simultaneous congruences, and $a_1,a_2,\ldots,a_{t_1-1}$ are randomly chosen in Z_M

$$\begin{aligned} X&\equiv s_{1j}(\mathrm{mod}p_1),\\ X&\equiv s_{2j}(\mathrm{mod}p_2),\\ &\vdots\\ X&\equiv s_{mj}(\mathrm{mod}p_m). \end{aligned}$$

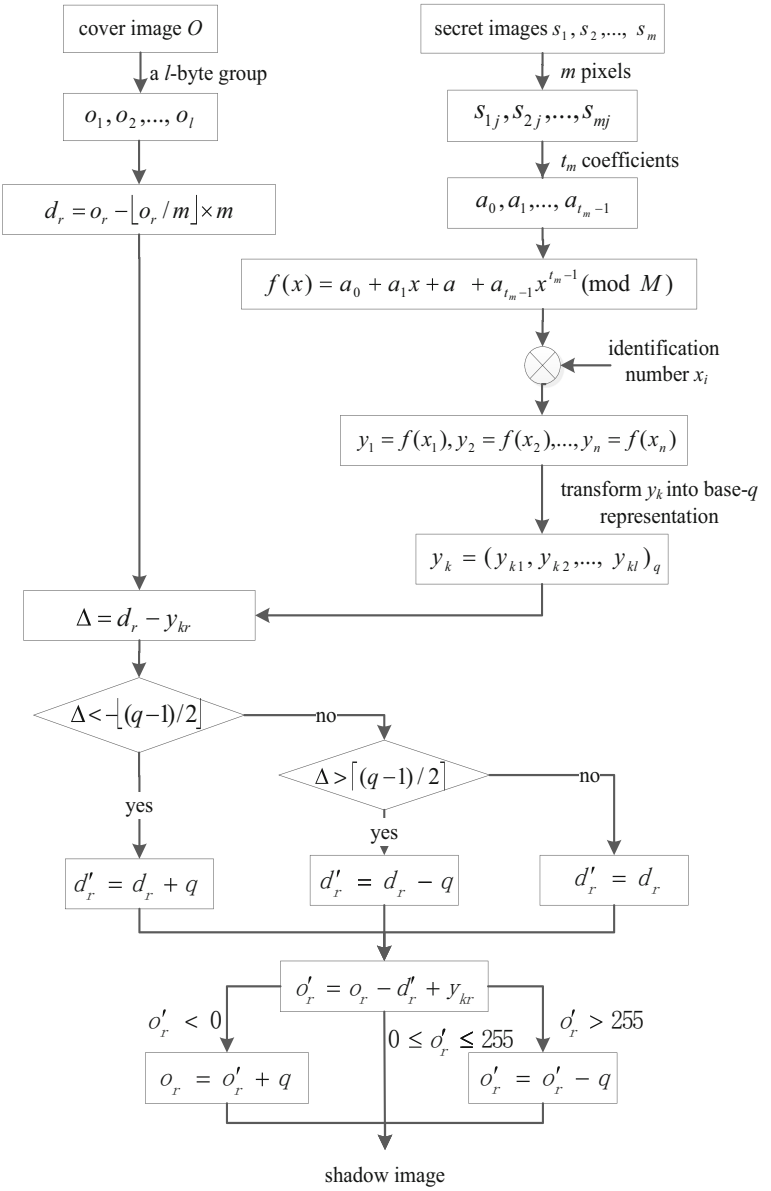


Fig. 1 The diagram of the secret image sharing scheme

Step 3 For each $i=1,2,\ldots,m-1$, the dealer constructs $(t_{i+1}-t_i)$ coefficients $a_{t_i}, a_{t_i+1}, \ldots, a_{t_{i+1}-1}$, where for each $l=t_i,t_i+1,\ldots,t_{i+1}-1$, let b_l be a random number in $\{0,1,2,\ldots,p_i-1\}$ and c_l be a random integer such that $a_l \equiv b_l \times c_l \times \prod_{r=1}^{i-1} p_r (\text{mod} M)$

Step 4 The dealer constructs a polynomial $f(X)$ of degree (t_m-1), as follows:

$$f(X) = a_0 + a_1 X + \cdots + a_{t_m-1} X^{t_m-1}$$

Step 5 For each $k=1,2,\ldots,n$, the dealer computes $y_k=f(x_k)(\mathrm{mod}M)$ as the jth secret value for the shadow image I_k.

Step 6 Repeat Step 2–5 until all pixels of the secret images are calculated.

Besides, in order to realize all monotone access structures, a deletion procedure can be employed, where the dealer modifies the secret value for shadow image I_k such that the participant P_k doesn't have the right to reconstruct the secret image s_i. For each $1\le j\le M_S\times M_S$, the jth modified secret value $y_k^{'}$ for $I_k^{'}$ can be computed according to the following simultaneous congruences whose solution is $y_k^{'}$:

$$X\equiv\left(y_k \bmod \frac{M}{p_i}\right)\left(\bmod \frac{M}{p_i}\right),$$
$$X\equiv R_i\left(\bmod p_i\right)^i,$$

where $R_i\in Z_{p_i}$. For instance, there is a set of $P=\{P_1,P_2,P_3,P_4\}$, and a secret image s_1 is associated with the access structure $\Gamma_1=\{P_1,P_4\}$. The dealer can revise the secret values for P_2 and P_3 such that only P_1 and P_4 can cooperate to retrieve the secret image s_1 and any other subset of P which doesn't contain P_1 and P_4 is incapable of getting any information about s_1.

3.1.3 Camouflage phase

The secret values can be embedded by using the quantization operation.

Step 1 The dealer chooses a prime q and computes l as $l=\lceil \log_q M\rceil$.

Step 2 Transform the secret value y_k into base-q representation, denoted as $y_k=(y_{k1},y_{k2},\ldots,y_{kl})_q$, for $k=1,2,\ldots,n$.

Step 3 Divide the pixels of the cover image into a series of l-byte groups whose pixels are $o_1, o_2,\ldots,o_l$

Step 4 For each $r=1,2,\ldots l$, compute the value d_r as

$$d_r = o_r-\lfloor o_r/q\rfloor\times q.$$

Step 5 Evaluate $d_r^{'}$ according to

$$d_r^{'}=\begin{cases} d_r+q & \text{if } (-q<\Delta<-\lfloor (q-1)/2\rfloor)\ , \\ d_r & \text{if } (-\lfloor (q-1)/2\rfloor\le\Delta\le\lceil (q-1)/2\rceil)\ , \\ d_r-q & \text{if } (\lceil (q-1)/2\rceil<\Delta<q)\ \ , \end{cases}$$

Where

$$\Delta = d_r-y_{kr}$$

Step 6 Derive the pixel $o_r^{'}$ in the following way:

$$o_r^{'}=o_r-d_r^{'}+y_{kr}.$$

Step 7 If underflow or overflow occurs, the dealer modifies the value $o_r^{'}$.

$$o_r^{'}=\begin{cases} o_r^{'}+q & \text{if } \left(o_r^{'}<0\right), \\ o_r^{'}-q & \text{if } \left(o_r^{'}>255\right). \end{cases}$$

Step 8 Repeat the above steps until all the secret values are embedded.

After the total secret values are camouflaged into a cover image O, the dealer can generate n shadow images and send them together with the prime factorization of M to the participants via secure channels.

In particular, let $q=7$ and the first six pixel values of the cover image are 214,240,192,60, 120,253. We can calculate $d_1,d_2,\ldots,d_6$ as 4,2,3,4,1,1, respectively. To embed the first secret value $y_1=3518=(0,1,3,1,5,4)_7$,, $d_1'=4-7=-3$, $d_2'=2$, $d_3'=3$, $d_4'=4$, $d_5'=1+7=8$ and $d_6'=1$ can be derived. Hence, we can obtain the pixel values of $o_1'=214+3+0=217$, $o_2'=240-2+1=239$, $o_3'=192-3+3=192$, $o_4'=60-4+1=57$, $o_5'=120-8+5=117$ and $o_6'=253-1+4=256$. Since that there occurs overflow in o_6', we adjust it as $o_6'=256-7=249$.

3.2 Secret image retrieving procedure

According to access structures, authorized participants can cooperate to reveal the secret image s_i, for $i=1,2,\ldots m$, without any loss.

Step 1 Divide the pixels of each involved shadow image into a series of l-byte groups.

Step 2 For each $r=1,2,\ldots l$, compute y_{kr} as

$$y_{kr} = o_{kr} \bmod q,$$

where o_{kr} denotes the pixel value in the kth shadow image I_k.

Step 3 Retrieve the secret value y_k by transform $(y_{k1}||y_{k2}||\cdots||y_{kl})_q$ into the decimal representation.

Step 4 Reconstruct the polynomial $f_i(X)$ using enough pairs of (x_k,y_k).

Step 5 The jth pixel of the secret image s_i can be calculated as follows:

$$f_i(0) \equiv s_{ij} (\bmod p_i).$$

Step 6 Repeat the above steps until all the pixels of s_i are extracted.

4 Experimental results and analysis

In this section, experimental results for multi-threshold secret image sharing are described to demonstrate the performance of the proposed scheme and the characteristics of multi-threshold access structures.

4.1 Simulation results

Assume that two secret images are shared among the participant set $\mathrm{P}=\{P_1,P_2,P_3,P_4\}$. The threshold basis for the secret images are $\Gamma_1=\{A\subset \mathrm{P}:|A|=2\}$ and $\Gamma_2=\{A\subset \mathrm{P}:|A|=3\}$, respectively. Fifteen grayscale test images with 512×512 pixels are shown in Fig. 2 and two secret images with 200×200 pixels are shown in Fig. 3. To measure the quality of the shadow images, the peak signal-to-noise rate (PSNR) is used:

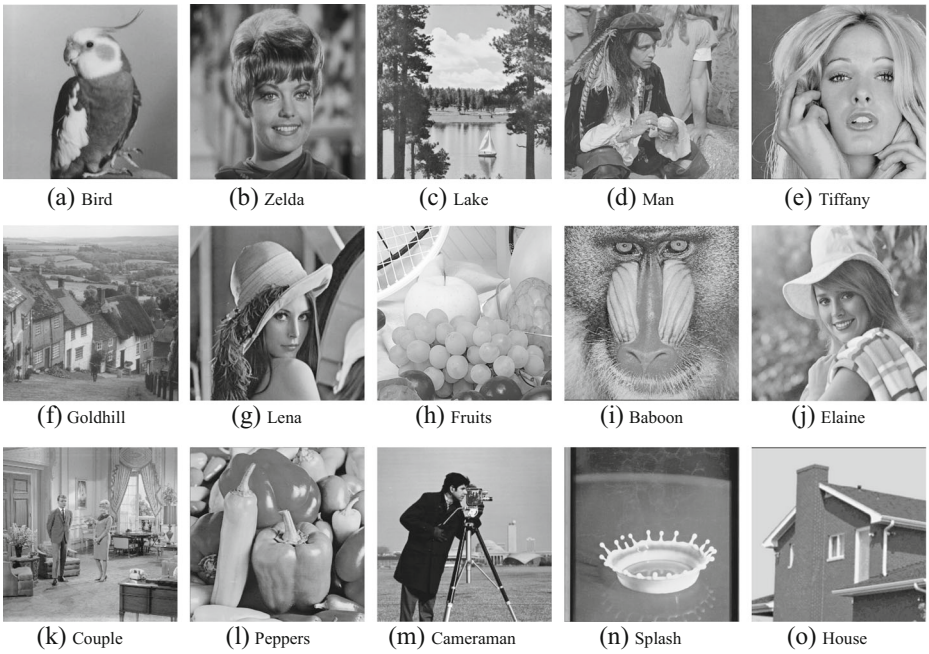


Fig. 2 The grayscale test images **a** Bird **b** Zelda **c** Lake **d** Man **e** Tiffany **f** Goldhill **g** Lena **h** Fruits **i** Baboon **j** Elaine **k** Couple **i** Peppers **m** Cameraman **n** Splash **o** House

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right)\mathrm{dB},$$

where *MSE* denotes the mean-square error of an image with $H\times W$ pixels. Suppose that p_{uv} is the original pixel value and p'_{uv} is the shadow pixel value. Then *MSE* can be defined as:

$$MSE = \frac{1}{H \times W}\sum_{u=1}^{H}\sum_{v=1}^{W}\left(p_{uv}-p'_{uv}\right)^2.$$

The prime q is set as q=7. Table 1 lists the PSNR values of the shadow images using the gray level cover images. It manifests that the shadow images can maintain satisfactory for different test images. To demonstrate the visual perception, we use *Lena* in Fig. 2g as a cover image. Fig. 4a-d show the results of the shadow images. Compared with the original cover image, the distortion of the shadow images is imperceptible. According to the defined threshold access structures, the first secret image *Boat* can be reconstructed by any two out of four shadow images, and the second secret image *Airplane* can be reconstructed by any three out of four shadow images. Any other subset of the shadow images gets no information about the secret images. Figure 4e-f show the retrieved lossless secret images.

The scheme can also realize any monotone access structure. Suppose that P_1 and P_3 can cooperatively recover the first secret image *Boat*, and the second secret image *Airplane* can be retrieve by P_1, P_3 and P_4. In the deletion procedure, the dealer deletes the right of P_2 and P_4 for recovering the first secret image and the right of P_2 for reconstructing the second secret image respectively as such any set of $\{P_1,P_3\}$, $\{P_1,P_2,P_3\}$, $\{P_1,P_3,P_4\}$ and $\{P_1,P_2,P_3,P_4\}$ is qualified to

(a) Boat (b) Airplane

Fig. 3 The grayscale secret images. **a** Boat **b** Airplane

reconstruct the first secret image, and any set of $\{P_1,P_3,P_4\}$ and $\{P_1,P_2,P_3,P_4\}$ is authorized to recover the second secret image while any other subset cannot get any information about the secret images. The PSNR values of the shadow images are shown in Table 2. Compared with the values in Table 1, the quality of the shadow images for the monotone access structures has the same satisfaction with that for the threshold access structures. Figure 5a-d show the results of the shadow images using the cover image *Lena*. The secret image *Boa*t reconstructed by $P_1$and P_3 and the secret image *Airplane* retrieved by P_1, P_3 and P_4 are given in Fig. 5e, f, respectively.

4.2 Discussions

Compared with traditional (t,n) secret image sharing schemes, our scheme can share several secret images among a group of participants during one sharing process. The ith secret image is related

Table 1 The PSNR value (dB) of the shadow images for test images for a multi-threshold access structure, $q=7$

Test images	PSNR (dB)			
	Shadow image 1	Shadow image 2	Shadow image 3	Shadow image 4
Bird	42.50	42.51	42.51	42.52
Zelda	42.49	42.48	42.50	42.49
Lake	42.50	42.50	42.49	42.50
Man	42.48	42.47	42.47	42.47
Tiffany	42.42	42.42	42.43	42.43
Goldhill	42.49	42.50	42.49	42.50
Lena	42.50	42.50	42.49	42.51
Fruits	42.45	42.45	42.46	42.47
Baboon	42.49	42.48	42.51	42.50
Elaine	42.51	42.49	42.50	42.49
Couple	42.48	42.50	42.49	42.48
Peppers	42.50	42.49	42.48	42.50
Cameraman	42.51	42.51	42.51	42.51
Splash	42.49	42.48	42.48	42.48
House	42.62	42.63	42.64	42.66

(a) The shadow image 1, PSNR=42.50 dB

(b) The shadow image 2, PSNR=42.50 dB

(c) The shadow image3, PSNR=42.49 dB

(d) The shadow image 4, PSNR=42.51 dB

(e) The extracted Boat, PSNR=∞ dB

(f) The extracted Airplane, PSNR=∞ dB

Fig. 4 The results of Lena, for a multi-threshold access structure, q=7. **a** The shadow image 1, PSNR=42.50 dB **b** The shadow image 2, PSNR=42.50 dB **c** The shadow image3, PSNR=42.49 dB **d** The shadow image 4, PSNR=42.51 dB **e** The extracted Boat, PSNR=∞ dB **f** The extracted Airplane, PSNR=∞ dB

to a (t_i,n) threshold access structure, and given any t_i out of n shadow images, the corresponding secret image can be retrieved losslessly, while t_i-1 or fewer shadow images cannot.

The secret capacity and the quality of the shadow images in the new method are influenced by factors M and q. Factor M is set by multiplying each prime $p_i(i=1,2,\ldots,m)$ whose value is larger than the maximum pixel value of the ith secret image. Each secret value is supposed to be embedded by $\lceil \log_q M \rceil$ pixels of the cover image. For a cover image with $H\times W$ pixels, it can hide at most $\frac{H\times W}{\left\lceil \log_q M \right\rceil}$ secret values, so the secret capacity is to be $\frac{H\times W}{\left\lceil \log_q M \right\rceil}$. Hence, given a certain value of q, the larger the value M, the lower the secret capacity is. In this case, for each $i=1,2,\ldots n$, selecting the smallest prime among all qualified primes as p_i can obtain higher capacity. Figure 6 shows the maximum pixel value of each image in Fig. 2. For the first image *Bird* in Fig. 2a whose maximum pixel value is 214, all the primes equal to or larger than 223 are qualified such that we choose 223 as the prime that we use in our scheme.

Table 3 shows the capacity and the related PSNR values in which three groups of secret images with 200×200 pixels are shared among four participants independently according to the multi-threshold access structure mentioned in subsection 4.1. The first group contains two grayscale images, *Woman* in Fig. 7a and *Crowd* in Fig. 7b where M=251×257=64507, the second group consists of two grayscale pictures, *Calligraphy*1 in Fig. 7c and *Calligraphy*2 in Fig. 7d where M=127×131=16637, and the third group contains two binary images, *Camel* in Fig. 7e and *Signature* in Fig. 7f where M=2×3=6. Besides, the test image *Lena* in Fig. 2g is used as the cover image. As

Table 2 The PSNR value (dB) of the shadow images for test images for a monotone access structure, q=7

Test images	PSNR (dB)			
	Shadow image 1	Shadow image 2	Shadow image 3	Shadow image 4
Bird	42.51	42.47	42.50	42.48
Zelda	42.48	42.49	42.49	42.50
Lake	42.49	42.50	42.48	42.48
Man	42.48	42.49	42.45	42.50
Tiffany	42.43	42.42	42.42	42.41
Goldhill	42.49	42.47	42.50	42.49
Lena	42.48	42.48	42.48	42.50
Fruits	42.45	42.42	42.45	42.43
Baboon	42.48	42.49	42.48	42.48
Elaine	42.48	42.47	42.50	42.50
Couple	42.48	42.48	42.48	42.47
Peppers	42.48	42.51	42.49	42.49
Cameraman	42.51	42.49	42.50	42.49
Splash	42.47	42.48	42.47	42.49
House	42.62	42.55	42.63	42.55

we can see, for factor q, a lower value is possible to get larger secret capacity, while the quality of the shadow images will be descended. When we share two or more grayscale secret images, the length of M is often longer than four bits, just as the case in group one and group two, which leads to low capacity. Thus, we select a middle value of m as 7 to get comparative high capacity as well as satisfactory quality of the shadow images. But if the secret images are in binary scale, the value of M is much smaller than that in gray level such that we can choose a small value of m to achieve higher quality of the shadow images at the same time that we can gain higher capacity. That is to say, our scheme is more suitable for binary images or some grayscale pictures with quite low pixel values than the normal gray-level images.

In our scheme, we do not supply any protection process to verify the validity of the shadow images. However, any method which is suitable for the threshold secret image sharing scheme based on Shamir's method can be used here.

Table 4 compares the functionality of our scheme with the related methods. As shown in Table 4, the new scheme can share multiple secret images and deal with not only multi-threshold access structures but also general access structures. Besides, the shadow images are meaningful and the quality is satisfactory, and the secret images can be reconstructed losslessly.

Compared with (Yang et al. [19]; Lin et al., [9]; Ulutas et al. [16]), which can only share one secret image during one share process, the new scheme provides a method to distribute multiple secret images with good performance. In the new scheme, m secret images can be shared in the way that one participant holds just one shadow image, while $m \times n$ shadow images are needed for a non-multisecret image sharing scheme.

Feng et al. [5] and Guo et al. [6] proposed two schemes to realize the function of multi-secret images sharing, however, both of them have some drawbacks mentioned before. Our method is a perfect scheme for general access structures in which qualified participants can cooperate to recover distortion-free secret images.

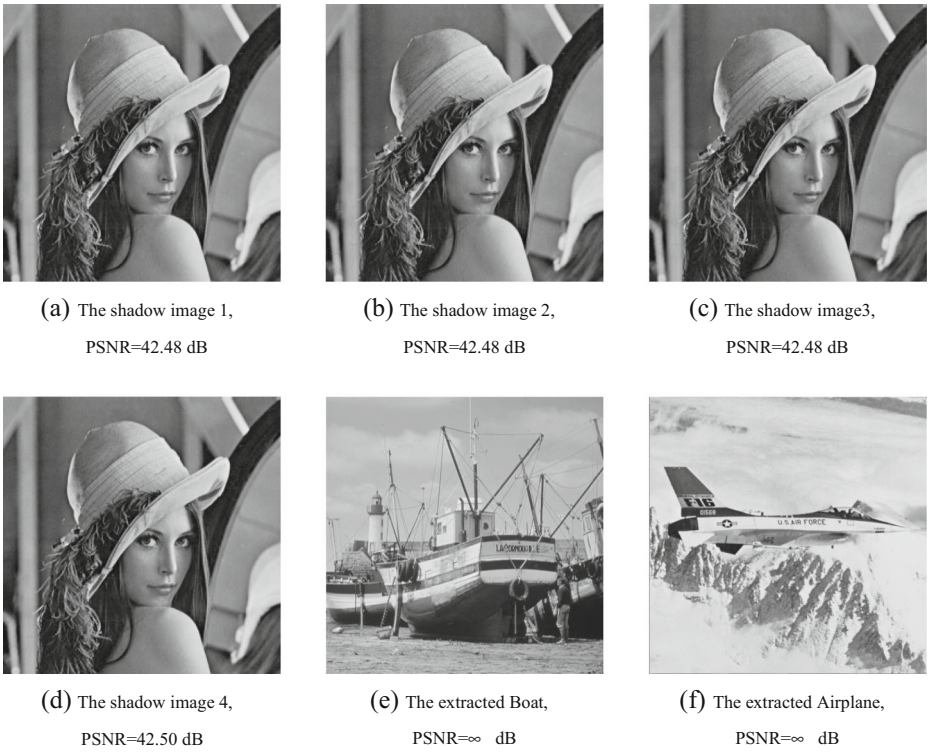


Fig. 5 The results of Lena, for a monotone access structure, q=7. **a** The shadow image 1, PSNR=42.48 dB **b** The shadow image 2, PSNR=42.48 dB **c** The shadow image3, PSNR=42.48 dB **d** The shadow image 4, PSNR=42.50 dB **e** The extracted Boat, PSNR=∞ dB **f** The extracted Airplane, PSNR=∞ dB

5 Conclusions

In this paper, a scheme for multi-threshold secret image sharing has been proposed. In a set of participants, multiple secret images are able to be shared where each secret image is associated with a threshold access structure. Each participant is supposed to hold only one shadow image, and given a qualified subset of the shadow images, each secret image can be reconstructed without distortion according to the corresponding access structure. Meanwhile, with a deletion

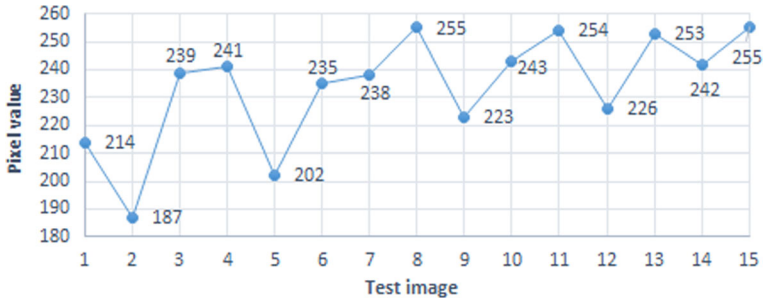


Fig. 6 The maximum pixel values of the test images

Table 3 The relationship of the capacity-distortion under different q and M

q	[0,q-1]	Group 1 (M=64507)		Group 2 (M=16637)		Group 3 (M=6)	
		Capacity	*PSNR* (dB)	Capacity	*PSNR* (dB)	Capacity	*PSNR* (dB)
3	[0,2]	$H\times W/11$	–	$H\times W/9$	–	$H\times W/2$	55.05
5	[0,4]	$H\times W/7$	–	$H\times W/7$	–	$H\times W/2$	47.26
7	[0.6]	$H\times W/6$	42.49	$H\times W/5$	42.50	$H\times W$	42.49
11	[0,10]	$H\times W/5$	38.13	$H\times W/5$	38.15	$H\times W$	38.11
13	[0,12]	$H\times W/5$	36.70	$H\times W/4$	36.68	$H\times W$	36.68
17	[0,16]	$H\times W/4$	34.31	$H\times W/4$	34.30	$H\times W$	34.32
19	[0,18]	$H\times W/4$	33.44	$H\times W/4$	33.42	$H\times W$	33.41

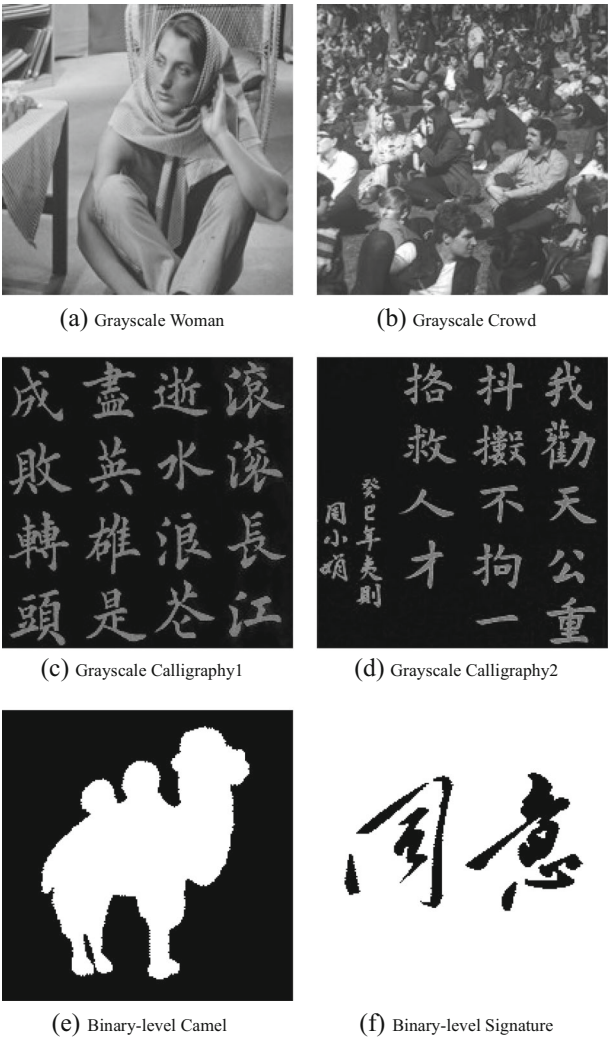


Fig. 7 Three groups of secret images **a** Grayscale Woman **b** Grayscale Crowd **c** Grayscale Calligraphy1 **d** Grayscale Calligraphy2 **e** Binary-level Camel **f** Binary-level Signature

(a) Grayscale Woman

(b) Grayscale Crowd

(c) Grayscale Calligraphy1

(d) Grayscale Calligraphy2

(e) Binary-level Camel

(f) Binary-level Signature

Table 4 Comparisons of the related secret image sharing schemes

Functionality	Feng et al. [5]	Yang et al. [19]	Lin et al. [9]	Guo et al. [6]	Ulutas et al. [16]	Ours
Multi-secret image sharing	Yes	No	No	Yes	No	Yes
Multi-threshold access structures	Yes	No	No	Yes	No	Yes
General access structures	Yes	No	No	No	No	Yes
Meaningful shadow image	Yes	Yes	Yes	Yes	Yes	Yes
Quality of shadow images (dB)	42	41	44	40	47	42
Lossless secret image	No	Yes	Yes	Yes	Yes	Yes
Computational complexity	$O(n\log^2 n)$	$O(n\log^2 n)$	$O(n\log^2 n)$	$O(n^2)$	$O(n\log^2 n)$	$O(n)$
Shadow memory	n	$m\times n$	$m\times n$	n	$m\times n$	n
Embedding capacity	$\left[\frac{1}{2},1\right]\times H\times W$	$\frac{H\times W}{4}$	$\frac{(t-3)\times H\times W}{3}$	$\frac{H\times W}{5}\times m$	$\frac{(t-2)\times H\times W}{4}$	$\frac{H\times W}{\lceil \log_q M\rceil}$

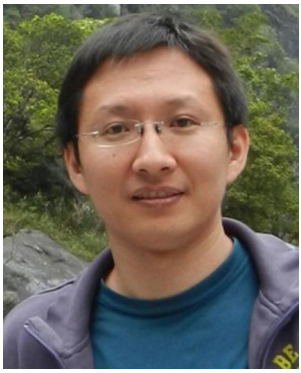
procedure, all monotone access structures are possible to be realized by the proposed scheme. The experimental results have shown that the new scheme is feasible and the quality of the shadow images is satisfactory.

Acknowledgments This paper is supported by the National Science Foundation of China under grant No. 61272173, 61100194, 61401060 and the general program of Liaoning Provincial Department of Education Science Research under grants L2014017.

References

1. Barwick SG, Jackson WA (2005) An optimal multisecret threshold scheme construction. Des Codes Crypt 37(3):367–389
2. J. Benaloh, J. Leichter (1989) Generalized secret sharing and monotone functions, in: S. Goldwasser (Ed.), Advances in Cryptology, CRYPTO'88, in: Lecture Notes in Computer Science, vol. 403, 1989, pp. 27–35
3. Blakley GR (1979) Safeguarding cryptographic keys. Proc AFIPS Nat Compu Conf 48:313–317
4. Chan CW, Chang CC (2005) A scheme for threshold multi-secret sharing. Appl Math Comput 166(1):1–14
5. Feng JB, Wu HC, Tsai CS, Chu YP (2005) A new multi-secret images sharing scheme using Largrange's interpolation. J Syst Softw 76(3):327–339
6. Guo C, Chang CC, Qin C (2012) A multi-threshold secret image sharing scheme based on MSP. Pattern Recogn Lett 33(12):1594–1600
7. Ito M, Saito A, Nishizeki T (1989) Secret sharing scheme realizing general access structure. Electron Commun Jpn (Part III: Fundamental Electronic Science) 72(9):56–64
8. Kumar S, Sharma RK (2014) Threshold visual secret sharing based on boolean operations. Sec Commun Net 7(3):653–664
9. Lin PY, Lee JS, Chang CC (2009) Distortion-free secret image sharing mechanism using modulus operator. Pattern Recogn 42(5):886–895
10. Lin C, Tsai W (2004) Secret image sharing with steganography and authentication. J Syst Softw 73(3):405–414
11. Naor M, Shamir A (1995) Visual cryptography. Lect Notes Comput Sci 950:1–12
12. Pakniat N, Noroozi M, Eslami Z (2014) Secret image sharing scheme with hierarchical threshold access structure. J Visual Commun Image Represent 25(5):1093–1101
13. Sasaki M, Watanabe Y (2014) Formulation of visual secret sharing schemes encrypting multiple images. In Acoustics, Speech and Signal Processing (ICASSP), 2014 I.E. International Conference on (pp. 7391–7395)
14. Shamir A (1979) How to share a secret. Commun ACM 22(11):612–613

15. Stinson DR (1994) Decomposition constructions for secret sharing schemes. IEEE Trans Inf Theory 40:118–125
16. Ulutas M, Ulutas G, Nabiyev VV (2013) Invertible secret image sharing for gray level and dithered cover images. J Syst Softw 86(2):485–500
17. Wu X, Sun W (2013) Random grid-based visual secret sharing with abilities of OR and XOR decryptions. J Vis Commun Image Represent 24:48–62
18. Yan X, Wang S, Niu X et al (2015) Random grid-based visual secret sharing with multiple decryptions. J Vis Commun Image Represent 26:94–104
19. Yang CN, Chen TS, Yu KH, Wang CC (2007) Improvements of image sharing with steganography and authentication. J Syst Softw 80–7:1070–1076



Cheng Guo received the B.S. degree in computer science from Xi'an University of Architecture and Technology in 2002. He received the M.S. degree in 2006 and his Ph.D in computer application and technology, in 2009, both from the Dalian University of Technology, Dalian, China. From July 2010 to July 2012, he was a post doc in the Department of Computer Science at the National Tsing Hua University, Hsinchu, Taiwan. Since 2013, he has been an associate professor in the School of Software Technology at the Dalian University of Technology. His current research interests include information security and cryptology.

Huan Zhang received the B. S. degree in software engineering from Dalian University of Technology, Dalian, China in 2013. She is currently pursuing her M. S. degree in Dalian University of Technology, Dalian, China. Her research interests include secret image sharing and cloud computing security.

Qiongqiong Song received the B. S. degree in software engineering from Dalian University of Technology, Dalian, China in 2013. She is currently a MS student in Dalian University of Technology, Dalian, China. Her interests are cloud computing security.

Mingchu Li received the B.S. degree in mathematics, Jiangxi Normal University and the M.S. degree in applied science, University of Science and Technology Beijing in 1983 and 1989, respectively. He worked for University of Science and Technology Beijing in the capacity of associate professor from 1989 to 1994. He received his doctorate in Mathematics, University of Toronto in 1997. He was engaged in research and development on information security at Longview Solution Inc, Compuware Inc. from 1997 to 2002. From 2002, he worked for School of Software of Tianjin University as a full professor, and from 2004 to now, he worked for School of Software Technology of Dalian University of Technology as a full Professor, Ph.D. supervisor, and vice dean. His main research interests include theoretical computer science and cryptography.