Multimed Tools Appl (2017) 76:21193–21210
DOI 10.1007/s11042-016-4065-z

(t, n) Threshold secret image sharing scheme with adversary structure

Cheng Guo[1,2] · **Qiongqiong Yuan**[1,2] · **Kun Lu**[1,2] · **Mingchu Li**[1,2] · **Zhangjie Fu**[3]

Received: 3 April 2016 / Revised: 29 August 2016 / Accepted: 12 October 2016 /
Published online: 22 October 2016

Abstract Secret image sharing has been researched intensively, and it has emerged as an alternative to data hiding for protecting the security and privacy of important data. In the traditional (t, n) threshold secret image sharing schemes, any t or more shadow images can reconstruct the shared secret image. However, in real applications, (t, n) threshold access structures cannot meet all of the requirements, such as the adversary structure, which means that unauthorized groups of participants cannot reconstruct the shared secret. Thus, in (t, n) threshold secret sharing with adversary structure, t participants who want to reconstruct the secret cannot do so if they happen to belong to the defined adversary structure. This novel characteristic has the potential to work in many applications. However, the existing secret image sharing mechanisms cannot achieve the adversary structure. To solve this problem, we proposed a secret image sharing scheme that can achieve the adversary structure. In addition, our scheme also is a (t, n) threshold secret image sharing scheme. That is, t or more shadow images can be used to reconstruct the secret image, but some subsets that contain at least t shadow images among the adversary structures cannot reconstruct the secret image. The experimental results showed that the validity of our scheme is satisfactory.

Keywords Adversary structure · Secret image sharing · (t, n) threshold · Distortion-free

✉ Cheng Guo
guocheng@dlut.edu.cn

[1] School of Software Technology, Dalian University of Technology, Development Zone, Dalian 116620, People's Republic of China

[2] Key Laboratory for Ubiquitous Network and Service Software of Liaoning Province, Dalian 116620, China

[3] School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing 210044, China

1 Introduction

With the development of network technology and cloud storage [19, 25], more and more multimedia data, such as image, video, and others, are outsourced to the cloud server for storage in order to reduce the storage cost. Meanwhile, large amounts of multimedia data have emerged from social networks. Therefore, the security and privacy [9, 15] of these data are becoming more and more important. The secret sharing scheme is an important method to protect the security and integrity of secret data, and it has been applied in many fields. In 1979, both Shamir [20] and Blakley [2] proposed (t, n) threshold secret sharing schemes. In their schemes, the secret is divided into n shadows that are distributed to n participants. Any t or more participants can cooperate to recover the secret by pooling their secret shadows. However, no information about the secret can be obtained using $t-1$ or fewer shadows.

Based on the previous work, several secret image sharing schemes have been proposed. First, Naor and Shamir [16] proposed a secret image sharing scheme known as visual secret sharing (VSS). In VSS schemes (Yang [28]; Wang and Su [24]; Lin and Wang [13]), the secret image can be reconstructed by stacking t or greater shadow images without any cryptographic computations. However, the shadow images are random-like in the VSS scheme. So, they will be more likely to attract the attention of malicious attackers when the shadows are delivered over an insecure channel. In order to solve this problem, some secret image sharing schemes have been proposed that utilized the steganography approach to camouflage the shadows into a cover image to generate meaningful shadow images. In 2003, Thien and Lin [23] proposed a user-friendly secret image sharing scheme utilizing the steganography approach in which the shadow images were meaningful. However, the shadow images in their scheme are just reduced versions of the secret image, and they can expose some information about the secret image. Then, Lin and Tsai [12] utilized the least significant bits (LSB) embedding technique to hide shared values into a cover image. Furthermore, an image watermarking technique was used to verify whether the shadow images had been tampered. But, in their scheme, the revealed secret image is distorted slightly. It is well known that revealing the secret image without distortion is of paramount importance in some fields. Thus, even a slight distortion may be intolerable. So, based on Lin and Tsai's scheme, Yang et al. [29] developed a secret image sharing scheme that can prevent distortion of the shared secret image. However, their scheme reduces the visual quality of the shadow images, which may increase the potential for attacks. In 2009, Lin et al. [11] used the modulus operation to improve the quality of the shadow images. Moreover, both the shared secret image and the cover image can be reconstructed losslessly in their scheme. But the embedding capacity of their scheme is unacceptable to some extent. So, Lin and Chan [10] introduced a novel secret image sharing scheme that increased the maximum embedding capacity. Of course, their scheme also can recover the secret image and the cover image without distortion. However, the camouflaged pixel values in their scheme may exceed the grayscale boundary, which will cause the overflow situation. And most secret image sharing schemes utilize least significant bit (LSB) to embed the secret value. Some steganalysis of LSB matching schemes have been proposed (Xia and Wang et al. [26], Xia and Wang et al. [27]).

All of these schemes are (t, n) threshold secret sharing schemes, but they cannot be applied directly to non-threshold configurations. So, general access structure secret sharing schemes (GASSS) were proposed (Ito et al. [8]; Benaloh et al. [1]). In these schemes, the dealer can designate certain authorized groups of participants, and only those participants can recover the shared secret. It is obvious that the (t, n) threshold

scheme is a special case of GASSS. Subsequently, secret sharing schemes with a general access structure were proposed (Chang et al. [3]; Tan et al. [22]; Pang et al. [17]). Based on the research of these authors, some secret image sharing schemes have been proposed that achieved various access structures. Shyu and Chen [21] proposed a secret image sharing scheme for a general access structure that also was a multi-secret image sharing scheme. However, their scheme is not secure. In 2012, Guo et al. [4] proposed a secret image scheme that achieved a hierarchical threshold access structure. In their scheme, the participants do not have equivalent roles, and the shadow images are partitioned into several levels, which are determined by a sequence of threshold requirements. The same authors proposed a secret image sharing scheme with a multi-threshold access structure based on monotone span programs (MSP) [5]. Their scheme simultaneously achieves both multi-secret image sharing and generalized access structure. Each shared secret image is associated with an access structure. So, the authorized subset of shadow images can cooperate to reveal the corresponding secret image losslessly. In 2014, Guo et al. proposed a (n, t, n) threshold secret image sharing scheme [6], and, in 2015, they proposed a multi-threshold secret image sharing scheme [7] based on the generalized Chinese Remainder Theorem.

GASSS concerns the authorized groups of participants rather than corrupt participants. In GASSS schemes, only participants in the "qualified subset" can cooperate to recover the shared secret, but participants in the "unqualified subset" cannot. This means that the generalized access structure concerns the "qualified subset," while the adversary structure focuses on the unqualified subset. In reality, sometimes it is difficult to obtain the access structure according to the security requirements.

In some situations, the adversary can make some subsets of participants corrupt, which means the adversary can get their shared shares to reconstruct the secret. GASSS cannot be used in the above case, because the access structure defines qualified subsets of participants. This problem can be solved by the secret sharing scheme based on adversary structure, which can exclude the corrupt subsets to reveal the secret. Therefore, secret sharing schemes with adversary structure were proposed, and the structure is described in detail in Section 2. Ma and Guo [14] proposed a secret sharing scheme that achieved the adversary structure, but their scheme cannot achieve the (t, n) threshold. In order to widen the applications of this scheme, Qin et al. [18] developed a scheme that achieved both the (t, n) threshold and the adversary structure. Even though t participants are required to reconstruct the secret in their scheme, they cannot recover the secret if they belong to the defined adversary structure. In addition, the scheme can prevent the participants from cheating. Nevertheless, the size of the participants' shares is somewhat large, while the shared secret is a large, private file. So, based on the properties of the Jordan matrix, Zhao et al. [30] made it possible to have a small share while sharing a large secret.

For example, concerning a (3, 5) threshold and an adversary structure $\{S_1, S_2, S_4\}$, there are five shadow images $\{S_1, S_2, S_3, S_4, S_5\}$ to share a secret image (generating five shadow images by embedding a secret image into a cover image), and we can reconstruct the shared secret image from three or more shadow images, with the exception of the subset $\{S_1, S_2, S_4\}$. Given such a requirement, the existing secret image sharing schemes cannot solve this problem, but we believe that the applications of secret image sharing with adversary structure have good prospects.

To the best of our knowledge, very few papers have discussed secret image sharing with an adversary structure. So, in this paper, we have proposed for the first time a secret image sharing

scheme that can achieve both an adversary structure and a (t, n) threshold. First, we studied the characterization of the adversary structure, and, based on the existing (t, n) threshold schemes and our knowledge of the adversary structure, we proposed a new secret image sharing scheme that can achieve both an adversary structure and the (t, n) threshold. That is, t or more shadow images can cooperate to retrieve the secret image without distortion, but the subsets in the adversary structure cannot reveal it. In our scheme, the shadow images are generated by embedding secret data into the cover image, and, also, an array is computed for each participant according to the adversary structure. Then, the dealer distributes the corresponding shadow image and the array to each participant. The experimental results demonstrated that our scheme achieved the requirements of the adversary structure and the (t, n) threshold. In addition, the quality of the shadow image and the embedding capacity of our scheme also were satisfactory.

The novel characteristic of the proposed scheme is not available in the existing secret image sharing mechanisms, so the proposed scheme has the potential to work in many applications. The key features of our proposed secret image sharing scheme are summarized below:

(1) The proposed scheme can achieve both the adversary structure and the (t, n) threshold.
(2) The shared secret image can be reconstructed losslessly.
(3) The scheme can solve the overflow and underflow problems.
(4) The shadow images are meaningful, and the visual quality of the shadow images is satisfactory.

The rest of the paper is organized as follows. In Section 2, we briefly introduce the correlative definitions about access structure and adversary structure. The proposed secret image sharing scheme is presented in Section 3. Section 4 presents some experimental results and analysis. Our conclusions are given in Section 5.

2 Definitions

Let $P = \{P_1, P_2, \ldots, P_n\}$ be the set of participants. The qualified subset of P means participants in this subset can cooperate to reveal the secret image. The set of all of these qualified subsets is called the access structure on P. On the contrary, the participants in the unqualified subset of P, all of which comprise the adversary structure on P, cannot reveal the secret image. Their concepts are defined as follows:

Definition 1 Access structure: Γ is the access structure on P, and $\Gamma = \{A|A$ is the qualified subset of $P\}$. And the elements in Γ must satisfy this condition: if $A \in \Gamma, A \subseteq B \subseteq P$, then $B \in \Gamma$ can be deduced.

Definition 2 Adversary structure: Λ is the adversary structure on P, and $\Lambda = \{A|A$ is the unqualified subset of $P\}$. And the elements in Λ must satisfy this condition: if $A \in \Lambda, B \subseteq A \subseteq P$, then, $B \in \Lambda$ can be deduced.

Obviously, if $A \in \Gamma$, the supersets of A all belong to Γ, which means the access structure is increased monotonously. In contrast, the adversary is decreased monotonously. So, the minimal access structure and the maximal adversary structure must exist, in which one element does not contain other elements. The concepts of maximal adversary structure in set theory can be defined as follows:

Definition 3 [18] Minimal access structure: if $\Gamma_{\min} \subseteq \Gamma$, and $\Gamma_{\min} = \{A | \text{if } A' \subseteq A \subseteq P, \text{ then } A' \notin \Gamma_{\min}\}$, then $\Gamma_{\min}$ is the minimal access structure on P.

Definition 4 [18] Maximal adversary structure: if $\Lambda_{\max} \subseteq \Lambda$, and $\Lambda_{\max} = \{A | \text{if } A \subseteq A' \subseteq P, \text{ then } A' \notin \Lambda_{\max}\}$, then $\Lambda_{\max}$ is the maximal adversary structure on P.

The above definitions show that, if each subset does not contain another subset in an adversary structure, then the adversary structure is the maximal adversary structure. The maximal adversary structure $\Lambda_{\max}$ is a subset of the adversary structure Λ. And Λ can be determined by $\Lambda_{\max}$, which is more concise than Λ. So, we will use the maximal adversary structure instead of the adversary structure in our scheme. In order to better illustrate the definition of maximal adversary structure, let $P = \{P_1, P_2, P_3, P_4\}$ denote the set of participants and let $\Lambda = \{\{P_1, P_2, P_4\}, \{P_1, P_2\}, \{P_1, P_4\}, \{P_2, P_4\}, \{P_2, P_3\}, \{p_1\}, \{p_2\}, \{p_3\}, \{p_4\}\}$ be the adversary structure on P. Then, according to the definition of the maximal adversary structure, we can get the corresponding maximal adversary structure $\Lambda_{\max} = \{\{P_1, P_2, P_4\}, \{P_2, P_3\}\}$. That is, the maximal adversary structure $\Lambda_{\max} = \{\{P_1, P_2, P_4\}, \{P_2, P_3\}\}$ contains all elements of the adversary structure $\Lambda = \{\{P_1, P_2, P_4\}, \{P_1, P_2\}, \{P_1, P_4\}, \{P_2, P_4\}, \{P_2, P_3\}, \{P_1\}, \{P_2\}, \{P_3\}, \{P_4\}\}$.

3 The proposed scheme

3.1 The initialization phase

In this section, we construct a secret image sharing scheme with both an adversary structure and a (t, n) threshold. So, first, we define the maximal adversary structure and initialize some parameters. Let $P = \{P_1, P_2, \ldots, P_n\}$ denote the set of n participants, $S = \{S_1, S_2, \ldots, S_n\}$ denote the corresponding set of shadow images, and $\Lambda_{\max} = \{A_1, A_2, \ldots, A_m\}$ denote the maximal adversary structure on P. Each shadow image S_i is distributed to the relative participant P_i. Obviously, there are m subsets in $\Lambda_{\max}$, and each subset contains at least t shadow images. If $|A|$ denotes the number of participants in subset A of P, the requirements of our secret image sharing scheme are as follows:

(1) If $|A| \geq t$ and $A \not\subset A_r (r = 1, 2, \ldots, m)$, then the participants in A can cooperate to reveal the shared secret image.
(2) If $|A| \leq t$ or $A \subseteq A_r (r = 1, 2, \ldots, m)$, then the shadow images in A cannot reveal the shared secret image.

In addition, the dealer also should initialize some other important parameters as follows:

Step 1. Select a large prime modulus, p.
Step 2. Choose m different positive integers, $d_1, d_2, \ldots, d_m$, that can satisfy $1 \leq d_1 + d_2 + \cdots + d_m \leq p - 255$, and compute d as follows:

$$d = d_1 + d_2 + \cdots + d_m. \tag{1}$$

Step 3. Construct n identical arrays, $H_i = \{d_1, d_2, \ldots, d_m\}, i = 1, 2, \ldots, n$.

For example, there is a (3, 4) threshold system in which $P = P_1, P_2, P_3, P_4$. Assume the adversary structure on P is $\Lambda_{\max} = \{A_1, A_2\}$, where $A_1 = \{P_1, P_2, P_3\}, A_2 = \{P_2, P_3, P_4\}$. Then, the dealer will

generate the shadow images $S = \{S_1, S_2, S_3, S_4\}$. The dealer initializes prime $p = 1021$ and the positive integers $d_1 = 121$, $d_2 = 589$, then $d = 121 + 589 = 710$, $H_i = \{121, 589\}$, $i = 1, 2, 3, 4$.

3.2 Secret image sharing phase

In this phase, we describe how to generate the shadow images from the cover image and the shared secret image. The procedure consists of two phases, i.e., (1) the sharing phase and (2) the embedding and distribution phase.

3.2.1 Sharing phase

For convenience, assume that $s_1, s_2, \ldots, s_t$ denotes the shared pixels of the secret image *SI*, which is a grayscale image. And the cover image $O = \{O_i | i = 1, 2, \ldots, (M \times N)\}$ is an $M \times N$ grayscale image. Thus, the dealer can perform the following steps:

Step 1. With the values of $s_1, s_2, \ldots, s_t$ and d, $c_1, c_2, \ldots, c_t$ can be computed as:

$$c_k = s_k + d, (k = 1, 2, \ldots, t). \tag{2}$$

Step 2. Construct a $(t-1)$ degree polynomial, $F(x)$, where p is a large prime number selected in the initialization phase.

$$F(x) = c_1 + c_2 x + \ldots + c_t x^{t-1} \bmod p. \tag{3}$$

Step 3. Compute the corresponding shadow data y_i as $y_i = F(i)$ for all of the shadow images $S_i (i = 1, 2, \ldots, n)$ by entering the integer i into $F(x)$.

For convenience, assume that there are four secret image pixels, s_1, s_2, s_3, s_4, which are 156, 183, 127, 83. The dealer computes c_1, c_2, c_3, c_4 as866, 893, 837, 793, and $F(x)$ can be formulated as $F(x) = 866 + 893x + 837x^2 + 793x^3 \bmod 1021$. Then, the shadow y_i can be computed by entering the integer i, such as $y_1 = F(1) = 326$.

3.2.2 Embedding and distribution phase

As stated earlier, most secret image sharing schemes utilize the modulus operation to embed the shadow data y_i into the corresponding cover image pixels in order to conceal the existence of the embedded secret image and improve the visual quality of the shadow images. In our scheme, we construct the polynomial $F(x)$ in a finite field, $GF(p)$, where p is a large prime number. Therefore, we cannot use those methods directly. However, note that the scheme of Lin and Chan [10] utilizes a quantization operation to embed the secret data, and the quality of the shadow images in their scheme is satisfactory. So, we also use the quantization operation to generate shadow images. In this phase, the dealer will perform the following steps:

Step 1. Choose the appropriate parameters K and σ, which must ensure that $\lfloor 255/K \rfloor \times K + \sigma \leq 255$.

Step 2. Convert each y_i into the σ -ary notational system and get the secret data $y_{i1} y_{i2} \ldots y_{ia}$, where the value of a is computed as:

$$a = \lceil \log_{\sigma} p \rceil. \tag{4}$$

Step 3. Assume that the corresponding pixels of cover image, O, which are utilized to embed the value $y_{i1}y_{i2}\ldots y_{ia}$, are $o_i, o_{i+1}, \ldots, o_{i+a-1}$. And, $q_{i1}, q_{i2}, \ldots, q_{ia}$ are the camouflaged pixels. The value of q_{i+j} can be computed as follows:

$$q_{ij} = \lfloor O_{i+j-1}/K \rfloor \times K + y_{ij}, 1 \le j \le a. \tag{5}$$

Step 4. Repeat the above processes until the shadow images are generated completely. Finally, the shadow images are sent to the corresponding participants.

The dealer also performs the following steps to achieve the adversary structure.

Step 1. For all of the shadow images $S_i (i = 1, 2, \ldots, n)$ in S, if $S_i \in A_j (j = 1, 2, \ldots, m)$, then delete d_j from $H_i = \{d_1, d_2, \ldots, d_m\}$.

Step 2. Send the reminding elements of H_i over a secure channel, which is important for the security of our scheme.

Considering the above example, assume that the dealer chooses $K = 8$, $\sigma = 7$ and that the cover image pixels $o_0 = 234, o_1 = 157, o_2 = 183, o_3 = 89$ are utilized to embed the shadow values. The dealer will convert y_1 into a 7-ary notational system as $y_1 = 326 = (0, 6, 4, 4)_7$. Then, the stego pixels are $q_{11} = \lfloor 234/8 \rfloor \cdot 8 + 0 = 232$, $q_{12} = \lfloor 157/8 \rfloor \cdot 8 + 6 = 158$, $q_{13} = \lfloor 183/8 \rfloor \cdot 8 + 4 = 180$, and $q_{14} = \lfloor 89/8 \rfloor \cdot 8 + 4 = 92$. All stego pixels can be obtained by repeating the above steps. Figure 1 shows the flowchart of our secret image sharing scheme. The array of each participant can be generated as $H_1 = \{589\}$, $H_2 = \{\}$, $H_3 = \{\}$, $H_4 = \{121\}$.

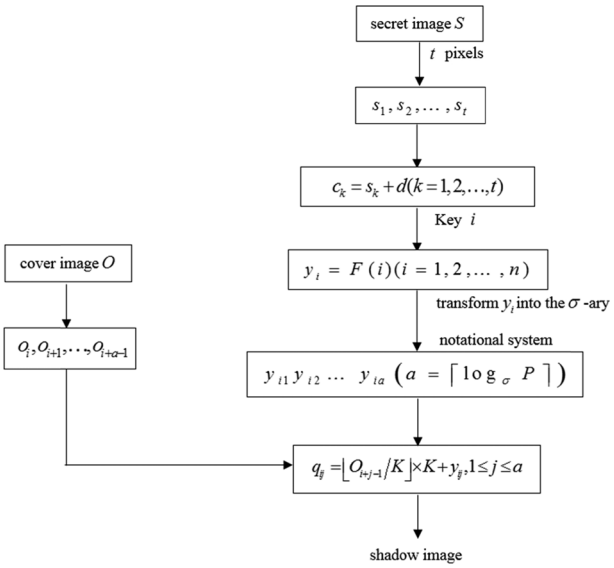


Fig. 1 Diagram of the secret image sharing scheme

3.3 Secret image retrieving phase

For the collection of participants A, the participants can share their shadow images and cooperate to reconstruct the shared secret image SI if, and only if, $|A| \geq t$ and $A \not\subset A_r (r = 1, 2, \ldots, m)$. Otherwise, they can get no information about the secret image. So, assume that the set A contains t participants and $A \not\subset A_r (r = 1, 2, \ldots, m)$. Thus, the participants in A can cooperate to reveal the secret image. For convenience, assume that $q_{i1}', q_{i2}', \ldots, q_{ia}'$ are a pixels of P_i's shadow image S_i, where $P_i \in A$, $1 \leq i \leq n$. Then, the participants in A can complete the following steps to reveal the corresponding secret image pixels $s_1', s_2', \ldots, s_t'$:

Step 1. Each participant P_i in A sends her or his shadow image S_i and array H_i to the designated combiner (DC), who may be a reliable participant in A or someone else.

Step 2. According to the shadow image from each participant P_i in A, the DC can utilize the modulo operation to obtain the corresponding $y_{ij}' (1 \leq j \leq a)$ as:

$$y_{ij}' = q_{ij}' \bmod K \tag{6}$$

Step 3. The DC concatenates $y_{iz}' (1 \leq z \leq a)$, which are obtained in Step 1, to get y_i'. The DC transforms y_i' into decimal representation.

Step 4. With t pairs of (i, y_i'), the polynomial $F(x)$ can be reconstructed by Lagrange's interpolation formula:

$$F(x) = c_1 + c_2 x + \cdots + c_t x^{t-1} \bmod p. \tag{7}$$

And, thereby, the DC can obtain $c_1, c_2, \ldots, c_t$ by extracting the coefficients of $F(x)$.

Step 5. With all H_i from the participants in A, the DC deletes the redundant d_l, for $l = 1, 2, \ldots, m$ and just keeps one for each different d_l. Then, the value of d can be computed as:

$$d = d_1 + d_2 + \cdots + d_m. \tag{8}$$

Step 6. With $c_1, c_2, \ldots, c_t$ and d, the DC can get the corresponding secret image pixels $s_1', s_2', \ldots, s_t'$ as follows:

$$\begin{aligned} s_1' &= c_1 - d \\ s_2' &= c_2 - d \\ &\vdots \\ s_t' &= c_t - d. \end{aligned} \tag{9}$$

By repeating these processes, the secret image SI can be reconstructed without distortion.

Assume the participants P_1, P_3, P_4 want to cooperate to reconstruct the secret image. We will describe how they get the secret pixels s_1, s_2, s_3, s_4 in the above example. The coefficients $c_1 = 866, c_2 = 893, c_3 = 837, c_4 = 793$ can be obtained by using Lagrange's interpolation formula, because the threshold requirement is satisfied. With all H_1, H_3, H_4 of participants P_1, P_3, P_4, the value of d can be computed as $d = 121 + 589 = 710$. With c_1, c_2, c_3, c_4 and d, s_1, s_2, s_3, s_4 can be computed as $s_1 = 866 - 710 = 156, s_2 = 893 -$

(a) Bird (b) Woman (c) Lake (d) Man (e) Tiffany

(f) Peppers (g) Lena (h) Fruits (i) Baboon (j) Airplane

(k) Couple (l) Crowd (m) Cameraman (n) Boat (o) House

Fig. 2 The test images

$710 = 183$, $s_3 = 837 - 710 = 127$, $s_4 = 793 - 710 = 83$. If the participants P_1, P_3, P_4 want to reveal the secret image, they can get c_1, c_2, c_3, c_4. However, they cannot get d for the lock of $d_2 = 589$. So P_1, P_3, P_4 cannot reveal s_1, s_2, s_3, s_4.

4 Experimental results and analysis

In this section, we demonstrate the characteristics of our proposed scheme by conducting simulations and analyzing their results.

To estimate the quality of the shadow images, we use the peak signal-to-noise ratio (PSNR) to measure the distortion of the shadow images, which is defined as:

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \text{ dB}. \tag{10}$$

And, the mean square error (MSE) of an image with $M \times N$ pixels is defined as:

$$MSE = \frac{1}{M \times N}\sum_{j=1}^{M\times N}\left(p_j - p_j^{'}\right)^2, \tag{11}$$

where p_j is the original pixel value and $p_j^{'}$ is the pixel value of the shadow image.

4.1 Simulation results

We performed experiments for $n = 8$ and $t = 4$. For the set of all participants $P = \{P_1, P_2, \ldots, P_8\}$, we designed the specific maximal adversary structure $\Lambda_{\max} = \{A_1, A_2, A_3\}$, where $A_1 = \{P_1, P_3, P_5, P_7\}$, $A_2 = \{P_1, P_2, P_4, P_5\}$ and $A_3 = \{P_2, P_5, P_7, P_8\}$. So, the secret image can be reconstructed without distortion if, and only if, the set A, which is the subset of P, contains at least four participants and $A \not\subset A_r (r = 1, 2, 3)$.

In these experiments, we used 15 grayscale images with sizes of 512×512 pixels as the test images, as shown in Fig. 2, and the secret image 'Airplane' was set to 256×256 pixels, as shown in Fig. 3.

We chose $p = 1021$, $d_1 = 219$, $d_2 = 352$ and $d_3 = 127$ in the initialization phase in our experiments. And, as stated earlier, we used the quantization operation to embed the secret data in the embedding and distribution phases. So, we must select the appropriate K and σ to guarantee both the quality of the shadow image and the embedding capacity. We performed our experiments for $K = 8$ and $\sigma = 7$, and Table 1 shows the PSNR of the shadow images with various test images.

Generally speaking, it is difficult for people to distinguish the original image from the shadow image if the PSNR of the shadow image is more than 35 dB. Table 1 shows that the PSNR values of the shadow images in our experiments were about 44–45. So, the quality of the shadow images is satisfactory in our scheme. In addition, we used Lena as the cover image and Airplane as the secret image to demonstrate the visual perception of the shadow images in our scheme. And the shared secret image can be reconstructed losslessly by any eligible subset of shadow images. Figure 4a and b show the cover image and the reconstructed secret image, respectively.

Figure 5 shows the corresponding eight shadow images for the cover image, Lena. So, judging from the visual perception of these shadow images, our scheme can successfully camouflage shadow images from intruders.

An array H_i is distributed to each participant $P_i (i = 1, 2, \ldots, 8)$ in order to develop the adversary structure, and H_i is constructed according to the maximum adversary structure $\Lambda_{\max} = \{A_1, A_2, A_3\}$. Table 2 shows H_i, which is distributed to P_i in the experiments. So, if

Fig. 3 The secret image

Table 1 PSNR of shadow images (dB)

Test images	Shadow Image1	Shadow image2	Shadow image3	Shadow image4	Shadow image5	Shadow image6	Shadow image7	Shadow image8
Bird	44.38	43.95	44.13	44.13	44.13	44.12	44.10	44.15
Woman	44.29	44.89	44.10	44.10	44.08	44.08	44.09	44.08
Lake	44.25	43.85	44.07	44.02	44.04	44.01	44.00	44.05
Man	44.36	43.98	44.17	44.16	44.14	44.16	44.15	44.15
Tiffany	44.33	44.95	44.14	44.15	44.12	44.12	44.14	44.13
Peppers	44.30	43.89	44.09	44.10	44.08	44.06	44.07	44.07
Lena	44.34	43.94	44.11	44.11	44.14	44.09	44.12	44.12
Fruits	44.21	43.83	44.03	44.00	44.03	44.99	44.03	44.02
Baboon	44.32	43.96	44.10	44.14	44.10	44.08	44.10	44.14
Airplane	44.28	43.88	44.05	44.09	44.05	44.07	44.06	44.07
Couple	44.26	43.88	44.08	44.09	44.11	44.07	44.09	44.09
Crowd	44.24	43.81	44.01	44.01	44.03	44.00	44.02	44.01
Cameraman	44.50	44.14	44.27	44.29	44.28	44.28	44.31	44.30
Boat	44.27	43.87	44.07	44.08	44.06	44.02	44.04	44.06
House	44.28	44.79	44.06	44.05	44.03	44.00	44.06	44.03
Average	44.23	44.04	44.02	44.03	44.03	44.07	44.02	44.03

the subsets of participants are in the adversary structure, they cannot get all d_1, d_2, d_3 at the same time. Thus, neither can they cooperate to reconstruct the secret image.

4.2 Security and correctness analysis

To prove the validity of our scheme, the concept of reconstruction property and confidentiality property are introduced.

Definition 5 Reconstruction property: if all qualified subsets of participants can reveal the secret image, then the secret image scheme satisfies the reconstruction property.

Fig. 4 Cover image and the extracted secret image

(a) The cover image (b) The extracted secret image

Fig. 5 Shadow images

Definition 6 Confidentiality property: if all unqualified subsets of participants cannot reveal the secret image, then the secret image scheme satisfies the confidentiality property.

If, and only if, a secret image scheme satisfies both the reconstruction property and the confidentiality property, can it be called a valid secret image scheme. So, we will prove that our scheme has both the reconstruction property and the confidentiality property. For convenience, let us assume that subset A of the participants is composed of at least t participants and $A \not\subset A_r (A_r \in \Lambda_{\max},\ r = 1, 2, \ldots, m)$, where $\Lambda_{\max}$ is the maximal adversary structure. We will prove our scheme is valid as follows:

(1) Our scheme satisfies the reconstruction property.

Table 2 Array H of participants

Participant	H
P_1	$H_1 = \{d_3\} = \{127\}$
P_2	$H_2 = \{d_1\} = \{219\}$
P_3	$H_3 = \{d_2, d_3\} = \{352, 127\}$
P_4	$H_4 = \{d_1, d_3\} = \{219, 127\}$
P_5	$H_5 = \{\}$
P_6	$H_6 = \{d_1, d_2, d_3\} = \{219, 352, 127\}$
P_7	$H_7 = \{d_2\} = \{352\}$
P_8	$H_8 = \{d_1, d_2\} = \{219, 325\}$

Table 3 Relationship of the capacity-distortion for different values of σ

K	σ	$log_{\sigma}P$	Capacity(pixels)	PSNR(dB)
8	7	4	$H \times W \times t/4$	44.06
8	6	4	$H \times W \times t/4$	44.46
8	5	5	$H \times W \times t/5$	42.84
8	4	5	$H \times W \times t/5$	42.94
8	3	7	$H \times W \times t/7$	40.65

Proof. If the subset A is a qualified subset of participants, it must satisfy $A \not\subset A_r$ and $|A| \geq t$. Because $A \not\subset A_r$, the participants in A can get $d_1, d_2, \ldots, d_m$, and they can compute d by using Eq. (8). Also, $c_1, c_2, \ldots, c_t$ can be extracted from the coefficients of $F(x)$ because $|A| \geq t$. Then, the participants can get the corresponding pixels of the secret image according to Eq. (9). By repeating this process, the secret image can be reconstructed. Figure 4b shows that the secret image was reconstructed without distortion.

(2) Our scheme satisfies the confidentiality property.

Proof. If subset A is an unqualified subset of participants, it must satisfy $|A| < t$ or $A \in \Lambda_{\max}$. If $|A| < t$, the participants in A cannot reconstruct the (t-1) degree polynomial, $F(x)$, through Lagrange interpolation, so they cannot get $c_1, c_2, \ldots, c_t$ and cannot reconstruct the secret image. If $A \in \Lambda_{\max}$, let us assume that $A \subseteq A_r (r = 1, 2, \ldots, m)$. Because all of the participants in A do not possess d_r in their own array H_r, they cannot get the true value of d according to Eq. (1). So, even though they can get c_1, $c_2, \ldots, c_t$, they cannot reveal the secret image.

Table 4 Comparisons of the related secret image sharing schemes

Functionality	Yang et al. [29]	Lin et al. [11]	Lin and Chan [10]	Guo et al. [4]	Ours
Adversary structure	No	No	No	No	Yes
(t, n)-threshold	Yes	Yes	Yes	No	Yes
Meaningful shadow image	Yes	Yes	Yes	Yes	Yes
Quality of shadow image	41 dB	43 dB	42 dB	38 dB	44 dB
Lossless secret image	Yes	Yes	Yes	Yes	Yes
Lossless cover image	Yes	Yes	Yes	No	No
Maximum capacity	$\frac{M \times N}{4}$	$(t-3)\frac{\times M \times N}{3}$	$^{(t-1)}\times M \times N/_{\lceil \log_{\sigma} p \rceil}$	$\lfloor {}^{M \times N}/_{\max\{r_i\}} \rfloor \times t_m$	${}^{t \times M \times N}/_{\lceil \log_{\sigma} p \rceil}$

4.3 Discussion

Since our scheme is a secret image sharing scheme, the embedding capacity and the quality of shadow images are the two main measurements. We will discuss them as follows. In our scheme, t secret image pixels are to be embedded into $\lceil \log_\sigma P \rceil$ cover image pixels. If the cover image has $H \times W$ pixels, the maximum embedding capacity of our scheme would be $t \times H \times W / \lceil \log_\sigma p \rceil$. From the value of the maximum embedding capacity, we can see that the larger the value σ is, the higher the maximum embedding capacity is. However, the value of σ also affects the quality of the shadow images. Concerning the two different values of σ, the smaller σ can make the quality of the shadow images better if the values of $\lceil \log_\sigma p \rceil$ are the same. However, the smaller σ may reduce the quality of the shadow images since the values of $\lceil \log_\sigma p \rceil$ are different. Thus, we must select an appropriate value of σ to make a tradeoff between the embedding capacity and the quality of the shadow images. Table 3 shows the embedding capacity and distortion for different values of σ. As Table 3 shows, we can choose a smaller σ to guarantee better quality of the shadow image when the capacities are the same.

In Table 4, we compared our scheme with other related schemes (Yang et al. [29]; Lin et al. [11]; Lin and Chan [10]; Guo et al. [4]). Table 4 indicates that our scheme can reconstruct the secret image losslessly and that the PSNRs of the shadow images are the maximum among all of these schemes for the same embedding capacity, which was 256×256 pixels. This means that the quality of the shadow images in our scheme is satisfactory. At the same time, if we choose appropriate values for K and σ, the maximum capacity of our scheme also is satisfactory. In addition, even though all of the schemes are (t, n) threshold secret image sharing schemes, only our scheme achieves the adversary structure. So, the proposed scheme can be used in applications that require both the adversary structure and the (t, n) threshold.

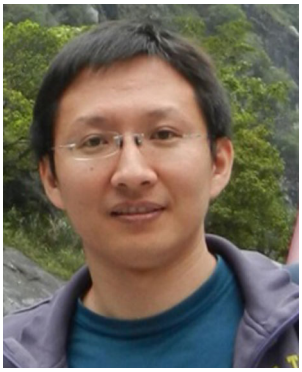
5 Conclusions

In this paper, we proposed for the first time a secret image sharing scheme that can achieve both an adversary structure and a (t, n) threshold. In our scheme, we calculated the shadow images in a finite field of size p, which is a large prime number, in order to achieve the adversary structure. And we used the quantization operation to embed the secret data into the cover image's pixels based on the scheme of Lin and Chan [10]. The secret image can be revealed without any distortion if, and only if, the participants involved satisfy the threshold requirement and the subsets of participants are not in the adversary structure. The experimental results indicated that our scheme can achieve both high-quality shadow images and high embedding capacity.

Acknowledgments This paper is supported by the National Science Foundation of China under grant No. 61401060, 61501080 and 61572095, the general program of Liaoning Provincial Department of Education Science Research under grants L2014017, and the Fundamental Research Funds for the Central Universities' under No. DUT16QY09.

References

1. Benaloh J, Leichter J (1989) Generalized secret sharing and monotone functions, Proc. Crypto'88, Lecture Notes in Computer Science. Springer, Berlin, pp 213–222
2. Blakley GR (1979) Safeguarding cryptographic keys. Proc AFIPS Natl Comput Conf 48:313–317
3. Chang CC, Lee HC (1993) New generalized group-oriented cryptoscheme without trusted centers. J IEEE J Sel Areas Commun 11(5):725–729
4. Guo C, Chang CC, Qin C (2012) A hierarchical threshold secret image sharing scheme. J Pattern Recognit Lett 33(1):83–91
5. Guo C, Chang CC, Qin C (2012) A multi-threshold secret image sharing scheme based on MSP. J Pattern Recognit Lett 33(12):1594–1600
6. Guo C, Chang CC, Qin C (2014) A novel (n, t, n) secret image sharing scheme without a trusted third party. Multimed Tools Appl 72(3):2195–2209
7. Guo C, Zhang H, Song QQ, Li MC (2015) A multi-threshold secret image sharing scheme based on the generalized Chinese remainder theorem. Multimed Tools Appl. doi:10.1007/s11042-015-2885-x, **Online 20 August 2015**
8. Ito M, Saito A, Nishizeki T, (1987) Secret sharing schemes realizing general access structure. Proc. IEEE Global Telecommunication Conference, IEEE Press, New Jersey, pp. 99–102
9. Li J, Li XL, Yang B et al (2015) Segmentation-based image copy-move forgery detection scheme. IEEE Trans Inf Forensic Secur 10(3):507–518
10. Lin PY, Chan CS (2010) Invertible secret image sharing with steganography. J Pattern Recognit Lett 31(13): 1887–1893
11. Lin PY, Lee JS, Chang CC (2009) Distortion-free secret image sharing mechanism using modulus operator. J Pattern Recognit 42(5):886–895
12. Lin CC, Tsai WH (2004) Secret image sharing with steganography and authentication. J Syst Softw 73(03):405–414
13. Lin YY, Wang RZ (2010) Scalable secret image sharing with smaller shadow images. J IEEE Signal Process Lett 17(3):316–319
14. Ma J, Guo Y (2004) Practical secret sharing scheme realizing generalized adversary structure. J Comput Sci Technol 19(4):564–569
15. Ma TH, Zhou JJ, Tang ML et al (2015) Social network and tag sources based augmenting collaborative recommender system. IEICE Trans Inf Syst E98-D(4):902–910
16. Naor M, Shamir A (1995) Visual cryptography. Advances in cryptology, Proc. Eurocrypt'94. Spring-Verlag, Berlin, pp 1–12
17. Pang L, Jiang Z, Yumin AW (2006) Multi-secret sharing scheme based on the general access structure. J Comput Res Dev 43(1):33–38
18. Qin H, Dai Y, Wang Z (2009) A secret sharing scheme based on (t, n) threshold and adversary structure. J Int J Inf Secur 8(5):379–385
19. Ren YJ, Shen J, Wang J et al (2015) Mutual verifiable provable data auditing in public cloud storage. J Internet Technol 16(2):317–323
20. Shamir A (1979) How to share a secret. Commun ACM 22(11):612–613
21. Shyu SJ, Chen YR (2008) On secret multiple image sharing," proc. The 25th workshop on combinatorial mathematics and computation theory. Chung-Hwa University, Hsinchu, pp 24–25
22. Tan KJ, Zhu HW (1999) General secret sharing scheme. J Comput Commun 22(8):755–757
23. Thien CC, Lin JC (2003) An image-sharing method with user-friendly shadow images. J IEEE Trans Circ Syst Video Technol 13(12):1161–1169
24. Wang RZ, Su CH (2006) Secret image sharing with smaller shadow images. J Pattern Recog Lett 27(6):551–555
25. Xia ZH, Wang XH, Sun XM et al (2015) A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data. IEEE Trans Parallel Distrib Syst 27(2):340–352
26. Xia Z, Wang X, Sun X, Xiong N (2014) Steganalysis of least significant bit matching using multi-order differences. J Secur Commun Netw 7(8):1283–1291
27. Xia Z, Wang X, Sun X, Xiong N (2016) Steganalysis of LSB matching using differences between nonadjacent pixels. J Multimed Tools Appl 75(4):1–16
28. Yang CN (2004) New visual secret sharing schemes using probabilistic method. J Pattern Recog Lett 25(4): 481–494
29. Yang CN, Chen TS, Yu KH, Wang CC (2007) Improvements of image sharing with steganography and authentication. J Syst Softw 80(7):1070–1076
30. Zhao D, Peng H, Wang C, Yang Y (2012) A secret sharing scheme with a short share realizing the (t, n) threshold and the adversary structure. J Comput Math Appl 64(4):611–615



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, cryptology and cloud security.

QiongQiong Yuan is currently pursuing his M.S. degree in the School of Software Technology at the Dalian University of Technology, Dalian, China. His research interests include information security, cloud security and cryptology.

Kun Lu received the B.S. degree in 2002 and the M.S degree in Computer Science and Technology in 2005 both from Dalian University of Technology, Dalian, China. From 2005 to now, he worked for School of Software Technology of Dalian University of Technology as a Lecture. Since 2010, he is currently pursuing his PhD degree in computer software and theory from the Dalian University of Technology. His research interests include information security, distribute system, reputation system.

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.

Zhangjie Fu received his Ph.D. in computer science from the College of Computer, Hunan University, China, in 2012. He is currently an Associate Professor at the College of Computer and Software, Nanjing University of Information Science and Technology, China. His research interests include Cloud & Outsourcing Security, Digital Forensics, Network and Information Security. His research has been supported by NSFC, PAPD, and GYHY. Zhangjie is a member of IEEE, and a member of ACM.