Research Article

Secret Image Sharing Scheme with Threshold Changeable Capability

Lifeng Yuan,^{1,2} Mingchu Li,^{1,2} Cheng Guo,^{1,2} Weitong Hu,³ and Xinjian Luo^{1,2}

¹School of Software Technology, Dalian University of Technology, Dalian 116620, China

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

³School of Computer and Technology, Hangzhou Dianzi University, Hangzhou 310018, China

Correspondence should be addressed to Cheng Guo; guocheng@dlut.edu.cn

Received 27 January 2016; Accepted 22 May 2016

Academic Editor: Nazrul Islam

Copyright © 2016 Lifeng Yuan et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In secret image sharing schemes, the threshold may have to be adjusted in case of changes in the security policy and the adversary structure before recovering the secret image. For example, if participants leave the group, their stego images are useless to them and may not be kept safely. As a result, these images can be easily stolen and utilized by intruders, which reduces the security of the scheme. To solve this problem, we propose a novel threshold changeable secret image sharing scheme with N potential changeable thresholds $t_1, t_2, \dots, t_N$. By preparing advance shares for thresholds $t_1, t_2, \dots, t_N$ and using the two-variable one-way function to generate the identification value, we can change the threshold when necessary. The experiments show that the quality of the stego images in our scheme is satisfactory and the secret image can be recovered without distortion. Moreover, the security analysis shows that we can change the threshold safely.

1. Introduction

The rapid development of Internet has brought much more convenience to people's daily lives, but it has also brought security risks. In the open communication networks, it is easy to intercept, modify, fabricate, and even destroy data. Modern cryptography provides an effective solution to ensure the security of information. Since the design details of most cryptography algorithms are public, the security of the encrypted information depends on the security of the key. Thus, it is important that the key be kept safely.

In order to solve this secret key protecting problem, Shamir [1] and Blakley [2] proposed (t, n) threshold secret sharing schemes independently. Shamir constructed his scheme based on polynomial interpolation, while Blakley provided a geometric construction. In a (t, n) threshold secret sharing scheme, a dealer encodes and divides the secret into n shares that are distributed to n participants, and then t or more participants can recover the secret, but less than t participants cannot get any information about the secret. In 1994, Naor and Shamir [3] proposed a visual secret image

sharing scheme. Utilizing the (t, n) threshold secret sharing technique, the secret image is encoded and divided into n random-noise-like images (called share images), and these share images are distributed to the participants, so that any t or more participants can see the secret image by stacking their share images together. However, the random-noise-like images, which are meaningless, can easily attract malicious intruders' attention. To solve this problem, Lin and Tsai [4] provided a (t, n) threshold image sharing scheme using steganography. In their scheme, the shares are camouflaged in a cover image to form the stego images, which cannot be distinguished by the human eye, so these shares can be concealed from intruders. At the same time, their scheme embeds watermarks into the stego images for verification.

In recent years, various secret image sharing techniques have been developed rapidly. In 2007, Yang et al. [5] proposed an image sharing scheme that can improve the authentication ability, but it degraded the quality of the stego images. In 2009, Lin et al. [6] utilized the modulo operation to camouflage the secret data in the cover image to overcome this drawback. Their scheme guarantees higher quality stego images, and

it can reconstruct the secret image and the cover image without distortion. In 2010, Lin and Chan [7] proposed an invertible secret image sharing scheme with satisfactory quality of the stego images. It can recover the secret image and the cover image without distortion, and it allows for a large capacity of secret data embedding. In reality, the single (t, n) threshold access structure cannot satisfy the demand of complex applications. To solve this problem, Guo et al. [8] first proposed a hierarchical secret image sharing, based on polynomial interpolation in 2012, which divided the secret share images into different hierarchies and set different threshold values. Also in 2012, Guo et al. [9] proposed another novel hierarchical secret image sharing scheme based on monotone span programs (MSPs). In 2013, Ulutas et al. [10] proposed an invertible secret image sharing scheme using modification direction and the modulo operation. Their scheme can improve the quality of the stego images effectively when grey-scale cover image is used, and it can also obtain acceptable quality stego images when dithered cover image is used. In 2014, Pakniat et al. [11] used cellular automata and Birkhoff interpolation to propose a novel secret image sharing scheme with hierarchical threshold access structure. In this scheme, each authorized subset of participants is able to recover the secret image and the cover image without distortion, and they can also check the validity of the secret image.

Before recovering the secret image, the security policies and adversary structures may change, so it may be necessary to adjust the threshold. For example, (1) the importance level of the secret image is increased or decreased; (2) some participants join or leave the group; (3) the mutual trust of participants is strengthened or weakened; (4) the adversary might have corrupted more than $n - t$ participants. Currently, there is not a secret image sharing scheme that can change the threshold after distributing the stego images and before recovering the secret image. Therefore, it is necessary to set up a changeable threshold secret image sharing scheme.

Currently, many researchers are interested in secret sharing schemes, especially threshold changeable secret sharing schemes. In 1991, Lai et al. [12] proposed the first threshold changeable secret sharing scheme. In recent years, some researchers have been developing threshold changeable secret sharing schemes based on various techniques, such as (1) the share redistributing technique in [13–15]; (2) the lattice basis reduction technique in [16–18]; (3) the redundant shares technique in [19, 20]; and (4) the advance shares technique in [21]. In 1997, Desmedt and Jajodia [13] used the share redistributing technique to propose a threshold changeable secret sharing scheme without the dealer's participation after the initialization phase. Some similar schemes can be found in [14, 15]. In these schemes, if the threshold needs to be adjusted, each original share is split into smaller shares which are then redistributed to all participants in the new access structure. Each participant P_i can combine all received smaller shares into one new share s_i by a suitable linear combination; thus each participant only has to store s_i . Note that all participants must simultaneously keep mutual secure communication channels. However, this may be impractical when the threshold changes, especially in the event of an urgent threshold change, so many schemes based on

broadcasting have been proposed. In 1999, Martin et al. [22] provided a general model for threshold changeable secret sharing schemes and also provided two threshold schemes which were based on polynomial interpolation and geometric construction. In 2005, Barwick et al. [23] proposed a novel threshold changeable secret sharing scheme based on broadcasting, which can minimize the storage space required for secret sharing and limit the size of the broadcast information in low-bandwidth environment. In 2007, Steinfeld et al. [18] provided a lattice-based threshold changeable secret sharing scheme in which the threshold can be increased by partial updating of shares. In 2012, Zhang et al. [21] also proposed two threshold changeable secret sharing schemes. In their schemes, the advance shares, which have a one-to-one relationship with all potential thresholds, are prepared in the initialization phase, and then the new threshold can be validated by broadcasting related information.

Inspired by Zhang et al.'s work [21], we propose a novel $(\{t_1, t_2, \dots, t_N\}, n)$ threshold changeable secret image sharing scheme that can adjust the threshold to t_i ($1 \leq i \leq N$) dynamically by broadcasting information. Since the novel characteristic of our scheme is not available in the existing secret image sharing schemes, it has the potential to work in many applications. Our scheme has the following characteristics:

- (1) The quality of stego images is satisfactory, and the secret image can be recovered without distortion.
- (2) The problem with Zhang et al.'s scheme, that is, that the encrypted shares are too large to be camouflaged in the cover image to form the stego images, is solved by our scheme.
- (3) The threshold can be adjusted in case of changes in the security policy or the adversary structure, and our scheme remains secure after these changes are made.

The rest of this paper is organized as follows. We describe Shamir's secret sharing scheme and the two-variable one-way function in Section 2, and we present our novel $(\{t_1, t_2, \dots, t_N\}, n)$ threshold changeable secret image sharing scheme in Section 3. Our experiments, the performance of our scheme, and the security analysis are presented in Section 4. Section 5 presents our conclusions.

2. Preliminaries

This section describes the concept of Shamir's (t, n) threshold secret sharing scheme [1] and the two-variable one-way function.

2.1. Shamir's (t, n) Threshold Secret Sharing Scheme. Let $S = GF(q)$ be the secret domain, where q is a big prime number. Secret $s \in S$ is shared amongst n participants $P_1, P_2, \dots, P_n$ and t is the threshold value. Each participant gets a piece of secret called share. Then, t or more participants can cooperate to reconstruct the secret by polynomial interpolation, and less than t participants cannot get any information about the secret. Shamir's (t, n) secret sharing scheme [1] can work as follows.

Sharing Procedure. The dealer chooses n distinct and nonzero elements $x_1, x_2, \dots, x_n$ for the unique identifications of the participants, where $x_i \in GF(q)$, $1 \leq i \leq n$. The identification can be known by everyone. Then, the dealer constructs a $(t-1)$ -degree polynomial

$$f(x) = (s + a_1x^1 + a_2x^2 + \dots + a_{t-1}x^{t-1}) \mod q, \quad (1)$$

where $a_1, a_2, \dots, a_{t-1} \in GF(q)$ are randomly chosen. For all $1 \leq i \leq n$, the dealer computes share $y_i = f(x_i)$ and then sends it to corresponding participant P_i by secure communication channels. The values of the shares are limited to $[0, q-1]$.

Recovery Procedure. Without loss of generality, assume that t participants $P_1, P_2, \dots, P_t$ provide their shares. With t points $(x_1, y_1), (x_2, y_2), \dots, (x_t, y_t)$, polynomial $f(x)$ can be reconstructed as follows:

$$f(x) = \sum_{i=1}^t y_i \prod_{j=1, j \neq i}^t \frac{x - x_j}{x_i - x_j} \mod q. \quad (2)$$

Then, secret s can be recovered as $s = f(0)$.

2.2. Two-Variable One-Way Function. If each participant's share data generated according to the secret image is sent directly, it can easily attract malicious intruders' attention, because it is meaningless. To solve this problem, in our scheme, each participant's share data is camouflaged in a cover image to form corresponding stego image. Since each stego image and cover image cannot be distinguished by the human eye, each participant's share data can be concealed from intruders.

In Zhang et al.'s $(\{t_1, t_2, \dots, t_N\}, n)$ threshold changeable secret sharing scheme [21], they prepare advance shares for all potential changeable thresholds $t_1, t_2, \dots, t_N$ and encrypt the advance shares by the symmetric encryption algorithm in the sharing procedure. But their encrypted shares are too large to be camouflaged in the cover image. To solve this problem, we used the two-variable one-way function to generate the identification values, which are fed into the polynomial to generate the shares. The details will be given in Section 3. For the reader's convenience, we introduce the two-variable one-way function represented by Chien et al. [24] as follows.

Function $h(r, s)$ is a two-variable one-way function that can map variables r and s into a value with a fixed length. The features of $h(r, s)$ are as follows:

- (1) Given r and s , $h(r, s)$ is easy to calculate.
- (2) Given s and $h(r, s)$, it is not feasible to calculate r .
- (3) Given r and $h(r, s)$, it is not feasible to calculate s .
- (4) It is not feasible to calculate $h(r, s)$ for any r without s .
- (5) It is not feasible to calculate $h(r, s)$ for any s without r .
- (6) Given s , it is not feasible for r_1 and r_2 to satisfy $h(r_1, s) = h(r_2, s)$.
- (7) Given r , it is not feasible for s_1 and s_2 to satisfy $h(r, s_1) = h(r, s_2)$.
- (8) Given any pairs of $(r_i, f(r_i, s))$, it is not feasible to calculate $h(r_j, s)$ when $r_i \neq r_j$.

3. Proposed Scheme

Given a grey-scale secret image $S = \{p_1, p_2, \dots, p_{h_s \times w_s}\}$ with $h_s \times w_s$ pixels and a grey-scale cover image $C = \{c_1, c_2, \dots, c_{h_c \times w_c}\}$ with $h_c \times w_c$ pixels, the dealer can derive shares from S and generate n stego images $S_1, S_2, \dots, S_n$ for n participants $P_1, P_2, \dots, P_n$. Before recovering secret image S , if the security policy and adversary structure are changed, the threshold can be adjusted to a suitable threshold $t_j \in \{t_1, t_2, \dots, t_N\}$, where $t_1, t_2, \dots, t_N$ are potential thresholds, and the scheme can remain secure after these changes are made. Then, t_j or more participants can recover secret image S without distortion.

In our scheme, the pixels of S and C are read from left to right and from top to bottom. Assume that the dealer knows N potential thresholds $t_1, t_2, \dots, t_N$ to which the threshold may be changed in the future, and these thresholds satisfy the condition $0 < t_{i+1} - t_i < t_1$ ($1 \leq i \leq N-1$). This condition can be achieved easily by adding new potential thresholds to shorten the difference between the two potential thresholds. For a univariate polynomial $f(x) = \sum_{i \geq 0} a_i x^i$, the degree operator $\deg(\cdot)$ is used to compute the degree of the polynomial, and the coefficient operator $[x^d]$ is defined, such that $[x^d]f(x) = a_d$. Our threshold changeable secret image sharing scheme can be divided into two procedures, that is, sharing and recovery. These procedures are described as follows.

3.1. Sharing Procedure. In the sharing procedure, the dealer derives shares from secret image S and generates n stego images $S_1, S_2, \dots, S_n$ for n participants $P_1, P_2, \dots, P_n$. Figure 1 displays the flowchart of this procedure. We describe how to generate the shares in Section 3.1.1 and how to camouflage these shares into the cover image to form the stego images in Section 3.1.2.

3.1.1. Share Derivation. The dealer selects a prime number m , n distinct and nonzero random integers $x_1, x_2, \dots, x_n$ as the real identifications of n participants, and N distinct and nonzero random integers $K_1, K_2, \dots, K_N$ as the corresponding secret keys of potential thresholds $t_1, t_2, \dots, t_N$. To share secret image S , the dealer converts S into m -ary data (called converted data). The size of this converted data is $h_s \times w_s \times \lceil \log_m 255 \rceil$, where $\lceil \cdot \rceil$ is the ceiling function. For instance, we can assume that the chosen m is equal to 5, and then $\lceil \log_m 255 \rceil = 4$. If two pixels in secret image S are 78 and 231, the converted digits become $(0, 3, 0, 3)_5$ and $(1, 4, 1, 1)_5$.

For convenience, assume that t_N converted digits, which are selected from the converted data, are $s_1, s_2, \dots, s_{t_N}$, and then N polynomials, which are used to hide these converted digits, can be constructed as follows:

$$\begin{aligned} f_N(x) &= s_1 + s_2x + \dots + s_{t_N}x^{t_N-1} \mod m \\ f_{N-1}(x) &= f_N(x) - x^{t_N-t_1}g_{N-1}(x) \mod m \\ &\vdots \\ f_1(x) &= f_2(x) - x^{t_2-t_1}g_1(x) \mod m, \end{aligned} \quad (3)$$

Input: $t_j, t_{j+1}, f_{j+1}(x)$
Output: $g_j(x)$
 $g_j(x) = 0$;
 $d = \deg(f_{j+1}(x) - x^{t_{j+1}-t_1} g_j(x))$;
While $d \geq t_j$ do
 $c = \lfloor x^d \rfloor f_{j+1}(x)$;
 $g_j(x) = g_j(x) + cx^{d-(t_{j+1}-t_1)}$;
 $d = \deg(f_{j+1}(x) - x^{t_{j+1}-t_1} g_j(x))$;
end
 $r(x)$ is a random polynomial function the order of which is $t_1 - (t_{j+1} - t_j) - 1$;
 $g_j(x) = g_j(x) + r(x)$;

ALGORITHM 1: Polynomial generator (Zhang et al. [21]).

FIGURE 1: Diagram of the sharing procedure.

where polynomial $g_j(x)$ is generated by Algorithm 1, $\deg(g_j(x)) < t_1$ and $\deg(f_j(x)) = t_j - 1$, for all $1 \leq j \leq N - 1$. Algorithm 1 is described as follows.

Then, each participant's advance shares $y_1^i, y_2^i, \dots, y_N^i$ ($1 \leq i \leq n$) are computed as follows:

$$y_j^i = f_j(h(K_j, x_i)) \quad (j = 1, 2, \dots, N), \quad (4)$$

where y_j^i is the j th advance shares of participant P_i and $h(K_j, x_i)$ is the fake identification that is computed by feeding key K_j and real identification x_i into two-variable one-way function $h(K, x)$.

3.1.2. Camouflage. In this phase, shares are camouflaged in cover image C to form stego images $S_1, S_2, \dots, S_n$, and then they are distributed to corresponding participants.

For convenience, assume that N pixels, which are selected from cover image C , are $cp_1, cp_2, \dots, cp_N$. With $y_1^i, y_2^i, \dots, y_N^i$ and $cp_1, cp_2, \dots, cp_N$, each participant's camouflaged pixels $sp_1^i, sp_2^i, \dots, sp_N^i$ ($1 \leq i \leq n$) are computed as

$$sp_j^i = \left\lfloor \frac{cp_j}{m} \right\rfloor \times m + y_j^i \quad (j = 1, 2, \dots, N), \quad (5)$$

where sp_j^i is j th camouflaged pixel of participant P_i and $\lfloor \cdot \rfloor$ is the floor function.

If all of the converted digits have been camouflaged in cover image C , the dealer can obtain each participant's stego image S_i ($1 \leq i \leq n$), and then the dealer distributes real identification x_i and stego image S_i to corresponding participant P_i through secure communication channel.

3.2. Recovery Procedure. Before recovering secret image S , if security policy and adversary structure are changed, the threshold can be adjusted to a suitable threshold t_j which is one of potential thresholds $t_1, t_2, \dots, t_N$, and the scheme can remain secure after these changes are made. Then, t_j or more participants can use their own stego images to recover secret image S without distortion. In this section, we describe how to change the threshold in Section 3.2.1 and how to recover secret image S without distortion in Section 3.2.2.

3.2.1. Threshold Changing. Assuming that the new threshold must be changed to t_j ($1 \leq j \leq N$), the dealer broadcasts keys $K_j, K_{j+1}, \dots, K_N$. With keys $K_j, K_{j+1}, \dots, K_N$ and real identification x_i , each participant P_i ($1 \leq i \leq n$) computes her/his

FIGURE 2: Recovery procedure.

fake identifications $h(K_j, x_i), h(K_{j+1}, x_i), \dots, h(K_N, x_i)$, which are used to reconstruct polynomials $f_j(x), f_{j+1}(x), \dots, f_N(x)$ in the next phase.

3.2.2. Secret Image Recovery. In this section, we describe how to recover secret image S with threshold t_j . The procedure for doing so is shown in Figure 2.

For convenience, assume that t_j participants $P_1, P_2, \dots, P_{t_j}$ provide their stego images $S_1, S_2, \dots, S_{t_j}$. Let N pixels $sp_1^i, sp_2^i, \dots, sp_N^i$ be the corresponding pixel value of stego image S_i . To extract the converted data, these participants must reconstruct polynomial $f_N(x)$ from their advance shares. Thus, by utilizing the modulo operation, advance shares $y_j^i, y_{j+1}^i, \dots, y_N^i$ ($1 \leq i \leq t_j$) can be computed as

$$y_k^i = sp_k^i \mod m \quad (k = j, j+1, \dots, N), \quad (6)$$

where y_k^i is the k th advance share of participant P_i .

If $t_j = t_N$, with shares $y_N^1, y_N^2, \dots, y_N^{t_N}$ and fake identification values $h(K_N, x_1), h(K_N, x_2), \dots, h(K_N, x_{t_N})$, polynomial $f_N(x)$ can be reconstructed as follows:

$$f_N(x) = \sum_{i=1}^{t_N} y_N^i \prod_{k=1, k \neq i}^{t_N} \frac{x - h(K_N, x_k)}{h(K_N, x_i) - h(K_N, x_k)} \mod m. \quad (7)$$

Then, converted digits $s_1, s_2, \dots, s_{t_N}$ can be recovered from t_N coefficients of polynomial $f_N(x)$.

If $t_1 \leq t_j < t_N$, since $\deg(f_N(x)) = t_N - 1$, t_j participants cannot reconstruct polynomial $f_N(x)$ directly. But, they can reconstruct polynomial $f_j(x)$ and then reconstruct polynomials $f_{j+1}(x), f_{j+2}(x), \dots, f_N(x)$ in turn by computing polynomials $g_j(x), g_{j+1}(x), \dots, g_{N-1}(x)$ where $f_{k+1}(x) = f_k(x) + x^{t_{k+1}-t_k} g_k(x)$ and $\deg(g_k(x)) < t_1$ ($j \leq k \leq N-1$).

With t_1 points $(h(K_{j+1}, x_i), (y_{j+1}^i - f_j(h(K_{j+1}, x_i))) / (h(K_{j+1}, x_i) - h(K_{j+1}, x_{t_1})))$ ($i = 1, 2, \dots, t_1$), polynomial $g_j(x)$ can be constructed as follows:

$$g_j(x) = \sum_{i=1}^{t_1} \frac{y_{j+1}^i - f_j(h(K_{j+1}, x_i))}{(h(K_{j+1}, x_i) - h(K_{j+1}, x_{t_1}))^{t_{j+1}-t_1}} \quad (8)$$

$$\cdot \prod_{k=1, k \neq i}^{t_1} \frac{x - h(K_{j+1}, x_k)}{h(K_{j+1}, x_i) - h(K_{j+1}, x_k)} \mod m.$$

Then, polynomial $f_{j+1}(x)$ can be constructed as $f_{j+1}(x) = f_j(x) + x^{t_{j+1}-t_j} g_j(x)$. By repeating above procedures, polynomials $f_{j+2}(x), f_{j+3}(x), \dots, f_N(x)$ can be recovered in turn, and then converted digits $s_1, s_2, \dots, s_{t_N}$ can be obtained from t_N coefficients of polynomial $f_N(x)$.

By repeating these processes, all converted digits can be extracted, and then secret image S can be recovered by transforming these converted digits to decimal representation.

4. Experiment and Analysis

In this section, we describe the tests we conducted to determine the feasibility and performance of our scheme using simulations and experiments, and then we discuss the security of our scheme.

To estimate the quality of the stego images, we used peak signal-to-noise ratio (PSNR):

$$\text{PSNR} = 10 \log_{10} \left(\frac{255^2}{\text{MSE}} \right) \text{ dB}. \quad (9)$$

The mean square error (MSE) of an image with $H \times W$ pixels is defined as

$$\text{MSE} = \frac{1}{H \times W} \sum_{u=1}^H \sum_{v=1}^W (p_{uv} - p'_{uv})^2, \quad (10)$$

where p_{uv} is the original pixel value of the cover image and p'_{uv} is the camouflaged pixel value of the stego image. Therefore, the higher the PSNR value, the smaller the difference between the cover image and the stego image. If the PSNR value is less than 35 dB, some of the important characteristics of the signal may be lost. When the PSNR value is less than 30 dB, the quality is unacceptable. But it is difficult for people to distinguish the original cover image from the stego image when the PSNR value is greater than 35 dB [26].

4.1. Simulation Results. The simulation settings of our experimental parameters were as follows: $N = 3$, $n = 6$, $m = 5$, $t_1 = 2$, $t_2 = 3$, and $t_3 = 4$ (i.e., this scheme is a $(\{2, 3, 4\}, 6)$ threshold changeable secret sharing scheme). Let the real identification of six participants be $X = \{1, 2, 3, 4, 5, 6\}$. We used image Baboon with 256×256 pixels as the secret image, as shown in Figure 3. We embedded shares into the original cover pixels, except for those pixels within $[\lfloor 255/m \rfloor \times m, 255]$ as Lin and Chan's scheme [7] does.

To compare the quality of the stego images for different cover images, we selected twelve gray-scale test cover images with 512×512 pixels to conduct the experiment. The twelve cover images are shown in Figure 4.

Table 1 displays the corresponding PSNR values of the stego images for the test cover images by our $(\{2, 3, 4\}, 6)$ threshold changeable secret image sharing scheme.

Table 1 indicates that the cover image has little effect on the quality of the stego images. All of the PSNR values of our experiments are about 40 dB, which is greater than 35 dB, indicating that the quality of the stego images is satisfactory.

In the recovery procedure of our $(\{2, 3, 4\}, 6)$ scheme, we set $t_2 = 3$ as the threshold value, and we broadcast the corresponding secret keys K_2, K_3 . For convenience, we used stego images (a), (b), and (c) to reconstruct the secret image. Figure 5 shows cover image Lena, six stego images, and reconstructed secret image Baboon. The average PSNR value of the six stego images (i.e., images (a), (b), (c), (d), (e), and (f)) is 40.02 dB. We observe that each stego image shown in Figure 5 has a natural appearance and cannot leak any information about the secret image. The secret image recovered by stego images (a), (b), and (c) is displayed as image (g), which is the same as the original secret image.

FIGURE 3: Secret image Baboon.

4.2. Performance Analysis. Factors m and N potential thresholds $t_1, t_2, \dots, t_N$ are important in our scheme's ability to maximize the secret capacity and preserve the fidelity of the stego images. The influence of these two factors is discussed in this section.

Table 2 displays the relationship of capacity and distortion for different m values. Image Baboon is used as the secret image in all of those experiments, and Lena is used as the cover image. The parameters are as follows: $N = 3$, $n = 6$, $t_1 = 2$, $t_2 = 3$, and $t_3 = 4$. Table 2 indicates that (1) the number of influenced bits is increased as the value of factor m increases; (2) the capacity of the embedded converted data is increased as the value of factor m increases; and (3) the value of PSNR is decreased as the value of factor m increases. Since the difference between the original pixel in the cover image and the camouflaged pixel in the stego image is limited to $[0, m - 1]$, it becomes smaller as the value of factor m decreases; that is, the quality of the stego images increases as factor m decreases. But a smaller m value can increase the number of converted digits; that is, the capacity of the embedded converted data is decreased. Different from Lin and Chan's scheme [7] which constructs one polynomial, we construct N polynomials to embed t_N converted digits into N pixels of the cover image in one iteration of polynomial calculation. Assuming that this cover image has $H_c \times W_c$ pixels, it can embed $H_c \times W_c \times t_N/N$ converted digits (i.e., $H_c \times W_c \times t_N/(N \times \lceil \log_m 255 \rceil)$ pixels). Table 2 indicates that the values of the PSNR are greater than 35 dB when the values of m are set as 5 and 7. Since the capacity when m is 7 is greater than that when m is 5, setting m as 7 is more suitable in this situation.

The selection of N potential thresholds $t_1, t_2, \dots, t_N$ is another critical factor that influences the quality of the stego images. Table 3 shows the performance comparisons of different potential thresholds. In these experiments, we set test potential thresholds as $[2, 3]$, $[3, 4]$, $[4, 5]$, $[3, 5]$, and $[4, 6]$, and we set factor $m = 5$. As in the above experiments, image Baboon is used as the secret image, and image Lena is the cover image.

In our $(\{t_1, t_2, \dots, t_N\}, n)$ threshold changeable secret image sharing scheme, since we camouflage t_N converted

FIGURE 4: Twelve cover images.

TABLE 1: PSNR values (dB) of the stego images tested in 12 cover images.

Cover images	PNSR of stego 1	PNSR of stego 2	PNSR of stego 3	PNSR of stego 4	PNSR of stego 5	PNSR of stego 6	Average
Airplane	41.24	39.99	40.44	39.62	38.51	40.46	40.04
Boat	41.24	39.98	40.42	39.59	38.48	40.46	40.02
Bird	41.24	39.98	40.43	39.60	38.47	40.46	40.03
Cameraman	41.19	39.93	40.37	39.55	38.41	40.41	39.98
Couple	41.26	40.01	40.46	39.64	38.52	40.49	39.97
Crowd	41.09	39.85	40.26	39.46	38.26	40.30	40.06
Fruits	41.26	40.01	40.45	39.63	38.48	40.48	40.05
House	41.29	40.17	40.68	39.87	39.53	40.73	40.38
Lake	41.25	39.98	40.43	39.62	38.49	40.48	40.04
Lena	41.23	39.97	40.42	39.60	38.47	40.45	40.02
Peppers	41.23	39.97	40.42	39.60	38.48	40.45	40.02
Tiffany	41.26	40.03	40.47	39.64	38.54	40.49	40.04

digits in $(t_N - 1)$ -degree polynomial $f_N(x)$, the order of polynomial $f_N(x)$ increases as t_N increases, which means that, for the same secret image and factor m , the number of camouflaged pixels decreases as t_N increases (i.e., the value of PSNR increases as t_N increases, and the capacity of embedding converted data in the cover image increases as t_N

increases, which were indicated in Table 3). At the same time, we focus on the performance when the potential thresholds were set as $[3, 5]$ and $[4, 5]$, and we observed that different potential thresholds had little effect on the quality of the stego images when t_N and N were fixed. In our scheme, we need to construct $H_s \times W_s \times \lceil \log_m 255 \rceil / t_N$ polynomials and

FIGURE 5: Six stego images, recovered secret image Baboon, and cover image Lena.

TABLE 2: Relationship of the capacity distortion for different m values.

m	Distortion		Capacity (pixels)	PSNR (dB)
	$[0, m - 1]$	Influenced bits		
5	$[0, 4]$	3	$H \times W \times t_N / (N \times 4)$	40.02
7	$[0, 6]$	3	$H \times W \times t_N / (N \times 3)$	38.41
11	$[0, 10]$	4	$H \times W \times t_N / (N \times 3)$	32.61
13	$[0, 12]$	4	$H \times W \times t_N / (N \times 3)$	30.60
17	$[0, 16]$	5	$H \times W \times t_N / (N \times 2)$	28.90
19	$[0, 18]$	5	$H \times W \times t_N / (N \times 2)$	28.22
23	$[0, 22]$	5	$H \times W \times t_N / (N \times 2)$	26.76

TABLE 3: Performance comparisons of different potential thresholds.

Number	Potential thresholds	Capacity	PSNR (dB)
1	$[2, 3]$	$H \times W \times 3/8$	43.79
2	$[3, 4]$	$H \times W \times 4/8$	45.06
3	$[4, 5]$	$H \times W \times 5/8$	46.08
4	$[3, 5]$	$H \times W \times 5/8$	46.03
5	$[4, 6]$	$H \times W \times 6/8$	46.86

camouflage $H_s \times W_s \times N \times \lceil \log_m 255 \rceil / t_N$ pixels of the cover image, where H_s and W_s are the height and width of gray-scale secret image S , respectively. Thus, the difference of potential thresholds cannot influence the quality of the stego images when t_N and N were fixed.

Table 4 compares our scheme with Chang et al.'s scheme (2008) [25], Lin et al.'s scheme (2009) [6], Lin and Chan's scheme (2010) [7], and Ulutas et al.'s scheme (2013) [10]. We still use image Baboon as the secret image and image Lena as the cover image, and set $m = 5$.

Table 4 indicates that our scheme has the unique threshold changeable characteristic and can recover the secret image without distortion. Since we camouflaged t_N converted digits in N pixels of the cover image in each iteration, which requires much more modification of the cover image, our scheme has lower quality of stego images and capacity of embedded converted digits. However, the average PSNR value of our scheme is 40 dB, which indicates that the quality of our stego images is acceptable. In addition, in practice, N is usually a small integer (such as $N = 3$) corresponding to the "low, middle, and high" level of security in computers while t_N could be linearly related to n , so the capacity of embedded converted digits usually is acceptable.

In some situation, we need to share important secret image using sensitive cover images (such as medical, military, or artistic images) and these cover images need to be recovered without distortion. To satisfy this requirement, our scheme can embed the recovery information of the cover image pixels into the polynomials as Lin and Chan's scheme [7] does. But in this situation, we can only embed $t_N - N$

TABLE 4: Comparisons of the related secret image sharing mechanisms.

Functionality	Chang et al. (2008) [25]	Lin et al. (2009) [6]	Lin and Chan (2010) [7]	Ulutas et al. (2013) [10]	Ours
Threshold	(t, n)	(t, n)	(t, n)	(t, n)	$(\{t_1, t_2, \dots, t_N\}, n)$
Threshold changeability	No	No	No	No	Yes
Quality of stego images	40.33 dB	43.02 dB	42.36 dB	46.79 dB	40.02 dB
Lossless secret image	Yes	Yes	Yes	Yes	Yes
Lossless cover image	No	Yes	Yes	Yes	No
Maximum capacity (pixels)	$\frac{H \times W}{4}$	$\frac{(t-3) \times H \times W}{3}$	$\frac{(t-1) \times H \times W}{\lceil \log_m 255 \rceil}$	$\frac{(t-2) \times H \times W}{4}$	$\frac{t_N \times H \times W}{N \times \lceil \log_m 255 \rceil}$

converted digits into N pixels of the cover image in one iteration, which weakens the quality of the stego images and reduces the capacity to $H_c \times W_c \times (t_N - N)/(N \times \lceil \log_m 255 \rceil)$, where H_c and W_c are the height and width of gray-scale cover image C , respectively.

4.3. Security Analysis. In this section, we analyze the security of our scheme.

First, we notice that our scheme can only change the threshold once. After the dealer broadcasts keys $K_j, K_{j+1}, \dots, K_N$ to validate threshold t_j ($1 \leq j \leq N$), then it takes at least t_j cooperating participants to recover the secret image without distortion. If the new threshold must be changed to t_k ($1 \leq k < j$), the dealer broadcasts keys $K_k, K_{k+1}, \dots, K_{j-1}$ to achieve this. On the contrary, if $j < k \leq N$, the shares must be updated. In schemes that have strict security requirements, it is inevitable that shares are updated. For instance, the threshold in schemes [27, 28] can be changed many times, but, when one participant leaves the group, the shares should be updated simultaneously.

Theorem 1. *Before broadcasting the keys, no participant can recover secret image S .*

Proof. In the worst situation, there are n participants in set $A' = \{P_1, P_2, \dots, P_n\}$ who want to recover the secret image. Assume that they want to recover the first t_N converted digits hidden in polynomial $f_N(x)$. Then, the participants in A' can obtain

$$\left(\bigcup_{1 \leq i \leq n} \bigcup_{1 \leq k \leq N} \{y_k^i\} \right) \cup \left(\bigcup_{1 \leq i \leq n} x_i \right). \quad (11)$$

Our scheme is based on polynomial interpolation; that is, given t points $(x_1, y_1), (x_2, y_2), \dots, (x_t, y_t)$ with distinct x_i , there is one and only one $(t-1)$ -degree polynomial $f(x)$ such that $f(x_i) = y_i$ for all $1 \leq i \leq t$. However, the polynomial cannot be reconstructed with less than t points. According to the features of the two-variable one-way function $h(K, x)$, without keys $K_1, K_2, \dots, K_N$, each participant P_i ($1 \leq i \leq n$) cannot compute her/his fake identifications $h(K_1, x_i), h(K_2, x_i), \dots, h(K_N, x_i)$, which are fed into polynomials $f_1(x), f_2(x), \dots, f_N(x)$ to generate the shares $y_1^i, y_2^i, \dots, y_N^i$ in the sharing procedure. Thus, utilizing only $(\bigcup_{1 \leq i \leq n} \bigcup_{1 \leq k \leq N} \{y_k^i\})$, no polynomial in $f_1(x), f_2(x), \dots, f_N(x)$ can be reconstructed by polynomial interpolation, and

they cannot obtain the converted digits that are hidden in the coefficients of polynomial $f_N(x)$. Likewise, the participants in A' cannot obtain other converted digits, so the secret image cannot be recovered by any participant. $\square$

Theorem 2. *After obtaining broadcast information $K_j, K_{j+1}, \dots, K_N$, less than t_j participants cannot recover secret image S .*

Proof. Without loss of generality, assume that there are $t_j - 1$ participants in set $A' = \{P_1, P_2, \dots, P_{t_j-1}\}$ who want to recover the secret image. Assume that they want to recover the first t_N converted digits that are hidden in polynomial $f_N(x)$. Then, the participants in A' can obtain

$$\left(\bigcup_{1 \leq i \leq t_j-1} \bigcup_{1 \leq k \leq j-1} \{y_k^i\} \right) \cup \left(\bigcup_{1 \leq i \leq t_j-1} x_i \right) \cup \left(\bigcup_{1 \leq i \leq t_j-1} \bigcup_{j \leq k \leq N} \{h(K_k, x_i), y_k^i\} \right). \quad (12)$$

According to the features of the two-variable one-way function $h(K, x)$, we know the following:

- (1) If x_i and x_j ($i \neq j$) are fed into $h(K, x)$ with the same key K , $h(K, x_i) \neq h(K, x_j)$.
- (2) If x_i is fed into $h(K, x)$ with different keys K and K' , $h(K, x_i) \neq h(K', x_i)$.

Thus, the fake identifications of participants in A' are different, and they cannot deduce their own unknown fake identifications $\bigcup_{1 \leq i \leq t_j-1} \bigcup_{1 \leq k \leq j-1} \{h(K_k, x_i)\}$ without $K_1, K_2, \dots, K_{j-1}$. Utilizing only $(\bigcup_{1 \leq i \leq t_j-1} \bigcup_{1 \leq k \leq j-1} \{y_k^i\}) \cup (\bigcup_{1 \leq i \leq t_j-1} x_i)$, polynomials $f_1(x), f_2(x), \dots, f_{j-1}(x)$ cannot be reconstructed by polynomial interpolation.

Utilizing $\bigcup_{1 \leq i \leq t_j-1} \{h(K_j, x_i), y_j^i\}$ for each candidate point $(h(K_j, x'), y')$, they can reconstruct one and only one polynomial $f_j'(x)$ of degree $t_j - 1$, such that $f_j'(h(K_j, x')) = y'$ and $f_j'(h(K_j, x_i)) = y_j^i$ ($1 \leq i \leq t_j - 1$). Constructed in the same way, these possible polynomials are equally likely; thus, there is absolutely nothing the opponent can deduce about the real polynomial $f_j(x)$. Likewise, utilizing

$\bigcup_{1 \leq i \leq t_j-1} \bigcup_{j+1 \leq k \leq N} \{h(K_k, x_i), y_k^i\}$, they cannot deduce anything about polynomials $f_{j+1}(x), f_{j+2}(x), \dots, f_N(x)$ either, where $\deg(f_k(x)) > \deg(f_j(x)) = t_j - 1$ ($k = j, j+1, \dots, N$).

In summary, the participants in A' cannot reconstruct polynomial $f_N(x)$ and obtain t_N hidden converted digits, which are the coefficients of polynomial $f_N(x)$. Likewise, they cannot obtain other converted digits. Thus, less than t_j participants cannot recover secret image S , after obtaining broadcast keys $K_j, K_{j+1}, \dots, K_N$. $\square$

Theorem 3. *If threshold t_j ($1 \leq j \leq N$) is validated by broadcasting information, thresholds $t_{j+1}, t_{j+2}, \dots, t_N$ are validated at the same time.*

Proof. In the recovery procedure, assume that threshold t_j ($1 \leq j \leq N$) is validated by broadcasting keys $K_j, K_{j+1}, \dots, K_N$; then any t_j or more participants can collaborate to recover the secret image using their stego images. In addition, any t' ($t_k \leq t' \leq t_{k+1}$, $j < k < N$) or more participants can also collaborate to recover the secret image with keys $K_k, K_{k+1}, \dots, K_N$. In other words, when threshold t_j is validated, thresholds $t_{j+1}, t_{j+2}, \dots, t_N$ are also validated. $\square$

5. Conclusions

Before recovering the secret image, the threshold may have to be adjusted for the change of the security policy and the adversary's structure. To solve this problem, we propose a $(\{t_1, t_2, \dots, t_N\}, n)$ threshold changeable secret image sharing scheme with N potential thresholds $t_1, t_2, \dots, t_N$. Our scheme can validate new threshold t_i ($1 \leq i \leq N$) by broadcasting the corresponding keys $K_i, K_{i+1}, \dots, K_N$, and then t_i or more participants can recover secret image S without distortion. The experiments and analysis showed that the threshold in our scheme can be changed dynamically and that the security can be maintained after these changes. In addition, the quality of the stego images is satisfactory.

However, in order to make the threshold changeable, we embed large amounts of redundant data into the cover image, which requires much more modification of the cover image, so the quality of the stego images is lower than other schemes. At the same time, we do not embed the recovery information of N pixels of the cover image in order to increase the capacity, so the cover image in our scheme cannot be recovered without distortion. We will address these issues in future work.

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

This paper is supported by the Nature Science Foundation of China under Grant nos. 61272173, 91315302, 61401060, 61501080, and 61572095, the General Program of Liaoning Provincial Department of Education Science Research under Grant no. L2014017, and the Fundamental Research Funds for the Central Universities under Grant no. DUT16QY09.

In addition, the authors are grateful to Jia Liu for insightful comments and discussions.

References

- [1] A. Shamir, "How to share a secret," *Communications of the Association for Computing Machinery*, vol. 22, no. 11, pp. 612–613, 1979.
- [2] G. R. Blakley, "Safeguarding cryptographic keys," in *Proceedings of the AFIPS National Computer Conference*, pp. 313–317, New York, NY, USA, June 1979.
- [3] M. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryptology- Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques (EUROCRYPT '94)*, pp. 1–12, Perugia, Italy, 1994.
- [4] C.-C. Lin and W.-H. Tsai, "Secret image sharing with steganography and authentication," *Journal of Systems and Software*, vol. 73, no. 3, pp. 405–414, 2004.
- [5] C.-N. Yang, T.-S. Chen, K. H. Yu, and C.-C. Wang, "Improvements of image sharing with steganography and authentication," *Journal of Systems and Software*, vol. 80, no. 7, pp. 1070–1076, 2007.
- [6] P.-Y. Lin, J.-S. Lee, and C.-C. Chang, "Distortion-free secret image sharing mechanism using modulus operator," *Pattern Recognition*, vol. 42, no. 5, pp. 886–895, 2009.
- [7] P.-Y. Lin and C.-S. Chan, "Invertible secret image sharing with steganography," *Pattern Recognition Letters*, vol. 31, no. 13, pp. 1887–1893, 2010.
- [8] C. Guo, C.-C. Chang, and C. Qin, "A hierarchical threshold secret image sharing," *Pattern Recognition Letters*, vol. 33, no. 1, pp. 83–91, 2012.
- [9] C. Guo, C.-C. Chang, and C. Qin, "A multi-threshold secret image sharing scheme based on MSP," *Pattern Recognition Letters*, vol. 33, no. 12, pp. 1594–1600, 2012.
- [10] M. Ulutas, G. Ulutas, and V. V. Nabiye, "Invertible secret image sharing for gray level and dithered cover images," *Journal of Systems and Software*, vol. 86, no. 2, pp. 485–500, 2013.
- [11] N. Pakniat, M. Noroozi, and Z. Eslami, "Secret image sharing scheme with hierarchical threshold access structure," *Journal of Visual Communication and Image Representation*, vol. 25, no. 5, pp. 1093–1101, 2014.
- [12] C. S. Lai, L. Harn, J. Y. Lee, and T. Hwang, "Dynamic threshold scheme based on the definition of cross-product in an n -dimensional linear space," *Journal on Information Science and Engineering*, vol. 7, no. 1, pp. 13–23, 1991.
- [13] Y. Desmedt and S. Jajodia, "Redistributing secret shares to new access structures and its applications," Tech. Rep. ISSE TR-97-01, George Mason University, Fairfax, Va, USA, 1997.
- [14] L. Chen, D. Gollmann, and C. J. Mitchell, "Key escrow in mutually mistrusting domains," in *Security Protocols: International Workshop Cambridge, United Kingdom, April 10–12, 1996 Proceedings*, vol. 1189 of *Lecture Notes in Computer Science*, pp. 139–153, Springer, Berlin, Germany, 1997.
- [15] K. M. Martin, R. Safavi-Naini, and H. Wang, "Bounds and techniques for efficient redistribution of secret shares to new access structures," *Computer Journal*, vol. 42, no. 8, pp. 638–649, 1999.
- [16] R. Steinfeld, J. Pieprzyk, and H. Wang, "Lattice-based threshold-changeability for standard CRT secret-sharing schemes," *Finite Fields and Their Applications*, vol. 12, no. 4, pp. 653–680, 2006.

- [17] H. A. Khorasgani, S. Asaad, T. Eghlidos, and M. Aref, "A lattice-based threshold secret sharing scheme," in *Proceedings of the 11th International ISC Conference on Information Security and Cryptology (ISCISC '14)*, pp. 173–179, Tehran, Iran, September 2014.
- [18] R. Steinfeld, J. Pieprzyk, and H. Wang, "Lattice-based threshold changeability for standard shamir secret-sharing schemes," *IEEE Transactions on Information Theory*, vol. 53, no. 7, pp. 2542–2559, 2007.
- [19] C. Blundo, A. Cresti, A. De Santis, and U. Vaccaro, "Fully dynamic secret sharing schemes," *Theoretical Computer Science*, vol. 165, no. 2, pp. 407–440, 1996.
- [20] K. M. Martin, "Untrustworthy participants in perfect secret sharing schemes," in *Cryptography and Coding III*, pp. 255–264, Oxford University Press, Oxford, UK, 1993.
- [21] Z. Zhang, Y. M. Chee, S. Ling, M. Liu, and H. Wang, "Threshold changeable secret sharing schemes revisited," *Theoretical Computer Science*, vol. 418, pp. 106–115, 2012.
- [22] K. M. Martin, J. Pieprzyk, R. Safavi-Naini, and H. Wang, "Changing thresholds in the absence of secure channels," *Australian Computer Journal*, vol. 31, no. 2, pp. 34–43, 1999.
- [23] S. G. Barwick, W.-A. Jackson, and K. M. Martin, "Updating the parameters of a threshold scheme by minimal broadcast," *IEEE Transactions on Information Theory*, vol. 51, no. 2, pp. 620–633, 2005.
- [24] H.-Y. Chien, J. Jinn-Ke, and Y. M. Tseng, "A practical (t, n) multi-secret sharing scheme," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 83, no. 12, pp. 2762–2765, 2000.
- [25] C.-C. Chang, Y.-P. Hsieh, and C.-H. Lin, "Sharing secrets in stego images with authentication," *Pattern Recognition*, vol. 41, no. 10, pp. 3130–3137, 2008.
- [26] K. Kyriakopoulos and D. J. Parish, "A live system for wavelet compression of high speed computer network measurements," in *Proceedings of the 8th International Conference on Passive and Active Network Measurement*, pp. 241–244, Louvain, Belgium, April 2007.
- [27] B. Blakley, G. R. Blakley, A. H. Chan, and J. L. Massey, "Threshold schemes with disenrollment," in *Advances in Cryptology—CRYPTO '92*, E. F. Brickell, Ed., vol. 740 of *Lecture Notes in Computer Science*, pp. 540–548, Springer, 1993.
- [28] K. M. Martin, "Dynamic access policies for unconditionally secure secret sharing schemes," in *Proceedings of the IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security*, pp. 61–66, Awaji Island, Japan, October 2005.

Hindawi

Submit your manuscripts at
<http://www.hindawi.com>