Secret Images Sharing Scheme Using Two-Variable One-Way Functions

Todorka ALEXANDROVA, Yoshiaki SUZUKI, Kan OKUBO, and Norio TAGAWA

***Abstract*—In this paper a method for realizing (t, n) secret images sharing scheme has been proposed. The proposed algorithm for secret images sharing is realized by applying multi-secret sharing schemes based on two-variable one-way functions and Shamir's secret sharing schemes. In the proposed scheme participants only need to pool their pseudo-shares instead of disclosing their secret shares when recovering secret images. Thus, each participant can share many secret images by holding only one secret share. Moreover, the size of each share does not depend on the size of the secret image and this is an important property for the further process of the image shares. The proposed method is a multi-use scheme that can be used in different secret sharing sessions without redistributing participants' secret shares. Compared with other image secret sharing techniques another main advantage of the proposed method is that it does not generate share images which are difficult to manage.**

***Keywords*—secret images sharing, polynomial interpolation, two-variable one-way function, Shamir's secret sharing scheme**

I. INTRODUCTION

The problem of information protection has received a lot of attention in the recent years. The need to protect electronic data from damages or lost has become essential with the development of the computers and computer networks. *Encryption* [15] is one of the popular methods to ensure the integrity and security of the protected information. However, the information can not be recovered if the decryption key has been lost or the information has been corrupted during the transmission. Being an important tool in the cryptographic key management, *secret sharing schemes* allow us to keep the protected information *secure* and at the same time always *available*. Secret sharing schemes were independently proposed by Shamir [13] and Blakley [1] in 1979. A *secret sharing scheme* is a technique of sharing a *secret* s into n pieces, called shares, and distributing them to a set of n users (participants) in such a way that only certain *qualified* subsets of users can recover the secret by combining their shares and any *unqualified* subset of users can not do so. A secret sharing scheme is called a (t, n) threshold secret sharing scheme for $t \leq n$ if the following two conditions are satisfied: i) knowledge of any t or more shares makes the secret s computable; ii) knowledge of any $t-1$ or fewer shares leaves s completely undetermined in information theoretic sense. An important class of secret sharing schemes are the so called *perfect* secret sharing schemes. A secret sharing scheme is called perfect if an unqualified subset of users obtains absolutely no information about the secret in information theoretic sense [14]. It has been proved that for perfect secret sharing schemes the size of the shares is at least the size of the secret [3]. Secret sharing schemes in which the size of the shares are smaller that the size of the secret are considered as *ramp* secret sharing schemes [2].

Security is a big concern when considering the storage of image information (e. g. satellite photos or medical images). Noar and Shamir [9] extended the secret sharing concept to the image secret sharing concept, called *visual cryptography*. Visual cryptography is a *perfect secret sharing scheme* and requires stacking of any t image shares to reveal the original image without using any cryptographic computation. However the size of the shared images is much bigger than the original image, as well as the contrast of the recovered image is lower than the original image, which makes the visual secret sharing schemes not suitable for lossless practical applications.

In a (t, n) secret image sharing scheme, the secret image is used to generate n image shares (shadows) such that: *i*) combining any t, $(t \leq n)$ image shares the secret image can be recovered and *ii*) combining any $t-1$, or fewer image shares the secret image can not be revealed. These schemes are considered as ramp secret sharing schemes. An important issue in the secret image sharing schemes is the size of each image share. The size of each secret image share should be as small as possible compared to the secret image and this is an important property for the further process of the image shares, such as storage, transmission, or image hiding. In 2002, Thien and Lin [16] proposed a new lossless (t, n) secret image sharing scheme based on Shamir's secret sharing. The size of each image share in Thien and Lin's scheme is $1/t$ of the size of the secret image. Later, combining matrix projection and Shamir's secret sharing schemes, Li Bai [8] proposed an image secret sharing scheme that avoids the usage of the permutation key that has been used in [16] and thus provides better security measure. However Li Bai's scheme generates larger secret image shares as compared to [16].Wang and Su [17] proposed a secret image sharing method using Huffman coding. The experimental results show that each generated image share in [17] is about 40% smaller than that generated in [16]. In 2008, Shi et. al. [11], proposed a new scheme for image encryption based on Shamir's secret sharing, where the size of each share is $2(\log_t m)/m^2$ of that of the shared $m \times m$ image. However, all these schemes are considered as *one-time-use* schemes, which means that after some particular secrets have been reconstructed, the dealer must redistribute fresh shares to participants in order to share the next secrets.

In this paper we propose a new (t, n) secret images sharing scheme, which has the following properties:

- the scheme is based on the (t, n) *multi-secret sharing scheme* presented in [10], that is realized by combining

The authors are with the Graduate School of System Design, Tokyo Metropolitan University, 6-6 Asahigaoka, Hino, Tokyo 191-0065, Japan, email: toty.alexandrova@gmail.com; yoshiaki.suzuki5@gmail.com; kanne@sd.tmu.ac.jp; tagawa@sd.tmu.ac.jp

978-1-4244-5852-3/10/$26.00 ©2010 IEEE

two-variable one-way functions and Shamir's secret sharing scheme;
- participants only need to pool their *pseudo-shares* instead of disclosing their secret shares when recovering secret images;
- each participant can share many secret images by holding only one secret share;
- the size of each secret share does not depend on the size of the secret image and this is an important property for the further process of the image shares;
- it is a lossless multi-use scheme that can be used in different secret sharing sessions without redistributing participants' secret shares;
- it does not generate shadow images which are difficult to mange and identify;
- the scheme improves the method proposed by Shi et. al. [11]

Integrating the above advantages, we can say that the proposed scheme is an effective, reliable and secure multi-use method to protect the secret image from getting lost, destroyed, stolen or corrupted. The scheme is a ramp multiple-secret sharing scheme.

The rest of this paper is organized as follows. The next section gives the basic preliminaries and definitions used in the paper. Sections III and IV present the proposed scheme and give analysis and discussions. Section V gives an example illustrating the proposed method and the last section concludes the paper and gives the aspects for future work.

II. Background and Preliminaries

In this section we give the basic preliminaries and mathematical concepts used in the paper.

A. Notations

Here we summarize the basic notations used in this paper:
- " $\oplus$" - exclusive-or bit by bit;
- $\mathbf{M}$ - a matrix;
- $m_{i,j}$ - the entry of the ith row and the jth column of a matrix $\mathbf{M}$;
- q - large prime number;
- $GF(q)$ - finite field;
- $f(r, s)$ - two variable one-way function;
- $h(x)$ - polynomial over $GF(q)$;
- $U_1, U_2, \ldots, U_n$ - a set of n participants;
- $u_1, u_2, \ldots, u_n$ - participants' public identity information;
- $D, (D \notin \{U_1, U_2, \ldots, U_n\})$ - a dealer
- K - a single secret to be shared among a set of n participants;
- $K_1, K_2, \ldots, K_p$ - a set of p secrets to be shared among a set of n participants;
- $s_1, s_2, \ldots, s_n$ - participants' secret shares;
- $f(r, s_i)$ - participants' pseudo-shares.

All the calculations in this paper are done in the Galois field $GF(q)$, for a large prime number q.

B. Shamir's Secret Sharing

Shamir's (t, n) threshold secret sharing scheme is based on the polynomial approach and it is described as follows [13]:

1. Let $K \in GF(q)$ be a secret to be shared among a set of n participants, where q is a prime number and $q \geq n + 1$.

2. D chooses elements $a_1, \ldots, a_{t-1} \in GF(q)$ independently and uniformly, and constructs the polynomial $h(x)$:

$$h(x) = K + a_1 x + a_2 x^2 + \ldots + a_{t-1} x^{t-1}. \quad (1)$$

3. D chooses n distinct points $x_i \in GF(q)$, $1 \leq i \leq n$. The values x_i are public.

4. D distributes shares $v_i = h(x_i)$ to users U_i, $1 \leq i \leq n$.

Without loss of generality we assume that the set of t users $U_1, U_2, \ldots, U_t$ combine their shares $v_1, v_2, \ldots, v_t$. Then they can recover the secret by using the Lagrange interpolation formula for polynomials. Knowing the t points $(x_1, h(x_1))$, $(x_2, h(x_2))$, $\ldots (x_t, h(x_t))$, the unique polynomial $h(x)$ can be constructed using the formula

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

The secret K is obtained by $K = h(0)$, i.e.,

$$K = \sum_{i=1}^{t} h(x_i) \prod_{1 \leq j \leq t, j \neq i} \frac{x_j}{x_j - x_i}. \quad (3)$$

C. (t, n) Multi-Secret Sharing Schemes [10]

In order to be able to share multiple secrets, *multi-secret sharing schemes* were proposed [5], [6], [7], [10], [18]. In the multi-secret sharing schemes [7], [10], [18] a set of p secrets can be shared at once, such that each participant needs to keep one share, called *secret share*. In a (t, n) multi-secret sharing scheme combining any t, $(t \leq n)$ shares the p secrets can be recovered at once and combining any $t - 1$, or fewer shares the p secrets can not be revealed. It is worth noting that in this scheme either all p secrets are recovered at once, or all p secrets are unrecoverable. In order to reconstruct the secrets, the participants need to submit a *pseudo-share* computed from their secret share instead of the secret share itself. The secret shares are well protected because of the properties of the two-variable one-way function. However, these schemes are also considered as ramp secret sharing schemes.

Definition 2.1. (Two-variable one-way function) [7]. *The two-variable one-way function $f(r, s)$ is a function that maps any r and s onto a bit string $f(r, s)$ of a fixed length. This function has the following properties:*

(a) Given r and s, it is easy to compute $f(r, s)$;

(b) Given s and $f(r, s)$, it is hard to compute r ;

(c) Having no knowledge of s, it is hard to compute $f(r, s)$ for any r;

(d) Given s, it is hard to find two different values r_1 and r_2 such that $f(r_1, s) = f(r_2, s)$;

(e) Given r and $f(r, s)$, it is hard to compute s;

(f) Given pairs of r and $f(r, s)$, it is hard to compute $f(r', s)$ for $r' = r$.

Here we describe Pang *et al.*'s [10] (t, n) multi-secret sharing scheme in which a dealer D shares a set of p secrets, $\{K_1, K_2, \ldots, K_p\}$, among a set of n participants $\{U_1, U_2, \ldots, U_n\}$. It is a multi-use secret sharing scheme and hence suitable for realizing a practical multi-secret images

sharing method. The method is described in the following three steps: system setup, secret image distribution and secret image reconstruction

1) System Setup: The dealer D randomly selects n distinct integers $s_1, s_2, \ldots, s_n \in GF(q)$ as participants secret shares and distributes them to every participant over a secure channel. For each participant there is a public identifier, which is a well-known number and it is used to represent each participant individually. D selects n distinct integers $u_1, u_2, \ldots, u_n \in [p, q-1]$ as participants' public identifiers.

2) Secrets Distribution: The dealer D performs the following steps in order to share the p secrets among the n users:

(a) Chooses a random integer r and computes the pseudo-shares $f(r, s_i)$, $i = 1, \ldots, n$.

(b) Uses the $(n+p)$ pairs of $(u_i, f(r, s_i))$, $i = 1, \ldots, n$ (n pairs); $(0, K_1)$, $(1, K_2)$,..., $(p-1, K_p)$, (p pairs); to construct an $(n+p-1)$st degree polynomial

$$h(x) = a_0 + a_1 x + \ldots + a_{n+p-1} x^{n+p-1}.$$

(c) Takes out the $(n + p - t)$ minimum integers $d_1, d_2, \ldots, d_{n+p-t} \in [p, q-1] \setminus \{u_i | i = 1, 2, \ldots, n\}$ and computes $h(d_i)$, $i = 1, 2, \ldots, n+p-t$.

(d) Publishes $(r, h(d_1), h(d_2), \ldots, h(d_{n+p-t}))$ in any authenticated manner such as those in [4], [12].

The number of the public values is $(n + p - t + 1)$.

3) Secret Reconstruction: The participants are able to calculate their pseudo-shares $f(r, s_i)$, $i = 1, 2, \ldots, n$ by using the public value r and their secret shares s_i. After the t users pool their pseudo-shares $f(r, s_{i_j})$ for $j = 1, 2, \ldots, t$, the t pairs $(u_{i_j}, f(r, s_{i_j}))$ for $j = 1, 2, \ldots, t$ are obtained. With the knowledge of the public values $h(d_i)$, $i = 1, 2, \ldots, n+p-t$, the $(n + p - t)$ pairs $(d_i, h(d_i))$, $i = 1, 2, \ldots, n+p-t$ are obtained as well. Therefore, there are $(n + p)$ pairs obtained in total and thus the $(n+p-1)$st degree polynomial $h(x)$ can be uniquely determined using Lagrange interpolation.

The p secrets are then obtained by

$$K_i = h(i-1), i = 1, 2, \ldots, p.$$

III. Proposed Image Secret Sharing

A. Image Characterization

An image $\mathbf{I}$ is defined by c number of colors and $d \times l$ pixels $m_{i,j}$, $1 \le i \le d$, $1 \le j \le l$, which form a matrix $\mathbf{M}$ with coefficients in Z_c such that:

i). If $\mathbf{I}$ is a black and white image, then $\mathbf{M}$ is an $d \times l$ matrix, where $m_{i,j} = 1$ if the corresponding pixel is black and $m_{i,j} = 0$ if the corresponding pixel is white, i.e., $m_{i,j} \in Z_2$ for $1 \le i \le d$, $1 \le j \le l$.

ii). If $\mathbf{I}$ is a gray level image, then for the *RGB* code of each pixel we have $R = G = B$ and thus $\mathbf{M}$ is an $d \times l$ matrix, where $0 \le m_{i,j} \le 255$, i.e., $m_{i,j} \in Z_{2^8}$ for $1 \le i \le d$, $1 \le j \le l$.

iii). If $\mathbf{I}$ is a color image, then each pixel is given by a three dimensional vector (R, G, B) and thus $\mathbf{M}$ is an $d \times l$ matrix, where each $m_{i,j}$ is represented by 24 bits (8 bits representing each of the colors red, green and blue), i.e., $m_{i,j} \in Z_{2^{24}}$ for $1 \le i \le d$, $1 \le j \le l$.

Hence we assume that the image is a matrix with coefficients satisfying one of the cases of i), ii), iii).

In this section we describe the proposed method for (t, n) secret image sharing, in which the secret image $\mathbf{I}$ is used to generate n shares such that: *i*) combining any t, $(t \le n)$ shares the secret image can be recovered and *ii*) combining any $t-1$, or fewer shares the secret image can not be revealed.

The proposed method for sharing the secret image $\mathbf{I}$ is based on a (t, n) multi-secret sharing scheme similar to Pang *et al.*'s [10] scheme and it is a further implementation of Shi *et al.*'s secret image sharing scheme [11]. It is described in the following three steps: system setup, secret image distribution and secret image reconstruction.

B. Proposed Method

1) System Setup: Let $\mathbf{I}$ be the secret image. Without loss of generality we assume $\mathbf{I}$ is defined by $m \times m$ pixels and $\mathbf{M}$ is the $m \times m$ matrix of it. Let also $k = \lceil \log_n m \rceil$.

The dealer D selects a large prime number $q > c$, where c is the number of the colors in $\mathbf{I}$. The dealer D randomly selects n distinct integers $s_1, s_2, \ldots, s_n \in GF(q)$ as participants secret shares and distributes them to every participant over a secure channel. For each participant there is a public identifier, which is a well-known number and it is used to represent each participant individually. D selects n distinct integers $u_1, u_2, \ldots, u_n \in [n-t+1, q-1]$ as participants' public identifiers.

2) Secret Image Distribution: The dealer D performs the following steps in $GF(q)$ in order to share the secret image $\mathbf{I}$ among the set of n users:

(a) D chooses random integers r_1, r_2, ..., r_{2k} in $GF(q)$ and computes the pseudo-shares

$$f(r_1, s_i), i = 1, \ldots, n,$$
$$f(r_2, s_i), i = 1, \ldots, n,$$
$$\ldots$$
$$f(r_{2k}, s_i), i = 1, \ldots, n.$$

(b) D uses the pairs of $(u_i, f(r_1, s_i))$, $(u_i, f(r_2, s_i))$, ..., $(u_i, f(r_{2k}, s_i))$, $i = 1, \ldots, n$ to construct the $2k$ polynomials of degree $n-1$ as follows:

$$h_1(x) = a_0^1 + a_1^1 x + \ldots + a_{n-1}^1 x^{n-1}, \quad (4)$$
$$h_2(x) = a_0^2 + a_1^2 x + \ldots + a_{n-1}^2 x^{n-1} \quad (5)$$
$$\ldots$$
$$h_{2k}(x) = a_0^{2k} + a_1^{2k} x + \ldots + a_{n-1}^{2k} x^{n-1}, \quad (6)$$

where for $i = 1, \ldots, n$ and $l = 1, \ldots, 2k$

$$h_l(u_i) = f(r_l, s_i). \quad (7)$$

(c) D computes

$$z_i^1 = h_1(i), i = 1, 2, \ldots, n-t, \quad (8)$$
$$z_i^2 = h_2(i), i = 1, 2, \ldots, n-t, \quad (9)$$
$$\ldots$$
$$z_i^{2k} = h_{2k}(i), i = 1, 2, \ldots, n-t. \quad (10)$$

(d) D computes the $n^k \times n^k$ secret matrix $\mathbf{M}'$ as follows. For $k = 1$ and $1 \leq i, j \leq n$

$$m'_{i,j} = (a^1_{i-1} + a^2_{j-1}) \, mod \, c, \tag{11}$$

and for $k > 1$, and $1 \leq i, j \leq n^k$

$$m'_{i,j} = \quad (\sum_{r=1}^{k-1} a^r_{\lfloor \frac{i}{n^{k-r}} \rfloor} + \sum_{r=k+1}^{2k-1} a^r_{\lfloor \frac{j}{n^{2k-r}} \rfloor} \tag{12}$$

$$+ a^k_{((i-1) mod \, n)} + a^{2k}_{((j-1) mod \, n)}) \, mod \, c. \tag{13}$$

(e) D computes the $m \times m$ matrix $\mathbf{M}''$ as follows

$$\mathbf{M}'' = \mathbf{M} \oplus \mathbf{M}^\star, \tag{14}$$

where $\mathbf{M}^\star$ is the following $m \times m$ matrix

$$m^\star_{i,j} = m'_{i,j} \quad \text{for } 1 \leq i, j \leq m. \tag{15}$$

(f) D publishes the values $(r_1, z^1_1, z^1_2, \ldots, z^1_{(n-t)})$, $(r_2, z^2_1, z^2_2, \ldots, z^2_{(n-t)})$, …, $(r_{2k}, z^{2k}_1, z^{2k}_2, \ldots, z^{2k}_{(n-t)})$ and the matrix $\mathbf{M}''$ in any authenticated manner such as those in [4], [12].

Hence, the number of the public values in this case is $2k(n-t+1) + m^2$.

3) Secret Image Reconstruction: In the following step we describe how t participants $U_{i_1}, U_{i_1}, \ldots, U_{i_t}$, for some $1 \leq i_1 < i_2 < \ldots < i_t \leq n$, are able to reconstruct the secret image $\mathbf{I}$ by combining their shares.

(a) The participants are able to calculate the pseudo-shares $f(r_1, s_{i_j}), f(r_2, s_{i_j}), \ldots, f(r_{2k}, s_{i_j})$ for $j = 1, 2, \ldots, t$ by using the public values $r_1, r_2, \ldots, r_{2k}$ and secret shares s_{i_j}.

(b) After the t users pool the pseudo-shares $f(r_1, s_{i_j})$ for $j = 1, 2, \ldots, t$, the t pairs $(u_{i_j}, f(r_1, s_{i_j}))$ are obtained. With the knowledge of the public values z^1_i, $i = 1, 2, \ldots, n-t$, the $(n-t)$ pairs (i, z^1_i), $i = 1, 2, \ldots, n-t$ are obtained as well. Therefore, there are n pairs obtained in total and the $(n-1)$st degree polynomial $h_1(x)$ can be uniquely determined using the Lagrange interpolation formula as described in Eq. (2).

Analogically, after the t users pool their pseudo-shares $f(r_2, s_{i_j})$, …, $f(r_{2k}, s_{i_j})$ for $j = 1, 2, \ldots, t$, the sets of t pairs $(u_{i_j}, f(r_2, s_{i_j}))$, …, $(u_{i_j}, f(r_{2k}, s_{i_j}))$ are obtained. With the knowledge of the public values z^2_i, …, z^{2k}_i, for $i = 1, 2, \ldots, n-t$, the sets of $(n-t)$ pairs (i, z^2_i), …, (i, z^{2k}_i) are obtained as well. Therefore, there are $2k-1$ sets of n pairs obtained in total and thus the set of nth degree polynomials $h_2(x)$, …, $h_{2k}(x)$ can be uniquely determined using the Lagrange interpolation formula in Eq. (2).

(c) Then, the secret matrix $\mathbf{M}'$ is computed as described in Eqs. (11)-(13).

(d) The matrix $\mathbf{M}$ is obtained by

$$\mathbf{M} = \mathbf{M}'' \oplus \mathbf{M}^\star. \tag{16}$$

(f) The secret image $\mathbf{I}$ is recovered from $\mathbf{M}$.

IV. Analysis and Discussions

A. Security Analysis

Here we discuss the security of the proposed (t, n) secret images sharing method from the following perspectives:

(1) From the public values z^1_i, z^2_i, …, z^{2k}_i, for $i = 1, 2, \ldots, n-t$, the $2k$ sets of $(n-t)$ pairs (i, z^1_i), (i, z^2_i), …, (i, z^{2k}_i) can be obtained. However, none of the polynomials $h_1(x)$, $h_2(x)$, …, $h_{2k}(x)$ can be determined using these pairs since their degree is n and thus the secret image can not be recovered by an adversary.

(2) If a set of l participants, where $l < t$ combine their shares then they can obtain the sets of l pairs $(u_{i_j}, f(r_1, s_{i_j}))$, $(u_{i_j}, f(r_2, s_{i_j}))$, …, $(u_{i_j}, f(r_{2k}, s_{i_j}))$, for $j = 1, 2, \ldots, l$. With the knowledge of the public values z^1_i, z^2_i, …, z^{2k}_i, for $i = 1, 2, \ldots, n-t$, in total $(l+n-t)$ pairs are obtained for each of these cases. Since $l + n - t < n$, for $l < t$, the set of l participants are not able to reconstruct any of the polynomials $h_1(x)$, $h_2(x)$, …, $h_{2k}(x)$ and thus, they are not able to to recover the secret image $\mathbf{I}$.

However, a set of at least t participants can recover the secret image as described in the previous section.

(3) Each participant's secret share s_i, $i = 1, 2, \ldots, n$ can be reused in the proposed scheme and it is not disclosed even after multiple secret images reconstructions. Even though n pseudo-shares have been exposed among many co-operating participants, the real secret shadows s_i are well protected by the properties of the two-variable one-way function.

In order to share the next secret image, the dealer D has to just select new random integers r_1, r_2, …, r_{2k} in $GF(q)$ and repeat steps (a) - (f) in the proposed algorithm. However, he does not have to distribute any new secret shares but just update the public values described in (f). i.e., if D wants to share another image $\mathbf{I_1}$ with corresponding matrix $\mathbf{M_1}$, then he has to compute $\mathbf{M'_1}$ for the new random numbers r_1, r_2, …, r_{2k} and publish $\mathbf{M''_1} = \mathbf{M_1} \oplus \mathbf{M^\star_1}$.

Changing the secret matrix $\mathbf{M}'$ for each new image $\mathbf{I}$ to be shared plays an essential role for the high security of the proposed scheme.

Considering the above security analysis the proposed scheme is a multi-use (t, n) secure secret image sharing scheme. However, the proposed scheme is ramp and we consider more precise theoretical security evaluation in the future.

B. Performance Analysis

In the proposed secret image sharing method, the size of each image share does not depend on the size of the secret image and this is an important property for the further process of the image shares, such as storage, transmission, or image hiding. Each participant only needs to hold one secret share s_i in order to be able to share the secret image. Thus the size of each image share is much smaller than the size of the image shares in other conventional methods.

The number of the public values is $2k(n-t+1) + m^2$. If the threshold value t is close to the number of the users n, then this number of public values does not differ much from the number of the pixels in the secret image.

Moreover, the proposed scheme recovers the secret image lossless and does not generate shadow images which are difficult to mange and identify.

However it is worth noting that while it is an advantage to archieve small image share size, in such sharing schemes most of the computation and transfer actions are performed by the dealer, that's why his presence plays an essential role.

V. EXAMPLE

Here we give an example to illustrate the proposed method.

Example 1. Let $t = 10$, $n = 16$, $q = 257$, $r_1 = 3$, $r_2 = 138$, $r_3 = 33$, $r_4 = 70$. The secret image is the 256×256 gray scale image of Lenna, given in Figure 1 and thus $k = 2$.

For $i = 1, 2 \ldots, 16$ participants public identifiers and participants secret shares are:

$u_i : [7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22]$,

$s_i : [224, 246, 141, 36, 30, 161, 25, 55, 39, 172, 115, 221, 203, 27, 59, 80]$.

Polynomials $h_1(x)$, $h_2(x)$, $h_3(x)$ and $h_4(x)$ are:

$h_1(x) = 226+228x+147x^2+239x^3+135x^4+4x^5+170x^6+197x^7+88x^8+110x^9+14x^{10}+69x^{11}+185x^{12}+147x^{13}+233x^{14}+9x^{15}$,

$h_2(x) = 34+43x+118x^2+171x^3+122x^4+48x^5+170x^6+150x^7+74x^8+99x^9+225x^{10}+86x^{11}+55x^{12}+57x^{13}+243x^{14}+15x^{15}$,

$h_3(x) = 184+230x+248x^2+39x^3+47x^4+106x^5+79x^6+236x^7+84x^8+25x^9+254x^{10}+123x^{11}+109x^{12}+201x^{13}+6x^{14}+225x^{15}$,

$h_4(x) = 161+43x+197x^2+208x^3+42x^4+173x^5+254x^6+100x^7+242x^8+72x^9+155x^{10}+0x^{11}+111x^{12}+230x^{13}+105x^{14}+112x^{15}$.

The public values for $i = 1, 2, \ldots, 6$ are:

$z_i^1 : [145, 208, 249, 64, 205, 182]$,

$z_i^2 : [168, 222, 52, 11, 229, 0]$,

$z_i^3 : [140, 199, 60, 94, 45, 14]$,

$z_i^4 : [149, 5, 28, 91, 183, 248]$.

The obtained 256×256 secret matrix $\mathbf{M}'$ and the public shared image $\mathbf{M}''$ are given in Fig. 2 and Fig. 3, respectively.

Fig. 1. Secret Image of Lenna.

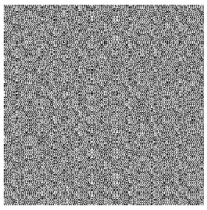

Fig. 2. Secret Matrix $\mathbf{M}'$.

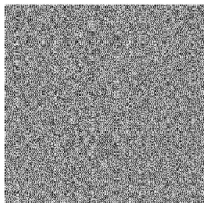

Fig. 3. Public Image $\mathbf{M}''$.

It can be seen that from the public image $\mathbf{M}''$, the secret image contents can not be figured out. However if a set of t participants pool out their pseudo-shares, then they can recover in a lossless manner the original secret image $\mathbf{I}$ in Figure 1 using the described reconstruction procedure. Moreover, a next image can be shared easily using the same secret sharing technique.

VI. CONCLUSIONS AND FUTURE WORKS

In this paper we propose a new lossless (t, n) secret images sharing method. It is realized by combining two-variable one-way functions and Shamir's secret sharing. Each participant only needs to hold one secret share in order to be able to share the secret image. Thus the size of each image share is much smaller than the size of the image shares in other conventional methods. Moreover, the proposed scheme is a multi-use secure secret image sharing scheme and does not generate shadow images which are difficult to mange and identify. The scheme is effective, secure and reliable, and suitable for network applications where a large number of users are required.

As a future work we consider the improving of the security performance of the proposed scheme. We also consider giving more precise and theoretical security analysis of the proposed method. In the current research we are considering the realization of the method to general access structure.

REFERENCES

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

[2] G. R. Blakley and C. Meadows, " Security of ramp schemes," *Advances in Cryptology-CRYPTO'84, LNCS 196*, pp.242-269, 1985.

[3] R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro, "On the size of the shares for secret sharing schemes," *Journal of Cryptology*, vol. 6, pp.157-167, 1993.

[4] T.ElGama, "A public-key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. on Inform. Theory*, vol. IF-31, pp.469-472, 1985.

[5] L. Harn, "Comment: Multistage secret sharing based on one-way function," *Electronics letters*, vol. 31(4), pp.262, 1995.

[6] J. He and E. Dawson, "Multistage secret sharing based on one-way function," *Electronics Letters*, vol. 30(19), pp.1591-1592, 1994.

[7] H.-X. Li, C.-T. Cheng and L.-J. Pang, "A new (t,n) Threshold Multi-secret Sharing Scheme," *CIS 2005*, vol. 3802, pp. 421 - 426, 2005.

[8] Li Bai, "A Reliable (k, n) Image Secret Sharing Scheme," *Proc. of the 2nd International symposium on Dependable, Autonomic and Secure Computing DASC'06*, pp.1-6, 2006.

[9] M. Noar and A. Shamir, "Visual Cryptography," *LNCS,* Vol. 950, pp.1-12, 1995.

[10] L.-J. Pang and Y.-M. Wang, "A new (t,n) multi- secret sharing scheme based on Shamir ' s secret sharing," *Applied Math*, vol. 167, pp. 840 - 848, 2005.

[11] S. Rinhua, Z. Hong, H. Liusheng and L. Yonglong, "A (t, n) Secret Sharing Scheme for Image Encryption," *Congress on Image and Signal Processing CISP 2008*, pp.3-6, 2008.

[12] R. L. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM 22,* vol. 21, pp.120-126, 1978.

[13] A. Shamir, "How to share a secret," *Communications of the ACM 22,* pp.612-613, 1979.

[14] G. J. Simmons, "How to (really) share a secret," *Proc. of Crypto'88,* Springer-Verlag, Berlin, LNCS 403, pp.390-448, 1990.

[15] D. R. Stinson, "Cryptography: Theory and Practice," CRC Press, 1995.

[16] C.-C. Thien and J.-C. Lin, "Secret image sharing," *Computers and Graphics,* Vol. 26, pp.765-770, 2002.

[17] R.-Z. Wang and C.-H. Su "Secret image sharing with smaller shadow images," *Pattern Recognition Letters,* Vol. 27, pp.551-555, 2006.

[18] C.-C.Yang, T.-Y.Chang, M.-S.Hwang, "A (t,n) multi-secret sharing scheme," *Applied Mathematics and Computation*, vol. 151, pp. 483-490, 2004.