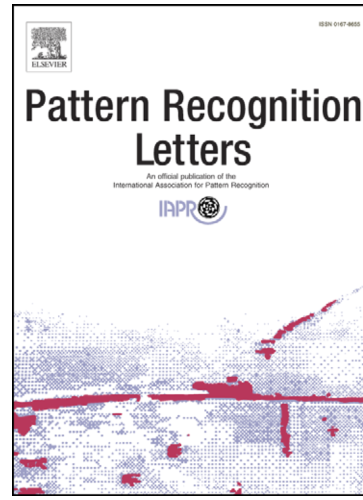


A Multi-threshold Secret Image Sharing Scheme Based on MSP

Cheng Guo, Chin-Chen Chang, Chuan Qin

PII: S0167-8655(12)00134-1
DOI: http://dx.doi.org/10.1016/j.patrec.2012.04.010
Reference: PATREC 5406

To appear in: *Pattern Recognition Letters*

Received Date: 28 November 2011

A Multi-threshold Secret Image Sharing Scheme Based on MSP

Cheng Guo[1], Chin-Chen Chang[2,3], Chuan Qin[2]

[1]Department of Computer Science,
National Tsing-Hua University, Hsinchu, 30013 Taiwan
E-mail: guo8016@gmail.com

[2]Department of Information Engineering and Computer Science,
Feng Chia University, Taichung 40724, Taiwan
E-mail: alan3c@gmail.com

[3]Department of Biomedical Imaging and Radiological Science,
Chinese Medical University, 40402, Taiwan
E-mail: alan3c@gmail.com

Correspondence address:
Professor Chin-Chen Chang
Department of Information Engineering and Computer Science,
Feng Chia University,
No. 100 Wenhwa Rd., Seatwen,
Taichung 40724, Taiwan, R.O.C.
Email: alan3c@gmail.com
TEL: 886-4-24517250 ext. 3790
FAX: 886-4-27066495

A Multi-threshold Secret Image Sharing Scheme Based on MSP

Cheng Guo[1], Chin-Chen Chang[2,3], Chuan Qin[2]

Abstract:

In this paper, we consider the problem of secret image sharing in groups with multi-threshold access structure. In such a case, multiple secret images can be shared among a group of participants, and each secret image is associated with a (potentially different) access structure. We employ Hsu et al.'s multi-secret sharing scheme based on monotone span programs (MSP) to propose a multi-threshold secret image sharing scheme. In our scheme, according to the real situation, we pre-defined the corresponding access structures. Using Hsu et al.'s method, we can achieve shadow data from multiple secret images according to these access structures. Then, we utilize the least significant bits (LSB) replacement to embed these shadow data into the cover image. Each secret image can be reconstructed losslessly by collecting a corresponding qualified subset of the shadow images. The experimental results demonstrate that the proposed scheme is feasible and efficient.

Keywords: Multi-threshold secret sharing, access structure, secret image sharing, monotone span programs

1. Introduction

Secret sharing was introduced in 1979 by Shamir (1979) and Blakley (1979), who developed two different methods to construct threshold secret sharing schemes based on the Lagrange interpolating polynomials and the linear projective geometry, respectively. By using a secret sharing scheme, a secret can be protected among a finite set of participants in such a way that only qualified sets of participants, which form the access structure of the scheme, can jointly reconstruct the secret.

Naor and Shamir (1995) developed visual cryptography that encrypts a secret image into some shares (transparencies) such that the secret image can be revealed to visual perception only by stacking any qualified subset of the shares without performing any cryptographic computations. However, in their scheme, the shadow images that are comprised of black and white pixels are meaningless. The interested reader can find more information about visual cryptography in (Yang, 2004; Wang and Su, 2006; Wang et al., 2007). In 2004, Lin and Tsai (2004) proposed a novel method for sharing secret images based on a (t, n) threshold scheme that had additional steganographic capabilities. In their scheme, shadow images are meaningful, and they look like the camouflage image. Furthermore, an image watermarking technique is employed to embed fragile watermark signals into the shadow images. Therefore, during the secret image reconstruction process, each shadow image can be verified for its fidelity. In 2007, Yang, Chen, Yu, and Wang (2007) presented a scheme to improve authentication ability and improve the quality of shadow images. However, the improved scheme resulted in the distortion of the visual quality of the shadow images. In 2009, Lin, Lee, and Chang (2009) employed the modulus operator to embed secret data into a cover image. In their scheme, some meaningful shadow images with satisfactory quality were obtained, and both the secret image and the cover image could be reconstructed losslessly. In addition, they utilized Rabin's signature to generate a certificate aimed at detecting cheaters. The above-mentioned schemes all proposed an authentication ability to protect the integrity of the shadow images. In 2010, Lin and Chan (2010) proposed an invertible secret image sharing scheme that almost satisfied all of the essential criteria of the secret image sharing mechanism. Also, their scheme offered a large embedding capacity compared with related secret image sharing schemes.

However, most researchers have focused on how to improve the visual quality of the shadow images and enlarge the embedding capacity, and very few people have paid any attention to research on the access structure of secret image sharing. In 2002, Tsai, Chang, and Chen (2002) proposed a multiple secret sharing method, in which multiple secret images can be shared among participants and each pair of shadow images can share a different secret image. But, their method can retrieve the secret image from only combinations of two shadow images. This is not a generalized secret image sharing scheme. In 2005, Feng, Wu, Tsai, and Chu (2005) proposed a scheme to achieve sharing multiple secrets according to any access structure, and each qualified set of the shadow images can share different secret images independently. However, Feng et al.'s scheme has following weaknesses. Firstly, the secret image cannot be recovered without distortion since all the pixels larger than 250 need to be modified to 250 in the secret sharing phase. Secondly, Feng et al.'s secret image sharing scheme is not perfect. That is, an attacker has a probability to get a correct secret image from an incomplete qualified subset of shadow images. Thirdly, the embedding capability of their scheme is instability. The radio of total secret capacity is within [1/2, 1]. In 2008, Feng, Wu, Tsai, and Chang (2008) also proposed a visual secret sharing scheme for hiding multiple secret images into two share images.

The access structure Γ of a secret sharing scheme is the collections of subsets of participant set P that can jointly compute the secret from their shadows. The characterization of the access structures of secret sharing schemes is one of the most important remaining problems in secret sharing. Due to the difficulty of finding efficient secret sharing schemes with generalized access structures, it is worthwhile to find families of access structures that have other useful properties for the applications of threshold cryptology. However, there are very few known constructions of secret image sharing schemes with generalized access structures. Therefore, we believe that it will be an interesting and challenging problem.

In the introductory work (Shamir, 1979), Shamir made the first attempt to propose a way to construct weighted threshold secret sharing. In his scheme, one positive weight is associated with each participant, and the secret can be reconstructed if, and only if, the sum of the weights assigned to participants who are reconstructing the secret is greater than or equal to a fixed threshold. Brickell (1990) proposed a method for constructing secret sharing schemes for multi-level and compartmented access structures. These two kinds of access structures were also proposed by Simmons (1990). In 2007, Farràs, Farré, and Padró (2007) presented a characterization of matroid-related, multipartite access structures in terms of discrete polymatroids. Also, they proposed an ideal multipartite secret sharing scheme. In 2007, Tassa (2007) proposed a hierarchical threshold secret sharing scheme based on the Birkhoff interpolation. In his scheme, the secret is shared by a set of participants partitioned into several levels, and the secret can be reconstructed by satisfying a sequence of threshold requirements.

In 1996, Jackson, Martin, and O’Keefe (1996) considered a kind of secret sharing scheme that permits a number of different secrets to be shared among a group of participants. Each secret is associated with a (potentially different) access structure, and a certain secret can be reconstructed by any group of participants from its associated access structure. Barwick and Jackson (2005) talked about the construction of a multi-secret threshold scheme in 2005. In 2011, Hsu, Cheng, Tang, and Zeng (2011) proposed an ideal multi-threshold secret sharing scheme based on monotone span programs (MSP). Later, they utilized the multi-threshold secret sharing scheme to provide secure and efficient group communication in wireless mesh networks (Hsu et al., 2011). Some secret sharing applications must protect more than one secret, possibly with different access structures associated with each secret. Also, secret image sharing has the same applications. For example, there are several secret images that must be shared among a group of people in such a way that different subsets of the group can cooperate to reconstruct the corresponding secret image. Inspired by the multi-threshold secret sharing scheme, we want to construct a multi-threshold secret image sharing scheme.

To the best of our knowledge, very few papers have discussed secret image sharing with a generalized access structure. In this paper, we study the characterization of the multi-threshold access structure and propose a new multi-threshold secret image sharing scheme based on MSP. In the process of driving shadow images, according to the real situation, we pre-defined the corresponding access structures. Then, we utilized Hsu et al.'s multi-threshold secret sharing scheme based on MSP to generate the corresponding shadow data. Then, we used the least significant bits (LSB) replacement to embed the shadow data into the cover image, aiming to generate the shadow images. According to the access structures, each secret image is associated with a certain subset of shadow images. The main contribution of this paper is to propose a novel multi-threshold secret image sharing scheme based on MSP. What's more, the shared multiple secret images can be recovered losslessly, and the embedding capability and the quality of shadow images are satisfactory.

2. Preliminary

In this section, first, we introduce monotone span programs (MSP), and then, we briefly review the multi-secret sharing scheme based on MSP proposed by Hsu et al. (2011), which is the major building blocks of our scheme.

2.1 Monotone span programs

In 1993, Karchmer and Wigderson (1993) introduced monotone span programs (MSP) as a linear algebraic model that computes a function. Let $\mathcal{M}(\kappa, M, \psi)$ be an MSP, where M is a $d \times l$ matrix over a finite field κ and $\psi : \{1, 2, \dots, d\} \rightarrow P\{P_1, P_2, \dots, P_n\}$ is a surjective labeling map. We call *d* the size of the MSP. For any subset $A \subseteq \{P_1, P_2, \dots, P_n\}$, there is a corresponding characteristic vector $\overrightarrow{\delta_A} = (\delta_1, \delta_2, \dots, \delta_n) \in \{0,1\}^n$. If, and only if, $P_i \in A$, $\delta_i = 1$. As to a target vector $\vec{v} \in \kappa^l \setminus (0, 0, \dots, 0)$, if, and only if, a monotone Boolean function $f : \{0,1\}^n \rightarrow \{0,1\}$,

$f(\overrightarrow{\delta_A})=1$, we can say that $\vec{v}\in span\{M_A\}$, where M_A consists of the rows ε of M with $\psi(\varepsilon)\in A$, and $\vec{v}\in span\{M_A\}$ means that a vector $\vec{w}$ exists such that $\vec{v}=\vec{w}M_A$.

2.2 Hsu et al.'s multi-secret sharing scheme

Hsu et al. (2011) proposed an ideal multi-secret sharing scheme based on MSP. They generalized the definition of an MSP to permit more than one target vector. Their scheme consists of three phases:

(1) The set up phase

Assume that m secrets $s_1,s_2,\ldots,s_m$ are shared among a set of participants $P=\{P_1,P_2,\ldots,P_n\}$ and that $s_i\in\kappa$. Let ϖ be the collection of all non-empty subsets of P. Suppose that $\varphi:\{s_1,s_2,\ldots,s_m\}\to\varpi$ is a bijection that associates each element in ϖ. We can define such an m-tuple $\vec{\Gamma}=(\Gamma_1,\Gamma_2,\ldots,\Gamma_m)$ of access structures as follows:

$(\Gamma_j)_{\min}=\{\varphi(s_j)\},\quad 1\le j\le m.$

Denote $\overline{V}=\kappa^n$ as the n-dimensional linear space over κ. Given a basis $\{e_1,e_2,\ldots,e_n\}$ of $\overline{V}$, the mapping $\mathrm{v}:\kappa\to\overline{V}$ can be constructed by $\mathrm{v}(x)=\sum_{i=1}^{n}x^{i-1}e_i$. Let $\vec{u_i}\in\{\mathrm{v}(x):x\in\kappa\}$, for i=1,2,…,n, be the n-dimensional vector associated with the participant P_i, where $\vec{u_i}$ is the row vector distributed to participant P_i, for $1\le i\le n$. Let $\vec{v_j}=\sum_{\substack{i\in\varphi(j)\\ x_i\in\kappa}}x_i\vec{u_i}$, for j = 1,2,…,m, be the m target vectors.

(2) The distribution phase

First, the dealer computes a vector $\vec{r} \in \kappa^n$ that satisfies the inner product $(\vec{v_j}, \vec{r}) = s_j$, for j = 1,2,…,m. Then, the dealer computes $M_i \vec{r}^{\tau}$ for participant P_i and transmits $M_i \vec{r}^{\tau}$ to each P_i as a shadow, for i = 1,2,…,n, where "τ" is the transpose and M_i denotes the matrix M restricted to the row i.

(3) The reconstruction phase

As to a qualified set of participants A, since $\vec{v_j} \in \sum_{i \in A} V_i$, where V_i is the space spanned by the row vectors of M distributed to participants i according to ψ, a vector $\vec{w}$ exists such that $\vec{v_j} = \vec{w} M_A$. The participants in A can compute $s_j = (\vec{v_j}, r) = \vec{v_j} \cdot \vec{r}^{\tau} = (\vec{w} M_A) \vec{r}^{\tau} = \vec{w}(M_A \vec{r}^{\tau})$. Therefore, the secret s_j can be reconstructed by a linear combination of the participants' shadows.

3. The proposed scheme

In the proposed scheme, we introduce MSP-based, multi-threshold secret sharing into secret image sharing, aiming at constructing a multi-threshold secret image sharing scheme in which there are multiple access structures on the set of shadow images, and the multiple secret images are shared among the shadow images in such a way that a different secret image is related to a corresponding access structure. That is, a different set of shadow images is likely to reconstruct different secret images.

Based on Hsu et al.'s multi-secret sharing scheme, we define the multi-threshold secret image sharing as follows:

Definition 1. Let *I* be a set of *n* shadow images and let $\vec{\Gamma} = (\Gamma_1, \Gamma_2, \ldots, \Gamma_m)$ be an *m*-tuple of access structures on the set of $I = \{I_1, I_2, \ldots, I_n\}$. There are *m* secret images $s_1, s_2, \ldots, s_m$, and each secret image s_i is associated with an access structure Γ_i on *I*, for $1 \le i \le m$. A qualified set of shadow images can reconstruct the corresponding secret image jointly.

For instance, assume that there is one set of shadow images $I = \{I_1, I_2, I_3\}$, and there is a set of three secret images $S = \{S_1, S_2, S_3\}$, which are shared in such a 3-tuple $\Gamma = (\Gamma_1, \Gamma_2, \Gamma_3)$ of access structures on *I* as follows:

$(\Gamma_1)_{\min} = \{\{I_1, I_2\}\}$, $(\Gamma_2)_{\min} = \{\{I_2, I_3\}\}$, and $(\Gamma_3)_{\min} = \{\{I_1, I_3\}\}$.

That is, shadow image I_1 and shadow image I_2 can jointly reconstruct the secret image S_1, shadow image I_2 and shadow image I_3 can jointly reconstruct the secret image S_2, and shadow image I_1 and shadow image I_3 can jointly reconstruct the secret image S_3. Obviously, a subset $A \in I$ is likely to reconstruct more than one secret image.

Assume that the cover image *O* has $M \times N$ pixels, $O = \{O_i \mid i = 1, 2, \ldots, (M \times N)\}$, and a set of secret images $S = \{S_1, S_2, \ldots, S_m\}$, and each secret image has $M_S \times N_S$ pixels. A dealer is responsible for constructing the access structures according to the real-life situation and generating related shadow images. In Section 3.1, we introduce a method to generate the shadow data for different secret images and corresponding access structures, and the embedding phase is presented in Section 3.2. Section 3.3 discusses how to retrieve the corresponding secret images from the qualified sets of shadow images according to different access structures.

3.1 Shadow data generation phase

Without loss of generality, $s_{11}, s_{21}, \ldots, s_{m1}$, for $0 \le s_{j1} \le 255,\ 1 \le j \le m$, denote the first pixel values of secret images $S = \{S_1, S_2, \ldots, S_m\}$, respectively, and $\vec{\Gamma} = (\Gamma_1, \Gamma_2, \ldots, \Gamma_m)$ denote the corresponding access structures. In our scheme, we continue to use some parameters from Hsu et al.'s scheme. The dealer performs the following steps:

Step 1. Let $\overline{V} = \kappa^n$ be the n-dimensional linear space over κ. Given a basis $\{e_1, e_2, \ldots, e_n\}$ of $\overline{V}$, the mapping $\mathrm{v}: \kappa \to \overline{V}$ can be constructed by $\mathrm{v}(x) = \sum_{i=1}^{n} x^{i-1} e_i$.

Step 2. Let $\vec{u}_i \in \{\mathrm{v}(x) : x \in \kappa\}$, for $1 \le i \le n$, be the n-dimensional vector associated with the ith shadow image. Let

$$\vec{v}_j = \sum_{\substack{i\in\varphi(j) \\ x_i\in\kappa}} x_i \vec{u}_i \text{, for } j = 1,2,\ldots,m, \qquad (1)$$

be the m target vectors.

Step 3. The dealer can build an MSP $\mathcal{M}(\kappa, M, \psi)$, where M is an $n \times n$ matrix over κ with the ith row vector $\vec{u}_i$.

Step 4. The dealer can compute a vector $\vec{r} \in \kappa^n$ that satisfies the inner product

$(\vec{v}_j, \vec{r}) = s_j$, for *j* = 1,2,…,*m*. Then, the dealer computes $M_i \vec{r}^{\tau}$ for each shadow image, for *i* = 1,2,…,*n*, where "τ" is the transpose and M_i denotes the matrix *M* restricted to the row *i*. The $M_i \vec{r}^{\tau}$ is the corresponding shadow data for each shadow image I_i, for *i* = 1,2,…,*n*, in view of the first pixel values $s_{11}, s_{21}, \ldots, s_{m1}$ of secret images and multi-threshold access structures $\vec{\Gamma} = (\Gamma_1, \Gamma_2, \ldots, \Gamma_m)$.

Step 5. By repeating Steps 1-4, the dealer can compute all shadow data according to the secret images and the access structures.

In Section 3.2, we will talk about how to embed these shadow data into the cover image. In the following, we will give an example to illustrate how to generate the shadow data.

Example 1. Let $\vec{\Gamma} = (\Gamma_1, \Gamma_2, \Gamma_3)$ be a 3-tuple of access structures on the set of shadow images $I = \{I_1, I_2, I_3\}$. There are three secret images S_1, S_2, S_3, and each secret image S_i is associated with an access structure Γ_i on *I*. Let s_{11}, s_{21} and s_{31} denote the first pixel values of the three secret images, respectively. The 3-tuple $\vec{\Gamma} = (\Gamma_1, \Gamma_2, \Gamma_3)$ of access structures on *I* is constructed as follows:

$\Gamma_1 = \{\{I_1, I_2\}\}$, $\Gamma_2 = \{\{I_2, I_3\}\}$ and $\Gamma_3 = \{\{I_1, I_3\}\}$.

Assume that $s_{11} = 5$, $s_{21} = 100$ and $s_{31} = 50$. Give a basis $\{e_1, e_2, e_3\}$ of $\overline{V}$ such that $e_1 = (1,0,0)$, $e_2 = (0,1,0)$ and $e_3 = (0,0,1)$.

The mapping v can be defined by $\mathrm{v}(x) = \sum_{i=1}^{n} x^{i-1} e_i$.

ACCEPTED MANUSCRIPT

Then, $\mathrm{v}(x) = (1,0,0) + (0,1,0)x + (0,0,1)x^2$, and

$$M = \begin{bmatrix} \mathrm{v}(1) \\ \mathrm{v}(2) \\ \mathrm{v}(3) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 9 \end{bmatrix}.$$

Associate I_1 with $\overrightarrow{u_1} = \mathrm{v}(1)$, I_2 with $\overrightarrow{u_2} = \mathrm{v}(2)$ and I_3 with $\overrightarrow{u_3} = \mathrm{v}(3)$.

According to (1), we can compute three target vectors $(\overrightarrow{v_1}, \overrightarrow{v_2}, \overrightarrow{v_3})$

$\overrightarrow{v_1} = (2,3,5)$, $\overrightarrow{v_2} = (2,5,13)$ and $\overrightarrow{v_3} = (2,4,10)$.

According to the equation $(\overrightarrow{v_i}, \vec{r}) = s_{i1}$, for i = 1,2,3, we can compute $\vec{r} = (-\frac{155}{2}, \frac{115}{2}, -\frac{5}{2})$.

Then, the shadow data SD_i for each shadow image I_i can be computed as follows:

$$SD_1 = M_1 \vec{r}^{\,\tau} = (1,1,1) \begin{pmatrix} -\frac{155}{2} \\ \frac{155}{2} \\ -\frac{5}{2} \end{pmatrix} = -\frac{45}{2},$$

$$SD_2 = M_2 \vec{r}^{\,\tau} = \frac{55}{2},$$

$$SD_3 = M_3 \vec{r}^{\,\tau} = \frac{145}{2}.$$

We can see that the corresponding pixel value of the secret image s_{i1}, for i = 1,2,3, can be reconstructed by computing a linear combination of their shadow data.

$s_{11} = SD_1 + SD_2 = 5$, $s_{21} = SD_2 + SD_3 = 100$, and $s_{31} = SD_1 + SD_3 = 50$.

3.2 Embedding phase

As was mentioned above, according to the secret images and the corresponding access structures, the dealer can compute shadow data for *n* shadow images. So far, the two most popular steganographic embedding methods are the modular operation and the least significant bits (LSB) replacement. Herein, we utilize the LSB-based steganographic method to embed the shadow data into the cover image.

From the example in Section 3.1, we can find that these shadow data are real numbers. In order to embed more shadow data into the cover image and recover the secret image without distortion, we correct the shadow data to 1 decimal place. As we know, the pixel value of the secret image can be reconstructed by a linear combination of the corresponding shadow data, and the pixel value is an integer. Therefore, if we correct the shadow data to 1 decimal place, the reconstructed pixel values will be complete and correct. And then, the secret image can be recovered losslessly.

Firstly, the shadow data is divided into two parts: the integral part and the decimal part. We utilize *Lena*, *Baboon*, and *Airplane* as the test images, and we can find that the integral part of the corresponding shadow data are within [-78, 200], [-90, 171], and [-45, 205], respectively. So, 10 bits are enough to represent the integral part of the shadow data and 4 bits are enough to represent the decimal part of the shadow data. In this paper, in order to simplify the proposed method, we utilize a simple 3-LSB substitution to embed shadow data into the cover image. Therefore, five-pixel blocks are enough to represent shadow data. Let o_i be the grayscale value of the cover image O and its binary representation be $(o_{i1}, o_{i2}, \ldots, o_{i8})$, where o_{i6}, o_{i7}, o_{i8} are the LSB bits. Let $(sd_{i1}, sd_{i2}, \ldots, sd_{i10})$ be the binary representation of the integral part of the shadow data SD_i, $(d_{i1}, d_{i2}, d_{i3}, d_{i4})$ be binary representation of the decimal part of the shadow data SD_i, and o_i' be the grayscale value of the corresponding shadow image. Fig. 1 shows one five-pixel square block of the cover image.

$o_i=(o_{i1},o_{i2},\ldots,o_{i8})$	$o_{i+1}=(o_{(i+1)1},o_{(i+1)2},\ldots,o_{(i+1)8})$
$o_{i+2}=(o_{(i+2)1},o_{(i+2)2},\ldots,o_{(i+2)8})$	$o_{i+3}=(o_{(i+3)1},o_{(i+3)2},\ldots,o_{(i+3)8}$
$o_{i+4}=(o_{(i+4)1},o_{(i+4)2},\ldots,o_{(i+4)8}$	

Fig. 1. The five-pixel square block of the cover image.

Fig. 2 demonstrates the five-pixel square block of the shadow image. Note that v_i represents the sign of the corresponding shadow data: The symbol "0" means negative and "1" means positive. The last four bits of the five-pixel square block are used to hide the decimal part of the shadow data $(d_{i1}, d_{i2}, d_{i3}, d_{i4})$, and other LSB bits are replaced by $sd_{i1}, sd_{i2}, \ldots, sd_{i10}$.

$o_i'=(o_{i1},o_{i2},\ldots,o_{i5},\boxed{v_i,}\ \boxed{sd_{i1}, sd_{i2})}$	$o_{i+1}'=(o_{(i+1)1},o_{(i+1)2},\ldots,o_{(i+1)5},\boxed{sd_{i3},sd_{i4},sd_{i5})}$
$o_{i+2}'=(o_{(i+2)1},o_{(i+2)2},\ldots,o_{(i+2)5},\boxed{sd_{i6},sd_{i7},sd_{i8})}$	$o_{i+3}'=(o_{(i+3)1},o_{(i+3)2},\ldots,o_{(i+3)5},\boxed{sd_{i9},sd_{i10},}\ \boxed{d_{i1})}$
$o_{i+4}'=(o_{(i+4)1},o_{(i+4)2},\ldots,o_{(i+4)5},\boxed{d_{i2},d_{i3},d_{i4})}$	

Fig. 2. The five-pixel square block of the shadow image.

We embed the generated shadow data into the cover image in this manner. Repeat the above procedure until all shadow data are embedded.

3.3 Protection phase

One fraudulent participant may provide a false shadow image and fool the other participants during the recovery of the secret image. Therefore, it is important to verify the integrity of the shadow images. In our scheme, the dealer can publish a little public information for shadow images that can be used to prevent the dishonest participants.

Step 1. Choose a public collision-free one-way hash function $h(x)$ and a large prime number q such that $h(x)<q$.

Step 2. Compute $T=\sum_{i=1}^{n} h(\tilde{O}_i)q^{2(i-1)}+\sum_{i=1}^{n-1} cq^{2i-1}$, where $\tilde{O}_i$ denotes the ith shadow image, and c is a positive constant randomly chosen over $GF(q)$.

Step 3. Publish T, $h(x)$ and q.

3.4 Secret image retrieving phase

Firstly, each involved participant can perform the following steps to determine the validity of the shadow images. Let G be a qualified subset of shadow images.

Step 1. Compute $T^*=\sum_{\tilde{O}_i\in G} h(\tilde{O}_i)q^{2(i-1)}$.

Step 2. For each shadow image $\tilde{O}_i \in G$, check whether $\left\lfloor \frac{T-T^*}{q^{2(i-1)}} \right\rfloor (\bmod q)=0$.

Step 3. If the equation holds, the shadow image is valid; otherwise, the shadow image is tampered.

In this paper, we will not iterate the mathematical background of this authentication mechanism. Readers can refer to the detail in Wu and Wu (1995).

According to access structures, given any qualified subset of shadow images, the corresponding secret image can be reconstructed. Extract the shadow data from the given shadow images, and the pixel value of the related secret image can be reconstructed by computing a linear combination of their shadow data. By repeating these processes, all pixel values of the secret image can be computed, and, the secret image can be reconstructed losslessly.

Example 2. Assume that the access structures are $\Gamma_1 = \{\{I_1, I_2\}\}$, $\Gamma_2 = \{\{I_1, I_3\}\}$ and $\Gamma_3 = \{\{I_1, I_2, I_3\}\}$. The *i*th pixel values of the three secret images are denoted as s_{1i}, s_{2i} and s_{3i}, respectively, and the corresponding shadow data are SD_{i1}, SD_{i2} and SD_{i3}, respectively. Then, the *i*th pixel values of the three secret images, s_{1i}, s_{2i} and s_{3i}, can be computed as follows:

$$s_{1i} = SD_{i1} + SD_{i2},$$

$$s_{2i} = SD_{i1} + SD_{i3},$$

$$s_{3i} = SD_{i1} + SD_{i2} + SD_{i3}.$$

4. Experimental results and analysis

In this section, we conduct simulations to demonstrate the feasibility of the proposed scheme, and the results of these simulations are discussed.

4.1 Simulation results

In the experiments, we assumed that there were three secret images that are shared in 3-tuple $\vec{\Gamma} = (\Gamma_1, \Gamma_2, \Gamma_3)$ access structures on shadow images $I = (I_1, I_2, I_3)$ as follows:

$(\Gamma_1)_{\min} = \{\{I_1, I_2\}\}$, $(\Gamma_2)_{\min} = \{\{I_2, I_3\}\}$, and $(\Gamma_3)_{\min} = \{\{I_1, I_3\}\}$.

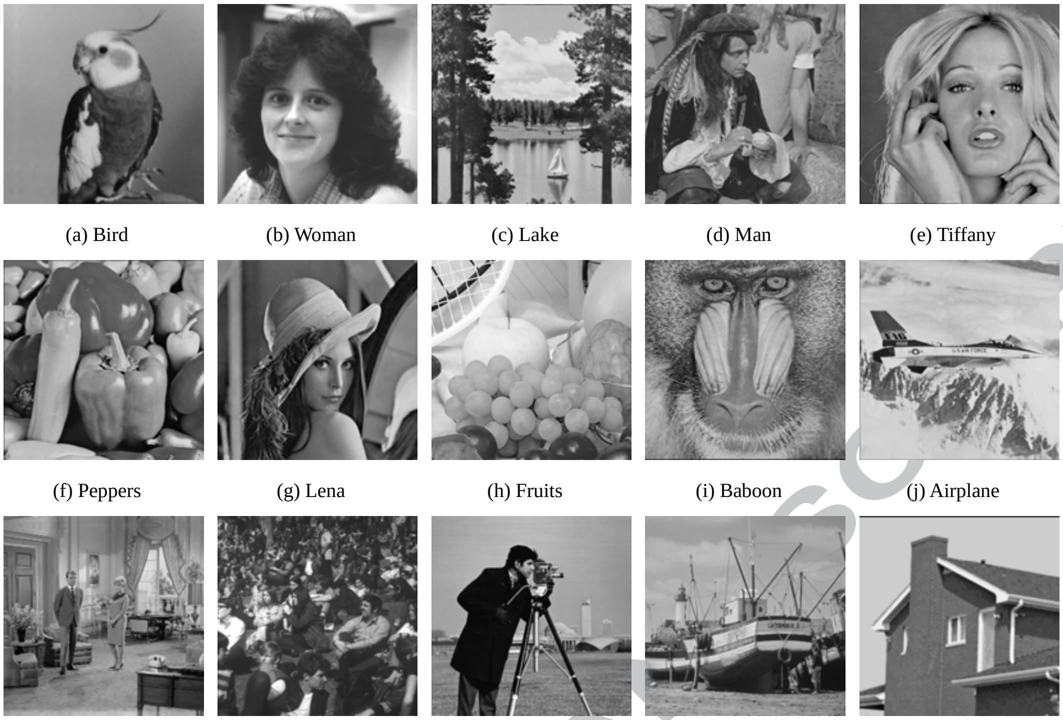
As shown in Fig. 3, the test images contain 15 gray-level images with sizes of 512×512 pixels. Fig. 4 shows three secret images, i.e., *Lena*, *Baboon*, and *Airplane*, that are 200×200 pixels. Herein, the criterion for the visual quality of the shadow images is the peak-signal-to-noise ratio (PSNR), which is defined as:

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

where *MSE* is the mean-square error between the cover image and the shadow image. If the cover image consists of $M \times N$ pixels, *MSE* is defined as:

$$MSE = \frac{1}{M \times N} \sum_{j=1}^{M \times N} (p_j - p'_j)^2, \qquad (3)$$

where p_j is the original pixel value, and p'_j is the pixel value of the shadow image.



(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. 3. The test images.

(a) Lena (b) Baboon (c) Airplane

Fig. 4. The secret images.

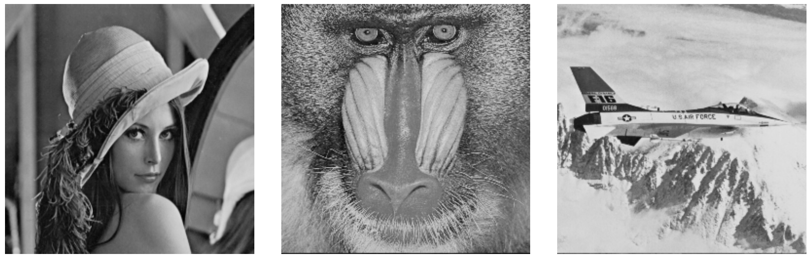
Table 1 lists the PSNR values of the shadow images with various test images using the given access structures. Since we utilize a simple LSB substitution to embed the shadow data into the cover image, the pixel values of the shadow images in the proposed scheme are slightly lower than those of the existing secret image sharing methods. However, our scheme presents a generalized threshold access structure for secret image sharing. Furthermore, the distortion between the shadow images and the cover image is acceptable.

Table 1

The PSNR value (dB) of the shadow images for test images.

Test images	PSNR (dB)		
	Shadow image 1	Shadow image 2	Shadow image 3
Bird	40.27	40.29	40.28
Woman	40.21	40.17	40.23
Lake	40.28	40.27	40.28
Man	40.28	40.28	40.27
Tiffany	40.33	40.34	40.33
Peppers	40.26	40.28	40.26
Lena	40.27	40.27	40.27
Fruits	40.26	40.27	40.26
Baboon	40.26	40.26	40.27
Airplane	40.30	40.34	40.30
Couple	40.27	40.27	40.27
Crowd	40.20	40.15	40.21
Cameraman	40.29	40.27	40.29
Boat	40.29	40.30	40.29
House	39.94	39.71	39.99

In the experiment, we designed a specific access structure in which shadow image 1 and shadow image 2 can cooperate to reconstruct secret image 1, "*Lena*." Similarly, shadow image 2 and shadow image 3 can cooperate to reconstruct secret image 2, "*Baboon*," and shadow image 1 and shadow image 3 can cooperate to reconstruct secret image 3, "*Airplane*." Of course, depending on the situation at hand, we also can design other access structures. Fig. 5 shows the extracted secret images. We can see that the secret images can be reconstructed losslessly.



(a) The reconstructed Pepper (b) The reconstructed Lena (c) The reconstructed Airplane

Fig. 5. The reconstructed secret images.

4.2 Validity and security analysis

In this subsection, we analyze the validity and the security of the proposed multi-threshold secret image sharing scheme.

Theorem 1. Any subset $A \in \Gamma_j$ of shadow data can reconstruct the pixel value of the secret image S_j by a linear combination of their shadow data.

Proof. Observe that $V_i = span\{\overrightarrow{u_i}\}$ for $1 \le i \le n$, and $\overrightarrow{v_j} = \sum_{\substack{i\in\varphi(j)\\ x_i \in K'}} x_i \overrightarrow{u_i}$ for $1 \le j \le m$, where $\overrightarrow{v_j}$ is a target vector associated with a pixel value of the secret image. They imply that there must exist a linear combination of the vectors in $\sum_{i\in\varphi(j)} V_i$ such that it equals to $\overrightarrow{v_j} = \sum_{\substack{i\in\varphi(j)\\ x_i \in K'}} x_i \overrightarrow{u_i}$. Namely, $\overrightarrow{v_j} = \sum_{\substack{i\in\varphi(j)\\ x_i \in K'}} x_i \overrightarrow{u_i} \in \sum_{i\in\varphi(j)} V_i$. Therefore, the pixel value of the secret image can be reconstructed by a linear combination of a qualified subset of shadow data.

Theorem 2. The proposed scheme is a perfect multi-threshold secret image sharing scheme, that is, any subset $B \notin \Gamma_j$ of shadow images cannot obtain any information on the secret image S_j.

Proof. Due to the fact that $\overrightarrow{u_i}$ for $1 \le i \le n$ is the form **v**(x), where the vectors **v**(x)

have Vandermonde coordinates with respect to the given basis of $\overline{V}$, and every set of at most n vectors of the form $\mathbf{v}(x)$ is independent, we obtain that $\overrightarrow{u_1}, \overrightarrow{u_2}, \ldots, \overrightarrow{u_n}$ are linearly independent. Furthermore, $V_i = span\{\overrightarrow{u_i}\}$ for $1 \le i \le n$, and the target vector $\overrightarrow{v_j} = \sum_{\substack{i\in\varphi(j)\\ x_i\in\kappa'}} x_i \overrightarrow{u_i}$. It implies that there is not a linear combination of their shadow data such that it equals to the corresponding pixel value of the secret image. Therefore, any subset $B \notin \Gamma_j$ of shadow images cannot reconstruct the secret image S_j.

4.3 Discussion

In the traditional (t, n) secret image sharing schemes, the secret image is shared among n shadow images, and only t or more shadow images can reconstruct the secret image; if the number of shadow images is equal to or less than (t-1), the shadow images cannot recover the secret image. However, a generalized threshold access structure could have other useful properties for the application. In the proposed scheme, we introduced multiple threshold access structures in secret image sharing. In our scheme, we define multiple threshold access structures according to the real situation, and every secret image is associated with a qualified subset of shadow images. Different qualified subsets of shadow images with different access structures can reconstruct different secret images.

The procedure of generating shadow images consists of two phases, i.e. the shadow data generation phase and the embedding phase. In the shadow data generation phase, we utilized Hsu et al.'s scheme based on MSP to generate shadow data with the properties of multiple threshold access structures. Then, in order to simplify the proposed scheme, we used a simple 3-LSB substitution to embed shadow data into the cover image. Since the corresponding shadow data are real numbers, we divided these shadow data into two parts: the integral part and the decimal part, to deal with. Meanwhile, correcting the shadow data to 1 decimal place is able to effectively ensure that the secret image can be reconstructed losslessly. Of course, many variations based on LSB substitution also can be utilized to embed shadow data. It may be possible for these steganographic methods to improve the visual quality of shadow images and enlarge the embedding capacity. However, it is beyond the scope of this paper to provide all of the details associated with this issue.

Table 2

Comparisons of the related secret image sharing schemes.

Functionality	Tsai et al. (2002)	Feng et al. (2005)	Yang et al (2007)	Chang et al. (2008)	Lin et al. (2009)	Lin and Chan (2010)	Ours
Multi-secret image sharing	Yes	Yes	No	No	No	No	Yes
Multi-threshold access structures	No	Yes	No	No	No	No	Yes
Meaningful shadow image	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Quality of shadow images	39 dB	42 dB	41 dB	41 dB	44 dB	43 dB	40 dB
Lossless secret image	Yes	No	Yes	No	Yes	Yes	Yes
Authentication	No	No	Yes	Yes	Yes	No	Yes
Embedding capacity	$\frac{M\times N}{9}\times\frac{n(n-1)}{2}$	$[\frac{1}{2}, 1]\times M\times N$	$\frac{M\times N}{4}$	$\frac{M\times N}{4}$	$\frac{(t-3)\times M\times N}{3}$	$\frac{(t-1)\times M\times N}{\lceil\log_\sigma 255\rceil}$	$\frac{M\times N}{5}\times m$

Table 2 gives the functionality comparison of our scheme and the related schemes. As presented in Table 2, the shadow images are meaningful, the visual quality of the shadow images is acceptable, as is the embedding capacity, and the secret image can be recovered without distortion. Tsai et al.'s scheme (2002) and Feng et al.'s scheme (2005) proposed two effective ways to share multiple secret images, respectively. These image sharing schemes had some additional advantages, but they also had to withstand some shortcomings, such that the secret hidden capacity is limited and their schemes did not provide the authentication ability. Compared with Tsai et al.'s scheme (2002) and Feng et al.'s scheme (2005), our proposed scheme achieves higher flexibility in various applications, and the secret image can be recovered losslessly. In addition, our proposed scheme provides authentication ability by publishing a little public information. The related works (Yang et al., 2007; Chang et al., 2008) achieved the authentication ability to verify the integrity of the shadow images by embedding some authentication bits into the shadow images. For Lin et al.'s scheme (2009), they prevented the dishonest participants by generating an additional certificate for each shadow image. In order to improve the quality of shadow images, increase the capacity of the embedded secret data, and retrieve the lossless secret image, Lin and Chan's scheme (2010) did not consider the authentication ability that prevents dishonest participants from cheating.

Compared with related schemes, our scheme not only satisfies all of these essentials, but also can share multiple secret images simultaneously and provide multiple threshold access structures.

5. Conclusions

In this paper, we proposed a multi-threshold secret image sharing scheme based on MSP. The main objective was to construct a multi-threshold access structure in secret image sharing. In our scheme, we can pre-define different access structures, and each secret image is associated with an access structure on shadow images. Meanwhile, in the secret image retrieving phase, we also provide an authentication mechanism to verify the integrity of the shadow images. And, each authorized subset of shadow images can reconstruct the corresponding secret image without distortion. The experimental results showed that the proposed scheme is feasible and that it also can achieve both the high visual quality of the shadow images and high embedding capacity.

It would be worthwhile to conduct research to determine how to construct an efficient secret sharing scheme for every given access structure. However, the problem of setting up secret image sharing schemes with generalized access structures has been largely ignored by researchers in this area. We hope that some innovative and ingenious approaches will be found by investigating and studying this problem.

References:

Barwick, S.G., Jackson, W.A., 2005. An optimal multisecret threshold scheme construction. Designs, Codes and Cryptography 37 (3), 367-389.

Blakley, G.R., 1979. Safeguarding cryptographic keys. In: Proc. AFIPS National Comput. Conf., 48, 313-317.

Brickell, E.F., 1990. Some ideal secret sharing schemes. Adv. Cryptol.: Eurocrypt'89, Springer-Verlag, Berlin, 468-475.

Chang, C.C., Hsieh, Y.P., Lin, C.H., 2008. Sharing secrets in stego images with authentication. Pattern Recogn. 41 (10), 3130-3137.

Farràs, O., Farré, J.M., Padró, C., 2007. Ideal multipartite secret sharing schemes. Adv. Cryptol.: Eurocrypt' 2007, Springer-Verlag, Berlin, 448-465.

Feng, J.B., Wu, H.C., Tsai, C.S., Chang, Y.F., 2008. Visual secret sharing for multiple secrets. Pattern Recogn. 41 (12), 3572-3581.

Feng, J.B., Wu, H.C., Tsai, C.S., Chu, Y.P., 2005. A new multi-secret images sharing scheme using Largrange's interpolation. J. Syst. Software 76 (3), 327-339.

Hsu, C.F., Cheng, Q., Tang, X.M., Zeng, B., 2011. An ideal multi-secret sharing scheme based on MSP. Information Sciences 181 (7), 1403-1409.

Hsu, C.F., Cui, G.H., Cheng, Q., Chen, J., 2011. A novel linear multi-secret sharing scheme for group communication in wireless mesh networks. J. Network and Computer Applications 34 (2), 464-468.

Jackson, W.A., Martin, K.M., O'Keefe, C.M., 1996. Ideal secret sharing schemes with multiple secrets. J. Cryptol. 9 (4), 233-250.

Karchmer, M., Wigderson, A., 1993. On span programes. In: Proc. the Eighth Annual Conf. on Structure in Complexity, San Diego, CA, 102-111.

Lin, P.Y., Chan, C.S., 2010. Invertible secret image sharing with steganography. Pattern Recogn. Lett. 31 (13), 1887-1893.

Lin, P.Y., Lee, J.S., Chang, C.C., 2009. Distortion-free secret image sharing mechanism using modulus operator. Pattern Recogn. 42 (5), 886-895.

Lin, C., Tsai, W., 2004. Secret image sharing with steganography and authentication. J. Syst. Software 73 (3), 405-414.

Noar, N., Shamir, A., 1995. Visual cryptography. Adv. Cryptol.: Eurocrypt'94. Springer- Verlag, Berlin. 1-12.

Shamir, A., 1979. How to share a secret. Commun. ACM 22 (11), 612-613.

Simmons, G.J., 1990. How to (really) share a secret. Adv. Cryptol.: Crypto'88, Springer-Verlag, Berlin, 390-448.

Tassa, T., 2007. Hierarchical Threshold Secret Sharing. J. Cryptol. 20 (2), 237-264.

Tsai, C.S., Chang, C.C., Chen, T.S., 2002. Sharing multiple secrets in digital images. J. Syst. Software 64 (2), 163-170.

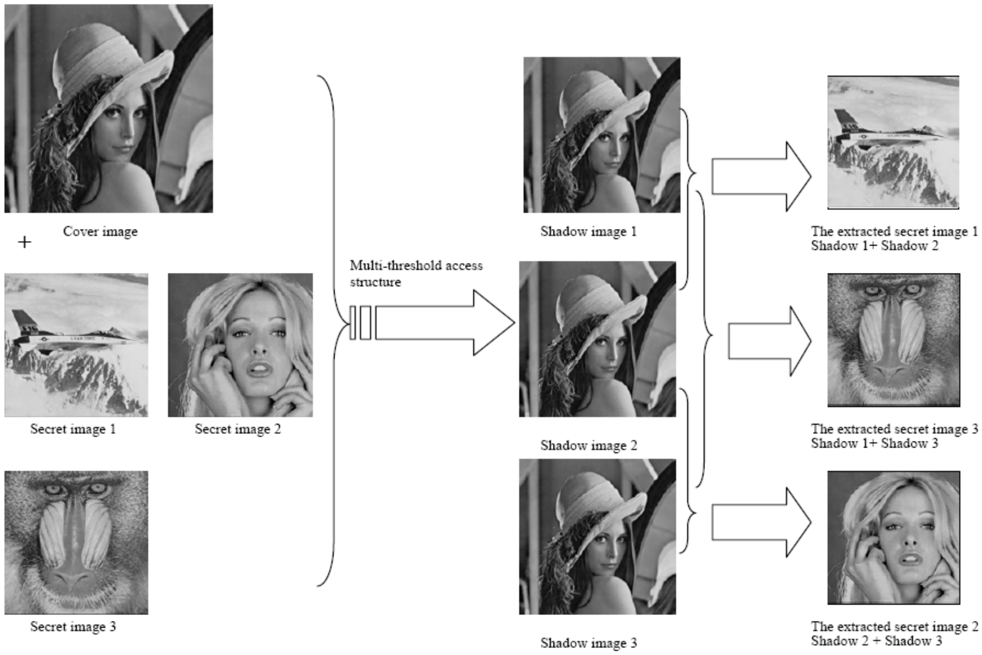
Wang, R.Z., Su, C.H., 2006. Secret image sharing with smaller shadow images. Pattern Recogn. Lett. 27 (6), 551-555.

Wang, D., Zhang, L., Ma, N., Li, X., 2007. Two secret sharing schemes based on Boolean operations. Pattern Recogn. 40 (10), 2776-2785.

Wu, T.C., Wu, T.S., 1995. Cheating detection and cheater identification in secret sharing schemes. IEE Pro. Comput. Digit. Tech. 142 (5), 367-369.

Yang, C. N., 2004. New visual secret sharing schemes using probabilistic method. Pattern Recogn. Lett. 25 (4), 481-494.

Yang, C.N., Chen, T.S., Yu, K.H., Wang, C.C., 2007. Improvements of image sharing with steganography and authentication. J. Syst. Software 80 (7), 1070-1076.

529 
Cover image
+
Secret image 1
Secret image 2
Secret image 3
Multi-threshold access structure
Shadow image 1
Shadow image 2
Shadow image 3
The extracted secret image 1
Shadow 1+ Shadow 2
The extracted secret image 3
Shadow 1+ Shadow 3
The extracted secret image 2
Shadow 2 + Shadow 3

Research Highlights

> The proposed scheme can share multiple secret images. > We can construct multiple threshold access structures. > Each secret image can be related to a corresponding access structure. > Each qualified subset of shadow images can reconstruct the different secret image.