Pattern Recognition Letters 33 (2012) 83–91

Contents lists available at SciVerse ScienceDirect

Pattern Recognition Letters

journal homepage: www.elsevier.com/locate/patrec

A hierarchical threshold secret image sharing

Cheng Guo [a], Chin-Chen Chang [b,c,*], Chuan Qin [b]

[a] Department of Computer Science, National Tsing-Hua University, Hsinchu 30013, Taiwan, ROC
[b] Department of Information Engineering and Computer Science, Feng Chia University, No. 100 Wenhwa Rd., Seatwen, Taichung 40724, Taiwan, ROC
[c] Department of Biomedical Imaging and Radiological Science, Chinese Medical University, Taichung 40402, Taiwan, ROC

ARTICLE INFO

Article history:
Received 31 March 2011
Available online 1 October 2011
Communicated by S. Sarkar

Keywords:
Hierarchical threshold
Distortion-free
Secret image sharing
Access structure

ABSTRACT

In the traditional secret image sharing schemes, the shadow images are generated by embedding the secret data into the cover image such that a sufficient number of shadow images can cooperate to reconstruct the secret image. In the process of reconstruction, each shadow image plays an equivalent role. However, a general threshold access structure could have other useful properties for the application. In this paper, we consider the problem of secret shadow images with a hierarchical threshold structure, employing Tassa's hierarchical secret sharing to propose a hierarchical threshold secret image sharing scheme. In our scheme, the shadow images are partitioned into several levels, and the threshold access structure is determined by a sequence of threshold requirements. If and only if the shadow images involved satisfy the threshold requirements, the secret image can be reconstructed without distortion.

1. Introduction

A secret sharing scheme is a technique to share a secret among a group of participants. The secret data can be divided into several pieces, called secret shadows, which are distributed to the participants. If enough participants cooperate to reconstruct the secret data and pool their secret shadows together, the secret data can be reconstructed.

In 1979, the first (t,n) threshold secret sharing schemes were proposed by Shamir (1979) and Blakley (1979), based on Lagrange interpolating and liner project geometry, respectively. In 1995, based on the concept of threshold secret sharing, Naor and Shamir (1995) introduced visual cryptology, or the visual secret sharing scheme (VSS scheme). In the (t,n) VSS schemes (Yang, 2004; Wang et al., 2007; Chang et al., 2009; Lin and Wang, 2010), the secret data is an image comprised of black and white pixels that is encoded into n shadow images, and the secret image can be reconstructed only by stacking t of the shadow images; no information about the secret image can be obtained from $t-1$ or fewer shadow images. However, in this kind of visual secret sharing scheme, the shadow images are meaningless, which tends to call attention to them. In 2003, Thien and Lin (2003) utilized the steganography approach to embed the secret image into a cover image to generate the shadow images. In their scheme, the shadow images are meaningful and the distortion between the cover image and the shadow images is imperceptible. Since then, the secret image sharing schemes (Lin and Tsai, 2004; Wu et al., 2004; Yang et al., 2007; Chang et al., 2008; Zhao et al., 2009; Lin et al., 2009; Eslami et al., 2010; Lin and Chan, 2010) have been extensively developed to meet the requirements of our daily lives. In 2004, Lin and Tsai (2004) proposed a secret image sharing scheme with steganography and authentication, in which the shadow images are meaningful, while the reconstructed secret image is distorted slightly. In 2007, Yang et al. (2007) improved Lin and Tsai's scheme by making it possible to restore a distortion free secret image, but their scheme reduces the visual quality of the shadow images and increases the risk of their being deceived by malicious intruders. In 2009, Lin et al. (2009) employed the modulus operator to embed the secret image into a cover image, where each participant can obtain a meaningful shadow image with high visual quality, the authorized participants can detect intruders, and the secret image and the cover image can be recovered losslessly. In 2010, Lin and Chan (2010) proposed a new secret sharing scheme that achieves an excellent combination of embedding capacity and the visual quality of shadow images. In addition, their scheme can reconstruct the secret image and the cover image without distortion.

However, in all of these schemes, all shadow images are equal in terms of privileges and authority in the process of reconstructing the secret image. In this paper, we consider a special situation in which the shadow images may be not equal. We achieve a hierarchical threshold access structure by introducing Tassa's threshold secret sharing scheme, and we present a novel hierarchical threshold secret image sharing scheme.

Secret sharing schemes have been extensively studied, and secret image sharing and its many variations form an important research direction. In 2007, Tassa (2007) proposed a hierarchical threshold secret sharing scheme. Tassa's scheme is based on the

* Corresponding author at: Department of Information Engineering and Computer Science, Feng Chia University, No. 100 Wenhwa Rd., Seatwen, Taichung 40724, Taiwan, ROC. Tel.: +886 4 24517250x3790; fax: +886 4 27066495.

E-mail addresses: guo8016@gmail.com (C. Guo), alan3c@gmail.com (C.-C. Chang), qin@usst.edu.cn (C. Qin).

0167-8655/$ - see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.patrec.2011.09.030

Birkhoff interpolation. In their scheme, the secret is shared by a set of participants partitioned into several levels, and the secret data can be reconstructed by satisfying a sequence of threshold requirements (e.g., it has at least t_0 participants from the highest level, as well as at least $t_1 > t_0$ participants from the two highest levels and so forth). There are many real-life examples of hierarchical threshold schemes. Consider the following example. According to a graduate school's policy, a graduate who wants to apply for a postgraduate position must have letters of recommendation. Assume that the graduate school's policy concerning such recommendations is that the candidate must have at least two recommendations from professors and at least five recommendations from a combination of professors and associate professors. In this scenario, the professor is the highest level, the associate professor is the second-highest level, the corresponding threshold values are $t_0 = 2$ and $t_1 = 5$, and the shadows of a higher level can substitute for those of a lower level. In this example, recommendations from two professors and three associate professors, three professors and two associate professors, four professors and one associate professor, or five professors are all acceptable.

The same situation also appears in the sharing of secret images. Inspired by the hierarchical secret sharing scheme, we construct a hierarchical threshold secret image sharing scheme.

The existing secret image sharing schemes (Lin and Tsai, 2004; Wu et al., 2004; Yang et al., 2007; Chang et al., 2008; Zhao et al., 2009; Lin et al., 2009; Eslami et al., 2010; Lin and Chan, 2010) have tried to improve the visual quality of the shadow images so the suspicions of malicious intruders won't be aroused. Two of the most popular steganographic methods are the least significant bits (LSB) replacement and the modulus operation. Shamir's (t,n) threshold scheme is an ingenious method with which to share secret data among n participants. Traditional secret image sharing schemes (Lin et al., 2009; Lin and Chan, 2010) usually transformed the secret image pixels into base-m representation, $s_1, s_2, \ldots, s_{M_S \times N_S} \times \lceil \log_m 255 \rceil$, where $M_S \times N_S$ denotes the size of the secret image, and then constructed a Lagrange interpolation polynomial $f(x)$ by using the $s_1, s_2, \ldots, s_{M_S \times N_S \times \lceil \log_m 255 \rceil}$ as the polynomial coefficients. In order to make the shadow images meaningful for the purposes of camouflage—that is, to diminish the distortion of the shadow images—they utilized the modulus operator to embed secret data into the pixel of the cover image.

However, in Tassa's scheme, the hierarchical threshold access structure can work so long as the modulus p is far greater than the threshold t, so it is difficult to combine the existing secret image sharing schemes based on the modulus operation directly with Tassa's hierarchical threshold access structure. Therefore, how to combine the hierarchical threshold access structure proposed by Tassa (2007) with steganographic methods is our scheme's main challenge. We also need to guarantee that the secret image can be reconstructed losslessly.

To the best of our knowledge, no hierarchical secret image sharing schemes have been proposed in the literature to date. Since we believe that the application of secret image sharing in groups with hierarchical structure has good prospects, we provide a novel hierarchical threshold secret image sharing scheme.

In our scheme, the n shadow images generated from the secret image and the cover image are partitioned into several levels such that each level has a certain number of shadow images and a corresponding threshold. The secret image can be reconstructed only by meeting a sequence of threshold requirements.

The novel characteristic of the proposed scheme is not available in the existing mechanisms, so the proposed scheme has the potential to work in many applications. In addition to the unique hierarchical threshold characteristic, our proposed scheme has three key characteristics:

1. The secret image can be retrieved losslessly.
2. The scheme solves the problems of overflow and underflow.
3. Unlike the traditional secret image sharing schemes in which the embedding capacity is proportional to the increase of t, the capacity of the embedded secret data is stable and large.

2. Review of Tassa's hierarchical threshold secret sharing scheme

In case of hierarchical threshold secret sharing, the set of participants is partitioned into some levels $P_0, P_1, \ldots, P_m$ and the access structure is then determined by a sequence of threshold requirements $t_0, t_1, \ldots, t_m$ according to their hierarchy. Tassa's method (2007) for hierarchical threshold secret sharing is based on Birkhoff interpolation. In this section, we briefly introduce Tassa's hierarchical threshold secret sharing scheme. Assume that there are n participants and one dealer responsible for generating the secret shadows and distributing them to the participants.

1. The dealer generates the polynomial $F(x)$ of degree at most $t_m - 1$ over GF_q, $F(x) = S + a_1 x + a_2 x^2 + \cdots + a_{t_m - 1} x^{t_m - 1}$, where S is the shared secret data.
2. An element $\mathrm{i} \in GF_q$ is assigned to the participant i, for all $1 \leqslant i \leqslant n$.
3. For any level j, each participant i from the jth level will receive the secret shadow $F^{t_j - 1}(i)$, where $F^{t_j - 1}(.)$ is the (t_{j-1})th derivative of $F(x)$ and $t_0 = 0$.
4. In the reconstruction phase, the participants can cooperate to reconstruct the shared secret data by using Birkhoff interpolation.

3. The proposed scheme

Given a shared secret image S and a cover image O, the dealer can generate n shadow images p_i, for $i = 1, 2, \ldots, n$. In the proposed scheme, the n shadow images do not have equal status; instead, the secret image is shared among n shadow images that are partitioned into several levels. Based on Tassa's definition (Tassa, 2007), we define the hierarchical secret image sharing as follows:

Definition 1. Let P be a set of n shadow images and assume that P is composed of levels; that is, $P = \cup_{i=0}^{m} P_i$, where $P_i \cap P_j = \phi$ for all $i \neq j$ and $i, j \in [0, m]$. Let $\mathbf{t} = \{t_i\}_{i=0}^{m}$ be a monotonically increasing sequence of integers. Then the $(\mathbf{t}, n)$ hierarchical threshold access structure is

$$\Gamma = \left\{ V \subset P : \left| V \cap \left(\bigcup_{j=0}^{i} P_j \right) \right| \geqslant t_i, \forall i \in \{0, 1, \ldots, m\} \right\}.$$

3.1. Initialization procedure

First, the dealer constructs n secret shadow images and divides these n shadow images into $(m+1)$ levels $P = \{P_0, P_1, \ldots, P_m\}$ according to the real-life situation. Then the dealer sets a sequence of threshold values $\{t_0, t_1, \ldots, t_m\}$, $0 < t_0 < t_1 \ldots < t_m$, where $t = t_m$ is the overall number of shadow images that are required for recovery of the secret image, and assumes that

$$\begin{aligned}
&p_1, p_2, \ldots, p_{l_0} \in P_0, \\
&p_{l_0+1}, p_{l_0+2}, \ldots, p_{l_1} \in P_1, \\
&\vdots \\
&p_{l_{m-1}+1}, p_{l_{m-1}+2}, \ldots, p_n \in P_m,
\end{aligned}$$

where $p_i, 0 \leqslant i \leqslant n$ denotes the ith shadow image and $P_i, 0 \leqslant i \leqslant m$ denotes the set of shadow images of the ith level. The secret image can be reconstructed by satisfying a sequence of threshold requirements, such as that it has at least t_0 secret shadow images from the highest level as well as at least $t_1 > t_0$ secret shadow images from the two highest levels and so forth.

Assume that the cover image O has $M \times N$ pixels, $O = \{o_i | i = 1, 2, \ldots, (M \times N)\}$, and secret image S has $M_S \times N_S$ pixels.

Step 1: The dealer selects a large prime modulus p.
Step 2: The dealer obtains all pixels of the secret image S, denoted as $S = \{s_j | j = 1, 2, \ldots, (M_S \times N_S)\}$, where $s_j \in [0, 255]$.

3.2. Secret image sharing procedure

The procedure consists of two phases: (1) the sharing phase, and (2) the embedding phase.

3.2.1. Sharing phase

Without loss of generality, assume that we want to embed $s_0, s_1, s_2, \ldots, s_{t-1}$ into the cover image to generate n shadow images using a hierarchical access structure. The dealer performs the following steps:

Step 1. Construct a $(t-1)$th-degree polynomial $F(x) = s_0 + s_1 x + \cdots + s_{t-1} x^{t-1} \bmod p$, where p is a large prime, $t = t_m$, and $s_0, s_1, s_2, \ldots, s_{t-1}$ denote the pixel values of the shared secret image.
Step 2. For the first level shadow images, utilize the $(t-1)$th-degree polynomial $F(x)$ to generate the shadow images. The shadow images of other levels are processed in the following manner. The shadow images of the ith level in the hierarchy can be generated by using the polynomial $F^{t_{i-1}}(x)$, where $F^{t_{i-1}}(x)$ is the (t_{i-1}) th derivative of $F(x)$.

For example, there are three levels in the shadow images, $P = P_0 \cup P_1 \cup P_2$. Assume that the threshold sequence requirements are $t_0 = 2$, $t_1 = 4$ and $t_2 = 7$; that is, the secret image can be reconstructed if and only if there are at least seven shadow images, of which at least four are from $P_0 \cup P_1$, and at least two are from P_0. In this example, we should construct a 6th-degree polynomial $F(x) = s_0 + s_1 x + \cdots + s_6 x^6 \bmod p$. First, the dealer utilizes $F(x)$ to generate the shadow images that belong to P_0. Since $t_0 = 2$, the second level shadow images are generated by using the polynomial $F''(x)$, and since $t_1 = 4$, the shadow images of the lowest level can be computed using the polynomial $F^{(4)}(x)$.

3.2.2. Embedding phase

In order to diminish the distortion of the shadow images, most existing secret image sharing schemes have utilized the modulus operator to embed the secret image data into the pixels of the cover image. However, in the proposed scheme, in keeping with Tassa's scheme, we calculate the shadow images in a finite field of size p, which is a large prime, so we need to develop a new method in order to embed the shadow data into the cover image.

Lin and Chan's scheme (Lin and Chan, 2010) formed a camouflaged pixel using

$$Q_i = \lfloor o_i/k \rfloor \times k, \\ q_i = Q_i + y_i, \tag{1}$$

where Q_i is the quantized value of o_i, and q_i represents the ith camouflaged pixel. Inspired by Lin and Chan's scheme, we also use a quantization operation to embed the secret data. However, in Lin and Chan's scheme, all operations are in a field modulo a small prime number σ, such as 5, 7, or 11, so y_i can be directly embedded into a pixel of the cover image without causing a large distortion. However, in our scheme, the modulus p must be far greater than the threshold t, so we obtain a large integer $y_i = F(i)$ by feeding an integer $i, i \in [1, n]$ into $F(x)$ and need to use r pixels of shadow images to represent shadow data y_i. In the traditional secret image sharing schemes, the dealer feeds a secret key or a unique ID_i into the polynomial $F(x)$ to obtain y_i; and in order to facilitate the embedding of y_i into the shadow image, the polynomial $F(x)$ can modulo a small prime. However, in the proposed scheme, the polynomial $F(x)$ needs to modulo a large prime, so we need more pixels to represent y_i. Obviously, the larger y_i is, the more pixels are needed to represent y_i.

Therefore, in order to minimize y_i, we feed a series of integers i, for $i = 1, 2, \ldots, n$ into $F(x)$ instead of feeding ID_i. In order to guarantee that r pixels are sufficient to represent y_i, we maximize the shared secret data s_i and assume that all $s_i = 255$, for $i = 1, 2, \ldots, n$.

We first talk about how to generate the highest level shadow images. Assume that the highest level P_0 includes l_0 shadow images $p_1, p_2, \ldots, p_{l_0}$, and the selected r camouflage pixels in the cover image O are $o_i, o_{i+1}, \ldots, o_{i+r-1}$. In the embedding phase, we perform the following steps:

Step 1. Assume that we want to generate the shadow image p_i, $i \in [1, l_0]$. The dealer first computes y_i by feeding i into $F(x)$.
Step 2. We utilize Lin and Chan's method (2010) to generate and camouflage the shadow images. Firstly, we convert the secret data y_i into the σ -ary notational system. In Lin and Chan's scheme (2010), Eq. (1) may lead to an overflow situation. Therefore, we must ensure that $\lfloor o_i/k \rfloor \times k + \sigma \leqslant 255$. Meanwhile, the parameters (k, σ) can also affect the quality of the shadow images and the embedding capacity. The greater the value σ is, the larger the embedding capacity is. However, the value σ may increase the gap between adjacent pixel values, especially for the smooth image. Therefore, the greater the value σ is, the less smooth the shadow image is. In regard to the different cover images, if the cover image is smooth, we need to select a small σ. On the contrary, if the cover image is rich, we can select a great σ aiming at improving the embedding capacity. In order to simplify the proposed method, in this paper, we let $k = 10$ and transform the y_i into base-5 representation. For instance, if $y_i = 1304$, we obtain $y_i = (2, 0, 2, 0, 4)_5$. This pair (10, 5) can effectively avoid the overflow problem since $\lfloor 255/10 \rfloor \times 10 + 5 \leqslant 255$. And, we need $r = \lceil \log_5 F(l_0) \rceil$ pixels of the shadow image to represent y_i. As to the ith level, r_i can be computed by $r_i = \lceil \log_5 F^{t_{i-1}}(l_i) \rceil$, where $F^{t_{i-1}}(l_i)$ denotes the (t_{i-1})th derivative of the function $F(x)$.
Step 3. Without loss of generality, assume that we use r pixels $p_{ij}, j = 1, 2, \ldots, r$ of the shadow image p_i to represent y_i as follows:

$$\begin{aligned} p_{i1} &= \lfloor o_i/10 \rfloor \times 10 + y_{i1}, \\ p_{i2} &= \lfloor o_{i+1}/10 \rfloor \times 10 + y_{i2}, \\ &\vdots \\ p_{ir} &= \lfloor o_{i+r-1} 10 \rfloor \times 10 + y_{ir}, \end{aligned} \tag{2}$$

where each $y_{ij}, j = 1, 2, \ldots, r$, denotes y_i 's base-5 representation.
Step 4. By repeating Steps 1–3, the dealer can camouflage all secret data y_i into the cover pixels, and by feeding i, for $i = 1, 2, \ldots, l_0$ into $F(x)$, the dealer can obtain the first level shadow images.

As to the shadow images at the second highest level, since the threshold values are $\{t0, t1, \ldots, tm\}$, the dealer uses the polynomial $F^{t_0}(x)$ to generate the shadow data yi, and so forth, so the shadow images of the ith level in the hierarchy are computed using the polynomial $F^{t_{i-1}}(x)$.

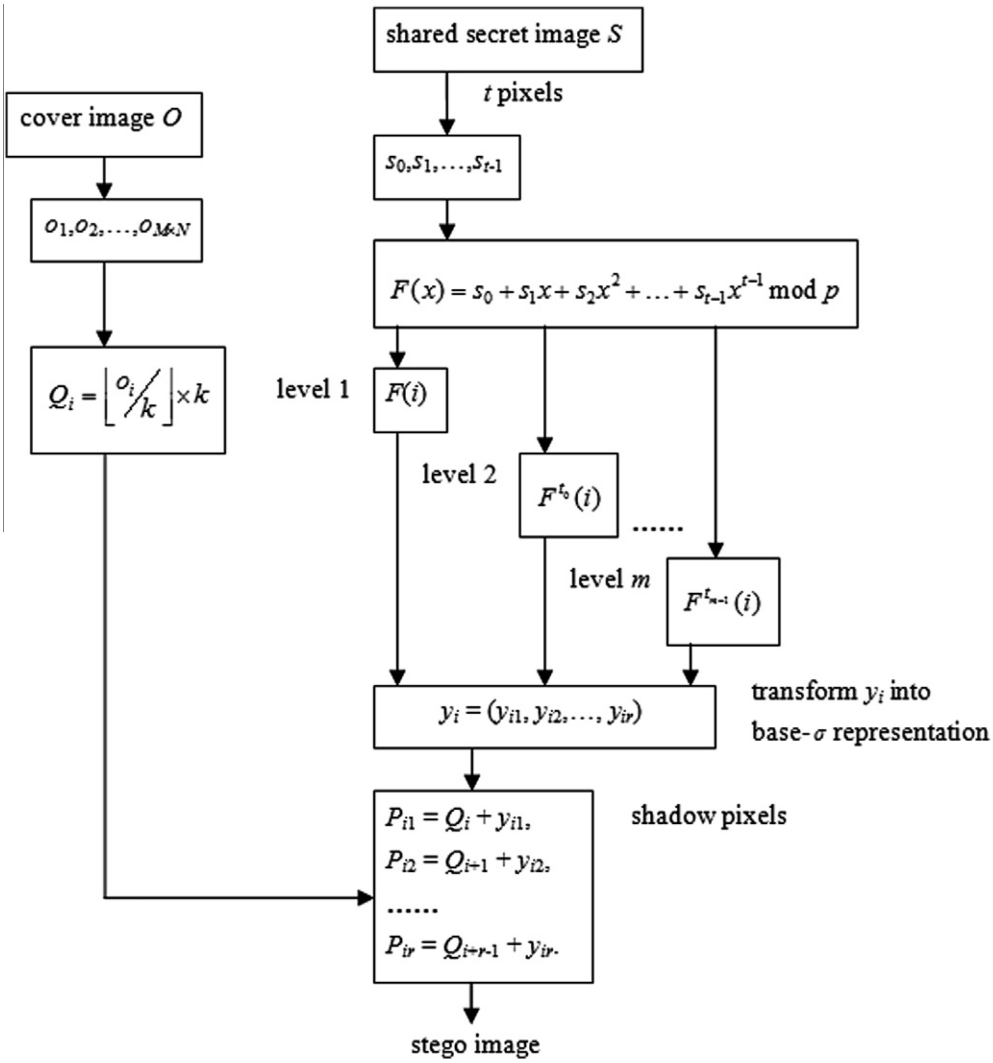

shared secret image S
t pixels
$s_0, s_1, \dots, s_{t-1}$
$F(x) = s_0 + s_1x + s_2x^2 + \dots + s_{t-1}x^{t-1} \bmod p$
cover image O
$o_1, o_2, \dots, o_{M\times N}$
$Q_i = \lfloor o_i/k \rfloor \times k$
level 1
$F(i)$
level 2
$F^{t_0}(i)$
......
level m
$F^{t_{m-1}}(i)$
$y_i = (y_{i1}, y_{i2}, \dots, y_{ir})$
transform y_i into
base-σ representation
$P_{i1} = Q_i + y_{i1}$,
$P_{i2} = Q_{i+1} + y_{i2}$,
......
$P_{ir} = Q_{i+r-1} + y_{ir}$.
shadow pixels
stego image

Fig. 1. The diagram of the secret image sharing scheme.

The generation process for the other levels of shadow images is the same as that of the highest level except that different polynomials are used. Repeat the above steps until all shadow images of various levels are generated. Fig. 1 displays the flowchart of the secret image sharing scheme.

3.3. Secret image retrieving procedure

In the traditional secret image sharing schemes, given any t shadow images, the shared secret image can be reconstructed. In our scheme, according to Tassa's threshold access structure, given shadow images must satisfy a sequence of threshold requirements. In order to extract the secret digits, the polynomial $F(x)$ must be reconstructed by retrieving the shadow data y_i from the shadow images p_i's. The same method is used for different levels of shadow images. The details are as follows:

Step 1. Compute y_i by

$$y_i = y_{i1}||y_{i2}||\dots||y_{ir}, \tag{3}$$

where $y_{ij} = p_{ij} \bmod 5$, for $j = 1, 2, \dots, r$, and p_{ij} denotes the jth pixel value of the ith shadow image, for $i = 1, 2, \dots, t_m$.

Step 2. Collect enough t pairs (i, yi) 's to satisfy the hierarchical threshold access structure and employ the Birkhoff interpolation to reconstruct the $(t-1)$ degree polynomial $F(x)$.

Step 3. Extract the corresponding t coefficients $s_0, s_1, s_2, \dots, s_{t-1}$.

Step 4. Repeat Steps 1–3 until all secret data is extracted.

Step 5. Reconstruct the secret image.

4. Experimental results and analysis

This section describes some experimental results in order to demonstrate the characteristics of the proposed scheme.

We perform experiments for $n = 10$. A secret image can be generated in ten shadow images, and the ten shadow images are partitioned into three levels. Assume that the first (highest) level has three shadow images, the second level has three shadow images, and the third (lowest) level has four shadow images. Assume a sequence of threshold requirements $t = (t_0, t_1, t_2) = (2, 4, 7)$; that is, the secret image can be reconstructed if and only if a subset of shadow images has at least seven shadow images, of which at least four are from the first two levels and at least two are from the first level.

4.1. Simulation results

The peak signal-to-noise ratio (*PSNR*), defined in Eq. (4), can be used to measure the distortion of the shadow images after the secret data have been embedded into the cover image.

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right)dB. \quad (4)$$

The mean square error (MSE) between the cover image with $M \times N$ pixels and the shadow image is defined as

$$MSE = \frac{1}{M \times N}\sum_{j=1}^{M\times N}(p_j - p'_j)^2, \quad (5)$$

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

We use fifteen grayscale images with size 512 × 512 pixels as the test images, as shown in Fig. 2, and the secret sharing image *Airplane* is set to 256 × 256 pixels, as shown in Fig. 3.

Table 1 displays the *PSNR* value of the shadow images achieved using the proposed scheme. Although the pixel values of the shadow images of the proposed scheme are slightly lower than those of the existing secret image sharing methods, it is clear that, regardless of what we use as the cover image, the *PSNR* values of the shadow images always maintain a steady level and are within [36.00,41.00]. Furthermore, we obtained a new access structure that may have many applications, and the distortion between the shadow images and the cover image is imperceptible by visual perception.

In order to demonstrate the visual perception of the shadow images, we use *Peppers* as the cover image with size 512 × 512 pixels and *Airplane* as the secret image with size 256 × 256 pixels. If the secret images involved meet the hierarchical threshold access structure, our method can reconstruct them without distortion. Fig. 4(a) and (b) shows the cover image and the extracted secret image, respectively.

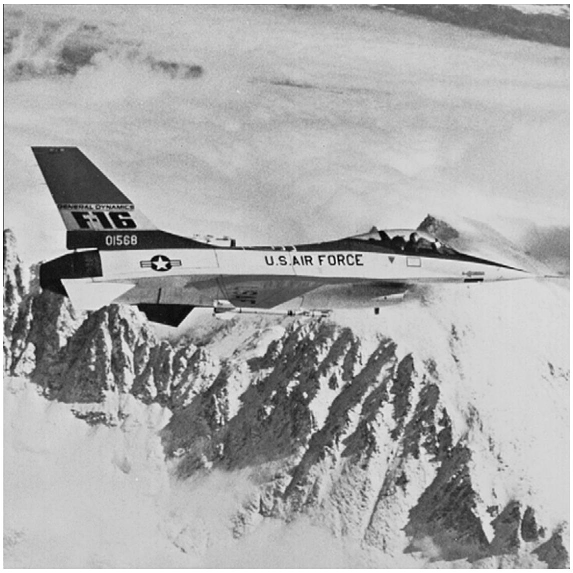
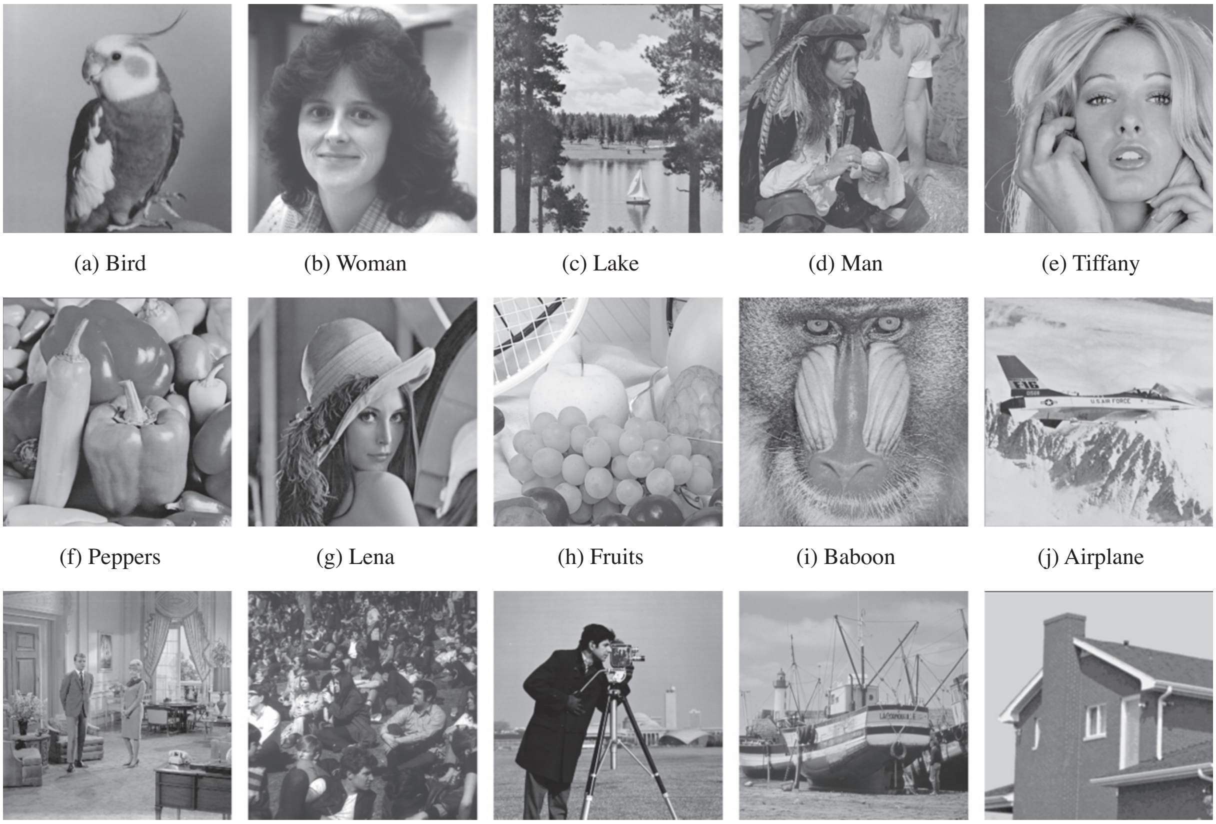


Fig. 3. The secret image.

Fig. 5(a)–(j) display ten shadow images of *Peppers* that are partitioned into three levels. Since the distortion between the cover image and the shadow images is slight, we can successfully conceal the embedded the secret image data's existence from intruders.



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

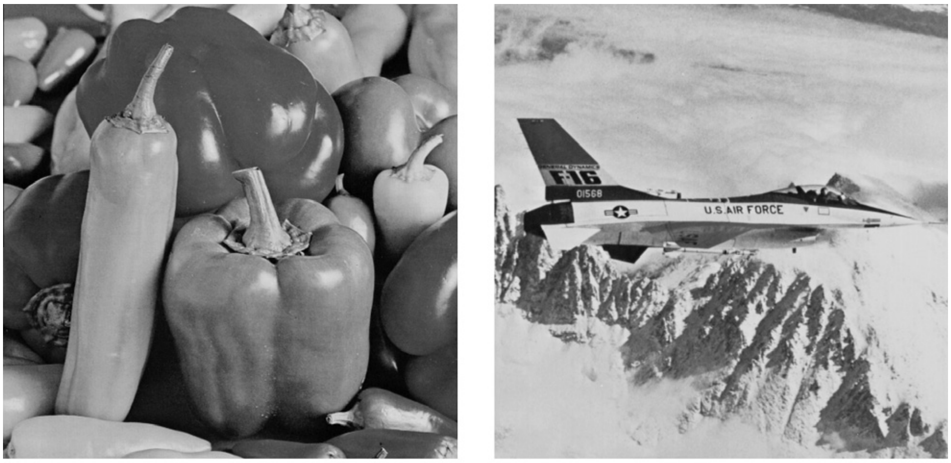
(f) Peppers (g) Lena (h) Fruits (i) Baboon (j) Airplane

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

Fig. 2. The test images.

Table 1
The *PSNR* value (dB) of the shadow images for test images, $n = 10$, $t_0 = 2$, $t_1 = 4$, $t_2 = 7$.

Test images	The first level			The second level			The third level			*PSNR*(dB)
	1	2	3	4	5	6	7	8	9	10
Bird	36.87	37.31	37.58	37.94	38.02	38.17	37.99	38.06	38.10	38.14
Woman	38.29	38.72	38.99	39.33	39.42	39.57	39.40	39.45	39.51	39.54
Lake	37.94	38.39	38.67	39.01	39.10	39.26	39.08	39.14	39.19	39.22
Man	37.73	38.17	38.42	38.76	38.86	39.01	38.83	38.87	38.94	38.97
Tiffany	36.37	36.81	37.08	37.43	37.52	37.67	37.49	37.55	37.59	37.63
Peppers	37.32	37.76	38.03	38.36	38.45	38.60	38.42	38.49	38.53	38.56
Lena	37.78	38.22	38.50	38.83	38.94	39.08	38.91	38.96	39.02	39.05
Fruits	38.42	38.86	39.14	39.49	39.58	39.74	39.55	39.59	39.65	39.69
Baboon	37.25	37.68	37.96	38.31	38.39	38.55	38.38	38.42	38.47	38.51
Airplane	37.48	37.92	38.18	38.53	38.61	38.77	38.59	38.64	38.69	38.72
Couple	38.38	38.84	39.10	39.45	39.55	39.69	39.51	39.56	39.63	39.66
Crowd	38.49	38.92	39.19	39.55	39.64	39.79	39.61	39.66	39.22	39.75
Cameraman	38.32	38.77	39.03	39.38	39.47	39.62	39.45	39.50	39.54	39.59
Boat	37.67	38.11	38.37	38.70	38.78	38.93	38.76	38.81	38.87	38.90
House	39.02	39.57	39.92	40.37	40.48	40.68	40.45	40.52	40.58	40.63
Average	37.82	38.27	38.54	38.90	38.99	39.14	38.96	39.01	39.04	39.10



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

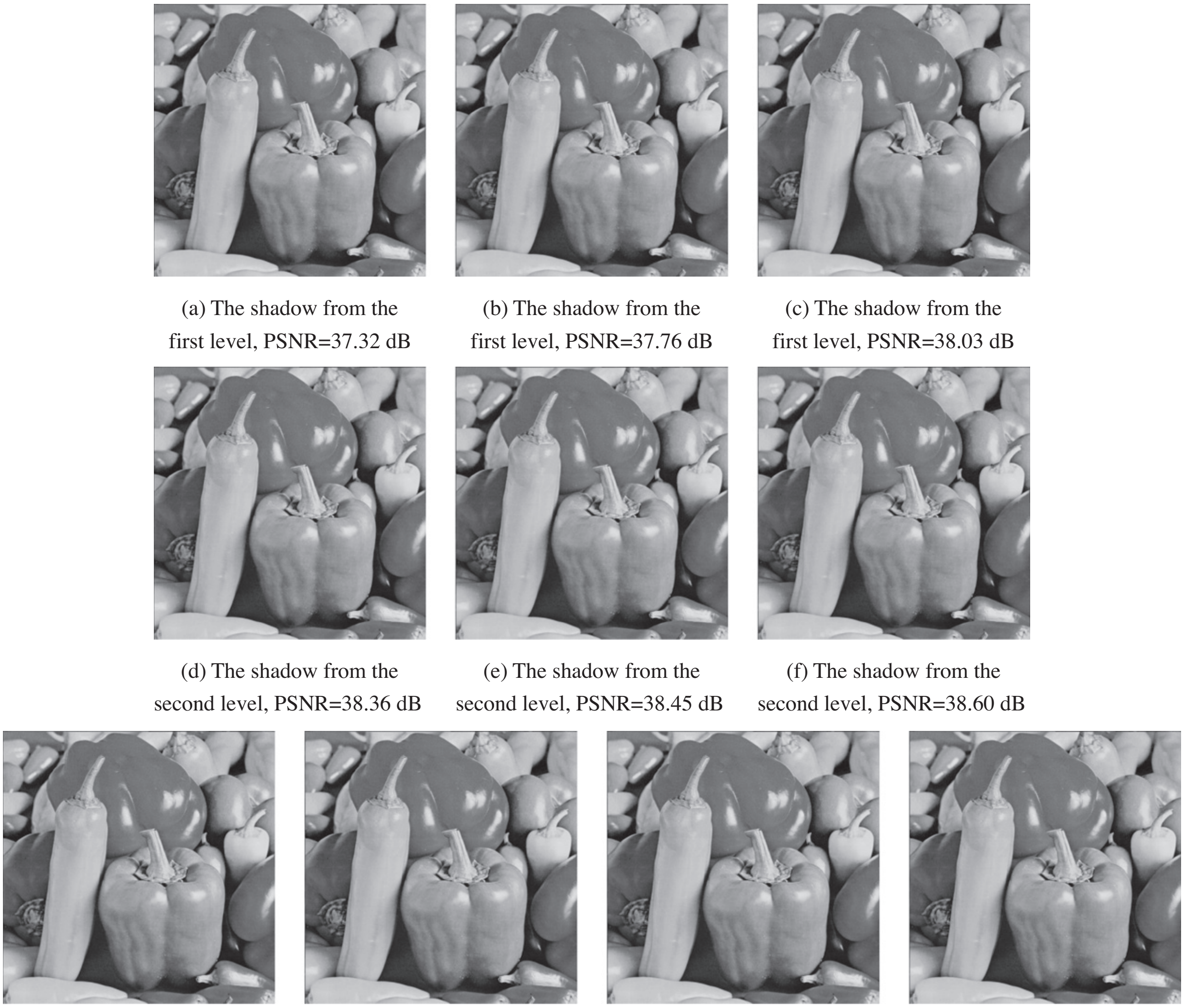
Fig. 4. The cover image and the extracted secret image.

5. Discussions

Progressive visual secret sharing mechanism (Fang, 2008; Huang et al., 2010) has the similar characteristics with our proposed scheme. Progressive visual secret sharing can be utilized to reconstruct the shared secret image gradually by superimposing more and more shadow images. By increasing the number of the shadow images being stacked, the details of the shared secret image can be revealed progressively. In our scheme, if we use the constant term and all coefficients of the polynomial $F(x)$ to hide the secret data, our proposed scheme also can achieve a progressive effect. Meanwhile, our scheme has a hierarchical threshold feature. That is, when the shadow images of a level involved meet a corresponding level threshold, the recovery of the shared secret image will be clearer. Further more, if we just use t_0 coefficients of the $F(x)$ to hide the secret data, the proposed scheme can achieve an ideal hierarchical threshold access structure. If the shadow images involved can not satisfy the hierarchical threshold requirement, they can not obtain anything about the secret image. Progressive visual secret sharing is an important mechanism for application in transmission while hierarchical threshold secret image sharing provides a hierarchical threshold access structure for secret image sharing. To the best of our knowledge, our proposed scheme has a unique hierarchical threshold characteristic as compared with the existing secret image sharing schemes.

Table 2 compares the functionality of the proposed scheme with that of related schemes. As presented in Table 2, the new method satisfied the camouflage purpose and provided the satisfactory quality of shadow images. Meanwhile, the secret image can be reconstructed lossless. And the proposed secret image sharing scheme can provide a hierarchical threshold access structure. The new mechanism allows the participants to be partitioned into several levels, and the access structure is then determined by a sequence of threshold requirements. In comparison with the traditional secret image sharing schemes (Yang et al., 2007; Chang et al., 2008; Lin et al., 2009; Lin and Chan, 2010), the proposed hierarchical threshold secret image sharing scheme can not recover the cover image. And, quality of shadow images needs to be improved.

In the proposed experiment, the ten shadow images are partitioned into three levels, and the corresponding thresholds are $t_0 = 2, t_1 = 4, t_2 = 7$. We can compute the secret image data y_i embedded into shadow images by using a $(t_2 - 1)$th-degree polynomial $F(x)$. Since y_i is a large integer, we need to use r pixels of the shadow image to represent y_i, so parameter r is important in order to maximize the secret capacity. In our experiment, three different r values correspond with the three levels of shadow images.



(a) The shadow from the first level, PSNR=37.32 dB

(b) The shadow from the first level, PSNR=37.76 dB

(c) The shadow from the first level, PSNR=38.03 dB

(d) The shadow from the second level, PSNR=38.36 dB

(e) The shadow from the second level, PSNR=38.45 dB

(f) The shadow from the second level, PSNR=38.60 dB

(g) The shadow from the third level, PSNR=38.42 dB

(h) The shadow from the third level, PSNR=38.49 dB

(i) The shadow from the third level, PSNR=38.53 dB

(j) The shadow from the third level, PSNR=38.56 dB

Fig. 5. The results of Peppers, $n = 10, t_0 = 2, t_1 = 4, t_2 = 7$.

Table 2
Comparisons of the related secret image sharing schemes.

Functionality	Yang et al. (2007)	Chang et al. (2008)	Lin et al. (2009)	Lin and Chan (2010)	Ours
Hierarchical threshold	No	No	No	No	Yes
Meaningful shadow image	Yes	Yes	Yes	Yes	Yes
Quality of shadow images	40 dB	40 dB	43 dB	42 dB	38 dB
Lossless secret image	Yes	Yes	Yes	Yes	Yes
Lossless cover image	No	No	Yes	Yes	No
Maximum capacity	$\frac{M\times N}{4}$	$\frac{M\times N}{4}$	$\frac{(t-3)\times M\times N}{3}$	$(t-1)\times M\times N/\lceil\log_{\sigma}255\rceil$	$\lfloor M\times N/\max\{r_i\}\rfloor\times t_m$

$$\begin{aligned} r_0 &= \lceil \log_5 F(l_0)\rceil,\\ r_1 &= \lceil \log_5 F''(l_1)\rceil, \quad .\\ r_2 &= \lceil \log_5 F^{(4)}(l_2)\rceil. \end{aligned}$$

In this example, the embedding capacity (the number of pixels) can be computed as

$$Capacity = \left\lfloor \frac{512\times 512}{\max\{r_0, r_1, r_2\}} \right\rfloor \times t_2.$$

Table 3
The maximum capacity under different n and t_i.

n	Level			Threshold value			Capacity (pixels)
	1	2	3	t_0	t_1	t_2	
7	2	2	3	1	2	4	174762
8	2	2	4	1	2	4	174762
10	3	3	4	2	4	7	166818
10	2	4	4	1	3	5	163940
12	2	4	6	1	3	6	157286
14	2	6	6	1	4	8	161318

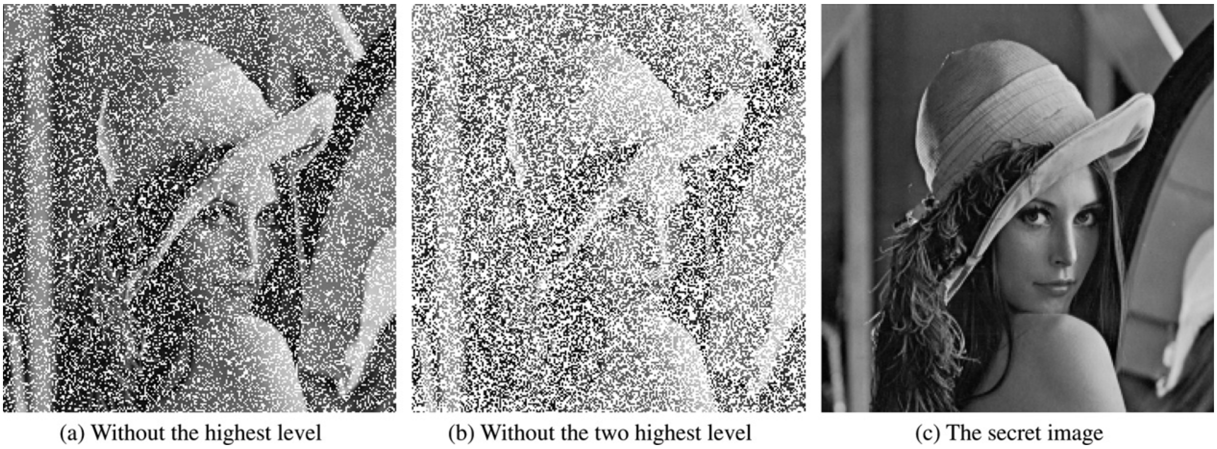

(a) Without the highest level
(b) Without the two highest level
(c) The secret image

Fig. 6. The extracted secret image without satisfying the hierarchical threshold access structure.

Assume also that the shadow images are partitioned into m levels, and the threshold of the mth level is t_m. We can compute the embedding capacity of our scheme using the following formula:

$$Capacity = \left\lfloor \frac{512 \times 512}{\max\{r_i\}_{1 \leqslant i \leqslant m}} \right\rfloor \times t_m, \tag{6}$$

where $r_i = \lceil \log_5 F^{t_{i-1}}(l_i) \rceil$.

In the secret image sharing scheme, the embedding capacity is an important measurement. In the traditional secret image sharing schemes, the embedding capacity is proportional to the threshold t. However, in our scheme, y_i may be increased with the rise of the threshold, so y_i should be represented using more pixels in the shadow image. Table 3 describes the maximum size of the secret image embedded into the 512 × 512 cover image under different n and different hierarchical threshold values t_i.

In the proposed scheme, the shadow images that must cooperate to reconstruct the secret image must satisfy the hierarchical threshold access structure; if the shadow images don't meet some hierarchical threshold value, the secret image cannot be fully reconstructed. Fig. 6(a) and (b) display the extracted secret images without satisfying the two threshold requirements, respectively.

Fig. 6(a) and (b) show that the secret image cannot be fully reconstructed. However, even this may not be secure enough for some secret images with highly sensitive information since the visual perception of Fig. 6(a) and (b) may leak out some information about the secret image. Our scheme uses the constant term and all coefficients of the polynomial $F(x)$ to hide the secret data, aiming to increase the embedding capacity. Therefore, some shadow images that satisfy only the third level threshold requirement or that satisfy only the second and third level requirements can also recover the corresponding coefficients of the $F(x)$. If we relax the restrictions for the embedding capacity, we can use just t_0 coefficients of the polynomial that includes the constant term to hide the secret data. In that case, if the shadow images do not meet the hierarchical threshold requirements, they cannot obtain anything about the secret image. (Of course, the changes that decrease the embedding capacity will not affect the visual perception of the shadow images.) The embedding capacity can be computed as follows:

$$Capacity = \left\lfloor \frac{512 \times 512}{\max\{r_i\}_{1 \leqslant i \leqslant m}} \right\rfloor \times t_0, \tag{7}$$

where $r_i = \lceil \log_5 F^{t_{i-1}}(l_i) \rceil$.

6. Conclusions and future work

In this paper, based on Tassa's hierarchical threshold secret sharing scheme, we propose a novel secret image sharing scheme with a hierarchical threshold access structure. In our scheme, the dealer can generate shadow images by embedding secret data into the cover images. The shadow images are partitioned into several levels, and the dealer sets a sequence of threshold values such that, if and only if the shadow images involved satisfy the threshold requirements, the secret image can be retrieved without distortion. The experimental results show that the shadow images generated by the proposed scheme have the hierarchical threshold characteristic, and the visual quality of the shadow images and the embedding capacity are both satisfactory.

However, there are also a number of technical problems that merit attention but that were not fully addressed in this paper. Foremost among these is the distortion-free reconstruction of the cover image. Another problem has to do with how to improve the visual quality of the shadow images and the embedding capacity. We believe that some new and interesting approaches will be found by investigating and studying this problem.

References

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

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

Chang, C.C., Lin, C.C., Ngan Le, T.H., Le, H.B., 2009. Sharing a verifiable secret image using two shadows. Pattern Recogn. 42 (11), 3097–3114.

Eslami, Z., Razzaghi, S.H., Ahmadabadi, J.Z., 2010. Secret image sharing based on cellular automata and steganography. Pattern Recogn. 43 (1), 397–404.

Fang, W.P., 2008. Friendly progressive visual secret sharing. Pattern Recogn. 41 (4), 1410–1414.

Huang, C.P., Hsieh, C.H., Huang, P.S., 2010. Progressive sharing for a secret image. J. Syst. Software 83 (3), 517–527.

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

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

Lin, Y.Y., Wang, R.Z., 2010. Scalable secret image sharing with smaller shadow image. IEEE Signal Process. Lett. 17 (3), 316–319.

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.

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.

Tassa, T., 2007. Hierarchical threshold secret sharing. J. Cryptol. 20 (2), 237–264.

Thien, C.C., Lin, J.C., 2003. An image-sharing method with user-friendly shadow images. IEEE Trans. Circ. Syst. Video Technol. 13 (12), 1161–1169.

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

Wu, Y.S., Thien, C.C., Lin, J.C., 2004. Sharing and hiding secret images with size constraint. Pattern Recogn. 37 (7), 1377–1385.

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.

Zhao, R., Zhao, J.J., Dai, F., Zhao, F.Q., 2009. A new image secret sharing scheme to identify cheaters. Comput. Stand Interfaces 31 (1), 252–257.