SIViP (2015) 9:499–510
DOI 10.1007/s11760-013-0465-y

ORIGINAL PAPER

New approaches for efficient information hiding-based secret image sharing schemes

Xuehu Yan · Shen Wang · Ahmed A. Abd El-Latif · Xiamu Niu

Received: 7 January 2013 / Revised: 6 March 2013 / Accepted: 20 March 2013 / Published online: 12 April 2013

Abstract In recent years, various secret sharing schemes for digital images have been developed in order to promote communication security. Previous methods in the literature have made efforts to achieve the merits properties for a good secret image sharing scheme such as implement (k, n) threshold, simple recovery, no pixel expansion, the generated shadow images are meaningful, the order of shadow images is alternative and lossless recovery of the secret image. To the best of our knowledge, no previous secret sharing scheme achieves all the above properties with good quality of meaningful shadow images. In this paper, we propose two different secret image sharing schemes, (n_1, n_1) and (k, n_2) thresholds, based on information hiding theory to improve the quality of meaningful shadow images with lower computation and good expansibility. In addition, the proposed schemes have the advantages of lossless and alternative order recovery and no pixel expansion. Comparisons with previous approaches show the performance of the proposed schemes.

Keywords Secret image sharing · (k, n) and (n, n) thresholds · Least significant bits matching · Maximum likelihood estimation

X. Yan · S. Wang (✉) · A. A. Abd El-Latif · X.Niu
School of Computer Science and Technology, Harbin Institute of Technology, Harbin 150080, China
e-mail: shen.wang@hit.edu.cn

X. Yan
e-mail: ictyanxuehu@163.com

X. Niu
e-mail: xiamu.niu@ict.hit.edu.cn

A. A. Abd El-Latif
Mathematics Department, Faculty of Science, Menoufia University, Shebin El-Koom 32511, Egypt
e-mail: ahmed_rahiem@yahoo.com

1 Introduction

Along with the rapid development of Internet and universal application of multimedia technology, multimedia data including audio, image, and video have been transmitted over insecure channels. In particular, the use of images is an ascending need because it is the main data information provided by most of the advanced sensors of today like infrared cameras, optical cameras, millimeter wave cameras, radar images, X-ray images, etc. In order to maintain security or privacy, digital images need to be protected before transmission or distribution. Secret sharing scheme (SSS) and information hiding are two important methods to protect secret. Herein, we review part of them that is relevant to the present work.

In recent years, secret image sharing techniques have attracted considerable attention to scientists and engineers as another branch alongside conventional cryptography to protect sensitive images from rapacious behaviors. It distributes a secret image among some participants through splitting the secret image into noise-like pieces (also called shares, stego-images or shadow images, are the images that already carried secret after sharing) and recovering the secret by collecting sufficient authorized participants (shadow images).

Until now, various SSSs [1–4] for digital images have been developed in order to promote communication security. The literature on secret image sharing is quit rich. Shamir's polynomial-based schemes and visual secret sharing (VSS), that is also called visual cryptography scheme (VCS), are the primary branches in this field. Some approaches [5–8] realize the secret image sharing based on Shamir's polynomial and Lagrange interpolation, and they have the properties of (k, n) threshold, meaningful shadow images, lossless recovery, and no pixel expansion.

Shamir [1] introduced an SSS called a (k, n) threshold scheme. The (k, n) $(k \leq n)$ threshold secret sharing mechanism, also called threshold-based VCS, is to partition the secret information into n shares and share them among n participants and needs at least k shares to recover the secret information. Notably, less than k participants cannot reveal any information of the secret image by inspecting their shares. The main merits of the VCS proposed by Naor and Shamir are simple recovery, which is the decryption of secret image is completely based on human visual system (HVS) without any additional computation, and alternative order of the shadow images. However, it suffers from meaningless shadow images, lossy recovery, and pixel expansion [2,3]. Based on the pioneer work of Naor and Shamir, many schemes [9–15] have been developed to overcome the above disadvantages. The previous schemes based on traditional visual cryptography (VC) have the properties of (k, n) threshold, simple computation complexity, and alternative order of shadow images.

However, Shamir's polynomial-based approaches suffer from complex recovery and known order of the shadow images. In addition, most of the previous schemes based on traditional VC suffer from pixel expansion, lossy recovered secret image, and low quality of shadow images.

Information hiding technique is another important method to protect secret information. It uses redundant data and random component of carriers (called cover images if images are selected, cover images are the selected original images that are used to cover secret but not carry secret), such as image [16,17] and video [18], to embed secret messages into the carrier through the way that could not be perceptible. It has properties of meaningful shadow images, no pixel expansion, and lossless recovery. However, it suffers from no (k, n) threshold.

Recently, in [3], Wu *et al*. have proposed (n, n) threshold scheme via combining Arnold permutation, error diffusion, and Boolean operation. And, in [4], Li *et al*. have proposed a visual sharing (k, n) scheme via combining Arnold permutation, error diffusion, and maximum likelihood estimation (MLE). In the two schemes, error diffusion technology is applied to generate meaningful shadow images, and Arnold Permutation technology to improve the security and make the shadow images as homogeneously as possible. Both of them satisfy simple recovery computation, alternative order of shadow images in recovery, meaningful shadow images, lossless recovery of binary secret image, avoiding the pixel expansion, and (n, n) or (k, n) threshold. However, the two schemes suffer from the low quality of shadow images and complex generating computation of shadow images for applying error diffusion and permutation technologies.

In this paper, we propose two different secret image sharing schemes, (n_1, n_1) and (k, n_2) thresholds, based on least significant bits matching (LSBM). LSBM is applied in the proposed two SSSs to improve the visual quality of shadow images and decrease the computational complexity by combining Boolean operations and MLE instead of error diffusion technology in [3,4], respectively. The proposed two schemes have several advantages, such as simple generation and recovery computation, alternative order of shadow images in recovery, meaningful shadow images, lossless recovery of binary secret image, and avoiding the pixel expansion. In another aspect, they have better quality and lower computation. Experimental results show the feasibility and effectiveness of the proposed schemes.

The outline of this paper is as follows. In Sect. 2, the related preliminaries are given. The proposed schemes are presented in Sect. 3. Section 4 is devoted to experimental results and analysis. Finally, Sect. 5 concludes this paper.

2 Preliminaries

This section introduces the related methods applied in the proposed schemes.

2.1 LSBM

LSBM is an effective steganographic method [19–22]. LSBM checks whether the secret bit matches the least significant bit (LSB) value of the cover image pixels. If not, then there is a random increment/decrement, as in Eq. (1), of the value of the cover image pixel (C_p), otherwise the pixel value remains unmodified.

$$SC_p = \begin{cases} C_p + 1 & \text{if random} > 0 \text{ or } C_p = 0 \\ C_p - 1 & \text{if random} \leq 0 \text{ or } C_p = 255 \end{cases} \quad (1)$$

where $random$ is a random number ranging from -1 to 1. SC_pdenotes the modified pixel of the shadow image.

2.2 MLE

MLE is one kind of estimation the parameters of a statistical model. MLE seeks the parameter values that are most likely to have produced the observed distribution. It begins with the mathematical expression known as a likelihood function of the sample data. Clearly, the likelihood of a set of data is the probability of obtaining that particular set of data given the chosen probability model [23].

Receive bits	MLE	Recover secret bit
00011	→	0
00111	→	1
0011	→	error

Fig. 1 Example of MLE decoding

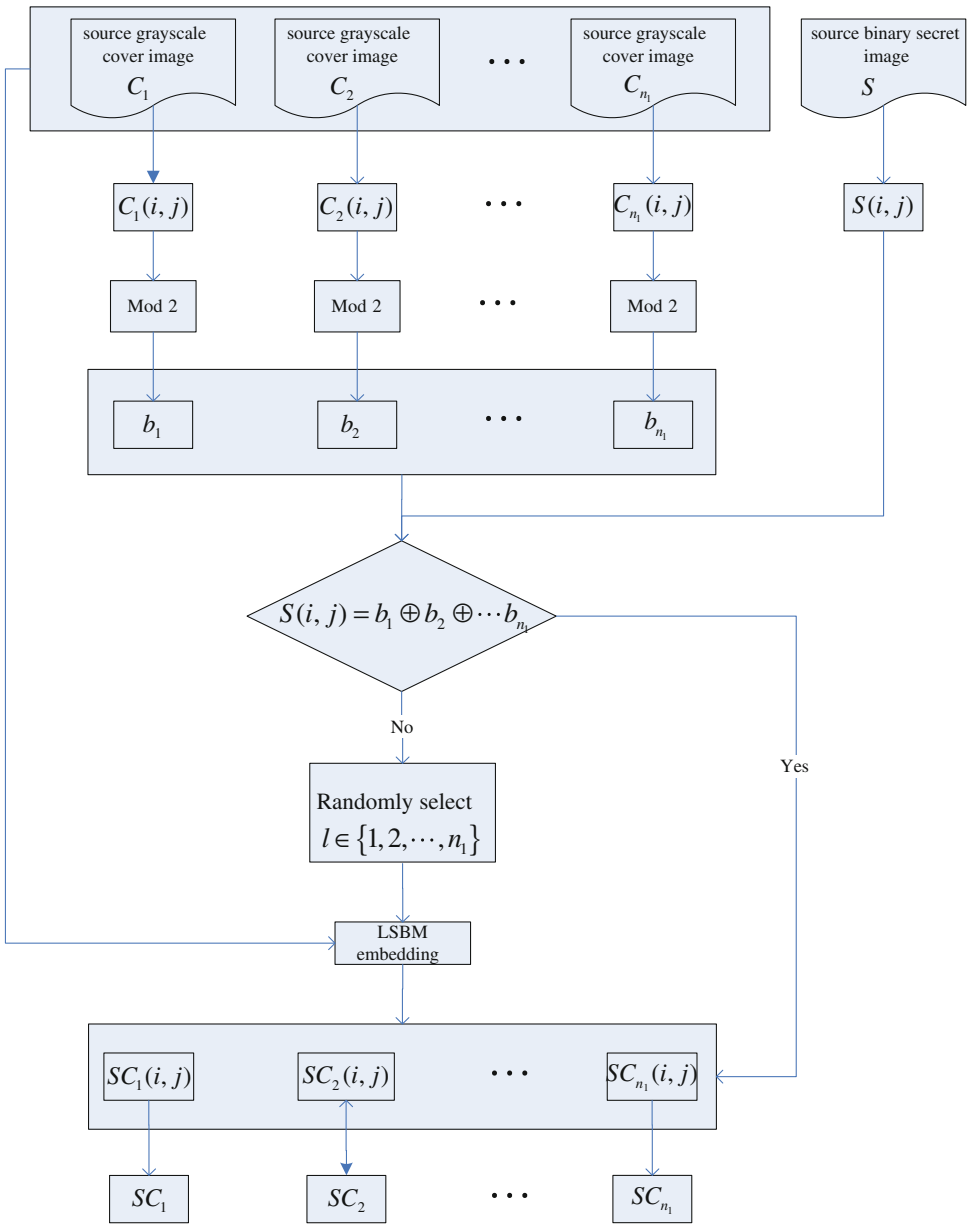


Fig. 2 Shadow images generation architecture of proposed (n_1, n_1) scheme

This expression contains the unknown parameters. Those values of the parameter that maximize the sample likelihood are known as the MLE. Figure 1 is an example for the MLE decoding. By MLE, we decode 00011→ 0. But if only 4 bits are received, such as 0011, it could not decode by MLE.

3 The proposed schemes

In this section, a $(n_1, n_1)\,(n_1 \geq 3, n_1 \in Z^+)$ SSS with enhanced quality is first introduced. In this approach, the binary secret image is shared among n_1 grayscale cover images. Then, a $(k, n_2)\,(3 \leq k \leq n_2,\ n_2 \in Z^+, k \in 2Z^+ + 1)$ scheme is presented applying MLE, and the secret image is recovered from k shadow images. The proposed (n_1, n_1) scheme based on Boolean operation has better shadow images quality and security, but not a general (k, n_2) threshold scheme. While the proposed (k, n_2) scheme based on MLE has general (k, n_2) threshold scheme, good quality of shadow images, and acceptable security.

The binary secret image is denoted as S with pixel value $S(i, j)$. Here, S is the sharing secret image. The source grayscale cover images are denoted as $C_p, 1 \leq p \leq n\,(n_1\ or\ n_2)\,, p \in Z^+$. The shadow images are denoted as SC_p. Assume t_k is the least equal bits number in the same location for k shadow images, that could be decoded

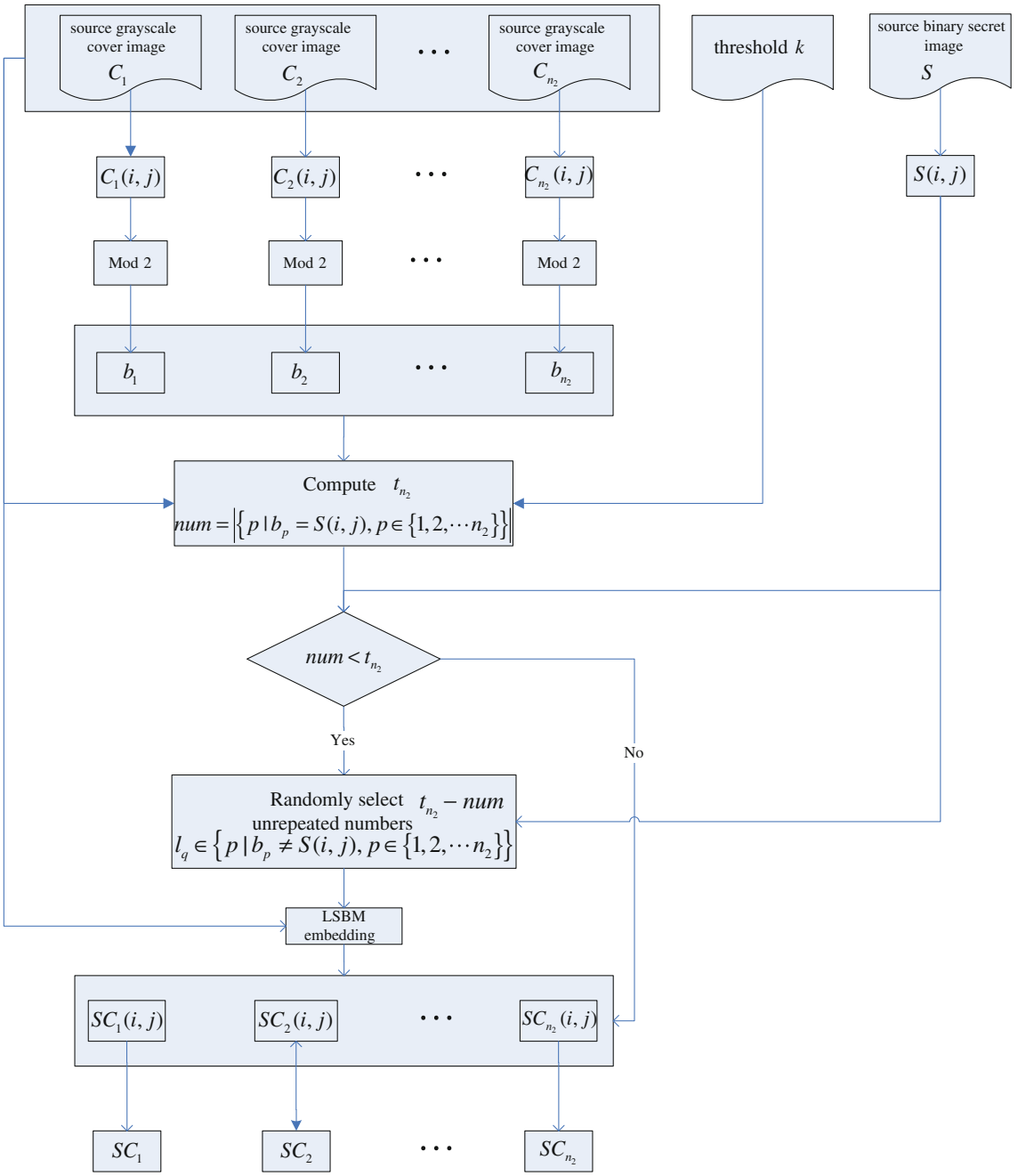


Fig. 3 Shadow images generation architecture of proposed (k, n_2) scheme

correctly in recovering phase based on MLE, t_{n_2} is for n_2 shadow images in sharing phase.

3.1 (n_1, n_1) scheme

In this section, we propose (n_1, n_1) threshold SSS. (n_1, n_1) threshold means that the secret image is shared among n_1 cover images and collecting n_1 shadow images to recover the secret image. The generation architecture is shown in Fig. 2, and the algorithms of generation and recovery of the (n_1, n_1) scheme are given in Algorithms 1 and 2 as below.

Algorithm 1. The proposed (n_1, n_1) threshold scheme.

Input: A $M \times N$ binary secret image S, n_1 $M \times N$ source grayscale cover images $C_1, C_2, \cdots C_{n_1}$

Output: n_1 shadow images $SC_1, SC_2, \cdots SC_{n_1}$.

Step 1: For each position $(i,j) \in \{(i,j) \mid 1 \le i \le M, 1 \le j \le N\}$, repeat Steps 2-5.

Step 2: Compute LSBs $b_p = C_p \bmod 2$,$1 \le p \le n_1$.

Step 3: Compute $X = b_1 \oplus b_2 \oplus \cdots b_{n_1}$. *If* $X \neq S(i,j)$ go to step 4; else go to step 5.
where $\oplus$ denotes the Boolean XOR operation.

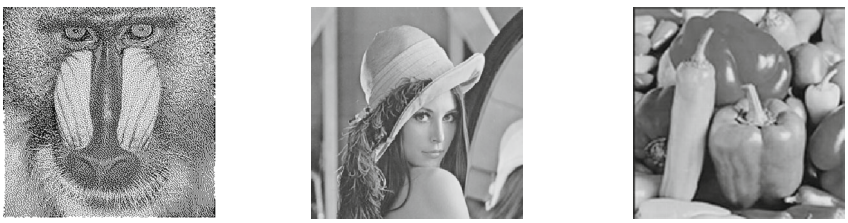
Step 4: Randomly select $l \in \{1,2,\cdots,n_1\}, SC_p(i,j) = C_p(i,j), p \in \{1,2,\cdots,n_1\}, p \neq l$.
If $C_l(i,j) = 0$ $SC_l(i,j) = 1$;
Else if $C_l(i,j) = 255$ $SC_l(i,j) = 254$;
Else $SC_l(i,j) = C_l(i,j) + 1$ *or* $C_l(i,j) - 1$ randomly.

Step 5: Compute $SC_p(i,j) = C_p(i,j), p \in \{1,2,\cdots,n_1\}$.

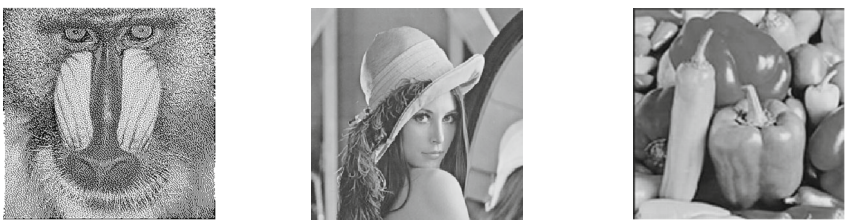
Step 6: Output the n_1 shadow images $SC_1, SC_2, \cdots SC_{n_1}$.

Table 1 Insights gleaned from the proposed schemes

Remark	Scheme	Explanations
The computation is simple	Proposed (n_1, n_1) and (k, n_2) schemes	The generation phase and recovery phase include operations of mod 2, Boolean, or addition and comparison
In the recovery phase, the order of the shadow images is alternative	Proposed (n_1, n_1) and (k, n_2) schemes	The shadow images are equal to each other
The proposed scheme has the advantage of (n_1, n_1) threshold	Proposed (n_1, n_1) scheme	The secret image could be recovered by all n_1 shadow images
The proposed scheme has the advantage of (k, n_2) threshold	Proposed (k, n_2) scheme	The secret image could be recovered by at least k shadow images



(a) Binary secret image **(b)** Original grayscale cover image 1 **(c)** Original grayscale cover image 2



(d) Recovered binary secret image **(e)** Shadow image 1 **(f)** Shadow image 2

Fig. 4 Images illustration of proposed (2, 2) scheme

Algorithm 2. Secret image recovery of the proposed (n_1, n_1) threshold scheme.
Input: n_1 shadow images $SC_1, SC_2, \cdots SC_{n_1}$.
Output: A $M \times N$ binary secret image S
Step 1: For each position $(i, j) \in \{(i, j) \mid 1 \le i \le M, 1 \le j \le N\}$, repeat Steps 2-3.
Step 2: Compute LSBs $b_p = SC_p(i, j) \bmod 2$, $1 \le p \le n_1$.
Step 3: Compute $S(i, j) = b_1 \oplus b_2 \oplus \cdots b_{n_1}$.
where $\oplus$ denotes the Boolean XOR operation.
Step 4: Output the binary secret image S.

3.2 (k, n_2) scheme

(k, n_2) threshold means that the secret image is shared among n_2 cover images and collecting at least k shadow images to recover the secret image. The MLE theory analysis of the proposed LSBM (k, n_2) scheme is described as follows.

First, since from Fig. 1 k should be odd, t_k should be greater than $\frac{k}{2}$ for decoding correctly; hence, Eq. (2) should be satisfied to perform MLE, and k LSBs of shadow images could be decoded correctly if Eq. (3) satisfies. In the extreme case (in the recovered phase with k shadow images, another $n_2 - k$ shadow images will not be used), the number of lost LSBs of shadow images $n_2 - k$ is equal to the change number of the determinant number $(t_{n_2} - t_k)$ to ensure correct decoding as shown in Eq. (4). Based on Eqs. (2–4), we obtain Eq. (5).

$$k \in 2Z^+ + 1, n_2 \in Z^+, k \le n_2 \tag{2}$$

$$t_k = \left\lceil \frac{k}{2} \right\rceil \tag{3}$$

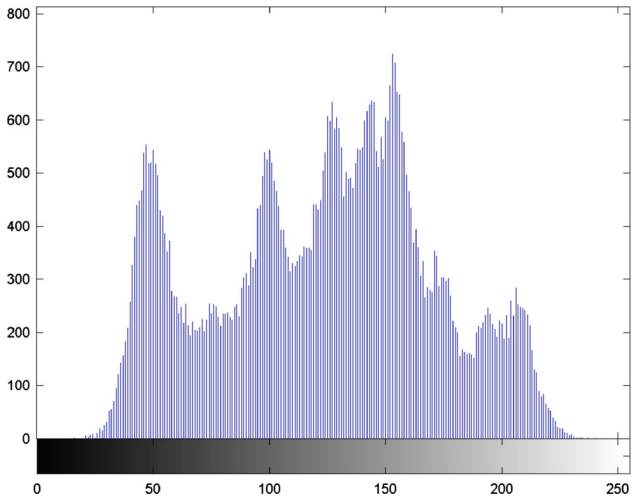
$$n_2 - k = t_{n_2} - t_k \tag{4}$$

$$t_{n_2} = \left\lceil n_2 - \frac{k}{2} \right\rceil, \quad t_{n_2}, n_2 \in Z^+, k \in 2Z^+ + 1, k \le n_2 \tag{5}$$

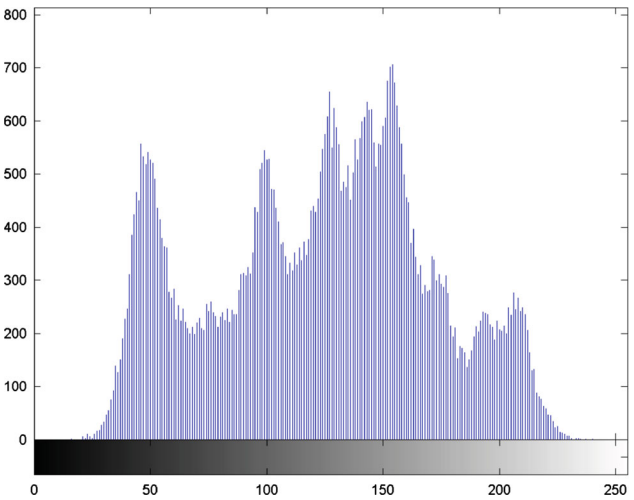
The generation architecture is shown in Fig. 3, and the algorithms of generation and recovery of the (k, n_2) scheme are given in Algorithms 3 and 4 as below.

(a) Histogram of original image of Fig. 4 (a)

(b) Histogram of recovered image of Fig. 4 (d)



(c) Histogram of original image of Fig. 4 (b)



(d) Histogram of recovered image of Fig. 4 (e)

Fig. 5 Histogram analysis of proposed (n_1, n_1) scheme

Algorithm 3. The proposed (k, n_2) threshold scheme.

Input: A $M \times N$ binary secret image S, n_2 $M \times N$ source grayscale cover images $C_1, C_2, \cdots C_{n_2}$, threshold k $(3 \le k \le n_2, k \in Z^+)$.

Output: n_2 shadow images $SC_1, SC_2, \cdots SC_{n_2}$.

Step 1: For each position $(i, j) \in \{(i, j) \mid 1 \le i \le M, 1 \le j \le N\}$, repeat Steps 2-5.

Step 2: Compute LSBs $b_p = C_p(i, j) \bmod 2$ $, 1 \le p \le n_2$.

Step 3: Compute $num = \left|\{p \mid b_p = S(i, j), p \in \{1, 2, \cdots n_2\}\}\right|$ and t_{n_2} using Eq.(5).

If $num < t_{n_2}$ go to step 4; else go to step 5.

where $|\ |$ denotes the elements number of a set.

Step 4: Randomly select $t_{n_2} - num$ unrepeated numbers $l_q \in \{p \mid b_p \ne S(i, j), p \in \{1, 2, \cdots n_2\}\}$

Compute $SC_p(i, j) = C_p(i, j), p \in \{1, 2, \cdots, n_2\}, p \ne l_q, q = 1, 2, \cdots t_{n_2} - num$

If $C_{l_q}(i, j) = 0$ $SC_{l_q}(i, j) = 1$;

Else if $C_{l_q}(i, j) = 255$ $SC_{l_q}(i, j) = 254$;

Else $SC_{l_q}(i, j) = C_{l_q}(i, j) + 1$ *or* $C_{l_q}(i, j) - 1$ randomly.

Step 5: Compute $SC_p(i, j) = C_p(i, j), p \in \{1, 2, \cdots, n_2\}$.

Step 6: Output the n shadow images $SC_1, SC_2, \cdots SC_{n_2}$.

Algorithm 4. Secret image recovery of the proposed (k, n_2) threshold scheme.

Input: k shadow images $SC_{l_1}, SC_{l_2}, \cdots SC_{l_k}$.

Output: A $M \times N$ binary secret image S.

Step 1: For each position $(i, j) \in \{(i, j) \mid 1 \le i \le M, 1 \le j \le N\}$, repeat Steps 2-3.

Step 2: Compute LSBs $b_p = SC_p \bmod 2$ $, 1 \le p \le k$.

Step 3: Compute $num = \sum_{r=1}^{k} b_r$ and t_k using Eq.(3).

If $num < t_k$ $S(i, j) = 0$; *Else if* $num > t_k$ $S(i, j) = 1$; *Else* error.

Step 4: Output the binary secret image S.

3.3 Remarks

Here, we remark some insights gleaned from the schemes in Table 1.

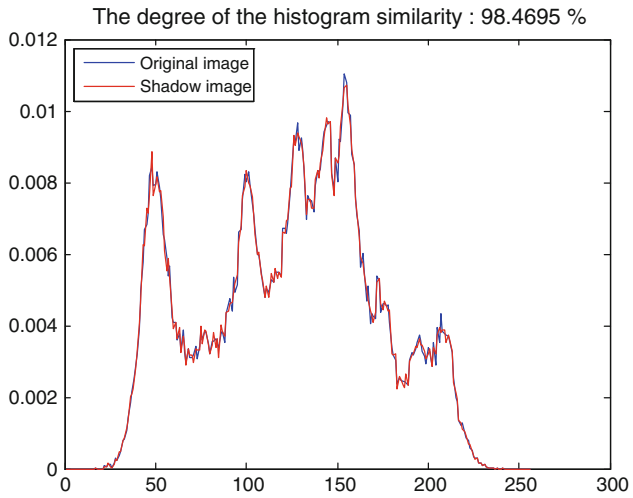


Fig. 6 HS of Fig. 4b, e

4 Experimental results and analysis

In this section, we have conducted experiments and analysis to evaluate the effectiveness of the proposed schemes. First, the images are illustrated to show the effectiveness of the schemes. Then, the comparisons of the proposed schemes with related schemes are presented, especially [3,4] since the two proposed schemes are the improvements of these schemes. In addition, schemes in [3,4] have good features in SSS, such as alternative order of shadow images in recovery, meaningful shadow images, lossless recovery of binary secret image, avoiding the pixel expansion, (n, n) or (k, n) thresholds, and so on.

Herein, average flipping rate (AFR) [24], histogram similarity (HS), and normalized correlation (NC) [25–27] are used to evaluate the quality of the shadow images and to be the similarity measurement between the original grayscale cover images and the shadow images.

The binary secret image and standard grayscale images with size 256×256 are used to test the efficiency of the proposed schemes.

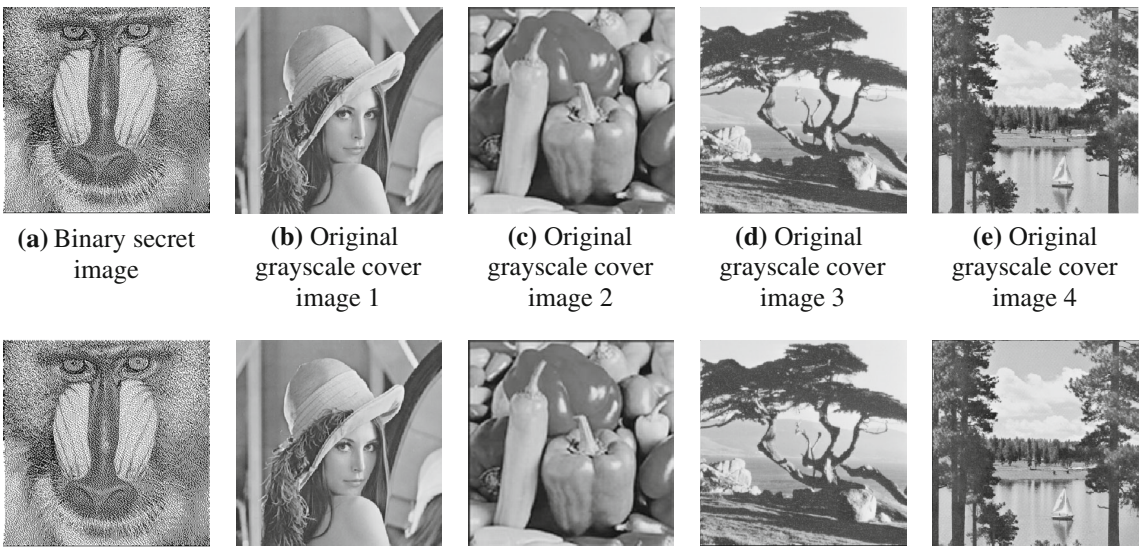
4.1 Image illustrations and HS of the proposed schemes

4.1.1 (n_1, n_1) scheme

In the experiments, we use $(2, 2)$ threshold to test the efficiency of the proposed (n_1, n_1) scheme. One binary secret image and two grayscale images are used as the cover images as shown in Fig. 4a–c. Figure 4e, f show the corresponding two shadow images. From HVS we cannot see the difference between the original grayscale cover images and the shadow images, the visual quality of the shadow images will be evaluated detailedly later. The recovered secret binary image with the two shadow images is shown in Fig. 4d, and it is the same as the binary secret image. The recovered secret image is lossless, since mean square error (MSE), as shown in Eq. (6), of Fig. 4a, d is equal to 0.

MSE, Eq. (6), is used to measure the mean square error between the cover image and shadow image.

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} [I'(i, j) - I(i, j)]^2 \tag{6}$$

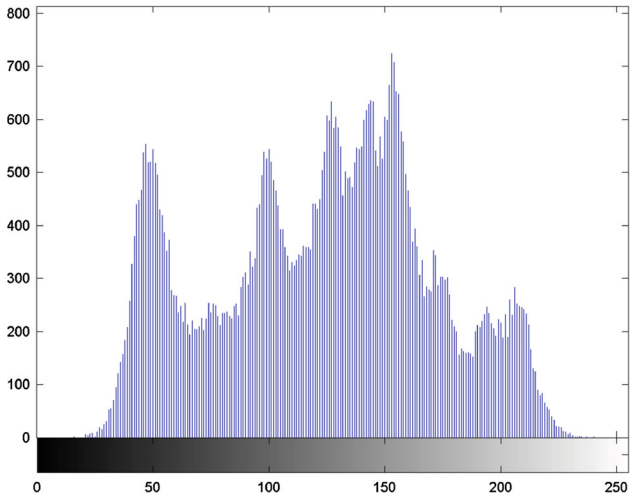


(a) Binary secret image
(b) Original grayscale cover image 1
(c) Original grayscale cover image 2
(d) Original grayscale cover image 3
(e) Original grayscale cover image 4
(f) Recovered binary secret image
(g) Shadow image 1
(h) Shadow image 2
(i) Shadow image 3
(j) Shadow image 4

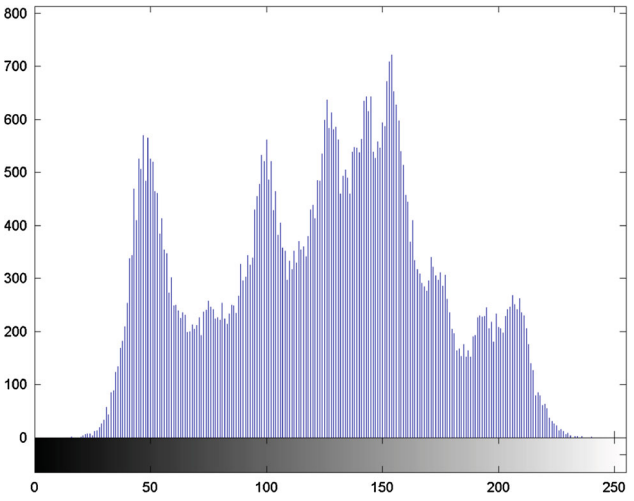
Fig. 7 Images illustration of proposed (3, 4) scheme

(a) Histogram of original image of Fig. 7 (a)

(b) Histogram of recovered image of Fig. 7 (f)



(c) Histogram of original image of Fig. 7 (b)



(d) Histogram of recovered image of Fig. 7 (g)

Fig. 8 Histogram analysis of proposed (k, n_2) scheme

The HS of original grayscale image I and modified grayscale image I' can be calculated by Eq. (8). p_i is the normalized histogram of I computed by Eq. (7).

$$p_i = \frac{T_i}{T}, \quad i = 0, 1, 2, \ldots, 255 \tag{7}$$

$$HS(I, I') = \sum_{i=1}^{255} \min\left(P_i, P_i'\right) \tag{8}$$

where T is the total number of pixels in image I, T_i is the number of pixels with value i.

$HS \in [0, 1]$, and bigger HS will indicate more similar between original grayscale image I and modified grayscale image I'.

Figure 5 shows the histogram analysis of the proposed (n_1, n_1) scheme for the original (Fig. 4a, b) and recovered (Fig. 4d) or shadow (Fig. 4e) image separately. The HS of the original cover grayscale image (Fig. 4b) and shadow (Fig. 4e) image is shown in Fig. 6, the degree of similarity, calculated by Eq. (8), of Fig. 4b, e is 98.4659 %, the average degree of the two shadow images is 98.4598 % and very close to 1.

The histogram of the recovered image (Fig. 4d) is the same with the original binary secret image (Fig. 4a), and the histogram of the shadow image(Fig. 4e) is approximately the same with the original grayscale cover image (Fig. 4b).

As observed during the above tests and illustrations, we can see the following merits for the proposed (n_1, n_1) :

1. The shadow images of the proposed (n_1, n_1) scheme are meaningful with perfect quality.
2. The recovery secret image is the same with the original secret image, and the recovery is lossless.

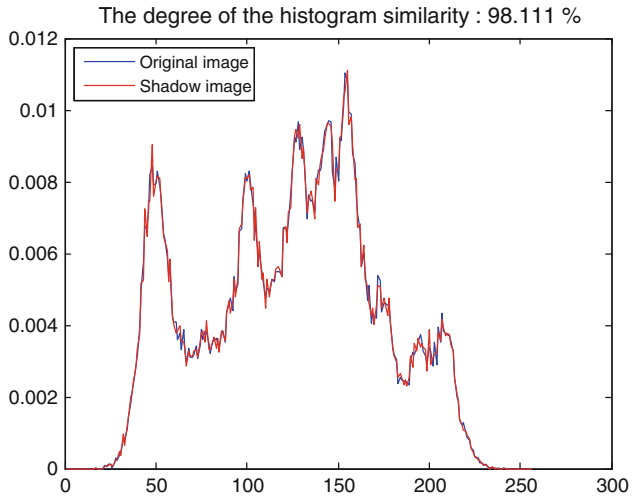


Fig. 9 HS of Fig. 7b, g

3. Since the shadow images have the same size with the binary secret image $M \times N$ binary secret image S, the proposed (n_1, n_1) scheme has no pixel expansion.

4.1.2 (k, n_2) scheme

In the experiments, we use (3, 4) threshold setting to test the efficiency of the proposed (k, n_2) scheme. One binary secret image and four grayscale images are used as the cover images as shown in Fig. 7a–e. Figure 7g–i shows the corresponding four shadow images. From HVS, we also cannot see the difference between the original grayscale cover images and the shadow images. And recovered secret binary image with the first 3 shadow images (also the same result with the other 3 shadow images) is shown in Fig. 7f, it is the same as the binary secret image. The recovered secret image is lossless, since MSE, as shown in Eq. (6), of Fig. 7a, f is equal to 0.

Figure 8 shows the histogram analysis of the proposed (k, n_2) scheme for the original (Fig. 7a, b) and recovered (Fig. 7f) or shadow (Fig. 7g) image separately. The HS of the original cover grayscale image (Fig. 7b) and shadow image (Fig. 7g) is shown in Fig. 9, the degree of similarity of Fig. 7b, g is 98.111 %, the average degree is 97.92635 % of the four shadow images and close to 1.

The histogram of the recovered image (Fig. 7f) is the same with the original binary secret image (Fig. 7a), and the histogram of the shadow image (Fig. 7g) is similar to the original grayscale cover image (Fig. 7b).

As observed during the above tests and illustrations, we can see the following merits for the proposed (k, n_2) :

1. The shadow images of the proposed (k, n_2) scheme are meaningful with good quality.
2. The recovery secret image is the same with the original secret image, and the recovery is lossless.
3. Since the shadow images have the same size with the binary secret image $M \times N$ binary secret image S,the proposed (k, n_2) scheme has no pixel expansion.

4.2 Comparisons of AFR [24]

In a (k, n), SSS based on error diffusion technique, let r be the sharing secret bits per sharing time, m denotes the pixel expansion, let s be the flipping bits for n cover images per sharing time, which can be calculated by Eq. (9).

$$s = f(n, k, m, r) \tag{9}$$

where f is depend on the secret sharing method based on error diffusion techniques. AFR could be defined [24] as Eq. (10).

$$\text{AFR} = \frac{s}{nt} = \frac{f(n, k, m, r)}{ntg} \tag{10}$$

where g denotes the average gray level of the original grayscale cover images.

AFR $\in (0, 1)$, and smaller AFR will indicate better visual quality of shadow images [11] theoretically before sharing.

In the proposed schemes, we assume that pixel values of the original grayscale cover images and the shadow images are random and independent with each other, which are reasonable since randomly selecting standard images and error diffusion technology, and since there is no pixel expansion, we have $m = 1, r = 1, g = 128$.

For the proposed (n_1, n_1) scheme, the flipping number in the n_1 bits is computed by Eq. (11).

$$s = \begin{cases} 0 \quad if\ S(i,j) = C^1_{i_1}(i,j) \oplus C^1_{i_2}(i,j) \cdots \oplus C^1_{i_{n_1}}(i,j) & p = \frac{1}{2} \\ 1 \quad if\ S(i,j) \neq C^1_{i_1}(i,j) \oplus C^1_{i_2}(i,j) \cdots \oplus C^1_{i_{n_1}}(i,j) & p = \frac{1}{2} \end{cases} \tag{11}$$

$s = 0$ or $s = 1$ with the same probability $\frac{1}{2}$, since the cover images are random and independent with each other.

Thus, we could gain the AFR of the proposed (n_1, n_1) scheme in Eq. (12).

$$\text{AFR} = \frac{0 \times \frac{1}{2} + 1 \times \frac{1}{2}}{128 n_1} = \frac{1}{256 n_1} \tag{12}$$

For the proposed (k, n_2) scheme, From Eq. (5), we obtain Eq. (13) from dividing the left and right equations by n_2. Since assuming the n_2 cover images are independent with each other. Then, the n_2 bits in the same position with one secret bit of each cover image are nearly random. That is, the number of bits 0 and 1 is both $n_2/2$, then the flipping number s in the n_2 bits is $s = f(n_2, k, m, r) = t_{n_2} - \frac{n_2}{2}$; thus, we use Eqs. (10) and (5) to obtain Eq. (14).

Table 2 AFR comparisons between proposed (n_1, n_1) scheme and Wu's (n_1, n_1) scheme, proposed (k, n_2) scheme and Li's (k, n_2) scheme

Schemes	Proposed (n_1, n_1) scheme	Wu's (n_1, n_1) scheme	Proposed (k, n_2) scheme	Li's (k, n_2) scheme
AFR	$\frac{1}{256n_1}$	$\frac{1}{2n_1}$	$\frac{1}{128n_2}\left\lceil n_2 - \frac{k}{2}\right\rceil - \frac{1}{256}$	$\frac{1}{n_2}\left\lceil n_2 - \frac{k}{2}\right\rceil - \frac{1}{2}$

Table 3 NC comparisons between proposed (n_1, n_1) scheme and Wu's (n_1, n_1) scheme

(n_1, n_1)	Images	NC	
		Proposed (n_1, n_1) scheme	Wu's (n_1, n_1) scheme
(2,2)	Shadow image 1	1.0000	0.9856
	Average shadow images	1.0000	0.9854
(3,3)	Shadow image 1	1.0000	0.9954
	Average shadow images	1.0000	0.9943
(4,4)	Shadow image 1	1.0000	0.9984
	Average shadow images	1.0000	0.9971
(5,5)	Shadow image 1	1.0000	0.9989
	Average shadow images	1.0000	0.9981
(6,6)	Shadow image 1	1.0000	1.0001
	Average shadow images	1.0000	1.0001
(7,7)	Shadow image 1	1.0000	1.0009
	Average shadow images	1.0000	1.0011
(8,8)	Shadow image 1	1.0000	1.0012
	Average shadow images	1.0000	1.0014
(9,9)	Shadow image 1	1.0000	1.0014
	Average shadow images	1.0000	1.0023
(10,10)	Shadow image 1	1.0000	1.0017
	Average shadow images	1.0000	1.0015
(11,11)	Shadow image 1	1.0000	1.0014
	Average shadow images	1.0000	1.0024

$$1 - \frac{t_{n_2}}{n_2} < \frac{k}{2n_2} \Rightarrow 1 - \frac{k}{2n_2} < \frac{t_{n_2}}{n_2} \tag{13}$$

$$\begin{aligned} \mathrm{AFR} &= \frac{t_{n_2} - \frac{n_2}{2}}{128n_2} = \frac{1}{128}\frac{t_{n_2}}{n_2} - \frac{1}{256} \\ &= \frac{\left\lceil n_2 - \frac{k}{2}\right\rceil}{128n_2} - \frac{1}{256} > \frac{1}{128}\left(1 - \frac{k}{2n_2}\right) \\ &\quad - \frac{1}{256} = \frac{1}{256}(1 - \frac{k}{n_2}) \end{aligned} \tag{14}$$

Applying the same index computation method, AFR of Wu's (n_1, n_1) scheme and Li's (k, n_2) scheme could also be calculated shown in Table 2, where we can find that the propose schemes have lower AFR that indicates better visual quality of shadow images.

4.3 Comparisons of NC

The NC is an evaluation metric that evaluates the quality between the original embedded secret image and the extracted secret image. NC is defined by Eq. (15).

$$\mathrm{NC}(I, I') = \frac{1}{\sum_{i=1}^{M}\sum_{j=1}^{N} I^2(i, j)} \sum_{i=1}^{M}\sum_{j=1}^{N} I(i, j) \times I'(i, j) \tag{15}$$

where M, N is the total number of pixels in the image, $I(i, j)$ and $I'(i, j)$ are the values of the (i, j)pixel in original and recovered image of size $M \times N$, respectively.

Using Fig. 4a as the secret image, Table 3 compares NC of shadow images between the proposed scheme and the method in Ref. [3] with $n_1 = 2, 3, \ldots, 11$. NC for the shadow image 1 and the average NC for the n_1 shadow images are illustrated in Table 3. As can be seen from Table 3, NC of the proposed (n_1, n_1) scheme is closer to 1 than Wu's scheme.

Using Fig. 7a as the secret image, Table 4 compares NC of shadow images between the proposed scheme and the method in Ref. [4] with $n_2 = 3, 4, \ldots, 11$ under $k = 3$. NC for the shadow image 1 and the average NC for the n_2 shadow images are illustrated in Table 4. As can be seen from Table 4, NC of the proposed (k, n_2) scheme is closer to 1 than Li's scheme.

Table 4 NC comparisons between proposed (k, n_2) scheme and Li's (k, n_2) scheme

(k, n_2)	Images	NC	
		Proposed (k, n_2) scheme	Li's (k, n_2) scheme
(3,3)	Shadow image 1	1.0000	0.9850
	Average shadow images	1.0000	0.9802
(3,4)	Shadow image 1	1.0000	0.9757
	Average shadow images	1.0000	0.9670
(3,5)	Shadow image 1	1.0000	0.9762
	Average shadow images	1.0000	0.9607
(3,6)	Shadow image 1	1.0000	0.9729
	Average shadow images	1.0000	0.9571
(3,7)	Shadow image 1	1.0000	0.9645
	Average shadow images	1.0000	0.9431
(3,8)	Shadow image 1	1.0000	0.9536
	Average shadow images	1.0000	0.9378
(3,9)	Shadow image 1	1.0000	0.9519
	Average shadow images	1.0000	0.9397
(3,10)	Shadow image 1	1.0000	0.9054
	Average shadow images	1.0000	0.8867
(3,11)	Shadow image 1	1.0000	0.9088
	Average shadow images	1.0000	0.8961

Table 5 Property comparison with relative schemes

Scheme	(k, n) threshold	Recovering measure	Shadow images are alternative	Meaningful	Lossless	No pixel expansion
Ref. [1]	√	Stacking	√	×	×	×
Ref. [3]	(n, n) threshold	Boolean	√	√	√	√
Ref. [4]	√	Addition and comparison	√	√	√	√
Ref. [9]	√	Stacking	√	√	×	×
Ref. [10]	√	Stacking	√	×	×	√
Ref. [11]	√	Stacking	√	√	×	×
Ref. [15]	√	Boolean	√	×	√	√
Proposed schemes	(n_1, n_1)/ (k, n_2) threshold	Mod and Boolean/addition and comparison	√	√	√	√

In addition:

- Since Wu's and Li's schemes embed the secret bits into binary images, the errors are diffused to adjacent pixels while the proposed schemes embed the secret bits into the LSBM of the grayscale images. Therefore, the quality of the shadow images in proposed schemes is better.
- Since error diffusion and permutation technologies are applied in the generation phase, hence Wu's and Li's schemes have higher complex computation than the proposed schemes.

4.4 General discussion

In the light of the above-mentioned simulation results, we can see that the proposed schemes achieve more properties of secret image sharing scheme. The properties comparisons between the proposed schemes and other relative SSSs are shown in Table 5. From Table 5, we can see that the proposed schemes outperform the state-of-the-art schemes in the literature. Furthermore, the proposed schemes have good quality of shadow images, which are easily extended to other information hiding and secret sharing methods. The first scheme is suitable for (n_1, n_1) $(2 \leq n_1,\ n_1 \in Z^+)$ applications with perfect shadow images quality and security, while the second scheme for (k, n_2) $(3 \leq k \leq n_2,\ n_2 \in Z^+, k \in 2Z^+ + 1)$

applications with high quality of shadow images and acceptable security.

5 Conclusion

Two different secret image sharing schemes, (n_1, n_1) and (k, n_2) threshold, based on information hiding theory have been proposed in this paper. The proposed schemes have several merits compared with previous schemes such as better quality of meaningful shadow images with lower computation, good expansibility, lossless, and alternative order recovery and no pixel expansion. Simulations results and analysis show that the proposed schemes outperform the recently proposed schemes.

Acknowledgments The authors wish to thank the anonymous reviewers for their suggestions to improve this paper. This work is supported by the National Natural Science Foundation of China (Grant Number: 61100187) and the Fundamental Research Funds for the Central Universities (Grant Number: HIT. NSRIF. 2010046, HIT. NSRIF. 2013061).

References

1. Naor, M., Shamir, A.: Visual cryptography. In: Advances in Cryptography, Eurocrypt'94, Italy, May 9–12, pp. 1–12 (1994)
2. Weir, J., Yan, W.Q.: A comprehensive study of visual cryptography. In: Transactions on DHMS V, LNCS 6010, pp. 70–105 (2010)
3. Wu, X.-T., Sun, W.: Image sharing scheme based on error diffusion. J. Comput. Appl. **31**(1), 74–81 (2011)
4. Li, L., Yan, X., Wang, N., Abd El-Latif, A.A., Niu, X.: Meaningful image sharing threshold scheme based on error diffusion. Int. J. Digit. Content Technol. Appl. (JDCTA) **6**(13), 275–284 (2012)
5. Feng, B.J., Wu, H.C., Tsai, C.S., et al.: A new multi-secret images sharing scheme using Lagrange's interpolation [J]. J. Syst. Softw. **76**(3), 327–339 (2005)
6. Thien, C.C., Lin, J.C.: Secret image sharing. Comput. Graph **26**(5), 765–770 (2002)
7. Thien, C.C., Lin, J.C.: An image-sharing method with user-friendly shadow images. IEEE Trans. Circuits Syst. Video Technol. **13**(12), 1161–1169 (2003)
8. Zhao, R., Zhao, J.J., Dai, F., Zhao, F.Q.: A new image secret sharing scheme to identify cheaters. Comput. Stand. Interfaces **31**(1), 252–257 (2009)
9. Ateniese, G., Blundo, C., De Santis, A., Stinson, D.R.: Extended capabilities for visual cryptography [J]. Theor. Comput. Sci. **250**(1/2), 143–161 (2001)
10. Yang, C.: New visual secret sharing schemes using probabilistic method [J]. Pattern Recognit. Lett. **25**(4), 481–494 (2004)
11. Zhou, Z., Arce, G.R., Crescenzo, G.D.: Halftone visual cryptography. IEEE Trans. Image Process. **15**(8), 2441–2453 (2006)
12. Myodo, E., Sakazawa, S., Takishima, Y.: Visual cryptography based on void and cluster halftoning technique. In: ICIP, Atlanta, GA, USA, Oct. 8-11, pp. 97–100 (2006)
13. Myodo, E., Takagi, K., Miyaji, S., Takishima, Y.: Halftone visual cryptography embedding a natural grayscale image based on error diffusion technique. In: ICME, Beijing, China, July 2–5, pp. 2114–2117 (2007)
14. Wang, Z., Arce, G.R.: Halftone visual cryptography through error diffusion. In: ICIP, Atlanta, GA, USA, Oct. 8-11, pp. 109–112 (2006)
15. Wang, D.-S., Zhang, L., Ning, M.A., et al.: Two secret sharing schemes based on Boolean operations [J]. Pattern Recognit. **40**(10), 2776–2785 (2007)
16. Niu, X.-M., Lu, Z.-M.: Digital watermarking of still image with grag-scale digital water marks. IEEE Trans. Consumer Electron. **46**(1), 137–145 (2000)
17. Wu, X., Ou, D., Liang, Q., Sun, W.: A user-friendly secret image sharing scheme with reversible steganography based on cellular automata. J. Syst. Softw. **85**, 1852–1863 (2012)
18. Liu, M., Huang, W.-J., Niu, X.-M.: The hiding information technology in video. J. Test Meas. Technol. **18**, 77–80 (2004)
19. Liu, Q., Sung, A.H.: Image complexity and feature mining for steganalysis of least significant bit matching steganography. Inf. Sci. **178**, 21–36 (2008)
20. van Schyndel, R.G., Tirkel, A.Z., Osborne, C.F.: A digital watermark [J]. In: Proceeding ICIP [C], Austin, Texas, USA, November 13–16 (1994)
21. Sharp, T.: An implementation of key-based digital signal steganography [C]. In: Proceedings of the 4th International Workshop on Information Hiding, vol. 2137, pp. 13–26. IEEE Press, Pittsburgh (2001)
22. Guo, C., Chang, C.-C., Qin, C.: A multi-threshold secret image sharing scheme based on MSP. Pattern Recognit. Lett. **33**, 1594–1600 (2012)
23. NIST/SEMATECH e-Handbook of Statistical Methods. http://www.itl.nist.gov/div898/handbook/eda/section3/eda3652.htm
24. Yan, X., Wang, S., Li, L., Wei, Z., Niu, X.: A new assessment measure of shadow image quality based on error diffusion techniques. J. Inf. Hiding Multimedia Signal Process. (JIHMSP) **4**(2), 118–126 (2013)
25. Hsu, C.T., Wu, J.L.: Hidden digital watermarks in images. IEEE Trans. Image Process. **8**(1), 58–68 (1999)
26. Chen, W.Y., Chen, C.H.: A robust watermarking scheme using phase shift keying with the combination of amplitude boost and low amplitude block selection. Pattern Recognit. **38**(4), 587–598 (2005)
27. Kutter, M., Petiteolas, F.: A fair benchnlark for image watermarking systems[J]. SPIE Secur. Watermarking Multimedia Contents **3657**, 226–239 (1999)