Frontiers of Information Technology & Electronic Engineering
www.jzus.zju.edu.cn; engineering.cae.cn; www.springerlink.com
ISSN 2095-9184 (print); ISSN 2095-9230 (online)
E-mail: jzus@zju.edu.cn

Public key based bidirectional shadow image authentication without pixel expansion in image secret sharing*

Xuehu YAN†‡, Longlong LI, Jia CHEN, Lei SUN

National University of Defense Technology, Hefei 230037, China

†E-mail: publictiger@126.com

Received Mar. 26, 2022; Revision accepted Aug. 26, 2022; Crosschecked Nov. 29, 2022

Abstract: Image secret sharing (ISS) is gaining popularity due to the importance of digital images and its wide application to cloud-based distributed storage and multiparty secure computing. Shadow image authentication generally includes shadow image detection and identification, and plays an important role in ISS. However, traditional dealer-participatory methods, which suffer from significant pixel expansion or storing auxiliary information, authenticate the shadow image mainly during the decoding phase, also known as unidirectional authentication. The authentication of the shadow image in the distributing (encoding) phase is also important for the participant. In this study, we introduce a public key based bidirectional shadow image authentication method in ISS without pixel expansion for a (k, n) threshold. When the dealer distributes each shadow image to a corresponding participant, the participant can authenticate the received shadow image with his/her private key. In the decoding phase, the dealer can authenticate each received shadow image with a secret key; in addition, the dealer can losslessly decode the secret image with any k or more shadow images. The proposed method is validated using theoretical analyses, illustrations, and comparisons.

Key words: Image secret sharing; Shadow image authentication; Public key; Pixel expansion; Lossless decoding
https://doi.org/10.1631/FITEE.2200118 **CLC number:** TP309

1 Introduction

Using image secret sharing (ISS) for a (k, n) threshold, the dealer encodes a secret image to output n shadow images, also known as shadows or shares, which are then distributed to the corresponding n participants. The dealer can decode the secret image with any k or more shadow images (i.e., at most $n-k$ shadow images are lost), which is known as the loss-tolerant property of ISS. Hence, ISS is currently used in several applications, such as access control (Yan et al., 2017; Beugnon et al., 2019), key management (Cheng et al., 2018), blockchain (Fukumitsu et al., 2017; Shen J et al., 2019), password transmission (Wang W et al., 2017), digital watermarking (El-Latif et al., 2018), identity authentication (Chavan et al., 2014; Li YN and Guo, 2018), and distributive storage in a cloud (Komargodski et al., 2017). The value of each binary pixel can be represented by 1 bit, and the value of each grayscale pixel can be represented by 1 byte; therefore, ISS is easily extended to secret sharing. Among many sharing principles of traditional ISS technologies (Wang GY et al., 2016; Shivani and Agarwal, 2018; Yan et al., 2018, 2020b; Meng et al., 2021; Harn et al., 2022), the use of polynomials (Pilaram and Eghlidos, 2017) is widely studied.

‡ Corresponding author
* Project supported by the National Natural Science Foundation of China (No. 62271496)
ORCID: Xuehu YAN, https://orcid.org/0000-0001-6388-1720

Shamir (1979) designed the first polynomial-based secret sharing for a (k, n) threshold by randomly building a $(k-1)$-degree polynomial. Inspired by Shamir's work, some follow-up works (Thien and Lin, 2002; Liu YX and Yang, 2017; Liu YX et al., 2018a, 2019; Yan et al., 2021) investigated several improved polynomial-based ISS schemes to obtain significant properties. Polynomial-based ISS is advantageous because the decoded secret image has high quality and does not exhibit pixel expansion. The dealer can encode a secret image to n shadow images using polynomial-based ISS. The dealer normally distributes the shadow images to n corresponding participants (Fig. 1). When any k or more shadow images are collected during the normal dealer-participatory decoding phase, the secret is decoded with high quality using the Lagrange interpolation (Fig. 1).

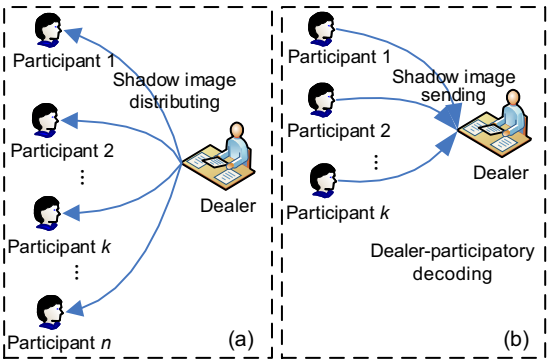

Fig. 1 Normal dealer-participatory shadow image distributing (a) and secret image decoding (b)

However, the above-mentioned polynomial-based ISS schemes cannot authenticate shadow images. The authentication plays an important role in ISS (Fig. 2). If a watch dog tampers with the shadow image during abnormal dealer participatory shadow image distribution, a participant cannot authenticate the received shadow image without authentication. Here, a watch dog represents an eavesdropper in cryptography or a third party on the network in communication security. In an abnormal secret image decoding phase, the dealer cannot successfully decode the original secret image or even distinguish the fake one if there is a fake shadow image among the k collected ones.

In contrast, in the distribution of an abnormal shadow image and the decoding of a secret image as shown in Fig. 3, authentication allows a participant to judge whether the received shadow image is fake or tampered with when receiving each shadow image from the corresponding participant; the dealer can also judge it based on the result of shadow image authentication, stop the decoding phase if a fake shadow image is detected and identified, and broadcast the fake one to all the other participants to avoid further deception.

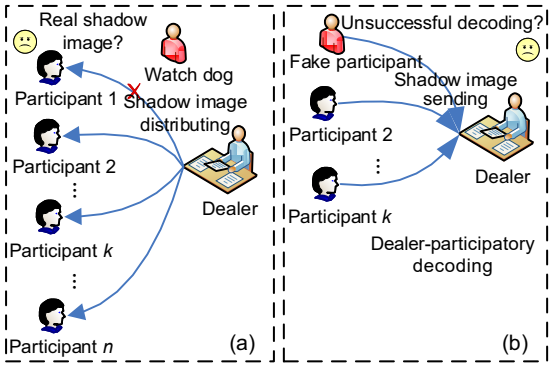

Fig. 2 Distribution of an abnormal shadow image (a) and decoding of a secret image without authentication (b)

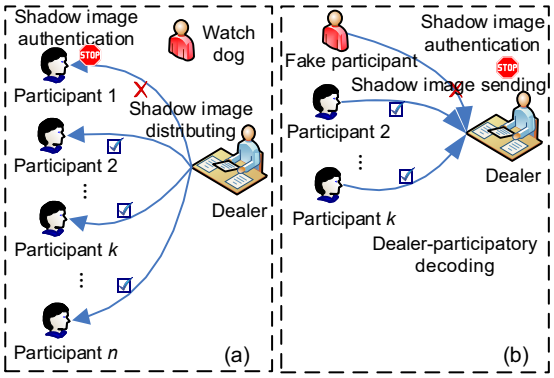

Fig. 3 Distribution of an abnormal shadow image (a) and decoding of a secret image with authentication (b), illustrating the motivation of this paper

Shadow image authentication is critical and ISS with shadow image authentication ability is gaining popularity. Most existing ISS schemes that support shadow image authentication can be classified into two categories. The first category uses information hiding (or fragile watermark) (Lin and Tsai, 2004; Chang et al., 2008; Liu YJ and Chang, 2018; Liao et al., 2022). A typical work is Liu YJ and Chang (2018), in which the authors realized shadow image authentication using turtle shell based information

hiding. This type of scheme embeds the shadow images in the cover images using existing information hiding techniques, resulting in a possible high pixel expansion (Fig. 4a). The other category uses auxiliary information (Li P et al., 2010; Ulutas et al., 2013; Du et al., 2020), such as hash. This type of scheme uses the auxiliary information to achieve authentication, which also results in possible pixel expansion or increase in the required storage space (Fig. 4b).

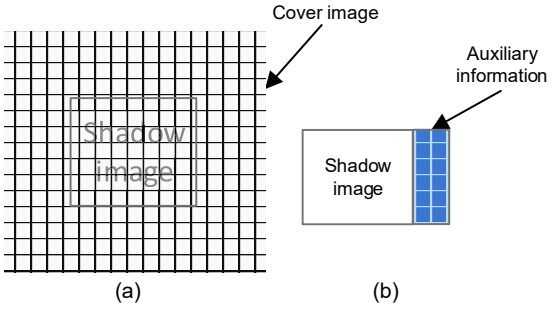

Fig. 4 Analyses of traditional image secret sharing schemes with shadow authentication ability: (a) using information hiding; (b) using auxiliary information

Liu YX et al. (2018b) proposed polynomial-based ISS for a (k, n) threshold with shadow image authentication based on improved polynomial-based ISS. They embed an authentication value into a polynomial coefficient. However, this scheme can authenticate the shadow image only in the decoding phase, also known as unidirectional authentication, and it cannot authenticate the shadow image during the shadow image distribution phase. It also has flaws in fake participant identification, auxiliary encryption, and lossy decoding.

Yan et al. (2020a) proposed a separate shadow authentication method using a fusing (2, 2)-threshold visual cryptographic scheme (VCS) (Shen G et al., 2017) and polynomial-based ISS. In the encoding phase, the shadow image bit generated using VCS is embedded in the most significant bit (MSB) of each shadow image pixel. However, their method is used only for shadow image authentication during the secret image decoding phase. Following Yan et al. (2020a), Jiang et al. (2020) developed an authentication using a $(2, n+1)$-threshold VCS and the least significant bit instead of the MSB. However, it cannot authenticate a shadow image during the distribution phase.

This study introduces a bidirectional shadow image authentication method without pixel expansion in ISS for a (k, n) threshold based on ISS rather than on information hiding (Fig. 3). Here "bidirectional shadow image authentication" shows that shadow image authentication in the shadow image distributing and secret image decoding (sending) phases (Fig. 3) achieves stronger authentication than "unidirectional shadow image authentication."

The following is the key challenge. The encoding and decoding methods usually entail the use of mathematical functions in ISS, such as polynomial and interpolation, which are sensitive to slight changes; thus, achieving bidirectional shadow image authentication is a key challenge.

In this study, we introduce a public key based bidirectional shadow image authentication method without pixel expansion in ISS for a (k, n) threshold.

In the encoding phase, the dealer first uses a random number generator with his/her secret key to generate two coordinates for each participant. Second, a hash of the pixels between the two coordinates is generated for the authentication of each shadow image. Third, the two coordinates are encrypted with the public key of each participant to obtain two encrypted coordinates. Finally, the encrypted coordinates and the hash value are fused into each shadow image to avoid any pixel expansion using a screening operation in the process of polynomial-based ISS. Here, a "screening operation" denotes an operation that can screen the polynomial coefficients to satisfy some requirements. When the dealer distributes each shadow image to a corresponding participant, the participant can authenticate the received shadow image with his/her private key.

In the decoding phase, the dealer can authenticate each received shadow image with a secret key, i.e., achieving a separate shadow image authentication ability; in addition, the dealer can losslessly decode the secret image with any k or more shadow images. The proposed scheme has no pixel expansion with a separate shadow image authentication ability. In addition, it achieves lossless decoding without auxiliary encryption. The proposed method is validated using theoretical analyses, illustrations, and comparisons.

2 Preliminaries

We describe some preliminaries for our introduced method in this section, including the principle

of polynomial-based ISS, public key encryption, and hash function. We use bidirectional authentication in polynomial-based ISS, public key encryption, and a hash function to authenticate a separate shadow image.

First, notations used in this study are presented in Table 1.

2.1 Polynomial-based ISS scheme

To encode a grayscale secret image, Shamir's original polynomial-based ISS scheme splits any secret pixel value s into n values, which are then assigned to n corresponding pixels in shadow images. We present Shamir's original polynomial-based scheme in Algorithm 1.

In the decoding phase, given any k pairs of the n pairs $\{(i,\mathrm{SC}_i)\}_{i=1}^{n}$, we can obtain the coefficients of $f(i)$ using Lagrange interpolation and obtain $s=f(0)$. However, secret s cannot be solved with fewer than k shadow images. Finally, an ISS for a (k,n) threshold is achieved.

In addition, when the original polynomial-based secret sharing is applied to the ISS, we conduct the following analysis: Because $0\le \mathrm{SC}_i(h,w)\le 255$, for $i=0,1,2,\cdots,k-1$, P cannot be any prime greater than a_0. The primes closest to 255 are 251 and 257. If 257 is used, we cannot store the i^{th} shadow pixel when $\mathrm{SC}_i(h,w)=256$; if 251 is used, we cannot reconstruct the secret pixel a_0 when $251\le a_0\le 255$. Finally, traditional polynomial-based ISS selects $P=251$ for a slight loss.

2.2 Public key encryption

The basic idea behind public key encryption is that a cryptosystem with two distinct keys may be possible. A public key is used to encode the plaintext and a private key is used to decode the ciphertext, where the public key can be public, i.e., known to everyone, and the private key is private, i.e., known to only one person. In this way, a public key encryption

Algorithm 1 Shamir's polynomial-based ISS

Input: a grayscale secret image S of size $H\times W$ and the threshold parameters (k,n).

Output: n shadow images $\mathrm{SC}_1,\mathrm{SC}_2,\cdots,\mathrm{SC}_n$.

Step 1: Select $P=251$. At each position $(h,w)\in\{(h,w)|1\le h\le H,1\le w\le W\}$, repeat steps 2 and 3.

Step 2: For $s=S(h,w)$, if $s\ge P$, fix $s=P-1$. To split s into pieces $\mathrm{SC}_1(h,w),\mathrm{SC}_2(h,w),\cdots,\mathrm{SC}_n(h,w)$, construct a $(k-1)$-degree polynomial as follows:

$$f(x)=(a_0+a_1x+\cdots+a_{k-1}x^{k-1})\bmod P, \tag{1}$$

in which $a_0=s$, and a_i is random in $[0,P-1]$, for $i=1,2,\cdots,k-1$.

Step 3: Calculate

$$\begin{aligned}&\mathrm{SC}_1(h,w)=f(1),\mathrm{SC}_2(h,w)=f(2),\cdots,\\&\mathrm{SC}_n(h,w)=f(n),\end{aligned} \tag{2}$$

where i can be used for an identifying index or an order label for the i^{th} participant.

Step 4: Output n shadow images $\mathrm{SC}_1,\mathrm{SC}_2,\cdots,\mathrm{SC}_n$.

Table 1 Chief notations in the paper

Notation	Description
(k,n)	Threshold, $2\le k\le n$
P	A prime number
$\oplus$	Boolean XOR operation
S	A grayscale secret image
$H\times W$	Size of the secret image
$\mathrm{SC}_1,\mathrm{SC}_2,\cdots,\mathrm{SC}_n$	Shadow images
t	Number of collected shadow images in the decoding phase
$S'_{\{i_1,i_2,\cdots,i_t\}}$ or $\mathrm{SC}_{\{i_1,i_2,\cdots,i_t\}}$	Decoding result S' by shadow images $\mathrm{SC}_{i_1},\mathrm{SC}_{i_2},\cdots,\mathrm{SC}_{i_t}$
$p(x)$	Probability of any event x
XOR4LBs(a)	XORing result of the four lower bits of a grayscale pixel a
k_{D}	Dealer's secret key
k_{p}^{i}	Public key of the i^{th} participant
k_{s}^{i}	Private key of the i^{th} participant
$\left(Z_{h_1}^{i},Z_{w_1}^{i}\right)$ and $\left(Z_{h_2}^{i},Z_{w_2}^{i}\right)$	Starting and ending plain coordinates for the i^{th} participant to be hashed
$Z_x'^{i},x=h_1,w_1,h_2,w_2$	Cipher coordinate for the i^{th} participant to be hashed
$bZ_x'^{i}$	Binary form of $Z_x'^{i}$
$0bZ_x'^{i}$	Expanded form of $bZ_x'^{i}$ with length of $W/4$ by adding 0 at the beginning
HV^{i}	Hash code for the i^{th} participant

system allows everyone to encode a plaintext to be sent to one person, and only that person can decode the ciphertext.

A public key encryption system is suitable for shadow image authentication in ISS, which is further analyzed as follows. If each participant has his/her public key and private key, the dealer can use the public key to generate an authenticating message and only the participant with the private key can authenticate the shadow image. It is a significant challenge to achieve bidirectional shadow image authentication using a public key encryption system with the condition of no pixel expansion.

The RSA cryptosystem is the best-known example of a public key encryption system, and it is used in our introduced method. Note that other public key encryption systems can also be used with our method.

2.3 Hash function

A hash function is used to compress a plaintext of arbitrary length to a random-looking and short plaintext digest with a fixed length, which is a public function known to all. A hash function has the property that it is computationally infeasible to yield collisions; i.e., it is difficult to decode the plaintext given digest. Additionally, if the plaintext is altered even a bit, the digest will no longer be valid. In this way, a hash function can achieve data authentication and integrity.

The hash function is suitable for detecting shadow images in ISS, which is further analyzed as follows. The dealer can compress a shadow image to a digest and send it to the participant along with the shadow image. The participant can use the digest to determine whether the shadow image has been altered. It is a significant challenge to achieve bidirectional shadow image authentication using a hash function without pixel expansion.

SHA-256 is a well-known hash function, and is used in our introduced method. Note that other hash functions can also be used in our method.

Above all, the difficult point is how to achieve bidirectional shadow image authentication by fusing the advantages of a public key encryption system and a hash function without pixel expansion.

3 Proposed public key based bidirectional shadow image authentication without pixel expansion

3.1 Proposed method

3.1.1 Framework

Fig. 5 shows the framework of the proposed public key based bidirectional shadow image authentication method without pixel expansion. The key modules in the framework are as follows: The dealer generates the coordinates using his/her secret key so that he/she knows the concentrated positions to be hashed to authenticate the shadow image when receiving each shadow image during the decoding phase. The dealer encrypts the coordinates using each participant's public key so that the true participant with the private key can authenticate the shadow image when receiving each shadow image during the shadow image distribution phase. The dealer embeds the encrypted coordinates and hash values into the first n and last n lines of each shadow image to avoid storing auxiliary information. In this way, no pixel expansion can be achieved.

The design idea of the proposed public key based bidirectional shadow image authentication method without pixel expansion is shown in Fig. 6.

3.1.2 Algorithms

Algorithm 2 is the proposed detailed encoding algorithm, and the decoding method is given in Algorithm 3. Fig. 6 is the overview of the proposed method only for the current position (h, w), which must be combined with Algorithm 2 to better

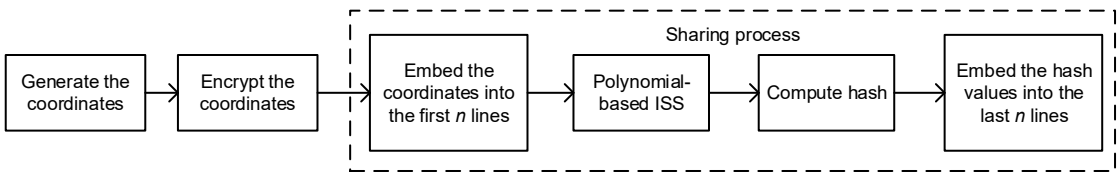

Fig. 5 Framework of the proposed public key based bidirectional shadow image authentication method

understand our method.

Regarding Algorithm 2, we comment as follows:

1. In step 1, k_{D} serves as a seed. Security and coordinate ranges are considered in the generation of Z_x^i. As in Table 1, $\left(Z_{h_1}^i, Z_{w_1}^i\right)$ and $\left(Z_{h_2}^i, Z_{w_2}^i\right)$ denote the starting and ending plain coordinates for the i^{th} participant to be hashed, respectively. Through the corresponding length of the binary bits, we can generate temporary random numbers, denoted by $\left(X_{h_1}^i, Y_{w_1}^i\right)$ and $\left(X_{h_2}^i, Y_{w_2}^i\right)$, to further satisfy that $Z_{h_1}^i \in (n, \frac{H}{2}], Z_{h_2}^i \in (\frac{H}{2}, H-n]$ and $Z_{w_1}^i \in [1, W], Z_{w_2}^i \in [1, W]$ using simple shift operations, i.e., $Z_{h_1}^i = X_{h_1}^i + n, Z_{w_1}^i = Y_{w_1}^i$ and $Z_{h_2}^i = H - n - X_{h_2}^i, Z_{w_2}^i = Y_{w_2}^i$. Here, the length of the binary form of $X_{h_1}^i$ and $X_{h_2}^i$ is $\lfloor \log_2(\frac{H}{2} - n) \rfloor$ and that of $Y_{w_1}^i$ and $Y_{w_2}^i$ is $\lfloor \log_2 W \rfloor$.

2. In step 1, the dealer uses his/her secret key, k_{D}, by a random number generator to generate $\left(Z_{h_1}^i, Z_{w_1}^i\right)$ and $\left(Z_{h_2}^i, Z_{w_2}^i\right)$. Therefore, the dealer knows the concentrated positions to be hashed in step 7 and he/she can authenticate the shadow image when receiving each shadow image during the decoding phase. The m-sequence is selected as the random number generator. Some other enhanced random number generators can also be used to obtain better quality randomness.

3. In step 1, the dealer uses each participant's public key to encrypt Z_x^i to obtain cipher $Z_x^{'i}$ and further $bZ_x^{'i}$ and $0bZ_x^{'i}$. Thus, only the participant with his/her private key can decrypt $Z_x^{'i}$ to obtain Z_x^i, i.e., the concentrated positions to be hashed in step 8. Thus, during the shadow image distribution phase, the participant with the private key can authenticate the shadow image when receiving each shadow image.

4. To avoid supplementary bits, we handle value 256 in our scheme as follows. In step 2, we select a prime number $P = 257$ rather than 251 and in steps 5, 7, and 10, we use a screening operation, $\mathrm{SC}_i(h, w) < P - 1$ to achieve a value of

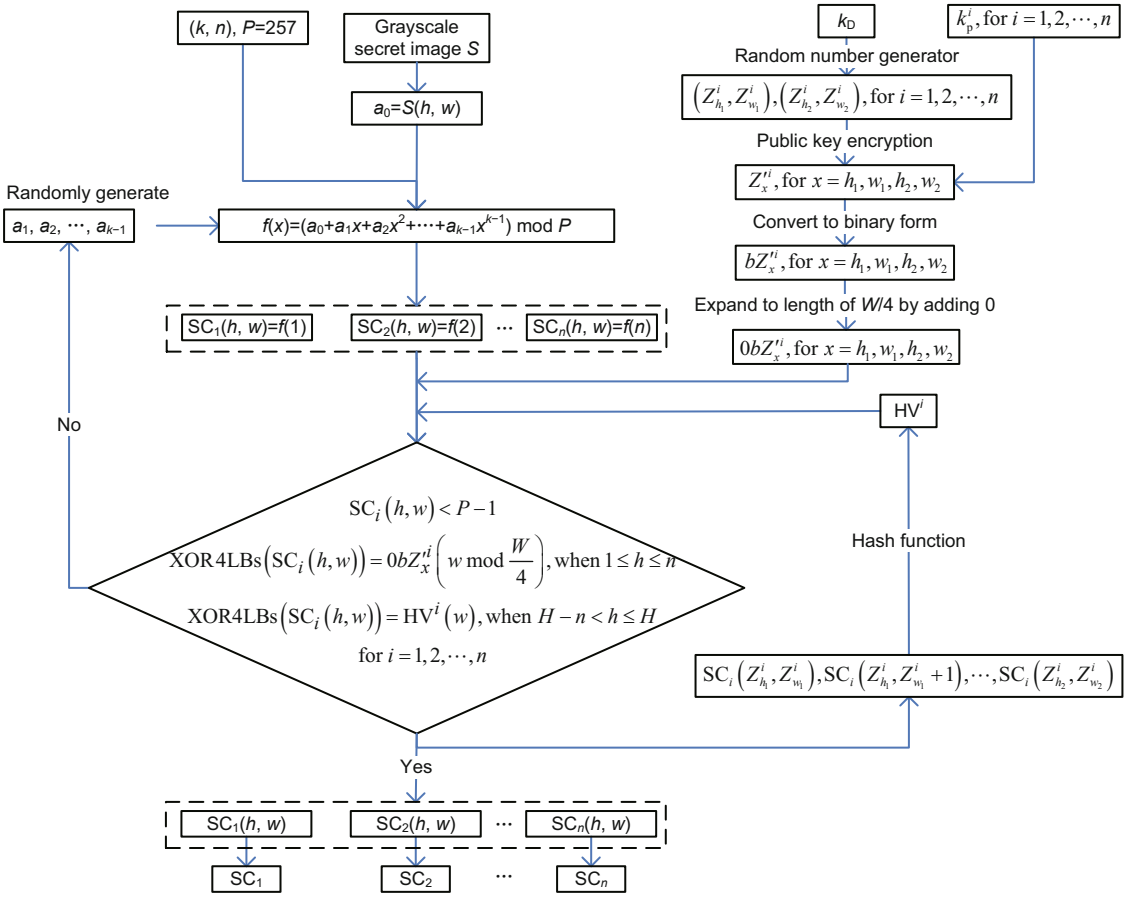

Fig. 6 Design concept of the proposed public key based bidirectional shadow image authentication method

the shadow image pixel ranging from 0 to 255 and lossless decoding. Here, a "screening operation" denotes an operation that will screen the polynomial coefficients to satisfy some requirements.

5. In step 3, our information embedding and processing order for the i^{th} shadow image is further illustrated in Fig. 7.

6. Steps 4, 6, and 9 are used to achieve a (k, n) threshold using the polynomial without pixel expansion.

7. Step 5 embeds $0bZ_x'^i$ into the i^{th} line of the i^{th} shadow image. Step 10 embeds hash code into the last i^{th} line of the i^{th} shadow image. Finally, no pixel expansion occurs. However,

Algorithm 2 Encoding phase of the proposed public key based method

Input: any grayscale secret image S with size of $H \times W$; k_{D}, k_{p}^i, and k_{s}^i, $i = 1, 2, \cdots, n$; threshold parameters (k, n).

Output: shadow images SC_i, $i = 1, 2, \cdots, n$.

Step 1: The dealer uses his/her secret key k_{D} to generate $\left(Z_{h_1}^i, Z_{w_1}^i\right)$ and $\left(Z_{h_2}^i, Z_{w_2}^i\right)$ using a random number generator, for $i = 1, 2, \cdots, n$, where $Z_{h_1}^i \in (n, \frac{H}{2}], Z_{h_2}^i \in (\frac{H}{2}, H-n]$ and $Z_{w_1}^i \in [1, W], Z_{w_2}^i \in [1, W]$. k_{p}^i is used to encode plain Z_x^i to obtain cipher $Z_x'^i$. $Z_x'^i$ is then converted to its binary form, denoted by $bZ_x'^i$, for $x = h_1, w_1, h_2, w_2$ and $i = 1, 2, \cdots, n$. Expand $bZ_x'^i$ by adding 0 at the beginning to obtain $0bZ_x'^i$ with length of $W/4$.

Step 2: $P = 257$ is selected. At each position $(h, w) \in \{(h, w) | 1 \le h \le H, 1 \le w \le W\}$, repeat steps 3–10.

Step 3: If $h \le n$, go to step 4; else if $n < h \le H - n$, go to step 6; else go to step 8.

Step 4: Construct a $(k-1)$-degree polynomial as follows:

$$f(x) = (a_0 + a_1 x + \cdots + a_{k-1} x^{k-1}) \bmod P, \quad (3)$$

where $a_0 = S(h, w)$, and a_i is random, for $i = 1, 2, \cdots, k-1$. Calculate $\text{SC}_i(h, w) = f(i)$, for $i = 1, 2, \cdots, n$.

Step 5: If $\text{SC}_i(h, w) < P-1$ and $\text{XOR4LBs}(\text{SC}_i(h, w)) =$

$$\begin{cases} 0bZ_x'^i\left(w \mod \frac{W}{4}\right), & \text{when } w \bmod \frac{W}{4} \neq 0, \\ 0bZ_x'^i\left(\frac{W}{4}\right), & \text{when } w \bmod \frac{W}{4} = 0, \end{cases}$$

go to the next position (step 2), for $i = 1, 2, \cdots, n$, where $x = h_1$ when $w \le W/4$, $x = w_1$ when $W/4 < w \le W/2$, $x = h_2$ when $W/2 < w \le 3W/4$, and $x = w_2$ when $3W/4 < w \le W$; otherwise, go to step 4.

Step 6: Construct a $(k-1)$-degree polynomial as follows:

$$f(x) = (a_0 + a_1 x + \cdots + a_{k-1} x^{k-1}) \bmod P, \quad (4)$$

where $a_0 = S(h, w)$, and a_i is random, for $i = 1, 2, \cdots, k-1$. Calculate $\text{SC}_i(h, w) = f(i)$, for $i = 1, 2, \cdots, n$.

Step 7: If $\text{SC}_i(h, w) < P - 1$, go to the next position (step 2), for $i = 1, 2, \cdots, n$; otherwise, go to step 6.

Step 8: Concentrate $\text{SC}_i(Z_{h_1}^i, Z_{w_1}^i)$, $\text{SC}_i(Z_{h_1}^i, Z_{w_1}^i + 1), \cdots, \text{SC}_i(Z_{h_2}^i, Z_{w_2}^i)$, and then the concentration result is compressed using a hash function on a digest, denoted by HV^i, for $i = 1, 2, \cdots, n$.

Step 9: Construct a $(k-1)$-degree polynomial as follows:

$$f(x) = (a_0 + a_1 x + \cdots + a_{k-1} x^{k-1}) \bmod P, \quad (5)$$

where $a_0 = S(h, w)$, and a_i is random, for $i = 1, 2, \cdots, k-1$. Calculate $\text{SC}_i(h, w) = f(i)$, for $i = 1, 2, \cdots, n$.

Step 10: If $\text{SC}_i(h, w) < P - 1$ and $\text{XOR4LBs}(\text{SC}_i(h, w)) = \text{HV}^i(w)$, where $i = H - h + 1$, go to the next position (step 2), for $i = 1, 2, \cdots, n$; otherwise, go to step 9.

Step 11: Output n grayscale shadow images $\text{SC}_1, \text{SC}_2, \cdots, \text{SC}_n$.

Algorithm 3 Authentication and decoding in the proposed public key based bidirectional shadow image authentication without pixel expansion

Input: grayscale shadow images $\text{SC}_1, \text{SC}_2, \cdots, \text{SC}_n$; k_{D}, k_{p}^i, and k_{s}^i, $i = 1, 2, \cdots, n$.

Output: decoded grayscale secret image S' with a size of $H \times W$ and authentication result of SC_i, for $i = 1, 2, \cdots, n$.

Step 1: In the shadow image distribution phase, when the i^{th} participant receives SC_i, extract $Z_x'^i$ through the XOR4LBs operation on the i^{th} line of SC_i, for $x = h_1, w_1, h_2, w_2$. Use k_{s}^i to decrypt $Z_x'^i$ to obtain Z_x^i. Concentrate $\text{SC}_i\left(Z_{h_1}^i, Z_{w_1}^i\right)$, $\text{SC}_i\left(Z_{h_1}^i, Z_{w_1}^i + 1\right), \cdots, \text{SC}_i\left(Z_{h_2}^i, Z_{w_2}^i\right)$, and then the concentration result is compressed by the hash function to HV^i. Perform the XOR4LBs operation on the last i^{th} line of SC_i. If the result is equal to HV^i, pass the authentication; otherwise, identify the fake one, denoted by i^*, and broadcast the fake one.

Step 2: In the secret image decoding phase, when the dealer receives SC_i, use his/her secret key k_{D} by the random number generator to generate $\left(Z_{h_1}^i, Z_{w_1}^i\right)$ and $\left(Z_{h_2}^i, Z_{w_2}^i\right)$. Concentrate $\text{SC}_i\left(Z_{h_1}^i, Z_{w_1}^i\right)$, $\text{SC}_i\left(Z_{h_1}^i, Z_{w_1}^i + 1\right), \cdots, \text{SC}_i\left(Z_{h_2}^i, Z_{w_2}^i\right)$, and then the concentration result is compressed by the hash function to HV^i. Perform the XOR4LBs operation on the last i^{th} line of SC_i. If the result is equal to HV^i, pass the authentication, and go to step 3; otherwise, identify the fake one, denoted by i^*, and broadcast the fake one.

Step 3: When collecting any k grayscale shadow images $\text{SC}_{q_1}, \text{SC}_{q_2}, \cdots, \text{SC}_{q_k}$, for each position $(h, w) \in \{(h, w) | 1 \le h \le H, 1 \le w \le W\}$, repeat steps 4 and 5.

Step 4: Solve Eq. (6) by Lagrange interpolation to obtain a_0:

$$\begin{cases} \text{SC}_{q_1}(h, w) = (a_0 + a_1 q_1 + \cdots + a_{k-1} {q_1}^{k-1}) \bmod P, \\ \text{SC}_{q_2}(h, w) = (a_0 + a_1 q_2 + \cdots + a_{k-1} {q_2}^{k-1}) \bmod P, \\ \quad \vdots \\ \text{SC}_{q_{k-1}}(h, w) \\ \quad = (a_0 + a_1 q_{k-1} + \cdots + a_{k-1} {q_{k-1}}^{k-1}) \bmod P, \\ \text{SC}_{q_k}(h, w) = (a_0 + a_1 q_k + \cdots + a_{k-1} {q_k}^{k-1}) \bmod P. \end{cases} \quad (6)$$

Step 5: Compute $S'(h, w) = a_0$.

Step 6: Output the decoded grayscale secret image S' with a size of $H \times W$ and the authentication result of SC_i, for $i = 1, 2, \cdots, n$.

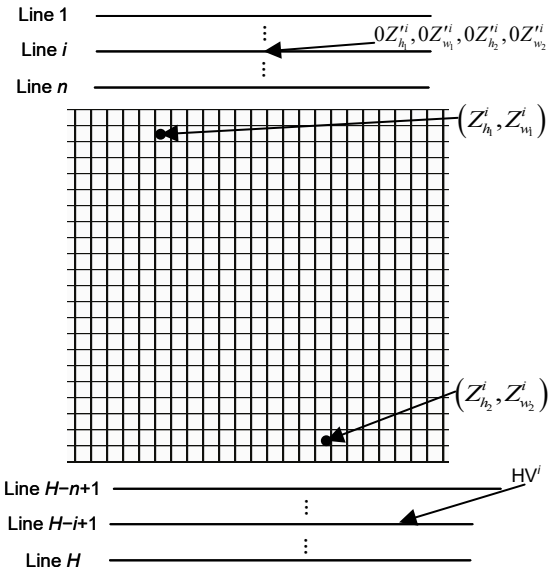

Fig. 7 Information embedding and processing order for the i^{th} shadow image

$0bZ'^{i}_{h_1}, 0bZ'^{i}_{w_1}, 0bZ'^{i}_{h_2}, 0bZ'^{i}_{w_2}$ are inserted only in line i (Fig. 6); HV^i is inserted only in line $H-i+1$. The probability of hash collisions is decided by the adopted hash function; thus, it is not discussed.

8. In steps 5, 7, and 10, we can screen $a_1, a_2, \cdots, a_{k-1}$ to satisfy the embedding and lossless decoding requirements because grayscales $a_1, a_2, \cdots, a_{k-1}$ are random, when $n-k$ is small.

9. Although it is possible to fake the $n-1$ lines of the first and last n lines in each shadow image, the influence on the secret image is minimal.

10. The authentication will not be broken if the attackers or cheaters attempt to modify the higher four bits of each generated shadow image $\text{SC}_i(h,w)$ because the grayscale pixel value (eight bits) is compressed in step 8.

Regarding Algorithm 3, we comment as follows:

1. Step 1 focuses on the authentication in the shadow image distribution phase, step 2 focuses on the authentication before decoding the secret image, and steps 3–5 focus on the secret image decoding during the secret image decoding phase. The dealers and participants are involved in different phases.

2. In step 1, the distributed shadow image is authenticated by the participant in the shadow image distribution phase to check whether the hash code is altered; thus, our method achieves the authentication of each distributed shadow image.

3. In step 2, each collected shadow image is authenticated by the dealer in the secret image decoding phase to check whether the hash code is altered; thus, our method achieves the ability of a separate shadow image authentication.

4. In step 4, at each position (h,w), to obtain $S'(h,w)$ we must construct a polynomial to solve a_0.

5. In this way, our method achieves bidirectional shadow image authentication without pixel expansion.

6. The decoding process is just like Shamir's approach except for the authentication phase.

7. Because the ISS algorithm complexity generally considers time complexity in the decoding phase, we analyze the time complexity of Algorithm 3. The decoding phase contains authentication and decoding. The main authentication operations are XOR and the hash function, and thus the main time complexity is $O(k)$ because the hash function is computed once and XOR is the key factor. The main decoding operation is an interpolation, so the main time complexity is $O(k(\log_2 k)^2)$.

3.2 Security and performance analyses

Here, we give the performance analyses and security proof of the proposed authentication method. Without loss of generality, the collected k grayscale shadow image pixels are denoted by $\text{sc}_{q_1}, \text{sc}_{q_2}, \cdots, \text{sc}_{q_k}$ in the decoding phase. s indicates $S(h,w)$.

Lemma 1 s and sc_i can range from 0 to 255, for $i=1,2,\cdots,n$.

Proof Because $P=257$, s can range from 0 to 255. Because $\text{SC}_i(h,w) < P-1$, sc_i can range from 0 to 255, for $i=1,2,\cdots,n$.

Lemma 2 s is losslessly decoded with sc_{q_1}, sc_{q_2}, $\cdots$, sc_{q_k}.

Proof From Eq. (6) and by Lagrange interpolation, a_0 and a_i are uniquely determined for $i=1,2,\cdots k-1$. According to Lemma 1 and $s=a_0<P$, s is losslessly decoded with $\text{sc}_{q_1}, \text{sc}_{q_2}, \cdots, \text{sc}_{q_k}$.

Theorem 1 Using SC_i and k_{D}, the dealer can authenticate whether SC_i is fake for $i=1,2,\cdots,n$. Using SC_i and k^i_{s}, the i^{th} participant can authenticate whether SC_i is fake.

Proof In step 8 of Algorithm 2, if an attacker intends to guess $\left(Z^i_{h_1}, Z^i_{w_1}\right)$ and $\left(Z^i_{h_2}, Z^i_{w_2}\right)$, i.e., the starting and ending plain coordinates for the i^{th} participant to be hashed, there are $\left(\frac{H}{2}-n\right)^2 \times W^2$ possible coordinates; i.e., the probability of brute-force

guessing the coordinates is $\left[\left(\frac{H}{2}-n\right)^2\times W^2\right]^{-1}$. The security essentially depends on the adopted random number generator, whose result is indistinguishable from a random number. The dealer with k_{D} can generate $\left(Z^i_{h_1},Z^i_{w_1}\right)$ and $\left(Z^i_{h_2},Z^i_{w_2}\right)$, i.e., the starting and ending plain coordinates for the i^{th} participant to be hashed.

However, the result of the XOR4LBs operation on the last i^{th} line of SC_i has 2^W possible values; i.e., the probability of brute-force guessing the hash code is $1/2^W$, whose security depends on the adopted hash function. However, the dealer receiving SC_i can extract the hash code.

In this way, using SC_i and k_{D}, the dealer can authenticate whether SC_i is fake for $i=1,2,\cdots,n$.

Similarly, the i^{th} participant can decrypt bZ'^i_x with his/her private key to obtain $\left(Z^i_{h_1},Z^i_{w_1}\right)$ and $\left(Z^i_{h_2},Z^i_{w_2}\right)$ to authenticate whether SC_i is fake, whose security essentially depends on the adopted public key encryption system.

Therefore, our method achieves public key based bidirectional shadow image authentication without pixel expansion.

Lemma 3 The secret image S cannot be decoded with any $k-1$ or fewer shadow images.

Proof If any $k-1$ equations are constructed in Eq. (6), there are a total of P solutions rather than only one for any $k-1$ equations in Eq. (6). Finally, the secret image S cannot be decoded with any $k-1$ or fewer shadow images.

Note that, although results from Lemma 3 are well known and are the property of a secret-sharing scheme, we provide the proof of their integrity here.

Theorem 2 Our method is a valid ISS for a (k,n) threshold with lossless decoding when $n-k$ is small.

Proof Based on Lemmas 2 and 3, the mentioned conditions for a (k,n) threshold are satisfied.

Because when k is fixed, n increases, more requirements must be satisfied, which is further analyzed as follows. Let N_{R} denote the number of available random values of $a_1,a_2,\cdots,a_{k-1}$ in our method.

For each line of the first or last n lines, $N_{\mathrm{R}}=P^{k-1}\times\left(\frac{256}{P}\right)^n\times\frac{1}{2}$; for the other lines, $N_{\mathrm{R}}=P^{k-1}\times\left(\frac{256}{P}\right)^n$. Thus, the weighted $N_{\mathrm{R}}=\left[P^{k-1}\left(\frac{256}{P}\right)^n\times\frac{1}{2}\times 2n+P^{k-1}\left(\frac{256}{P}\right)^n(H-2n)\right]/H$. There are enough available random values to guarantee searchability.

However, in practice $\frac{n-k}{n}\le\frac{1}{2}$ is suggested to obtain admirable performance.

Note that the inherent information-theoretic property of secret sharing may be compromised as we introduce our method, which is shown in Theorem 2.

Note that there is one possible security risk. If an attacker only modifies the pixels beyond the two random coordinates, it does not cause the decoding stage authentication to fail because the coordinates and the pixel values between the coordinates in the decoding stage are the same as those in the encoding stage; however, the received shadow image has been altered, in which case it is possible to bypass the encoding stage authentication and complete the modification of the shadow image. We call the possible risk the "beyond-coordinates-issue." If the attacker modifies too many pixels, it will be detected. If the attacker modifies fewer pixels, it is possible to bypass the authentication although it has little effect on the image. One possible solution to the risk is to take the coordinates to both ends as much as possible; however, there will be a trade-off problem of brute force guessing. At present, we have not thought of a more suitable solution, so we will continue to study it in the future work.

4 Experimental results and comparisons

In this section, we perform experiments to validate the effectiveness of the proposed public key based bidirectional shadow image authentication method without pixel expansion. Some discussions on our parameters are also provided. Finally, a comparison of illustrations and features with the most related schemes is provided to describe the features of our scheme.

4.1 Experimental settings

In our experiments, all the test images are of the same size, 256×256, because there is no pixel expansion in the proposed ISS. More experiments are required to show that our scheme is suitable for general thresholds and different secret images.

RSA-1024 is used as the public key encryption system, SHA-256 is used as the hash function, and m-sequence is used for the random number generator. Note that other functions can also be applied to our method. $k_{\mathrm{D}}=[1\ 1\ 0\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0]$.

4.2 Image illustration

Fig. 8 presents the results of the proposed (k,n) threshold ISS scheme with bidirectional shadow image authentication without pixel expansion, where k=2, n=2, $k_{\rm s}^1$={36 296 023, 42 414 499}, $k_{\rm s}^2$={6 980 681, 34 960 501}, $k_{\rm p}^1$={7, 42 414 499}, $k_{\rm p}^2$={5, 34 960 501}, and the input grayscale secret image S is displayed in Fig. 8a. Figs. 8b and 8c illustrate the output two shadow images SC_1 and SC_2, respectively. Fig. 8d shows the secret image decoded with the two shadow images by Lagrange interpolation, where the secret image is losslessly decoded; i.e., Fig. 8d is the same as the secret image in Fig. 8a. A randomly generated fake shadow image, denoted by SC_1', is shown in Fig. 8e. Fig. 8f shows the secret image decoded with SC_1' and SC_2 using Lagrange interpolation, which reveals no information on the secret image and thus fails to decode the secret.

We will provide a detailed numerical encoding and authentication process of SC_1. The detailed parameters are given in Table 2.

The result of the XOR4LBs operation on the last $i^{\rm th}$ line of SC_i is equal to HV^i, for $i=1,2$, and thus SC_1 and SC_2 are real images. Finally, the real shadow images, i.e., SC_1 and SC_2, can be authenticated. However, the coordinate extraction of SC_1' fails and thus SC_1' is fake. In the following experiments, we will omit the detailed parameters to save space.

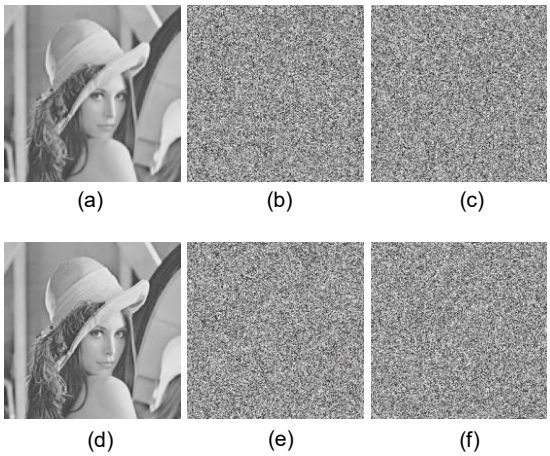

Fig. 8 Experimental results of the proposed (k,n) threshold ISS scheme with bidirectional shadow image authentication without pixel expansion, where $k=2$ and $n=2$: (a) grayscale secret image S; (b–c) two grayscale shadow images SC_1 and SC_2; (d) grayscale secret image S' decoded with SC_1 and SC_2; (e) fake shadow image SC_1'; (f) grayscale secret image S' decoded with SC_1' and SC_2

Fig. 9 presents the results of the proposed (k,n) threshold ISS scheme with bidirectional shadow image authentication without pixel expansion, where k=3, n=4, $k_{\rm s}^1$={5 999 297, 30 045 641}, $k_{\rm s}^2$={10 558 901, 52 880 551}, $k_{\rm s}^3$={24 523 229, 30 704 257}, $k_{\rm s}^4$={37 471 565, 46 915 867}, $k_{\rm p}^1$={5, 30 045 641}, $k_{\rm p}^2$={5, 52 880 551}, $k_{\rm p}^3$={5, 30 704 257}, $k_{\rm p}^4$={5, 46 915 867}, and the input grayscale secret image S is displayed in Fig. 9a. Figs. 9b–9e present the four shadow images. Figs. 9f–9i illustrate the secret images decoded with two or more shadow images using Lagrange interpolation, where almost only the first $t^{\rm th}$ shadow images are used to save space. From Figs. 9f–9i, the secret image decoded with any three or more shadow images is lossless, while no part of the secret image with two or fewer shadow images is recognized. A randomly generated fake shadow image, denoted by SC_1', is illustrated in Fig. 9j. Figs. 9k–9n illustrate the secret images S' decoded with SC_1' and another one or more shadow images using Lagrange interpolation, which reveals no information on the secret image and thus fails to decode the secret.

Based on the above-mentioned experimental results, we conclude the following:

1. Each shadow image has no pixel expansion or cross-interference with the secret image.

2. No secret information is leaked with fewer than k shadow images, demonstrating the security of the proposed ISS.

3. The secret image is losslessly decoded with any k or more shadow images.

4. A separate shadow image is provided to achieve authentication.

5. An ISS scheme with bidirectional shadow image authentication without pixel expansion for a general (k,n) threshold is achieved, where $2\le k\le n$ and $n-k$ is small.

4.3 Parameter analyses

We discuss the values of entropy, encoding time, and $N_{\rm R}$ for k and n because k and n are important in our method, where the entropy of SC_1 is given as follows:

$$H(Y)=-\sum_{y\in Y}\mathrm{Prob}(y)\log_2\mathrm{Prob}(y), \qquad (7)$$

where y means a pixel value, and its statistical probability in an image Y is denoted by $\mathrm{Prob}(y)$.

Here, x indicates that the low x bits of the shadow image is XORed, where in our introduced method $x = 4$. We also state why we set $x = 4$.

The grayscale secret image shown in Fig. 8 is used in our study.

Fig. 10 presents the entropy, encoding time, and N_{R} curves for n when $k = 3$, where we set the theoretical entropy 8, from which we know the following:

1. The entropy is almost the same as n increases and the experimental entropy fits well with the perfect theoretical value. This demonstrates that the shadow image is almost random, that our method is secure, and that our analyses are effective.

2. The encoding time is a monotonically increasing function of n. As n increases, the number of screening operations increases, and thus the encoding time increases.

3. N_{R} is a monotonically decreasing function of n. As n increases, the number of screening requirements increases, and hence the available random values of $a_1, a_2, \cdots, a_{k-1}$ decrease.

Fig. 11 shows the entropy, encoding time, and

Table 2 Some parameters and their values in Fig. 8

Parameter	Value
$\left(Z^1_{h_1}, Z^1_{w_1}\right)$, $\left(Z^1_{h_2}, Z^1_{w_2}\right)$, $\left(Z^2_{h_1}, Z^2_{w_1}\right)$, $\left(Z^2_{h_2}, Z^2_{w_2}\right)$	(3, 1), (248, 1), (8, 1), (247, 49)
$\left(Z'^1_{h_1}, Z'^1_{w_1}\right)$, $\left(Z'^1_{h_2}, Z'^1_{w_2}\right)$, $\left(Z'^2_{h_1}, Z'^2_{w_1}\right)$, $\left(Z'^2_{h_2}, Z'^2_{w_2}\right)$	(2187, 1), (34 067 233, 1), (32 768, 1), (1 931 210, 2 791 241)
$0bZ'^1_{h_1}$	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 1 0 0 0 1 0 1 1
$0bZ'^1_{w_1}$	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1
$0bZ'^1_{h_2}$	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 1 1 1 1 1 0 1 0 0 1 1 0 0 1 0 0 0 0 1
$0bZ'^1_{w_2}$	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1
$0bZ'^2_{h_1}$	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
$0bZ'^2_{w_1}$	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1
$0bZ'^2_{h_2}$	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 0 1 0 1 1 1 0 1 1 1 1 1 0 0 1 0 1 0
$0bZ'^2_{w_2}$	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 1 0 1 0 1 0 0 1 0 1 1 1 0 1 0 0 1 0 0 1
HV^1 of SC_1	0 0 0 0 0 0 1 0 0 0 0 0 1 1 0 0 1 0 1 1 1 1 0 0 0 0 1 1 0 0 0 1 0 1 0 0 0 1 1 0 0 1 0 0 1 1 1 0 0 0 1 0 1 0 0 1 0 1 1 1 0 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 1 1 1 1 0 0 1 0 0 1 1 0 1 1 0 0 1 1 0 1 1 1 0 0 0 0 0 1 0 0 1 0 1 1 1 1 0 0 0 0 0 0 1 0 0 0 0 1 1 0 1 1 0 1 0 0 1 1 0 1 0 1 0 1 1 0 1 1 0 1 0 0 0 0 1 0 0 0 0 1 1 0 0 1 1 0 0 0 0 1 0 0 0 1 0 1 1 1 0 1 1 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 1 1 0 0 0 1 1 0 1 0 1 1 0 0 0 1 1 1 0 0 1 0 0 0 0 1 1 1 0 0 1 1 1 1 1 0 0 1 1 0 0 1 0 0 1 1 1 0 0 1 0 1 0 0 1 0 0 0 0 0 0 1 1
Result of the XOR4LBs operation on the last line of SC_1	0 0 0 0 0 0 1 0 0 0 0 0 1 1 0 0 1 0 1 1 1 1 0 0 0 0 1 1 0 0 0 1 0 1 0 0 0 1 1 0 0 1 0 0 1 1 1 0 0 0 1 0 1 0 0 1 0 1 1 1 0 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 1 1 1 1 0 0 1 0 0 1 1 0 1 1 0 0 1 1 0 1 1 1 0 0 0 0 0 1 0 0 1 0 1 1 1 1 0 0 0 0 0 0 1 0 0 0 0 1 1 0 1 1 0 1 0 0 1 1 0 1 0 1 0 1 1 0 1 1 0 1 0 0 0 0 1 0 0 0 0 1 1 0 0 1 1 0 0 0 0 1 0 0 0 1 0 1 1 1 0 1 1 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 1 1 0 0 0 1 1 0 1 0 1 1 0 0 0 1 1 1 0 0 1 0 0 0 0 1 1 1 0 0 1 1 1 1 1 0 0 1 1 0 0 1 0 0 1 1 1 0 0 1 0 1 0 0 1 0 0 0 0 0 0 1 1
HV^1 of SC'_1	Coordinates are larger than image size, error
Result of the XOR4LBs operation on the last line of SC'_1	1 0 0 0 1 1 0 0 1 1 0 1 0 0 0 0 1 1 1 0 1 0 0 1 0 0 0 1 0 0 0 1 1 0 0 0 1 0 0 1 0 0 1 0 0 0 1 1 0 1 0 1 1 1 1 0 0 0 1 0 1 0 1 0 1 0 0 1 1 1 0 0 0 0 1 0 1 1 1 0 0 1 1 1 1 1 1 1 1 1 0 1 1 1 1 0 0 0 1 0 1 0 0 0 1 0 0 0 0 1 1 1 1 0 0 0 1 1 0 1 0 0 0 1 1 1 0 0 1 0 1 0 1 0 1 0 0 0 0 1 0 0 0 1 0 1 0 0 1 1 1 1 1 0 0 1 1 0 0 0 1 1 1 0 1 0 1 1 0 1 1 1 1 1 1 0 1 1 0 1 0 1 1 1 1 0 1 1 0 1 1 1 0 1 0 1 0 1 0 0 0 0 0 0 0 1 1 0 1 1 0 1 1 1 0 1 0 1 0 0 0 1 1 1 0 1 0 0 1 1 0 1 1 0 1 1 1 0 0 1 0 0 0 1 0 0 1 0 1 0 0 0 0 0 1 0 1

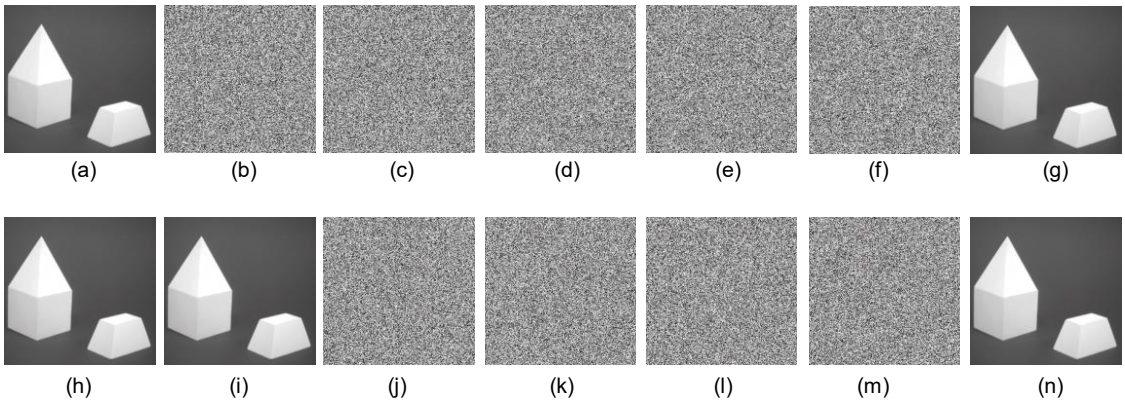

Fig. 9 More experimental results of the proposed (k, n) threshold ISS scheme with bidirectional shadow image authentication without pixel expansion, where $k = 3$ and $n = 4$: (a) grayscale secret image S; (b–e) grayscale shadow images SC_1, SC_2, SC_3, and SC_4; (f–i) grayscale secret image S' decoded with two or more shadow images; (j) fake shadow image SC'_1; (k–n) grayscale secret image S' decoded with SC'_1 and the other one or more shadow images

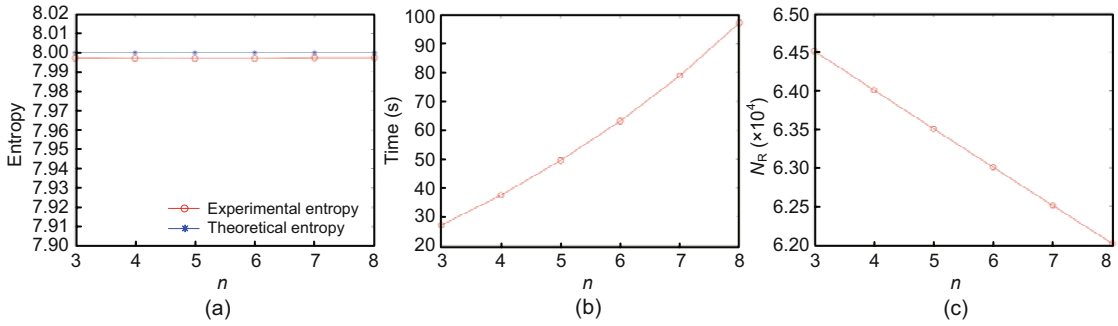

Fig. 10 Entropy (a), encoding time (b), and N_{R} (c) curves for n when $x = 4$, $k = 3$

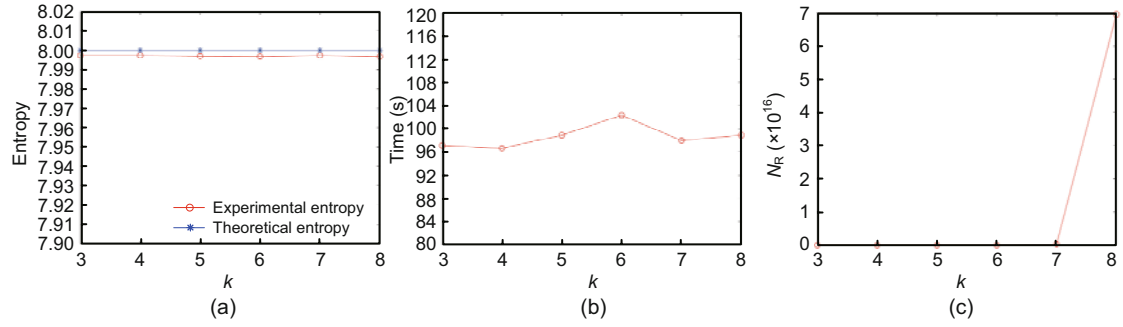

Fig. 11 Entropy (a), encoding time (b), and N_{R} (c) curves for k when $x = 4, n = 8$

N_{R} curves for k when $n = 8$, from which we know the following:

1. The entropy is almost the same as k increases, and the experimental entropy fits well with the perfect theoretical value. This demonstrates that the shadow image is almost random, that our method is secure, and that our analyses are effective.

2. The encoding time has a close value as k increases. There are enough available random values of $a_1, a_2, \cdots, a_{k-1}$, and thus it is easy to screen the available values.

3. N_{R} is a monotonically increasing function of k and increases dramatically when $k \geq 7$. The space of available random values of $a_1, a_2, \cdots, a_{k-1}$ increases, as k increases.

Figs. 12 and 13 show why we set $x = 4$, where

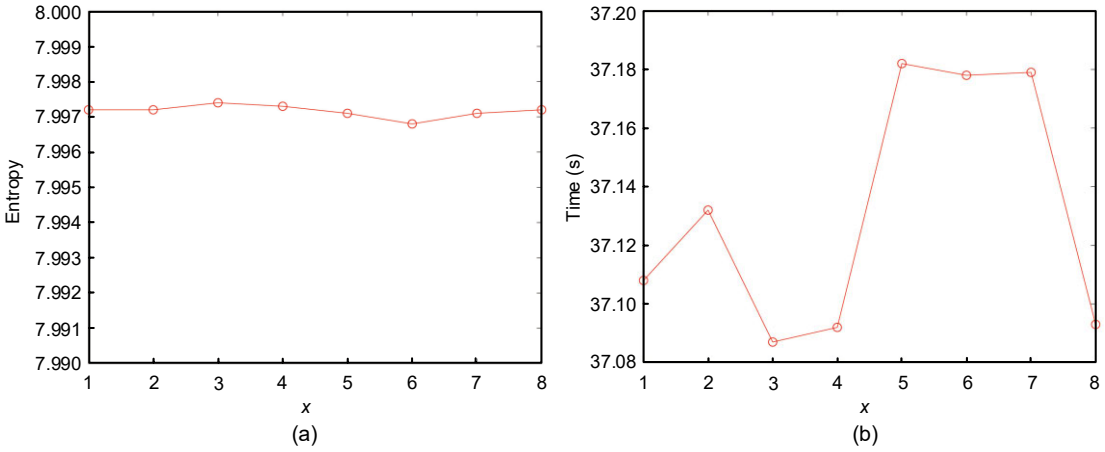

Fig. 12 Entropy (a) and encoding time (b) curves for x when $k=2, n=4, N_{\mathrm{R}}=249$

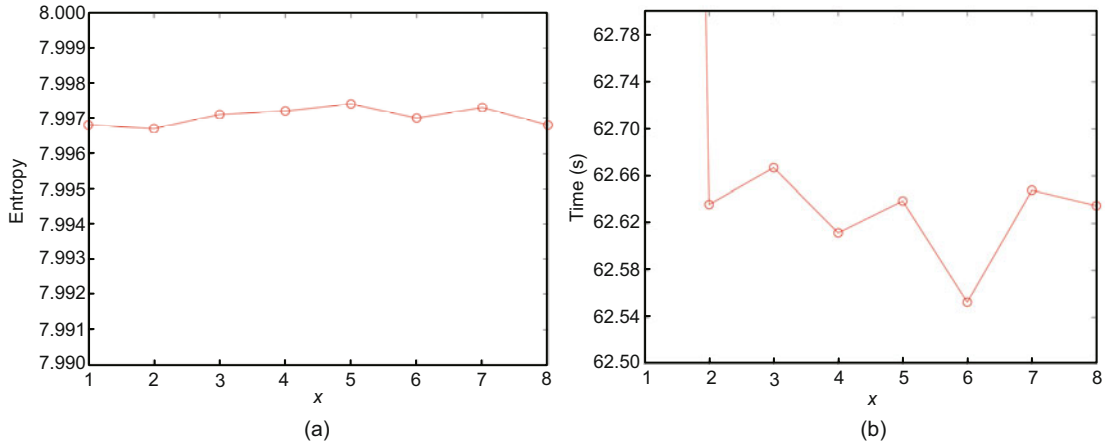

Fig. 13 Entropy (a) and encoding time (b) curves for x when $k=2, n=6, N_{\mathrm{R}}=245$

$k=2$.

1. The values 3, 4, and 5 are the alternative candidates of x because their entropy is larger.

2. Considering the encoding time, $x=4$ represents an acceptable time.

3. In our method, we set $x=4$ to balance security and efficiency.

4.4 Comparison with related schemes

We compare our method with that of Yan et al. (2020a) using experiments and features in which the same secret image as shown in Fig. 9a and the (2, 3) threshold can be used. We choose the scheme of Yan et al. (2020a) for comparison because their scheme has a separate shadow authentication ability for a (k, n) threshold, which is also based on a polynomial.

Fig. 14 displays the results of Yan et al. (2020a), where $k=2$ and $n=3$, and the grayscale secret image S is shown in Fig. 14a. Fig. 14b is a binary authentication image. Figs. 14c–14e illustrate the three shadow images SC_1, SC_2, and SC_3. Fig. 14f is the output additional binary image preserved by the dealer for authentication. Fig. 14g presents the authentication result of SC_1 by the dealer. Fig. 14h presents the secret image decoded with the first two shadow images using Lagrange interpolation. Fig. 14h shows that the decoded secret image with any two or more shadow images is lossless.

Fig. 15 shows the results of our method with the same parameters.

According to Figs. 14 and 15, the schemes of Yan et al. (2020a) and ours are compared as follows:

1. Both our scheme and the scheme of Yan et al. (2020a) have the features of no pixel expansion,

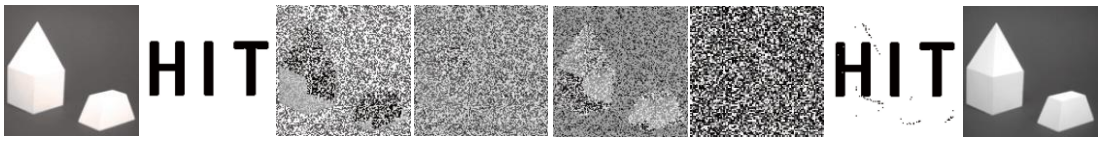

Fig. 14 Experimental results of Yan et al. (2020a), where $k = 2$ and $n = 3$: (a) grayscale secret image S; (b) binary authentication image; (c–e) shadow images SC_1, SC_2, and SC_3; (f) additional binary image preserved by the dealer for authentication; (g) authentication result of SC_1 by the dealer; (h) grayscale secret image S' decoded with SC_1 and SC_2

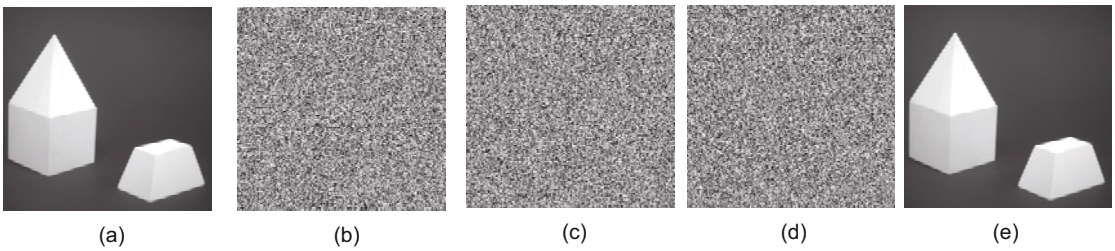

Fig. 15 Our experimental results, where $k = 2$ and $n = 3$: (a) grayscale secret image S; (b–d) shadow images SC_1, SC_2, and SC_3; (e) grayscale secret image S' decoded with SC_1 and SC_2

dealer-participatory separate shadow image authentication ability, (k, n) threshold, lossless decoding, and the use of a polynomial.

2. The scheme of Yan et al. (2020a) can authenticate the shadow image only in the decoding phase, i.e., unidirectional authentication, whereas our method can authenticate the shadow image in both distributing and decoding phases, i.e., bidirectional authentication.

3. The scheme of Yan et al. (2020a) requires an additional image preserved by the dealer to achieve authentication, whereas our method does not.

4. A little information leakage may appear in the shadow image in the scheme of Yan et al. (2020a) because they use only the MSB in their scheme, whereas no information leakage appears in our method because we set $x = 4$ to balance security and efficiency.

5. Only a binarization operation is used to achieve authentication in the scheme of Yan et al. (2020a). Thus, their scheme has lower computational cost than ours.

We compare the proposed method with more related studies (Liu YJ and Chang, 2018; Liu YX et al., 2018b; Jiang et al., 2020; Yan et al., 2020a) in terms of features.

Feature comparisons between the proposed method and related methods are presented in Table 3.

Compared with conventional schemes, the proposed method with bidirectional shadow image authentication without pixel expansion achieves bidirectional separate shadow image authentication, lossless decoding, no pixel expansion, and no auxiliary information, and thus outperforms traditional schemes.

5 Conclusions

The main contribution of this study is the introduction of an image secret sharing (ISS) scheme with bidirectional shadow image authentication with no pixel expansion, lossless decoding, and no auxiliary information. The public key system and hash function were first introduced into the ISS to achieve admirable bidirectional shadow image authentication without pixel expansion or additional information, except for the secret key of the dealer and the public/private keys of participants. Theoretical analyses and experimental examples demonstrated the effectiveness of our method. The proposed ISS can losslessly decode secret images with bidirectional shadow image authentication without pixel expansion. We performed experiments and feature comparisons with related competitive schemes to show the advantages of our method. In the future, we will

Table 3 Feature comparisons with related methods

Feature	Description				
	Liu YJ and Chang (2018)	Liu YX et al. (2018b)	Yan et al. (2020a)	Jiang et al. (2020)	Our method
(k, n) threshold	Yes	Yes	Yes	Yes	Yes
No pixel expansion	No	Yes	Yes	Yes	Yes
Lossless decoding	High quality	High quality	Yes	Yes	Yes
Key idea	Information hiding	Polynomial	ISS	ISS	ISS and hash
Authentication in the distributing phase	No	No	No	No	Yes
Authentication in the decoding phase	Yes	Yes	Yes	Yes	Yes
Authentication ability	Requiring one shadow image	Requiring k shadow images	Requiring one shadow image	Requiring one shadow image	Requiring one shadow image

focus on the use of other ISS principles, public key systems, and hash functions in our method to obtain more admirable features. In addition, we will study the ISS security analysis methods and consider the "beyond-coordinates-issue."

Contributors

Xuehu YAN designed the research. Longlong LI processed the data. Jia CHEN drafted the paper. Lei SUN revised and finalized the paper.

Compliance with ethics guidelines

Xuehu YAN, Longlong LI, Jia CHEN, and Lei SUN declare that they have no conflict of interest.

Data availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

References

Beugnon S, Puteaux P, Puech W, 2019. Privacy protection for social media based on a hierarchical secret image sharing scheme. IEEE Int Conf on Image Processing, p.679-683. https://doi.org/10.1109/ICIP.2019.8803836

Chang CC, Hsieh YP, Lin CH, 2008. Sharing secrets in stego images with authentication. *Patt Recogn*, 41(10):3130-3137. https://doi.org/10.1016/j.patcog.2008.04.006

Chavan PV, Atique M, Malik L, 2014. Signature based authentication using contrast enhanced hierarchical visual cryptography. IEEE Students' Conf on Electrical, Electronics and Computer Science, p.1-5. https://doi.org/10.1109/SCEECS.2014.6804453

Cheng YQ, Fu ZX, Yu B, 2018. Improved visual secret sharing scheme for QR code applications. *IEEE Trans Inform Forens Secur*, 13(9):2393-2403. https://doi.org/10.1109/TIFS.2018.2819125

Du L, Chen Z, Ho ATS, 2020. Binary multi-view perceptual hashing for image authentication. *Multim Tools Appl*, 80(2):22927-22949. https://doi.org/10.1007/s11042-020-08736-6

El-Latif AAA, Abd-El-Atty B, Hossain MS, et al., 2018. Efficient quantum information hiding for remote medical image sharing. *IEEE Access*, 6:21075-21083. https://doi.org/10.1109/ACCESS.2018.2820603

Fukumitsu M, Hasegawa S, Iwazaki JY, et al., 2017. A proposal of a secure P2P-type storage scheme by using the secret sharing and the blockchain. Proc IEEE 31st Int Conf on Advanced Information Networking and Applications, p.803-810. https://doi.org/10.1109/AINA.2017.11

Harn L, Hsu CF, Xia Z, 2022. A novel threshold changeable secret sharing scheme. *Front Comput Sci*, 16(1):161807. https://doi.org/10.1007/s11704-020-0300-x

Jiang Y, Yan XH, Qi JQ, et al., 2020. Secret image sharing with dealer-participatory and non-dealer-participatory mutual shadow authentication capabilities. *Mathematics*, 8(2):234. https://doi.org/10.3390/math8020234

Komargodski I, Naor M, Yogev E, 2017. Secret-sharing for NP. *J Cryptol*, 30(2):444-469. https://doi.org/10.1007/s00145-015-9226-0

Li P, Ma PJ, Su XH, 2010. Image secret sharing and hiding with authentication. Proc 1st Int Conf on Pervasive Computing, Signal Processing and Applications, p.367-370. https://doi.org/10.1109/PCSPA.2010.95

Li YN, Guo LL, 2018. Robust image fingerprinting via distortion-resistant sparse coding. *IEEE Signal Process Lett*, 25(1):140-144. https://doi.org/10.1109/LSP.2017.2777881

Liao X, Yin JJ, Chen ML, et al., 2022. Adaptive payload distribution in multiple images steganography based on image texture features. *IEEE Trans Depend Sec Comput*, 19(2):897-911. https://doi.org/10.1109/TDSC.2020.3004708

Lin CC, Tsai WH, 2004. Secret image sharing with steganography and authentication. *J Syst Softw*, 73(3):405-414. https://doi.org/10.1016/S0164-1212(03)00239-5

Liu YJ, Chang CC, 2018. A turtle shell-based visual secret sharing scheme with reversibility and authentication. *Multim Tools Appl*, 77(19):25295-25310. https://doi.org/10.1007/s11042-018-5785-z

Liu YX, Yang C, 2017. Scalable secret image sharing scheme with essential shadows. *Signal Process Image Commun*, 58:49-55. https://doi.org/10.1016/j.image.2017.06.011

Liu YX, Yang C, Wang YC, et al., 2018a. Cheating identifiable secret sharing scheme using symmetric bivariate polynomial. *Inform Sci*, 453:21-29. https://doi.org/10.1016/j.ins.2018.04.043

Liu YX, Sun QD, Yang CN, 2018b. (k, n) secret image sharing scheme capable of cheating detection. *EURASIP J Wirel Commun Netw*, 2018(1):72. https://doi.org/10.1186/s13638-018-1084-7

Liu YX, Yang CN, Wu CM, et al., 2019. Threshold changeable secret image sharing scheme based on interpolation polynomial. *Multim Tools Appl*, 78(13):18653-18667. https://doi.org/10.1007/s11042-019-7205-4

Meng KJ, Miao FY, Ning Y, et al., 2021. A proactive secret sharing scheme based on Chinese remainder theorem. *Front Comput Sci*, 15(2):152801. https://doi.org/10.1007/s11704-019-9123-z

Pilaram H, Eghlidos T, 2017. An efficient lattice based multi-stage secret sharing scheme. *IEEE Trans Depend Sec Comput*, 14(1):2-8. https://doi.org/10.1109/TDSC.2015.2432800

Shamir A, 1979. How to share a secret. *Commun ACM*, 22(11):612-613. https://doi.org/10.1145/359168.359176

Shen G, Liu F, Fu ZX, et al., 2017. Perfect contrast XOR-based visual cryptography schemes via linear algebra. *Des Codes Cryptogr*, 85(1):15-37. https://doi.org/10.1007/s10623-016-0285-5

Shen J, Zhou TQ, He DB, et al., 2019. Block design-based key agreement for group data sharing in cloud computing. *IEEE Trans Depend Sec Comput*, 16(6):996-1010. https://doi.org/10.1109/TDSC.2017.2725953

Shivani S, Agarwal S, 2018. VPVC: verifiable progressive visual cryptography. *Patt Anal Appl*, 21(1):139-166. https://doi.org/10.1007/s10044-016-0571-x

Thien CC, Lin JC, 2002. Secret image sharing. *Comput Graph*, 26(5):765-770. https://doi.org/10.1016/S0097-8493(02)00131-0

Ulutas G, Ulutas M, Nabiyev VV, 2013. Secret image sharing scheme with adaptive authentication strength. *Patt Recogn Lett*, 34(3):283-291. https://doi.org/10.1016/j.patrec.2012.10.017

Wang GY, Liu F, Yan WQ, 2016. Basic visual cryptography using braille. *Int J Dig Crime Forens*, 8(3):6. https://doi.org/10.4018/IJDCF.2016070106

Wang W, Liu F, Guo T, et al., 2017. Temporal integration based visual cryptography scheme and its application. Proc 16$^{\text{th}}$ Int Workshop Digital Forensics and Watermarking, p.406-419. https://doi.org/10.1007/978-3-319-64185-0_30

Yan XH, Lu YL, Liu LT, et al., 2017. Exploiting the homomorphic property of visual cryptography. *Int J Dig Crime Forens*, 9(2):5. https://doi.org/10.4018/IJDCF.2017040105

Yan XH, Lu YL, Liu LT, et al., 2018. Chinese remainder theorem-based two-in-one image secret sharing with three decoding options. *Dig Signal Process*, 82:80-90. https://doi.org/10.1016/j.dsp.2018.07.015

Yan XH, Gong QH, Li LL, et al., 2020a. Secret image sharing with separate shadow authentication ability. *Signal Process Image Commun*, 82:115721. https://doi.org/10.1016/j.image.2019.115721

Yan XH, Lu YL, Liu LT, et al., 2020b. Reversible image secret sharing. *IEEE Trans Inform Forens Secur*, 15:3848-3858. https://doi.org/10.1109/TIFS.2020.3001735

Yan XH, Liu LT, Li LL, et al., 2021. Robust secret image sharing resistant to noise in shares. *ACM Trans Multim Comput Commun Appl*, 17(1):24. https://doi.org/10.1145/3419750