Research Article

Efficient Secret Image Sharing Scheme with Authentication and Cheating Prevention

Lina Zhang,1,2 Xuan Dang,1 Li Feng,3 and Junhan Yang,1,2

1College of Computer Science and Technology, Xi’an University of Science and Technology, Xi’an 710054, China
2School of Computer Science, Shaanxi Normal University, Xi’an 710119, China
3College of Energy Engineering, Xi’an University of Science and Technology, Xi’an 710054, China

Correspondence should be addressed to Lina Zhang; zhangln@xust.edu.cn

Received 23 April 2021; Revised 28 July 2021; Accepted 12 August 2021; Published 23 August 2021

1. Introduction

With the development of computer science and technology, online transactions developed rapidly and improved our daily life. People are increasingly conducting business activities online, and the development prospects of online transactions are very broad [1]. Information security is an important and effective mechanism on the Internet. Information security in transactions has attracted more attention. Some works [2, 3] are all discussing the security of online transactions.

Secret sharing is a very important branch in the field of modern cryptography. It provides new ideas for solving the key management of information security. It plays a crucial role in the safe preservation and transmission of secret data. Secret sharing uses an algorithm to divide the secret that needs to be hidden into several shares or subkeys. The shadow image itself is meaningless. However, when the shares reach the threshold $k$, the secret can be restored through a certain reconstruction algorithm. On the contrary, if the number of shadows is less than the threshold $k$, the secret cannot be reconstructed. SIS is an extension of secret sharing technology. When using this technology to share images, the integrity and security of the images can be guaranteed.

In practical applications, shadow identity authentication is necessary. The scheme without authentication may have the following deceptions: (1) the dealer cheated. Before the original secret image is restored, the shares of the secret share cannot confirm whether the shadow image they hold can be restored to the original image. Actually, it is assumed that the dealer is trusted. (2) The deception of the secret-sharing members. When a member deliberately sabotages or provides a fake shadow image, other participants will not only be unable to detect it but also regard the wrong secret information as correct. Using this technology to share images can ensure the integrity and security of the images.
Currently, there are a variety of SIS schemes. However, they cannot meet the requirements of the users in terms of the quality of reconstructed images, the amount of data in the process of secret distribution, and the security during Internet transmission. Shamir was the first to propose the \((k, n)\)-threshold secret sharing scheme [4], where \(n\) shadow images are generated and distributed to \(n\) participants. When there are \(k\) shadows or more other shadows, the original secret image can be reconstructed or restored through Lagrange interpolation. Less than \(k\) shadows reveal no image information. To obtain better performance, an increasing number of researchers design several polynomial-based SIS schemes [5–7] based on the approach in [4]. In the Thien-Lin \((k, n)\) secret image sharing scheme [5], the author proposes lossy restoration and lossless restoration. Because the gray value of a pixel is between 0 and 255, and 251 is the greatest prime number not larger than 255. In order to apply this scheme, the gray values of the original secret image should be pretreated. Namely, we change all the gray values 251–255 of the original secret image to 250 so that all gray values are in the range 0–250. The work in [7–10] used this lossy processing method. The authors of [10] analyzed the PSNR value between the original secret image and the restored image. This lossy method does not cause visual errors. In lossless restoration, if the pixel value \(a < 250\), it is directly processed as a pixel value; otherwise, the pixel value \(a\) is divided into 250 and \(a - 250\). This lossless method is described in detail in [5]. The processes will slightly increase the size of the shadow image.

There are two types of SIS: one is Visual Cryptography (VC) and the other is polynomial-based SIS. The former is directly performed by the human visual system. Some previous studies [11–13] attempt to improve the visual quality and reduce pixel expansion. In addition, some deception problems caused by false shadows with noise have been taken seriously [14, 15]. However, these schemes do not make authentic the shadow image before recovering the secret image, which is very insecure. Progressive VC [16] and multilevel VC [17] can gradually obtain the original secret image through stacking. If the shadow image is not authenticated, the adversary can obtain the relevant secret information through the superposition of less than \(k\) shadow images in the front and submit a fake shadow to reconstruct the secret image.

The polynomial-based SIS schemes have threshold properties. According to the three modes of multisecret mode, priority mode and progressive mode, a polynomial-based \((2, n)\)-threshold scalable SIS scheme is constructed [18]. Some studies [19–21] extend \((2, n)\)-threshold to the general \((k, n)\)-threshold scheme based on the approach [18], which is suitable for faster transmission in image distributed systems. Progressive Secret Image Sharing (PSIS) is suitable for multilevel services, which gives different participants different priorities. Nevertheless, the authentication of the shadow image is not considered so that the adversary can tamper or forge shares to participate in the reconstruction of the secret image and steal the secret information. They are applied in the image distribution system due to the threshold characteristics and scalability of the \((k, n)\)-threshold. Besides, the failure of \(n-k\) shadow images in the transmission process will only lose the resolution of the image and will not affect the image reconstruction phase. The work in [22] proposes a novel \((k, k^2)\) progressive secret image sharing based on modular operations. This method can divide important images stored in the Internet of Things into many parts and then pass them to people in different places. This scheme has fine-grained gradual progress but has certain limitations in threshold setting.

In the previous SIS schemes, the threshold \(k\) is determined by the dealer based on the security level. References [7, 9] propose a threshold changeable SIS scheme; each participant only needs to keep one initial shadow. When reconstructing the image, the dealer decides the threshold according to security level. If the threshold is unchanged, any \(k\) or more initial shadows can recover the image; else, if the threshold is increased or decreased, the dealer publishes additional information, each participant updates their shadows such that the threshold of updated shadows is changed corresponding. However, this threshold changeable SIS scheme does not consider the authentication of shadow images. If falsified sharing is involved when recovering the secret image, the wrong secret information will be recovered.

An increasing number of researchers have proposed SIS schemes with authentication recently. Its purpose is to prevent cheaters from getting real secrets. Many works were proposed to prevent the cheating problem in secret sharing schemes. These schemes can be divided into two categories, cheating detection schemes [8, 10, 23–25] and cheating identification schemes [26, 27]. In the image restoration phase, we need to perform share authentication on the shadow image. A trusted third party calculates the \(k\) shadow images used to restore the image block by block, and the calculated value is compared with the authentication code. If they are equal, the authentication is passed and the original image is restored. Otherwise, there is a fake shadow image.

The trusted third party stops recovering. The study in [26] proposes an independent shadow authentication scheme based on SIS, which applies visual secret sharing to polynomial-based SIS. In the sharing phase, the users input a binary authentication image and a shared secret image to the dealer. In the restoration phase, participants use stacking or XOR operations for identity authentication by sending the lowest plane of the shadow. The work in [27] proposes two mutual shadow authentication functions with dealer participation and nondealer participation. All participants and dealers can mutually authenticate other participants. Both of these methods have low complexity, and there is no need to separately consider shadow authentication capabilities.

In cheating detection schemes, honest users can detect the cheating behaviour but cannot identify cheaters. The work in [10] is based on the Thien-Lin scheme and the intractability of the discrete logarithm. It can identify the cheaters no matter if the original secret image holder or the participants. No security channel exists between the holder and the participants. Reference [23] demonstrates that Shamir scheme is not secure against cheating. The work in [24] is based on [23], which makes relevant theoretical derivations for secret sharing schemes to prevent such
attacks. Reference [25] discusses the significance of detecting cheating in linear secret sharing schemes and constructs a new \((k, n)\) linear secret sharing scheme with the capability of cheating detection. In the phase of cheating detection, only one honest player can detect the cheating from other cheating detection. In the phase of cheating detection, only cheating in linear secret sharing schemes and constructs a Mathematical Problems in Engineering 3 manpower, and material resources.

If there is no reliable third-party identity authentication, all users through deception in online transactions, it is not safe.验证 before the transaction, malicious attacks such as adversary without a share can obtain the share of other normal usersthrough deception in online transactions, it is not safe. If there is no reliable third-party identity authentication, all shares can be sent to each other, and the adversary may obtain secret information through forgery and tampering. On the other hand, when the amount of image restoration is huge, if the detection is not performed first, it will cost time, manpower, and material resources.

1.1. Our Contribution. In this paper, the shadow authentication of the image sharing is taken into account in the image restoration phase. Our contributions are as follows:

(1) Based on the knowledge of cryptography, we propose two SIS schemes that can cheating prevention. Scheme I processes \(k - 2\) pixel values at a time and constructs two authentication codes. This scheme uses XOR operation, so it is suitable for Internet chips or some resource-constrained, embedded devices.

(2) The scheme II has a further improvement in security. It uses related cryptographic algorithms to construct an authentication code through a hash algorithm. Despite its high storage and efficiency, it is suitable for environments and devices with larger storage space and higher security levels. The shadow size of this scheme is similar to that of Thien-Lin’s scheme.

(3) In the authentication process of the shadow images, all pixels of the secret image participate in the authentication. It is obvious that it can prevent the shadow images from being tampered with and greatly improve security.

1.2. Organization. The rest of the paper is organized as follows: in Section 2, we focus on some preliminary knowledge related to the proposed schemes; in Section 3, we propose two SIS schemes for detecting deception and analyze their performance; in Section 4, experimental results and security analysis are used to show the performance of proposed scheme and comparisons of shadow size; the conclusion part is in Section 5.

2. Preliminaries

The idea of secret sharing was first proposed by Shamir [4]. The main idea is to divide data \(S\) into shares in such a way that it is easily reconstructed from any \(k\) shares, and complete knowledge of \(k - 1\) shares reveals absolutely no information about \(S\). In [4], a Lagrange interpolation polynomial needs to be constructed. Then, let the secret data \(S\) be a constant term of the polynomial. From the polynomial, \(n\) values can be calculated as \(n\) shares, where any \(k\) shares can recover \(S\). Later, this idea was followed by many research scholars, such as these schemes [5, 28–30]. The approach in [5] proposes a SIS scheme based on Shamir’s threshold secret sharing method. The difference between [5] and [4] is that Thien-Lin group image pixels, each group of pixels, are used as polynomial coefficients. At present, many works [8, 31] including our proposed scheme, are based on Thien-Lin’s scheme. Next, we introduce the whole process of the two classic schemes and discuss the schemes.

2.1. Polynomial-Based SIS. In [5], Thien-Lin proposed \((k, n)\)-SIS scheme based on interpolated polynomial. This scheme consists of two phases: the Shadow generation phase and the image restoration phase. In the shadow generation phase, a dealer takes a secret image \(I\) as input and invokes an algorithm to output \(n\) shadows. During the image restoration phase, a set of \(m\) shadows \(k \leq m \leq n\) is capable of recover the secret image \(I\).

2.1.1. Shadow Generation Phase. Input a secret image \(I\), output \(n\) shadow image \(S_1, S_2, \ldots, S_n\).

Step 1: the dealer divides the secret image \(I\) into nonoverlapping \(t\) pixel blocks \(P_1, P_2, \ldots, P_t\). Each pixel block contains \(k\) pixel values.

Step 2: the pixel values in each pixel block \(P_i, \ i \in [1, t]\) are \(a_{i,0}, a_{i,1}, \ldots, a_{i,k-1}\).

Step 3: construct a \(k - 1\) degree polynomial \(f_i(x) = a_{i,0} + a_{i,1}x + \cdots + a_{i,k-1}x^{k-1}\).

Step 4: for each pixel block \(P_i, \ i \in [1, t]\), use the formula in step 3 to calculate the subshadow \(O_{i,j}\), \(j \in [1, n]\), and distribute it to different participants—the final shadow \(S_j = O_{i,j}, j \in [1, n]\).

2.1.2. Image Restoration Phase. Input \(k\) shadow images and output the original secret image \(I\).

Step 1: select \(k\) shadows \(S_1, S_2, \ldots, S_k\) from \(S_j, j \in [1, n]\)
2.2.2. Image Restoration Phase. Input a secret image $I$, output $n$ shadow images $S_1, S_2, \ldots, S_n$.

Step 1: the dealer divides the secret image $I$ into $t$ nonoverlapping pixel blocks $P_1, P_2, \ldots, P_t$. Each pixel block contains $2k - 2$ pixel values.

Step 2: XOR operation in equation (1) is used to calculate the shadow image $S_i = P_i \oplus P_{i+1} \oplus \cdots \oplus P_t$, $i \in [1, t]$, where all pixel values participate in the authentication. We proposetwo new schemes based on that, where all pixel values participate in the authentication.

Step 3: if there is an integer $r_i$ that satisfies

$$r_i \cdot a_{i,0} + b_{i,0} = 0 \pmod{251}$$

then the pixel block $P_i = \{a_{i,0}, a_{i,1}, \ldots, a_{i,k-1}, b_{i,0}, b_{i,1}, \ldots, b_{i,k-1}\}$ can be restored. Finally, the original secret image $I = P_1 \parallel P_2 \parallel \cdots \parallel P_t$ can be further restored. Otherwise, it can be concluded that there exist false shadows participating in the image restoration.

It can be observed from this scheme that the authentication for detecting fraud must be performed before the restoration phase. If a false shadow is detected, the restoration of the original secret image should be stopped. The shadow size in this scheme is $1/(k - 1)$ of that of the original image.

3. The Proposed Scheme

SIS technology has matured and increasing researchers are beginning to pay attention to the security of the sharing phase, which is the shadow authentication in the image restoration phase. The approach in [8] is to share the secret image by constructing two polynomials. This method increases the storage space. In the restoration phase, only the first two pixels participate in the authentication. We propose two new schemes based on that, where all pixel values participate in the authentication. Besides, only one polynomial is used to calculate the shadow image, which reduces the storage space. SchemeI is a completely lightweight and fast calculation. SchemeI uses a cryptographic hash algorithm, although it is slightly lower in efficiency but has a higher level of security. Compared with schemeI, schemeII has a further improvement in security. SchemeII uses related cryptographic algorithms to construct an authentication code for authentication through a hash algorithm. Although it is slightly higher in storage and efficiency, it is suitable for environments and equipment with larger storage space and a higher level of security.

3.1. The Proposed Scheme I.

Since shemeonly uses the XOR operation, it is a lightweight and fast operation scheme. ShemeI takes $k - 2$ pixel values as a block and calculates two authentication codes for each block, thereby constructing a $k - 1$ degree polynomial to calculate the shadow image. When the image is restored, by judging whether it conforms to the formula of the exclusive OR operation to obtain the authentication code, it is further detected whether there is a false shadow. If the authentication is successful, the original secret image can be recovered. Else, there are fake shadows participating in image reconstruction; the cheating prevented.

3.1.1. Shadow Generation Phase. Input a secret image $I$, output $n$ shadow images $S_1, S_2, \ldots, S_n$.

Step 1: the dealer divides the secret image $I$ into $t$ nonoverlapping pixel blocks $P_1, P_2, \ldots, P_t$. Each pixel block contains $k - 2$ pixel values.

Step 2: the pixel values in each pixel block $P_i$, $i \in [1, t]$ are $a_{i,0}, a_{i,1}, \ldots, a_{i,k-1}$ and $b_{i,0}, b_{i,1}, \ldots, b_{i,k-1}$. Then, we construct a $k - 1$ degree polynomial $f_i(x) = a_{i,0} + a_{i,1}x + \cdots + a_{i,k-1}x^{k-1} \pmod{251}$.

Step 3: for each pixel block $P_i$, $i \in [1, t]$, we calculate the subshadow $O_{i,j} = [f_i(j), g_i(j)]$ using two polynomials and distribute the final shadow $S_j = O_{1,j} \parallel O_{2,j} \parallel \cdots \parallel O_{t,j}$, $j \in [1, n]$ to different participants.
\[
\begin{align*}
\{ b_{i,0} &= a_{i,0} \oplus a_{i,1} \cdots a_{i,k-4} \pmod{251}, \\
\{ b_{i,1} &= a_{i,1} \oplus a_{i,2} \cdots a_{i,k-3} \pmod{251}. 
\end{align*}
\] (1)

Step 4: for each pixel block \( P_i \), \( i \in [1, t] \), we calculate the subshadow \( O_{i,j} = f_i(j) \) and distribute it to different participants. The final shadow \( S_j = O_{i,j} \| O_{i,j} \cdots \| S_{i,j}, j \in [1, n] \).

3.1.2. Image Restoration Phase. Input \( k \) shadow images and output the original secret image I.

Step 1: select \( k \) shadows \( S_1, S_2, \cdots, S_k \) from \( S_j, j \in [1, n] \).
Step 2: use the Lagrange interpolation formula to calculate the secret pixel values \( a_{i,0}^{t}, a_{i,1}^{t}, \cdots, a_{i,k-2}^{t} \) and \( b_{i,0}^t, b_{i,1}^t \).
Step 3: detect whether there exist fake shadows. If these values \( a_{i,0}^{t}, a_{i,1}^{t}, \cdots, a_{i,k-2}^{t} \) and \( b_{i,0}^t, b_{i,1}^t \), satisfy equation (2), the pixel block \( P_i = \{ a_{i,0}^{t}, a_{i,1}^{t}, \cdots, a_{i,k-3}^{t} \} \) can be restored. Finally, the original secret image \( I' = P_1^t \| P_2^t \cdots \| P_t^t \) can be further restored.

\[
\begin{align*}
\{ a_{i,0}^{t} \oplus a_{i,1}^{t} \cdots a_{i,k-4}^{t} \pmod{251} &= b_{i,0}^t, \\
a_{i,1}^{t} \oplus a_{i,2}^{t} \cdots a_{i,k-3}^{t} \pmod{251} &= b_{i,1}^t. 
\end{align*}
\] (2)

Else, it can be detected that fake shadows participate in the reconstruction of the secret image. Thus, the cheating was prevented.

Scheme only uses very lightweight operations and is suitable for Internet chips or embedded devices with limited resources. For scheme, we have the following instructions:

(a) Our scheme processes \( k - 2 \) pixel values at a time.
   The first \( k - 3 \) pixel values and the last \( k - 3 \) pixel values are used to construct two secret authentication codes \( b_{i,1}^t, b_{i,2}^t \) participating in the authentication of the shadow image.
(b) In this scheme, the threshold should satisfy \( k - 3 \geq 4 \), namely \( k \geq 4 \).
(c) The shadow size is \( 1/(k - 2) \) of that of the original image.

The polynomial constructed in scheme 1 processes \( k - 2 \) secret pixel values at a time, and the size of the shadow image is \( 1/(k - 2) \) of the original secret image. The authentication code is generated by XOR the first \( k - 3 \) and the last \( k - 3 \) secret pixel values for authentication. Obviously, \( k - 3 \geq 4 \), which means \( k \geq 4 \). This scheme selects two authentication codes, and the number of polynomial coefficients is \( k \), which is limited. More locations must be used to store secret pixel values. If a larger number of authentication codes are selected, the number of secret pixel values processed each time will be reduced, which will cause the shadow image to become larger. In addition, without knowing any secret information, the probability of an adversary guessing one authentication code is \( 1/2^k \), and the probability of guessing both authentication codes is \( 1/2^{10} \).

3.2. The Proposed Scheme II. Scheme I takes \( k - 1 \) pixel values as a block and uses a cryptographic hash algorithm to generate an authentication code. In the image restoration phase, it is determined whether the authentication codes are equal. If the authentication is successful, the original secret image can be restored. Else, there are fake shadows participating in image reconstruction; the cheating was prevented. Although this scheme is slightly less efficient, it has higher security.

3.2.1. Shadow Generation Phase. Input a secret image I, output \( n \) shadow image \( S_1, S_2, \ldots, S_n \).
Step 1: the dealer divides the secret image I into \( t \) nonoverlapping pixel blocks \( P_1, P_2, \ldots, P_t \). Each pixel block contains \( k - 1 \) pixel values.
Step 2: the pixel values \( a_{i,j}^{t}, a_{i,1}^{t}, \ldots, a_{i,k-2}^{t} \) in each pixel block \( P_i, i \in [1, t] \) constitute a message sequence \( M_i \) in the following equation:
\[
M_i = a_{i,0}^{t} \| a_{i,1}^{t} \cdots \| a_{i,k-2}^{t}
\] (3)
Step 3: the generation of the authentication code. For each message sequence \( M_i \), we use a hash function to generate a message digest with a fixed bit length. In this scheme, we use the MD5 algorithm. For the 128-bit hash value generated by the MD5 algorithm, perform a bit-by-bit XOR on every 16 bit to obtain a value of 1 bit. There is a total of 8-bit value \( b_i \) as the authentication code.
Step 4: construct a \( k - 1 \) degree polynomial \( f_i(x) = a_{i,0} + a_{i,1}x + \cdots + a_{i,k-2}x^{k-2} + b_i x^{k-1} \pmod{251})
Step 5: for each pixel block \( P_i, i \in [1, t] \), we calculate the subshadow \( O_{i,j} = f_i(j) \) and distribute it to different participants—the final shadow \( S_j = O_{i,j} \| O_{i,j} \cdots \| S_{i,j}, j \in [1, n] \).

3.2.2. Image Restoration Phase. Input \( k \) shadow images and output the original secret image I.
Step 1: select \( k \) shadows \( S'_1, S'_2, \ldots, S'_k \) from \( S_j, j \in [1, n] \).
Step 2: calculate the multireality coefficients \( a_{i,0}^{t}, a_{i,1}^{t}, \cdots, a_{i,k-2}^{t} \) and \( b_i^t \) through the Lagrange interpolation polynomial.
Step 3: use step 2 and step 3 in the shadow generation phase to calculate and generate the authentication code \( b_i^t \) for \( a_{i,0}^{t}, a_{i,1}^{t}, \cdots, a_{i,k-2}^{t} \).
Step 4: detect whether there exist fake shadows. If \( b_i^t = b_i^t \), the pixel block \( P_i = \{ a_{i,0}^{t}, a_{i,1}^{t}, \cdots, a_{i,k-3}^{t} \} \) can be restored, and the original secret image \( I' = P_1^t \| P_2^t \cdots \| P_t^t \) can be further restored. Else, it can be detected that fake shadows participate in the reconstruction of the secret image. Thus, the cheating was prevented.

For scheme II, we have the following instructions:
(a) There are several kinds of hash functions, such as MD5, SHA1, SHA256, etc. All of them encrypt messages of any bit length to generate fixed bit length message digests.

(b) The shadow size is $1/(k - 1)$ of that of the original image.

Obviously, the size of the shadow image in scheme I is $1/(k - 2)$, but the size of the shadow image in scheme II is $1/(k - 1)$. Scheme II uses a slightly more complicated hash algorithm. It is the lightest operation in cryptography, far smaller than the basic password such as modular multiplication and modular exponentiation. Relative to these, it can be ignored. It can be said that scheme II is a very efficient and lightweight algorithm. Compared with scheme I, scheme II has a further improvement in security. Although it is slightly higher in storage and efficiency, it is suitable for environments and equipment with larger storage space and a higher level of security.

4. Experiment Results and Analysis

4.1. Experiment Results. In this section, we use two experiments to illustrate the proposed schemes in this paper.

For scheme I, we set the threshold $(k, n) = (5, 6)$, then each pixel block contains three pixels values. Supposing the first pixel block $P_1 = (57, 121, 90)$, the dealer calculates the secret authentication codes $b_0 = 57 \oplus 121 = 64$, $b_1 = 121 \oplus 90 = 35$. Then, we construct $k - 1 = 4$ degree polynomial $f(x) = 57 + 121x + 90x^2 + 64x^3 + 35x^4 \pmod{251}$. Finally, we calculate the six shadows: $S_1 = f(1) = 116$, $S_2 = f(2) = 225$, $S_3 = f(3) = 208$, $S_4 = f(4) = 228$, $S_5 = f(5) = 157$, $S_6 = f(6) = 206$. In the restoration phase, we choose five shadows, namely $S_1, S_2, S_3, S_4, S_5$ to reconstruct the secret image. Suppose we forge a false shadow $S'_1 = 110$, and then select $S_2, S_3, S_4, S_5, S'_1$. Next, we generate the polynomial $f(x)' = 27 + 34x + 135x^2 + 193x^3 + 223x^4$ through the Lagrange interpolation function. Here, $b_0 = 193$, $b_1' = 223$. Since $27 \times 34 = 57 \neq b_0$, $34 \times 135 = 165 \neq b_1'$, so we can successfully detect there exists fake shadow and the cheating prevention. We take $(5, 6)$-threshold scheme to test the proposed scheme I, the test image is the well-known image “Lena.” The goal is that any five out of six shadow images can be used for image reconstruction. The corresponding experimental results are shown in Figure 1.

In Figure 1, (a) shows the original secret image, its size is $256 \times 256$; (b) is the reconstructed image by using the Lagrange interpolating polynomial and the five shadow images chosen randomly (we choose the first five shadow images to reconstruct the original secret image); (c–h) are the shadow images, and the sizes of the six shadow images are $256 \times 256/(k - 2)$.

For scheme II, we let the threshold $(k, n) = (4, 6)$, then each pixel block contains three pixels values. Supposing that the first pixel block $P_1 = (57, 121, 90)$, we generate a 128-bit message digest $M_1$ through the MD5 algorithm. Next, perform a bit-by-bit XOR on every 16 bit to obtain a value of 1 bit. There is a total of 8-bit value as the secret authentication code $b = 10100001 = 161$. Next, we construct a $k - 1 = 3$ degree polynomial $f(x) = 57 + 68x + 90x^2 + 161x^3 \pmod{251}$. Finally, we calculate the six shadows: $S_1 = f(1) = 178$, $S_2 = f(2) = 190$, $S_3 = f(3) = 55$, $S_4 = f(4) = 237$, $S_5 = f(5) = 196$, $S_6 = f(6) = 145$. In the restoration phase, we choose four shadows to reconstruct the secret image. Suppose that we forge a fake shadow $S'_1 = 177$ and then select $S'_1, S_2, S_3, S_4$. Next, we calculate the polynomial $f(x) = 53 + 209x + 214x^2 + 203x^3$ through the Lagrange interpolation function. Here, $b_0 = 203$. We use the same MD5 algorithm to calculate the authentication message digest $b_0' = 30$ for $P_1' = (53, 209, 214)$. Since $b_0' \neq b_0$, so we can successfully detect the presence of deception and cheating prevention. We take $(4, 6)$-threshold scheme to test the proposed scheme II. The goal is that any four out of six shadow images can be used for image reconstruction. The corresponding experimental results are shown in Figure 2.

In Figure 2, (a) shows the original secret image, its size is $256 \times 256$; (b) is the reconstructed image by using the Lagrange interpolating polynomial and the four shadow images chosen randomly (we choose the first four shadow images to reconstruct the original secret image); (c–h) are the shadow images, and the sizes of the six shadow images are $256 \times 256/(k - 1)$ (here $k = 4$).

Figure 3 shows the experimental results of the other two typical pictures. Through the histogram, we can clearly find that the pixel values in image "Rice" are all less than 250, and the restored image is lossless. In image "Landscape," there are pixel values greater than 250, so the restored image is lossy. Visually, there is not much difference.

4.2. Performance Analysis. Normally, the shadow size is an important factor in evaluating the performance of an SIS scheme, since a smaller size has lower storage and transmission costs. Table 1 shows the comparisons between our scheme and other related schemes.

The scheme in [26] is based on the SIS. The visual secret sharing is applied to the polynomial-based SIS, and the shadows can be mutually authenticated by exchanging the lowest plane. This scheme has low complexity of shadow generation and authentication. However, the shadow image is larger, which is the same as the original image. The scheme in [8] is based on polynomial information hiding, and the shadow size is small.

In the restoration phase, only part of the pixel values participated in the authentication. In fact, the values of pixels that do not participate in authentication may be tampered, and the security level is low. The shadow size in scheme I and scheme II is almost the same as the original scheme, and all pixel values are involved in the authentication. Therefore, malicious tampering by forgers can be prevented during the authentication phase.

Figure 4 shows the shadow image size comparison between our scheme and other schemes. As the threshold $k$ increases, the ratio of the shadow image to the original image changes.

In addition, there are shadows in the application system in the image distribution, there are shadows and each shadow is stored in any distributed storage node. Due to the
(k, n)-threshold characteristic of the SIS scheme, when the threshold \( k \) is reached, the original secret image can be recovered. The failed transmission of the remaining \( n - k \) shadows will not affect the entire reconstruction phase.

The Peak Signal to Noise Ratio (PSNR) is an objective criterion for evaluating images. Usually, the output image will be different from the original image to some extent after encryption and decryption. To measure the processed image, the PSNR value is usually used to measure whether the processing method is satisfactory. The formula is as follows:

\[
\text{PSNR} = 10 \times \log_{10} \left( \frac{2^n - 1}{\text{MSE}} \right)
\]

where \( n \) is the mean square error between the original image and the processed image, expressed as

\[
\text{MSE} = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} (x_{i,j} - x'_{i,j})^2
\]

where \( m \times n \) is the size of the image, and \( x_{i,j}, x'_{i,j} \) is the pixel value of the original image and the reconstructed image at the point \((i, j)\). Therefore, the smaller the difference between the two images, the greater the PSNR value. In general, if PSNR \( \geq 30 \text{dB} \), the difference between the reconstructed image and the original secret image is difficult to detect by the human eye. Table 2 is the comparison of PSNR values between the four classic images processed by digital image processing shown in Experiment 1 and Experiment 2.

Since the pixel value in the rice grain image is not greater than 250, then PSNR = \( \infty \). On the other hand, all the PSNR of Lena, Landscape, and People image are greater than 30dB. Therefore, it is very difficult to detect the difference between the original secret image and the reconstructed image with human eyes.

4.3. Security Analysis. In this section, we will analyze the security of the proposed scheme from two aspects: the security of the secret sharing mechanism and the security of our proposed scheme. In the proposed scheme, it is mainly necessary to prove that the (k, n)-threshold must be met in the two phases of shadow image generation and secret image restoration and whether the presence of a fraudster can be detected when the participant reaches the threshold \( k \).

**Theorem 1.** The proposed scheme satisfies the property of (k, n)-threshold.

The scheme proposed in this paper satisfies the security of the secret sharing mechanism. A trusted third party distributes the shadow images to different participants evenly and randomly, and any two participants are completely independent. We discuss the case of less than \( k \) shadows in image reconstruction and select \( r (r < k) \) shadows \( S_1^r, S_2^r, \ldots, S_r^r \) from \( n \) shadow images \( S_j^r, j \in [1, n] \) for the reconstruction. Since there are \( k \) coefficients for the \( k - 1 \) degree Lagrange interpolation polynomial, according to the nature of the polynomial, it can be obtained that the coefficients of the polynomial cannot be solved by using Lagrange interpolation for \( k - 1 \) sub-shadows. Therefore, no image information can be generated. We can clearly see that \( k \) coefficients cannot be generated from \( r \) equations in the following equation:

\[
\begin{align*}
\left[ f' (1) \right] & = a_0 + a_1 + \cdots + a_{k-1}, \\
\left[ f' (2) \right] & = a_0 + 2a_1 + \cdots + 2^{k-1} a_{k-1}, \\
& \vdots \\
\left[ f' (r) \right] & = a_0 + ra_1 + \cdots + r^{k-1} a_{k-1}.
\end{align*}
\]  

(4)

In addition, we scramble the secret image before generating the shadow image. Thus, the shadow image in this scheme is disordered (Figures 1(c)–1(h)) and will not reveal any
Figure 2: Experiment 2 results: (a) the original secret image; (b) the reconstructed image; (c–h) the six shadow images.

Figure 3: The experiment for other images: (a) the secret image of Rice; (b) the histogram of Rice; (c) the reconstructed image of Rice; (d) the secret image of Landscape; (e) the histogram of Landscape; (f) the reconstructed image of Landscape.
The scheme in [19] The scheme in [18] The scheme in [26] SIS SIS 1/1 |1| Yes Yes Yes
Scheme in [8] Information hiding 1/k – 1/1| No No
Our proposed scheme I Information hiding 1/k – 2/1| Yes Yes
Our proposed scheme II Information hiding 1/k – 1/1| Yes Yes

The ratio of the shadow image to the original image

| Experimental image | Lena | Landscape | People | Rice |
|--------------------|------|-----------|--------|------|
| PSNR               | 71.78| 87.23     | 69.86  | ∞    |

information related to the original secret image. Considering that the number of shadow images reaches the threshold \( k \) during the image restoration process, the \( k \) shadow images participating in the reconstruction must be authenticated before the image reconstruction and restoration. According to the nature of the Lagrange interpolation polynomial, the secret pixel value and the authentication code can be solved. Prevent fraud by judging whether the authentication code is correct. When the authentication is successful, the secret pixel value is used to restore the original secret image.

On the contrary, when the authentication fails, the presence of deception shadows can be detected, the reconstruction and restoration of the secret image can be terminated. Therefore, when there is no shadow image with deception, any \( k \) or more shadow images can be reconstructed to recover the original secret image.

**Theorem 2.** Our scheme I can successfully detect the presence of cheaters.

Suppose \( S_1, S_2, \ldots, S_k \) participate in secret reconstruction phase and \( S_1, S_2, \ldots, S_{k-1} \) are cheaters. Since cheating prevention algorithm is used in each block \( P_i, i \in [1, r] \), we only analyze the cheating prevention in decoding \( P_1 \) in this theorem. Suppose the fake shares from cheaters are \( O_i = O_i + O_i^*, \ i = 1, 2, \ldots, k - 1 \). They can get a polynomial \( f^*(x) = f(x) + f^*(x) \) in the image reconstruction phase, where \( f^*(x) = a_0^* + a_1^*x + \ldots + b_1^{k-2} + b_1^{k-1} \). Since \( f^*(x) \) can be decided by cheaters exclusively, they can select two values \( b_0^*, b_1^* \), and satisfy that \( b_0^* = a_0^* \oplus a_{i+1}^* \oplus \cdots \oplus a_{k-1}^* \), \( b_1^* = a_1^* \oplus a_{i+1}^* \oplus \cdots \oplus a_{k-3}^* \). According to our algorithm, if there exist two values \( b_0^*, b_1^* \), satisfying \( b_0^* = (a_0^* + a_1^*) \oplus (a_1^* + a_2^*) \oplus \cdots \oplus (a_{k-3}^* + a_{k-2}^*) \), the cheating avoids detection. We can easily observe that cheating succeeds only when \( b_0^* = b_0, b_1^* = b_1^* \). As analyzed in Theorem 1, these \( k - 1 \) cheaters have no information on authentication codes; the possibility of \( b_0^* = b_0, b_1^* = b_1^* \) is 1/2\(^16\). As a result, the successful cheating probability \( \delta = 1/2^{16} \) means that scheme is effective in detecting the cheating.

**Theorem 3.** Scheme II can successfully detect the presence of cheaters.

Compared with scheme I, there is only one authentication code in scheme II. They can get a polynomial \( f^{**}(x) = f(x) + f^*(x) \) in the image reconstruction phase, where \( f^*(x) = a_0^* + a_1^*x + \cdots + a_{k-2}^*x^{k-2} + a_{k-1}^*x^{k-1} \). Since \( f^*(x) \) can be decided by cheaters exclusively, they can select one value \( b_0^* \) and satisfy step 2 and step 3 in the shadow generation phase in scheme II—the sequence \( M^* = a_0^* \parallel a_1^* \parallel \cdots \parallel a_{k-2}^* \) at this time. If there exists one value \( b_0^* \) satisfying \( M^* = (a_0^* + a_1^*) \parallel (a_1^* + a_2^*) \parallel \cdots \parallel (a_{k-3}^* + a_{k-2}^*) \), the cheating avoids detection. We can easily observe that cheating succeeds only when \( b_0^* = b_0^* \). As analyzed in Theorem 1, these \( k - 1 \) cheaters have no information on authentication codes; the possibility of \( b_0^* = b_0^* \) is 1/251. As a
result, the successful cheating probability $\delta = 1/251$ means that scheme II is effective in detecting the cheating.

5. Conclusions

Many security fields such as online transactions, digital image storage, and transmission require high security. There may be tampered with and forged secret sharing to participate in the reconstruction of secret information. Therefore, a secret scheme that can detect deception and prevent tampering has a wide range of practical applications.

We are considering the problem of cheating based on SIS itself, which can prevent the presence of cheaters among participants. In the process of polynomial-based design, the value processed by the polynomial each time is fixed $k$ coefficients. Too many authentication codes will cause the shadow image to increase, which is not conducive to storage. When performing antispooﬁng share authentication, how to balance between complexity and storage is very critical. In the first scheme proposed in this paper, two authentication codes are generated for authentication through a simple XOR operation. The size of the shadow image is $1/(k-2)$. This lightweight solution with less complexity is suitable for Internet of Things (IoT) devices or some resource-constrained embedded devices. In contrast, the second scheme is to generate an authentication code for authentication based on a hash algorithm, and the size of the shadow image is the same as the original Thien-Lin scheme. This kind of solution with higher complexity, although the storage efficiency is slightly increased, which is suitable for environments and devices with larger storage space and higher security levels. Another interesting work is the ability to accurately detect which one is a cheater. This is the focus of our next research.

Data Availability

The image data used to support the ﬁndings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conﬂicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (no. 62102309), Shaanxi Provincial Department of Science and Technology Youth Project (no. 2021JQ-575 and 2021JQ-576), Shaanxi Provincial Department of Education Project (no. 19JK0526), and Yulin Science and Technology Bureau Project (no. 2016-24-4 and 2019-173).

References

[1] J. Carlos Roca, J. José García, and J. José de la Vega, “The importance of perceived trust, security and privacy in online trading systems,” Information Management & Computer Security, vol. 17, no. 2, pp. 96–113, 2009.

[2] O. Ghazali, C. Y. Leow, S. Qaiser et al., “Cloud-based global online marketplaces review on trust and security,” International Journal of Interactive Mobile Technologies (IJIM), vol. 13, no. 4, p. 96, 2019.

[3] P. Zhao, Z. Ding, M. Wang, and R. Cao, “Behavior analysis for electronic commerce trading systems: a survey,” IEEE Access, vol. 7, pp. 108703–108728, 2019.

[4] A. Shamir, “How to share a secret,” Communications of the ACM, vol. 22, no. 11, pp. 612–613, 1979.

[5] C.-C. Thien and J.-C. Lin, “Secret image sharing,” Computers & Graphics, vol. 26, no. 5, pp. 765–770, 2002.

[6] Y. Liu, C. Yang, Y. Wang, L. Zhu, and W. Ji, “Cheating identiﬁable secret sharing scheme using symmetric bivariate polynomial,” Information Sciences, vol. 453, pp. 21–29, 2018.

[7] Y.-X. Liu, C.-N. Yang, C.-M. Wu, Q.-D. Sun, and W. Bi, “Threshold changeable secret image sharing scheme based on interpolation polynomial,” Multimedia Tools and Applications, vol. 78, no. 13, pp. 18653–18667, 2019.

[8] Y.-X. Liu, Q.-D. Sun, and C.-N. Yang, “(k, n) secret image sharing scheme capable of cheating detection,” EURASIP Journal on Wireless Communications and Networking, vol. 2018, no. 1, p. 72, 2018.

[9] L. Yuan, M. Li, C. Guo et al., “Secret image sharing scheme with threshold changeable capability,” Mathematical Problems in Engineering, vol. 2016, Article ID 9576074, 2016.

[10] Q. Zhao, J.-J. Zhao, F. Dai, and F.-Q. Zhao, “A new image secret sharing scheme to identify cheaters,” Computer Standards & Interfaces, vol. 31, no. 1, pp. 252–257, 2009.

[11] R. Ito, H. Kuwakado, and H. Tanaka, “Image size invariant visual cryptography,” Ieice Trans Fundamentals, vol. 82, no. 10, pp. 2172–2177, 1999.

[12] C.-N. Yang, “New visual secret sharing schemes using probabilistic method,” Pattern Recognition Letters, vol. 25, no. 4, pp. 481–494, 2004.

[13] S. Cimato, R. De Prisco, and A. De Santis, “Probabilistic visual cryptography schemes,” The Computer Journal, vol. 49, no. 1, pp. 97–107, 2006.

[14] G. Ateniese, C. Blundo, A. D. Santis et al., “Extended capabilities for visual cryptography,” Theoretical Computer Science, vol. 250, no. 1–2, pp. 143–161, 2001.

[15] C.-N. Yang and T.-S. Chen, “Extended visual secret sharing schemes: improving the shadow image quality,” International Journal of Pattern Recognition and Artificial Intelligence, vol. 21, no. 05, pp. 879–898, 2007.

[16] W.-P. Fang and J.-C. Lin, “Progressive viewing and sharing of sensitive images,” Pattern Recognition and Image Analysis, vol. 16, no. 4, pp. 632–636, 2006.

[17] R. Z. Wang, Y. K. Lee, S. Y. Huang et al., in Proceedings of the IEEE Second International Conference on Innovative Computing, Informatio and Control (ICICIC 2007), p. 283, Kumamoto, Japan, September 2007.

[18] R.-Z. Wang and S.-J. Shyu, “Scalable secret image sharing,” Signal Processing: Image Communication, vol. 22, no. 4, pp. 363–373, 2007.

[19] K. Ali and M. Ghebleh, “An efficient (t, n)-threshold secret image sharing scheme,” Journal of Intelligent and Fuzzy Systems, vol. 38, no. 5, pp. 1–10, 2019.

[20] L. Peng, C. N. Yang, and Z. Zhou, “Essential secret image sharing scheme capable of cheating detection,” International Journal of Interactive Mobile Technologies (IJIM), vol. 2019, no. 1, p. 72, 2019.

[21] Y.-X. Liu, C.-N. Yang, C.-M. Wu, Q.-D. Sun, and W. Bi, “Threshold changeable secret image sharing scheme based on interpolation polynomial,” Multimedia Tools and Applications, vol. 78, no. 13, pp. 18653–18667, 2019.
approach,” Concurrency and Computation: Practice and Experience, vol. 2020, Article ID e6000, 2020.

[23] M. Tompa and H. Woll, “How to share a secret with cheaters,” Journal of Cryptology, vol. 1, no. 3, pp. 133–138, 1989.

[24] W. Ogata, K. Kurosawa, and D. R. Stinson, “Optimum secret sharing scheme secure against cheating,” SIAM Journal on Discrete Mathematics, vol. 20, no. 1, p. 79C95, 2006.

[25] Y. Liu, “Linear (k, n ) secret sharing scheme with cheating detection,” Security and Communication Networks, vol. 9, no. 13, pp. 2115–2121, 2016.

[26] X. Yan, Q. Gong, L. Li et al., “Secret image sharing with separate shadow authentication ability,” Signal Processing: Image Communication, vol. 82, Article ID 115721, 2019.

[27] Y. Jiang, X. Yan, J. Qi, Y. Lu, and X. Zhou, “Secret image sharing with dealer-participatory and non-dealer-participatory mutual shadow authentication capabilities,” Mathematics, vol. 8, no. 2, p. 234, 2020.

[28] Y. K. Meghrajani, L. S. Desai, and H. S. Mazumdar, “Secure and efficient arithmetic-based multi-secret image sharing scheme using universal share,” Journal of Information Security and Applications, vol. 47, pp. 267–274, 2019.

[29] W. Hu, Y. Yao, D. Zhou et al., “A novel image secret sharing scheme without third-party scrambling method,” Mobile Networks and Applications, vol. 24, no. 4, pp. 1–19, 2018.

[30] X. Wu and C.-N. Yang, “Partial reversible AMBTC-based secret image sharing with steganography,” Digital Signal Processing, vol. 93, pp. 22–33, 2019.

[31] X. Wu and C.-N. Yang, “A combination of color-black-and-white visual cryptography and polynomial based secret image sharing,” Journal of Visual Communication and Image Representation, vol. 61, pp. 74–84, 2019.