EURASIP Journal on Image and Video Processing

RESEARCH Open Access

# Applying cheating identifiable secret sharing scheme in multimedia security

Ma Zheng[1,2], Ma Yan[1], Huang Xiaohong[1], Zhang Manjun[2] and Liu Yanxiao[3*]

*Correspondence:
liuyanxiao@xaut.edu.cn
[3]Xi'an University of Technology, Xi'an, 710048 China
Full list of author information is available at the end of the article

**Abstract**

In $(k, n)$ secret sharing scheme, one secret is encrypted into $n$ shares in such a way that only $k$ or more shares can decrypt the secret. Secret sharing scheme can be extended into the field of multimedia that provides an efficient way to protect confidential information on multimedia. Secret image sharing is just the most important extension of secret sharing that can safely guard the secrecy of images among multiple participants. On the other hand, cheating detection is an important issue in traditional secret sharing schemes that have been discussed for many years. However, the issue of cheating detection in secret image sharing has not been discussed sufficiently. In this paper, we consider the cheating problem in the application of secret image sharing schemes and construct a $(k, n)$ secret image sharing scheme with the ability of cheating detection and identification. Our scheme is capable of identifying cheaters when $k$ participants involve in reconstruction. The cheating identification ability and size of shadow in the proposed scheme are improved from the previous cheating identifiable secret image sharing scheme.

**Keywords:** Multimedia security, Secret image sharing, Secret sharing, Cheating identification

## 1 Introduction

$(k, n)$ secret sharing (SS) scheme was first proposed by Shamir [1] in 1979 to safeguard secret information among a group of participants. In Shamir's scheme, a secret $s$ is divided into $n$ shares $v_1, v_2, ..., v_n$ using a $k-1$ degree polynomial in such a way that any $k-1$ or less shares get no information about the secret $s$ and any $k$ or more shares can reconstruct the secret $s$ efficiently. In [2], the researchers designed reliable and secure devices that can realize Shamir's SS [1]. In 2002, Thien and Lin combined Shamir's SS scheme with image and proposed a secret image sharing (SIS) scheme [3] that can protect information on secret image among multiple users. After years of research, many SIS schemes were constructed, and all existing SIS schemes can be mainly divided into two categories: one is polynomial-based SIS schemes [4–6], and the other is visual cryptography (VC)-based schemes [7–9]. Polynomial-based SIS schemes can reconstruct lossless image with reduced shadow size; the image reconstruction in VC-based SIS schemes can be

simply accomplished by human visual system without any computation. However, the reconstructed image is lossy and the size of shadow is expanded from the original image.

The cheating problem in SS schemes was first introduced by Tompa and Woll [10] in 1989. They considered the scenario that some dishonest participants (cheaters) pool fake shares when reconstructing the secret. Through this method, the cheaters can get the valid secret exclusively; the other honest participants can only decode a forged secret. Many works have focused on solving cheating problem in SS schemes. Some of them [11–13] were interested in detecting the cheating behavior, and others [14–16] focused on not only detecting the cheating, but also identifying the cheaters. The cheating identifiable schemes have stronger capability to resist cheating, and it results that the shares are larger and the schemes are more complicated than those cheating detectable schemes.

As a result, the cheating problem is also an important issue in the field of SIS schemes. However, this issue has not been discussed sufficiently in SIS so far. In the works [17–19], some SIS schemes with steganography and authentication were capable of detecting or identifying the cheating behavior. However, those SIS schemes were not based on Shamir's scheme and the capabilities of cheating detection or identification were not strong enough to prevent the cheating. In [20], Liu et al. proposed a SIS with the capability of cheating detection, but the identification of cheaters is still unknown. In [21], Yang et al. proposed a SIS scheme that can identify cheaters during reconstruction. In their scheme, shadows are generated from bivariate polynomial and each shadow has extra bits which is used for authentication. The cheating identification is based on the property of symmetry in bivariate polynomial; however, the power on identifying cheaters in [21] is limited.

In this paper, we focus on the cheating problem in the fundamental polynomial-based SIS [3]. Since cheating identifiable scheme has much stronger power to prevent cheating behavior, we construct a $(k, n)$ SIS scheme capable of identifying up to $\left\lfloor \frac{k-2}{2} \right\rfloor$ cheaters. The rest of this paper is organized as follows. In Section 2, we introduce some related works, which includes Shamir's $(k, n)$ SS scheme, polynomial-based SIS scheme, and the model of cheating identification in SS scheme. In Section 3, we construct a $(k, n)$ SIS scheme capable of cheating identification, and the theoretical analysis is also provided in this section. In Section 4, we use an example to illustrate the cheating identification in the proposed scheme and give a comparison between the scheme in [21] and the proposed scheme. Section 5 gives the conclusion of this paper.

## 2 Related works

### 2.1 Shamir's $(k, n)$ SS scheme

A $(k, n)$ SS scheme is an approach where a secret is decrypted into $n$ shares, in such way that any $k$ or more shares can reconstruct the secret and fewer than $k$ shares get nothing about the secret. More formally, in secret sharing scheme, there exist $n$ participants $\mathcal{P} = \{P_1, P_2, ..., P_n\}$ and a dealer $\mathcal{D}$. A $(k, n)$ secret sharing scheme consists of two phases:

1. *Sharing phase:* During this phase, the dealer $\mathcal{D}$ divides the secret $s$ into $n$ shares $v_1, v_2, ..., v_n$ and sends each share $v_i$ to a participant $P_i$.
2. *Reconstruction phase:* During this phase, a group of at least $k$ participants submit their shares to reconstruct the secret.

In the *sharing phase*, the dealer $\mathcal{D}$ computes $n$ shares in such a way that satisfies the following conditions:

1 *Correctness:* Any set of at least $k$ shares can reconstruct the valid secret.
2 *Secrecy:* Any fewer than $k$ shares have no information about the secret.

Shamir's $(k, n)$ SS scheme is shown in the following Scheme 1.

**Scheme 1**: *Shamir's* $(k, n)$ *SS scheme*

***Sharing phase***:

1 The dealer $\mathcal{D}$ chooses a $k-1$ degree polynomial $\psi(x) \in GF(q)[X]$ which satisfies $s = \psi(0) \in GF(q)$.
2 The dealer $\mathcal{D}$ computes $n$ shares $v_i = \psi(i), i = 1, 2..., n$, and sends each share $v_i$ to a participant $P_i$.

***Reconstruction phase***:

1 $m(\geq k)$ participants (say $P_1, P_2..., P_m$) submit their shares $v_1, v_2..., v_m$ together.
2 Computing the interpolated polynomial $\psi(x)$ on $v_1, v_2..., v_m$ by the equation: $\psi(x) = \sum_{i=1}^{m} \left( v_i \prod_{u \neq i} \frac{x-u}{i-u} \right)$. Then the secret $s = \psi(0)$.

### 2.2 Cheating identification in SS scheme

Tompa and Woll [10] first introduced the cheating problem in secret sharing schemes, for instance, some cheaters submit fake shares during the *reconstruction phase*, which makes the honest participants reconstruct a forged secret and the cheaters can get the real secret exclusively. Cheating identification is a strong strategy to resist such cheating. The model of cheating identifiable secret sharing scheme is shown as follows:

*Sharing phase:* During this phase, the dealer $\mathcal{D}$ divides the secret $s$ into $n$ shares $v_1, v_2..., v_n$ and sends each share $v_i$ to a user $P_i$.
*Reconstruction phase:* During this phase, a group of $m$ users $(m \geq k)$ submit their shares to reconstruct the secret.

1 A public cheating identification algorithm is applied on these $m$ shares to identify cheaters.
2 Let $L$ be the set of users who are identified to be cheaters using cheating identification algorithm.
If $(m - |L|) \geq k$, reconstruct the secret $s$ from those shares of users who are not in $L$, and output $(s, L)$;
If $(m - |L|) < k$, output $L$.

### 2.3 Polynomial-based SIS

In [3], Thien and Lin proposed a remarkable $(k, n)$ SIS which was based on Shamir's SS scheme. An image $O$ is made up of multiple pixels, and the gray value of each pixel is in $GF(251)$. In fact, the range of gray scale is $[0, 255]$; for each pixel larger than 250, they are replaced by the value 250. Therefore, the reconstructed image would be of a little quality distortion from the original image. However, in majority cases, this quality distortion can be omitted with large number of pixels in an image. If all the pixels in an image are treated as secrets, a polynomial-based SIS can be extended from Shamir's SS. Thien-Lin's SIS scheme consists of two phases: *shadow generation phase* and *image reconstruction phase*.

In the shadow generation phase, a dealer regards a secret image $O$ as input and outputs $n$ shadows $S_1, S_2..., S_n$; during image recovery phase, any set of $m$ shadows $k \leq m \leq n$ reconstruct the secret image $O$.

**Scheme 2**: *Thien-Lin's* $(k, n)$ *SIS*

***Shadow Generation phase***:

Input secret image $O$, output $n$ shadows $S_1, S_2..., S_n$

1 The dealer divides $O$ into $l$-non-overlapping $k$-pixel blocks, $B_1, B_2..., B_l$.
2 For $k$ pixels $a_{j,0}, a_{j,1}..., a_{j,k-1} \in GF(251)$ in each block $B_j, j \in [1, l]$, the dealer generates a $k-1$ degree polynomial $\psi_j(x) \in GF(251)[X]$, namely, $\psi_j(x) = a_{j,0} + a_{j,1}x + a_{j,2}x^2 + ..., +a_{j,k-1}x^{k-1}$, and computes $n$ pixel-shares $v_{j,1} = \psi_j(1), v_{j,2} = \psi_j(2)..., v_{j,n} = \psi_j(n), j \in [1, l]$ as Shamir's secret sharing scheme.
3 Outputs $n$ shadows $S_i = v_{1,i} \parallel v_{2,i} \parallel, ..., \parallel v_{l,i}, i = 1, 2..., n$, the symbol $\parallel$ is the combination of pixel-shares.

***Image reconstruction phase***:

On input $m$ shadows $S_1, S_2..., S_m.(m \geq k)$.

1 Extract the pixel-shares $v_{1,j}, v_{2,j}..., v_{m,j}, j \in [1, l]$ from $S_1, S_2..., S_m$.
2 Using the approach of Shamir's scheme, and reconstructing the polynomial $\psi_j(x) = a_{j,0} + a_{j,1}x + a_{j,2}x^2 + ..., +a_{j,k-1}x^{k-1}$ from $v_{1,j}, v_{2,j}..., v_{m,j}, j \in [1, l]$. The block $B_j = a_{j,0} \parallel a_{j,1} \parallel ..., \parallel a_{j,k-1}$.
3 Outputs $O = B_1 \parallel B_2 \parallel, ..., \parallel B_l$.

It is obvious that Scheme 2 satisfies the $k$-threshold property: $k$ or more shadows can reconstruct entire image; less than $k$ shadows get nothing about secret image. The size of each shadow in Scheme 2 is $\frac{1}{k}$ times of the original image.

## 3 Methods

In this section, we consider the cheating problem in Scheme 2 and then proposed a cheating identifiable SIS that has the ability of identifying cheaters; then, the theoretical analysis is discussed to prove the correctness of the proposed work.

### 3.1 The proposed scheme

Suppose that during the image reconstruction phase, cheaters can submit forged shadows. It results that the honest participants can only get a fake secret image, while the cheaters can even reconstruct the secret image exclusively. In order to prevent this problem, we construct a $(k, n)$ SIS with cheating identification under the model in Section 2.2. Our scheme is based on Thien-Lin's fundamental scheme which can be also extended in other polynomial-based SIS schemes. Our scheme is shown in the following Scheme 3.

**Scheme 3:** $(k, n)$ SIS scheme with cheating identification

**Shadow Generation Phase:** Input a secret image $O$, output $n$ shadows $S_1, S_2, ..., S_n$.

1 The dealer divides $O$ into $l$-non-overlapping $k + \left\lfloor \frac{k-2}{2} \right\rfloor$-pixel blocks, $B_1, B_2, ..., B_l$. (Let $\omega = \left\lfloor \frac{k-2}{2} \right\rfloor$ in the rest of this paper)

2 For each block $B_i, i \in [1, l]$, there are $k + \omega$ secret pixels $a_{i,0}, a_{i,1}, ..., a_{i,k-1}$ and $b_{i,0}, b_{i,1}, ..., b_{i,\omega-1} \in GF(251)$. The dealer generates a $k-1$ degree polynomial $\psi_i(x) = a_{i,0} + a_{i,1}x + ..., +a_{i,k-1}x^{k-1} \in GF(251)[X]$.

3 The dealer chooses a random integer $\gamma_i$, and computes $k-\omega$ pixels $b_{i,\omega}, b_{i,\omega+1,..,b_{i,k-1}}$ which satisfy that: $a_{i,\omega} + \gamma_i b_{i,\omega} = 0, a_{i,\omega+1} + \gamma_i b_{i,\omega+1} = 0, ..., a_{i,k-1} + \gamma_i b_{i,k-1} = 0$ over $GF(251)$. Then the dealer generates another $k-1$ degree polynomial $\varphi_i(x) = b_{i,0} + b_{i,1}x + ..., +b_{i,k-1}x^{k-1}$. It also implies that $\eta_i(x) = \psi_i(x) + \gamma_i\varphi_i(x)$ is of degree $\omega - 1$.

4 For each block $B_i, i \in [1, l]$, the dealer computes pixel-shares $v_{i,j} = \{m_{i,j}, d_{i,j}\}, m_{i,j} = \psi_i(j), d_{i,j} = \varphi_i(j), j = 1, 2..., n$ for each participant $P_j$. The shadow $S_j$ for $P_j$ is $S_j = v_{1,j} \parallel v_{2,j} \parallel, ..., \parallel v_{t,j}$.

**Image Reconstruction Phase**: Input $k$ shadows, without loss of generality $(S_1, S_2, ..., S_k)$

1 Extract the pixel-shares $v_{i,j} = (m_{i,j}, d_{i,j}), i = 1, 2..., l, j = 1, 2..., k$ from $S_1, S_2..., S_k$.

2 For each group of $v_{i,1}, v_{i,2}, ..., v_{i,k}, i \in [1, l]$, using Lagrange interpolation to reconstruct $\psi_i(x)$ and $\varphi_i(x)$ from $m_{i,1}, m_{i,2}, ..., m_{i,k}$ and $d_{i,1}, d_{i,2}, ..., d_{i,k}$ respectively.

   (a) If there exists a $\omega - 1$ polynomial $\eta_i(x)$ and an integer $\gamma_i$, namely $\eta_i(x) = \psi_i(x) + \gamma_i\varphi_i(x), i \in [1, l]$, recover the block $B_i = (a_{i,0}, a_{i,1}, ..., a_{i,k-1}, b_{i,0}, b_{i,1}, ..., b_{i,\omega-1}), i = 1, 2, ..., l$. The image $O$ is reconstructed as $O = B_1 \parallel B_2, ..., \parallel B_l$.

   (b) Otherwise, if there exists no integer $\gamma_j, j \in [1, l]$ which satisfies that $\psi_j(x) + \gamma_j\varphi_j(x)$ with degree $\omega - 1$, using the following Algorithm 1 to identify cheaters.

The cheating identification process is described in Algorithm 1. For simplicity, it takes $k$ pixel-shares $v_i = (m_i, d_i), i = 1, 2, ..., k$ as input and outputs the set of cheaters.

**Algorithm 1**: Cheating identification: input $v_i = (m_i, d_i), i = 1, 2, ..., k$; output the set $\mathcal{X}$ of cheaters.

(1) Generating $C_k^{\omega+1}$ subsets $\varepsilon_1, \varepsilon_2, ..., \varepsilon_{C_k^{\omega+1}}$ on the set of $k$ pixel-shares $\{v_1, v_2, ..., v_k\}$.

(2) For each subset $\varepsilon_i, i \in \left[1, C_k^{\omega+1}\right]$, computing its corresponding checking polynomial $\eta_i^{'}(x)$. For example, $\varepsilon_1 = \{v_1, v_2, ..., v_\omega, v_{\omega+1}\}$, compute two $\omega-$th interpolated polynomials $\psi_1^{'}(x)$ and $g_1^{'}(x)$ on $m_1, m_2, ..., m_{\omega+1}$ and $d_1, d_2, ..., d_\omega, d_{\omega+1}$ respectively. Figure out an integer $\gamma_1^{'}$ such that $\eta_1^{'}(x) = \psi_1^{'}(x) + \gamma_1^{'}g_1^{'}(x)$ is of degree $\omega - 1$. Then $\eta_1^{'}(x)$ is the checking polynomial on the subset $\varepsilon_1$.

(3) Figure out the majority polynomial $\eta^m(x)$ among all the $C_k^{\omega+1}$ checking polynomials. Suppose $\varepsilon_1, \varepsilon_2, ..., \varepsilon_w$ are all the $w$ subsets whose checking polynomial equals to the majority polynomial $\eta^m(x)$, then the set of cheaters is presented by $\mathcal{X} = \{P_1, P_2, ..., P_k\} - (\varepsilon_1 \bigcup \varepsilon_2, ..., \bigcup \varepsilon_w)$.

In Thien-Lin's scheme, it can be noticed that the size of the shadow is $\frac{1}{k}$ times of the secret image. In our scheme, the pixel-share $v_{i,j} = (m_{i,j}, d_{i,j})$ are generated from each $k + \omega$-pixels block; therefore, the size of the shadow in our scheme is $\frac{2}{k+\omega}$ times of the secret image $O$. The most complicated operation of cheating identification in our scheme is computing $C_k^{\omega+1}$ polynomials with $\omega - 1$ degree; thus, the time complexity is $O\left(C_k^{\omega+1} * \omega^2\right)$.

Observing that in the proposed scheme, each block of the secret image is shared using Shamir's $(k, n)$ secret sharing scheme. Therefore, our proposed scheme is a perfect $(k, n)$ threshold scheme, namely, $k$ or more shadows can reconstruct the image, while $k-1$ or less shadows get no information about the image.

### 3.2 Theoretical analysis

The capability of cheating identification of the proposed scheme is summarized by the following lemma and theorem. Since in our scheme, the secret image is divided into multiple blocks and each block is encrypted into shares using the same approach, we use one block of $k+u$ pixels instead of the entire image to analyze its cheating identification ability.

**Lemma 1** *Sharing a $(k+\omega)$-pixel block $B = (a_0, a_1, ..., a_{k-1}, b_0, b_1, ..., b_{\omega-1})$ as shown in Scheme 2, any $\omega+1$ participants can get $\gamma$ and $\omega-1$ degree polynomial $\eta(x)$. The dealer D decides the parameters of $\eta(x)$. ($\eta(x) = \gamma\varphi(x) + \psi(x)$, any $\omega+1$ participants can get $\eta(x)$ and $\gamma$ without acknowledgment on $\psi(x)$ and $\varphi(x)$) but $\omega$ participants are unable to get any information about $\gamma$ and $\eta(x)$.*

*Proof* Supposing $\omega+1$ participants are $P_1, P_2, ..., P_{\omega+1}$, respectively, and they possess $\omega+1$ pixel-shares, $v_i = \{m_i, d_i\}, i = 1, 2, ..., \omega+1$. The $\omega+1$ points $(1, m_1), (2, m_2), ..., (\omega+1, m_{\omega+1})$ determine an interpolated polynomial $\psi'(x)$. And another interpolated polynomial $\varphi'(x)$ is determined by $\omega+1$ points $(1, d_1), (2, d_2), ..., (\omega+1, d_{\omega+1})$. A conclusion can be made easily, $\omega+1$ points $(1, m_1), (2, m_2), ..., (\omega+1, m_{\omega+1})$ are linear independent; otherwise, the interpolated polynomial on $(1, m_1), (2, m_2), ..., (k, m_k)$ would be less than $k-1$, since the $n$ points $(1, m_1), (2, m_2), ..., (k, m_k)$ deduce a interpolated polynomial with $k-1$ degree $\psi(x)$ and $k > \omega+1$. So, $\psi'(x)$ and $\varphi'(x)$ are both $\omega$-degree interpolated polynomials.

Now, we have $\eta(x) = \gamma\varphi(x) + \psi(x)$ and $\eta'(x) = \psi'(x) + \gamma'\varphi'(x)$. Let $R(x) = \eta(x) - \eta'(x)$. Therefore, we get:

$$R(x) = \psi(x) - \psi'(x) + \gamma\varphi(x) - \gamma'\varphi'(x). \tag{1}$$

We get $\psi(i) = \psi'(i), i = 1, 2, ..., \omega+1$, since $\psi(x)$ and $\psi'(x)$ must pass through $(i, m_i), i = 1, 2, ..., \omega+1$. Similarly, we get $\varphi(i) = \varphi'(i), i = 1, 2, ..., \omega+1$. Together with Eq. (1), we can get that $R(i) = \left(\gamma - \gamma'\right)\varphi'(i), i = 1, 2, ..., \omega+1$, which means that $R(x)$ intersects $\left(\gamma - \gamma'\right)\varphi'(x)$ at $\omega+1$ points, since both $R(x)$ and $\left(\gamma - \gamma'\right)\varphi'(x)$ are of degree no more than $\omega$.

Thus, we get a conclusion that:

$$R(x) = \left(\gamma - \gamma'\right)\varphi'(x). \tag{2}$$

Obviously, $R(x) = \eta(x) - \eta'(x)$, where $R(x)$ is an interpolated polynomial, and the degree which is no more than $\omega-1$. Similarly, the $\varphi'(x)$ is of degree $\omega$ exactly. Therefore, we get that $\gamma = \gamma'$ and $\eta'(x) = \eta(x)$. Otherwise, it would contradict to Eq. (2).

Next, we prove that $\gamma$ and $\eta(x)$ cannot be gotten by $\omega$ shareholders. The $\varphi(x)$ is dependent with $\psi(x)$, such that there exists a $\omega-1$ degree polynomial $\eta(x)$ and a value $\gamma$, which satisfies $\eta(x) = \psi(x) + \gamma\varphi(x)$. If we consider the $\omega$ coefficients of $\eta(x)$ and the value $\gamma$ as $\omega+1$ unknowns, then each participant $P_i$ can build a linear equation $\eta(i) = m_i + \gamma \cdot d_i$ on these $\omega+1$ unknowns using their share $(m_i, d_i)$. As a result, $\omega$ participants can build

$\omega$ linear equations on these $\omega+1$ unknowns. These $\omega+1$ unknowns cannot be figured out, according to the property of linear equations. Otherwise, by using their $\omega$ shares, $\omega$ participants can only get two $\omega-1$-th degree interpolated polynomials $\psi^{''}(x)$ and $\varphi^{''}(x)$. $\eta(x)$ and $\gamma$ can be denoted as

$$\eta(x) = \gamma\varphi^{''}(x) + \psi^{''}(x). \tag{3}$$

However, $\eta(x)$, $\psi^{''}(x)$ and $\varphi^{''}(x)$ are $\omega-1$-degree interpolated polynomials. According to Eq. (3), with probabilities $\frac{1}{p}$, each element $e$ in $GF(p)$ could be $\gamma$. Therefore, $\gamma$ and $\eta(x)$ cannot be gotten by $\omega$ shareholders. End proof.

□

**Theorem 1** *If the number t of cheaters satisfies* $t \le \omega = \left\lfloor \frac{k-2}{2} \right\rfloor$, *these cheaters can be identified in the proposed scheme.*

*Proof* According to Lemma 1, $\gamma$ and $\eta(x)$ can be obtained by $\omega+1$ cheaters using their valid pixel-shares. Among these cheaters, the $P_j$ is a critical cheater, which can even forge his pixel-share $v_j^{'} = \left(m_j^{'}, d_j^{'}\right)$ where $m_j^{'} \neq m_j$ to satisfy $m_j^{'} + \gamma \cdot d_j^{'} = \eta(j)$. Each combination of $\omega+1$ submitted pixel-shares including $v_j^{'}$ deduces an identical checking polynomial $\eta(x)$, during *secret reconstruction and cheater identification*, the cheater $P_j$ succeeds in cheating.

As illustrated in Lemma 1, when $t \le \omega = \left\lfloor \frac{k-2}{2} \right\rfloor$, $\omega$ cheaters can get no information about $\gamma$. Thus, forged shares cannot be made successfully by any $\omega$ or less cheaters, to avoid identification. A checking polynomial can be generated by any $\omega+1$ participants, according to Lemma 1, and $t \le \omega = \left\lfloor \frac{k-2}{2} \right\rfloor$. There are $\omega+2$ valid shares selected from $k$ submitted shares at least. $C_{\omega+2}^{\omega+1} = \omega+2$ valid checking polynomials can be generated in CI. Without loss of generality, supposing $P_1$ is a critical cheater who releases a forged pixel-share $v_1^{'}$. If and only if there is a set of $\omega+2$ submitted pixel-shares including $v_1^{'}$, and this set of pixel-shares has the property, a same checking polynomial $\eta_1(x)$ can be made by each $\omega+1$ combined shares.

The $\omega+2$ submitted pixel-shares are $v_1^{'}, v_1^{'}, ..., v_t^{'}, v_{t+1}, ..., v_{i_{\omega+2}}$ where $P_1, P_2, ..., P_t$ are $t$ cheaters and $P_1$ is a critical cheater who knows $v_2^{'}, v_3^{'}, ..., v_t^{'}$. $\eta_1(x)$ and the value $\gamma_1$ are made by $v_1^{'}, v_2^{'}, ..., v_t^{'}, v_{t+1}, ..., v_{\omega+1}$, then $v_{\omega+2} = (m_{\omega+2}, d_{\omega+2})$ has to satisfy

$$m_{\omega+2} + \gamma_1 d_{\omega+2} = \eta_1(\omega+2). \tag{4}$$

It is noticed that the $t$ cheaters can get no information about $\gamma_1, \eta_1(x)$ and $v_{\omega+2} = (m_{\omega+2}, d_{\omega+2})$, and the probability of (4) is $\frac{1}{p}$. In other words, the successful cheating probability of $P_1$ is $\frac{1}{p}$. End proof. □

## 4 Results and discussion

In this part, we show the experimental results and give a comparison between our scheme and other cheating detectable SIS. In this example, let the threshold is $(k, n) = (6, n)$, and the secret image $O$ is divided into $l$ blocks where each block includes $k + \left\lfloor \frac{k-2}{2} \right\rfloor = 8$ secret pixels. Assuming one block $B$ consists of the following 8 pixels: $(a_0, ..., a_5, b_0, b_1) = (57, 68, 90, 231, 42, 89, 124, 186)$, the dealer selects an integer $\gamma = 10$, then generates two $k-1=5$ degree polynomials: $\psi(x) = 57 + 68x + 90x^2 + 231x^3 + 42x^4 + 89x^5$ and $\varphi(x) = 124 + 186x + 242x^2 + 2x^3 + 46x^4 + 217x^5$, where $a_i + \gamma \cdot b_i = 0, i = 2, 3, 4, 5$. Supposing

$P_1, P_2, ..., P_6$ participate in image reconstruction, the pixel-shares are $v_1 = (75, 64), v_2 = (148, 124), v_3 = (209, 135), v_4 = (220, 151), v_5 = (59, 134), v_6 = (160, 141)$.

If all these 6 participants are honest, they submit real pixel-shares in image reconstruction, and two polynomials $\psi(x) = 57 + 68x + 90x^2 + 231x^3 + 42x^4 + 89x^5$ and $\varphi(x) = 124 + 186x + 242x^2 + 2x^3 + 46x^4 + 217x^5$ can be reconstructed, respectively. They can also find $\gamma = 10$, such that $\eta(x) = \psi(x) + \gamma \cdot \varphi(x) = 42 + 171x$ is of degree $\left\lfloor \frac{k-2}{2} \right\rfloor - 1$. It means that there is no cheating behavior, and the pixel-block $B = (57, 68, 90, 231, 42, 89, 124, 186)$ is reconstructed.

Now we assume $P_1, P_2$ are two cheaters $\left(t = 2 \leq \left\lfloor \frac{k-2}{2} \right\rfloor\right)$ who submit fake pixel-shares $v_1' = (98, 109), v_2' = (215, 81)$ in image reconstruction. The cheating behavior can be easily detected using our scheme. During cheating identification algorithm, all the 4 subsets which contain 3 honest participants can compute the same checking polynomial $\eta(x) = 42 + 171x$. For example, $(P_3, P_4, P_5)$ can get two interpolated polynomials $\psi^*(x) = 148 + 111x + 165x^2, \varphi^*(x) = 140 + 6x + 109x^2$. Then, they can figure out a unique integer $\gamma = 10$ such that $\eta(x) = \psi^*(x) + \gamma \cdot \varphi^*(x) = 42 + 171x$. For another subset of 3 honest participants $(P_3, P_4, P_6)$, they can reconstruct two interpolated polynomials $\psi^*(x) = 12 + 23x + 70x^2, \varphi^*(x) = 3 + 65x + 244x^2$ from their pixel-shares. Then, they can also figure out the integer $r = 10$ such that $\eta(x) = \psi^*(x) + \gamma \cdot \varphi^*(x) = 42 + 171x$. On the other side, each subset of three participants which contain $P_1$ or $P_2$ deduces different checking polynomials. Therefore, $\eta(x) = \psi^*(x) + \gamma \cdot \varphi^*(x) = 42 + 171x$ is regarded as the majority polynomial, and the cheaters can be identified successfully accordingly.

In [21], Yang et al. proposed an authentication approach in secret image sharing which is also capable of identifying cheaters during secret reconstruction phase. The scheme in [21] is also based on Thien-Lin's scheme [3], but uses symmetric bivariate polynomial to generate shadows. It encrypts each $\frac{k(k+1)}{2}$ secret pixels into $k$ pixel-shares, and the size of the shadow is $\frac{2}{k+1}$ times of the secret image. The shadow size in our scheme is $\frac{2}{k+\omega}$, which is smaller than the size in Yang et al.'s scheme when $\omega = \left\lfloor \frac{k-2}{2} \right\rfloor \geq 1$. In cheating identification, not only the $k$ participants, but also the other $n - k$ participants work together to vote for the $k$ participants using the property of symmetry bivariate polynomial. The participants who get less than $\left\lfloor \frac{n-1}{2} \right\rfloor$ votes are identified as cheaters. However, in most cheating identifiable secret sharing schemes, the cheating identification is carried out only by the participants in secret reconstruction, and it is not practical to involve other $n - k$ participants in cheating identification. In fact, if $k$ participants work together to identify cheaters in Yang et al.'s scheme, the cheaters cannot be identified since the cheater can always get more votes than honest participants. The comparison between Yang et al.'s scheme and the proposed scheme is shown in the following Table 1. The symbol CI in Table 1 means the capability of cheating identification.

**Table 1** Comparison between the proposed scheme and Yang et al.'s scheme

| | Yang et al.'s scheme | Proposed scheme |
|---|---|---|
| Pixel number in each block | $\frac{k(k+1)}{2}$ | $k + \left\lfloor \frac{k-2}{2} \right\rfloor$ |
| Shadow size | $\frac{2}{k+1}$ | $\frac{2}{k+\left\lfloor \frac{k-2}{2} \right\rfloor}$ |
| CI ($k$ participants) | Failed | $t \leq \left\lfloor \frac{k-2}{2} \right\rfloor$ |
| CI ($n$ participants) | $t \leq \left\lfloor \frac{n-1}{2} \right\rfloor$ | |

**Fig. 1** 512 × 512 secret image

We can also use 512 × 512 Lena (Fig. 1) as the secret image $O$ to generate shadows using our $(4, 7)$ SIS scheme with cheating identification. The $n = 7$ shadows are shown in Fig. 2 where each shadow has $\frac{2}{k+\left\lfloor\frac{k-2}{2}\right\rfloor} = \frac{2}{5}$ times of the secret image. Each 4 participants can reconstruct the image that can identify $\left\lfloor\frac{k-2}{2}\right\rfloor = 1$ cheaters.

## 5 Conclusion

In this paper, we consider the well-known cheating problem in polynomial-based $(k, n)$ SIS, such that a group of malicious participants submit fake shadows during image reconstruction. In order to prevent such cheating behavior, we construct a $(k, n)$ SIS scheme with cheating identification under the model of cheating identifiable SS scheme. Our scheme is capable of identifying $\left\lfloor\frac{k-2}{2}\right\rfloor$ cheaters when $k$ participants involve in image reconstruction. In addition, the proposed scheme is based on the landmark Thien-Lin's polynomial-based SIS scheme, which can be easily extended into other polynomial-based SIS schemes. Both the size of shadow and the capability of cheating identification are enhanced from previous SIS schemes with cheating identification.

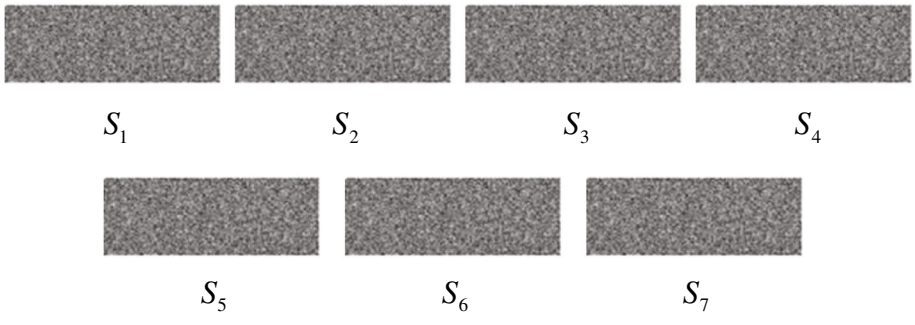


**Fig. 2** Seven shadows on the secret image

**Abbreviations**
SS: Secret sharing; SIS: Secret image sharing; VC: Visual cryptography

**Acknowledgements**
We want to thank Professor Lein Harn from the University of Missouri-Kansas city for his help in English improvement.

**Authors' contributions**
Zheng Ma provides the main concept, Yan Ma and Xiaohong Huang design the algorithms, Manjun Zhang gives the experiments, and Yanxiao Liu makes the comparisons. The authors read and approved the final manuscript.

**Funding**
The research presented in this paper is supported by the National Key R&D Program of China under No. 2018YFB1800100.

**Availability of data and materials**
Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

**Competing interests**
The authors declare that they have no competing interests.

**Author details**
[1]Beijing University of Posts and Telecommunications, Beijing, China. [2]China Unicom Network Technology Research Institute, Beijing, China. [3]Xi'an University of Technology, Xi'an, 710048 China.

Received: 15 April 2020 Accepted: 25 August 2020
Published online: 17 September 2020

**References**

1. A. Shamir, How to share a secret. Commun. ACM. **22**(11), 612–613 (1979)
2. Z. Wang, M. Karpovsky, L. Bu, Design of reliable and secure devices realizing Shamir's secret sharing. IEEE Trans. Comput. **65**(8), 2443–2455 (2016)
3. C. C. Thien, J. C. Lin, Secret image sharing. Comput. Graph. **26**(5), 765–770 (2002)
4. Y. X. Liu, C. N. Yang, Q. D. Sun, Y. C. Chen, $(k, n)$ scalable secret image sharing with multiple decoding options. J. Intell. Fuzzy Syst. **38**(1), 219–228 (2020)
5. Y. X. Liu, C. N. Yang, Q. D. Sun, Thresholds based image extraction schemes in big data environment in intelligent traffic management. IEEE Trans. Intell. Transp. Syst. (2020). https://doi.org/10.1109/TITS.2020.2994386
6. Y. X. Liu, C. N. Yang, C. M. Wu, Q. D. Sun, W. Bi, Threshold changeable secret image sharing scheme based on interpolation polynomial. Multimed. Tools Appl. **78**(13), 18653–18667 (2019)
7. R. Z. Wang, Region incrementing visual cryptography. IEEE Sig. Process. Lett. **16**(8), 659–662 (2009)
8. C. N. Yang, H. W. Shih, C. C. Wu, L. Harn, $k$ out of $n$ region incrementing scheme in visual cryptography. IEEE Trans. Circ. Syst. Video Technol. **22**(5), 799–809 (2012)
9. C. N. Yang, Y. C. Lin, C. C. Wu, Region in region incrementing visual cryptography scheme. Proc. IWDW2012, LNCS. **7809**, 449–463 (2013)
10. M. Tompa, H. Woll, How to share a secret with cheaters. J. Cryptol. **1**(3), 133–138 (1989)
11. P. Y. Lin, Chang C.C., Cheating resistance and reversibility-oriented secret sharing mechanism. IET Inf. Secur. **5**(2), 81–92 (2011)
12. S. Obana, T. Araki, in *Proceedings of ASIACRYPT, LNCS 4284*, Almost optimum secret sharing schemes secure against cheating for arbitrary secret distribution (Springer, Heidelberg, 2006), pp. 364–379
13. W. Ogata, Kurosawa K., Stinson D.R., Optimum secret sharing scheme secure against cheating. SIAM J. Discret. Math. **20**(1), 79–95 (2006)
14. K. Kurosawa, S. Obana, W. Ogata, in *Proceedings of CRYPTO, LNCS 563*, $t$-cheater identifiable $(k, n)$ secret sharing schemes (Springer, Heidelberg, 1995), pp. 410–423
15. S. Obana, in *Proceedings of EUROCRYPT, LNCS 6632*, Almost optimum $t$-cheater identifiable secret sharing schemes (Springer, Heidelberg, 2011), pp. 284–302
16. L. Harn, C. L. Lin, Detection and identification in $(t, n)$ secret sharing scheme. Des. Code Crypt. **52**(1), 15–24 (2009)
17. C. C. Lin, W. H. Tsai, Secret image sharing with steganography and authentication. J. Syst. Softw. **73**, 405–414 (2004)
18. C. N. Yang, T. S. Chen, K. H. Yu, C. C. Wang, Improvements of image sharing with steganography and authentication. J. Syst. Softw. **80**, 1070–1076 (2007)
19. C. C. Chang, Y. P. Hsieh, C. H. Lin, Sharing secrets in stego images with authentication. Pattern Recog. **41**, 3130–3137 (2008)
20. Y. X. Liu, Q. D. Sun, C. N. Yang, $(k, n)$ secret image sharing scheme capable of cheating detection. EURASIP J. Wirel. Commun. Netw. **2018**, 72 (2018)
21. C. N. Yang, J. F. Quyang, L. Harn, Steganography and authentication in image sharing without party bits. Opt. Commun. **285**, 1725–1735 (2012)

## Publisher's Note