Liu *et al. EURASIP Journal on Wireless Communications and Networking* (2018) 2018:72
https://doi.org/10.1186/s13638-018-1084-7

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

(k, n) secret image sharing scheme capable of cheating detection

Yan-Xiao Liu[1*], Qin-Dong Sun[1] and Ching-Nung Yang[2]

Abstract

In a (k, n) threshold secret image sharing scheme, a secret image is encrypted into n image-shadows that satisfy the following: (1) any less than k image-shadows get no information on the image and (2) any k or more image-shadows can reconstruct the entire image. Cheating problem is an important issue in traditional secret sharing scheme. However, this issue has not been discussed sufficiently in the field of secret image sharing. In this paper, we consider the scenario of cheating behavior in secret image sharing scheme and construct a (k, n) threshold secret image sharing scheme which is capable of cheating detection. Our proposed scheme is able to detect the cheating behavior from up to $k - 1$ cheaters, and the size of image-shadow is almost same as the image-shadow in the original secret image sharing scheme.

Keywords: Secret sharing, Secret image sharing, Cheating detection

1 Introduction

(k, n) threshold secret sharing scheme was first proposed by Shamir [1] in 1979 for safeguarding secret information among a group of participants. In [1], a secret s is encrypted into n shares $v_1, v_2, ..., v_n$ using a $k - 1$-th degree polynomial in such a way that less than k shares get no information on the secret s; any k or more shares can recover the secret s efficiently. Secret sharing scheme is a fundamental tool for other cryptographic protocols [2]. In 2002, Thien and Lin extended Shamir's secret sharing and proposed a (k, n) threshold secret image sharing scheme [3] by regarding an image as secret information. The (k, n) secret image sharing schemes can be mainly divided into two categories: polynomial-based schemes [4–6] and visual cryptography schemes [7–9]. Polynomial-based secret image sharing schemes can reconstruct a lossless image with reduced shadow size; the image reconstruction in visual cryptography schemes can be simply accomplished by human visual system without any computation. However, a reconstructed image is lossy and the size of shadow is greatly expanded from the original image.

The cheating scenario in secret sharing scheme was first proposed in 1989 by Tompa and Woll [7]. They considered the scenario that some dishonest participants (cheaters) pool fake shares when reconstructing the secret. In this way, the cheaters could recover a secret exclusively, and the honest participants can only recover a forged secret. Many works have focused on solving the cheating problem in secret sharing schemes. Some [10–12] were interested in detecting the cheating behavior, and some works [13–15] focused on not only detecting the cheating behavior, but also identifying the cheaters. The cheating identifiable schemes have stronger capability to resist cheating; it results that the shares are larger and the schemes are more complicated than those cheating detectable schemes. Polynomial-based secret image sharing scheme was extended from Shamir's scheme [1]. As a result, the problem of cheating is also an important topic in polynomial-based secret image sharing. However, this issue has not been discussed sufficiently so far. In [16–19], some secret image sharing schemes with authentication and steganography were capable of detecting the cheating. However, these secret image sharing schemes were not extensions of Shamir's scheme and the capabilities of cheating detection were not strong enough to prevent cheating.

In this work, we consider the problem of cheating in the fundamental polynomial-based secret image sharing scheme [3]. Since cheating identifiable scheme requires

*Correspondence: liuyanxiao@xaut.edu.cn
[1] Department of Computer Science and Engineering, Xi'an University of Technology, Xi'an, China
Full list of author information is available at the end of the article

large size expansion on shadows and much more complicated identification algorithm, we consider the cheating detection to prevent cheating behavior in this work. A (k, n) threshold secret image sharing scheme capable of detecting $k - 1$ cheaters is constructed. In addition, the size of image-shadow in our scheme is almost same as the shadow size in the scheme [3]. The computational complexity of cheating detection is efficient. The rest of this paper is organized as follows: Some preliminaries which include Shamir's (k, n) secret sharing scheme, polynomial-based secret image sharing scheme, and the model of cheating detection in secret sharing scheme are introduced in Section 2. In the next section, a (k, n) threshold secret image sharing scheme with cheating detection is proposed. The properties of proposed scheme and experimental results will be shown in Section 4, and we make a conclusion in Section 5.

2 Preliminaries

2.1 Shamir's (k, n) secret sharing scheme

A (k, n) threshold secret sharing scheme is a protocol where a secret is divided into n shares. The n shares satisfy that (1) k or more shares can recover the secret and less than k shares get nothing on the secret. More formally, there exists n participants $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ and a mutually trusted dealer $\mathcal{D}$. A secret sharing scheme is made up of the following two phases:

1. ***Sharing phase***: The dealer $\mathcal{D}$ encrypts secret s into n shares $v_1, v_2, \ldots, v_n$ and sends each share v_i to a participant P_i.
2. ***Reconstruction phase***: k or more participants submit their shares to recover secret.

The n shares generated by the dealer should satisfy the following two conditions:

1. ***Correctness***: Any group of at least k shares can recover the valid secret s.
2. ***Secrecy***: Fewer than k shares get no information on the secret s.

Shamir's scheme was based on interpolation polynomial which is shown in **Scheme 1**.

Scheme 1: *Shamir's (k, n) secret sharing scheme*

Sharing phase:

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

Reconstruction phase:

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

2.2 Cheating detection in secret sharing scheme

The cheating scenario in secret sharing was first introduced by Tompa and Woll [20] such that some malicious participants disclose fake shares in *Reconstruction phase*, which makes the honest participants reconstruct a forged secret and the cheaters can get the real secret exclusively. In [20], they also introduced the model of secret sharing with cheating detection, which also consists of two phases as follows:

1. *Sharing phase:* The dealer $\mathcal{D}$ divides the secret s into n shares $v_1, v_2, \ldots., v_n$ and sends each share v_i to a participant P_i.
2. *Reconstruction phase:* A group of m participants $(m \geq k)$ submit their shares.

    (1) A public cheating detection algorithm is applied on these shares to detect cheating.

    (2)
    - If cheating is detected, stop the Reconstruction phase and output $\perp$.
    - Else, reconstruct the secret s from these shares and output s.

2.3 Polynomial-based secret image sharing scheme

In [3], a remarkable (k, n) secret image sharing scheme was proposed by Thien and Lin which was based on Shamir's scheme. An image I is made up of multiple pixels $(p_1, p_2, \ldots, p_w)$, where each pixel p_i can be presented as its gray value in $GF(251)$. If all the pixels in an image are treated as secrets, a secret image sharing scheme can be extended from original secret sharing scheme. The scheme [3] consists of two phases: *shadow generation phase* and *image reconstruction phase*. In the first phase, a dealer encrypts I into n image-shadows $S_1, S_2, \ldots, S_n$; in the second phase, any set of m image-shadows $k \leq m \leq n$ reconstructs the secret image I.

Scheme 2: *Thien-Lin's secret image sharing*
Shadow generation phase:

Input secret image I, outputs n image-shadows $S_1, S_2, \ldots, S_n$

1. The dealer divides I into l-non-overlapping k-pixels blocks, $B_1, B_2, \ldots, B_l$.
2. For k pixels $a_{j,0}, a_{j,1}, \ldots, a_{j,k-1} \in GF(251)$ in each block $B_j, j \in [1, l]$, the dealer generates a $k - 1$-th

degree polynomial $f_j(x) \in GF(251)[X]$, such that $f_j(x) = a_{j,0} + a_{j,1}x + a_{j,2}x^2 + \ldots, +a_{j,k-1}x^{k-1}$, and computes n shares $v_{j,1} = f_j(1), v_{j,2} = f_j(2), \ldots, v_{j,n} = f_j(n), j \in [1,l]$ as Shamir's scheme.

3 Outputs n shadows $S_i = v_{1,i} \parallel v_{2,i} \parallel, \ldots, \parallel v_{l,i}, i = 1, 2, \ldots, n$.

Image reconstruction phase:
On input m shadows $S_1, S_2, \ldots, S_m.(m \geq k)$.

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

It is obvious that **Scheme 2** satisfies k-threshold property that k or more image-shadows are capable of recovering the entire image; fewer than k image-shadows get noting on the image. The size of image-shadow in **Scheme 2** is $\frac{1}{k}$ times of the image I.

3 (k,n) secret image sharing with cheating detection

The problem of cheating in secret image sharing is considered in this part, such that some cheaters submit forged image-shadows during image reconstruction phase. It results that these cheaters are able to recover secret image exclusively, and the honest participants recover only a fake image. In order to solve this problem, we construct a (k,n) threshold secret image sharing scheme capable of detect cheating under the model in Section 2.2. Our scheme is extended from Thien-Lin's fundamental scheme which can be adopted in other polynomial-based secret image sharing schemes. Our scheme is shown in **Scheme 3**.

Scheme 3: (k,n) secret image sharing scheme capable of detect cheating

Shadow Generation Phase: Input a secret image I, output n image-shadows $S_1, S_2, \ldots, S_n$

(1) The dealer divides I into t-non-overlapping $2k-2$-pixel blocks, $B_1, B_2, ..., B_t$.
(2) For each block $B_i, i \in [1,t]$, there are $2k-2$ secret pixels $a_{i,0}, a_{i,1}, \ldots, a_{i,k-1}$ and $b_{i,2}, b_{i,3}, \ldots, b_{i,k-1} \in GF(251)$. The dealer generates a $k-1$-th degree polynomial $f_i(x) = a_{i,0} + a_{i,1}x+, \ldots, +a_{i,k-1}x^{k-1} \in GF(251)[X]$.
(3) The dealer chooses a random integer r_i, and computes two pixels $b_{i,0}, b_{i,1}$ which satisfy that: $r_ia_{i,0} + b_{i,0} = 0, r_ia_{i,1} + b_{i,1} = 0$ over $GF(251)$. Then the dealer generates another $k-1$-th degree polynomial $g_i(x) = b_{i,0} + b_{i,1}x + \ldots, +b_{i,k-1}x^{k-1}$.
(4) For each block $B_i, i \in [1,t]$, the dealer computes sub-shadow $v_{i,j} = \{m_{i,j}, d_{i,j}\}, m_{i,j} = f_i(j), d_{i,j} = g_i(j), j = 1, 2, \ldots, n$ for each participant P_j. The shadow S_j for P_j is $S_j = v_{1,j} \parallel v_{2,j} \parallel, \ldots, \parallel v_{t,j}$.

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

(1) Extract $v_{i,j} = (m_{i,j}, d_{i,j}), i = 1, 2, \ldots, t, j = 1, 2, \ldots, k$ from $S_1, S_2, \ldots, S_k$.
(2) For each group of $v_{i,1}, v_{i,2}, \ldots, v_{i,k}, i \in [1,t]$, reconstruct $f_i(x)$ and $g_i(x)$ from $m_{i,1}, m_{i,2}, \ldots, m_{i,k}$ and $d_{i,1}, d_{i,2}, \ldots, d_{i,k}$ using Lagrange interpolation respectively.
(3) Let $a_{i,0}, a_{i,1}, b_{i,0}$ and $b_{i,1}$ be the coefficients of x^0 and x in $f_i(x)$ and $g_i(x)$ respectively.
   - If there exist a common integer r_i which satisfies that $r_ia_{i,0} + b_{i,0} = 0$ and $r_ia_{i,1} + b_{i,1} = 0$, recover the $2k-2$-pixel block $B_i = \{a_{i,0}, a_{i,1}, \ldots, a_{i,k-1}, b_{i,2},_{i,3}, \ldots, b_{i,k-1}\}$, the secret image I is $I = B_1 \parallel B_2 \parallel, \ldots, \parallel B_t$.
   - Else, there are fake shadows participating in image reconstruction; the cheating is detected, output $\perp$.

Notice that in Thien-Lin's scheme, the size on image-shadow is $\frac{1}{k}$ times of the image. In our scheme, the share $v_{i,j} = (m_{i,j}, d_{i,j})$ are generated from each $2k-2$-pixel block; therefore, the size on image-shadow in our scheme is $\frac{2}{2k-2} = \frac{1}{k-1}$ times of image I.

The features of our scheme will be described in following theorems. Theorem 1 proves that our scheme satisfies the property of (k,n) threshold, such that less than k image shadows get no information on secret image; k or more image-shadows are able to recover secret image. In **Scheme 3**, the secret image I is cut into $2k-2$-pixels blocks $B_1, B_2, \ldots, B_t$. Each block is encrypted by the same approach; we only need to prove that the n shares $v_{1,j}, j = 1, 2, \ldots, n$ on block B_1 satisfy the (k,n) threshold property. The property of detect cheating will be analyzed in Theorem 2.

It seems that the relationship between a_0, a_1, b_0, b_1 would leak some information on the secret. However, the following Theorem 1 will prove that $a_0, a_1, b_0, b1$ leak no information about the secret at all, and the proposed scheme is a perfect (k,n) threshold secret image sharing scheme that satisfies the threshold property. The capability of cheating detection of proposed scheme is discussed in Theorem 2.

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

Proof In our scheme, any $2k-2$ pixels in a block B_i are encrypted into n shares $v_{i,j}, j = 1, 2, \ldots, n$ using Shamir's scheme; it is easy to prove that k or more shares can recover all the $2k-2$ pixels in B_i. □

In the following, we will prove that $k-1$ participants are unable to get any information of the $2k-2$ pixels. Since in the proposed scheme, $a_{i,0}, a_{i,1}, b_{i,0}, b_{i,1}$ have the relationships that $r_i a_{i,0} + b_{i,0} = 0$ and $r_i a_{i,1} + b_{i,1} = 0$, it seems that the method of exhaustion could resolve the $2k-2$ pixels. We describe the method of exhaustion below.

(1) all $k-1$ participants use all possible shares on the k-th participant and generates $p = 251$ corresponding interpolation polynomials $f_i^u(x), u = 1, 2, \ldots, 251$ and $g_j^u(x), u = 1, 2, \ldots, 251$.

(2) If $f_i^{u^*}(x)$ and $g_i^{v^*}(x)$ satisfy $r_i a_0^{'} + b_0^{'} = 0$ and $r_i a_1^{'} + b_1^{'} = 0$ where $a_0^{'}, b_0^{'}, a_1^{'}, b_1^{'}$ are coefficients of x^0, x in $f_i^{u^*}(x)$ and $g_j^{v^*}(x)$. Then $f_i^{u^*}(x)$ and $g_i^{v^*}(x)$ would be the original polynomials selected by dealer, and all the $2k-2$ pixels can be gotten from $f_i^{u^*}(x)$ and $g_i^{v^*}(x)$.

Assume that $m^*(k)$ is the share of k-th participant that is randomly selected, then the $k-1$ participants generates a $k-1$-th degree polynomial $f_i(x)$ from $(1, m_1), (2, m_2), \ldots, (k-1, m_{k-1}), \left(k, m_k^*\right)$. Let $a_0^{'}, a_1^{'}$ be the corresponding coefficients in $f_i(x)$. According to the method of exhaustion described previously, if there exists a $k-1$-th degree polynomial $g_j(x) = b_0^{'} + b_1^{'}x +, \ldots, + b_{k-1}^{'}x^{k-1}$ which is interpolated by $(1, d_1), (2, d_2), \ldots, (k-1, d_{k-1}), \left(k, d_k^*\right)$, satisfies that $r^{'}a_0^{'} + b_0^{'} = 0, r^{'}a_1^{'} + b_1^{'} = 0$ ($r^{'}$ could be any value in $GF(251)$), then $f_i(x)$ and $g_i(x)$ are the two polynomials selected by the dealer. $b_0^{'}, b_1^{'}, \ldots, b_{k-1}^{'}$ and $r^{'}$ can be regarded as $k+1$ unknowns, then $k+1$ linear equations on these unknowns can be established: $g^{'}(i) = d_i, i = 1, 2, \ldots, k-1, r^{'}a_0^{'} + b_0^{'} = 0, r^{'}a_1^{'} + b_1^{'} = 0$. (Here $a_0^{'}, a_1^{'}$ are known to the $k-1$ participants.) Therefore, all the unknowns $b_0^{'}, b_1^{'}, \ldots, b_{k-1}^{'}$ can be obtained from these equations; we can also get the polynomial $g_i(x)$. It means that the $k-1$ participants will find that each possible share could be the valid share of the kth participant. This proves that the approach of exhaustion cannot work in the proposed scheme.

An example is used to show the approach of exhaustion in proposed scheme. Assume $k = 4$ and two polynomials $f(x) = 1 + 3x + 4x^2 + 5x^3$ and $g(x) = 4 + 5x + x^2 + 3x^3$ over $GF(7)$ are chosen by the dealer. It is obvious that $3a_0 + b_0 = 0, 3a_1 + b_1 = 0$. Let $P_1.P_2, P_3, P_4$ be the four participants; the shares of them are P_1: $(m_1 = 6, d_1 = 6)$, P_2: $(m_2 = 0, d_2 = 0)$, P_3: $(m_3 = 6, d_3 = 4)$, and P_4: $(m_4 = 5, d_4 = 1)$. Suppose P_1, P_2, P_3 try to recover secret using approach of exhaustion. As described previously, they can randomly assume the sub-share of P_4: $m_4^* = 0$ and generate an interpolation polynomial $f^{'}(x) = 6 + 2x + 2x^2 + 3x^3$ correspondingly. Then they try each possible sub-share d_4^* of P_4 and verify whether it is fit. For instance, when they use $d_4^* = 2$, the interpolating polynomial is $g^{'}(x) = 3 + x + 2x^3$. The coefficients $a_0^{'}, a_1^{'}, b_0^{'}, b_1^{'}$ satisfy that $3a_0^{'} + b_0^{'} = 0, 3a_1^{'} + b_1^{'} = 0$. Then they get the conclusion that $f^{'}(x), g^{'}(x)$ would be the valid polynomials and $s^{'} = f^{'}(0) = 6$ is the secret. In fact, they recover a wrong secret. End of proof.

The capability of cheating detection in our scheme is analyzed in Theorem 2.

Theorem 2 *Our scheme is able to detect cheating from $k-1$ cheaters.*

Proof Suppose $P_1, P_2, ..., P_k$ participate in secret reconstruction phase and $P_1, P_2, ..., P_{k-1}$ are cheaters. Since cheating detection algorithm is used in each block $B_i, i \in [1, t]$, we only analyze the cheating detection in decoding B_1 in this theorem. Suppose the fake shares from cheaters are $v_i^* = \left(m_i + m_i^*, d_i + d_i^*\right), i = 1, 2, \ldots, k-1$. They can get two polynomials $f^{**}(x) = f(x) + f^*(x), g^{**}(x) = g(x) + g^*(x)$ in ***image reconstruction phase***, where $f^*(x) = a_0^* + a_1^*x + \cdots + a_{k-1}^*x^{k-1}$ and $g^*(x) = b_0^* + b_1^*x + \cdots + b_{k-1}^*x^{k-1}$ are interpolated polynomials on the k points $(1, m_1^*), \left(2, m_2^*\right), \ldots, \left(k-1, m_{k-1}^*\right), (k, 0)$ and $\left(1, d_1^*\right), \left(2, d_2^*\right), \ldots, \left(k-1, d_{k-1}^*\right), (k, 0)$ respectively. Since $f^*(x)$ and $g^*(x)$ can be decided by cheaters exclusively, they can select a random number r^*, and satisfy that $r^*a_0^* + b_0^* = 0, r^*a_1^* + b_1^* = 0$. According to our algorithm, if there exists a common number $r^{'}$, satisfying $r^{'}\left(a_0 + a_0^*\right) + b_0 + b_0^* = 0, r^{'}\left(a_1 + a_1^*\right) + b_1 + b_1^* = 0$, the cheating avoids detection. We can easily observe that the cheating succeeds only when $r^* = r$. As analyzed in **Theorem 1**, these $k-1$ cheaters have no information on r; the possibility of $r^* = r$ is $\frac{1}{251}$. As a result, the successful cheating probability is $\epsilon = \frac{1}{251}$. Since all the pixels are in $GF(251)$, the successful cheating possibility $\epsilon = \frac{1}{251}$ means that our scheme is effective to detect the cheating. End of proof. □

4 Results and discussion

In this part, we use an example to describe the cheating detection using our scheme. Let $(k, n) = (4, 7)$ and the secret image I is divided into t blocks where each block includes $2k-2=6$ secret pixels. Assume the first block B_1 consists of the following 6 pixels: $(57, 68, 90, 231, 42, 89)$, the dealer selects an integer $r_1 = 9$, and generates two $k-1 = 3$-th degree polynomials: $f_1(x) = 57 + 68x + 90x^2 + 231x^3$ and $g_1(x) = 161 + 104x + 42x^2 + 89x^3$, where $57 + 9 * 161 = 0(mod 251), 68 + 9 * 104 = 0(mod 251)$. The $n = 7$ shares from B_1 are $v_{1,1} = (195, 145), v_{1,2} = (142, 245), v_{1,3} = (29, 242), v_{1,4} = (238, 168), v_{1,5} = 147, 55, v_{1,6} = (138, 186), v_{1,7} = (91, 91)$.

Suppose P_1, P_2, P_3, and P_4 participate in image reconstruction and P_1, P_2, P_3 are $k-1 = 3$ cheaters. They submit forged shares $v^*_{1,1} = (105, 87), v^*_{1,2} = (162, 31), v^*_{1,3} = (23, 98)$ in image reconstruction. As a result are two polynomials $f^*_1(x) = 55 + 188x + 105x^2 + 8x^3$ and $g^*(x) = 135 + 167x + 56x^2 + 231x^3$. Since there is no common integer r_1 satisfying that $55r_1 + 135 = 0(mod 251)$ and $188r_1 + 167 = 0(mod 251)$, the cheating is successfully detected.

The cheating detection approach in our scheme is also efficient with other cheating detectable secret sharing schemes. Table 1 shows the comparisons between our scheme and other schemes in cheating detection. When comparing to those cheating detectable secret image sharing schemes [16–19], our scheme achieves much stronger capability. It can detect cheating from up to $k-1$ cheaters, while other schemes work only when there are less than $\frac{k}{2}$ cheaters.

5 Conclusions

In this paper, we consider the well-known cheating problem in polynomial-based (k, n) secret image sharing scheme, 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) secret image sharing scheme with cheating detection under the model of cheating detectable secret sharing scheme. Our scheme is capable of detecting the cheating from up to $k-1$ cheaters with only Lagrange interpolations. In addition, the proposed scheme is based on the landmark Thien-Lin's polynomial-based secret image sharing which can be easily extended into other polynomial-based secret image sharing schemes. The size of shadow in our scheme is only $\frac{1}{k-1}$ times of the secret image, which is almost same as the shadow size in original (k, n) secret image sharing scheme.

Table 1 Comparisons between cheating detectable secret sharing schemes

	Size of share	Capability of detection	
Harn's scheme[10]	$\|V\| = \|S\|$	Fail	
Pieprzyk's scheme[11]	$\|V\| = \|S\|$	1	$\epsilon = \frac{1}{p}$
Sergio's scheme[12]	$\|V\| = 2\frac{\|S\|}{\epsilon}$	$k-1$	$\epsilon = \frac{2}{p}$
Proposed scheme	$\|V\| = \frac{\|S\|}{\epsilon}$	$k-1$	$\epsilon = \frac{1}{p}$

6 Method

In this work, we aim to solve the cheating problem in polynomial-based secret image sharing scheme. Since polynomial-based secret image sharing is extended from traditional secret sharing scheme, we also used a cheating detection algorithm in traditional secret sharing in the field of secret image sharing. The experimental results are generated using Matlab software.

Funding

The research presented in this paper is supported in part by the China National Natural Science Foundation (No. 61502384, 61571360), Shaanxi Science and Technology Coordination and Innovation Project (No. 2016KTZDGY05-09), and the Innovation Project of Shaanxi Provincial Department of Education (No. 17JF023).

Availability of data and materials

Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Authors' contributions

Y-XL contributed in algorithm designing; Q-DS was responsible for experiment and analysis; and C-NY took part in correctness checking. All authors read and approved the final manuscript.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Author details

[1]Department of Computer Science and Engineering, Xi'an University of Technology, Xi'an, China. [2]Department of CSIE, National Dong Hwa University, Hualien County, Taiwan.

Received: 8 March 2018 Accepted: 21 March 2018
Published online: 02 April 2018

References

1. A Shamir, How to share a secret. Commun. ACM. **22**(11), 612–613 (1979)
2. YN Liu, C Cheng, JY Cao, T Jiang, An improved authenticated group key transfer protocol based on secret sharing. IEEE Trans. Comput. **62**(11), 2335–2336 (2013)
3. CC Thien, JC Lin, Secret image sharing. Comput. Graph. **26**(5), 765–770 (2002)
4. CN Yang, YY Chu, A general (k, n) scalable secret image sharing scheme with smooth scalability. J. Syst. Softw. **84**(10), 1726–1733 (2011)
5. YX Liu, CY Yang, PH Yeh, Reducing shadow size in smooth scalable secret image sharing. Secur. Commun. Netw. **7**(12), 2237–2244 (2014)
6. YX Liu, Scalable secret image sharing scheme with essential shadows. Signal Proc. Image Commun. **58**, 49–55 (2017)
7. RZ Wang, Region incrementing visual cryptography. IEEE Signal Proc. Lett. **16**(8), 659–662 (2009)
8. CN Yang, HW Shih, CC 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. CN Yang, YC Lin, CC Wu, in *Proc. IWDW2012, LNCS*. Region in region incrementing visual cryptography scheme, vol. 7809, (2013), pp. 449–463
10. L Harn, C Lin, Detection and identification of cheaters in (t, n) secret sharing scheme. Des. Codes. Crypt. **52**(1), 15–24 (2009)

11. J Pieprzyk, XM Zhang, in *Proceedings of ACISP, LNCS 2384*. Cheating prevention in linear secret sharing. (Springer, Heidelberg, 2002), pp. 121–135
12. C Sergio, P Carles, S German, Secret sharing schemes with detection of cheaters for a general access structure. Des. Codes. Crypt. **25**(2), 175–188 (2002)
13. 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
14. S Obana, in *Proceedings of EUROCRYPT, LNCS 6632*. Almost optimum t-cheater identifiable secret sharing schemes, (2011), pp. 284–302
15. YX Liu, Efficient t-cheater identifiable (k, n) secret sharing scheme for $t \leq \lfloor \frac{k-2}{2} \rfloor$. IET Inf. Secur. **8**(1), 37–41 (2014)
16. CC Lin, WH Tsai, Secret image sharing with steganography and authentication. J. Syst. Softw. **73**, 405–414 (2004)
17. CN Yang, TS Chen, KH Yu, CC Wang, Improvements of image sharing with steganography and authentication. J. Syst. Softw. **80**, 1070–1076 (2007)
18. CC Chang, YP Hsieh, CH Lin, Sharing secrets in stego images with authentication. Pattern Recog. **41**, 3130–3137 (2008)
19. CN Yang, JF Quyang, L Harn, Steganography and authentication in image sharing without party bits. Optics Commun. **285**, 1725–1735 (2012)
20. M Tompa, H Woll, How to share a secret with cheaters. J. Cryptol. **1**(3), 133–138 (1989)