Threshold changeable secret image sharing using bivariate polynomial

YANXIAO LIU (liuyanxiao@xaut.edu.cn)
XI'AN University of Technology https://orcid.org/0000-0002-2507-5143

Ping Wu
XI'AN University of Technology

Qindong Sun
XI'AN University of Technology

Zhili Zhou
Nanjing University of Information Science and Technology

Research

Keywords: secret image sharing, threshold changeable, bivariate polynomial

Posted Date: May 18th, 2020

DOI: https://doi.org/10.21203/rs.3.rs-16037/v2

RESEARCH

Threshold changeable secret image sharing using bivariate polynomial

Liu Yanxiao[1*], Wu Ping[1], Sun Qindong[1] and Zhou Zhili[2]

*Correspondence:
liuyanxiao@xaut.edu.cn
[1]XI'AN University of Technology, XI'AN, China
Full list of author information is available at the end of the article
†Equal contributor

Abstract

In secret image sharing (SIS) scheme, a confidential image is encrypted into multiple shadows, any group of shadows that reaches the threshold can reconstruct the image, otherwise nothing can be reconstructed at all. Most existing SIS schemes have a fixed threshold, however in this work, we consider more complicated cases that the threshold may be adjusted due to the changeable security environment. In this paper, we construct a $(k \leftrightarrow h, n)$ threshold changeable SIS (TCSIS) scheme using bivariate polynomial, which has $h - k + 1$ possible thresholds $k, k + 1, ..., h$. During image reconstruction, each participant can update the his shadow according to the current threshold T only based on his initial shadow. Comparing with previous TCSIS schemes, the proposed scheme achieves unconditional security, and can overcome the information disclosure problem caused by homomorphism.

Keywords: secret image sharing; threshold changeable; bivariate polynomial

1 Introduction

Researching on image and video related secure issues are important in the field of information security, such as image based data hiding [1-3], water marking technologies [4], secure image retrieval [5] or other aspects [6-10]. SIS scheme is an important issue in information security that can protect confidential images among multiple participants. Most SIS schemes satisfy a (k, n) threshold, that an image is encrypted into n shadows, any k or more shadows can reconstruct the image, less than k shadows get nothing. There are two mainly approaches for SIS, visual cryptography based SIS schemes [11-13] and polynomial based SIS schemes [14-16]. Visual cryptography based SIS uses human visual system to recover image, but the shadow size is greatly expanded from original image and the reconstructed image is quality loss; Polynomial based SIS is capable to recover lossless image and the shadow size is reduced from original image, but the computation for image reconstruction is more complicated than visual cryptography based SIS. Many research issues are developed on SIS, such as progressive SIS [17-19], SIS with essential shadows [20][21], SIS with authentication [22].

Most existing SIS schemes consider a single security policy, and the threshold is fixed. However, the security environment for image reconstruction is probably changeable in fact, and therefore it is more reasonable to design a SIS scheme with the capability of threshold changeability. The necessity for threshold changeability includes: (1) the confidential level of secret image changes. (2) the number of total participants varies. (3) the power of adversary increases. (4) information disclosure caused by some malicious participants. The discussion of changing threshold

in traditional secret sharing [23-25] have already been proposed. However, SIS and traditional secret sharing are different, the researches on threshold changeable secret sharing could not be directly copied into TCSIS. In fact, the discussion on TCSIS is not enough, two TCSIS schemes [26][27] have been constructed. In TCSIS scheme [26], there are N possible thresholds $T_1, T_2, ..., T_N$, but extra two-variable one way functions are included for image reconstruction, the computational complexity is greatly increased, and the security is based on the assumption of one-way functions, it is not unconditional secure; the other TCSIS scheme [27] can reduce the computational complexity, but it has only three possible thresholds $(k^{'}, k, k^{''})$. Besides, it requires the dealer involved in shadow updating, and also suffers the problem of information leakage.

In this paper, we construct a $(k \leftrightarrow h, n)$ TCSIS scheme which has $h - k + 1$ possible thresholds $(k, k+1, .., h-1, h)$. Three different secure levels are considered in our scheme, and the advantages of proposed scheme comparing to previous TCSIS schemes are

1. our scheme provides more thresholds than scheme [27].
2. our scheme does not require the dealer involve in changing threshold, that has lower cost than scheme [26][27] reduces the risk of information leakage.
3. our scheme does not adopt one-way functions, it achieves unconditional secure.
4. the computation is only based on polynomial interpolation, which has higher efficiency than previous scheme [26]

The rest of this paper is organized as follows. In next section 2.1, some preliminaries are prepared which includes Thien-Lin's polynomial based (k, n) SIS and some results of previous TCSIS. The motivation and proposed scheme is described in section 2.2 and 2.3. Experimental results and comparisons between proposed scheme and previous TCSIS schemes are shown in section 3. The conclusion of our work is proposed in section 4 at last.

2 Methods

In this section, we describe some related works to TCSIS and introduce the design motivation of our work. The methods of proposed TCSIS scheme is described at last.

2.1 Related works

In this part, the related works are introduced, which consists of polynomial based SIS and the results on previous TCSIS.

2.1.1 Polynomial based (k, n) SIS

In 2002, Thien and Lin proposed a polynomial based (k, n) threshold SIS scheme, which is foundation of later polynomial based SIS schemes. Thien-Lin's (k, n) SIS consists of two phases: ***Shadow Encryption Phase*** and ***Image Reconstruction Phase***. In first phase, a confidential image O is encrypted into n shadows $S_1, S_2, ..., S_n$; during second phase, k or more shadows are able to recover the image O.

Scheme 1: *Thien-Lin's* (k, n) *SIS*

Shadow Encryption Phase:

Input: image O, Output: n shadows $S_1, S_2, ..., S_n$

1 The dealer divides O into l-non-overlapping k-pixel groups, $G_1, G_2, ..., G_l$.
2 For k pixels $p_{j,0}, p_{j,1}, ..., p_{j,k-1}$ in each group $G_j, j \in [1, l]$, the dealer builds a $k-1$ degree polynomial $f_j(x) = p_{j,0} + p_{j,1}x + p_{j,2}x^2 + ..., +p_{j,k-1}x^{k-1}$.
3 Computing n sub-shadows, $s_{j,1} = f_j(1), s_{j,2} = f_j(2), ..., s_{j,n} = f_j(n), j \in [1, l]$.
4 Outputs n shadows $S_i = s_{1,i} \parallel s_{2,i} \parallel, ..., \parallel s_{l,i}, i = 1, 2, ..., n$.

Image Reconstruction Phase:

Input: m shadows $S_1, S_2, ..., S_m.(m \geq k)$. Outputs: secret image O.

1 Reconstructing $f_j(x)$ from $s_{1,j}, s_{2,j}, ..., s_{m,j}, j \in [1, l]$ using Lagrange interpolation:

$$f_j(x) = \sum_{i=1}^{m} [s_{i,j} * \prod_{w=1, w \neq i}^{m} \frac{x-w}{i-w}] \tag{1}$$

then the block G_j is recovered from all k coefficients in $f_j(x)$.
2 Outputs $O = G_1 \parallel G_2 \parallel, ..., \parallel G_l$.

2.1.2 Results on TCSIS

In this part, we give a definition on TCSIS and then describe some results on previous TCSIS schemes.

The model of TCSIS scheme consists of two phases: ***Shadow Encryption Phase*** and ***Image Reconstruction Phase***, which have the following steps in detail.

Shadow Encryption Phase

1 A dealer encrypts a confidential image O into initial shadows $S_1, S_2, ..., S_n$.
2 Each initial shadow S_i is sent to participant $\mathcal{P}_i$ through secure channel.

Image Reconstruction Phase

1 Selecting a threshold T from the set of all possible thresholds $T_1, T_2, ..., T_d$.
2 Each participant $\mathcal{P}_i$ updates the shadow according to current threshold T.
3 Any group of participants that satisfy the access structure can reconstruct the image O using updated shadows.

The difference between SIS model and TCSIS model is that during ***Image Reconstruction Phase***, each participant needs to update the shadow according to the current threshold T.

The previous TCSIS schemes [26][27] are both practical scheme that can change threshold for image reconstruction according to different security levels. Both the two schemes can provide three security levels and the threshold can be adjusted efficiently. The scheme [26] is a polynomial based scheme that satisfies the model of TCSIS, however some one-way functions are adopted in [26] to changing threshold. Therefore the security of [26] is based on the security assumption of those one-way functions, and the computational complexity is much higher than the computation in polynomial interpolation. The TCSIS scheme [27] can reduce computational complexity from [26], but there are only three possible thresholds and the dealer has to involve in shadow updating, which is not reasonable. Besides, the problem of information leakage would be caused in [27] due to the property of homomorphism.

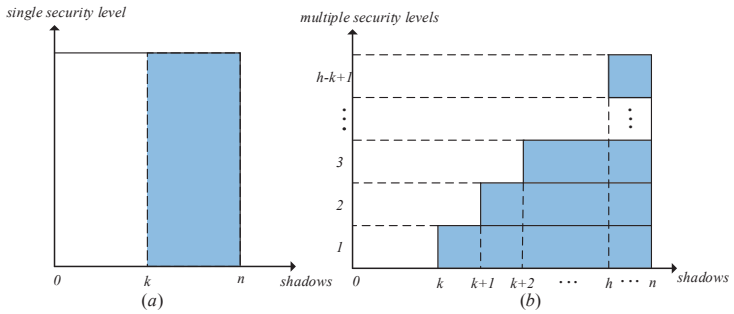

Figure 1 Thresholds for different schemes: (a) (k, n) SIS scheme (b) $(k \leftrightarrow h, n)$ TCSIS scheme

2.2 Aim and design motivation

In real applications, security conditions are probably changeable after dealer sends shadows in a SIS scheme to all participants. In this work, we assume there more multiple security levels for image reconstruction. For instance, a confidential image should be reconstructed immediately due to emergency cases such as medical or traffic. However, the number of available participants does not satisfy the access structure for image reconstruction, it would cause loss or even loss of life. Therefore a SIS with capability of changing threshold is more reasonable since it can reconstruct image under multiple security levels. The design concept of our work can be shown in Fig.1.

2.3 Proposed TCSIS using bivariate polynomial

In this part, we describe our $(k \leftrightarrow h, n)$ TCSIS using bivariate polynomial, which has $h - k + 1$ possible thresholds $\{k, k+1, ..., h\}$.

Scheme 2: $(k \leftrightarrow h, n)$ TCSIS

Shadow Encryption Phase:

1 The dealer $\mathcal{D}$ divides O into l non-overlapping kh-pixel groups, $G_1, G_2, ..., G_l$.

2 For kh pixels $\begin{cases} p_{0,0}, p_{0,1}, ..., p_{0,h-1}, \\ p_{1,0}, p_{1,1}, ..., p_{1,h-1}, \\ ... \\ p_{k-1,0}, p_{k-1,1}, ..., p_{k-1,h-1} \end{cases}$ in each block $G_r, r \in [1, l]$, $\mathcal{D}$ builds a bivariate polynomial:

$$F_r(x, y) = \begin{cases} p_{0,0} + p_{0,1}y +, ..., +p_{0,h-1}y^{h-1}, \\ p_{1,0}x + p_{1,1}xy +, ..., +p_{1,h-1}xy^{h-1}, \\ ... \\ p_{k-1,0}x^{k-1} + p_{k-1,1}x^{k-1}y +, ..., +p_{k-1,h-1}x^{k-1}y^{h-1} \end{cases} \quad (2)$$

3 For each each block G_r in $\{G_1, G_2, ..., G_l\}$, $\mathcal{D}$ computes $f_{r,i}(y) = F_r(i, y), g_{r,i}(x) = F_r(x, i)$. The sub-shadow $s_{i,r}$ for $\mathcal{P}_i$ is $s_{i,r} = (f_{r,i}(y), g_{r,i}(x))$.

3 The initial shadow S_i for each participant $\mathcal{P}_i$ is $S_i = s_{i,1}||s_{i,2}||...||s_{i,l}$.

Image Reconstruction Phase:

1 Selecting a threshold T from the set $\{k, k+1, ..., h\}$.

(a) If current threshold is $T = k$, each participant $\mathcal{P}_i$ updates his sub-shadows by $s^k_{i,r} = f_{r,i}(y), r = 1, 2, ..., l$, then the updated shadow is $S^k_i = s^k_{i,1}||s^k_{i,2}||...||s^k_{i,l}$.

(b) If current threshold is $T = h$, each participant $\mathcal{P}_i$ updates his sub-shadows by $s^h_{i,r} = g_{r,i}(x), r = 1, 2, ..., l$, then the updated shadow is $S^h_i = s^h_{i,1}||s^h_{i,2}||...||s^h_{i,l}$.

(c) If current threshold T satisfies $k < T < h$, the participants select $h - T + 1$ integers $e_1, e_2, ..., e_{h-T+1}$ other than $1, 2, ..., n$. Each participant $\mathcal{P}_i$ computes $f_{r,i}(e_1), f_{r,i}(e_2), ..., f_{r,i}(e_{h-T+1}), r = 1, 2, ..., l$, and the updated shadow S^T_i is:

$$\begin{aligned} S^T_i = \; & S^h_i||(f_{1,i}(e_1), f_{1,i}(e_2), ..., f_{1,i}(e_{h-T+1})) \\ & ||(f_{2,i}(e_1), f_{2,i}(e_2), ..., f_{2,i}(e_{h-T+1})) \\ & ||... \\ & ||(f_{l,i}(e_1), f_{l,i}(e_2), ..., f_{l,i}(e_{h-T+1})) \end{aligned}$$

2 The any group of T participants can reconstruct original image O using Lagrange Interpolation.

The thresholds for image reconstructions in our proposed scheme are analyzed in following theorems. Without loss of generality, we only describe the thresholds on the first kh-block G_1 from different shadows. Since each shadow consists of similar information on each block $G_i, i = 1, 2, ..., l$, the threshold for G_1 is identical to the entire image $O = G_1||G_2||...||G_l$.

Theorem 1 *The threshold T for updated shadows $\mathcal{S}^k_1, \mathcal{S}^k_2, ...\mathcal{S}^k_n$ on G_1 is $T = k$.*

Proof The sub-shadow in $\mathcal{S}^k_i$ for G_1 is $s^k_{i,1} = f_{1,i}(y) = F_1(i, y)$. $F_1(x, y)$ in Eq.(2) can be rewrote as:

$$F_1(x, y) = u_0(x) + u_1(x)y + u_2(x)y^2 +, ..., +u_{h-1}(x)y^{h-1} \tag{3}$$

where $u_0(x), u_1(x), ..., u_{h-1}(x)$ are all $k-1$ degree univariate polynomials. Suppose that

$$s^k_{i,1} = F_1(i, y) = b_{i,0} + b_{i,1}y +, ..., b_{i,h-1}y^{h-1}, i = 1, 2, ..., n \tag{4}$$

Comparing E.q.(3) E.q.(4), we can observe that $(b_{1,0}, b_{2,0}, ..., b_{n,0})$ are interpolations on $u_0(x)$ that $b_{i,0} = u_0(i), i = 1, 2, ..., n$. Since $u_0(x)$ is $k-1$ degree polynomial, the threshold on $(b_{1,0}, b_{2,0}, ..., b_{n,0})$ to reconstruct $u_0(x)$ is k, and the reconstruction can be executed using Lagrange Interpolation E.q.(1). Because each $b_{i,0}$ comes from sub-shadow $s^k_{i,1}$, the threshold on $(s^k_{1,1}, s^k_{2,1}, ..., s^k_{n,1})$ for $u_0(x)$ is k. By the same way, the threshold for the other polynomials $u_1(x), u_2(x), ..., u_{h-1}(x)$ on $(s^k_{1,1}, s^k_{2,1}, ..., s^k_{n,1})$ are also k. In sum, the threshold for the kh-pixel block G_1 from $(\mathcal{S}^k_1, \mathcal{S}^k_2, ..., \mathcal{S}^k_n)$ is $T = k$. □

Theorem 2 *The threshold T for updated shadows $\mathcal{S}^h_1, \mathcal{S}^h_2, ...\mathcal{S}^h_n$ is $T = h$.*

Proof The sub-shadow in $\mathcal{S}_i^h$ for G_1 is $s_{i,1}^h = g_{1,i}(x) = F_1(x,i)$. $F_1(x,y)$ in Eq.(2) can be rewrote as:

$$F_1(x,y) = v_0(y) + v_1(y)x + v_2(y)x^2 +, ..., +v_{k-1}(y)x^{k-1} \tag{5}$$

where $v_0(y), v_1(y), ..., v_{k-1}(y)$ are all $h-1$ degree univariate polynomials. Suppose that

$$s_{i,1}^h = F_1(x,i) = c_{i,0} + c_{i,1}x +, ..., c_{i,k-1}x^{k-1}, i = 1, 2, ..., n \tag{6}$$

Comparing E.q.(5) E.q.(6), we can observe that $(c_{1,0}, c_{2,0}, ..., c_{n,0})$ are interpolations on $v_0(y)$ that $c_{i,0} = v_0(i), i = 1, 2, ..., n$. Since $v_0(y)$ is $h-1$ degree polynomial, the threshold on $(c_{1,0}, c_{2,0}, ..., c_{n,0})$ to reconstruct $v_0(y)$ is h, and the reconstruction can be executed using Lagrange Interpolation E.q.(1). Because each $c_{i,0}$ comes from sub-shadow $s_{i,1}^h$, the threshold on $(s_{1,1}^h, s_{2,1}^h, ..., s_{n,1}^h)$ for $v_0(y)$ is h. By the same way, the threshold for the other polynomials $v_1(y), v_2(y), ..., v_{k-1}(y)$ on $(s_{1,1}^h, s_{2,1}^h, ..., s_{n,1}^h)$ are also h. In sum, the threshold for the kh-pixel block G_1 from $(\mathcal{S}_1^h, \mathcal{S}_2^h, ..., \mathcal{S}_n^k)$ is $T = h$. □

Theorem 3 *The threshold on updated shadows* $(\mathcal{S}_1^T, \mathcal{S}_2^T, ..., \mathcal{S}_n^T)$ *when* $k < T < h$ *is* T.

Proof The sub-shadow in $\mathcal{S}_i^T$ for G_1 is $s_{i,1}^T = s_{i,1}^h || (f_{1,i}(e_1), f_{1,i}(e_2), ..., f_{1,i}(e_{h-T}))$. Without loss of generality, there are T sub-shadows $s_{1,1}^T, s_{2,1}^T, ..., s_{T,1}^T$ on G_1. Since $f_{1,i}(e_j) = F_1(i, e_j)$, $f_{1,i}(e_j)$ is an interpolation on $g_{e_j}(x) = F_1(x, e_j)$. On the other hand, $T > k$ and $g_{e_j}(x)$ is of degree $k-1$, it can be reconstructed from $f_{1,i}(e_j), i = 1, 2, ..., T$. As a result, $F_1(x, e_j), F_1(x, e_2), ..., F_1(x, e_{h-T})$ can be reconstructed from T sub-shadows $s_{1,1}^T, s_{2,1}^T, ..., s_{T,1}^T$. According to E.q.(5), $F_1(x, e_j), j = 1, 2, ..., h-T$ can be presented as:

$$F_1(x, e_j) = v_0(e_j) + v_1(e_j)x + v_2(e_j)x^2 +, ..., +v_{k-1}(e_j)x^{k-1} \tag{7}$$

Therefore, $h - T$ extra Interpolations can be obtained on each polynomial in $v_0(y), v_1(y), ..., v_{k-1}(y)$. On the other hand, other T Interpolations can be obtained from $s_{1,1}^h, s_{2,1}^h, ..., s_{T,1}^h$, there are totally $h - T + T = h$ Interpolations on each polynomial $v_0(y), v_1(y), ..., v_{k-1}(y)$. Then $F_1(x,y)$ can be reconstructed. When there are $T-1$ or less shadows, at most $h-1$ interpolations can be gathered on $v_0(y), v_1(y), ..., v_{k-1}(y)$, $F_1(x,y)$ cannot be reconstructed. In sum, the threshold for the kh-pixel block G_1 from $(\mathcal{S}_1^T, \mathcal{S}_2^T, ..., \mathcal{T}_n^k)$ when $k < T < h$ is T. □

3 Results

In this section, we use the results of experiments and comparisons to show the advantages of proposed scheme.

3.1 Experiments

In this part, we use examples and experimental results to show the performance of proposed scheme, and then gives comparison between proposed scheme and previous TCSIS schemes.

Suppose the secret image is
$O = (97, 46, 253, 12, 165, 19, 247, 251, 214, 142, 191, 180, 210, 172, 152)$.
We construct a proposed $(3 \leftrightarrow 5, 7)$ TCSIS on this image. Our proposed scheme is based on the computation over a $GF(P)$, here $P = 251$ and $P = 2^8$ are adopted in our examples. When using $P = 251$, all pixels that larger than 250 are transformed to 250 instead, and the computation is over $mod(251)$, therefore the reconstructed image is quality-loss from the original image; when using $P = 2^8$, no distortion would be caused from reconstructed image, but each pixel needs to be transferred into a polynomial, and the computation is over $mod(x^8 + x^4 + x^3 + x + 1)$, which is much more complicated than the computation in $mod(251)$.

Example 1: Proposed $(3 \leftrightarrow 5, 7)$ TCSIS on O over $GF(251)$.

First the original image O is transformed into image $O^{'}$ where the pixels larger than 250 is transformed to 250. Then we get
$O^{'} = (97, 46, 250, 12, 165, 19, 247, 250, 214, 142, 191, 180, 210, 172, 152)$.
Next, a bivariate $F(x, y)$ with degree 2 on x and degree 4 on y is constructed based on $O^{'}$.

$$F(x,y) = \begin{cases} 97 + 46y + 250y^2 + 12y^3 + 165y^4, \\ 19x + 247xy + 250xy^2 + 214xy^3 + 142xy^4, \\ 191x^2 + 180x^2y + 210x^2y^2 + 172x^2y^3 + 152x^2y^4 \end{cases} \tag{8}$$

Then the dealer computes $f_i(y) = F(i, y), g_i(x) = F(x, i), i = 1, 2, ..., 7$ over $GF(251)$, the initial shadow $\mathcal{S}_i = (f_i(y), g_i(x))$ is sent to each participant $P_i, i = 1, 2, ..., 7$ confidentially. The initial shadows $\mathcal{S}_1, \mathcal{S}_2, ..., \mathcal{S}_7$ are listed in Eq(9).

$$\begin{cases} \mathcal{S}_1 : f_1(y) = 56 + 222y + 208y^2 + 147y^3 + 208y^4, g_1(x) = 68 + 119x + 152x^2 \\ \mathcal{S}_2 : f_2(y) = 146 + 5y + 84y^2 + 124y^3 + 53y^4, g_2(x) = 160 + 226x + 179x^2 \\ \mathcal{S}_3 : f_3(y) = 116 + 148y + 129y^2 + 194y^3 + 202y^4, g_3(x) = 110 + 210x + 250x^2 \\ \mathcal{S}_4 : f_4(y) = 217 + 149y + 92y^2 + 106y^3 + 153y^4, g_4(x) = 101 + 86x + 226x^2 \\ \mathcal{S}_5 : f_5(y) = 198 + 8y + 224y^2 + 111y^3 + 157y^4, g_5(x) = 9 + 14x + 102x^2 \\ \mathcal{S}_6 : f_6(y) = 59 + 227y + 23y^2 + 209y^3 + 214y^4, g_6(x) = 156 + 48x + 7x^2 \\ \mathcal{S}_7 : f_7(y) = 51 + 53y + 242y^2 + 149y^3 + 73y^4, g_7(x) = 55 + 136x + 204x^2 \end{cases} \tag{9}$$

During image reconstruction, suppose the threshold is T, and $P_1, P_2, .., P_T$ are involved.

1 If $T = 3$, P_1, P_2, P_3 publishes $S_i^3 = f_i(y), i = 1, 2, 3$, all coefficients in $F(x, y)$ can be computed using Lagrange interpolation according to Theorem 1, then the image $O^{'}$ can be reconstructed.

2 If $T = 4$, P_1, P_2, P_3, P_4 publish $S_i^4 = g_i(x)||f_i(e_1), i = 1, 2, 3, 4$. Here $e_1 = 8$. The interpolation polynomial on $f_i(e_1), i = 1, 2, 3, 4$ is $g_{e_1}(x) = F(x, e_1) = 167 + 120x + 86x^2$ for Example 1. Then, all coefficients in $F(x, y)$ can be computed using Lagrange interpolation according to Theorem 3, then the image $O^{'}$ can be reconstructed.

3 If $T = 5$, $P_1 - P_5$ publish $S_i^5 = g_i(x), i = 1, 2, ..., 5$, all coefficients in $F(x, y)$ can be computed using Lagrange interpolation according to Theorem 1, then the image $O^{'}$ can be reconstructed.

Example 2: Proposed $(3 \leftrightarrow 5, 7)$ TCSIS on O over $GF(2^8)$.

A bivariate $F(x, y)$ with degree 2 on x and degree 4 on y is constructed based on O as follows.

$$F(x,y) = \begin{cases} 97 + 46y + 253y^2 + 12y^3 + 165y^4, \\ 19x + 247xy + 251xy^2 + 214xy^3 + 142xy^4, \\ 191x^2 + 180x^2y + 210x^2y^2 + 172x^2y^3 + 152x^2y^4 \end{cases} \tag{10}$$

Then the dealer computes $f_i(y) = F(i, y), g_i(x) = F(x, i), i = 1, 2, ..., 7$ over $GF(2^8)$, the initial shadow $\mathcal{S}_i = (f_i(y), g_i(x))$ is sent to each participant $P_i, i = 1, 2, ..., 7$ confidentially. The initial shadows $\mathcal{S}_1, \mathcal{S}_2, ..., \mathcal{S}_7$ are listed in Eq(11).

$$\begin{cases} \mathcal{S}_1 : f_1(y) = 205 + 109y + 212y^2 + 118y^3 + 179y^4, g_1(x) = 27 + 71x + 237x^2 \\ \mathcal{S}_2 : f_2(y) = 141 + 61y + 117y^2 + 61y^3 + 244y^4, g_2(x) = 58 + 245x + 253x^2 \\ \mathcal{S}_3 : f_3(y) = 33 + 126y + 92y^2 + 71y^3 + 226y^4, g_3(x) = 104 + 99x + 106x^2 \\ \mathcal{S}_4 : f_4(y) = 40 + 106y + 179y^2 + 87y^3 + 232y^4, g_4(x) = 168 + 119x + 50x^2 \\ \mathcal{S}_5 : f_5(y) = 132 + 41y + 154y^2 + 45y^3 + 254y^4, g_5(x) = 34 + 153x + 200x^2 \\ \mathcal{S}_6 : f_6(y) = 196 + 121y + 59y^2 + 102y^3 + 185y^4, g_6(x) = 168 + 219x + 2x^2 \\ \mathcal{S}_7 : f_7(y) = 104 + 58y + 18y^2 + 28y^3 + 175y^4, g_7(x) = 10 + 247x + 61x^2 \end{cases} \tag{11}$$

The reconstruction with different thresholds are similar as Example 1. Here we only emphsize that when the threshold is $T = 4$, the participants can decide $e_1 = 8$, and compute $g_{e_1}(x) = 13 + 248x + 98x^2$ in $GF(2^8)$, which is different from the $g_{e_1}(x)$ in Example 1.

The following Fig.2 shows the experimental results of proposed $(5 \leftrightarrow 7, 9)$ over $GF(251)$, where original image and initial shadows are included.

3.2 Comparison and discussion

In this part, we give the discussion of comparisons between proposed TCSIS with previous two TCSIS schemes [26] and [27] in detail. First we illustrate the information disclosure problem of scheme [27]. The initial shadows S_i for each participant P_i in [27] is generated from a $k-1$ degree polynomial $F_i^*(x) = F(x) + f_i(x)$, where $F(x)$ is of degree $k-1$, $f_i(x)$ is of degree $k^{'}-1$, and $f_i(x)$ contains the pixels of secret image O. When the threshold is $k^{'}$, each participant P_i modifies his initial shadow by $S_i^{'} = S_i - F(i)$, thus the threshold of updated shadows is reduced to $k^{'}$ from k. However, any $k^{'}$ participants can recover a distortion image

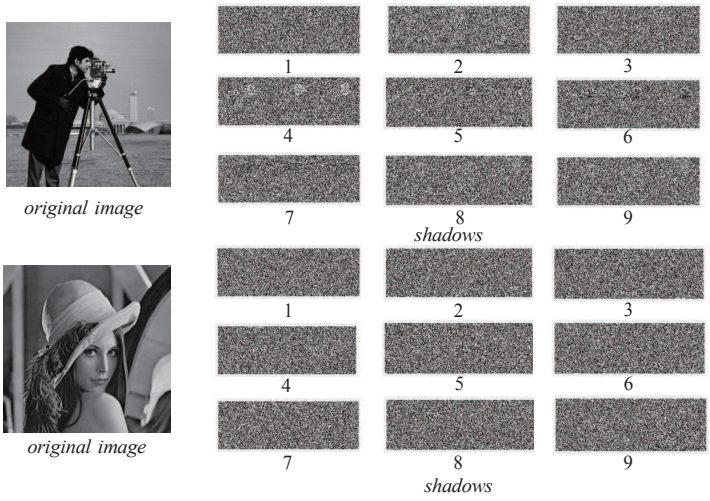

Figure 2 Original images and shadows using proposed scheme

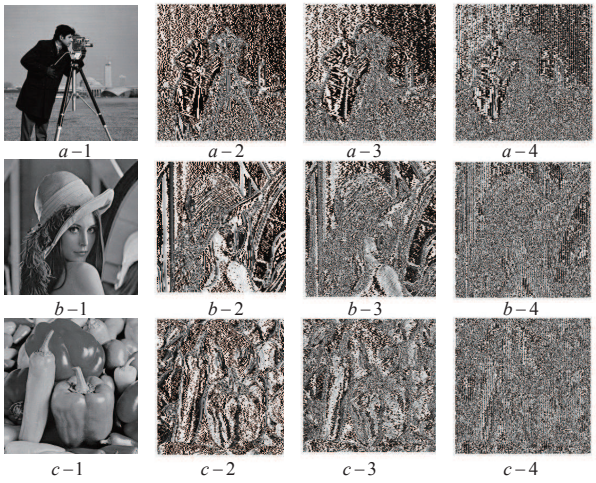

Figure 3 (a-1,b-1,c-1): original images, (a-2,b-2,c-2): quality lossy images with $(k^{'} = 2, k = 3)$, (a-3,b-3,c-3): quality lossy images with $(k^{'} = 3, k = 4)$, (a-4,b-4,c-4): quality lossy images with $(k^{'} = 4, k = 5)$

without updating their shadows, based on the homm, $S_i - S_j$ is generated from $F_i^*(x) - F_j^*(x) = f_i(x) - f_j(x)$. Since $f_i(x) - f_j(x)$ is of degree $k^{'} - 1$, any $k^{'}$ participants can recover $f_i(x) - f_j(x)$. As a result, a distortion image can be recovered from the pixel information in $f_i(x) - f_j(x)$. The experimental results of information disclosure problem in [26] are shown in Fig.3.

The proposed TCSIS scheme generates initial shadows using bivariate polynomial $F(x, y)$, where image pixels are hidden in all coefficients in $F(x, y)$. Thus the proposed scheme avoids such information disclosure problem in [27]. On the other hand, the scheme [27] only provides three potential thresholds $k^{'}, k, k^{''}$ for low, media and high security levels, and our scheme can provide $h - k + 1$ thresholds

Table 1 Comparisons of three TCSIS schemes

Approach	Thresholds	Threshold update	Security level	Computation	Shadow size
[27]	$k^{'}, k, k^{''}$	Dealer involve	Uncondition	Interpolation	$\frac{1}{k^{'}}$
[26]	$T_1, T_2, ..., T_N$	Dealer involve	Conditional	Hash	$\frac{N}{T_N}$
Proposed	$k, k+1, ..., h$	Without dealer	Uncondition	Interpolation	$\frac{k+h}{kh}$

$k, k+1, k+2, ..., h$ to satisfy more complicated security requirements. The previous scheme [26] can also provides more thresholds than scheme [27], but there are two weaknesses of scheme [26]. One is that the dealer needs to publish necessary information when changing threshold, the participation of dealer in this process would not only reduces the efficiency of image reconstruction, but also brings risk of information leakage from the communication between dealer and participants. Such problem also exists in the scheme [27]. The other problem in [26] is that the security is based on the security assumption on two-verifiable one way functions, it is not unconditional secure. In addition, the computation in one way functions is much more complicated than the computation of polynomial interpolation. The comparisons between proposed scheme and previous TCSIS schemes [26][27] is listed in Tab.1.

4 Conclusion

In this paper, we construct a $(k \leftrightarrow h, n)$ TCSIS scheme based on bivariate polynomial, that provides three secure levels for image reconstruction and $h-k+1$ potential thresholds to choose. Comparing with previous TCSIS schemes, our scheme provides more possible thresholds and the most important improvement is that the dealer is not required to participate in shadow update, which greatly improves the security of proposed scheme.

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

Acknowledgements
We want to thank Professor Chingnung Yang from National DongHwa University for his help of English improvement.

Abbreviations
SIS: secret image sharing; TCSIS: threshold changeable secret image sharing.

Authors' contributions
Yanxiao Liu provides the main concept, Ping Wu and Qindong Sun design the algorithms and Zhili Zhou gives the experiments and comparisons.

Funding
The research presented in this paper is supported in part by the National Natural Science Foundation (No.: 61571360), the Youth Innovation Team of Shaanxi Universities, the Innovation Project of Shaanxi Provincial Department of Education (No.17JF023), and the Shaanxi Provincial Natural Science Basic Project (No.2019JQ-736), and Xi'an Science and technology plan projects GXYD14.12 and GXYD14.13.

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

Author details
[1]XI'AN University of Technology, XI'AN, China. [2]Nanjing University of Information Science and Technology, Nanjing, China.

References

1. Chan C.K., Cheng L.M., Hiding data in image by simple LSB substitution, Pattern Recognition, vol.37, no.3, pp.469-474, 2004.
2. Xiao D., Liang J., Ma Q.Q., Xiang Y.P., Zhang Y.S., High capacity data hiding in encrypted image based on compressive sensing for nonequivalent resources, Computers, Materials & Continua, vol.58, no.1, pp.1-13, 2019.
3. Zhou Z.L.,?Mu Y., Wu Q.M. Jonathan, Coverless image steganography using partial-duplicate image retrieval, Soft Computing, vol.23, no.13, pp.4927-4938, 2019.
4. Liu J., Li J.B., Cheng J.R., Ma J.X,, Sadiq N., Han B.R., Geng Q., Ai Y., A novel robust watermarking algorithm for encrypted medical image based on DTCWT-DCT and chaotic map, Computers, Materials & Continua, vol.61, no.2, pp.889-910, 2019.
5. Yan C., Gong B., Wei Y., Gao Y. Deep multi-view enhancement hashing for image retrieval, IEEE Transactions on Pattern Analysis and Machine Intelligence, 2020, DOI: 10.1109/TPAMI.2020.2975798.
6. Wang J.W., Wang H., Li J., Luo X.Y., Shi Y.Q., Jha Sunil Kr., Detecting double JPEG compressed color images with the same quantization matrix in spherical coordinates, IEEE Transactions on Circuits and Systems for Video Technology, DOI: 10.1109/TCSVT.2019.2922309.
7. Zhou Z.L., Wu Q.M. Jonathan, Sun X.M., Multiple distances-based coding: toward scalable feature matching for large-scale web image search, IEEE Transactions on Big Data. DOI: 10.1109/TBDATA.2019.2919570. 2019.
8. Qin C., Chen X.Q., Ye D.P., Wang J.W., Sun X.M., A Novel image hashing scheme with perceptual robustness using block truncation coding, Information Sciences, vol.361-362, pp.84-99, 2016.
9. Yan C., Shao B., Zhao H., Ning R., Zhang Y., Xu F. 3D Room layout estimation from a single RGB image, IEEE Transactions on Multimedia, 2020, DOI: 10.1109/TMM.2020.2967645.
10. Yan C., Tu Y., Wang X., et.al. STAT: spatial-temporal attention mechanism for video captioning, IEEE Transactions on Multimedia, vol.22, no.1, pp.229-241, 2019.
11. Naor M, Shamir A. Visual cryptography. Proc. Eurocrypt94, LNCS, vol.950, pp.1-12, 1995.
12. Wang R.Z. Region incrementing visual cryptography. IEEE Signal Processing Letters, vol.16, no.8, pp.659-662, 2009.
13. Yang C.N, Shih H.W, Wu C.C, Harn L. k out of n region incrementing scheme in visual cryptography. IEEE Transactions on Circuits and Systems for Video Technology, vol.22, no.5, pp.799-809, 2012.
14. Thien C.C, Lin J.C. Secret image sharing. Computers and Graphics, vol.26, no.5, pp.765-770, 2002.
15. Wang R.Z, Shyu S.J. Scalable secret image sharing. Signal Processing:. Image Communication, vol.22, no.4, pp.363-373, 2007.
16. Liu Y.X, Yang C.Y, Yeh P.H. Reducing shadow size in smooth scalable secret image sharing. Security and Communication Networks, vol.7, no.12, pp.2237-2244, 2014.
17. Wang Z.H, Di Y.F, Li J.J, Chang C.C, Liu H. Progressive secret image sharing scheme using meaningful shadows. Security and Communication Networks, vol.9, no.17, pp.4075-4088, 2016.
18. Yan X.H, Wang S, Niu X.M. Threshold progressive visual cryptography construction with unexpanded shares. Mutimedia Tools and Applications, vol.75, no.14, pp.8657-8674, 2016.
19. Liu Y.X., Yang C.N., Wu S.Y., Chou Y.S. Progressive (k, n) secret image sharing schemes based on Boolean operations and covering codes. Signal Processing: Image Communication, vol.66, pp.77-86, 2018.
20. Liu Y.X, Yang C.N. Scalable secret image sharing scheme with essential shadows. Signal Processing: Image Communication, vol.58, pp.49-55, 2017.
21. He Q.,, Yu S.,, Xu H.F., Liu J., Huang D.M., Liu G.H., Xu F.Q., Du Y.L. A weighted threshold secret sharing scheme for remote sensing images based on Chinese remainder theorem. Computers, Materials & Continua, vol.58, no.2, pp.349-361, 2019.
22. Yang C.N, Ouyang J.F, Harn L. Steganography and authentication in image sharing without parity bits. Optics communications, vol.285, no.7, pp.1725-1735, 2012.
23. Zhang Z, Chee Y.M, Ling S, Liu M, Wang H. Threshold changeable secret sharing schemes revisited. Theoretical Computer Science, vol.418, pp.106-115, 2012.
24. Steinfeld R, Pieprzyk J, Wang H.X. Lattice-based threshold-changeability for standard crt secret- sharing schemes. Finite Fields and Their Applications, vol.12, no.4, pp.653-680, 2006.
25. Harn L, Hsu C.F. Dynamic threshold secret reconstruction and its application to the threshold cryptography. Information Processing Letters, vol.115, no.11, pp.851-857, 2015.
26. Yuan L.F, Li M.C, Guo C, Hu W.T, Luo X.J. Secret image sharing scheme with threshold changeable capability, Mathematical Problems in Engineering, vol.2016, pp.1-11, 2016.
27. Liu Y.X., Yang C.N., Wu C.M., Sun Q.D., Bi W. Threshold changeable secret image sharing scheme based on interpolation polynomial. Multimedia Tools and Applications, vol.78, no.13, pp.18653-18667, 2019.

Figures

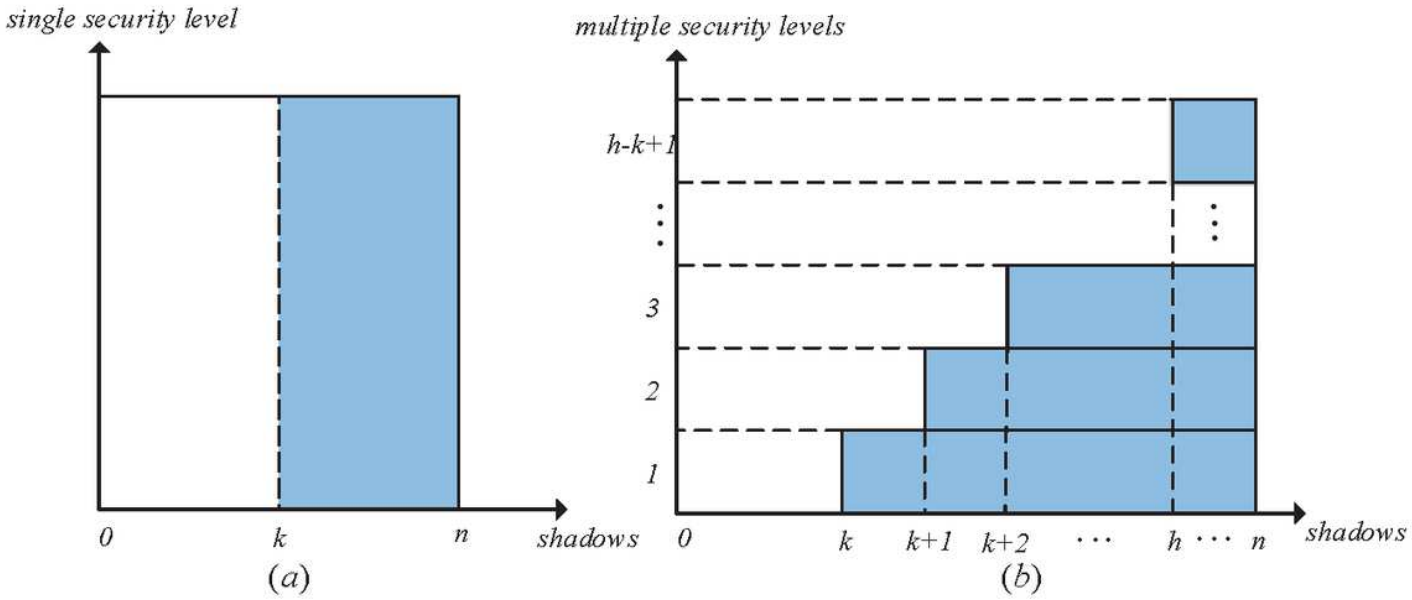

Figure 1

Thresholds for different schemes: (a) (k, n) SIS scheme (b) (k <–> h, n) TCSIS scheme

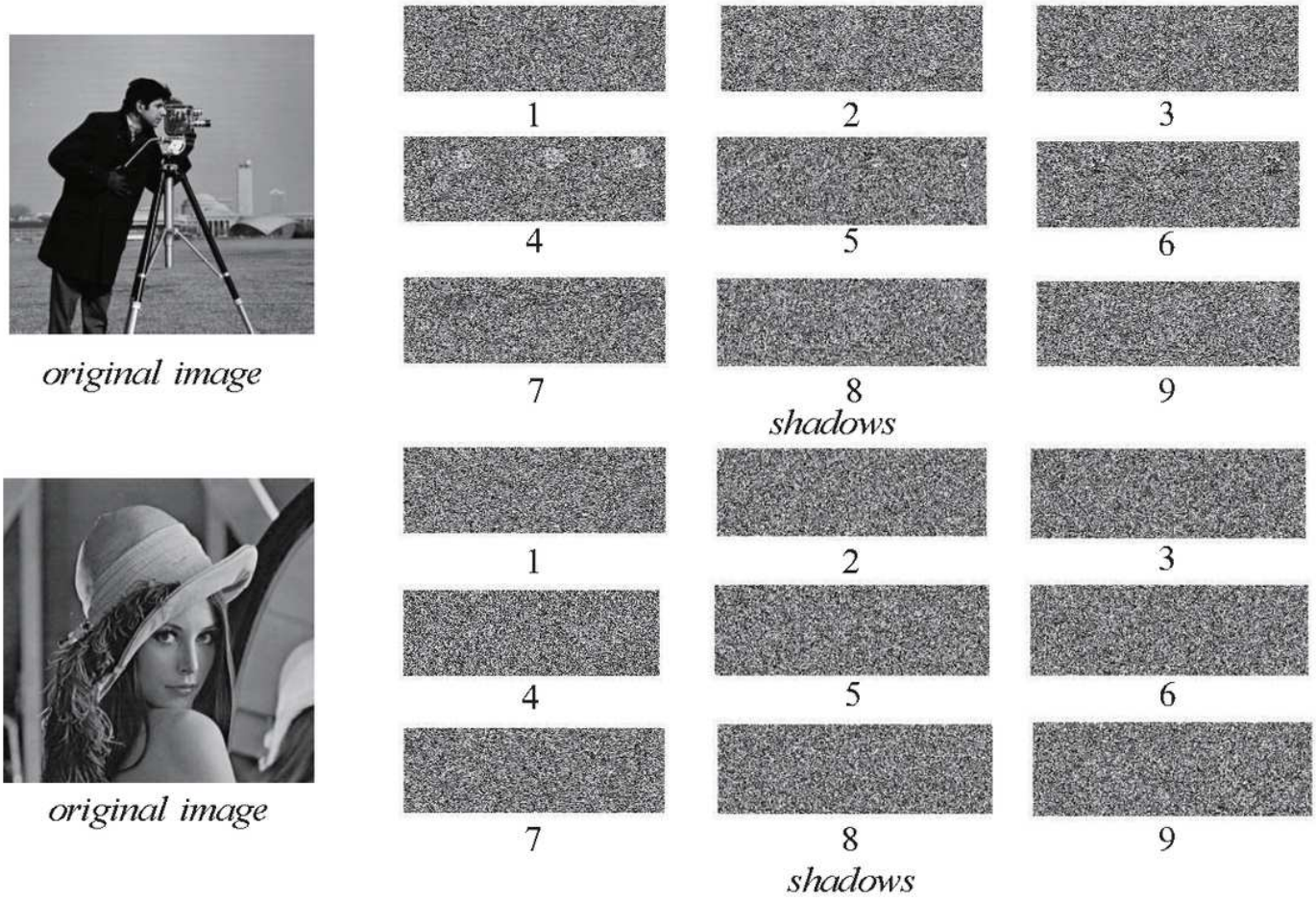

Figure 2

Original images and shadows using proposed scheme

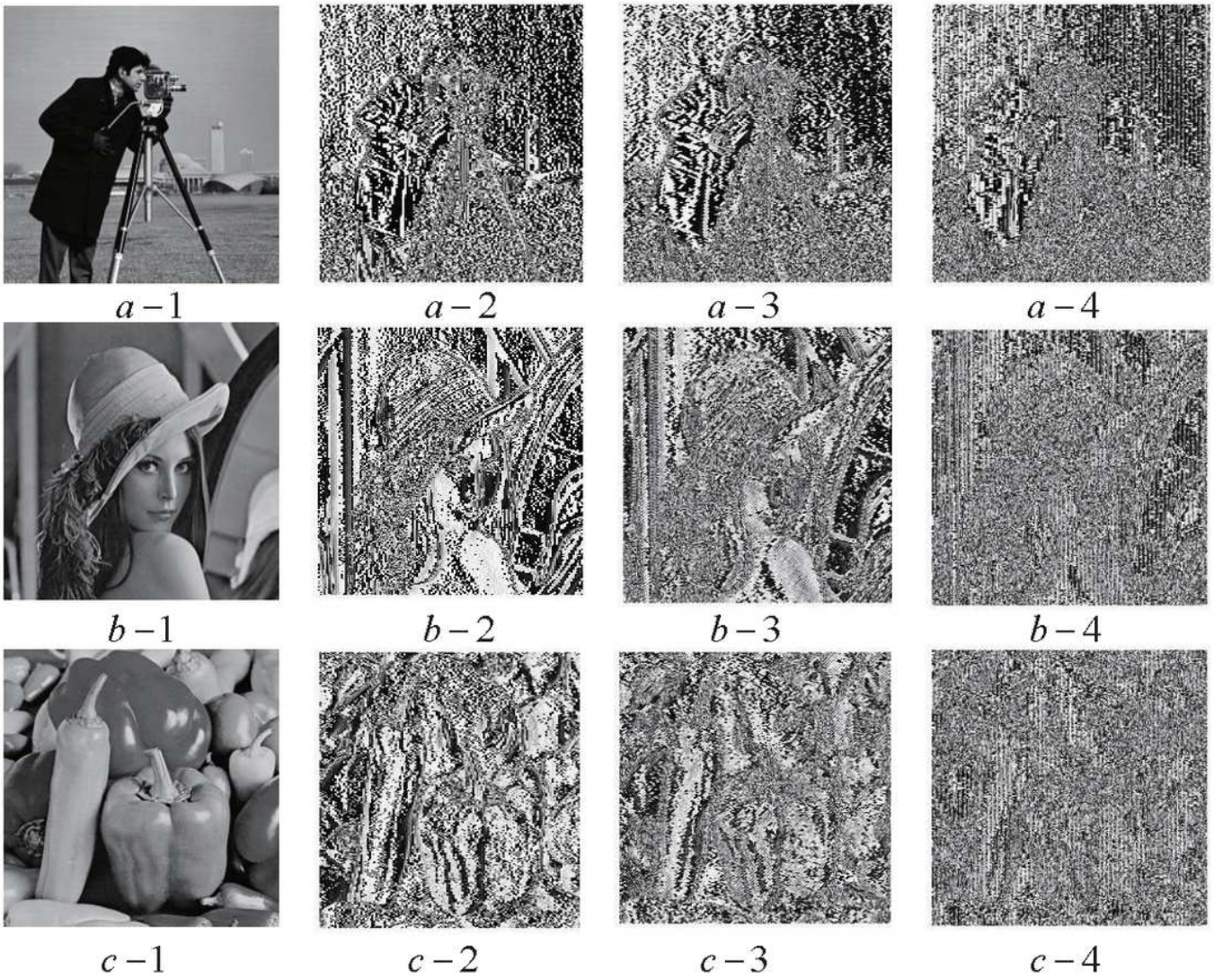

Figure 3

(a-1,b-1,c-1): original images, (a-2,b-2,c-2): quality lossy images with (k'= 2; k = 3), (a-3,b-3,c-3): quality lossy images with (k'= 3; k = 4), (a-4,b-4,c-4): quality lossy images with (k'= 4; k = 5)

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- SILiu.tex