Egyptian Informatics Journal (2014) 15, 201–209

Cairo University

Egyptian Informatics Journal

www.elsevier.com/locate/eij
www.sciencedirect.com

ORIGINAL ARTICLE

# A new $(k,n)$ verifiable secret image sharing scheme (VSISS)

**Amitava Nag [a,*], Sushanta Biswas [b], Debasree Sarkar [b], Partha Pratim Sarkar [b]**

[a] *Academy of Technology, West Bengal University of Technology, Hooghly 712121, India*
[b] *Department of Engineering and Technological Studies, University of Kalyani, Kalyani 741 235, India*

Received 13 March 2014; revised 27 September 2014; accepted 11 October 2014
Available online 2 December 2014

**KEYWORDS**

VSISS;
LFSR-based public key cryptosystem;
Cheating prevention;
Encrypted share

**Abstract** In this paper, a new $(k,n)$ verifiable secret image sharing scheme (VSISS) is proposed in which third order LFSR (linear-feedback shift register)-based public key cryptosystem is applied for the cheating prevention and preview before decryption. In the proposed scheme the secret image is first partitioned into several non-overlapping blocks of $k$ pixels. Every $k$ pixel is then used to form $m = \lceil k/4 \rceil + 1$ pixels of one encrypted share. The original secret image can be reconstructed by gathering any $k$ or more encrypted shared images. The experimental results show that the proposed VSISS is an efficient and safe method.



## 1. Introduction

With rapid growth of networking technology, digital data can be transferred easily over the Internet. But security and protection of sensitive digital information during transmission is a great concern in commercial, medical and military applications. Two methods cryptography [1,2] and data hiding [3] have been used to increase the security of the digital data such as images. Nevertheless, one of the common vulnerabilities of both these methods is "single point of failure" (SPOF) as they use single storage mechanism and therefore data can be easily misplaced or damaged. Secret image sharing schemes (SISS) are useful options. The basic idea behind secret sharing is to transform a secret into $n$ number of "shadows" or "shares" that can be carried and stored disjointedly. The secret can only be restored from any $k$ shadows $(k \leqslant n)$ and any $(k-1)$ or fewer shadows cannot reveal anything close to that secret.

The secret sharing schemes (SIS) were first introduced by Blakley [4] and Shamir [5] separately in 1979. Shamir's secret sharing scheme is a $(k,n)$ threshold-based secret sharing scheme. It is based on $(k-1)$ degree polynomial and Lagrange interpolation. In 2002, Thien and Lin [6] proposed an $(k,n)$ threshold based secret image sharing scheme (SISS) by extending Shamir's polynomial approach. In their scheme, the pixel value larger than 250 is always truncated to 250 before the generation of shares. This loss of pixel value has the truncation distortion which is the chief drawback of Thien–Lin scheme. Thien's work attracted many researchers to suggest different techniques which are applied in the literature [7,8]. Recently, Wu [9] has smartly solved the "truncation distortion" problem.

Blakley's proposed secret sharing scheme is established by using geometric approach. According to his method, the secret

* Corresponding author.

Peer review under responsibility of Faculty of Computers and Information, Cairo University.

Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.eij.2014.10.001
1110-8665 

is a point in a $k$-dimensional space and the hyper-planes in that space are defined by the $n$ number of shadows. For sharing of secret image, Blakley's geometric approach has been taken by Chen–Fu [10]. The probability of only containing one shared image to obtain the secret image of Chen–Fu is higher than Lin–Thien's scheme. In 2008, Tso first quantized the secret image and then applied Blakley's concepts to share the quantized image [11]. However, due to quantization errors, reconstructed image is not distortion free.

Another common drawback of all the above $(k,n)$ threshold secret image sharing schemes is the lack of the property of verification, i.e. in all these schemes it is presumed that the original secret image holder known as the dealer and the participants are not cheated. However, the following two situations may also arise:

(1) *The cheating by the dealer:* A dealer may provide a fake share to a particular participant.
(2) *The cheating by a participant:* One participant may supply a fake shadow to the other participants.

In [7], the author proposed verifiable secret image sharing scheme (VSISS) in which the cheaters (a dishonest dealer or a dishonest participant) can easily be distinguished. Merely as the authors of [7] adopted Thien–Lin scheme for share generation and secret reconstruction, their scheme suffers from the major drawback of Thien–Lin which has already been hashed out before. Thus to perfectly recover, Zhao employed the technique of carving up a pixel whose value is larger than 250 into two which charge extra storage. In [12], Wu et al. proposed a secret sharing scheme based on cellular automata. Though Wu et al. remove the problems of truncation distortion or pixel division it does not bring out any verification to identify cheaters.

In this paper, we propose a novel $(k,n)$ threshold verifiable secret image sharing scheme (VSISS) which generates encrypted shares. The proposed method can identify cheaters and recover the original secret without any deprivation. Moreover the probability of guessing of one correct shared image of the proposed method is minimized.

## 2. Preliminaries

### 2.1. The 3rd order LFSR sequence

In this section we briefly present the 3rd order linear-feedback shift register (LFSR) sequence [13]. Let $f(x)$ be an irreducible polynomial over $F = GF(p)$, where $p$ is a prime. Then $f(x)$ is defined as

$$f(x) = x^3 - ax^2 + bx - 1, \quad a, b \in F \tag{1}$$

A sequence $\boldsymbol{S} = \{S_t\}$ is a third-order homogeneous LFSR sequence with a characteristic polynomial $f(x)$ if the elements of **S** satisfy the following recursive relation

$$S_t = aS_{t-1} - bS_{t-2} + S_{t-3}, \quad t \geq 3 \tag{2}$$

where $S_0 = 3, S_1 = a$ and $S_2 = a^2 - 2b$, then $f(x)$ generates the characteristic sequence $\boldsymbol{S} = \{S_t\}$. We represent $S_t$ as $S_t(a,b)$ or $S_t(f)$, and $S$ as $S(a,b)$ or $S(f)$.

Assume that $a_1, a_2, a_3$ are all three roots of $f(x)$ in the splitting field of $f(x)$ over $F$. According to Newton's formula, the elements of $S$ can be represented by the symmetric $t$th power sum of the roots as follows:

$$S_t = a_1^t + a_2^t + a_3^t, \quad t = 0, 1 \tag{3}$$

The period of $f(x)$ is denoted as per$(f)$.

**Lemma 1** *([13][14]). Let $f(x) = x^3 - ax^2 + bx - 1$ be a polynomial over $F$, $a_1, a_2, a_3$ be three roots of $f(x)$ over $F$, and $S = \{S_t\}$ be the characteristic sequence generated by $f(x)$. Let $f(x) = (x - a_1^t)(x - a_2^t)(x - a_3^t)$.*

(i) $f_t(x) = x^3 - S_t(a,b)x^2 + S_t(a,b)x - 1$, where $S_{-t}(a,b) = S_t(b,a)$.
(ii) If $f(x)$ is irreducible over $F$, then $f(x)$ and $f_t(x)$ have the same period if and only if (per$(f)$, $t$) = 1.
(iii) If (per$(f)$, $k$) = 1, then $f(x)$ is irreducible over $F$ if and only if $f_t(x)$ is irreducible over $F$.

**Theorem 1** *([13]). Let $f(x) = x^3 - ax^2 + bx - 1$ be a polynomial over $F$, and let $S$ be the characteristic sequence generated by $f(x)$. Then for all positive integers $t$ and $e$,*

$$S_t(S_e(a,b), S_{-e}(a,b)) = S_{te}(a,b) = S_e(S_t(a,b), S_{-t}(a,b)) \tag{4}$$

The theorem 1 has been proved in [13]. This theorem guarantees the commutative property. If we consider $a$ and $b$ as variables in $F$ and $t$ as a fixed integer, then $S_t(a,b)$ and $S_{-t}(a,b)$ are Waring polynomials.

Fact 1 ([13,14]): For a fixed positive integer $t$, if $gcd(t, p^i - 1) = 1$, $i = 1, 2, 3$, then for any $u, v \in F$, the following system of equations has a unique solution $(a, b) \in F \times F$.

$$S_t(a,b) = u \text{ and } S_{-t}(a,b) = v \tag{5}$$

Otherwise, $S_t(a, b)$ and $S_t(a, b)$ are orthogonal in $F$ in variables $a$ and $b$.

**Lemma 2** *([14]). Let $f(x) = x^3 - ax^2 + bx - 1$ be an irreducible polynomial over $F$ of the period $Q = p^2 + p + 1$ and $S = \{S_t\}$ be the characteristic sequence generated by $f(x)$. Let $t$ and $t'$ be different coset leaders modulo $Q$, and both $t$ and $t'$ are relatively prime to $Q$. Then*

$$(S_t, S_{-t}) \neq (S_{t'}, \quad S_{-t'}) \tag{6}$$

Lemma 2 provides a one-to-one correspondence between the private key space and the public key space. Fact 1 together with Lemma 2 can be used to construct a public key encryption scheme, which is described in next section.

### 2.2. The LFSR-based public key cryptography

In this section, we introduce the LFSR-based public key cryptography by the 3rd order characteristic sequences. We apply the following steps to select the public and private keys:

1. Choose two secret prime number $p$ and $q$.
2. Calculates $N = p \times q$.
3. Calculate the period $\Phi$ of the irreducible polynomial as $\Phi = (p^2 + p + 1)(q^2 + q + 1)$.
4. Choose a random integer $e$ with $gcd(e, p^i - 1) = 1$ for $i = 2, 3$.

5. Compute $f$ so that $f \times e = 1 \bmod \Phi$.
6. Public keys: $(e, N)$.
7. Private key: $f$.

*Encryption:* If the plaintext $P = (P_1, P_2)$, where $0 < P_1, P_2 < N$, the cipher text $C = (C_1, C_2)$ can be generated by $C_1 = S_e(P_1, P_2)$ and $C_2 = S_{-e}(P_1, P_2)$.

*Decryption:* The plaintext $P = (P_1, P_2)$ can be generated from the given the cipher text $C = (C_1, C_2)$ as $P_1 = S_f(C_1, C_2)$ and $P_2 = S_{-f}(C_1, C_2)$.

## 3. Proposed secret image sharing scheme (SISS)

In this section we propose a verifiable $(k,n)$ secret image sharing scheme based on the 3rd order LFSR-based public key cryptosystem [13] for verification. Our proposed verifiable secret image sharing scheme (VSISS) consists of three phases: Initialization phase, share generation and reconstruction. Section 3.1 presents initialization phase, Section 3.2 presents the proposed share generation scheme and Section 3.3 introduces the verification and recovery strategy.

### 3.1. Initialization phase

Dealer (original secret holder) $D$ first selects two prime number $p$ and $q$ to calculate $N = p \times q$ and two positive integers $a$ and $b$ to obtain an irreducible polynomial $f(x)$ over $F = GF(p)$, where $f(x) = x^3 - ax^2 + bx - 1$. Then dealer publishes $N$, $a$ and $b$.

On the other hand, each participant $A_i$ $(1 \leqslant i \leqslant n)$ also selects a random number $e_i$ from the interval $[2, N]$ as its own secret shadow where $\gcd(e_i, p^r - 1) = 1$ for $r = 2,\ 3$. Then each participant $A_i$ computes $(S_{e_i}(a,b), S_{-e_i}(a,b))$ and provides it to the dealer. $A_i$ also provides its identity number $ID_i$ to the dealer and publishes $\{ID_i, s_{e_i}(a,b)\}$. For any two participants $A_i$ and $A_j$, the dealer has to ensure that $(S_{e_i}(a,b), S_{-e_i}(a,b)) \neq (S_{e_j}(a,b), S_{-e_j}(a,b))$ and $ID_i \neq ID_j$. The dealer then generates $n$ shares each of size $\frac{m \times M \times N}{k}$ where $m$ is defined as

$$m = \lceil k/4 \rceil + 1 \tag{7}$$

### 3.2. Share construction phase

The share construction phase generates $n$ encrypted shadow images of size $\frac{m \times M \times N}{k}$ from a secret image $I_s$ of size $M \times N$ where $2 \leqslant k \leqslant n$. The steps of share generation are listed given below:

1. The dealer $D$ randomly chooses an integer $e_0$, where $e_0 \in \{2 \text{ to } \Phi\}$. Then $D$ computes f such that $f \times e_0 = 1 \bmod \Phi$. Here $\Phi$ is the period of $f(x) = x^3 - ax^2 + bx - 1$.
2. $D$ calculates $R_0 = (S_{e_0}(a,b), S_{-e_0}(a,b))$ and $T_i = S_{e_0}(S_{e_i}(a,b), S_{-e_i}(a,b))$ for each $A_i$, $i = 1, 2, \ldots, n$. Publishes $\{R_0, f\}$.
3. Generate a permutation sequence by a secret key $K_S$.
4. Obtain permuted image $I'$ by permuting the pixels of original secret image with the help of permutation sequence generated in step 3.
5. Set $i$ to 1.
6. Divide the Secret Image into $T$ number of non-overlapping blocks $\{B_t\}_{t=1}^{T}$ of $1 \times k$ pixels, where $T = \frac{M \times N}{k}$.
7. Set $t$ to 1.
8. Select an appropriate hash function and compute $M_i = H(T_i)$ for each participant $A_i$. $M_i$ is also divided into $k$ non-overlapping blocks of length $k$ bits in such a way that $k \times k \leq |M_i|$ ($|\cdot|$ represents the length).
9. Each $j$th $(1 \leqslant j \leqslant k)$ block is converted into $k$ bits number $a_j$, where $a_j \in \{0, 1, \ldots, (2^k - 1)\}$.
10. Create an equation based on $k$ consecutive pixels $\{R_1, R_2, \ldots, R_k\}$ of block $B_t$ (generated in step 6) as
$$s_t = \sum_{j=1}^{k} r_j R_j \quad \text{where } r_j = a_j + 1 \tag{8}$$
11. $S_t$ is converted into $r = (8 + 2k)$ bits number as $b_{r-1} \ldots b_1 b_0$.
12. Compute $x = (8m - r)$. If $r \neq 8m$, then go to step 13. Otherwise i.e. if $r = 8m$, then go to step 14.
13. Generate a random number of length $x$ bits as $b'_{x-1}$ to $b'_0$ and add this $x$ bits sequence in MSB position of $b_{r-1} \ldots b_1 b_0$. Thus an $8m$ bits number $b'_{x-1} \ldots b'_0\, b_{r-1} \ldots b_1 b_0$ i.e. $b_{8\mathrm{m}-1} b_{8\mathrm{m}-2} \ldots b_1 b_0$ is obtained.
14. Obtain $m$ gray (8 bits) pixels from $8m$ bit sequence (generated in step 12).
$$\begin{array}{lll} p_1^i = b_7 & \ldots & b_1 b_0 \\ p_2^i = b_{15} & \ldots & b_9 b_8 \\ \vdots & \vdots & \vdots \\ p_m^i = b_{8m-1} & \ldots & b_{8m-7} b_{8m-8} \end{array} \tag{9}$$
15. Sequentially assign $p_1^i, p_2^i, \ldots, p_m^i$ to the $i$th shadow.
16. Increase $t$ by 1.
17. Repeat steps 7 through 16 until $t > T$.
18. Increase $i$ by 1.
19. Repeat step 5 through 18 until $i > n$.
20. End.

### 3.3. The verification and recovery phase

This section introduces a scheme to reconstruct the original secret image from $k$ or more shared images. The members of $A = \{A_1, A_2, \ldots, A_n\}$ will recover the secret image. If any $k$ number of participants verify each other and gathers their shares, then the original secret will be reconstructed. The steps of verification and recovery of original secret image $I_s$ of size $M \times N$ from the verified encrypted shares $E_i$ $(1 \leqslant i \leqslant k)$ of size $\frac{m \times M \times N}{k}$ are given as follows:

1. Each $A_i \in A$ first produces $T'_i = S_{e_i}(S_{e_0}(a,b), S_{-e_0}(a,b))$ to get the share, where $e_i$ represents the shadow of $P_i$.
2. Any participant $A_j$ in $A$ $(A_i \neq A_j)$ can verify $T'_i$ provided by $A_i$ with a test if $S_f(T'_i) = S_{e_i}(a,b)$. If this test is successful, then $A'_i$ is true and verified and then goto step 3, otherwise $A'_i$ is false and is identified as cheater and exit.
3. Each verified participant $A_i$ generates $M'_i = H(T'_i)$. $M'_i$ is divided into $k$ non-overlapping blocks $D'_r$ $(1 \leqslant r \leqslant k)$ of size $B = k$ bits where $k \times k \leq |M_i|$.

4. Divide each shadow image $E_i$ into $T$ number of non-overlapping blocks $\{B_t^i\}_{t=1}^{T}$ of $1 \times m$ pixels, where $T = \frac{M \times N}{k}$ and $1 \leqslant i \leqslant k$.
5. Set $t$ to 1.
6. Set $i$ to 1.
7. For $m$ consecutive pixels $p_1^i, p_2^i, \ldots p_m^i$ of block $B_r^i$ in shadow image $S_i$ obtain the binary sequence as

$$\begin{array}{lll} p_1^i = b_7^i & \ldots & b_1^i b_0^i \\ p_2^i = b_{15}^i & \ldots & b_9^i b_8^i \\ \vdots & \vdots & \vdots \\ p_m^i = b_{8m-1}^i & \ldots & b_{8m-7}^i b_{8m-8}^i \end{array} \tag{10}$$

8. Concatenate the bits stream of all $m$ pixels and generate a bit sequence of size $8m$ as $b_{8m-1}^i \ldots b_1^i b_0^i$.
9. Compute $r$ as $r = (8 + 2k)$. If $r = 8m$, then goto step 11.
10. Divide the $8m$ bits sequence into two different sequences, one of $x = (8m - r)$ bits long and another of $r$ bits as $b_{8k-1}^i \ldots b_{r+1}^i b_r^i$ and $b_{r-1}^i \ldots b_1^i b_0^i$ respectively.
11. Obtain a $r$ bits number $S_t^i$ as $S_t^i = b_{r-1}^i \ldots b_1^i b_0^i$ and discard $b_{8k-1}^i \ldots b_{r+1}^i b_r^i$.
12. Create a linear equation:

$$\sum_{j=1}^{k} r_{ij} R_{jt} = S_t^i \quad \text{where } r_{ij} = a_j + 1 \tag{11}$$

13. Increase $i$ by 1.
14. Repeat steps 7 through 13 until $i > k$.
15. $k$ number of linear equations of type (11) are created.
16. Use these $k$ equations to solve $R_{1t}, R_{2t}, \ldots, R_{kt}$ in Eq. (11). They are the corresponding $k$ pixel values of the $t$th block in the permuted image $I'_s$.
17. Repeat steps 6 through 16 until $t > T$.
18. Generate a permutation sequence by a secret key $K_S$.
19. Apply the inverse permutation operation to the permuted image $I'_s$ to recover the original secret image $I_s$.
20. End.

Step 1 and step 2 ensure that all participants can work together to verify whether one or more participant among them are cheaters. This verification could be performed without revealing the corresponding shares. In other words, even if any $(k - 1)$ verified participants gather their shares, then also revealing the original secret is not possible. Because $(k - 1)$ verified participants can create exactly $(k - 1)$ numbers of equations of type (11) which is insufficient to obtain the values of $k$ number of variables (in this case the values of $R_{1t}$, $R_{2t}$, ..., $R_{kt}$). To obtain the values of $R_{1t}, R_{2t}, \ldots, R_{kt}$ at least $k$ equations of type (11) are required. Thus the proposed scheme fulfills the requirement of Shamir's $(k,n)$ secret sharing (SS) scheme i.e. using proposed VSISS any $k$ or more than $k$ shadow images can reconstruct the original secret image, but any $(k - 1)$ cannot reveal any information.

## 4. Experimental results and discussion

### 4.1. Experimental results

This section presents the experimental results of the proposed $(k, n)$ secret image sharing system. A (4,6) secret sharing experiment is chosen to indicate the operation of the proposed method. Grayscale test images "Lena", "Airplane", "Barbara", "Peppers" and "Couple" of size $256 \times 256$ are used as a secret (input) images as depicted in Figs. 1(a), 2(a), 3(a), 4(a), 5(a) and Figs. 1(b), 2(b), 3(b), 4(b), 5(b) are the reconstructed image respectively. Both of the set of ({1(a), 2(a), 3(a), 4(a), 5(a)} and ({1(b), 2(b), 3(b), 4(b), 5(b)}) images are indistinguishable. Figs. 1–5(c)–(h) show the noisy share images of size $256 \times 128$.

### 4.2. Analysis of correlation coefficient

The correlation coefficient $r_{xy}$ between a pair of random variables $(x, y)$ can be calculated by the following formula:

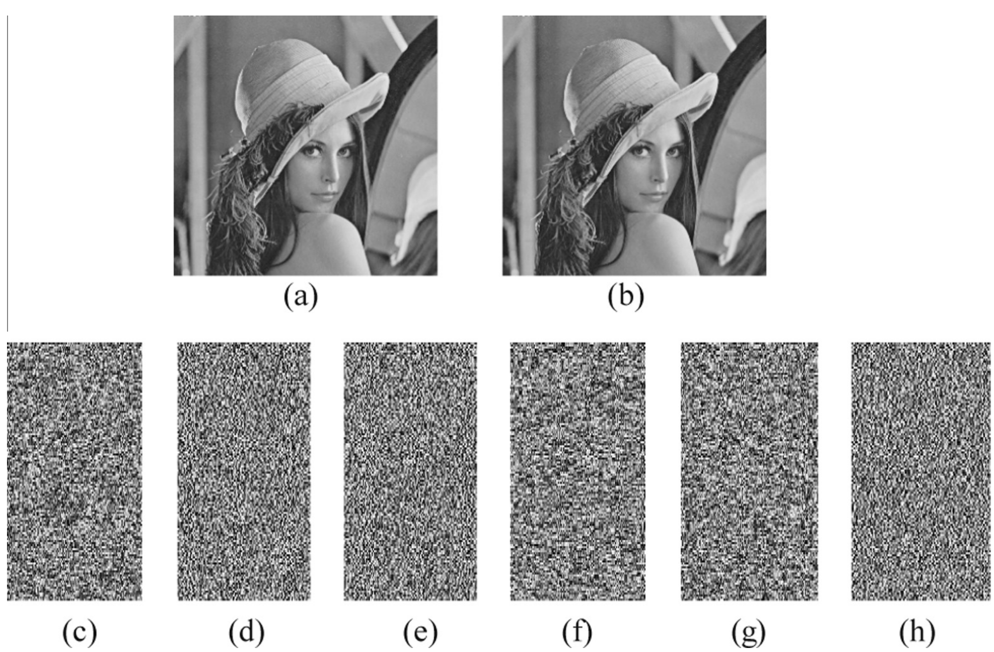

**Figure 1** (a) Secret image (Lena), (b) reconstructed image, (c)–(h): four shadow images.

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

where

$$cov(x,y) = \frac{1}{M\times N}\sum_{i=1}^{M\times N}(x_i - E(x))(y_i - E(y))$$
$$E(x_i) = \frac{1}{M\times N}\sum_{i=1}^{M\times N}x_i,\ D(x) = \frac{1}{M\times N}\sum_{i=1}^{M\times N}(x_i - E(x))^2 \tag{12}$$

In our experiment $(x,y)$ pair chosen as one pair of adjacent pixels in vertical, horizontal and diagonal directions. To compute the correlation coefficients of pairs of adjacent pixels, we choose 2048 random pairs of neighboring pixels in all three directions from the secret image and encrypted shared images. The correlation coefficients of two adjacent pixels in Fig. 1 in all three directions are listed in Table 1 and compared with the results in Refs. [2,12]. With regard to obtained results listed in Table 1 it is clear that the pixels in the encrypted shares of the proposed method are in feeble correlations, then the encryption result is quite serious.

### *4.3. Analysis of structural similarity index metric (SSIM)*

To check how dissimilar the encrypted shares from each other, we have used another well-known quality metric know as the Structural Similarity Index Metric (SSIM). It was developed by Wang et al. [15] in 2004. SSIM compares local patterns of pixel intensities that have been normalized for luminance distortion and contrast distortion. The values of the SSIM index are ranging from 0 to 1. A value of 0 shows two images (original and encrypted) are all dissimilar and 1 means the reverse one. If two images are $X$ and $Y$, the SSIM is defined as:

$$\text{SSIM }(X,Y) = \frac{(2\mu_X\mu_Y + C_1)(2\sigma_{XY} + C_2)}{(\mu_X^2 + \mu_Y^2 + C_1)(\sigma_X^2 + \sigma_Y^2 + C_2)} \tag{13}$$

where $\mu_X$ and $\mu_Y$ are the mean intensity of $X$ and $Y$ respectively, $\sigma_X^2$ and $\sigma_Y^2$ are the variance of $X$ and $Y$ respectively; $\sigma_{XY}$ the covariance between $X$ and $Y$. $C_1 = (k_1L)^2$, $C_2 = (k_2L)^2$ are two variables to stabilize the division with weak denominator and L is the dynamic range of the pixel-values chosen as $L = 255$. The value of $k_1$ (1) and $k_2$ (1) is chosen as $k_1 = 0.01$; $k_2 = 0.03$. SSIM values of share images for our experimentation are given in Table 2. The SSIM values of Table 2 shows that each encrypted share is totally dissimilar from the other encrypted shares. These strengthen the claim of the security of the proposed method.

### *4.4. Cheating prevention*

Each participant can easily prevent cheating before secret image reconstruction by verifying that if another participant provides correct or faulty data. Theorem 2 analyzes the verification capability of the proposed scheme. Hence the proposed method has the power to preclude cheating. On the other hand, the scheme [6,8–12] does not support verification thus cannot prevent cheating. The length of the key (private/public) used in cheating prevention is shorter in comparison with Zhao et al.'s [7] scheme for same for the same degree of protection.

**Theorem 2.** *Anyone can verify by another participant $A_i$ by computing $S_f(T_i') = S_{e_i}(a,b)$.*

**Proof.** In Section 3.3 if a participant $A_i$ provides true $T_i' = S_{e_i}(S_{e_0}(a,b), S_{-e_0}(a,b))$, then anyone can check whether $T_i'$ is a cheater as

$$\begin{aligned} S_f(T_i') &= S_f(S_{e_i}(S_{e_0}(a,b), S_{-e_0}(a,b))) \\ &= S_f(S_{e_0}(S_{e_i}(a,b), S_{-e_i}(a,b))) \\ &= S_{fe_0}(S_{e_i}(a,b), S_{-e_i}(a,b)) \\ &= S_{e_i}(a,b) \text{ since } fe_i = 1\,mod\ \Phi \end{aligned}$$

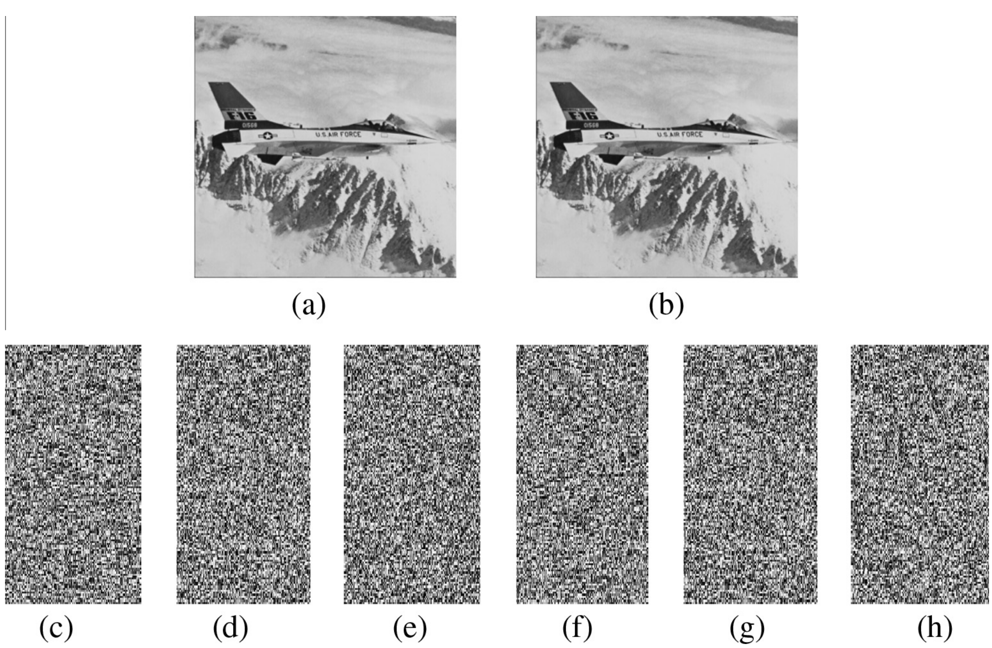

Figure 2 (a) Secret image (Airplane), (b) reconstructed image, (c)–(h): four shadow images.

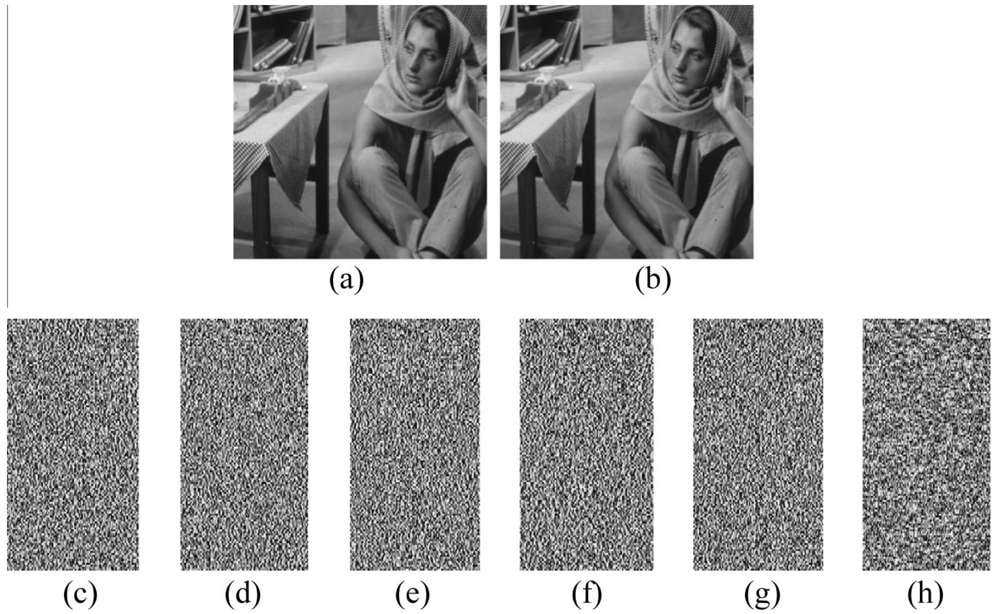


**Figure 3** (a) Secret image (Barbara), (b) reconstructed image, (c)–(h): four shadow images.

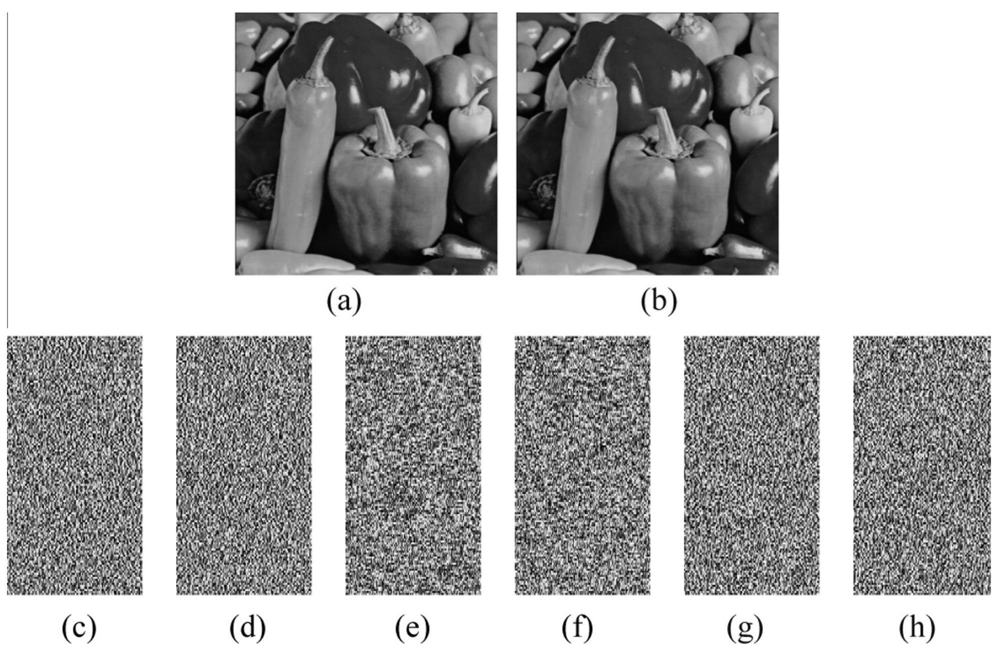


**Figure 4** (a) Secret image (Peppers), (b) reconstructed image, (c)–(h): four shadow images.

Let a participant $A_i$ publishes wrong information $T_i' = S_{e_v}(S_{e_0}(a,b), S_{-e_0}(a,b))$ by providing wrong key $S_{e_v}$. Now if participant $A_j$ wants to verify whether $T_i'$ is true by computing $S_f(T_i') = S_{e_v}(a,b) \neq S_{e_i}(a,b)$. So our proposed scheme has anti-cheating property and thus a verifiable scheme.

### *4.5. Computation overhead*

The proposed scheme uses an LFSR-based public key cryptosystem for cheating prevention. The LFSR is a one-way function which has lower computation cost than exponentiation function [16]. Hence the proposed scheme has low computational overhead for cheating prevention than Zhao et al.'s scheme as it involves exponentiation computation for cheating prevention.

### *4.6. Security of the proposed scheme*

The security of the proposed scheme is employed according to the 3rd order LFSR-based public key cryptosystem. This section presents the resistance capability of the proposed scheme against the attacks such as brute-force attack and collusion attack:

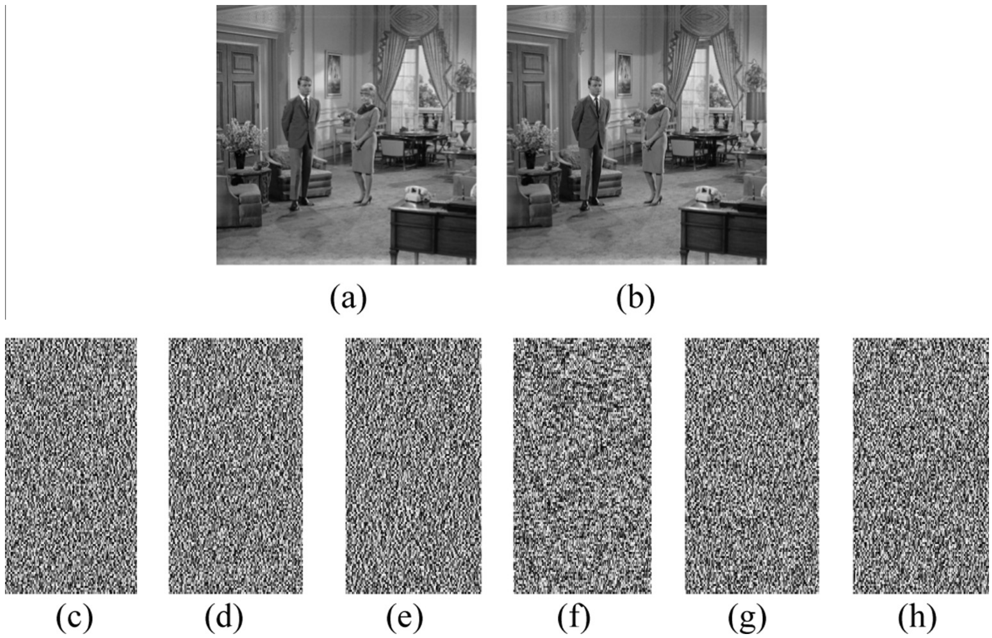


**Figure 5** (a) Secret image (Couple), (b) reconstructed image, (c)–(h): four shadow images.

**Table 1** Comparisons of the correlation coefficient $r_{xy}$ of Lena (gray-scale).

| Direction | Original – Fig(a) ($r_{xy}$) | Proposed | | Ref. [2] $r_{xy}$ of encrypted image | Ref. [12] | |
|---|---|---|---|---|---|---|
| | | Encrypted shares | $r_{xy}$ | | Encrypted shares | $r_{xy}$ |
| Horizontal | 0.9768 | Fig. 1 (c) | 0.0117 | 0.0004 | 1 | 0.0066 |
| | | Fig. 1 (d) | 0.0058 | | 2 | −0.0010 |
| | | Fig. 1 (e) | 0.0074 | | 3 | −0.0027 |
| | | Fig. 1 (f) | 0.0022 | | 4 | 0.0090 |
| | | Fig. 1 (g) | 0.0014 | | | |
| | | Fig. 1 (h) | 0.0047 | | | |
| Vertical | 0.9132 | Fig. 1 (c) | −0.0091 | 0.0021 | 1 | 0.0211 |
| | | Fig. 1 (d) | 0.0064 | | 2 | −0.0101 |
| | | Fig. 1 (e) | 0.0029 | | 3 | 0.0097 |
| | | Fig. 1 (f) | 0.0012 | | 4 | −0.089 |
| | | Fig. 1 (g) | 0.0108 | | | |
| | | Fig. 1 (h) | 0.0052 | | | |
| Diagonal | 0.9428 | Fig. 1 (c) | 0.0021 | −0.0038 | 1 | −0.0074 |
| | | Fig. 1 (d) | 0.0053 | | 2 | 0.0056 |
| | | Fig. 1 (e) | −0.0029 | | 3 | −0.0101 |
| | | Fig. 1 (f) | −0.0030 | | 4 | 0.0205 |
| | | Fig. 1 (g) | 0.0073 | | | |
| | | Fig. 1 (h) | 0.0019 | | | |

*Brute-force attack:* As there are totally 256 possible values for each $P_j^i$ and at least $k$ shares are required to reconstruct the secret image, attackers have to guess at least $k$ number of $P_j^i$ values, which has $P(256,k) = 256 \times 255 \times \cdots \times (256-k+1)$ possible values. Now for all $T$ number of blocks of the secret image, the probability to reconstruct the original secret is $\frac{1}{(p(256,k))^T} = \frac{1}{(p(256,k))^{\frac{M\times N}{k}}}$. This probability is really depressed; yet less than the probability of Li et al.'s [17] scheme. Thus the proposed scheme is completely secure scheme that could protect the original secret against the brute force attack in a high probability.

**Table 2** SSIM values between each pair of shares generated by the proposed scheme.

| Shares | SSIM | | | | |
|---|---|---|---|---|---|
| | Fig. 1(h) | Fig. 1(g) | Fig. 1(f) | Fig. 1(e) | Fig. 1(d) |
| Fig. 1(c) | 0.0201 | −0.0033 | 0.0101 | 0.0036 | 0.0044 |
| Fig. 1(d) | 0.0083 | 0.0013 | 0.0057 | 0.0012 | |
| Fig. 1(e) | 0.0105 | 0.0108 | 0.0089 | | |
| Fig. 1(f) | 0.0015 | 0.0208 | | | |
| Fig. 1(g) | 0.0103 | | | | |

**Table 3** Comparisons among the proposed scheme and the other related schemes.

| | Thien–Lin [6] | Zhao et al. [7] | Lin–Wang [8] | Wu [9] | Chen–Fu [10] | Proposed |
|---|---|---|---|---|---|---|
| Probability of guessing one correct share image | $\left(\frac{1}{251}\right)^{\frac{M\times N}{k}}$ | $\left(\frac{1}{251}\right)^{\frac{M\times N}{k}}$ | $\left(\frac{1}{251}\right)^{\frac{M\times N}{k}}$ | $\left(\frac{1}{256}\right)^{\frac{M\times N}{k}}$ | $\left(\frac{1}{128}\right)^{\frac{M\times N}{k}}$ | $\left(\frac{1}{256}\right)^{\frac{M\times N}{k}}$ |
| Cheating prevention/Verification capability | NO | YES | NO | NO | NO | YES |
| Distortion free recovery | NO | NO | NO | YES | YES | YES |
| Extra storage | YES | YES | NO | NO | NO | NO |
| Encrypted shadow size | $\frac{M\times N}{k}$ | $\frac{M\times N}{k}$ | $\frac{M\times N}{k}$ | $\frac{M\times N}{k}$ | Same as original secret image $(M \times N)$ | $\frac{m\times M\times N}{k}$, where $m = \lceil k/4 \rceil + 1$ |
| Secure channel is needed | YES | YES | NO | YES | YES | NO |
| Probability of brute force attack | Low | Low | Low | Low | Very low | Very low |
| Can resists collusion attack | NO | NO | YES | NO | NO | YES |

*Collusion attack* [18]*:* The proposed scheme can easily resist collusion attack as at the beginning each of the participants has to pass the verification phase (step 2 of Section 3.3). Even if two participants $A_i$ and $A_j$ plan to recover the original secret image by exchanging their $S_{e_i}$ and $S_{e_j}$ values, their conspiracy will be identified as each of participants $A_i$ have provided their unique identity number $ID_i$ to the dealer and published $\{ID_i, s_{e_i}(a,b)\}$. This type conspiracy can easily be detected by other participants. Thus proposed scheme is robust against collusion attack.

### 4.7. Merit of the proposed scheme

To further assess the performance of the proposed scheme, comparisons among the proposed scheme and the other related schemes [6–11] are listed in Table 3. The virtues of the proposed scheme are drawn as follows:

- *Probability of guessing:* For a secret image of size $(M \times N)$, there are $\frac{N\times N}{k}$ blocks as secret image is decomposed into blocks of size $k$ pixels. In the recovery phase, to obtain $k$ pixels, which are the coefficients of Eq. (11), at least $k$ equations are required. If a malicious user gathers $(k-1)$ shadow images, he/she can create only $(k-1)$ equations. The possibility of exact solution is then only $\frac{1}{256}$. Hence, for $\frac{M\times N}{k}$ blocks, the possibility of receiving the correct image is $\left(\frac{1}{256}\right)^{\frac{M\times N}{k}}$. In contrast, the probability of Thien–Lin [6] and Chen–Fu [10] are $\left(\frac{1}{251}\right)^{\frac{M\times N}{k}}$ and $\left(\frac{1}{128}\right)^{\frac{M\times N}{k}}$ respectively, which are less than proposed scheme of $\left(\frac{1}{256}\right)^{\frac{M\times N}{k}}$.
- *Extra storage and distortion free recovery:* To avoid the truncation distortion and lossless recovery, the schemes [6,7] divide one pixel into two and used extra storage to storage than new pixel. On the other hand, the proposed scheme and the schemes [9,10] can recover the original secret image losslessly without extra storage. Though the scheme [8] does not use any extra storage, but recovery is not lossless.
- *Shadow size:* The shadows of our scheme are little larger than the schemes [6–9] but smaller (for $k > 3$) than Chen-Fu's scheme [10].

Our proposed verifiable secret image sharing approach has the following properties:

1. The proposed scheme can produce the highly confidential encrypted shadows.
2. The generated shadow images are smaller in size with respect to the secret image.
3. The secret image can be perfectly reconstructed from any $k$ different shadows.
4. The original secret image cannot be reconstructed when any $(k-1)$ fewer shadows are gathered.
5. Each shadow is verifiable by others and thus no secure channel is required.
6. The proposed scheme can easily resist brute force attack and collusion attack.

The theoretical analysis and experimental results show that our proposed approach gives the above excellent properties.

## 5. Conclusion

Secret image sharing is an effective scheme which provides confidentiality and integrity of the sensitive image. In this paper a novel verifiable secret image sharing scheme based on the $(k,n)$ threshold and 3rd order LFSR-based public key cryptosystem is proposed. This new VSISS generates meaningless shares, which are hard to identify. It can also prevent cheating in the existing secret image sharing schemes and robust against brute force attack and collusion attack. The size of each shadow image is relatively small $(k > 3)$. What is more, the proposed system can reconstruct the original secret without any loss and for that it does not load any additional memory. Experimental results and analyses indicate the strength and efficiency of the proposed scheme.

## References

[1] Huang CK, Nien HH. Multi chaotic systems based pixel shuffle for image encryption. Opt Commun 2009;282:2123–7.
[2] Liu H, Wang X, Kadir A. Image encryption using DNA complementary rule and chaotic maps. Appl Soft Comput 2012;12:1457–66.

[3] Cheddad Abbas, Condell Joan, Curran Kevin, Mc Kevitt Paul. Digital image steganography: survey and analysis of current methods. Signal Process 2010;90(3):727–52.
[4] Blakley GR. Safeguarding cryptography keys. Proc AFIPS Natl Comput Conf 1979;48:313–7.
[5] Shamir A. How to share a secret. Commun ACM 1979;22(11): 612–3.
[6] Thien CC, Lin JC. Secret image sharing. Comput Graph 2002;26(5): 765–70.
[7] Zhao R, Zhao JJ, Dai F, Zhao FQ. A new image sharing scheme to identify cheaters. Comput Stand Interfaces 2009;31(1):252–7.
[8] Lin YY, Wang RZ. Scalable secret image sharing with smaller shadow images. IEEE Signal Process Lett 2010;17(3):316–9.
[9] Wu. A secret image sharing scheme for light images. EURASIP J Adv Signal Process 2013:49.
[10] Chen CC, Fu WY. A geometry-based secret image sharing approach. J Inf Sci Eng 2008;24(5):1567–77.
[11] Tso H-K. Sharing secret images using Blakley concept. Opt Eng 2008;47(7).
[12] Wu X, Ou D, Liang Q, Sun W. A user-friendly secret image sharing scheme with reversible steganography based on cellular automata. J Syst Softw 2012;85:1852–63.
[13] Chunqiang Hu, Liao Xiaofeng, Cheng Xiuzhen. Verifiable multi-secret sharing based on LFSR sequences. Theoret Comput Sci 2012;445:52–62.
[14] Gong G, Harn L. Public-key cryptosystems based on cubic finite field extensions. IEEE Trans Inf Theory 1999;45(7):2601–5.
[15] Wang Z, Bovik AC, Sheikh HR, Simoncelli EP. Image quality assessment: from error visibility to structural similarity. IEEE Trans Image Process 2004;13(4):600–12.
[16] Sun Hung-Min. On-line multiple secret sharing based on a one way function. Comput Commun 1999;22(8):745–8.
[17] Li Li, Abd El-Latif Ahmed A, Wang Chuanjun, Li Qiong, Niu Xiamu. A novel secret image sharing scheme based on chaotic system. In: Proc SPIE 8334, fourth international conference on digital image processing (ICDIP 2012), May 1; 2012. p. 833412-1–833412-5.
[18] Zhang Xiujie, He Mingxing. Collusion attack resistance and practice-oriented threshold changeable secret sharing schemes. In: 24th IEEE international conference on advanced information networking and applications; 2010. p. 745–52.