

[Egyptian Informatics Journal (2014) 15, 201](http://dx.doi.org/10.1016/j.eij.2014.10.001)–[209](http://dx.doi.org/10.1016/j.eij.2014.10.001)

Cairo University

Egyptian Informatics Journal

[www.elsevier.com/locate/eij](http://www.elsevier.com/locate/eij) [www.sciencedirect.com](http://www.sciencedirect.com/science/journal/11108665)

ORIGINAL ARTICLE

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



Amitava Nag [a](#_bookmark0),[\*](#_bookmark2), Sushanta Biswas [b](#_bookmark1), Debasree Sarkar [b](#_bookmark1), Partha Pratim Sarkar [b](#_bookmark1)

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

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* = )*k*/4¶+ 1 pixels of one encrypted share. The original secret image can be reconstructed by

KEYWORDS

VSISS;

LFSR-based public key cryptosystem;

Cheating prevention; Encrypted share

gathering any *k* or more encrypted shared images. The experimental results show that the proposed VSISS is an efficient and safe method.

© 2014 Production and hosting by Elsevier B.V. on behalf of Faculty of Computers and Information,

Cairo University.

1. Introduction

With rapid growth of networking technology, digital data can be transferred easily over the Internet. But security and protec- tion of sensitive digital information during transmission is a great concern in commercial, medical and military applica- tions. Two methods cryptography [[1,2]](#_bookmark15) and data hiding [[3]](#_bookmark17) 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)

\* Corresponding author.

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

**Production and hosting by Elsevier**

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* 6 *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]](#_bookmark17) and Shamir [[5]](#_bookmark17) 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 interpola- tion. In 2002, Thienand Lin[[6]](#_bookmark17) proposedan(*k*, *n*) thresholdbased secret image sharing scheme (SISS) by extending Shamir’s poly- nomial 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]](#_bookmark17). Recently, Wu [[9]](#_bookmark17) 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

<http://dx.doi.org/10.1016/j.eij.2014.10.001>

1110-8665 © 2014 Production and hosting by Elsevier B.V. on behalf of Faculty of Computers and Information, Cairo University.

202 A. Nag et al.

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]](#_bookmark17). 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 quan- tized image [[11]](#_bookmark17). However, due to quantization errors, recon- structed image is not distortion free.

Another common drawback of all the above (*k*, *n*) threshold

elements of *S* can be represented by the symmetric *t*th power sum of the roots as follows:

*St* = *at* + *at* + *at* ; *t* = 0; 1 (3)

1 2 3

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

Lemma 1 (*[13][14]*). *Let f(x) = x3* — *ax2* + *bx* — *1 be a polynomial over F, a1, a2, a3 be three roots of f(x) over F, and S* = {*St*} *be the characteristic sequence generated by f(x)*. *Let f*(*x*)= (*x* — *at* )(*x* — *at* ) *x* — *at* .

ÿ

1

2

3

secret image sharing schemes is the lack of the property of ver-

ification, i.e. in all these schemes it is presumed that the origi- nal secret image holder known as the dealer and the participants are not cheated. However, the following two situ- ations 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 sup- ply a fake shadow to the other participants.

In [[7]](#_bookmark17), 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]](#_bookmark17) adopted Thien–Lin scheme for share gen- eration 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 tech- nique of carving up a pixel whose value is larger than 250 into two which charge extra storage. In [[12]](#_bookmark17), 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. More- over the probability of guessing of one correct shared image of the proposed method is minimized.

1. Preliminaries
   1. *The 3rd order LFSR sequence*

In this section we briefly present the 3rd order linear-feedback shift register (LFSR) sequence [[13]](#_bookmark18). 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; *a*; *b* ∈ *F* (1)

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

*St* = *aSt*—1 — *bSt*—2 + *St*—3; *t* ≥ 3 (2)

where *S*0 = 3; *S*1 = *a* and *S*2 = *a*2 — 2*b*, then *f*(*x*) generates the characteristic sequence *S* = {*St*}. We represent *St* as *St*(*a*; *b*) or *St*(*f*), and *S* as *S*(*a*, *b*) or *S*(*f*).

Assume that *a* , *a* , *a* are all three roots of *f*(*x*) in the split-

* + 1. *f t* (*x*)= *x*3 — *St*(*a*; *b*)*x*2 + *St*(*a*; *b*)*x* — 1; where *S*—*t*(*a*; *b*)

= *St*(*b*; *a*).

* + 1. If *f*(*x*) is irreducible over *F*, then *f*(*x*) and *ft*(*x*) have the same period if and only if (per(*f*), *t*) = 1.
    2. If (per(*f*), *k*) = 1, then *f*(*x*) is irreducible over *F* if and only if *ft*(*x*) is irreducible over *F*.

Theorem 1 (*[13]*). *Let f(x) = x3* — *ax2 + bx* — *1 be a polyno- mial over F, and let S be the characteristic sequence generated by*

*f(x). Then for all positive integers t and e*,

*St*(*Se*(*a*; *b*); *S*—*e*(*a*; *b*)) = *Ste*(*a*; *b*)= *Se*(*St*(*a*; *b*); *S*—*t*(*a*; *b*)) (4)

The theorem 1 has been proved in [[13]](#_bookmark18). This theorem guaran- tees the commutative property. If we consider *a* and *b* as vari- ables in *F* and *t* as a fixed integer, then *St*(*a*, *b*) and *S*—*t*(*a*, *b*) are Waring polynomials.

Fact 1 ([[13,14]](#_bookmark18)): For a fixed positive integer *t*, if *gcd*(*t*, *pi* — 1) = 1, *i* = 1, 2, 3, then for any *u*, *v* ∈ *F*, the following sys- tem of equations has a unique solution (*a*, *b*) ∈ *F* · *F*.

*St*(*a*; *b*)= *u* and *S*—*t*(*a*; *b*) = *v* (5)

Otherwise, *St*(*a*, *b*) and *St*(*a*, *b*) are orthogonal in *F* in variables

*a* and *b*.

Lemma 2 (*[14]*). *Let f(x) = x3* — *ax2 + bx* — *1 be an irre- ducible polynomial over F of the period Q = p2 + p + 1 and S= {St} 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*

(*St*; *S*—*t*) – (*St*' ; *S*—*t*' ) (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.

* 1. *The LFSR-based public key cryptography*

In this section, we introduce the LFSR-based public key cryp- tography 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* · *q*.
3. Calculate the period U of the irreducible polynomial as

U = (*p*2 + *p* + 1)(*q*2 + *q* + 1).

1. Choose a random integer *e* with *gcd*(*e*, *pi* — 1) = 1 for

1 2 3

ting field of *f*(*x*) over *F*. According to Newton’s formula, the

*i* = 2, 3.

A new (*k*, *n*) verifiable secret image sharing scheme 203

1. Compute *f* so that *f* · *e* = 1 mod U.
2. Public keys: (*e*, *N*).
3. 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 = *Se*(*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 = *Sf*(*C*1, *C*2) and *P*2 = *S*—*f* (*C*1, *C*2).

1. Proposed secret image sharing scheme (SISS)

In this section we propose a verifiable (*k*, *n*) secret image shar- ing scheme based on the 3rd order LFSR-based public key cryptosystem [[13]](#_bookmark18) for verification. Our proposed verifiable secret image sharing scheme (VSISS) consists of three phases: Initialization phase, share generation and reconstruction. Sec- tion [3.1](#_bookmark3) presents initialization phase, Section [3.2](#_bookmark4) presents the proposed share generation scheme and Section [3.3](#_bookmark5) introduces the verification and recovery strategy.

* 1. *Initialization phase*

Dealer (original secret holder) *D* first selects two prime number *p* and *q* to calculate *N* = *p* · *q* and two positive integers *a* and *b* to obtain an irreducible polynomial *f*(*x*) over *F* = *GF*(*p*),

1. Divide the Secret Image into *T* number of non-over- lapping blocks {*Bt*}*T* of 1 · *k* pixels, where *T* = *M*×*N*.
2. Set *t* to 1.

*t*=1

*k*

1. Select an appropriate hash function and compute *Mi* = *H* (*T i*) for each participant *Ai*. *Mi* is also divided into *k* non-overlapping blocks of length *k* bits in such a way that *k* × *k* ≤ |*Mi*| (|·| represents the length).
2. Each *j*th (1 6 *j* 6 *k*) block is converted into *k* bits number *aj*, where *aj* ∈ {0; 1; ... ; (2*k* — 1)}.
3. Create an equation based on *k* consecutive pixels

{*R*1, *R*2,.. ., *Rk*} of block *Bt* (generated in step 6) as

*k*

X

*st* = *rjRj* where *rj* = *aj* + 1 (8)

*j*=1

1. *St* is converted into *r* = (8 + 2*k*) bits number as

*br*—1.. .*b*1*b*0.

1. Compute *x* = (8*m* — *r*). If *r* „ 8*m*, then go to step 13. Otherwise i.e. if *r* = 8*m*, then go to step 14.
2. Generate a random number of length *x* bits as *b*' to ' and add this *x* bits sequence in MSB position of *br*—1.. .*b*1*b*0. Thus an 8*m* bits number *b*' ... *b*' *br*—1 ... *b*1*b*0 i.e. *b*8m—1*b*8m—2.. .*b*1*b*0 is obtained.

*x*—1

*b*

*x*—1

0

0

1. Obtain *m* gray (8 bits) pixels from 8*m* bit sequence (generated in step 12).

*pi* = *b*7 ... *b*1*b*0 *pi* = *b*15 ... *b*9*b*8

1

2

where *f*(*x*) = *x*3 — *ax*2 + *bx* — 1. Then dealer publishes *N*, *a*

and *b*.

*p*

. . .

. . .

(9)

On the other hand, each participant *Ai*

(1 6 *i* 6 *n*) also

*i* = *b*8*m*—1 ... *b*8*m*—7*b*8*m*—8

selects a random number *ei* from the interval [2, *N*] as its own secret shadow where gcd (*ei*; *pr* — 1) = 1 for *r* = 2, 3. Then each participant *Ai* computes (*Sei* (*a*; *b*); *S*—*ei* (*a*; *b*)) and provides it to the dealer. *Ai* also provides its identity number *IDi* to the dealer and publishes {*IDi*; *sei* (*a*; *b*)}. For any two participants *Ai* and *Aj*, the dealer has to ensure that (*Sei* (*a*; *b*); *S*—*ei* (*a*; *b*)) – (*Sej* (*a*; *b*); *S*—*ej* (*a*; *b*)) and *IDi* „ *IDj*. The dealer then generates *n* shares each of size *m*×*M*×*N* where *m* is

*k*

*m*

defined as

*m* = )*k*/4¶+ 1 (7)

* 1. *Share construction phase*

The share construction phase generates *n* encrypted shadow images of size *m*×*M*×*N* from a secret image *I* of size *M* · *N*

1. Sequentially assign *pi* ; *pi* ; ... ; *pi* to the *i*th shadow.
2. Increase *t* by 1.

1 2 *m*

1. Repeat steps 7 through 16 until *t* > *T*.
2. Increase *i* by 1.
3. Repeat step 5 through 18 until *i* > *n*.
4. End.
   1. *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,.. ., *An*} 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

*k s* of verification and recovery of original secret image *Is* of size

where 2 6 *k* 6 *n*. The steps of share generation are listed given

below:

*M* · *N* from the verified encrypted shares *Ei* (1 6 *i* 6 *k*) of size

*m*×*M*×*N* are given as follows:

*k*

1. The dealer *D* randomly chooses an integer *e*0, where
2. Each *A* ∈ *A* first produces *T* ' = *S* (*S*

(*a*; *b*); *S*

*e*0 ∈ {2 to U}. Then *D* computes f such that *i*

*i ei e*0

—*e*0

*f* · *e*0 = 1 mod U. Here U is the period of

*f* (*x*) = *x*3 — *ax*2 + *bx* — 1.

(*a*; *b*); *S*

(*a*; *b*)) and *T*

= *S*

(*a*; *b*)) to get the share, where *ei* represents the shadow

of *Pi*.

ÿ

1. Any participant *A* in *A A* – *A* can verify *T* ' provided

*i*

*j*

*i*

*j*

*i*

*i*

*f*

*i*

*ei*

0 *e*0

1. *D* calculates *R*

= (*S*

(*Sei* (*a*; *b*); *S*—*ei* (*a*; *b*)) for each *Ai*, *i* = 1, 2,.. ., *n*. Pub-

—*e*0

*i e*0

by *A* with a test if *S* ÿ*T* ' = *S*

(*a*; *b*). If this test is suc-

lishes {*R*0, *f*}.

1. Generate a permutation sequence by a secret key *KS*.
2. Obtain permuted image *I*' by permuting the pixels of original secret image with the help of permutation

cessful, then *A*' is true and verified and then goto step 3, otherwise *A*' is false and is identified as cheater and exit.

1. Each verified participant *Ai* generates *M* ' = *H T* ' . *M* ' is

*i*

ÿ

*r*

*i*

*i*

*i*

sequence generated in step 3.

divided into *k* non-overlapping blocks *D*' (1 6 *r* 6 *k*) of

1. Set *i* to 1.

size *B* = *k* bits where *k* × *k* ≤ |*Mi*|.

204 A. Nag et al.

1. Divide each shadow image *Ei* into *T* number of non-overlapping blocks *Bi T* of 1 · *m* pixels, where

}

Step 1 and step 2 ensure that all participants can work together to verify whether one or more participant among

*T* = *M*×*N* and 1 6 *i* 6 *k*.

*k*

1. Set *t* to 1.
2. Set *i* to 1.

*t t*=1

them are cheaters. This verification could be performed with- out revealing the corresponding shares. In other words, even if any (*k* — 1) verified participants gather their shares, then also

1. For *m* consecutive pixels *pi* ; *pi* ; .. . *pi*

1

2

*m*

of block *Bi* in

revealing the original secret is not possible. Because (*k* — 1)

shadow image *Si* obtain the binary sequence as

*r*

verified participants can create exactly (*k* — 1) numbers of

*pi* = *bi*

... *bi bi*

equations of type [(11)](#_bookmark6) which is insufficient to obtain the values

1 7 1 0

*pi* = *bi*

... *bi bi*

of *k* number of variables (in this case the values of *R*1*t*, *R*2*t*,-

2 15 9 8

. . .

. . .

(10)

.. ., *Rkt*). To obtain the values of *R*1*t*, *R*2*t*, .. ., *Rkt* at least *k*

equations of type [(11)](#_bookmark6) are required. Thus the proposed scheme

*i* *i*

*p* = *b*

*m* 8*m*—1

*i* *i*

8*m*—7 8*m*—8

... *b b*

fulfills the requirement of Shamir’s (*k*, *n*) secret sharing (SS) scheme i.e. using proposed VSISS any *k* or more than *k* sha-

1. Concatenate the bits stream of all *m* pixels and generate dow images can reconstruct the original secret image, but

1 0

a bit sequence of size 8*m* as *bi*

8*m*—1

... *bi bi* .

any (*k* — 1) cannot reveal any information.

1. Compute *r* as *r* = (8 + 2*k*). If *r* = 8*m*, then goto step 11.
2. Divide the 8*m* bits sequence into two different

sequences, one of *x* = (8*m* — *r*) bits long and another of *r* bits as *bi* ... *bi bi* and *bi* .. . *bi bi* respectively.

1. Experimental results and discussion
   1. *Experimental results*

8*k*—1

*r*+1 *r*

*r*—1 1 0

1. Obtain a *r* bits number *Si* as *Si* = *bi*

... *bi bi*

and dis-

card *bi* .. . *bi bi* .

8*k*—1 *r*+1 *r*

1. Create a linear equation:

X*k*

*t t r*—1 1 0

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 pro- posed method. Grayscale test images ‘‘Lena’’, ‘‘Airplane’’,

*j*=1

*t*

*rijRjt* = *Si*

where *rij* = *aj* + 1 (11)

‘‘Barbara’’, ‘‘Peppers’’ and ‘‘Couple’’ of size 256 · 256 are used as a secret (input) images as depicted in Figs. [1](#_bookmark7)(a), [2](#_bookmark8)(a), [3](#_bookmark9)(a),

1. Increase *i* by 1.
2. Repeat steps 7 through 13 until *i* > *k*.
3. *k* number of linear equations of type [(11)](#_bookmark6) are created.
4. Use these *k* equations to solve *R*1t, *R*2t, .. ., *Rkt* in Eq.

[(11)](#_bookmark6). They are the corresponding *k* pixel values of the

*t*th block in the permuted image *I*' .

*s*

1. Repeat steps 6 through 16 until *t* > *T*.
2. Generate a permutation sequence by a secret key *KS*.
3. Apply the inverse permutation operation to the per- muted image *I*' to recover the original secret image *Is*.

*s*

1. End.

[4](#_bookmark10)(a), [5](#_bookmark11)(a) and Figs. [1](#_bookmark7)(b), [2](#_bookmark8)(b), [3](#_bookmark9)(b), [4](#_bookmark10)(b), [5](#_bookmark11)(b) are the recon- structed 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](#_bookmark7)(c)–(h) show the noisy share images of size 256 · 128.

* 1. *Analysis of correlation coefficient*

The correlation coefficient *rxy* between a pair of random vari- ables (*x*, *y*) can be calculated by the following formula:

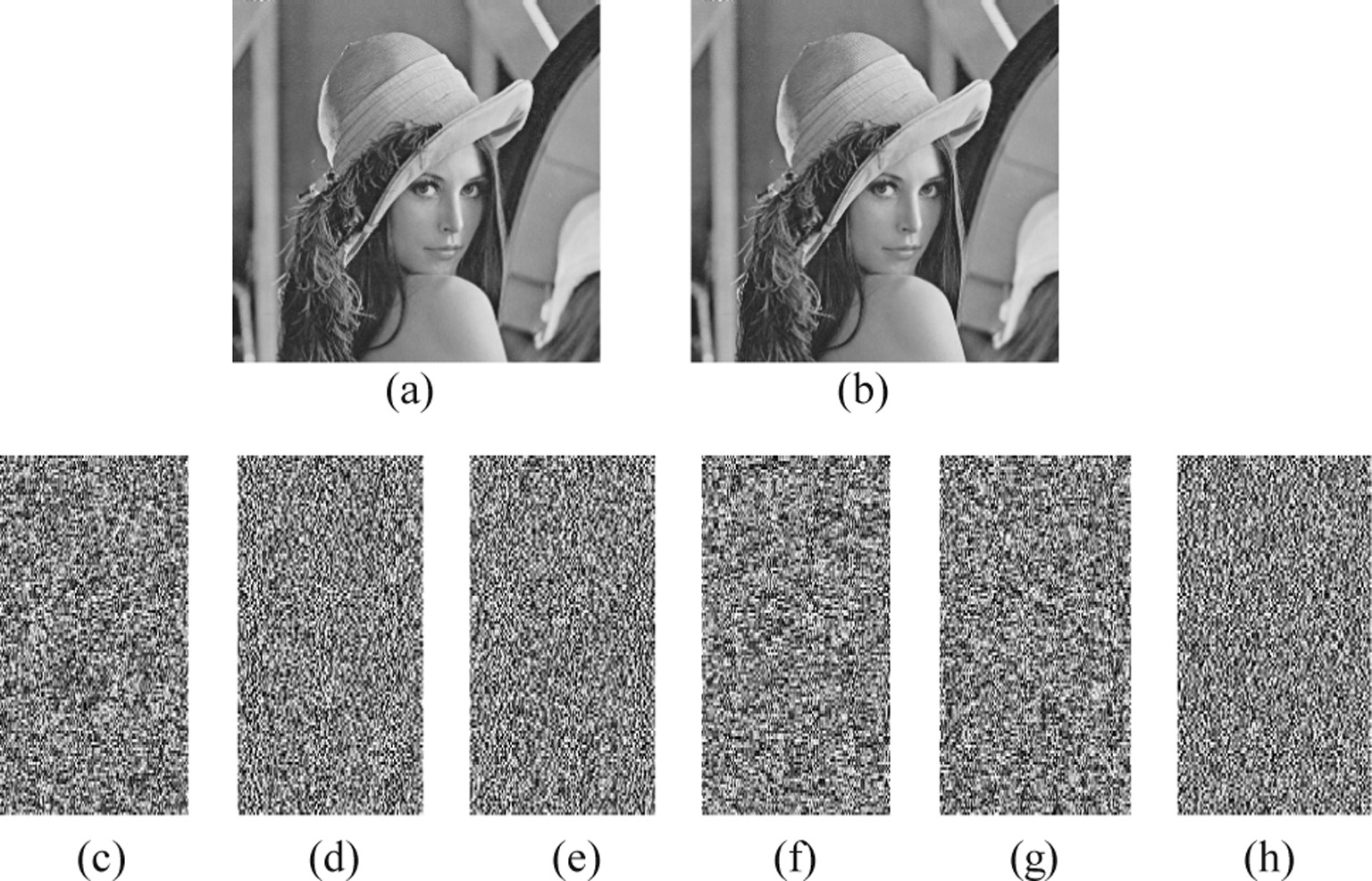


Figure 1 (a) Secret image (Lena), (b) reconstructed image, (c)–(h): four shadow images.

A new (*k*, *n*) verifiable secret image sharing scheme 205

*cov*(*x*; *y*)

*r*

*xy* = p*D*ﬃﬃﬃﬃ(ﬃﬃ*x*ﬃﬃﬃ)ﬃp*D*ﬃﬃﬃﬃ(ﬃﬃ*y*ﬃﬃ)ﬃﬃ

where l*X* and l*Y* are the mean intensity of *X* and *Y* respec- tively, r2 and r2 are the variance of *X* and *Y* respectively;

where

*X*

*Y*

*cov*(*x*; *y*) = 1 X(*x* — *E*(*x*))(*y* — *E*(*y*))

*M*×*N*

r*XY* the covariance between *X* and *Y*. *C*1 = (*k*1*L*)2, *C*2 = (*k*2*L*)2 are two variables to stabilize the division with weak denominator and L is the dynamic range of the pixel-val-

*M* × *N*

1 *M*X×*N*

*i*

*i*=1

*i*

1 *M*X×*N*

(12)

2

ues 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](#_bookmark13). The SSIM values of

*E*(*xi*) = *M* × *N*

*i*=1

*xi*; *D*(*x*) = *M* × *N*

*i*=1

(*xi* — *E*(*x*))

[Table 2](#_bookmark13) shows that each encrypted share is totally dissimilar from the other encrypted shares. These strengthen the claim

In our experiment (*x*, *y*) pair chosen as one pair of adjacent

pixels in vertical, horizontal and diagonal directions. To com- pute 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](#_bookmark7) in all three directions are listed in [Table 1](#_bookmark12) and compared with the results in Refs. [[2,12]](#_bookmark16). With regard to obtained results listed in [Table 1](#_bookmark12) it is clear that the pixels in the encrypted shares of the proposed method are in feeble correlations, then the encryp- tion result is quite serious.

* 1. *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]](#_bookmark18) in 2004. SSIM compares local patterns of

of the security of the proposed method.

* 1. *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 verifi- cation capability of the proposed scheme. Hence the proposed method has the power to preclude cheating. On the other hand, the scheme [[6,8–12]](#_bookmark17) 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]](#_bookmark17) scheme for same for the same degree of protection.

Theorem 2. *Anyone can verify by another participant Ai by computing Sf T*' = *Se* (*a*; *b*).

ÿ

*i*

*i*

pixel intensities that have been normalized for luminance dis- tortion and contrast distortion. The values of the SSIM index are ranging from 0 to 1. A value of 0 shows two images (origi- nal and encrypted) are all dissimilar and 1 means the reverse

one. If two images are *X* and *Y*, the SSIM is defined as:

Proof. In Section [3.3](#_bookmark5) if a participant *Ai* provides true *T*' = *Se* (*Se* (*a*; *b*); *S*—*e* (*a*; *b*)), then anyone can check whether *T*' is a cheater as

*Sf*(*T*') = *Sf*(*Se* (*Se* (*a*; *b*); *S*—*e* (*a*; *b*)))

*i*

*i i* 0 0

*i i* 0 0

= *Sf*(*Se*0 (*Sei* (*a*; *b*); *S*—*ei* (*a*; *b*)))

SSIM (*X*; *Y*) = (2l*X*l*Y* + *C*1)(2r*XY* + *C*2)

(13)

= *S* (*S* (*a*; *b*); *S* (*a*; *b*))

(l2 + l2 + *C* )(r2 + r2 + *C* )

*fe*0 *ei*

—*ei*

*X Y* 1 *X Y* 2

= *S* (*a*; *b*) since *fe* = 1 *mod* U

*ei* *i*

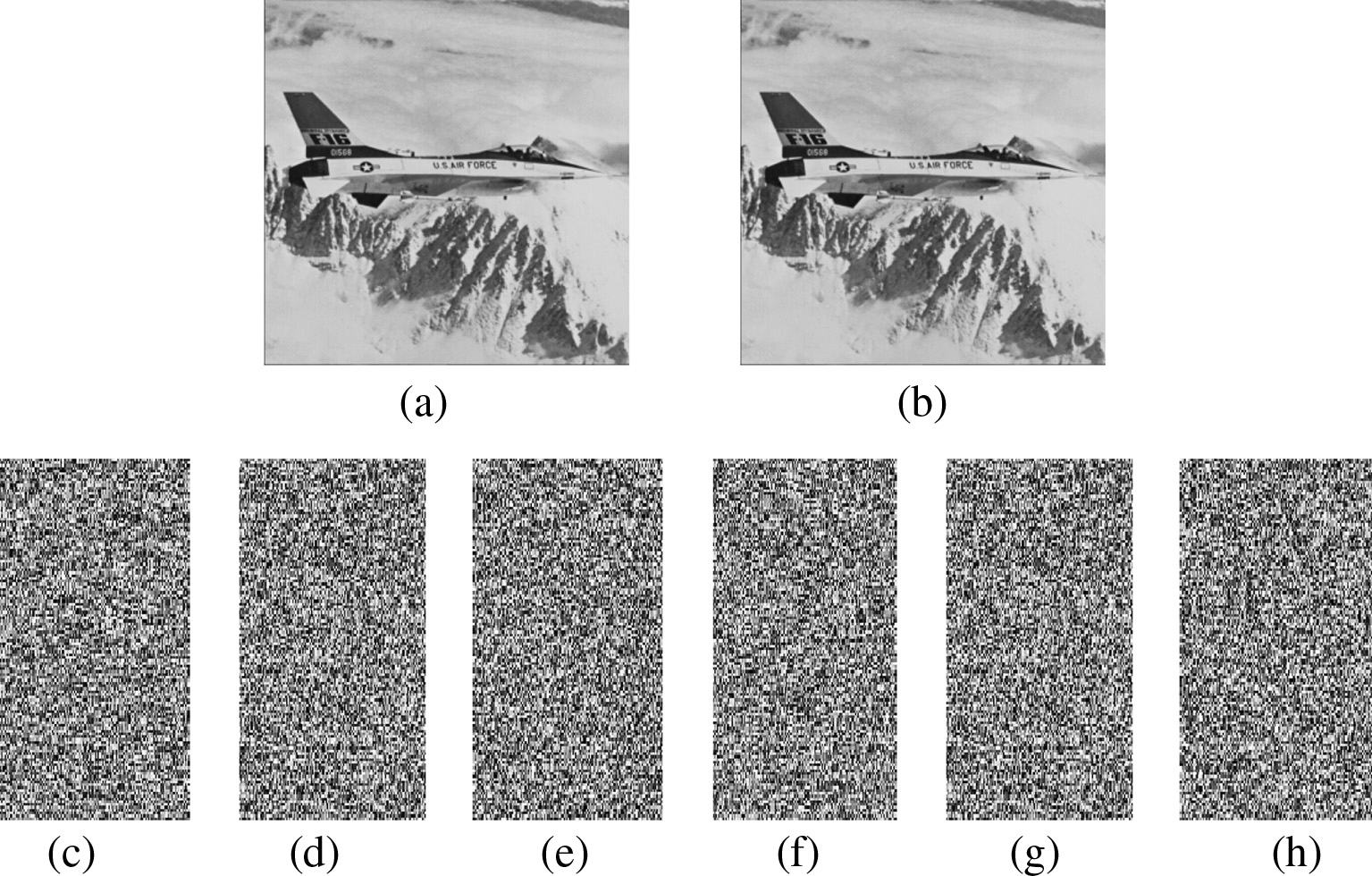


Figure 2 (a) Secret image (Airplane), (b) reconstructed image, (c)–(h): four shadow images.

206 A. Nag et al.

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 *Ai* publishes wrong information *T*' = *Se*

*i*

*v*

(*Se*0 (*a*; *b*); *S*—*e*0 (*a*; *b*)) by providing wrong key *Sev* . Now if par- ticipant *Aj* wants to verify whether *T*' is true by computing

function [[16]](#_bookmark18). Hence the proposed scheme has low computa- tional overhead for cheating prevention than Zhao et al.’s

scheme as it involves exponentiation computation for cheating

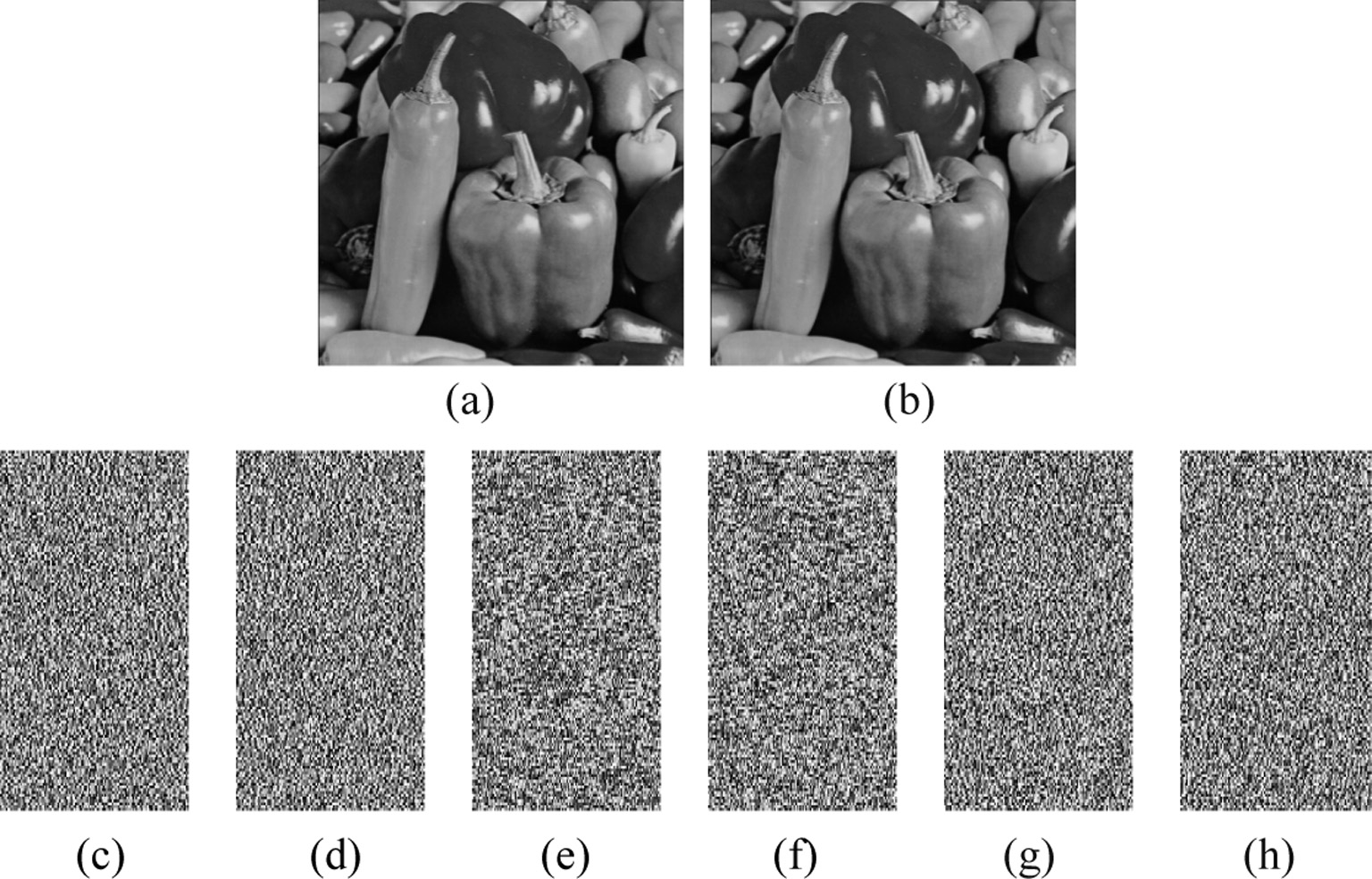
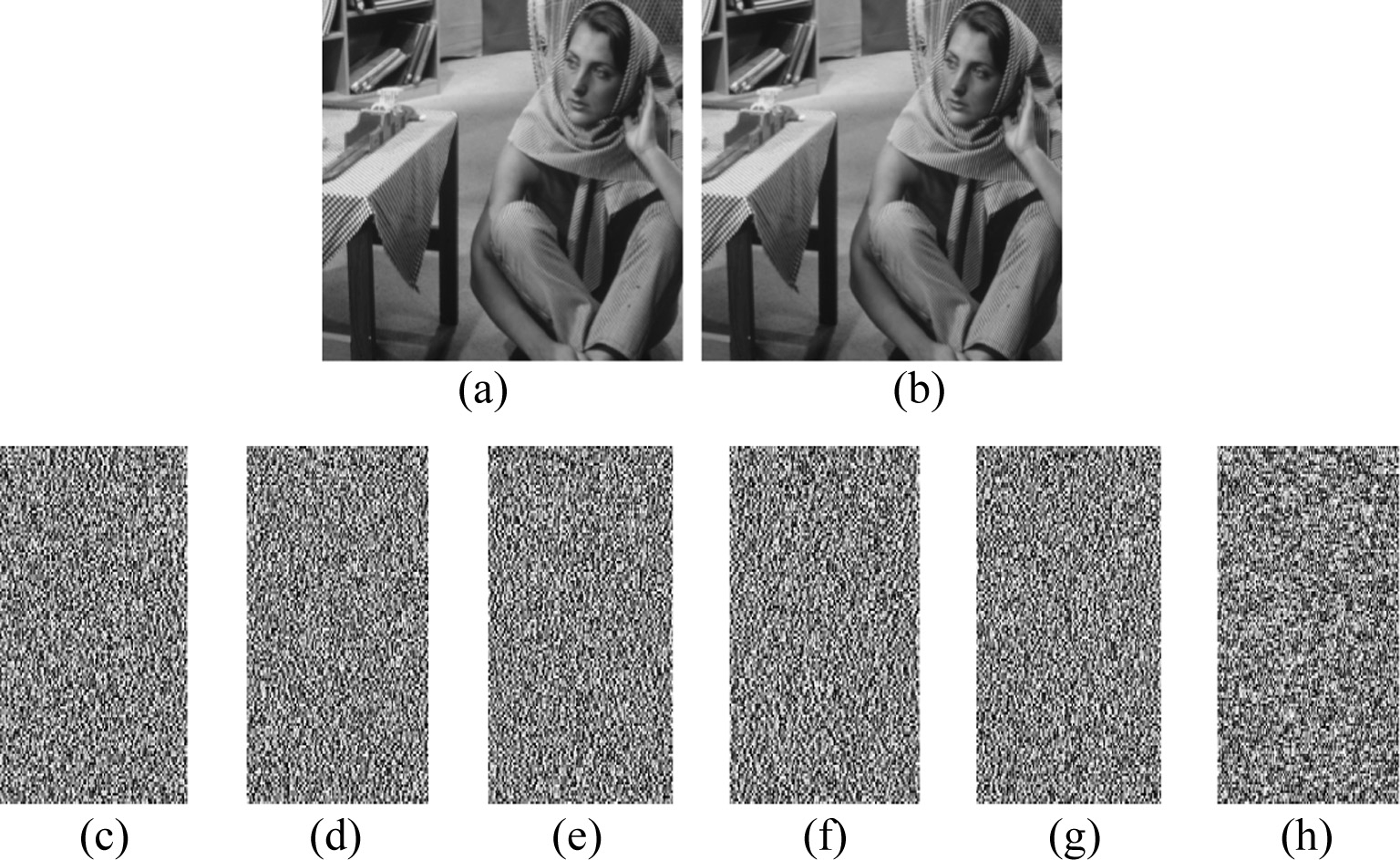
ÿ ' *i*

*Sf Ti*

= *Sev* (*a*; *b*) – *Sei* (*a*; *b*). So our proposed scheme has

prevention.

anti-cheating property and thus a verifiable scheme.



* 1. *Computation overhead*

The proposed scheme uses an LFSR-based public key crypto- system for cheating prevention. The LFSR is a one-way func- tion which has lower computation cost than exponentiation

* 1. *Security of the proposed scheme*

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

A new (*k*, *n*) verifiable secret image sharing scheme 207

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Table 1 Comparisons of the correlation coefficient *rxy* of Lena (gray-scale). | | | | | | |
| Direction | Original – Fig(a) (*rxy*) | Proposed  Encrypted shares | *rxy* | Ref. [[2]](#_bookmark16) *rxy* of encrypted image | Ref. [[12]](#_bookmark17)  Encrypted shares | *rxy* |
| Horizontal | 0.9768 | [Fig. 1](#_bookmark7) (c) | 0.0117 | 0.0004 | 1 | 0.0066 |
|  |  | [Fig. 1](#_bookmark7) (d) | 0.0058 |  | 2 | —0.0010 |
|  |  | [Fig. 1](#_bookmark7) (e) | 0.0074 |  | 3 | —0.0027 |
|  |  | [Fig. 1](#_bookmark7) (f) | 0.0022 |  | 4 | 0.0090 |
|  |  | [Fig. 1](#_bookmark7) (g) | 0.0014 |  |  |  |
|  |  | [Fig. 1](#_bookmark7) (h) | 0.0047 |  |  |  |
| Vertical | 0.9132 | [Fig. 1](#_bookmark7) (c) | —0.0091 | 0.0021 | 1 | 0.0211 |
|  |  | [Fig. 1](#_bookmark7) (d) | 0.0064 |  | 2 | —0.0101 |
|  |  | [Fig. 1](#_bookmark7) (e) | 0.0029 |  | 3 | 0.0097 |
|  |  | [Fig. 1](#_bookmark7) (f) | 0.0012 |  | 4 | —0.089 |
|  |  | [Fig. 1](#_bookmark7) (g) | 0.0108 |  |  |  |
|  |  | [Fig. 1](#_bookmark7) (h) | 0.0052 |  |  |  |
| Diagonal | 0.9428 | [Fig. 1](#_bookmark7) (c) | 0.0021 | —0.0038 | 1 | —0.0074 |
|  |  | [Fig. 1](#_bookmark7) (d) | 0.0053 |  | 2 | 0.0056 |
|  |  | [Fig. 1](#_bookmark7) (e) | —0.0029 |  | 3 | —0.0101 |
|  |  | [Fig. 1](#_bookmark7) (f)  [Fig. 1](#_bookmark7) (g) | —0.0030  0.0073 |  | 4 | 0.0205 |
|  |  | [Fig. 1](#_bookmark7) (h) | 0.0019 |  |  |  |
|  |  |  |  |  |  |  |

*Brute-force attack:* As there are totally 256 possible values for each *Pi* and at least *k* shares are required to reconstruct the secret image, attackers have to guess at least *k* number

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

Shares SSIM

[Fig. 1](#_bookmark7)(h) [Fig. 1](#_bookmark7)(g) [Fig. 1](#_bookmark7)(f) [Fig. 1](#_bookmark7)(e) [Fig. 1](#_bookmark7)(d)

*j*

of *Pi* values, which has *P*(256; *k*) = 256 × 255 × ··· ×

*j*

(256 — *k* + 1) possible values. Now for all *T* number of blocks of the secret image, the probability to reconstruct the original

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| [Fig. 1](#_bookmark7)(c) | 0.0201 | —0.0033 | 0.0101 | 0.0036 | 0.0044 |
| [Fig. 1](#_bookmark7)(d) | 0.0083 | 0.0013 | 0.0057 | 0.0012 |  |
| [Fig. 1](#_bookmark7)(e) | 0.0105 | 0.0108 | 0.0089 |  |  |
| [Fig. 1](#_bookmark7)(f) | 0.0015 | 0.0208 |  |  |  |
| [Fig. 1](#_bookmark7)(g) | 0.0103 |  |  |  |  |

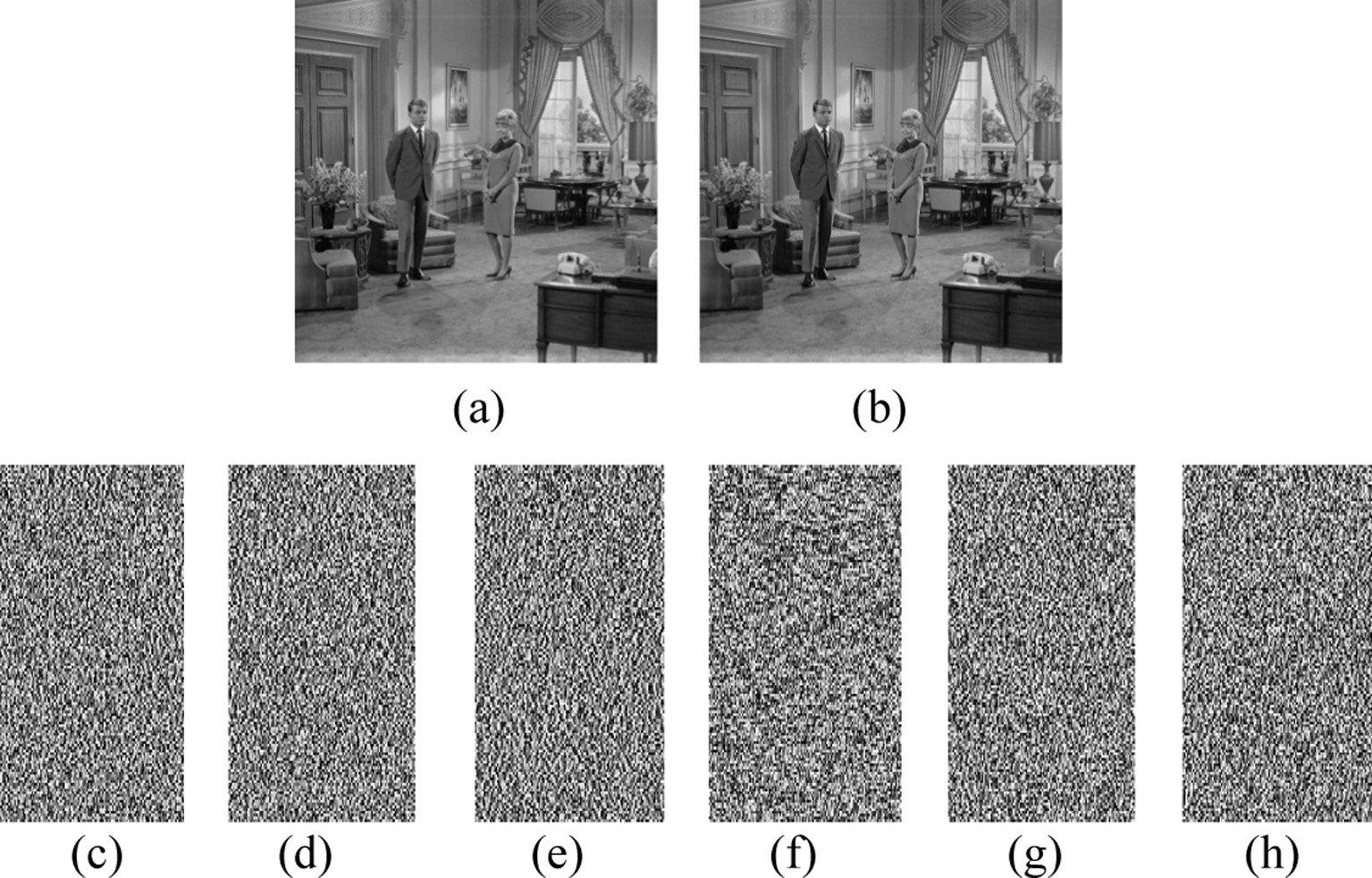
secret is 1 *T* = 1

*M*×*N* . This probability is really

(*p*(256;*k*))

(*p*(256;*k*)) *k*

depressed; yet less than the probability of Li et al.’s [[17]](#_bookmark18) scheme. Thus the proposed scheme is completely secure scheme that could protect the original secret against the brute force attack in a high probability.



208 A. Nag et al.

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

d

251

251

251

256

128

256

capability

where *m* = )*k*/4¶+ 1

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Thien–Lin [[6]](#_bookmark17) Zhao et al. [[7]](#_bookmark17) Lin–Wang [[8]](#_bookmark17) Wu [[9]](#_bookmark17) Chen–Fu [[10]](#_bookmark17) Propose | | | | | | | | | | | | |
|  |  | *M*×*N* |  | *M*×*N* |  | *M*×*N* |  | *M*×*N* |  | *M*×*N* |  | *M*×*N* |
| Probability of guessing  one correct share image | ÿ 1 | *k* | ÿ 1 | *k* | ÿ 1 | *k* | ÿ 1 | *k* | ÿ 1 | *k* | ÿ 1 | *k* |
| Cheating prevention/Verification NO | |  | YES |  | NO |  | NO |  | NO |  | YES |  |
| Distortion free | NO |  | NO |  | NO |  | YES |  | YES |  | YES |  |
| recovery |  |  |  |  |  |  |  |  |  |  |  |  |
| Extra storage | YES |  | YES |  | NO |  | NO |  | NO |  | NO |  |
| Encrypted shadow *M*×*N M*×*N M*×*N M*×*N* Same as original *m*×*M*×*N* ,  *k k k k k* | | | | | | | | | | | | |

*Collusion attack* [[18]](#_bookmark18)*:* 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](#_bookmark5)). Even if two participants *Ai* and *Aj* plan to recover the original secret image by exchanging their *Sei* and *Sej* values, their conspiracy

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| size  Secure channel is needed | YES | YES | NO | YES | secret image (*M* × *N*)  YES | NO |
| Probability of brute | Low | Low | Low | Low | Very low | Very low |
| force attack |  |  |  |  |  |  |
| Can resists collusion attack | NO | NO | YES | NO | NO | YES |

will be identified as each of participants *Ai* have provided their

unique identity number *IDi* to the dealer and published

{*IDi*, *sei* (*a*, *b*)}. This type conspiracy can easily be detected by other participants. Thus proposed scheme is robust against collusion attack.

* 1. *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]](#_bookmark17) are listed in [Table 3](#_bookmark14). The virtues of the pro- posed scheme are drawn as follows:

* *Probability of guessing:* For a secret image of size (*M* × *N* ), there are *N*×*N* 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)](#_bookmark6), at least *k* equa- tions are required. If a malicious user gathers (*k* — 1) sha- dow images, he/she can create only (*k* — 1) equations. The possibility of exact solution is then only 1 . Hence, for

*k*

256

*M*

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.

1. The original secret image cannot be reconstructed when any (*k* — 1) fewer shadows are gathered.
2. Each shadow is verifiable by others and thus no secure channel is required.
3. 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.

1. 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 meaning-

×*N* blocks, the possibility of receiving the correct image

*k M* less shares, which are hard to identify. It can also prevent

is ÿ 1 ×*N* . In contrast, the probability of Thien–Lin [[6]](#_bookmark17)

*k*

cheating in the existing secret image sharing schemes and

256

and Chen–Fu [[10]](#_bookmark17) are ÿ 1 *M* ×*N*

*k*

*k*

and ÿ 1 *M* ×*N*

respectively,

robust against brute force attack and collusion attack. The size

251

which are less than proposed scheme of ÿ 1 .

128

*M N*

of each shadow image is relatively small (*k* > 3). What is

×

*k*

256

* *Extra storage and distortion free recovery:* To avoid the truncation distortion and lossless recovery, the schemes [[6,7]](#_bookmark17) 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]](#_bookmark17) can recover the original secret image losslessly without extra storage. Though the scheme [[8]](#_bookmark17) 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]](#_bookmark17) but smaller (for *k* > 3) than Chen- Fu’s scheme [[10]](#_bookmark17).

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](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0005) [for image encryption. Opt Commun 2009;282:2123–7](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0005).
2. [Liu H, Wang X, Kadir A. Image encryption using DNA](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0010) [complementary rule and chaotic maps. Appl Soft Comput](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0010) [2012;12:1457–66](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0010).

A new (*k*, *n*) verifiable secret image sharing scheme 209

1. [Cheddad Abbas, Condell Joan, Curran Kevin, Mc Kevitt Paul.](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0015) [Digital image steganography: survey and analysis of current](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0015) [methods. Signal Process 2010;90(3):727–52](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0015).
2. [Blakley GR. Safeguarding cryptography keys. Proc AFIPS Natl](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0020) [Comput Conf 1979;48:313–7](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0020).
3. [Shamir A. How to share a secret. Commun ACM 1979;22(11):](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0025) [612–3](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0025).
4. [Thien CC, Lin JC. Secret image sharing. Comput Graph 2002;26(5):](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0030) [765–70](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0030).
5. [Zhao R, Zhao JJ, Dai F, Zhao FQ. A new image sharing scheme](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0035) [to identify cheaters. Comput Stand Interfaces 2009;31(1):252–7](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0035).
6. [Lin YY, Wang RZ. Scalable secret image sharing with smaller](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0040) [shadow images. IEEE Signal Process Lett 2010;17(3):316–9](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0040).
7. [Wu. A secret image sharing scheme for light images. EURASIP J](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0045) [Adv Signal Process 2013:49](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0045).
8. [Chen CC, Fu WY. A geometry-based secret image sharing](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0050) [approach. J Inf Sci Eng 2008;24(5):1567–77](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0050).
9. [Tso H-K. Sharing secret images using Blakley concept. Opt Eng](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0055) [2008;47(7)](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0055).
10. [Wu X, Ou D, Liang Q, Sun W. A user-friendly secret image](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0060) [sharing scheme with reversible steganography based on cellular](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0060) [automata. J Syst Softw 2012;85:1852–63](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0060).
11. [Chunqiang Hu, Liao Xiaofeng, Cheng Xiuzhen. Verifiable multi-](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0065) [secret sharing based on LFSR sequences. Theoret Comput Sci](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0065) [2012;445:52–62](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0065).
12. [Gong G, Harn L. Public-key cryptosystems based on cubic finite](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0070) [field extensions. IEEE Trans Inf Theory 1999;45(7):2601–5](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0070).
13. [Wang Z, Bovik AC, Sheikh HR, Simoncelli EP. Image quality](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0075) [assessment: from error visibility to structural similarity. IEEE](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0075) [Trans Image Process 2004;13(4):600–12](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0075).
14. [Sun Hung-Min. On-line multiple secret sharing based on a one](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0080) [way function. Comput Commun 1999;22(8):745–8](http://refhub.elsevier.com/S1110-8665(14)00033-4/h0080).
15. 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.

1. 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.