A New (k, n) Secret Image Sharing Scheme (SISS)

Amitava Nag[1], Sushanta Biswas[2], Debasree Sarkar[2], and Partha Sarkar[2]
[1]Academy of Technology, West Bengal University of Technology, India.
[2] Department of Engineering and Technological studies, University of Kalyani, India

Abstract: *In this paper, a new (k, n) threshold Secret Image Sharing Scheme (SISS) is proposed. In the proposed scheme the secret image is first partitioned into several non-overlapping blocks of k pixels. Every k pixel is assumed as the vertices of a complete graph G. Each spanning tree of G is represented by k pixels along with sequence and used to form k pixels of a share image. The original secret image can be restored by k or more shares and cannot be reconstructed by (k-1). The experimental results indicate that the proposed SISS is an efficient and safe method.*

Keywords: *(k, n) threshold secret image sharing, complete graph, spanning tree, Prüfer sequence.*

Received May 28, 2014; accepted March 3, 2015

1. Introduction

With rapid development of networking technologies, digital data is being transmitted easily through Internet. But security and protection of sensitive digital data during transmission is threaded concern in commercial, medical and military applications. Two methods cryptography [1, 6, 9, 16] and Steganography [4, 8, 19] have been used to increase the security of the digital data such as images. However, one of the common vulnerabilities of both of these methods is 'single point of failure' (SPOF) as they use single storage mechanism and thus data can be easily lost or damaged. Secret Image Sharing Schemes (SISS) are useful alternatives. The basic idea behind secret sharing is to transform a secret into n "shadows" or "shares" that can be transmitted and stored disjointedly. The secret can only be reconstructed from any k shadows ($k \leq n$) and any (k - 1) or fewer shadows cannot reveal anything about the secret.

In 1979, the secret sharing scheme (SIS) was first independently introduced by Blakley [2] and Shamir [13]. Shamir's secret sharing scheme is a (k, n) threshold-based secret sharing technique ($k \leq n$) in which (k - 1) degree polynomial function $f(x) = (d_0 + d_1x + d_2x^2 +…….. + d_{k-1}x^{k-1})$ mod P is created such that the coefficient d_0 is the secret data, P is a prime number and $d_1,d_2,…..d_{k-1}$ are random integers within [0,k - 1]. The secret shares are the pairs of values (x_i , y_i) where $y_i = f(x_i)$, $1 \leq i \leq n$ and $0 < x_1 < x_2 ….. <x_n \leq P -1$. When k or more secret shares are available, the coefficients $d_0,d_1,d_2,…..d_{k-1}$ of $f(x)$ can be derived with the help of the Lagrange interpolation and thus the secret value d_0 can be easily obtained.

In 2002, Thien and Lin [14] proposed an (k, n) threshold based secret image sharing scheme (SISS) by extending Shamir's polynomial approach. In their scheme, the authors cleverly applied the function $f(x) = (d_0 + d_1x + d_2x^2 +…….. + d_{k-1}x^{k-1})$ mod P, where d_0, d_1, d_2, …, d_{k-1} are the k consecutive pixels of secret image, P is chosen as 251 since 251 is the largest prime number within the range 0 to 255 for gray-scale images. Consequently, the pixel value larger than 250 is always truncated to 250 before the generation of shares. This loss of pixel value causes the truncation distortion which is the main drawback of Thien-Lin scheme. Another drawback of Thien-Lin scheme in terms of security is that before the computation of image share, this scheme requires the secret image to be permuted by a secret key. Thien's work attracted many researchers to propose different techniques which are given in the literature [7, 20]. However those two drawbacks are untouched. In 2013, Wu [18] solve the "truncation distortion" problem, but did not remove the permutation by secret key before share generation. Recently, Liu et.al. Proposed a secret image sharing approach which first quantized the secret image and then applied Shamir's (k, n) threshold concepts to share the quantized image [10]. However, due to quantization errors, the reconstructed image is not distortion free.

Blackley also proposed a secret sharing method by using geometric approach. According to his method, the secret is a point in a k-dimensional space and the hyper-planes in that space are defined by n shadows. The set of solutions $x=(x_1,x_2,….x_k)$ to the equation

$$\sum_{j=1}^{k} a_j x_j = B \qquad (1)$$

Creates a hyperplane. The secret is represented by the intersection point of any k or more of these hyperplane equations. For sharing of secret image, Blackley's geometric approach has been adopted by Chen-Fu [5]. 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 Blackley's concepts to share the quantized image [15]. Thus, reconstructed image is not lossless due to the quantization errors.

Another common drawback of all the above (k, n) threshold secret image sharing schemes is that none of these schemes deals with the identification of cheaters which is one of the standard security aspect. In all these schemes it is assumed that the original secret image holder (dealer) and the participants are honest. However the following two situations may also arise:

1. The cheating by the dealer: A dealer may send a fake share to a particular participant.

2. The cheating by a participant: One participant may submit a fake shadow during secret reconstruction.

The author proposed verifiable secret image sharing scheme in which the cheaters (a dishonest dealer or a dishonest participant) can easily be identified in [20]. But as the authors of [20] adopted Thien-Lin scheme for share generation and secret reconstruction, they used extra storage to avoid truncation distortion and lossless recovery.

In this paper, we propose a new (k, n) threshold secret image sharing scheme that does not involve the extra overheads such as permutation by secret key and quantization. The proposed scheme generates extremely noisy share images and can efficiently recover the distortion free secret image. Furthermore the proposed method only allows k or more verified participants to reconstruct the original secret.

2. Preliminaries

The proposed SISS discussed in this paper is based on the following basic principles:

1. A set of k pixels in the original secret image is represented using a complete graph G with k vertices.
2. A complete graph G may generate several spanning tress. Each can be uniquely identified using the *Prüfer* [3] sequence.
3. Any m bit number can be represented as X-ORed pair of m bit numbers. Such pairs if randomly chosen can be used to replace the original m bit number.

The equation (1) given in section 3 of the proposed SISS is developed using this *Prüfer* sequence. An m bit number is generated after performing certain operation on Equation 1. The principal 3 is then applied to this m bit number.

In this paragraph, the procedure of generating the Prüfer sequence of the spanning trees of the graph G is described. For a complete graph with k vertices, the number of spanning trees is $n=k^{k-2}$[3]. Thus for a graph with four vertices, there are 16 possible spanning trees as shown in figure 1, where a two-number sequence known as Prüfer sequence is associated with each spanning tree. A Prüfer sequence [12] of a complete graph of k vertices is any sequence of integers between 1 and k of length (k - 2). A complete graph G is given in figure 1-a with four vertices labelled as 1,2,3,4 and the 16 Prüfer sequences each of length two-number are {(1,1), (1,2), (1,3), (1,4), (2,1), (2,2), (2,3), (2,4), (3,1), (3,2), (3,3), (3,4), (4,1), (4,2), (4,3), (4,4)}. On the other hand, a Prüfer sequence of length (k-2) can find a unique labelled tree with k vertices. For example a two-number Prüfer sequence (2, 3) can uniquely decode a tree of label 1, 2, 3, 4 as shown in Figure 1-h.

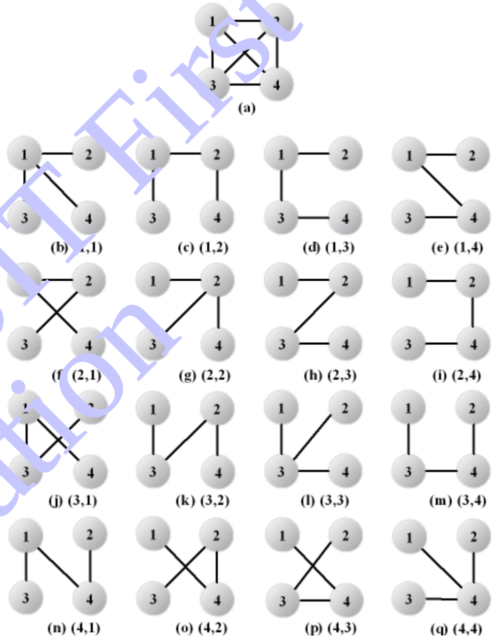


Figure 1. spanning trees of graph G with their corresponding Prüfer sequence.

In this paper we will generate share images with the help of the concept discussed above. A set of k consecutive pixels R_1, R_2, …, R_k of a secret image are first assumed as k vertices labelled as 1, 2, …, k of a complete graph and thus k^{k-2} Prüfer sequences each of length (k-2)-number can be obtained. Each *Prüfer* sequence of length (k-2)-number is combined with k pixels of original secret image and generates k pixels of a share image of the corresponding Prüfer sequence. The complete procedure of share generation and original secret reconstruction with the help of Prüfer sequence is discussed in section 3.

Now before going into the proposed SISS, let us consider how many m-bit pairs can be generated according to principal 3. The extent of this range will determine in how many different ways the pairs may be randomly chosen and thus guarantee the dissimilarity of the original number with the chosen pair.

- Lemma 1: The maximum number of usable possible m bit pairs whose X-OR will result in a particular m bit number is $(2^{m-1}-1)$.

- Proof: Number of m bits number are 2^m. If one pair of m bit number is used to generate a m bits number by X-OR operation, then there are 2^{m-1} number of pairs possible. Now one pair with 0 and the number itself cannot be included as $0 \oplus N=N$. Thus number of usable pairs i.e. excluding 0 and the number itself are $(2^{m-1}-1)$.

3. Proposed Secret Image Sharing Scheme (SISS)

In this section we propose a verifiable secret image sharing scheme based on the Zhao *et al.* [20] scheme for verification and Pr iifer [12] sequence for share generation and reconstruction. Our proposed secret image sharing scheme (SISS) consist of three phases: Initialization phase, share construction and reconstruction. Section 3.1 presents initialization phase, section 3.2 presents the share generation phase and section 3.3 presents the recovery with verification phase.

3.1. Initialization phase

Let, D denotes the trusted dealer and $P=\{P_1, P_2, \ldots, P_n\}$ denotes the set of n participants. In this phase, no secure communication channel is required between the dealer and the participants. The detail description of the initialization phase is given in Algorithm 1.

Algorithm 1: The initialization phase

1. *The dealer D first chooses two large prime number p and q and compute $N= p\times q$.*
2. *D selects an integer g from interval $[\sqrt{N}, N]$ such that g is relatively prime to p and q and publishes {g.N} in public bulletin.*
3. *Each participant $P_i \in P$, randomly selects an integer k_i (i=1,2,….n) from the interval [2,N] as its own secret shadow and compute $Z_i = g^{k_i} modN$ .Then each participant P_i supply Z_i and its identity number Id_i to D via public channel.*
4. *For any two participants P_i and P_j, D must ensure that $Z_i \neq Z_j$. If D has $Z_i=Z_j$ for two different participants P_i and P_j, then D ask P_i to select another new integer k_i (i=1,2,….n) from the interval [2,N].*
5. *Finally each participant P_i publishes $\{Id_i, Z_i\}$ in public bulletin.*

3.2. Share construction Phase

This section discusses how to construct noisy share images from original secret image. To generate shadows, we first partition a secret image into non-overlapping blocks of k pixels. Each of the k pixels is assumed to be the vertices of a complete graph. The spanning trees of the graph are parameterized with Prüfer sequence and stored into share images. Shares construction mechanism is illustrated in Algorithm 2.

Algorithm 2: Shares construction mechanism

Input: A Secret Image I_s of size $H\times W$, the value of k ($k\geq 3$) and n

Output: n share images $S_1,S_2,\ldots\ldots,S_n$ of size $H\times W$

1. *Dealer D randomly chooses an integer k_0 from the interval [2, N], such that k_0 is relatively prime to (p - 1) and (q - 1) and generates an integer d such that $d\times K_0=1mod\phi(N)$, where $\phi(N)$ is the Euler phi-function.*
2. *D performs the following:*

   a) Computes $Z0=g^{K0}modN$ and $I_i = Z_i^{k_0} modN$ for each participant P_i and publishes (Z_0,d).

   b) Selects a hash function H and generates $M_i=H(I_i)$ for each participant P_i.
3. *Divide the Secret Image into T number of non-overlapping blocks $\{B_r\}_{r=1}^{T}$ of $1\times k$ pixels, where $T = \frac{H\times W}{k}$.*
4. *Set i to 1*
5. *Set r to 1.*
6. *Obtain the sum of k consecutive pixels $\{R_1,R_2,\ldots\ldots R_k\}$ of block B_i with the help of i^{th} Pr iifer as*

$$s_i = \sum_{j=1}^{k} C_j R_j \quad (2)$$

Where $\forall j=1\ldots k$, $C_j = m+1$ and m represents the number of times j is repeated in the i^{th} Pr iifer sequence.

7. *a) Obtain a bit sequence of size $M=(K-2)log_2k$ from i^{th} Pr iifer sequence as $b^p_{M-1}\ldots\ldots\ldots b^p_1 b^p_0$,where b^i_j Î { 0,1} .*

   b) Obtain a bit sequence of size B = (4k-M) from s_i as $b^S_B\ldots\ldots b^S_1 b_0$

   c) Divide M_i (M_i is generated in step 2(b)) into k non-overlapping blocks D_r of size B bits, where $1\leq r\leq k$, $k\times B< |M_i|$ and $D_r = b^H_{B-1}\ldots\ldots b^H_1 b^H_0$ (The symbol $|.|$ represents cardinality)

   d) Perform X-OR operation between $Dr(1\leq r\leq k)$ and s_i and obtain a B bits sequence as $b'_{B-1}\ldots\ldots\ldots b'_1 b'_0$ .Each is repeated for X-OR operation with s_i after every k blocks of original secret image.

   e) Obtain a number N_c of 4k bits long by appending the bit sequence $b'_{B-1}\ldots\ldots b'_1 b'_0$ at the end of the sequence $b^p_{M-1}\ldots\ldots\ldots b^p_1 b^p_0$ as $N_c = b^p_{M-1}\ldots\ldots b^p_1 b^p_0 = b_{4k-1} b_{4k-2}\ldots\ldots b_1 b_0$
8. *Obtain two 4k bits number $N_1 = b^1_{4k-1}\ldots\ldots b^1_1 b^1_0$ and $N_2 = b^2_{4k-1}\ldots\ldots b^2_1 b^2_0$ such that $b_{4k-1} b_{4k-2}\ldots\ldots b_1 b_0 = b^1_{4k-1}\ldots\ldots b^1_1 b^1_0$ Å $b^2_{4k-1}\ldots\ldots b^2_1 b^2_0$.*
9. *Concatenate the bits sequence N_1 and N_2 and generates an 8k bits sequence as $b^i_{8k-1}\ldots\ldots b^i_1 b^i_0 = b^2_{4k-1}\ldots\ldots b^2_1 b^2_0 b^1_{4k-1}\ldots b^1_1 b^1_0$*
10. *Generate k pixels:*

$$p^i_1 = b^i_7\ldots\ldots\ldots\ldots b^i_1 b^i_0$$

$$p^i_2 = b^i_{15}\ldots\ldots\ldots\ldots b^i_9 b^i_8$$

………………………

………………………

$$p^i_k = b^i_{8k-1}\ldots\ldots\ldots b^i_{8k-7} b^i_{8k-8}$$

and sequentially assign them to the i^{th} shadow

11. *Increase r by 1*
12. *Repeat steps 6 through 11 until r>T for the i^{th} Pr iifer sequence*
13. *Increase i by 1*
14. *Repeat step 5 through 13 until i>n.*

The dealer D each time performs the above steps to shares a new secret image I_s and generates n encrypted share images {S_1, S_2, …, S_n}. D is also responsible to distributes the share images {S_1, S_2, …, S_n} to n participants {P_1, P_2, …, P_n}. According to Lemma 1, (N_1, N_2) pair can be randomly chosen from (2^{4k-1}-1) pairs, which makes the shared images {S_1, S_2, …, S_n} more noisy.

3.3. Recovery phase with verification

This section introduces a scheme to reconstruct the original secret image from k or more share images. Let k legal members of P={P_1, P_2, …, P_n} are agreed to recover the secret image. The verification and recovery scheme of the original secret image from the shares supplied by k verified participants is described in Algorithm 3.

```
Algorithm 3: Recovery phase with verification
Input: Any k number of share images $S_1,S_2,\ldots\ldots,S_n$ of size H×W and the value of k
Output: Original Secret Image $I_s$ of size H×W
1. Each $P_i$ computes $I_i^{'} = Z_0^{k_i} modN$ to get the share
2. Any participants $P_j$ in P $P_i {}^{1} P_j$ can verify $I_i^{'}$ provided by $P_i$ and then test if $I_i^{'d} = Z_i modN$ .If the test is successful, then $P_i$ is identified as legal participant and share $S_i$ given by $P_i$ is accepted and then goto step 3, otherwise $P_i$ considered as cheater and exit.
3. Each legal participant $P_i$ generates $M_i^{'} = H(I_i^{'})$ . $M_i^{'}$ is divided into k non-overlapping blocks $D_r^{'}$ $(1 \leq r \leq k)$ of size B=(4k - M) bits, where $M = (k - 2)log_2 k$ and $k \times B <|M_i|$.
4. Divide each shadow image $S_i$ into T number of non-overlapping blocks $\{B_r^i\}_{r=1}^T$ of 1×k pixels, where $T = \frac{H \times W}{k}$ and $1 \leq i \leq k$
5. Set r to 1.
6. Set i to 1.
7. For k consecutive pixels $p_1^i, p_2^i, \ldots\ldots, p_k^i$ of block $B_r^i$ in shadow image $S_i$ obtain the binary sequence as
   $p_1^i = b_7^i \ldots\ldots\ldots b_1^i b_0^i$
   $p_2^i = b_{15}^i \ldots\ldots\ldots b_9^i b_8^i$
   ……………………….
   ……………………….
   $p_k^i = b_{8k-1}^i \ldots\ldots b_{8k-7}^i b_{8k-8}^i$
8. Concatenate the bits stream of all k pixels and generate a bit sequence of size 8k as $b_{8k-1}^i \ldots\ldots b_1^i b_0^i$
9. Divide the 8k bits sequence into two, 4k bit sequence as $N_1 = b_{4k-1}^1 \ldots\ldots\ldots b_1^1 b_0^1$ and $N_2 = b_{4k-1}^{22} \ldots\ldots b_1^2 b_0^2$
10. Obtain one 4k bits sequence $N_c = b_{4k-1} b_{4k-2} \ldots\ldots b_1 b_0$ as
   $b_{4k-1} b_{4k-2} \ldots\ldots b_1 b_0 = b_{4k-1}^1 \ldots\ldots b_1^1 b_0^1$ Å $b_{4k-1}^2 \ldots\ldots b_1^2 b_0^2$
    11. Extract first (from MSB) M bits stream from $N_c$ and generate a Pr iifer sequence {$f_1$, $f_2$, ……, $f_{k-2}$}. The remaining (4k - M) bits of $N_c$ and (4k - M) bits of $D_r$ ($D_r$ is generated in step 3) are XORed and generates a number $s_i$.
    12. Create a linear equation:
        $\sum_{j=1}^{k} C_{ij} R_j = s_i$    (3)
        where $\forall j = 1 \ldots k$ , $C_{ij}$ = m +1 and m represents the number of times j is repeated in the Pr iifer sequence {$f_1$, $f_2$, ……, $f_{k-2}$}.
    13. Increase i by 1.
    14. Repeat steps 7 through 13 until i>k
    15. k number of linear equations of type (3) are created
    16. Use these k equations to solve $R_1$, $R_2$, …., $R_k$ in Equation 3. They are the corresponding k pixel values of the secret image $I_s$.
    17. Repeat steps 6 through 16 until r>T.
```

The above steps are when performed can recover the original secret image I_s of size $H \times W$ without any distortion. The proposed scheme can also be applied to the color images. This scheme performs well on color images as it completely free from any type of truncation distortion. For generation of shared images from a color image first it is divided into three gray scale images corresponding to the Red, the Green and the Blue planes. Then shared images are generated from each of the Red, Green and Blue planes separately by applying the proposed share generation scheme for gray scale image. Finally shadows for color images are generated by gathering the corresponding shadows from the Red, Green and Blue planes. Figure 2 illustrates the complete procedure to generate n share images from a color image.

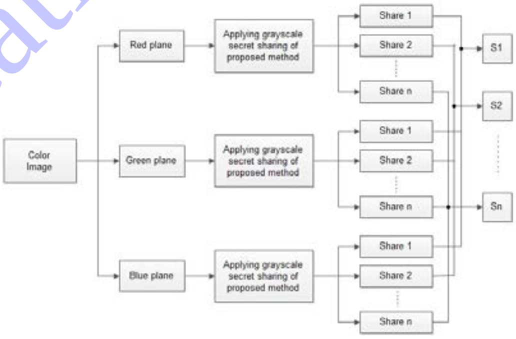

Color Image
Red plane
Green plane
Blue plane
Applying grayscale secret sharing of proposed method
Applying grayscale secret sharing of proposed method
Applying grayscale secret sharing of proposed method
Share 1
Share 2
Share n
Share 1
Share 2
Share n
Share 1
Share 2
Share n
S1
S2
Sn

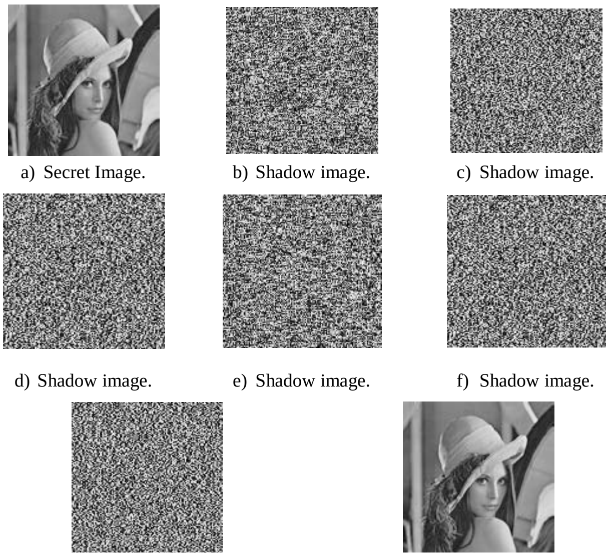
Figure 2. Share generation scheme of the color image.

Though the color channels are generally correlated, however in our paper, the proposed scheme is basically based on randomness. So in this case the color channels are almost uncorrelated. This may be clear from the experimental results as shown in Figure 4 and Table 2.

4. Experimental Results and Discussion

4.1. Experimental Results

This section demonstrates the experimental results of the proposed (k, n) secret image sharing scheme. A (4, 6) secret sharing experiment is selected to demonstrate the performance of the proposed method. Gray scale test image “Lena” of size 256×256 is used as secret (input) image as shown in Figure 3-a and figure 3-h is the reconstructed image. Both of these images are identical. Figure 3-b, 3-c, 3-d, 3-e, 3-f and 3-g shows six noisy share images.



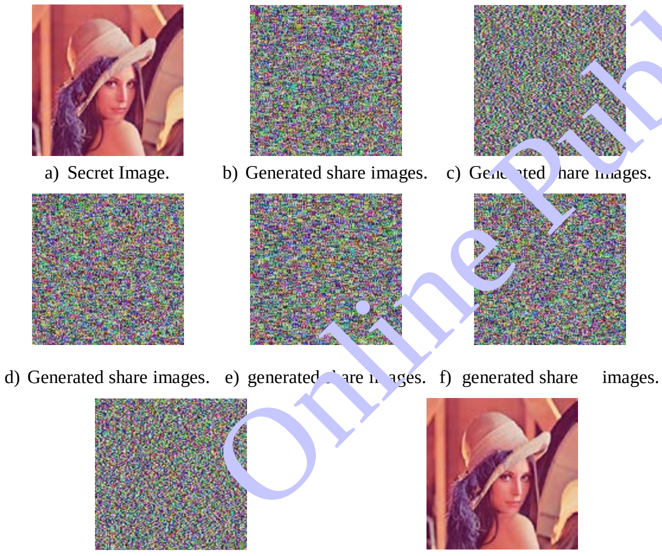
a) Secret Image. b) Shadow image. c) Shadow image.

d) Shadow image. e) Shadow image. f) Shadow image.

g) Shadow image. h) Reconstructed image.

Figure 3. Secret (input) images.

To demonstrate the performance of the proposed (4,6) secret sharing method on color images the image of Lena of size 256×256 is used as secret (input) image as shown in Figure 4-a and 4-h is the reconstructed image. Both of these images are identical Figure 4-b, 4-c, 4-d, 4-e, 4-f and 4-g shows generated noise like shadows using the proposed method for color images.



a) Secret Image. b) Generated share images. c) Generated share images.

d) Generated share images. e) generated share images. f) generated share images.

g) generated share images. h) reconstructed image.

Figure 4. A (4, 6) secret image sharing example of proposed method for color images.

4.1. Analysis of Correlation Coefficient

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

Where: $cov(x,y) = \frac{1}{H\times W}\sum_{i=1}^{H\times W}(x_i - E(x))(y_i - E(y))$

$$E(x_i) = \frac{1}{H\times W}\sum_{i=1}^{H\times W} x_i, D(x) = \frac{1}{H\times W}\sum_{i=1}^{H\times W}(x_i - E(x))^2$$

In our experiment (x, y) pair chosen as one pair of adjacent pixels in vertical, horizontal and diagonal directions. To calculate the correlation coefficients of pair of adjacent pixels, we selects 2048 random pairs of adjacent pixels in all three direction from the secret image and encrypted shared images. The correlation coefficients in three directions are listed in table 1. For color images, the correlation between shared pixels in all three directions have been computed and tabulated in Table 2 with a comparison with a purely image encryption scheme described in [5]. The comparison shows that computed results of the proposed method is really encouraging.

4.3. Analysis of Structural Similarity Index Metric (SSIM).

To check how dissimilar our shares from the original secret image, we have used another well-known quality metric know as Structural Similarity Index Metric (SSIM). It was developed by Wang et al. [17] 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 ranges from 0 to 1. A value of 0 means two images (original and encrypted) are totally dissimilar and 1 means the reverse one. If two images are I_1 and I_2, the SSIM is defined as:

$$SSIM(I_1, I_2) = \frac{(2\mu_{I_1}\mu_{I_2} + C_1)(2\sigma_{I_1I_2} + C_2)}{(\mu_{I_1}^2 + \mu_{I_2}^2 + C_1)(\sigma_{I_1}^2 + \sigma_{I_2}^2 + C_2)} \quad (5)$$

Where μ_{I_1} and μ_{I_2} are the mean intensity of I_1 and I_2 respectively, $\sigma_{I_1}^2$ and $\sigma_{I_2}^2$ are the variance of I_1 and I_2 respectively; $\sigma_{I_1I_2}$ the covariance between I_1 and I_2. $C_1=(k_1L)^2$, $C_2=(k_2L)^2$ 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) are chosen as k_1=0.01; k_2=0.03. SSIM values of share images for our experimentation are given in Table 3 and table 4. The SSIM values of the table 3 and table 4 shows that each encrypted share is completely dissimilar from original image and other encrypted shares. These strengthen the claim of the security of the proposed method.

4.4. Analysis of Differential Attack

The number of changing pixel rate (NPCR) and the unified average changed intensity (UACI) are used to measure the resistance capability of encrypted image for differential attack. These two quantities are mathematically defined by Equations 7 and 8:

$$D(i,j) = \begin{cases} 0, if I^1(i,j) = I^2(i,j) \\ 1, if I^1(i,j) \neq I^2(i,j) \end{cases} \quad (6)$$

$$NPCR = \frac{\sum_{i,j} D(i,j)}{H \times W} \times 100\% \quad (7)$$

$$UACI = \frac{1}{H \times W} \sum_{i,j} \frac{|I^1(i,j) - I^2(i,j)|}{255} \times 100\% \quad (8)$$

Where $I^1(i, j)$ and $I^2(i, j)$ are the gray-scale value of the original image and the encrypted image, respectively. The high NPCR values represent that the position of each pixel is dramatically randomized and the proper UACI values indicate that the intensity levels of almost all pixels in the shared encrypted image are changed [6]. Table 5 and table 6 show that the proposed method has high NPCR and proper UACI values, which indicates that the encrypted shared images generated by our proposed scheme are robust against differential attack.

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

Direction	Original-Figure-a (r_{xy})	Proposed		Wu *et.al.* [19]		Lin *et.al.* [9] (r_{xy})
		Shares	r_{xy}	Shares	r_{xy}	
Horizontal	0.9768	Figure 3-b	0.0024	1	0.0066	0.0004
		Figure 3-c	0.0228	2	-0.0010	
		Figure 3-d	0.0074	3	-0.0027	
		Figure 3-e	0.0062	4	0.0090	
		Figure 3-f	0.0149			
		Figure 3-g	0.0055			
Vertical	0.9132	Figure 3-b	0.0089	1	0.0211	0.0021
		Figure 3-c	0.0045	2	-0.0101	
		Figure 3-d	-0.0019	3	0.0097	
		Figure 3-e	-0.0013	4	-0.089	
		Figure 3-f	0.0030			
		Figure 3-g	0.0035			
Diagonal	0.9428	Figure 3-b	0.0026	1	-0.0074	-0.0038
		Figure 3-c	0.0050	2	0.0056	
		Figure 3-d	-0.0093	3	-0.0101	
		Figure 3-e	-0.0020	4	0.0205	
		Figure 3-f	0.0145			
		Figure 3-g	0.0019			

Table 2. Comparisons of the correlation coefficient r_{xy} of Lena (color).

Direction	Original (r_{xy})	Proposed		Huang *et al.* [6] (r_{xy})
		Shares	r_{xy}	
Horizontal	0.9581	Figure 4-b	[illegible]	0.1257
		Figure 4-c	0.0225	
		Figure 4-d	[illegible]	
		Figure 4-e	0.0047	
		Figure 4-f	0.0070	
		Figure 4-g	0.0089	
Vertical	0.9801	Figure 4-b	0.0011	0.0581
		Figure 4-c	0.0107	
		Figure 4-d	-0.0086	
		Figure 4-e	-0.0083	
		Figure 4-f	0.0009	
		Figure 4-g	0.0002	
Diagonal	0.9491	Figure 4-b	0.0020	-0.0504
		Figure 4-c	0.0038	
		Figure 4-d	-0.0033	
		Figure 4-e	-0.0026	
		Figure 4-f	0.0048	
		Figure 4-g	0.0031	

Table 3. SSIM values between each share and original image of the proposed scheme.

Shares	SSIM Figure 3-a
Figure 3-b	0.0093
Figure 3-c	0.0097
Figure 3-d	0.0072
Figure 3-e	0.0080
Figure 3-f	0.0095
Figure 3-g	0.0102

Table 4. SSIM values between each pair of shares generated by the proposed scheme.

Shares	SSIM				
	Figure 3-g	Figure 3-f	Figure 3-e	Figure 3-d	Figure 3-c
Figure 3-b	0.0100	-0.0033	0.0051	-0.0066	0.0042
Figure 3-c	0.0115	0.0016	0.0111	0.0007	
Figure 3-d	0.0085	0.0190	0.0094		
Figure 3-e	0.0008	0.0128			
Figure 3-f	0.0093				

Table 5. Results of NPCR and UACI tests of gray- image (Lena).

	Proposed (average)	Ar[illegible] *et al.*[1]	Lin et al. [9] (rxy)	Wu *et al.* [19]
NPCR (%)	[illegible]	99.61	99.60	87.65
UACI (%)	32.23	30.50	28.13	32.80

Table 6. Results of NPCR and UACI tests of color image (Lena).

	Proposed (average)			Huang *et al.* [9]		
	R	G	B	R	G	B
NPCR (%)	99.48	99.65	99.56	99.42	99.60	99.54
UACI (%)	[illegible]	26.01	24.05	27.78	27.66	24.94

4.5. Reconstruction Complexity

The computation complexity of Shamir's (k, n) threshold scheme in recovery phase is O(k $\log^2$ k) as it uses polynomial evaluation and interpolation. Since Thien *et al.*[5] used Shamir's (k, n) threshold scheme directly in their proposed SISS ,thus the computation complexity of [5] for the recovery phase is the same as that of Shamir's. The SISSs proposed in [6, 10, 18, 20] are all based on Thien *et al.*[5] scheme and thus the reconstruction complexity is also $O(k \log^2 k)$. However, after reconstruction the schemes in [7,14,18,20] requires inverse permutation by secret key for complete decryption of the secret image. This also charge some extra computation cost.

On the other hand, the scheme of Chen-Fu [5] and proposed scheme uses LUP decomposition in the recovery phase. Because of the triply nested loop structure of LUP decomposition, both of Chen-Fu [5] and proposed (k,n) threshold SISS have an algorithmic complexity for the recovery phase of $O(k^3)$. After reconstruction, the secret image is completely decrypted without any permutation by secret key and thus no extra cost is needed in both of Chen-Fu [5] and proposed SISS.

4.6. Security Analysis

This section analyzes the security performance of the proposed scheme from the angle of confidentiality and participant verification. By theoretical analysis, we prove in the following that the proposed scheme is secure and verifiable.

4.6.1. Confidentiality

Suppose only (k - 1) participants desire to pull the original secret. However, in share reconstruction k equations are needed to obtain the k coefficients (actually pixels) R_1 to R_k from Eq. (3). But from (k - 1) shares, only (k - 1) equations can be created. Thus to reconstruct the original secret successfully the only way is to guess one missing share for creating Eq. (3). In this case, the probability of guessing the exact solution is then $\frac{1}{256}$. Hence for $\frac{H \times W}{k}$ blocks, the possibility of obtaining the correct image is $(\frac{1}{256})^{\frac{H \times W}{k}}$. As a result, it is very difficult for the (k - 1) participants to reconstruct the original secret image. Hence the proposed scheme holds enough confidentiality.

4.6.2. Participant Verification

The proposed SISS owns the participant verification capability which can easily prevent cheating by identifying illegal participant.

- Lemma 2: Other participants can verify whether a participant is a legal member or not.
- Proof: In the proposed scheme each participant P_i computes $Z_i = g^{k_i} \bmod N$ at the initialisation phase and publishes it. Other participants can use Z_i for verification of P_i. Now assume that P_i wants to impersonate as a legal member and provides a secret key $k_i^{'}$ to compute $I_i^{'} = Z_0^{k_i^{'}} \bmod N$ and supply it gain original secret. Now anyone could test whether P_j is legal by computing:

$$\begin{aligned} I_i^{'d} &= Z_0^{k_i^{'}d} \bmod N \\ &= \left(g^{k_0} \bmod N\right)^{k_i^{'}d} \bmod N \\ &= \left(g^{k_0 k_i^{'} d} \bmod N\right) \bmod N \\ &= \left(g^{k_i^{'} k_0 d} \bmod N\right) \bmod N \\ &= \left(g^{k_i^{'}} \bmod N\right) \bmod N \\ &= Z_i^{'} \bmod N \end{aligned}$$

[Since $d \times k_0 = 1 \bmod \phi(N)$]

If a participant P_i is legal and does not intends to cheat, then $k_i^{'} = k_i$ and thus $I_i^{'d} = Z_i^{'} \bmod N = Z_i \bmod N$. On the other hand if $I_i^{'d} \neq Z_i \bmod N$ for a secret key $k_i^{'}$, then P_i is not a legal one and has provided wrong secret key $k_i^{'}$.

- *Theorem 1*: The proposed secret sharing is verifiable because any member is able to clearly distinguishes the legal and illegal (cheater) participant.
- *Proof*: From Lemma 2, it can be concluded that the proposed scheme is verifiable.

4.7. Comparison

Comparative studies among the proposed scheme and the related secret image sharing schemes [5, 7, 10, 11, 18, 20] have been presented in table 7. Comparing to these recently recorded (k, n) secret image sharing schemes, the merits of the proposed (k, n) SISS are summarized as follows:

- *Robustness*: The proposed SISS is robust because in the proposed scheme only k honest participants can together recover the original secret image.
- *Confidentiality*: The proposed scheme can produce highly confidential encrypted share images.
- *Probability of Guessing*: The probability of guessing one correct share image of our proposed method is the least one among all existing secret image sharing schemes.
- *No Extra Overhead*: The proposed scheme does not involve any extra overhead such as permutation or quantization (share construction phase) and inverse permutation or inverse quantization (recovery phase). Such type of extra overhead increases the total computation cost of the schemes [6, 12, 16, 17].
- *Cheating Prevention*: The proposed approach has cheating prevention capability which is one of the main security requirements of secret image sharing schemes.
- *Recovery Type*: The proposed scheme can reconstruct the original secret image without any loss. This is one of the prime merits.

The theoretical analysis and experimental results show that the proposed (k, n) secret image sharing scheme has better merits that existing (k, n) secret image sharing scheme.

Table 7. Comparison among related (k,n) secret image sharing schemes

	Chen *et al.* [5]	**Zhao *et al.* [20]**	**Lin *et al.* [7]**	**Wu [18]**	**Liu *et al.* [10]**	**Ou *et al.* [11]**	**Proposed**
Probability of guessing one correct share image	$\left(\frac{1}{128}\right)^{\frac{H \times W}{k}}$	$\left(\frac{1}{251}\right)^{\frac{H \times W}{k}}$	$\left(\frac{1}{251}\right)^{\frac{H \times W}{k}}$	$\left(\frac{1}{256}\right)^{\frac{H \times W}{k}}$	$\left(\frac{1}{256}\right)^{P_s}$	$\left(\frac{1}{2}\right)^{H \times W}$	$\left(\frac{1}{256}\right)^{\frac{H \times W}{k}}$
Participant Verification	No	Yes	No	No	No	Yes	Yes
Reconstruction complexity	$O(k^3)$	$O(k \log^2 k)$	$O(k \log^2 k)$	$O(k \log^2 k)$	$O(k \log^2 k)$	$O(n)$	$O(k^3)$
Extra Overhead	No Extra Overhead	Permutation and Inverse Permutation	Permutation and Inverse Permutation	Permutation and Inverse Permutation	Quantization and Inverse Quantization	No Extra Overhead	No Extra Overhead
Recovery Type	Lossless	Lossy	Lossy	Lossless	Lossy	Lossless	Lossless
Color Depth	Gray	Gray	Gray	Gray	Gray	Binary	Gray and Color

7. Conclusion

The proposed scheme presents a novel Secret Image Sharing Scheme (SISS) with two components - namely, a complete graph construction by selecting the pixels of original secret image as vertices and representation of spanning trees with Pr*iifer* sequence along with secret pixels. This scheme owns the following properties:

1. Except k, no extra information is required;
2. the secret image can be reconstructed by any k or more shares without any loss i.e. the proposed method does not suffer from truncation distortion.
3. the secret cannot be reconstructed by any (k - 1) as the probability of guessing of one share is too low;
4. The proposed scheme perform well on color images as truncation distortion problem is completely eliminated.
5. As each share is verifiable by other participants, the proposed scheme can prevent the participants from cheating before decryption.
6. The proposed scheme can recover the original secret without any distortion. The experimental results and comparisons show the novelty of the work.

References

[1] Arthanari S., Mastan M., and Bagank B, Chaotic Image Encryption using Modular Addition and Combinatorial Techniques, The International Arab Journal of Information Technology, Vol. 12, No. 2, pp.110-117, March 2015.

[2] Blakely G-R, “Safeguarding cryptography keys,” in Proc. of AFIPS National Computer Conference, vol. 48, pp. 313 - 317, 1979.

[3] Cayley A., “A theorem on trees,” J. Math., 23:376 - 378,1889.

[4] Cheddad A, Condell J., Curran K., Paul Mc Kevitt, “Digital image steganography: Survey and analysis of current methods”, Signal Processing Volume 90, Issue 3, March 2010, Pages 727-752.

[5] Chen C-C. and Fu W-Y., “A geometry-based secret image sharing approach.”, Journal of Information Science and Engineering, 24(5). 1567 - 1577 (2008).

[6] Huang C-K., Nien H-H., "Multi chaotic systems based pixel shuffle for image encryption," Optics Communications, vol. 282, pp. 2123-2127, 2009.

[7] Lin Y-Y., Wang R-Z., “Scalable Secret Image Sharing with Smaller Shadow Images”, in IEEE Signal Processing Letters, vol. 17, no. 3, pp. 316 - 319, March 2010.

[8] Lip Y-P., Delina B., Tan F-A., and Sim Y- O., “An Enhanced Mechanism for Image Steganography Using Sequential Colour Cycle Algorithm,” IAJIT International Arab Journal of Information Technology, Vol.10, No. 1,pp. 51-60,January 2013.

[9] Liu H., Wang X., Kadir A., “Image encryption using DNA complementary rule and chaotic maps”, Applied Soft Computing Vol.12, pp.1457-1466, (2012).

[10] Liu L, Wang A, Chang CC, Li Z. A novel real-time and progressive secret image sharing with flexible shadows based on compressive sensing. Signal Processing: Image Communication Vol.29,No.1,pp.128-134,2014.

[11] Ou D., Ye L., Sun. W, "User-friendly secret image sharing scheme with verification ability based on block truncation coding and error diffusion", Journal of Visual Communication and Image Representation Vol. 29,No. 1, pp. 46-60,2015.

[12] Prufer H., “Never beweis eined satzes uber permutation,”Arch.Math.Phys.Sci.,27:742-744,1918.

[13] Shamir A., “How to share a secret,” in Communications of the ACM, vol. 22, no. 11, pp. 612-613,1979.

[14] Thien C-C., Lin J-C., “Secret image sharing”, in Computer Graphics, vol. 26, no.5, pp. 765 - 770, 2002.

[15] Tso H-K., “Sharing secret images using Blakely concept”, Optical Engineering, vol 47,no 7, 2008.

[16] Wang X., Liu L., Zhang Y., "A novel chaotic block image encryption algorithm based on dynamic random growth technique", Optics and Lasers in Engineering vol. 66, no.1 pp.10-18,2015.

[17] Wang Z., Bovik A-C., Sheikh H-R., and Simoncelli E-P., “Image quality assessment: from error visibility to structural similarity”, IEEE Transactions on Image Processing, vol. 13, no. 4, pp. 600-612, 2004.

[18] Wu X., A secret image sharing scheme for light images, EURASIP Journal on Advances in Signal Processing 2013:49.

[19] Wu X., Ou D., Liang Q., Sun W., “A user-friendly secret image sharing scheme with reversible steganography based on cellular automata”, The Journal of Systems and Software 85 (2012) 1852- 1863.

[20] Zhao R., Zhao J-J., Dai F., Zhao F-Q., “A new image sharing scheme to identify cheaters.”, Computer Standard and Interfaces, vol. 31, no. 1,pp.252 - 257, 2009.

Amitava Nag received his M. Tech. degree from University of Calcutta,Kolkata,India in 2005. Currently he is working as an Assistant Professor and Head in Dept. of IT, Academy of Technology, India and also working towards his PhD at the Dept. of Engineering and Technological Studies, University of Kalyani,,India. He is a member of IEEE, ACM and CSI. His areas of interest include Image Processing, Information Security, and Data Mining.

Sushanta Biswas obtained his Ph.D in engineering from Jadavpur University in the year 2004. He obtained his M.E from Jadavpur University and B.E from Bengal Engineering College (Presently known as Bengal Engineering and Science University, Shibpur) in the year 1994 and 1990 respectively. He is presently working as Associate Professor in the Dept. of Engineering and Technological Studies, University of Kalyani. He has more than 14 years of teaching experience. His area of interest includes, Artificial Neural Network, Image Processing, Frequency Selective Surfaces, Microstrip Antennas.

Debasree Sarkar has obtained her Ph.D degree in Engineering from Jadavpur University in the year 2005. She has obtained her M.E and B.E from Bengal Engineering College (presently known as Bengal Engineering and Science University, Shibpur) in the year 1994 and 1991 respectively. She is presently working as Associate Professor in Dept. of Engineering and Technological Studies, University of Kalyani. She has more than 14 years of teaching experience. Her area of research includes Artificial Neural Network, Microstrip Antenna, Frequency Selective Surfaces, and Embedded Systems.

Partha Sarkar obtained his Ph.D in engineering from Jadavpur University in the year 2002. He has obtained his M.E from Jadavpur University in the year 1994. He earned his B.E degree in Electronics and Telecommunication Engineering from Bengal Engineering College (Presently known as Bengal Engineering and Science University, Shibpur) in the year 1991. He is presently working as Professor and Head at the Dept. of Engineering and Technological Studies, University of Kalyani. His area of research includes, Microstrip Antenna, Microstrip Filter, Frequency Selective Surfaces, and Artificial Neural Network. He has contributed to numerous research articles in various journals and conferences of repute. He is also a life Fellow of IETE.