DE GRUYTER OPEN

BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **14**, No 2

Sofia • 2014

Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.2478/cait-2014-0023

Secret Image Sharing Scheme Based on a Boolean Operation

Amitava Nag, Sushanta Biswas**, Debasree Sarkar**, Partha Pratim Sarka***

** Academy of Technology West Bengal University of Technology Hooghly 721212 – India*
*** Department of Engineering and Technological studies University of Kalyani Kalyani 741 235 – India*
E-mail: amitavanag.09@gmail.com

Abstract: *Traditionally extensive researches have been done on secret image sharing which support the fault tolerance property. But their reconstruction complexity is high. Some research papers on secret image sharing are also available with smaller reconstruction complexity, due to the use of a Boolean operation. But these research works lack the fault tolerance property which is the heart of secret sharing. This paper deals with a general (k, n) secret image sharing scheme for gray scale images with both low reconstruction complexity and preservation of the fault tolerance property. Moreover, the proposed sharing generation technique can also be applied on colour images.*

Keywords: *Secret image sharing, Boolean operation, reconstruction complexity, fault tolerance property.*

1. Introduction

Due to the widespread use of Internet, the sharing and transmission of secure information over insecure networks causes one of the most challenging security issues. Therefore, finding ways to transmit secretly data through Internet has become an important issue. Two methods, cryptography and steganography have been used to protect secure data from malicious users on Internet. Cryptography

transforms the secret data into a meaningless form, which can easily attract malicious users during transmission through Internet. The other method – steganography, is used to provide secure transmission by hiding the secret data into a cover medium to avoid observation. These two methods are of Single Point Of Failure (SPOF) type since they use a single storage mechanism. Therefore these two methods are not robust against loss or modification.

The secret sharing schemes were proposed by B l a k l e y [1] and S h a m i r [2] independently in 1979. It is technique of protecting secret data, like images by dividing the secret data into n pieces (each piece is known as a shadow share) and distribute the shares among n participants. Each participant is allocated a share of the secret that looks meaningless. The original image can be recovered only when any k of them are combined together, but any $k - 1$ or fewer shares cannot have sufficient information to reconstruct the original one.

In 1979 Shamir developed the idea of a (k, n) threshold-based secret sharing technique ($k \leq n$). The technique allows a polynomial function of order $k - 1$ constructed as follows

(1) $$f(x) = d_0 + d_1x + d_2x^2 + \ldots + d_{k-1}x^{k-1} \pmod{P},$$

where the value d_0 is the secret, P is a prime number and d_1, d_2, …, d_{k-1} are randomly determined from integers within $[0, P - 1]$. The secret shares are the pairs of values (x_i , y_i) where $y_i = f(x_i)$, $1 \leq i \leq n$ and $0 < x_1 < x_2, \ldots, <x_n \leq P - 1$.

The polynomial function $f(x)$ is destroyed after each shareholder possesses a pair of values (x_i, y_i), so that no single shareholder knows the secret value d_0. In fact, no groups of $k - 1$ or fewer secret shares can discover the secret d_0. Note that for a larger degree (larger value of k) of the polynomial $f(x)$, more shares are distinguished from the secret d_0.

On the other hand, when k or more secret shares are available, then we may set at least k linear equations $y_i = f(x_i)$ for the unknown d_i's. The unique solution to these equations shows that the secret value d_0 can be easily obtained using Lagrange interpolation. In Shamir's SSS, knowing even $k - 1$ linear equations does not expose any information about the secret. The recombination of shares to generate the secret k is done by using the following Lagrange interpolation formula

(2) $$\begin{cases} d_0 = \sum_{i=0}^{k-1} y_i \beta_i, \\ \beta_i = \prod_{j=0, j\neq i}^{k-1} \frac{-x_j}{x_i - x_j}. \end{cases}$$

The algorithmic complexity is $O\left(k\log^2 k\right)$ for polynomial evaluation and interpolation which indicates that Samir's method has computational complexity of $O\left(k\log^2 k\right)$.

In 2002 T h i e n and L i n [3] proposed a (k, n) threshold based secret image sharing scheme by cleverly applying Shamis's polynomial approach. The essential idea is to use a polynomial function of order $k - 1$ to construct n image shares, in which the size of each share image is only $1/k$ times of the original image, but the computational complexity is the same as in Samir's scheme. This work attracted many researchers to propose different techniques which are given in references [4-7]. But in [3] T h i e n and L i n proposed a method in which the pixels having

a value greater that 251, are truncated into 250. Recently, in [8] Lin and Wang proposed a (k, n) secret sharing method. In [8] the reconstructed image is lossy in nature for $k < n$ and lossless for $k = n$. The method proposed in [8] supports the fault tolerance property, but the computational complexity at the recovery phase is $O\left(k\log^2 k\right)$, since they also adopted Thien and Lin secret sharing method. Recently, W u [16] proposed a secret image sharing scheme for light images. This scheme improves the Thien-Lin scheme by replacing the prime number 251 by 257. These types of secret sharing schemes are known as traditional non-visual Secret Sharing (SS).

Another type of a secret sharing scheme is Visual Secret Sharing (VSS) [9-15], which was first designed in 1995 by N o a r and S h a m i r [9], based on the (k, n)-threshold concept. In VSS scheme, out of n, any k or more shares can reconstruct the original image "visually" by superimposing the shares and it does not involve any complex computations. One of the major drawbacks of VSS is the pixel expansion and low image quality.

W a n g et al. [14] proposed in 2007 a lossless (n, n) secret sharing scheme for gray scale images based on a Boolean operation without pixel expansion and preserving the reconstruction accuracy. The authors first generate $n - 1$ random matrices R_1, R_2, ..., R_{n-1} and then generate n ($n \geq 2$) shadows from the secret gray-scale image G as given below:

$$\begin{cases} S_1 = R_1 \\ S_2 = R_1 \oplus R_2 \\ \quad \ldots \ldots \ldots \\ S_{n-1} = R_{n-2} \oplus R_{n-1} \\ S_n = R_{n-1} \oplus G \end{cases} . \tag{3}$$

The original image is reconstructed with the help of all n shares S_1, S_2, …, S_n by the following computation:

$$G = S_1 \oplus S_2 \oplus S_3 \oplus \ldots \oplus S_n \ldots \tag{4}$$

From the above reconstruction technique it can be observed that to reconstruct the original secret image, all n shares are required, any $n - 1$ or fewer cannot reconstruct a lossy or lossless version of the original secret image, i.e,. Wang's technique does not support the fault tolerance property which is the main requirement of secret sharing.

The aim of this paper is to improve the scheme proposed by W a n g et al. [14] by developing a (k, n), $2 \leq k \leq n$, secret image sharing scheme based on a Boolean operation with the same reconstruction complexity.

In this paper we have proposed a (k, n), $2 \leq k \leq n$, secret image sharing scheme based on a Boolean operation with no reconstruction complexity.

2. The proposed scheme

In this section a secret sharing (k, n) algorithm is proposed based on a Boolean operation. The work is divided into three phases: (i) initialization phase, (ii) share generation phase, and (iii) reconstruction phase.

2.1. Initialization phase

In this section the original secret holder (also known as dealer) and the participant need some inter-communication. Each participant T_i chooses ID_i as his/her own identity number and provides their own identity number to the dealer. For any pair of participants T_i and T_j, the dealer must ensure that $\mathrm{ID}_i \neq \mathrm{ID}_j$.

2.2. Share generation phase

In the proposed (k, n), $2 \le k \le n$, secret image sharing scheme, n noise-like shares are generated from a secret image G of the same size $h \times w$ by three steps.

Step 1. n–1 distinct matrices $\{R_1, R_2, \ldots, R_{n-1}\}$ of size $h \times w$ are generated, such that

$$\begin{cases} S = G + 2^n, \\ \sum_{i=1}^{n-1} R_i = S, \\ R_i \neq R_j \ \text{for } 1 \le i \ne j \le n-1, \end{cases} \tag{5}$$

where $R_i = \{R_i[a,\ b]\ |R_i[a,\ b] \in [0, 255],\ 1 \le a \le h,\ 1 \le b \le w\}$.

Step 2. Generate a random matrix R_n, where

$$R_n = \{R_n[a, b]\ |R_n[a, b] \in [0, 255], \quad 1 \le a \le h, \quad 1 \le b \le w\}.$$

Step 3. Generate n share images S_i

$$S_i = \begin{cases} R_i \oplus R_n & \text{if } 1 \le \mathrm{i} \le \mathrm{n} - 1, \\ R_n. \end{cases} \tag{6}$$

The symbol $\oplus$ represents a bitwise X-OR.

The correlation among the elements of the individual matrix R_i generated at Step 1 is not lost though the elements are generated randomly from the original secret images, as these elements are generated from the correlated elements of the generated matrix. But this correlation is totally broken after the Boolean operation (X-OR) with the elements of totally randomly chosen elements of matrix R_n. Thus the elements of S_i in Step 3 generated by (6) are totally uncorrelated and noise-like, which is desired for secret sharing. The complete share generation scheme is shown in Fig. 1.

Definition [20]. A cryptosystem has perfect secrecy if $H(A/B)=A(A)$, where $H(A/B)$ represents conditional entropy, which is the amount of uncertainty in A, given B.

Theorem 1. Each share image S_i gives no information about the original secret image.

Proof: Consider the X OR operation $B = A \oplus R$, where $A, B, R \in \{0, 1\}^n$. Now, if we X OR A on both sides of $B = A \oplus R$ as

$$A \oplus B = A \oplus A \oplus R = R\,.$$

This has for each A and B, R a unique value because $R = A \oplus \mathrm{B}$. Since there is a total number of 2^n possible sequences of $R \in \{0, 1\}^n$, the probability of R is $1/2^n$ which is the same as B.

Since R and B have the same probability $1/2^n$, we have

$$H(R) = H(B) = -\log_2(1/2^n) = n,$$

where $H(R)$ And $H(B)$ are the entropy of R and B respectively.

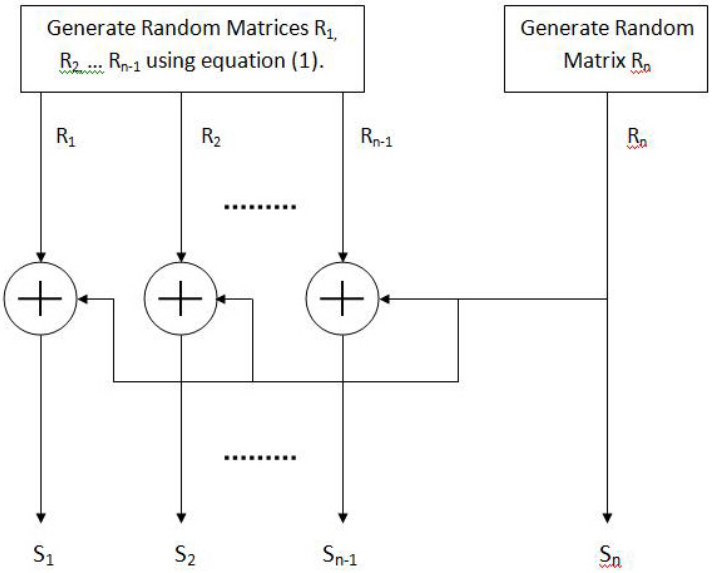


Fig. 1. Share generation

$H(A, R, B)$ can be calculated in two different ways.

Case 1. Knowing that (A, R, B) is the same as (A, R) and since A and R are independent, $H(A, R, B)$ can be represented as

$$H(A, R, B) = H(A, R) = H(A) + H(R).$$

Again, knowing that (A, R, B) is the same as (A, B) and since $R = A \oplus B$, i.e., A and B determine R for XOR operation and hence we have

$$H(A, R, B) = H(A, B) = H(A/B) + H(B).$$

Therefore from case 1 and case $2H(A/B) = H(A)$, since $H(R)=H(B)$.

This proves that X-OR operation $B = A \oplus R$ has perfect secrecy (from Definition 1), i.e., $B = A \oplus R$ is completely unbreakable and encrypted.

Now in our proposed share generation scheme, as S_n is a random matrix, the obtained share images $S_i = R_i \oplus R_n$ (generated in Step 3) are completely encrypted, unbreakable and distinct. This proves that each share image S_i gives no information about the original secret image.

The following example illustrates the proposed share generation scheme in details. Let G be the original image:

$$G = \begin{bmatrix} 124 & 138 & 153 & 116 \\ 117 & 121 & 151 & 127 \\ 106 & 95 & 118 & 153 \\ 95 & 87 & 149 & 127 \end{bmatrix}.$$

We can find out R_i, i=1, 2, 3, using equation (5) as:

$$R_1 = \begin{bmatrix} 93 & 59 & 152 & 106 \\ 53 & 28 & 88 & 92 \\ 14 & 77 & 32 & 147 \\ 50 & 19 & 79 & 114 \end{bmatrix},$$

$$R_2 = \begin{bmatrix} 30 & 58 & 2 & 2 \\ 44 & 75 & 75 & 2 \\ 11 & 2 & 61 & 5 \\ 2 & 16 & 59 & 2 \end{bmatrix},$$

$$R_3 = \begin{bmatrix} 17 & 37 & 15 & 25 \\ 36 & 34 & 4 & 49 \\ 97 & 32 & 41 & 17 \\ 59 & 68 & 27 & 27 \end{bmatrix},$$

where $R_1 + R_2 + R_3 = G + 16$. Next, we generate another random matrix R_4, $0 \leq R_4 \leq 255$,

$$R_4 = \begin{bmatrix} 82 & 130 & 110 & 158 \\ 224 & 27 & 251 & 253 \\ 249 & 214 & 45 & 146 \\ 236 & 35 & 106 & 154 \end{bmatrix}.$$

Now four different shares can be generated by equation (6) as follows:

$$S_1 = R_1 \oplus R_4 = \begin{bmatrix} 15 & 185 & 246 & 244 \\ 213 & 7 & 163 & 161 \\ 247 & 155 & 13 & 1 \\ 222 & 48 & 37 & 232 \end{bmatrix},$$

$$S_2 = R_2 \oplus R_4 = \begin{bmatrix} 76 & 184 & 108 & 156 \\ 204 & 80 & 176 & 255 \\ 242 & 212 & 16 & 151 \\ 238 & 51 & 81 & 152 \end{bmatrix},$$

$$S_3 = R_3 \oplus R_4 = \begin{bmatrix} 67 & 167 & 97 & 134 \\ 196 & 57 & 255 & 204 \\ 152 & 246 & 4 & 131 \\ 215 & 103 & 113 & 129 \end{bmatrix},$$

$$S_4 = R_4 = \begin{bmatrix} 80 & 130 & 110 & 158 \\ 224 & 27 & 251 & 253 \\ 249 & 214 & 45 & 146 \\ 236 & 35 & 106 & 154 \end{bmatrix}.$$

In this phase when the share images are generated, the dealer assigns a name to the share images S_1, S_2, ..., S_n as ID_1, ID_2 ... ID_n respectively. Then each participant T_i (whose identity number is ID_i) chooses his/her own share image S_i (whose name is ID_i. This naming convention will help to apply an appropriate reconstruction algorithm discussed in Section 2.3).

2.3. Reconstruction scheme

Our reconstruction phase involves two different cases. In the first case, if any one or more number of shares and the last shares are available, the secret can be easily reconstructed. In the second case if any two or more shares, excluding the last one

are available, then the secret image can be recovered, which is never possible by Wang's method.

Let $T = \{T_1, T_2, \ldots, T_n\}$. The members of T will cooperate to recover the original secret.

2.3.1. Reconstruction technique 1

While any one or more members of

$$T = \{T_1, T_2, \ldots, T_{n-1}\}$$

and the participant T_n gather their shares, then the original secret is reconstructed, using similar calculation of the share construction scheme in two steps.

Step 1. Any k–1 shares and the last share S_n (total k shares) collected together are first X OR and $k - 1$ number of random matrices is produced $\{R_1, R_2, \ldots, R_{k-1}\}$ as follows:

$$R_i = S_i \oplus S_n \quad for \quad 1 \leq i \leq k-1 \ldots \tag{7}$$

Step 2. Number $k - 1$ of matrices $\{R_1, R_2, \ldots, R_{k-1}\}$ are then added and they reconstruct the secret image as follows:

$$G = \begin{cases} \left(\sum_{i=1}^{k-1} R_i\right) \bmod 256 & \text{for } k < n, \\ \sum_{i=1}^{k-1} R_i - 2^n & \text{for } k = n. \end{cases} \tag{8}$$

For reconstruction of the original image, any $k - 1$ shares S_i, $1 \leq i \leq k-1$ and the last share S_n of uncorrelated elements are used. Each share S_i after a Boolean operation (X-OR) with the share S_n produces R_i which are again correlated to some extent. Now if one or more than one of these R_i is available, the original secret image will be recovered. When all R_i $1 \leq i \leq n$ will be available, the secret image will be recovered without any loss. Here lies the novelty of the work.

To demonstrate the revealing process using the first reconstruction scheme, we choose $k = n = 4$ and the original image G is reconstructed without any loss as

$$G = S_1 \oplus S_4 + S_2 \oplus S_4 + S_3 \oplus S_4 = \begin{bmatrix} 124 & 138 & 153 & 116 \\ 117 & 121 & 151 & 127 \\ 106 & 95 & 118 & 153 \\ 95 & 87 & 149 & 127 \end{bmatrix}.$$

2.3.2. Reconstruction technique 2

The main problem of the above reconstruction algorithm is that if the last share S_n (share of the participant T_n) is lost or damaged or not available, the reconstruction is not possible. Thus we have proposed another reconstruction method, in which if any two or more numbers of shares are available, the reconstruction is possible by simple XOR and add operations. However, if a fewer number of shares are available. the quality of reconstruction is to be sacrificed to some extent, though the secret image is recognizable preserving the fault tolerance property. Thus the limitation of the availability of the last share for reconstruction is completely

avoided. An important point may be noted here that if any two or more (multiple of two) shares (S_i, where $I \neq n$) except the last one are available, then

$$R = S_i \oplus S_j = R_i \oplus S_n \oplus R_j \oplus S_n = R_i \oplus R_j \ldots \tag{9}$$

The matrix R here is not dependent on S_n as above shown. R is dependent on R_i and R_j. The elements of R_i and the elements of R_j are self correlated. Thus the elements of $R_i \oplus R_j$ or R are also correlated. The share reconstruction process from any k shares without the last share is described as follows:

Step 1. Calculate G_{ij} and G as

$$G = \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} (S_i \oplus S_j) \bmod 256, \tag{10}$$

where $(S_i \oplus S_j) = G_{ij}$ is independent of the last share S_n.

To demonstrate the revealing process using the second reconstruction scheme, first $k = 2$ has been chosen and the secret image G_{ij} is reconstructed as:

$$G_{12} = S_1 \oplus S_2 = \begin{bmatrix} 67 & 1 & 154 & 104 \\ 25 & 87 & 19 & 94 \\ 5 & 79 & 29 & 150 \\ 48 & 3 & 116 & 112 \end{bmatrix},$$

$$G_{23} = S_2 \oplus S_3 = \begin{bmatrix} 76 & 30 & 151 & 114 \\ 17 & 62 & 92 & 109 \\ 111 & 109 & 9 & 130 \\ 9 & 87 & 84 & 105 \end{bmatrix},$$

$$G_{13} = S_1 \oplus S_3 = \begin{bmatrix} 15 & 31 & 13 & 26 \\ 8 & 105 & 79 & 51 \\ 106 & 34 & 20 & 20 \\ 57 & 84 & 32 & 25 \end{bmatrix},$$

$$G = G_{12} + G_{23} + G_{13} = S_1 \oplus S_2 + S_2 \oplus S_3 + S_1 \oplus S_3 =$$

$$= \begin{bmatrix} 158 & 62 & 255 & 244 \\ 50 & 254 & 190 & 254 \\ 222 & 222 & 58 & 255 \\ 114 & 174 & 232 & 242 \end{bmatrix}.$$

This reconstruction scheme is applied when any k members of $T = \{T_1, T_2, \ldots, T_{n-1}\}$ except the participant T_n provide their share images.

We can extend our proposed scheme to colour images. A colour image can be broken into three gray scale images corresponding to the Red, the Green and the Blue planes and generate shadows from each plane individually, using the proposed share generation scheme for gray scale image. Then final shadows for the colour images are generated by composing the corresponding shadows from the Red, Green and Blue planes. Fig. 2 shows how to generate n share images from one colour image.

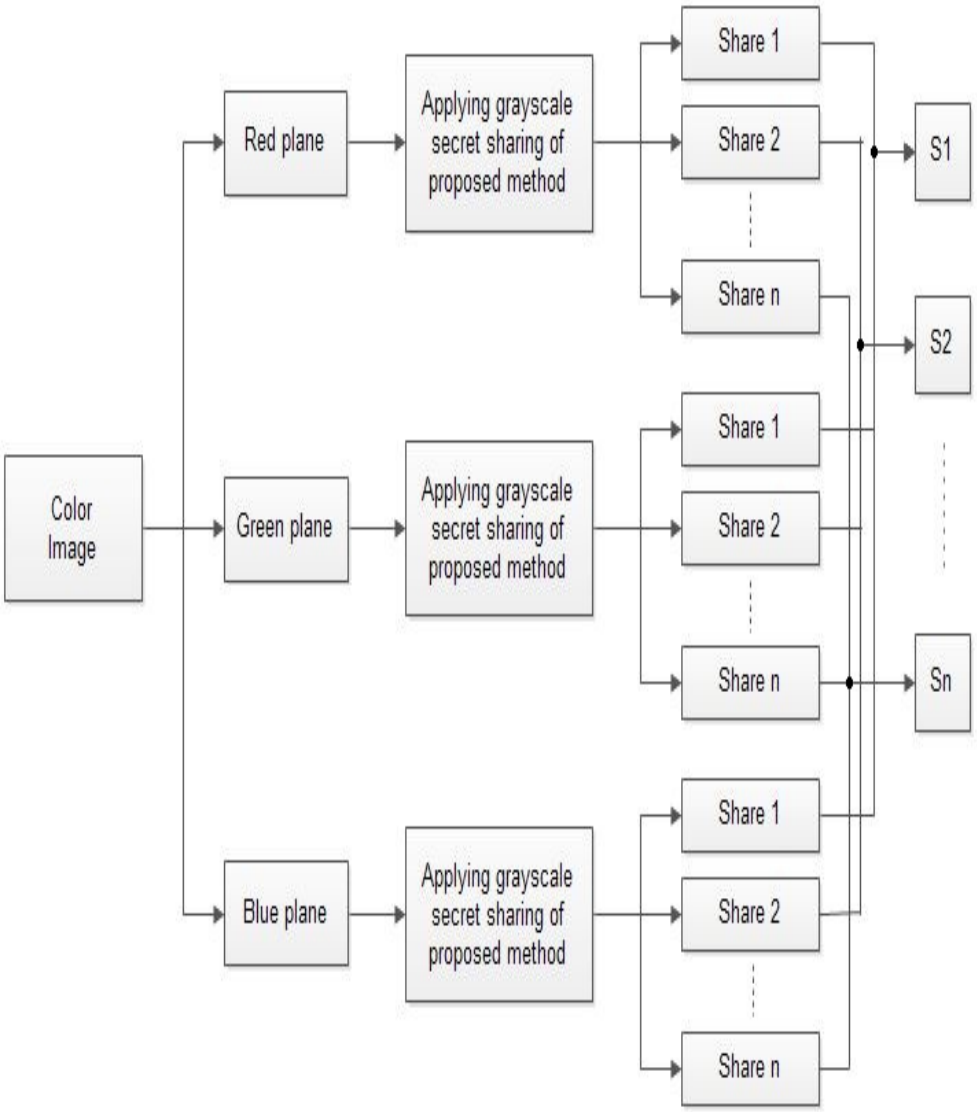
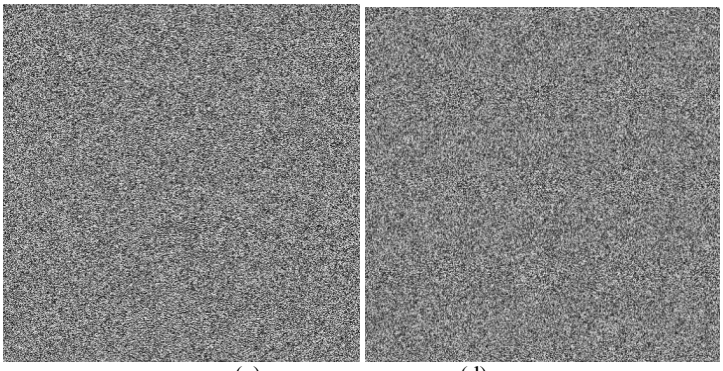


Fig. 2. Share generation scheme of a colour image

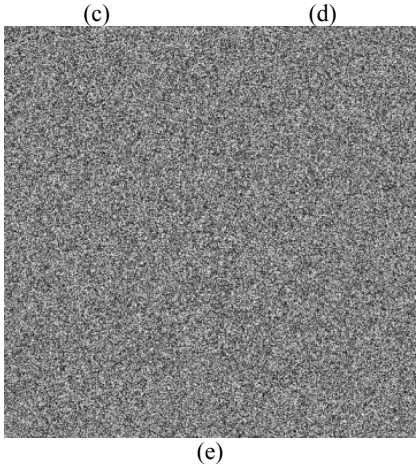
3. Experimental results

This section presents the experimental results of the proposed (k, n) secret image sharing scheme. A (2, 4) secret sharing experiment is selected to demonstrate the performance of the proposed method. A test image "Lenna" of size 512×512 is used as a secret (input) image as shown in Fig. 3(a). Fig. 3(b)-(e) shows the generated noise like a shadow image using the proposed method.

(a) (b)



(c) (d)



(e)

Fig. 3. A (2, 4) secret image sharing example of the proposed method: (a) secret image; (b) – (e) generated share images

Fig. 4 shows the reconstructed secret images discussed in Subsection 2.2.1, where Fig. 4(a), (b) and (c) are the reconstructed images from any one and the last one (S_n), the reconstructed image from any two and the last one (S_n) and the reconstructed image from all four shares.

(a) PSNR=25.71 (b) PSNR=31.48

(c) PSNR=∞

Fig. 4. Images reconstructed in the proposed (2, 4) sharing method with any (k–1) and last share

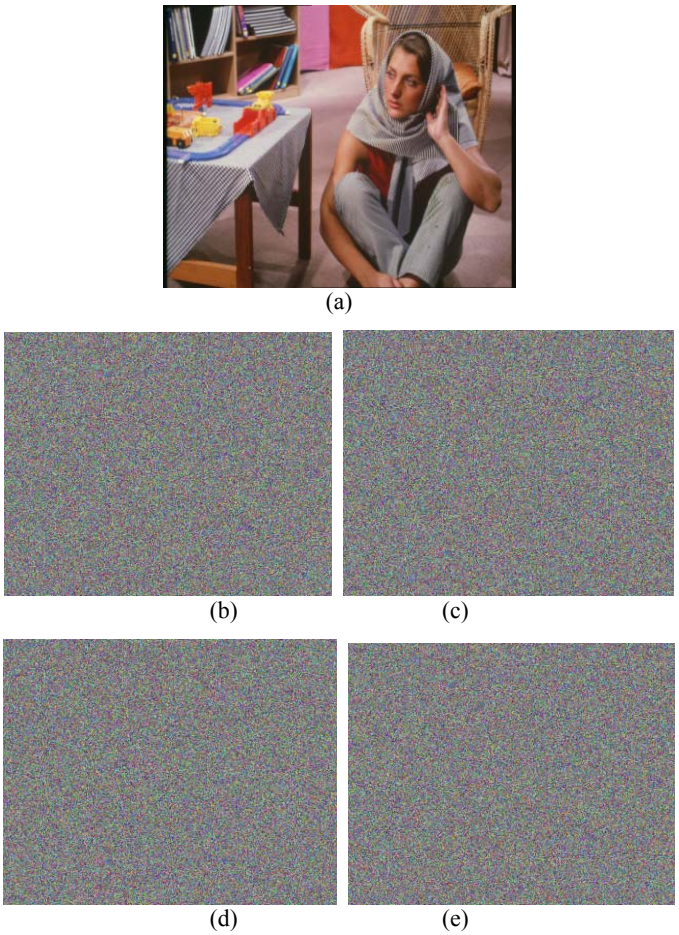
The images that are reconstructed using the technique discussed in Subsection 2.2 have been shown in Fig. 5. In Fig. 5, (a) and (b) show the reconstructed images from any two share images and from any three share images respectively, using the proposed (2, 4) sharing method.

(a) PSNR=25.68 (b) PSNR=32.19

Fig. 5. Images reconstructed from any 2 or more shares except the last one

To demonstrate the performance of the proposed (2, 4) secret sharing method on colour images the image of Barbara of size 640×512 is used as a secret (input)

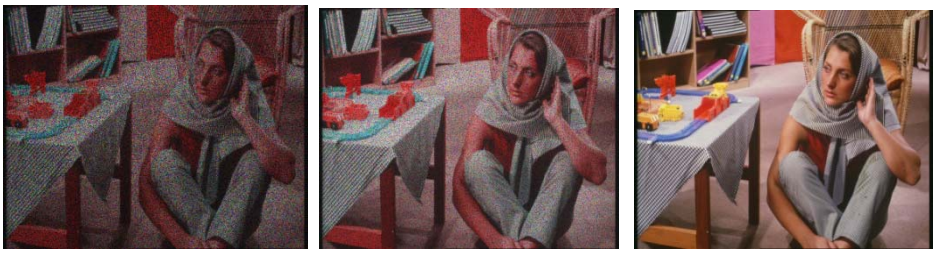
image, shown in Fig. 6(a). Fig. 6(b) to (e) show the generated noise like a shadow image using the proposed method for colour images.



(a) (b) (c) (d) (e)

Fig. 6. A (2, 4) secret image sharing example of the proposed method for colour images: (a) secret image; (b)-(e) generated share images

Fig. 7(a), (b) and (c) are the reconstructed images from any one and the last one (S_n), the reconstructed image from any two and the last one (S_n) and the reconstructed image from all four shares.



(a) PSNR=25.88 (b) PSNR=33.01 (c) PSNR=∞

Fig. 7. Images reconstructed in the proposed (2, 4) sharing method with any k–1 and the last share

In Fig. 8, (a) and (b) show the reconstructed images from any two share images and from any three share images respectively, using the proposed (2, 4) sharing method.

(a) PSNR=24.91 (b) PSNR=31.02

Fig. 8. Images reconstructed from any 2 or more shares except the last one

3.1. Accuracy

The Peak Signal to Noise Ratio (PSNR) is applied to measure the quality of the reconstructed image. The higher PSNR indicates a better quality and lower PSNR denotes worse quality. The definition of PSNR is given in (11), (12). The typical values for PSNR in a lossy image are within the range from 20 to 40 dB [17]:

$$\mathrm{PSNR(dB)} = 20\log_{10}\frac{255}{\sqrt{\mathrm{MSE}}}, \tag{11}$$

where MSE is the mean squared error between the original image and the modified image which is defined as

$$\mathrm{MSE} = \frac{1}{M\times N}\sum_{x=1}^{M}\sum_{y=1}^{N}\big(I(x,y) - I'(x,y)\big)^2. \tag{12}$$

Table 1. Comparison of PSNR of the reconstructed images of C h a n g et al. [17] and the proposed scheme

Scheme	Gray-scale image (Lena)		Colour image (Barbara)	
	max	min	max	min
Proposed scheme	∞	25.68	∞	24. 91
C h a n g et al. [17]	33.70		33.75	

The PSNR of the reconstructed gray-scale and of the reconstructed colour image is 33.70 and 33.75 respectively. On the other hand, the lowest and height PSNR of the proposed scheme are 24.91 and ∞ respectively. Table 1 shows the PSNR values of the proposed scheme and the scheme of C h a n g et al. [17].

3.2. Analysis of a differential attack

The Number of the Changing Pixel Rates (NPCR) and the Unified Average Changed Intensity (UACI) are designed to measure the resistance ability of the encrypted image against a differential attack. These two quantities are mathematically defined in following equations:

$$D(i,j) = \begin{cases} 0 & \text{if } C^1(i,j) = C^2(i,j), \\ 1 & \text{if } C^1(i,j) \neq C^2(i,j), \end{cases} \tag{13}$$

(14) $$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\ \%,$$

(15) $$\text{UACI} = \frac{1}{M \times N} \sum_{i,j} \frac{|C^1(i,j) - C^2(i,j)|}{255} \times 100\ \%,$$

where $C^1(i, j)$ and $C^2(i, j)$ are the gray-scale value of the original image and the encrypted image, respectively. The theoretical NPCR and UACI values of the image are 99.6094% and 33.4635%, respectively [19]. The 99.6094% value of NPCR represents that the position of each pixel is dramatically randomized and the 33.4635% value of UACI values indicates that the intensity levels of almost all pixels in the shared encrypted image are changed [17]. Table 2 shows that the average values of NPCR (> 99%) and UACI (≈ 33%) of the proposed method are very close to the theoretical values, which indicates that a tiny change in the original secret image will create a significant change in the encrypted (share) image. Therfore, the encrypted shared images generated by our proposed scheme are robust against a differential attack.

Table 2. Values of NPCR and UACI tests of encrypted images of a gray image

Test	Proposed (average)	[17]	[18]
NPCR (%)	99.67	56.2	99.60
UACI (%)	32.23	56.2	28.13

Table 3. Values of NPCR and UACI tests of encrypted images of a colour image

Test	Proposed (average)			[17]
	R	*G*	*B*	
NPCR (%)	99.48	99.65	99.56	70.1
UACI (%)	26.85	26.01	24.05	32.8

Table 3 shows the average values of NPCR (> 99%) and UACI (≈ 33%) for each component of the colour images which are also close to the theoretical value. Hence, the proposed scheme for colour images is also robust against a differential attack.

3.3. Complexity analysis

In [2] the computational complexity for the polynomial evaluation and interpolation is $O(k\log^2 k)$. Since Thien, and Lin have adopted Shamir's (k, n) scheme, their computational complexity for the recovery phase is the same as that of Shamir's scheme, i.e. $O(k\log^2 k)$. Lin and Wang's scheme in [10] is also based on the scheme proposed by Thien, and Lin, which raises the computational complexity to $O(k\log^2 k)$ for the recovery phase.

The reconstruction process presented in this paper computes n images using X-OR and algebraic addition operations, resulting in computational time proportional to n. The image construction is proportional to $k - 1$ because it includes X-OR of all n shares and addition of $k - 1$ shares. Therefore, the computational complexity is also dependent on the image size. So, computational complexity of $O(k)$, $k \leq n$ is established in this paper.

Our method employs only arithmetic and Boolean operations rather than any geometric calculation, that is why it leads to low computational complexity. The

methods related are compared with the proposed scheme in Table 4. The second row of Table 3 shows the comparison in terms of computational complexity of the proposed method and the related works.

Table 4. Comparison between the related image sharing and the proposed scheme

Image scheme	Wang et al. [14]	Chang et al. [17]	Lin et al.[8]	Our Proposed Method
(k, n) secret sharing	No	No	Yes	Yes
Reconstruction complexity	$O(n)$	$O(n)$	$O(k\log^2 k)$	$O(k)$
Lossless secret construction	Lossless	Lossy	Lossy for k<n and Lossless for $k=n$	Lossy for k<n and Lossless for $k=n$
Fault tolerance property	No	No	Yes	Yes

From Table 4 it is obvious that the reconstruction complexity of the method described in this paper is considerably lower than the one of the method described in [8]. Besides, the fault tolerance property of the method developed by us is better than that of the method in [14, 17]. Thus, considering both these properties, this research work is superior in the aspect that it includes both the properties which have not been included simultaneously in a single work.

4. Conclusion

A typical (k, n) secret sharing scheme provides a high fault-tolerant property due to its distributed storage mechanism. In this paper we propose a new (k, n) secret sharing scheme, based on a Boolean operation. In the proposed scheme even if $n - k$ shares are lost or corrupted, the remaining k shares are sufficient to recover the secret. Moreover, the reconstruction complexity of the method proposed is $O(n)$ due to its Boolean operation. These are the main advantages of our proposed scheme compared to the existing methods. Moreover, our secret sharing can also be applied on colour images and it produces excellent results.

References

1. Blakely, G. R. Safeguarding Cryptography Keys. – In: Proc. of AFIPS National Computer Conference, Vol. **48**, 1979, 313-317.
2. Shamir, A. How to Share a Secret. – Communications of the ACM, Vol. **22**, 1979, No 11, 612-613.
3. Thien, C. C., J. C. Lin. Secret Image Sharing. – Computer Graphics, Vol. **26**, 2002, No 5, 765-770.
4. Thien, C. C., J. C. Lin. An Image-Sharing Method with User-Friendly Shadow Images. – IEEE Transactions on Circuit System, Vol. **13**, 2003, No 12, 1161-1169.
5. Chang, C. C., I. C. Lin. A New (t, n) Threshold Image Hiding Scheme for Sharing a Secret Color Image. – In: Proc. of ICCT'2003, Vol. **1**, 2003, 196-202.
6. Wang, R. Z., C. H. Su. Secret Image Sharing with Smaller Shadow Images. – Pattern Recognition Letter, Vol. **27**, 2006, No 6, 551-555.

7. W a n g, R. Z., S. J. S h y u. Scalable Secret Image Sharing. – Signal Processing: Image Communication, Vol. **22**, 2007, No 4, 263-373.
8. L i n, Y. Y., R. Z. W a n g. Scalable Secret Image Sharing with Smaller Shadow Images. – IEEE Signal Processing Letters, Vol. **17**, March 2010, No 3, 316-319.
9. N a o r, M., A. S h a m i r. Visual Cryptography. – In: Proc. of the Advances in Cryptology-Eurocrypt'94. Lecture Notes in Computer Science, Vol. **950**, 1995, 1-12.
10. B l u n d o, C., A. D. S a n t i s, D. R. S t i n s o n. On the Contrast in Visual Cryptography Schemes. – Journal of Cryptology, Vol. **12**, 1999, No 4, 261-289.
11. Y a n g, C. N. New Visual Secret Sharing Schemes Using Probabilistic Method. – Pattern Recognition Letters, Vol. **25**, 2004, No 4, 481-494.
12. Y a n g, C. N., T. S. C h e n. Aspect Ratio Invariant Visual Secret Sharing Schemes with Minimum Pixel Expansion. – Pattern Recognition Letters, Vol. **26**, 2005, No 2, 193-206.
13. S h y u, S. J., S. Y. H u a n g, Y. K. L e e, R. Z. W a n g. Sharing Multiple Secrets in Visual Cryptography. – Pattern Recognition, Vol. **40**, 2007, No 12, 3633-3651.
14. W a n g, D., L. Z h a n g, N. M a, X. L i. Two Secret Sharing Schemes Based on Boolean Operations. – Pattern Recognition, Vol. **40**, 2007, No 10, 2776-2785.
15. C h e n, T.-H., C.-S. W u. Efficient Multi-Secret Image Sharing Based on Boolean Operations. – Journal of Signal Processing, Vol. **91**, 2011, 90-97.
16. W u. A Secret Image Sharing Scheme for Light Images. – EURASIP Journal on Advances in Signal Processing, 2013.
17. C h a n g, C-C., C h i a-C h e n L i n c, T. H o a n g N g a n L e d, H o a i B a c L e. Sharing a Verifiable Secret Image Using Two Shadows. – Pattern Recognition, Vol. **42**, November 2009, Issue 11, 3097-3114.
18. L i u, H., X. W a n g, A. K a d i r. Image Encryption Using DNA Complementary Rule and Chaotic Maps. – Applied Soft Computing, Vol. **12**, 2012, 1457-1466.
19. Z h u, C. A Novel Image Encryption Scheme Based on Improved Hyper-Chaotic Sequences. – Optics Communications, Vol. **285**, 2012, No 1, 29-37.
20. W a d e, T., C. L. W a s h i n g t o n. Introduction to Cryptography with Coding Theory. Pearson, August 2005.