BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **17**, No 2
Sofia • 2017 Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.1515/cait-2017-0022

Significant Secret Image Sharing Scheme Based on Boolean Operation

Monu Verma, Rajneesh Rani

DR B R Ambedkar National Institute of Technology Jalandhar, Punjab, India
E-mails: monuverma1010@gmail.com ranir@nitj.ac.in

Abstract**:** *Traditionally,* (k, n) *secret image sharing is an approach of breaking down a secret image into n number of shadow images to assign them to n number of users, so that any k or more then k users can bring back the secret image. But in case of less than k, users cannot reveal any partial information about the original image. We have proposed a significant secret image sharing technique based on XOR with arithmetic operations that upgrade the performance of traditional secret image sharing approaches by serving importance to shadow images according to user's significance. This scheme also conserves the fault tolerance property which plays a vital role in image sharing field.*

Keywords**:** *Secret Image Sharing* (*SIS*)*, Visual Cryptography* (*VCS*)*, Polynomial Secret Image Sharing* (*PSIS*)*, image encryption, image decryption, Boolean operation.*

1. Introduction

Multimedia technologies are growing very fast with the rapid development of digital technologies and wide growth of the Internet. Multimedia technologies over networks boost the demand of image transmission. Transmission of images over network channels creates many security issues. Many methods like information hiding, digital watermarking, secret sharing, etc., have been introduced to resolve these issues. But the first two approaches suffer because a drawback-Original cannot be retrieved if the host image got damaged or altered.

Secret image sharing can put off these issues by breaking down an original image into number of shadow images and then transmit them on disparate network channels.

In 1979 Shamir [2] and Blakely [1] individually initiated an approach to protect secret images which is known as secret image sharing. Shamir's secret image sharing scheme was based on polynomial linear interpolation and Blakely's secret image sharing scheme was based on hyper plane geometry.

In 2002 T h i e n and L i n [3] provide an improved image sharing approach of Shamir's approach, a (k, n) secret image sharing scheme, where k signifies the threshold value ($k \leq n$) and n signifies the total number of shadow images. Users are able to generate secret image at the time of recovery only if they have k and more than k shadow images. This approach generates shadow images of $1/k$ of an original image. After that, many other SIS Schemes were proposed with extended functionality [4-7].

Later, in 1995, N a o r and S h a m i r [8] proposed the concept of the Visual Cryptography (VCS) approach. VCS is a cryptographic approach that does not require any mathematic computation and cryptographic knowledge. This approach is working on Human Visual Model. To upgrade the functionality of VCS many approaches have developed for binary images [9, 10], gray-scale images [11, 12] and color images [13].

But Visual Cryptography suffers from pixel expansion and poor visual quality of the recovered images due to OR operation. Comparatively, polynomial based secret image sharing approaches have better quality images at the time of reconstruction.

After that, in 2007, W a n g et al. [14] and V e r m a and R a n i [22] proposed a secret image sharing approach based on Boolean operation. This approach resolves the problem of pixel expansion and improves the quality of retrieved image. Working on this approach is divided into two parts.

Share generation phase. First $n - 1$ random images (R_1, R_2, …, R_{n-1}) are generated by using random generator and then generates n numbers of shadow images from the grayscale image I as illustrate in the next equations [9]:

(1)
$$\begin{cases} S_1 = R_1, \\ S_2 = R_1 \oplus R_2, \\ S_n = R_{n-1} \oplus I, \end{cases}$$

where $\oplus$ represents the XOR operation.

Share reconstruction phase. In this phase, participants assemble their shadow images to retrieve the original image by using the next equation [9]:

(2)
$$I = S_1 \oplus S_2 \oplus S_3 \dots \oplus S_n.$$

In this approach, at the time of reconstruction all n numbers of shadow images are necessary to retrieve a secret image. With less than n shadow images users are not able to recreate the original image. This scheme does not support the fault tolerance property.

In all of above approaches each participant has the same importance at the time of reconstruction of secret image. But in real life, each participant may not be having the same importance because of their duties and status in official and social fields.

By considering this point, C h e n, C h e n and L i n [15] initiated a weighted secret image sharing method in which generated shadow images have different weights according to participants' privileges. In this approach secret image is revealed only when the total weight of shadow images achieves the threshold value. But equating the weight of the participants with respect to their status creates problems.

To resolve this problem in 2013 L i et al. [16] proposed an essential secret image sharing approach, where shares are broken down into two groups, one is as essential and other is as non-essential.

In both of above approaches participants play different role at the time of reconstruction. But there is a common drawback of these approaches – size of generated shadow images is distinct to each other. If the size of shares is not equal then it may be possible that attacker monitors the status of the share sizes and get some important information.

Being inspired from essential image sharing approach and Boolean based image sharing schemes, we propose Significant Secret Image Sharing based on XOR with arithmetic operations in this paper. Lossless image Reconstruction, different shares have different importance and conserve fault tolerance property are primary objectives of our scheme. The paper is organised as follows:

Section 2 explains the pithy introduction of the proposed method. Section 3 stands for experimental results and performance analysis. Section 4 gives a summary of the comparative study of the proposed method with respect to other available image sharing methods. In Section 5 we conclude the work on this method.

2. The proposed scheme

In this portion, a significant secret image sharing method based on XOR with arithmetic operation is introduced, which provides different importance to different participants. For this method, first we need to generate two random key matrices-Key1 $[R\times1]$ and Key2 $[C\times1]$.

Here $[R, C] \in I$ [rows, columns], I is an original secret image.

$0 \leq [\text{Key1}] \leq 255$,

$0 \leq [\text{Key2}] \leq 255$.

The method consists of three steps.

2.1. Initialization

In this section, the dealer who holds the secret and participants are communicating with each other. All participants provide his/her unique Identity Number (ID) to the dealer. The dealer collects these IDs and ensures that all are unique, i.e., for i and j participants $\text{ID}_i \neq \text{ID}_j$.

2.2. Share generation

Share generation process is broken down into three phases as shown in Fig. 1. In the first phase, the encryption algorithm is applied to the secret image that permutes the position of the pixels belonging to the secret image. After that encrypted secret image is broken down into $n-1$ intermediate images ($D_1, D_2, \ldots, D_{n-1}$) and then with the help of these images n number of shadow images (share) (Sh_1, Sh_2, …, Sh_n) are generated.

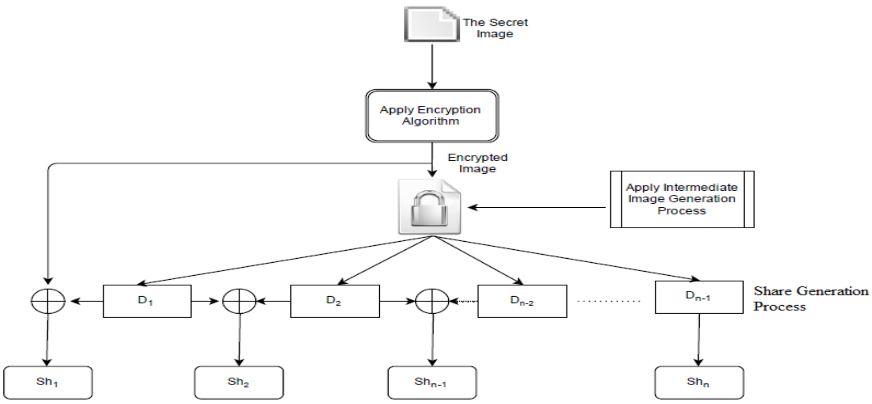


Fig. 1. The proposed secret image sharing process

2.2.1. Image encryption phase

In this zone, we generate the encrypted image E from the original secret image by applying below algorithm.

Image_Encryption Algorithm
Input: I [R, C], [R, C] ∈ I [rows, columns], Key1, Key2
Output: E [R, C]
Step 1. Repeat until $i \neq R$
Step 2. Repeat until $j \neq C$
Step 3. $\alpha = j + \text{Key1}(i, j)$
Step 4. If $\alpha \leq C$, then
Step 5. $E_{en} = I(i, \alpha)$
Step 6. Otherwise, $E_{en} = I(i, \alpha - C)$
Step 7. Repeat until $i \neq C$
Step 8. Repeat until $j \neq R$
Step 9. $\beta = j + \text{Key2}(i, j)$
Step 10. If $\beta \leq R$, then
Step 11. $E = E_{en}(i, \beta)$
Step 12. Otherwise $E = E_{en}(i, \beta - R)$
Step 13. End

2.2.2. Intermediate image generation phase

After generating encrypted image E, in this phase $n - 1$ intermediate image matrices (D_1, D_2,…, D_{n-1}) of size [R, C] are generated by using one of the next two equations:

(3) $$\sum_{i=1}^{n-1} D_i = \sum_{i=1}^{n-1} i * \left[E - \left[\frac{2^n}{n-1}\right]\right],$$

(4)
$$\begin{cases} D_1 = \left(E - \left\lceil \frac{2^n}{n-1} \right\rceil\right) \bmod p, \\ D_2 = \left(E + D_1 - \left\lceil \frac{2^n}{n-1} \right\rceil\right) \bmod p, \\ D_{n-1} = \left(E + D_{n-2} - \left\lceil \frac{2^n}{n-1} \right\rceil\right) \bmod p, \end{cases}$$

where $D_i \neq D_j$, $D_i \in E\ [R, C]\ \|[R, C] \in [0, 255]$, $n \geq 2$ and for 8-bit data type gray scale image p is 255.

Elements of intermediate matrices D_i have correlation among them because intermediate matrices are generated by using encrypted image E of original secret image I. These intermediate images play an important role to preserve the fault tolerance quality of the proposed image sharing approach.

2.2.3. Share generation phase

In this phase, we generate n number of shares, using n – 1 intermediate image matrices such that:

(5)
$$\begin{cases} \mathrm{Sh}_1 = E \oplus \mathrm{D}_1, \\ \mathrm{Sh}_2 = D_1 \oplus \mathrm{D}_2, \\ \mathrm{Sh}_{n-1} = D_{n-2} \oplus \mathrm{D}_{\mathrm{n}-1}, \\ \mathrm{Sh}_n = D_{n-1}, \end{cases}$$

where $\oplus$ Symbol represents a bitwise XOR operation.

Generated Shares are divided into two parts – significant and insignificant, as shown in equitation (6) and (7) so that first part shares have more information about the secret image compare to second part shares at the time of reconstruction.

(6)
$$S_{\mathrm{g}} = \left\lfloor \frac{n}{2} \right\rfloor,$$

(7)
$$I_{\mathrm{g}} = n - \left\lfloor \frac{n}{2} \right\rfloor,$$

where S_{g} represents a significant group of shares and I_{g} represents an insignificant group of shares.

Finally, generated shares, assign to each participant by the dealer according to their IDs and priorities.

Example. The proposed share generation process is illustrated by the following example. Let I (5×5) be the original image and n=4 (number of participants).

$$I = \begin{bmatrix} 25 & 125 & 80 & 155 & 200 \\ 10 & 87 & 123 & 245 & 89 \\ 180 & 213 & 50 & 54 & 254 \\ 100 & 96 & 75 & 254 & 87 \\ 95 & 121 & 149 & 27 & 153 \end{bmatrix}.$$

After applying encryption algorithm, we get the E matrix as

$$E = \begin{bmatrix} 200 & 87 & 75 & 80 & 155 \\ 10 & 50 & 95 & 245 & 89 \\ 213 & 96 & 125 & 254 & 180 \\ 100 & 153 & 123 & 254 & 87 \\ 27 & 25 & 54 & 121 & 149 \end{bmatrix}.$$

By using matrix E, we can find out $n-1$ intermediate matrices D_1, D_2, D_3 using Equation (1) as:

$$D_1=\begin{bmatrix} 67 & 138 & 162 & 82 & 169 \\ 32 & 52 & 154 & 247 & 202 \\ 243 & 90 & 238 & 31 & 117 \\ 122 & 201 & 174 & 31 & 138 \\ 168 & 200 & 12 & 206 & 241 \end{bmatrix},$$

$$D_2=\begin{bmatrix} 0 & 219 & 231 & 57 & 0 \\ 36 & 6 & 207 & 0 & 0 \\ 0 & 45 & 0 & 0 & 0 \\ 27 & 0 & 0 & 0 & 219 \\ 189 & 219 & 60 & 0 & 0 \end{bmatrix},$$

$$D_3=\begin{bmatrix} 19 & 0 & 0 & 193 & 217 \\ 20 & 76 & 0 & 175 & 154 \\ 171 & 225 & 190 & 127 & 45 \\ 158 & 153 & 222 & 127 & 0 \\ 75 & 119 & 54 & 158 & 169 \end{bmatrix}.$$

Now four different shares can be generated by using Equation (3) as:

$$Sh_1=\begin{bmatrix} 139 & 221 & 233 & 2 & 50 \\ 42 & 6 & 197 & 2 & 147 \\ 38 & 58 & 147 & 225 & 193 \\ 30 & 80 & 213 & 225 & 221 \\ 179 & 209 & 58 & 183 & 100 \end{bmatrix},$$

$$Sh_2=\begin{bmatrix} 67 & 81 & 69 & 107 & 169 \\ 4 & 50 & 85 & 247 & 202 \\ 243 & 119 & 238 & 31 & 117 \\ 97 & 201 & 174 & 31 & 81 \\ 21 & 19 & 48 & 206 & 241 \end{bmatrix},$$

$$Sh_3=\begin{bmatrix} 19 & 219 & 231 & 248 & 217 \\ 48 & 74 & 207 & 175 & 154 \\ 171 & 204 & 190 & 127 & 45 \\ 133 & 153 & 222 & 127 & 219 \\ 246 & 172 & 10 & 158 & 169 \end{bmatrix},$$

$$Sh_4=\begin{bmatrix} 19 & 0 & 0 & 193 & 217 \\ 20 & 76 & 0 & 175 & 154 \\ 171 & 225 & 190 & 127 & 45 \\ 158 & 153 & 222 & 127 & 0 \\ 75 & 119 & 54 & 158 & 169 \end{bmatrix}.$$

3. Secret reconstruction

Proposed secret reconstruction process divided into two phases.

3.1. Image reconstruction phase

In this section secret image is revealed by collecting shares of available participants using next equation:

(8) $$R_{\text{ev}} = \text{Sh}_1 \oplus \text{Sh}_2 \oplus \text{Sh}_3 \ldots \oplus \text{Sh}_n.$$

3.2. Image decryption phase

After getting a meaningless image R_{ev} from the equation (8), we apply the decryption algorithm as explained below to retrieve the secret image.

Image_Decryption Algorithm
Input: R_{ev} [R, C], Key1, Key2
Output: I [R, C]
Step 1. Repeat until $i \neq C$
Step 2. Repeat until $j \neq R$
Step 3. $\beta = j$ – Key2 (i, 1)
Step 4. if $\beta \geq 1$, then
Step 5. Set $I_{\text{en}} = R_{\text{ev}}(\beta, i)$
Step 6. Otherwise, Set $I_{\text{en}} = R_{\text{ev}}(\beta + R, i)$
Step 7. Repeat until $i \neq R$
Step 8. Repeat until $j \neq C$
Step 9. $\alpha = j$ – Key1 (i, 1)
Step 10. if $\alpha \geq 1$, then
Step 11. Set $I = I_{\text{en}}(\alpha, i)$
Step 12. Otherwise, Set $I = I_{\text{en}}(\alpha + C, i)$
Step 13. END

Example. To illustrate the proposed reconstruction process, we use all four (n=4) shares that are generated in the share generation phase and matrix R_{ev} is retrieved by using Equation (8) as:

$$R_{\text{ev}} = \text{Sh}_1 \oplus \text{Sh}_2 \oplus \text{Sh}_3 \oplus \text{Sh}_4,$$

$$R_{\text{ev}} = \begin{bmatrix} 200 & 87 & 75 & 80 & 155 \\ 10 & 50 & 95 & 245 & 89 \\ 171 & 96 & 125 & 254 & 180 \\ 158 & 153 & 123 & 254 & 87 \\ 75 & 25 & 54 & 121 & 149 \end{bmatrix}.$$

Then original image I is revealed without any loss by applying the decryption algorithm as:

$$I = \begin{bmatrix} 25 & 125 & 80 & 155 & 200 \\ 10 & 87 & 123 & 245 & 80 \\ 180 & 213 & 50 & 54 & 254 \\ 100 & 96 & 75 & 254 & 87 \\ 95 & 121 & 149 & 27 & 153 \end{bmatrix}.$$

We can also apply this method on color images. A color image has three planes – Red, Green and Blue. By applying our method on these planes individually, we can generate *n* number of shares and also retrieve secret image by combining these shares as shown on Figs 2 and 3.

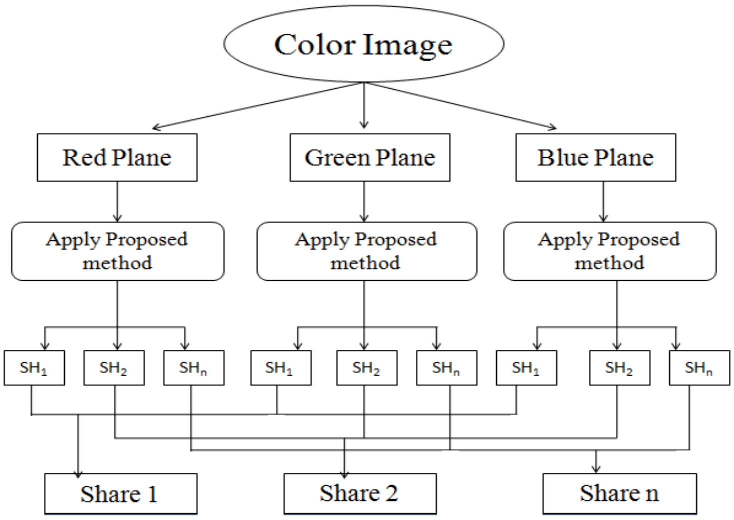


Fig. 2. Generation process for color image

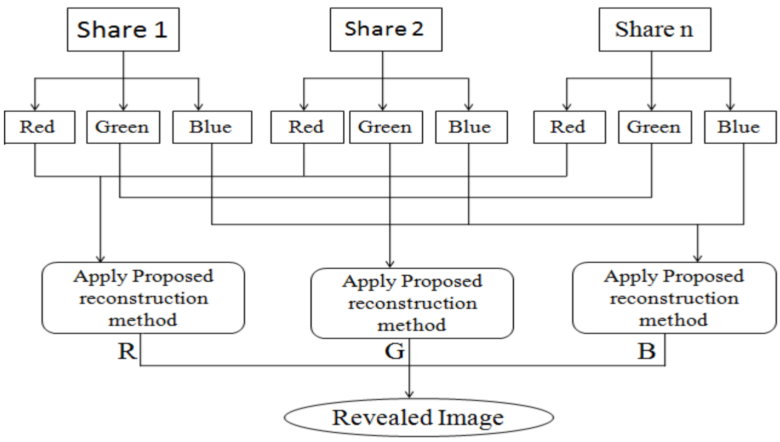
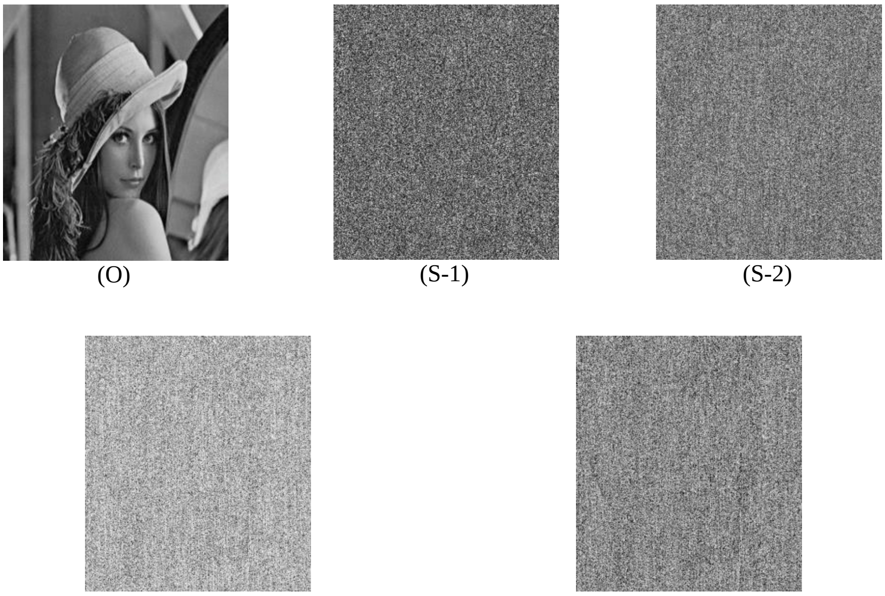


Fig. 3. Secret reconstruction process for color image

4. Experimental results and performance analysis

This portion explains experimental results and performance of the proposed approach. The technique was tested on several images and the following results were obtained.

Case1. A test Gray-Scale image "Lenna (512×512)" is used as input image to exhibit the performance of the proposed technique as shown in Fig. 4O. Fig. 4S shows the resultant shadow images.

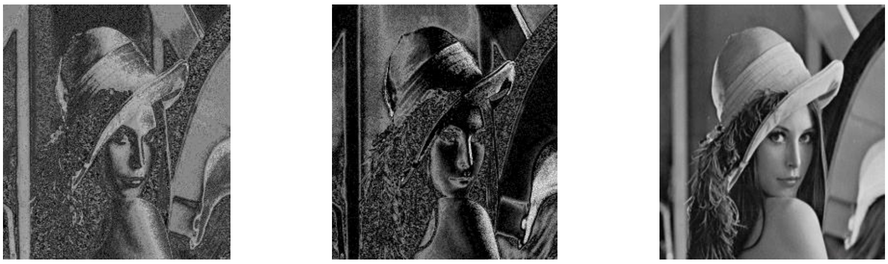


(O) (S-1) (S-2)

(S-3) (S-4)

Fig. 4. The Proposed Scheme for Gray-Scale image Lenna: The Secret Image (O); Generated shadow images (S) (Sh_1-Sh_4)

As explained in Section 2, at the time of reconstruction, the $\left\lfloor \frac{n}{2} \right\rfloor$ number of shadow images belonging to the *Sg* group have more importance as compared to I_g group shadow images. This is exemplified by Fig. 5r_1-r_2, which shows the revealed images using Sh_1, Sh_2 and Sh_3, Sh_4 shadow images respectively. Fig. 5R shows the revealed image by using all generated shadow images.

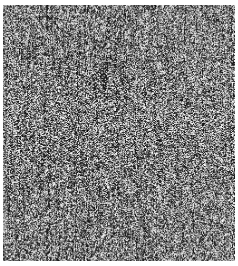


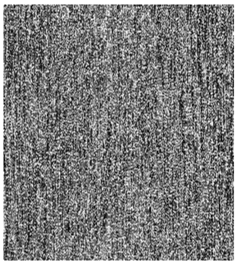
(r_1) PSNR=30.43DB (r_2) PSNR=26.67DB (R) PSNR=∞

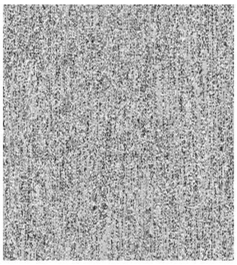
Fig. 5. Revealed images of Gray-Scale image Lenna: by using Sh_1 and Sh_2 shadow images (r_1); by using Sh_3 and Sh_4 shadow images (r_2); by using Sh_1, Sh_2, Sh_3, Sh_4 shadow images (R)

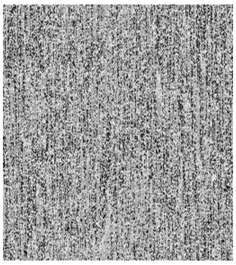
Case2. An another Gray-Scale image “Ship (256×256)” is used as input image to exhibit the performance of the proposed technique as shown in Fig. 6O. Fig. 6S shows the resultant shadow images.


(O)


(S-1)


(S-2)


(S-3)


(S-4)

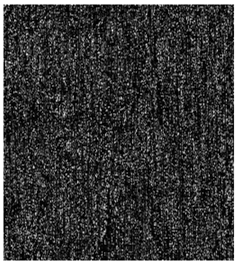
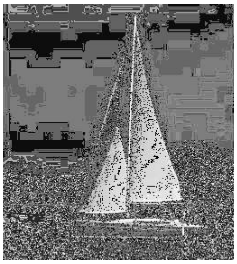
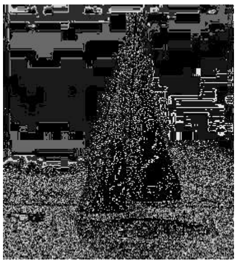

(S-5)

Fig. 6. The Proposed Scheme for Gray-Scale image Ship: the secret image (O); generated shadow images (S) (Sh_1-Sh_5)

Reconstructed images by using Sh_1, Sh_2 and Sh_3, Sh_4, Sh_5 shadow images are shown in Fig. 7r_1-r_2 respectively. Fig. 7R shows the revealed image by using all generated shares.

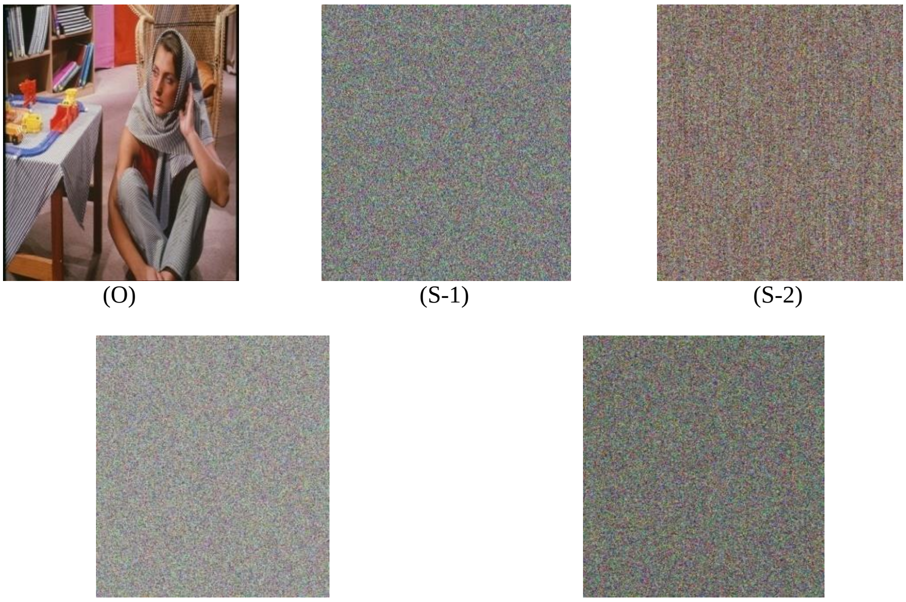

(r_1)PSNR=31.50DB


(r_2)PSNR=25.71DB


(R)PSNR=∞

Fig. 7. Revealed images of Gray-Scale image Lenna: by using Sh_1 and Sh_2 shadow images (r_1); by using Sh_3, Sh_4 and Sh_5 shadow images (r_2); by using Sh_1, Sh_2, Sh_3, Sh_4, Sh_5 shadow images (R)

Case3. A Color image "Barbara (512×512)" is used as input image to exhibit the performance of the proposed technique for color images as shown in Fig. 8O. Fig. 8S represents the resultant shadow images.



(O) (S-1) (S-2)

(S-3) (S-4)

Fig. 8. The Proposed Scheme for Color image Barbara: the secret image (O); generated shadow images (S) (Sh_1-Sh_4)

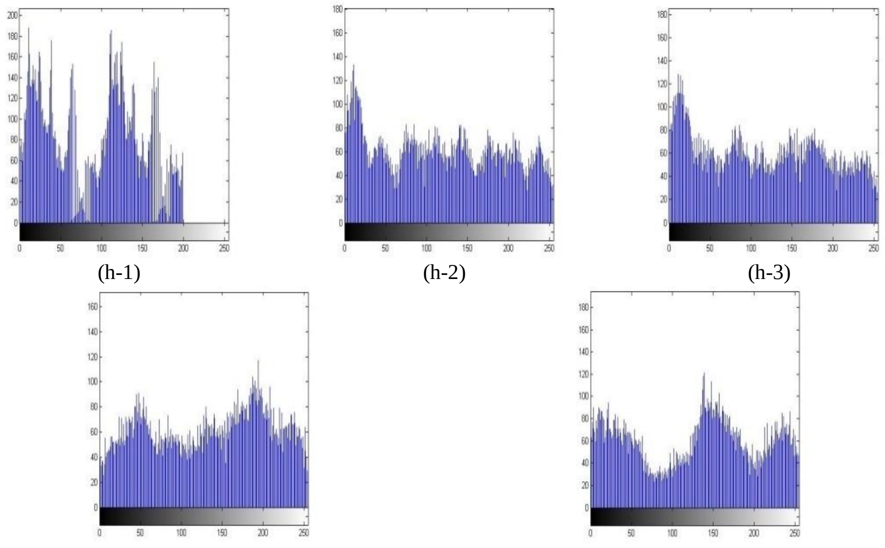
The reconstructed images that are demonstrating the importance of shares discussed in Section 2 have been shown in Fig. 9. Fig. 9r_1-r_2 show the reconstructed images generated by using Sh_1, Sh_2 and Sh_3, Sh_4 shadow images. Fig. 9R shows the revealed image generated by using all shadow images (Sh_1, Sh_2, Sh_3, Sh_4).

(r_1) PSNR=30.52DB (r_2) PSNR=26.32DB (R) PSNR=∞

Fig. 9. Revealed images of color image Barbara: by using Sh_1 and Sh_2 shadow images (r_1); by using Sh_3 and Sh_4 shadow images (r_2); by using Sh_1, Sh_2, Sh_3, Sh_4 shadow images (R)

4.1. Histogram analysis

Histograms of the input image (Lenna) and generated shadow images (Sh_1, Sh_2, Sh_3, Sh_4) are shown on Fig. 10h respectively.



(h-1) (h-2) (h-3)

(h-4) (h-5)

Fig. 10. Histogram of Gray-Scale image Lenna (h-1). Histogram of generated shares (h-2)-(h-5)

Histograms of shadow images show a good distribution with gray scale levels. But as shown in the Fig 10(h-1), original image histogram is not distributed uniformly. The results represent, that any single generated shadow image can’t leak partial information about the original image.

4.2. Correlation analysis

Most of the time, adjacent pixels of the real images are highly correlated to each other. This kind of images are not secured from statistical attacks. At the time of share distribution it is required that there should be a low correlation between two adjacent pixels. Following equation (9) is used to calculate correlation coefficient of n pairs of adjacent pixels,

$$\text{Corr} = \frac{\sum_{i=1}^{n}(x_i - x')(y_i - y')}{\sqrt{(\sum_{i=1}^{n}(x_i - x')^2)(\sum_{i=1}^{n}(y_i - y')^2)}}, \tag{9}$$

where x_i and y_i denotes the correlation pixel values of the image and x' and y' are calculates by using following equation:

$$x' = \frac{1}{n}\sum_{i=1}^{n} x_i \quad \text{and} \quad y' = \frac{1}{n}\sum_{i=1}^{n} y_i. \tag{10}$$

To analyze the correlation in horizontal, vertical and diagonal directions, random 8000 pairs of pixels are taken from the original secret image and shadow images are generated. Correlation graphs between adjacent pixels of the input gray scale image (Ship) and shadow images ($\text{Sh}_1, \text{Sh}_2, \text{Sh}_3, \text{Sh}_4, \text{Sh}_5$) are shown in Fig. 11 and correlation coefficient values are shown in Table 1.

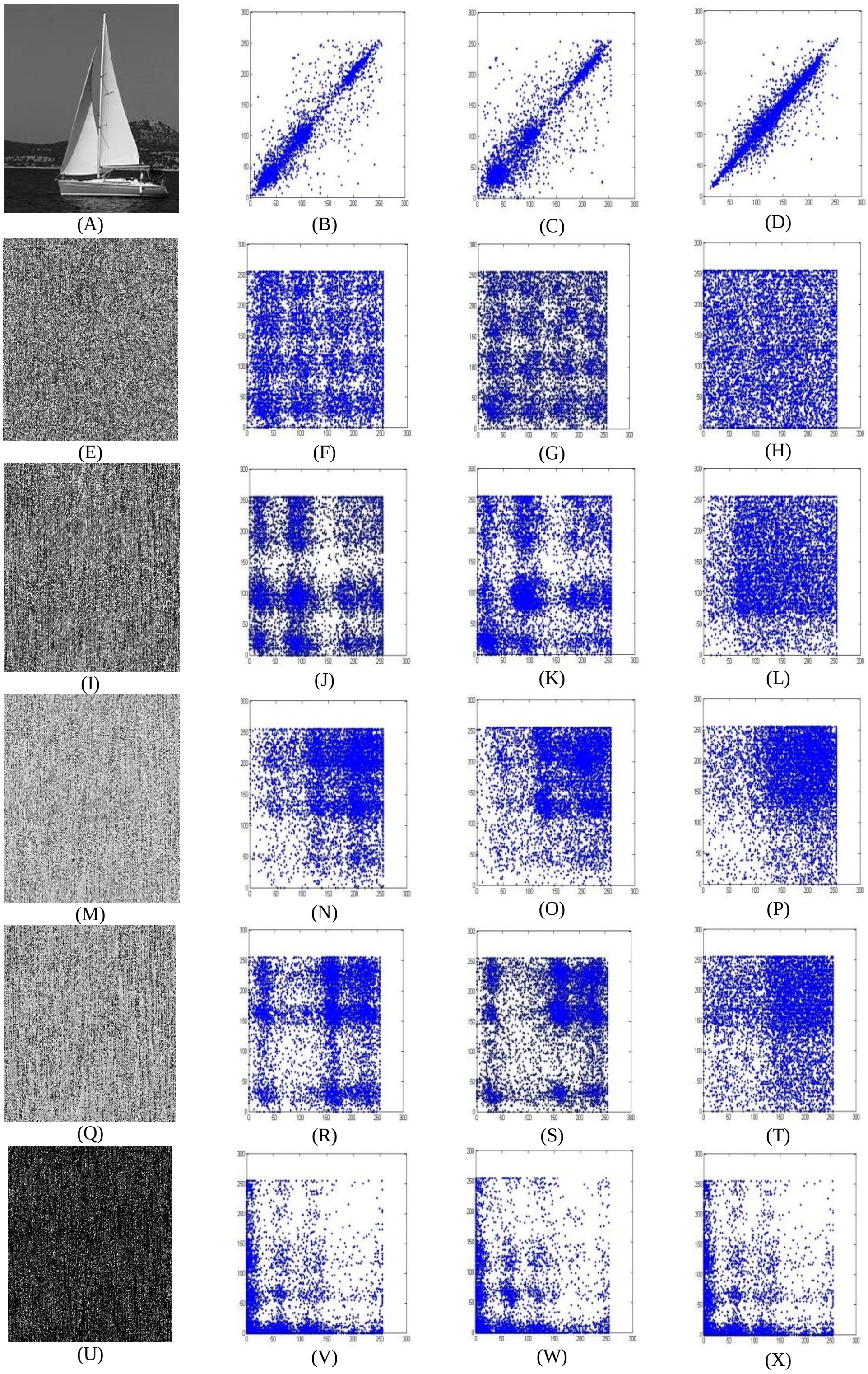


Fig. 11. Correlation graphs between adjacent pixels in the horizontal, vertical and diagonal directions

Table 1. Correlation coefficient values of adjacent pixels in the horizontal, vertical and diagonal directions

Input Image	Correlation coefficients		
	Horizontal	Vertical	Diagonal
Gray-Scale (Lenna)	0.9504	0.9256	0.9441
Shadow Sh_1	0.0075	0.0307	0.0306
Shadow Sh_2	0.0126	0.0108	0.0078
Shadow Sh_3	0.0091	0.0149	0.0104
Shadow Sh_4	0.0248	0.0071	0.0129
Shadow Sh_5	0.0109	0.0167	0.0168

4.3. PSNR analysis

The Peak Signal to Noise Ratio (PSNR) is used to compare image compression quality. Here PSNR in DB is used to analyze the accuracy of the reconstructed image. The higher PSNR value shows the less error rate (noise), i.e., better quality of image and lower PSNR value show more error rate and worse quality of image as compared to the original. The (PSNR=∞) value shows that there is no error, i.e., both images, original and reconstructed image, are exactly the same. Following equations [17] are used to calculate PSNR value between the two images (Original image and Reconstructed image),

$$\text{PSNR}=10\log_{10}\left(\frac{R^2}{\text{MSE}}\right), \quad (11)$$

where R represents maximum fluctuation value. For 8-bit data type images R is 255 and MSE is defined by the following equation:

$$\text{MSE}=\sum_{M,N}\frac{[\,I_n(m,n)-R_e(m,n)]^2}{M\times N}, \quad (12)$$

where $I_n(m, n)$ and $R_e(m, n)$ represent input image and recreated image respectively. For 8-bits depth, typical values for PSNR in a lossy image lie between 30 and 50 DB. In case of 16-bit data, these values are between 60 and 80 DB [23] [24].

The PSNR values of the significant and insignificant group of shares are shown in Table 2. These values assure that significant group has more importance compare to insignificant group at the time of reconstruction for both grayscale and color images. Table 3 shows the maximum and minimum PSNR values of the proposed method and other existing schemes of Nag et al. [17], Chang et al. [18].

Table 2. PSNR Values of reconstructed images with the contribution of significant and insignificant shares

Image type	Number of shares		
	Significant group	Insignificant group	All shares
Gray-scale (Lenna)	30.43	26.67	Infinite
Gray-scale (Ship)	31.05	25.71	Infinite
Color (Barbara)	30.52	26.32	Infinite

Table 3. Comparison of PSNR values of reconstructed images of Nag et al. [17], Chang et al. [18] and Proposed method

Method	Gray-scale image (Lenna)		Color image (Barbara)	
	Max	Min	Max	Min
Proposed method	∞	24.47	∞	24.35
Nag et al. [17]	∞	25.68	∞	24.91
Chang et al. [18]	33.70		33.75	

4.4. Sensitivity analysis

To test the proposed scheme performance against different attacks, two measures are used: 1) The Number of Changing Pixels Rate (NPCR) and 2) Unified Average Changed Intensity (UACI). These measures are defined in following equations [20],

$$\text{NPCR}=\frac{\sum_{m,n} D(m,n)}{M\times N}\times 100\%, \tag{13}$$

where,

$$D(m,n)=\begin{cases}0 & \text{if } I_n(m,n)= R_{\text{e}}(m,n),\\ 1 & \text{if } I_n(m,n)\neq R_{\text{e}}(m,n),\end{cases} \tag{14}$$

$$\text{UACI}=\frac{1}{M\times N}\sum_{m,n}\frac{|I_n(m,n)-R_{\text{e}}(m,n)|}{255}\times 100\%. \tag{15}$$

Here, $I_n(m, n)$ and $R_{\text{e}}(m, n)$ represent input image and recreated image, respectively.

The expected estimate values of NPCR and UACI of the images are calculated by using the following equations:

$$\text{NPCR}_{\text{E}}= (1-2^{-n})\times 100\%, \tag{16}$$

$$\text{UACI}_{\text{E}}=\frac{1}{2^{2n}}\sum_{i=1}^{2^n-1}\frac{i(i+1)}{2^n-1}\times 100\%, \tag{17}$$

Here n represents the data type of images. For grayscale images and is 8. So for gray scale images NPCR_{E}= 99.6094% and UACI_{E}= 33.4635%.

Tables 4 and 5 represent the average NPCR and UACI grayscale and color images that are very close to estimate NPCR and UACI estimate values. This indicates that the proposed method has robustness property against different attacks.

Table 4. Average values of NPCR and UACI of shadow images (Sh_1, Sh_2, Sh_3 Sh_4) of gray scale image "Lenna (512×512)"

Test	Chang et al. [18]	Nag et al. [17]	Liu and Wang [19]	Proposed method
NPCR (%)	56.2	99.67	99.60	99.47
UACI (%)	56.2	32.23	28.13	32.58

Table 5. Average values of NPCR and UACI of shadow images (S1, S2, S3, S4) of color image "Barbara (512×512)"

Test	Chang et al. [18]	Nag et al. [17]	Proposed method
NPCR (%)	70.10	99.56	99.59
UACI (%)	32.80	25.63	32.90

4.5. Complexity analysis

The reconstruction of an image in this scheme is achieved by computing XOR operation on k, $k \leq n$, available shadow with Image_Decryption algorithm. So, the computation time depends on the number of available shadow images and the size of the secret image. Total computational complexity of the recovery process is the addition of $O(k)$ and complexity of the decryption algorithm, that varies according to image size.

5. Comparison

This section represents a comparison of the proposed method and other recent Secret Image Sharing methods. Some basic properties of the Images are listed in Table 6 and are used for comparative study.

Table 6. Comparison between the proposed approach and exist approaches

Properties	Chang et al. [18]	Chen and Wu [21]	Peng et al. [16]	Nag et al. [17]	Proposed method
(K, n) Threshold	No	No	Yes	Yes	Yes
Recovery type	Lossy	Lossless	Lossless/ Lossy for < n	Lossless/ Lossy for < n	Lossless/ Lossy for < n
Fault tolerance	No	No	Yes	Yes	Yes
Importance of shadows	No	No	Yes	No	Yes
Generated shares size	Same as original image	Same as original image	Small compare to original image	Same as original image	Same as original image
Construction method	Arithmetic operation	Boolean	PSIS	Boolean	Boolean operation with encryption

6. Conclusion

This work proposes a “Significant Secret Image Sharing based on Boolean Operation”. The scheme preserves fault tolerance property in the revealed images. This scheme maintains the importance of participants: it distributes the generated shadow images to participants according to their priority. The simulation results of a gray scale image “Lenna” considers two $(\left\lfloor\frac{n}{2}\right\rfloor)$ shadows as significant and remaining two $(n-\left\lfloor\frac{n}{2}\right\rfloor)$ are the insignificant. At the time of reconstruction, image that is recreated by using significant group is more recognizable compare to another image that is created by using insignificant group. On the other hand, if all participants are available, then the recreated image is lossless, i.e., the recreated image is exactly same as the original input image. Also, the analysis results show that this scheme is robust against statistical and differential attacks. These are the main advantages of the scheme. Moreover, the proposed scheme can also be applied to color images and it also generates good results. On the basis of the experimental results we can say that this scheme is suitable for modern visual communication applications where feature such as participants’ priorities, secure transmission and storage is the main point of the concern.

References

1. Blakely, G. R. Safeguarding Cryptographic Keys. – Proc. AFIPS, Vol. **48**, 1979, pp. 313-317.
2. Shamir, A. How to Share a Secret. – Communications of the ACM, Vol. **22**, 1979, No 11, pp. 612-613.

3. T h i e n, C. C., J. C. L i n. Secret Image Sharing. – Computers & Graphics, Vol. **26**, 2002, No 5, pp. 765-770.
4. L i n, C. C., W. H. T s a i. Secret Image Sharing with Steganography and Authentication. – Journal of Systems and Software, Vol. **73**, 2004, No 3, pp. 405-414.
5. W a n g, R. Z., C. H. S u. Secret Image Sharing with Smaller Shadow Images. – Pattern Recognition Letters, Vol. **27**, 2006, No 6, pp. 551-555.
6. C h a n g, C. C., C. C. L i n, C. H. L i n, Y. H. C h e n. A Novel Secret Image Sharing Scheme in Color Images Using Small Shadow Images. – Information Sciences, Vol. **178**, 2008, No 11, pp. 2433-2447.
7. T s a i, D. S., G. H o r n g, T. H. C h e n, Y. T. H u a n g. A Novel Secret Image Sharing Scheme for True-Color Images with Size Constraint. – Information Sciences, Vol. **179**, 2009, No 19, pp. 3247-3254.
8. N a o r, M., A. S h a m i r. Visual Cryptography. – In: Advances in Cryptography Eurocrypt’94. Lecture Notes in Computer Science. Vol. **950**. Springer-Verlag, 1995, pp. 1-12.
9. A t e n i e s e, G., C. B l u n d o, A. D e S a n t i s, D. R. S t i n s o n. Extended Capabilities for Visual Cryptography. – Theoretical Computer Science, Vol. **250**, 2001, No 1, pp. 143-161.
10. T s a i, D. S., T. H. C h e n, G. H o r n g. A Cheating Prevention Scheme for Binary Visual Cryptography with Homogeneous Secret Images. – Pattern Recognition, Vol. **40**, 2007, No 8, pp. 2356-2366.
11. L i n, C. C., W. H. T s a i. Visual Cryptography for Gray-Level Images by Dithering Techniques. – Pattern Recognition Letters, Vol. **24**, 2003, No 1, pp. 349-358.
12. B l u n d o, C., A. D e S a n t i s, M. N a o r. Visual Cryptography for Grey Level Images. – Information Processing Letters, Vol. **75**, 2000, No 6, pp. 255-259.
13. H o u, Y. C. Visual Cryptography for Color Images. – Pattern Recognition, Vol. **36**, 2003, No 7, pp. 1619-1629.
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, pp. 2776-2785.
15. C h e n, C. C., C. C. C h e n, Y. C. L i n. Weighted Modulated Secret Image Sharing Method. – Journal of Electronic Imaging, Vol. **18**, 2009, No 4, pp. 043011-043011.
16. L i, P., C. N. Y a n g, C. C. W u, Q. K o n g, Y. M a. Essential Secret Image Sharing Scheme with Different Importance of Shadows. – Journal of Visual Communication and Image Representation, Vol. **24**, 2013, No 7, pp.1106-1114.
17. N a g, A., S. B i s w a s, D. S a r k a r, P. P. S a r k a. Secret Image Sharing Scheme Based on a Boolean Operation. – Cybernetics and Information Technologies, Vol. **14**, 2014, No 2, pp. 98-113.
18. C h a n g, C. C., C. C. L i n, T. H. N. L e, H. B. L e. Sharing a Verifiable Secret Image Using Two Shadows. – Pattern Recognition, Vol. **42**, 2009, No 11, pp. 3097-3114.
19. L i u, H., X. W a n g. Image Encryption Using DNA Complementary Rule and Chaotic Maps. – Applied Soft Computing, Vol. **12**, 2012, No 5, pp. 1457-1466.
20. Z h u, C. A Novel Image Encryption Scheme Based on Improved Hyperchaotic Sequences. – Optics Communications, Vol. **285**, 2012, No 1, pp. 29-37.
21. C h e n, T. H., C. S. W u. Efficient Multi-Secret Image Sharing Based on Boolean Operations. – Signal Processing, Vol. **91**, 2011, No 1, pp. 90-97.
22. V e r m a, M., R. R a n i. Strong Thershold Secret Image Sharing Based on Boolean Operation. – In: Proc. of International Conference on Computing, Communication and Automation (ICCCA’16), IEEE, 2016, pp. 1145-1149.
23. T h o m o s, N., N. V. B o u l g o u r i s, M. G. S t r i n t z i s. Optimized Transmission of JPEG2000 Streams over Wireless Channels. – IEEE Transactions on Image Processing, Vol. **15**, 2006, No 1.
24. X i a n g j u n, L., C. J i a n f e i. Robust Transmission of JPEG2000 Encoded Images over Packet Loss Channels. – ICME, School of Computer Engineering, Nanyang Technological University**,** 2007, pp. 947-950.