VOL. 13, NO. 13, JULY 2018 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences
©2006-2018 Asian Research Publishing Network (ARPN). All rights reserved.
www.arpnjournals.com

A NOVEL SECURED BOOLEAN BASED SECRET IMAGE SHARING SCHEME

Javvaji V. K. Ratnam[1], T. Sreenivasulu Reddy[2] and P. Ramana Reddy[1]
[1]Department of Electronics and Communication Engineering, Jawaharlal Nehru Technological University, Anantapur, India
[2]Department of Electronics and Communication Engineering, Sri Venkateswara University, Tirupati, India
E-Mail: ratnamjvklakshmi@yahoo.co.in

ABSTRACT

A novel *(k, n)* secret image sharing scheme with high security by using Boolean XOR operations and circular shift operations for gray-scale and color secret images is designed and its performance is evaluated in this paper. The original secret image is encoded into *n* noise-like share images, transmitted over channel, and any *k* or more number of share images is gathered to reconstruct the secret image at the receiver side. The share images with less than *k* in number never reconstruct the original secret image. In this technique, the security of the secret image is improved by combining the secret with same sized random image and using distinct 8-bit identifier to each share. The generated shares have high randomness which indicates high security to the secret image. The overheads like codebook design, pixel expansion and basis matrices are not needed in this proposed method compared to other methods. The performance evaluation parameters such as correlation, mean square error and peak signal-to-noise ratio gives the performance and consistency of the proposed design. The experimental results prove the feasibility and security of the proposed Boolean based image sharing scheme.

Keywords: Boolean XOR, visual cryptography, visual secret image sharing, circular shift, security.

1. INTRODUCTION

The secret image sharing (SIS) schemes receive more attention by many researchers now-a-days for secured transmission of multimedia data over internet. SIS overcomes difficulties of the traditional cryptography methods. In the secret image sharing scheme, the original secret image is converted to different noise-like share images and transmitted these shares over communication networks. These share images are printed on transparencies and stacked or superimposed together for reconstruction of original secret image at the receiving end. The reconstructed secret is visible by using human visual system without using any computations. The generated multiple share images do not give any information about the original secret image. Hence the security of the image is satisfied by this secret sharing scheme.

The secret sharing scheme was proposed initially by Blakley [1] and Shamir [2] independently. The Visual Cryptography (VC) based VSS concept is first initiated by Naor and Shamir [3]. The *(k, n)* visual secret sharing introduced by them encodes the binary secret image into *n* meaningless noise-like shadow or share images by using Basis matrices. The original secret image is recovered by stacking at least *k* share images or more together. The share images with less than *k* in number never reveal the secret data.

The two Basis matrices for (2, 2) visual secret sharing scheme used to encrypt the binary secret image are denoted by S^0 and S^1 and are given by

$$S^0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \text{ and } S^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

The secret image pixels are encoded into subpixels by a factor *m*, known as pixel expansion factor, using Basis matrices. In secret image, white pixels are encoded into subpixels of two share images with [0 1] and [0 1] using the matrix S^0 and black pixels in the secret are encoded into subpixels of two share images with [0 1] and [1 0] from the matrix S^1. In this example, the pixel expansion factor, *m* is 2. And the size of the share images and the reconstructed secret image is proportional to the pixel expansion factor, *m*. Hence this technique requires more storage and bandwidth for share images and reconstructed images. The underlying operation in this scheme is logical OR operation. The disadvantages of this traditional visual cryptography based VSS are pixel expansion, requirement for Basis matrices, design of codebook, poor contrast of the reconstructed secret image, problems related to perfect alignment of share images, more storage space and bandwidth requirement.

Random grid based visual secret sharing scheme proposed by Kafri and Keren [4] eliminates the disadvantages mentioned in the earlier scheme. Different researchers [5], [6], [7], [8], [9] and [10] proposed various schemes using random grid based VSS for improvement in security and visual quality of the reconstructed image. The sizes of share images and reconstructed image are same as the original secret. So the need for additional memory and bandwidth are eliminated. These schemes involve proper alignment of share images and computational complexity. Researchers proposed different secret image sharing techniques to enhance visual quality [11], pixel expansion factor reduction [12], sharing of color image [13], prevention of cheating [14], region incrementing [15] and quality metrics to assess the image quality [16].

There is a scope in the design of secret image sharing schemes to improve the security of the secret image from different attacks and visual quality improvement in the reconstructed secret image.

©2006-2018 Asian Research Publishing Network (ARPN). All rights reserved.

The rest the paper is organized in the following manner: Section 2 presents related work on secret image sharing. Section 3 gives the proposed work. The corresponding experimental results and discussion is given in the section 4. Section 5 discussed various performance evaluation parameters. Finally, section 6 gives conclusion.

2. RELATED WORK

A Boolean operation based secret sharing scheme eliminates the problems of computational complexity and perfect alignment of share images. Various Boolean based visual secret sharing schemes [17], [18], [19], [20] and [21] are suggested to improve contrast of the reconstructed image and require little computations during the recovery process of the secret. An improvement in the security of the secret image is further needed.

In this paper, a novel Boolean operation based visual secret sharing scheme with improved security to gray-scale and color images is suggested. Here, the main contribution is to improve the security of the secret image by providing additional feature of different id to each share of the original secret image. The performance of the proposed scheme is evaluated by using different quantitative metrics such as correlation, Mean Square Error (MSE), and Peak Signal-to-Noise Ratio (PSNR). The proposed scheme feasibility and consistency is checked by comparing with the existing related schemes.

3. PROPOSED SCHEME

In this section, a novel *(k, n)* secret image sharing scheme based on Boolean XOR operations and circular shift operations is proposed. The *n* noise-like meaningless share images are generated by encoding the original secret image with a random image and application of circular shift operation using a distinct identifier. The sizes of secret image and random share images are same. The generated share images are transmitted through a communication channel. The original secret image will be reconstructed by stacking or superimposing at least *k* share images at the receiving side. The shares less than *k* do not reconstruct the original secret image.

A random image *R* is generated with a size same as original secret. This random image is XORed with the original secret image. The resultant image *M* is divided by *k* (minimum number of share images needed to recover the secret image) to obtain the encrypted image *G*. For each share, an 8-bit random number, x_i is generated separately. The range of generated random number is between 0 and 255. An identifier is generated by rearranging the bits of this random number x_i. The four Most Significant Bits (MSBs) of the identifier are calculated by using Boolean XOR operation on four least significant bits and four most significant bits of this random number. The four Least Significant Bits (LSBs) of the identifier are kept as same as the four least significant bits of this random number. The resultant 8-bit number is treated as the identifier y_i to the respective share image. Hence *n* numbers of identifiers are generated during share image generation. This identifier is used during reconstruction of the secret image which is supplied by the owner of the secret image. The encrypted image *G* is circular right shifted by number of bit positions specified by the identifier. The resultant right shifted image will be the share image S_i of the respective identifier. Hence *n* numbers of share images S_i ($for\ 1 \le i \le n$) are generated by using distinct identifiers. The resultant share images are looks like meaningless noisy shares which does not leak any information about original secret.

At least *k* share images needed to recover the secret image during reconstruction process. The share images S_i ($for\ 1 \le i \le k$) are circularly left shifted by respective identifiers y_i and are added together. The resultant *P* is Boolean XORed with the random image *R* for reconstruction the secret image I_1.

The use of distinct identifier and corresponding circular shift operations for each share during share generation process is the novelty in the proposed technique which improves the security of the secret image from different attacks.

Advantages of the proposed scheme

a) The proposed algorithm has no pixel expansion problem.
b) Share images and reconstructed image does not require additional memory and bandwidth.
c) The specific codebook design for share generation is not necessary.
d) No need of Basis matrices for encoding the secret image.
e) The proposed technique is suitable for wide image format such as gray-scale and color images.

The proposed algorithms for generation of share images and secret image recovery are given below:

Algorithm for share generation

Input: Secret image, *I*

Output: *n* meaningless share images $\{S_1, S_2, S_3, ..., S_n\}$

1. Generate a random image *R*

$R = random(255)$

2. Combine secret image with random image

$M = I \oplus R$

where, $\oplus$ denotes Boolean XOR operation.

3. Divide the resulted image with *k*

$G = M / k$

4. Generate *n* random numbers

$x_1 = random(255)$
$x_2 = random(255)$
$x_3 = random(255)$
.
.
.
$x_{n-1} = random(255)$
$x_n = random(255)$

5. Generate *n* identifiers

$y_1 = [XOR(4\text{-bit } MSB(x_1), 4\text{-bit } LSB(x_1))$
$4\text{-bit } LSB(x_1)]$
$y_2 = [XOR(4\text{-bit } MSB(x_2), 4\text{-bit } LSB(x_2))$
$4\text{-bit } LSB(x_2)]$
$y_3 = [XOR(4\text{-bit } MSB(x_3), 4\text{-bit } LSB(x_3))$

©2006-2018 Asian Research Publishing Network (ARPN). All rights reserved.

4-bit LSB(x_3)]
.
.
.
y_{n-1} = *[XOR(4-bit MSB(x_{n-1}), 4-bit LSB(x_{n-1}))*
4-bit LSB(x_{n-1})]
y_n = *[XOR(4-bit MSB(x_n), 4-bit LSB(x_n))*
4-bit LSB(x_n)]

6. Generate *n* share images by using identifiers
S_1 = *circularrightshift(G, y_1)*
S_2 = *circularrightshift(G, y_2)*
S_3 = *circularrightshift(G, y_3)*
.
.
.
S_{n-1} = *circularrightshift(G, y_{n-1})*
S_n = *circularrightshift(G, y_n)*

Algorithm for secret image reconstruction:
Input: *n* meaningless share images *{S_1, S_2, S_3, ..., S_n}*
Output: Recovered secret image I_1
1. Combine *k* shares
P = 0
P = P + circularleftshift(S_1, y_1)
P = P + circularleftshift(S_2, y_2)
.
.
.
P = P + circularleftshift(S_{k-1}, y_{k-1})
P = P + circularleftshift(S_k, y_k)

2. Reconstructed secret image I_1
$I_1 = P \oplus R$

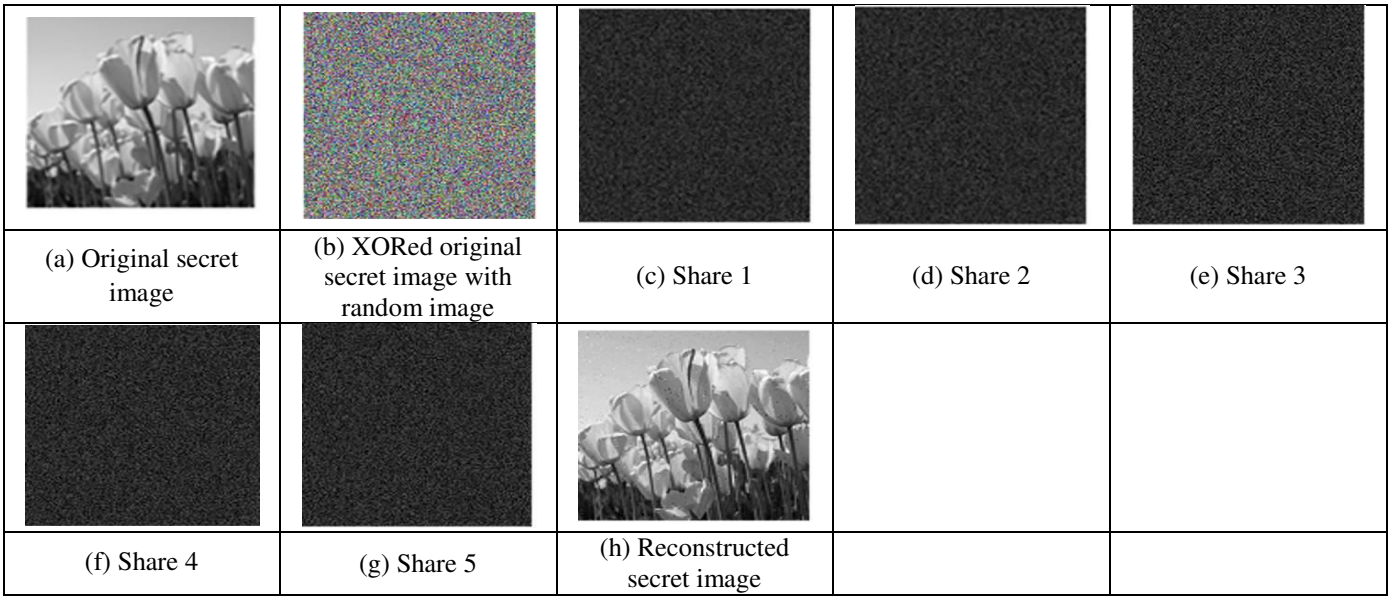
4. EXPERIMENTAL RESULTS AND DISCUSSIONS

The proposed *(k, n)* secret image sharing scheme experimental results for gray-scale and color secret images are discussed in this section. The proposed scheme is applicable to both gray-scale and color images. Experiments are conducted on 110 different images to analyze the randomness, efficiency and security of the proposed scheme. It is observed that this scheme works efficiently for any number of secret images. For experimental analysis and discussion, gray-scale image and color image of Tulip with dimensions 256 × 256 pixels has been considered in this paper.

Figure-1 demonstrates the experimental results of (3, 5) secret image sharing scheme conducted on gray-scale image. The original secret image is shown in Figure-1(a) is combined with a random image of size 256 × 256 to get encrypted image as shown in Figure-1(b). The meaningless noise-like share images shown in Figures-1(c)-1(g) are generated by circular right shifting the XORed image with number of bits indicated by the respective identifier. These share images are observed to be highly random and does not give any information about the original secret image. Figure-1(h) shows the reconstructed secret image by stacking or superimposing three shares images.

Figure-2 demonstrates the experimental results of (3, 5) secret image sharing scheme conducted for color secret image. The original secret color image shown in Figure-2(a) is XORed by random image of same 256 × 256 size. The resulted image is given in Figure-2(b). The noise-like share images shown in Figures 2(c)-2(g) are generated by circular right shifting operation of resulted image pixels using distinct identifier. These share images does not leak any information about the secret. They are highly random. Figure-2(h) shows the reconstructed color image by stacking three share images. The reconstructed image is observed to be more similar to original secret image.

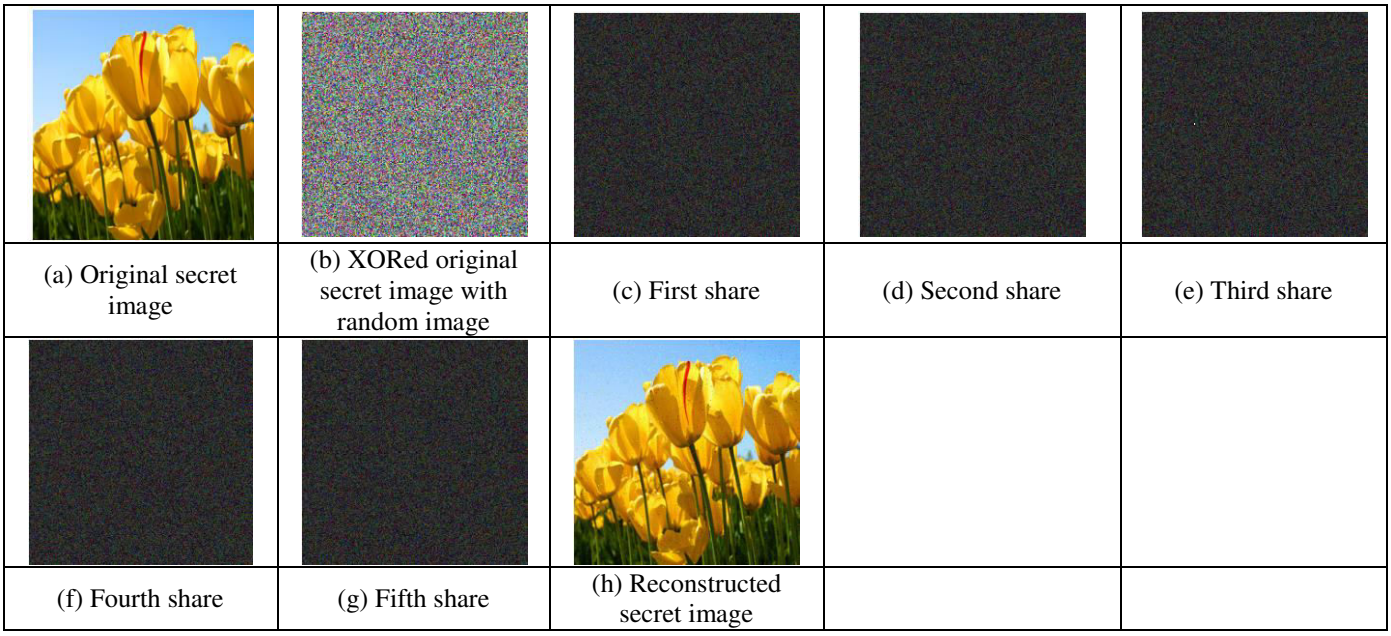
©2006-2018 Asian Research Publishing Network (ARPN). All rights reserved.



(a) Original secret image | (b) XORed original secret image with random image | (c) Share 1 | (d) Share 2 | (e) Share 3

(f) Share 4 | (g) Share 5 | (h) Reconstructed secret image

Figure-1. Experimental results of (3, 5) visual secret sharing scheme on 256 × 256 gray-scale image.



(a) Original secret image | (b) XORed original secret image with random image | (c) First share | (d) Second share | (e) Third share

(f) Fourth share | (g) Fifth share | (h) Reconstructed secret image

Figure-2. Experimental results of (3, 5) visual secret sharing scheme on 256 × 256 color image.

5. PERFORMANCE EVALUATION PARAMETERS

The performance of the proposed scheme is evaluated by various quantitative evaluation parameters such as Correlation, Mean Square Error (MSE) and Peak Signal-to-Noise ratio (PSNR).

Correlation

The correlation represents a relationship between two images. Correlation gives a strong relationship between images and is a statistical property.

Eq. (1) gives correlation coefficient, r between two data sets X and Y as,

$$r = \frac{\sum_{i=1}^{N}(X_i-\overline{X})(Y_i-\overline{Y})}{\sqrt{\sum_{i=1}^{N}(X_i-\overline{X})^2}\sqrt{\sum_{i=1}^{N}(Y_i-\overline{Y})^2}} \quad (1)$$

where, X and Y represents data sets having N values

$\overline{X}$ and $\overline{Y}$ represents mean value of the data sets, given by Eq. (2) and Eq. (3) respectively.

$$\overline{X} = \frac{1}{N}\sum_{i=1}^{N} X_i \quad (2)$$

and,

$$\overline{Y} = \frac{1}{N}\sum_{i=1}^{N} Y_i \quad (3)$$

©2006-2018 Asian Research Publishing Network (ARPN). All rights reserved.

The range of correlation coefficient is -1 and +1. The value $r = 0$ represents no correlation between images, r = +1 indicates positive correlation and r = -1 indicates negative correlation between them. Two images are said to be more correlated to each other when the value of r is nearer to 1.

Mean Square Error (MSE)

The mean square error determines similarity between two images. MSE between two images X and Y is given by the Eq. (4) as,

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (X(i,j) - Y(i,j))^2 \quad (4)$$

where, X and Y represents images,

M × N represents dimensions of images

The larger value of mean square error indicates that X and Y images are less similar to each other and vice versa.

Peak Signal-to-Noise Ratio (PSNR)

The Peak Signal-to-Noise Ratio measures the quality of the image. PSNR is measured in decibel (dB). Basically, PSNR value greater than 20 dB represents good image quality. Normally the contrast of the reconstructed image is measured by PSNR value. PSNR value of the image is given in Eq. (5) as,

$$PSNR = 10 log_{10} \frac{N^2}{MSE} \quad (5)$$

where, N represents maximum pixel value of the given image.

For binary image, N = 1. Generally, the value of N is 255 for gray-scale image and color image. The higher value of PSNR represents better image quality.

The evaluation of quantitative performance parameters of the proposed *(k, n)* secret image sharing scheme between the original secret image and the recovered gray-scale secret images are given in the Table-1. The correlation between original and reconstructed secret images is more and the contrast of the reconstructed image is high for (3, 5) VSS scheme. The MSE is less in (3, 5) scheme compared to other schemes.

Table-1. Quantitative performance evaluation parameters for proposed secret image sharing scheme on 256 × 256 gray-scale image.

Scheme	MSE	PSNR	Correlation
(2,5)	247.2893	72.1963	0.9823
(3,5)	413.6920	84.3895	0.9918
(4,5)	401.8623	73.4287	0.9635
(5,5)	398.3017	85.1744	0.9844

Table-2. Mean square error between original gray-scale image and share images for n=5.

Original, Share	MSE
I, S_1	287.3722
I, S_2	287.4527
I, S_3	287.3421
I, S_4	287.6683
I, S_5	287.1005

Table-3. Quantitative performance evaluation parameters for proposed secret image sharing scheme on 256 × 256 color image.

Scheme	MSE	PSNR	Correlation
(2,5)	549.7443	74.2649	0.9848
(3,5)	306.5495	85.4953	0.9924
(4,5)	327.2970	74.5672	0.9766
(5,5)	335.4682	84.2784	0.9929

Table-4. Mean square error between original color image and share image for n=5.

Original, Share	MSE
I, S_1	306.5495
I, S_2	306.5267
I, S_3	306.5375
I, S_4	306.4995
I, S_5	305.8996

The mean square error between original secret image and share images is very large as shown in Table-2 which indicates large randomness in the generated share images. Hence it is unable to leak any secret information from attacks. The strength of the proposed algorithm is observed to be very high and the security gets improved.

Similarly, quantitative performance evaluation parameters of the proposed scheme for 256 × 256 color image are shown in the Table-3. The (3, 5) secret image sharing scheme has large values of Peak Signal-to-Noise Ratio and correlation between original secret image and reconstructed color image in comparison with other schemes as given in Table-3.

The Table-4 gives the strength of the proposed scheme by comparing mean square error between original secret and share images. The larger mean square error values justifies that this technique never leaks any secret information to attackers.

The Table-5 gives comparison between proposed scheme with other related schemes. The proposed method is compared with existing schemes [3], [4], [5], [17] and [19]. The performance is compared in terms of pixel expansion, codebook design, Basis matrices requirement, hiding method, recovery process, security and contrast.

©2006-2018 Asian Research Publishing Network (ARPN). All rights reserved.

Pixel expansion: The secret image, share images and reconstructed image has same dimensions in the proposed scheme. Hence there is no pixel expansion. The scheme [3] has pixel expansion and the schemes [4], [5], [17], [19] and proposed scheme have no pixel expansion.

Codebook design: The codebook design is not necessary for generation of share images in the proposed scheme. The scheme [3] requires necessary codebook for generation of share images whereas schemes [4], [5], [17] and [19] does not require necessary codebook.

Basis matrices: The proposed *(k, n)* secret image sharing scheme does not require any Basis matrices for generation of share images. The scheme [3] requires necessary Basis matrices for generation of share images whereas schemes [4], [5], [17] and [19] does not require them.

Hiding method: The Boolean XOR and circular left shift operations are used for encoding the original secret image in the proposed scheme. The existing scheme [3] used Basis matrices for hiding secret image. The existing schemes [4] and [5] used random grids, and schemes [17] and [19] used Boolean XOR operations for encoding of the secret image.

Recovery Process: The proposed scheme uses Boolean XOR and circular left shift operations to reconstruct the secret image. The existing schemes [3], [4] and [5] used stacking of share images for reconstruction of the secret image. And, schemes [17] and [19] used Boolean XOR operations to recover the secret image.

Security: The proposed *(k, n)* secret sharing scheme has strong security compared to existing schemes [3], [4], [5], [17] and [19].

Contrast: The visual quality of the proposed scheme is good due to high PSNR value of the reconstructed secret image. The schemes [3] and [4] have less visual quality whereas the schemes [5], [17] and [19] have good contrast value.

Randomness: The parameters such as correlation, mean square error and peak signal-to-noise ratio are used to measure the randomness of the share images. The proposed *(k, n)* secret image sharing scheme achieves better correlation, mean square error and peak signal-to-noise ratio values. The proposed scheme randomness is high compared to schemes [3], [4], [5], [17] and [19] as shown in Table-5.

The proposed method has good contrast and strong security compared to other methods. The hiding and recovery methods of the proposed scheme involve Boolean XOR and circular shift operations which reduces number of computations.

Table-5. Comparison of the proposed and existing schemes.

Parameter	Naor and Shamir [3]	Kafri and Keren [4]	Shyu [5]	Wang, Zhang, Ma and Li [17]	Chen and Wu [19]	Proposed scheme
Pixel Expansion	Yes	No	No	No	No	No
Codebook design	Required	Not required	Not required	Not required	Not required	Not required
Basis matrices	Required	Not required	Not required	Not required	Not required	Not required
Hiding method	Basis matrices	Random grid	Random grid	Boolean XOR	Boolean XOR	Boolean XOR and Circular right shift
Recovery process	Stacking	Stacking	Stacking	Boolean XOR	Boolean XOR	Boolean XOR and Circular left shift
Security	Weak	Weak	Weak	Weak	Weak	Strong
Contrast	Less	Less	Good	Good	Good	Good
Randomness	Low	Low	Average	Average	Average	High

6. CONCLUSIONS

A Boolean operation based secret image sharing scheme is proposed with improved security for gray-scale and color images. The performance of the algorithm is evaluated by using performance metrics such as correlation, mean square error and peak signal-to-noise ratio. The proposed scheme uses Boolean operations during encoding and decoding processes which reduces the computational complexity of the algorithm. A distinct identifier for each share image and circular shifting of pixels increases the security of the secret image further. The recovered secret image is identical to original secret image with high security and less computational complexity. Also, there is an improvement in visual quality of the reconstructed secret image. The proposed scheme may further extended to multiple secret images.

REFERENCES

[1] G. R. Blakley. 1979. Safeguarding cryptographic keys. Afips. p. 313.

[2] A. Shamir. 1979. How to Share a Secret. Commun. ACM. 22(1): 612-613.

©2006-2018 Asian Research Publishing Network (ARPN). All rights reserved.

[3] M. Naor and A. Shamir. 1995. Visual cryptography. Advances in Cryptology - EUROCRYPT'94. 950: 1-12.

[4] O. Kafri and E. Keren. 1987. Encryption of pictures and shapes by random grids. Opt. Lett. 12(6): 377-379.

[5] S. J. Shyu. 2007. Image encryption by random grids. Pattern Recognit. 40(3): 1014-1031.

[6] S. J. Shyu. 2007. Image encryption by multiple random grids. Pattern Recognit. 42(7): 1582-1596.

[7] K. S. Lin, C. H. Lin and T. H. Chen. 2014. Distortionless visual multi-secret sharing based on random grid. Inf. Sci. (Ny). 288(1): 330-346.

[8] H. C. Chao and T. Y. Fan. 2017. XOR-based progressive visual secret sharing using generalized random grids. Displays. 49: 6-15.

[9] X. Yan, S. Wang, X. Niu and C. N. Yang. 2015. Generalized random grids-based threshold visual cryptography with meaningful shares. Signal Processing. 109: 317-333.

[10] X. Yan, S. Wang, A. A. A. El-Latif and X. Niu. 2015. Visual secret sharing based on random grids with abilities of AND and XOR lossless recovery. Multimed. Tools Appl. 74(9): 3231-3252.

[11] D. S. Wang, T. Song, L. Dong and C. N. Yang. 2013. Optimal contrast grayscale visual cryptography schemes with reversing. IEEE Trans. Inf. Forensics Secur. 8(12): 2059-2072.

[12] S. J. Shyu and M. C. Chen. 2011. Optimum pixel expansions for threshold visual secret sharing schemes. IEEE Trans. Inf. Forensics Secur. 6(3, PART 2): 960-969.

[13] I. Kang, G. R. Arce and H. K. Lee. 2011. Color extended visual cryptography using error diffusion. IEEE Trans. Image Process. 20(1): 132-145.

[14] Y. C. Chen, G. Horng, and D. S. Tsai. 2012. Comment on cheating prevention in visual cryptography. IEEE Trans. Image Process. 21(7): 3319-3323.

[15] S. J. Shyu and H. W. Jiang. 2012. Efficient construction for region incrementing visual cryptography. IEEE Trans. Circuits Syst. Video Technol. 22(5): 769-777.

[16] Z. Wang, C. Bovik, H. R. Sheikh and E. P. Simmoncelli. 2004. Image quality assessment: form error visibility to structural similarity. Image Process. IEEE Trans. 13(4): 600-612.

[17] D. Wang, L. Zhang, N. Ma and X. Li. 2007. Two secret sharing schemes based on Boolean operations. Pattern Recognit. 40(10): 2776-2785.

[18] S. Kumar and R. K. Sharma. 2014. Threshold visual secret sharing based on Boolean operations. Secur. Commun. Networks. 7(3): 653-664.

[19] C. C. Chen and W. J. Wu. 2014. A secure Boolean-based multi-secret image sharing scheme. J. Syst. Softw. 92(1): 107-114.

[20] P. M. Fathimala and P. A. J. Rani. 2015. K out of N Secret Sharing Scheme for Gray and Color Images. IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT). pp. 1-4.

[21] J. V. K. Ratnam, T. S. Reddy and P. R. Reddy. 2017. A Review on Visual Secret Sharing Schemes. Int. J. Emerg. Technol. Adv. Eng. 7(11): 223-227.