International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 4 (2018) pp. 1827-1832

Design and Performance Evaluation of Boolean based Secret Image Sharing Scheme

Javvaji V.K. Ratnam[1], T. Sreenivasulu Reddy[2] and P. Ramana Reddy[3]

[1]Research Scholar, Faculty of Electronics and Communication Engineering,
Jawaharlal Nehru Technological University Anantapur, Ananthapuramu, Andhra Pradesh, India.
[1]Orcid: 0000-0003-3099-6673

[2]Professor, Department of Electronics and Communication Engineering,
Sri Venkateswara University College of Engineering, Sri Venkateswara University, Tirupati, Andhra Pradesh, India.

[3]Professor, Department of Electronics and Communication Engineering, University College of Engineering,
Jawaharlal Nehru Technological University Anantapur, Ananthapuramu, Andhra Pradesh, India.

Abstract

A new *(k, n)* secret image sharing scheme by using Boolean XOR and circular shift operations for gray-scale and color secret images having improved security is designed and performance of the proposed scheme is evaluated in this paper. A secret image is encoded into *n* meaningless noise-like share images, transmitted over communication channel, and any *k* or more share images are gathered to reconstruct the secret image by staking them at receiving end. Share images less than *k* in number never reveal the original image. The security of the secret is improved by combining secret image with a random image of same size and by using distinct 8-bit authentication id to each share. The generated share images have high randomness which indicates high security to the secret image. Additional overheads like pixel expansion, codebook design and basis matrices are not required in this scheme compared to other methods. The performance parameters such as mean square error, peak signal-to-noise ratio, correlation and mean absolute error evaluates performance and consistency of the proposed design. Experimental results confirm the security and feasibility of the proposed image sharing scheme.

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

INTRODUCTION

The visual secret sharing scheme (VSS) receives more attention by many researchers recently. It overcomes many difficulties of traditional cryptography techniques. The secret image is converted to different share images and transmitted over the communication networks. The share images are printed on transparencies and superimposed or stacked together to identify the reconstructed secret image at the receiving side by human visual system without computational complexity. These multiple share images do not give any information about the original secret. Hence the basic property of the image security is satisfied by the secret sharing scheme.

Initially, the secret sharing scheme was proposed by Blakley [1] and Shamir [2]. The concept of Visual Cryptography (VC) based VSS is first introduced by Naor and Shamir [3]. The *(k, n)* visual secret sharing proposed by them divides the binary secret image into *n* meaningless noise-like share or shadow images with the help of Basis matrices. The secret image is recovered by stacking at least *k* share images or more together and less than *k* shares never reveal the secret information. For example, the two Basis matrices for (2, 2) visual secret sharing scheme used to encrypt the original binary image are denoted by S^0 and S^1 are $S^0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$ and $S^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. The pixels of secret image are encoded into subpixels by pixel expansion factor, denoted by *m* using Basis matrices. Each white pixel in secret image is encoded as subpixels of two share images with [0 1] and [0 1] from matrix S^0 and for each black pixel in the secret is encoded as subpixels of two share images with [0 1] and [1 0] from matrix S^1. The pixel expansion factor, m is 2 in this example. The size of share images and reconstructed image is proportional to the pixel expansion factor. Hence this scheme requires more memory and bandwidth for share images and reconstructed images. Logical OR is the underlying operation in this scheme. The drawbacks of this traditional VC based VSS are pixel expansion, need for Basis matrices, design of codebook, low visual quality of the reconstructed secret, share alignment problems, more storage space and bandwidth requirement.

Kafri and Keren [4] proposed random grid based visual secret sharing scheme which eliminates the problems of codebook design, basis matrices and pixel expansion. Researchers [5]-[10] suggested various schemes using random grid based VSS to improve the security and visual quality of the reconstructed image. The size of the reconstructed image is same as the original secret. Hence additional requirements of memory and bandwidth are eliminated. These schemes require complex computations and proper alignment of share images.

Researchers suggested different VSS methods to enhance visual quality [11], reduction in pixel expansion [12], sharing of color image [13], cheating prevention [14] and region incrementing [15] and quality metrics for assessing the image quality [16].

A secret sharing scheme based on Boolean operations eliminates the problems of complex computations and perfect alignment of share images. Various Boolean based schemes

[17-22] are suggested to improve contrast of the reconstructed image and require little computations during the recovery process of the secret.

In this paper, a Boolean operation based visual secret sharing scheme is proposed for gray-scale and colour images. The main contribution in this paper is to improve the security of the secret image by providing additional feature of distinct authentication id to each share of the secret image. The performance of the proposed scheme is evaluated by using different quantitative metrics such as Mean Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR), correlation and Mean Absolute Error (MAE). The consistency of the proposed scheme is compared with the existing schemes.

PROPOSED *(k, n)* SECRET IMAGE SHARING SCHEME

In this section, a new *(k, n)* secret image sharing scheme based on Boolean XOR operations and circular shift operations is proposed. The *n* numbers of meaningless share images are generated by encrypting the secret image with a random image of same size and applying circular shift operations. These share images are transmitted over communication channel. The secret image will be reconstructed by stacking at least *k* number of share images and less than *k* shares never reveal the secret image.

A random image X of same size as original secret is generated and combined with the secret image. The resultant image Y is divided by *k* (minimum number of shares required to reconstruct the secret) to obtain the encrypted image B. An 8-bit random number is chosen for each share separately. Range of the random number is 0 to 255. An authentication id is generated by rearranging 8 bits of this random number. The four Least Significant Bits (LSB) are kept as same and four Most Significant Bits (MSB) are calculated by performing Boolean XOR operation on four least significant bits and four most significant bits. The resultant 8-bit number is considered as Authentication id to the respective share image. Hence *n* number of authentication ids is generated. This authentication id, supplied by the owner of the secret image, is used during reconstruction of the original secret. The encrypted image B is circularly right shifted by a number of bit positions specified by authentication id. The resultant right shifted image will be the share image S of the corresponding authentication id. Hence *n* numbers of share images S_i (for $1 \le i \le n$) are generated by using unique authentication ids. The resultant share images are noise-like meaningless shares which does not give any information about original secret image.

During the reconstruction process, at least *k* share images are required to recover the secret image. All *k* or more share images are circularly left shifted by respective authentication ids. The output values are summed together and Boolean XORed with random image X to obtain the reconstructed secret image G_1.

MERITS OF THE PROPOSED SCHEME

1. There is no pixel expansion problem.
2. Additional storage and bandwidth are not required for share images and reconstructed image.
3. There is no specific codebook design for share generation.
4. Basis matrices are not needed during the encoding process.
5. The proposed scheme is suitable for wide image format such as binary, gray-scale and color images.

The generation of distinct authentication id and corresponding circular shift operations to each share is the novelty in the proposed technique which further improves the security of the secret image from different attacks.

The algorithms for generation of share images and recovered image are given below:

Algorithm 1: Generation of share images S_i of the secret image

Input: Secret image G having $w \times h$ dimensions
Output: Noise-like meaningless share images S_i, for $i=1,2,\ldots\ldots,n$ having $w \times h$ dimensions

1. Generation of random image X
   $X(i,j) = random(255)$, *for* $i=1,2,\ldots\ldots,w$ *and for* $j=1,2,\ldots\ldots,h$.
2. Combine secret image with random image
   $Y(i,j) = G(i,j) \oplus X(i,j)$, *for* $i=1,2,\ldots\ldots,w$ *and for* $j=1,2,\ldots\ldots,h$.
   where, $\oplus$ denotes Boolean XOR operation.
3. Generation of encrypted image B
   $B(i,j) = Y \div k$, *for* $i=1,2,\ldots\ldots,w$ *and for* $j=1,2,\ldots\ldots,h$.
4. Generation of share images
   while $(1 \le i \le n)$
   {
   $ran(i) = random(255)$
   authentication_id(i) = [4-bit MSB(ran(i) $\oplus$ *4-bit LSB(ran(i) 4-bit LSB(ran(i))]*
   Share_image, S_i *= circularrightshift(B, authentication_id(i))*
   }
5. Output share images $S_1, S_2, \ldots\ldots\ldots, S_n$.

Algorithm 2: Reconstruction of secret image G_1

Input: share images $S_1, S_2, \ldots\ldots\ldots, S_k$ having $w \times h$ dimensions
Output: Recovered secret image G_1 having $w \times h$ dimensions

1. *k* shares are combined

while $(1 \le i \le k)$
{
$R = circularleftshift(B, authentication\_id(i))$
}

2. Generation of reconstructed secret image G_1

$G_1(i,j) = R(i,j) \oplus X(i,j)$, *for* $i=1,2,\ldots\ldots,w$ *and for* $j=1,2,\ldots\ldots,h$.

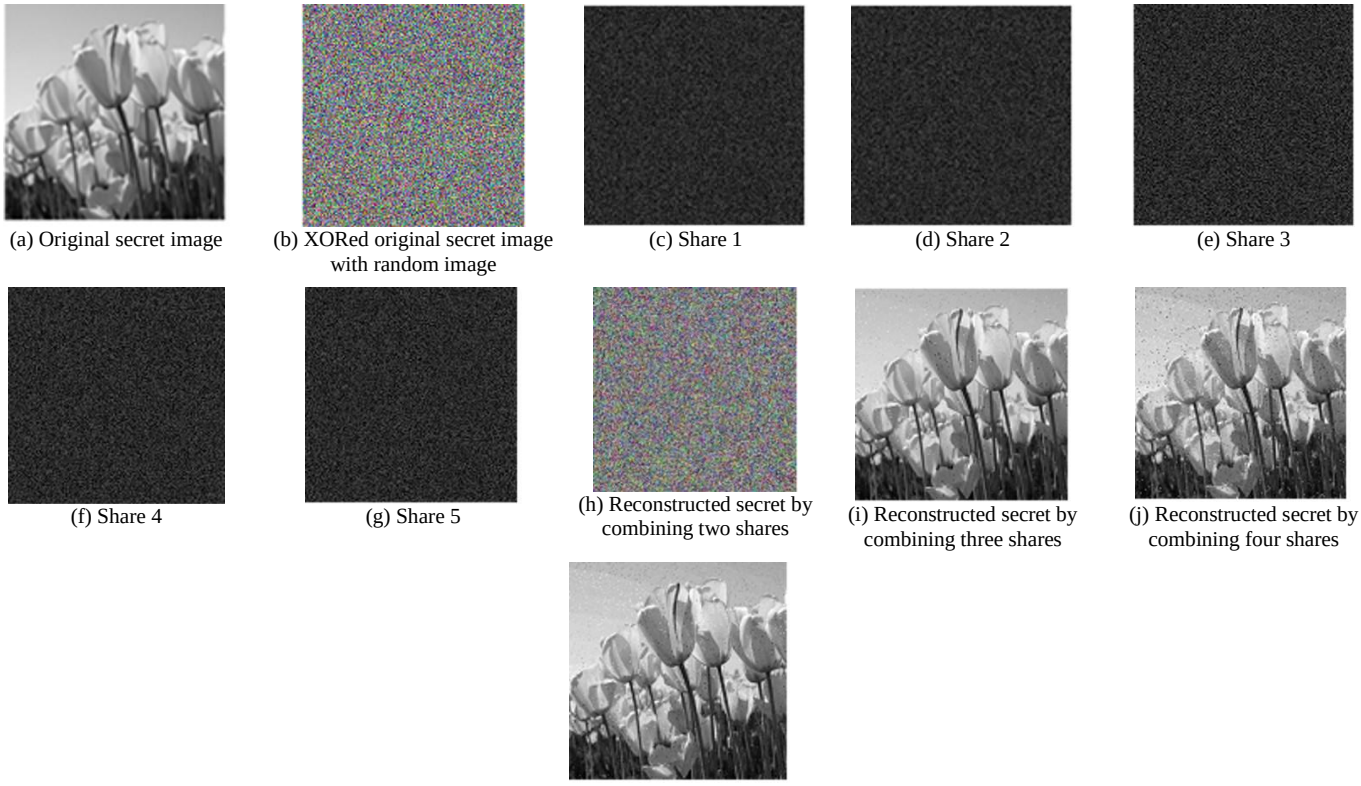
3. Output reconstructed image G_1

EXPERIMENTAL RESULTS AND DISCUSSION

The experimental results and corresponding analysis of the proposed *(k, n)* secret image sharing scheme is discussed in this section. The proposed scheme is applied to both gray-scale and color images. The experiments are performed on 200 different images to analyze the randomness, security and efficiency of the scheme. This scheme functions efficiently for any number of original secret images. The gray-scale image of Tulip having dimensions 256 × 256 pixels has been considered for experimental analysis and discussion. Similarly, color image of Lighthouse with dimensions of 256 × 256 pixels is chosen for experimental analysis and discussion in the paper.

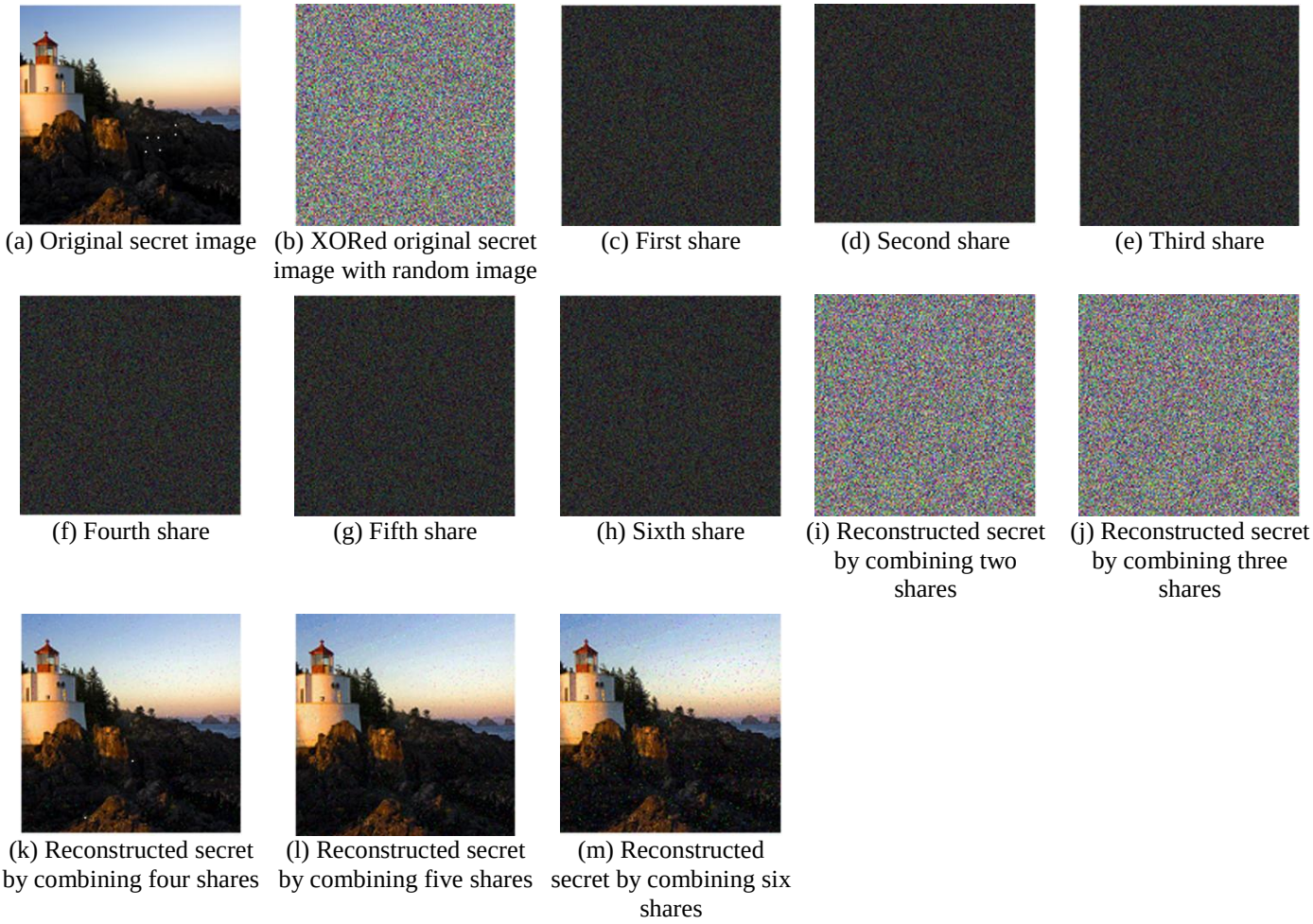
Figure 1 demonstrates the experimental results of (3, 5) visual secret sharing scheme conducted on gray-scale secret image. This original image shown in Figure 1(a) is combined with random image of 256 × 256 size to obtain encrypted image shown in Figure 1(b). The noise-like random shares shown in Figures 1(c)-1(g) are generated by circular shift operation and authentication ids. It is observed that these share images does not give any information about the original secret image. Figure 1(h) shows the recovered secret by stacking two shares images and gives no information about original secret. The recovered secret images shown in Figure 1(i), Figure 1(j) and Figure 1(k) are obtained by stacking three, four and five meaningless noise-like share images respectively. It is observed that the secret will be visually recovered by staking at least three shares, and less than three shares do not reveal the secret image.

The experimental results of (4, 6) secret image sharing scheme for color secret image are given in Figure 2. The secret color image as shown in Figure 2(a) is encrypted by combining random image of same size, i.e. 256 × 256. The encrypted image is given in Figure 2(b). The meaningless noise-like share images shown in Figures 2(c)-2(h) are generated by performing circular right shift operation of encrypted image pixels by using distinct authentication ids. Figures 2(i)-2(j) are obtained by stacking two and three share images respectively. These stacked images do not give information about secret image. The secret image is reconstructed by stacking four, five and six share images as shown in Figures 2(k), 2(l) and 2(m) respectively. It is observed that at least four images are required to visually reconstruct the secret image, and less than four shares do not reveal the secret.



(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 by combining two shares
(i) Reconstructed secret by combining three shares
(j) Reconstructed secret by combining four shares
(k) Reconstructed secret by combining five shares

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) Sixth share (i) Reconstructed secret by combining two shares (j) Reconstructed secret by combining three shares

(k) Reconstructed secret by combining four shares (l) Reconstructed secret by combining five shares (m) Reconstructed secret by combining six shares

Figure 2. Experimental results of (4, 6) visual secret sharing scheme on 256 × 256 color image

PERFORMANCE EVALUATION MEASURES

The performance of the designed scheme is evaluated by different quantitative evaluation metrics such as Mean Square Error (MSE), Peak Signal-to-Noise ratio (PSNR), Correlation and Mean Absolute Error (MAE).

Mean Square Error (MSE)

Mean square error determines the similarity between two images. MSE between two images X and Y is given by Eq. (1).

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

where, X and Y represents images,

M × N represents dimensions of images

Higher value of MSE indicates that the images X and Y are less similar and vice versa.

Peak Signal-to-Noise Ratio (PSNR)

The quality of the image is measured by using Peak Signal-to-Noise Ratio. The PSNR is measured in decibel (dB). Generally PSNR value greater than 20 dB represents good quality of the image. Generally the contrast of the reconstructed image is measured by PSNR value. The Eq. (2) gives PSNR value of the given image.

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

where N indicates maximum pixel value.

The value of N is 1 for binary images. Generally, the value of N is 255 for gray-scale and colour images. Higher value of PSNR indicates better image quality.

Correlation

The relationship between two images is represented by correlation among them. It is a statistical property which gives a strong relation between images.

The correlation coefficient, *r* is given by the Eq. (3).

$$r = \frac{\sum_{i=1}^{N} (X_i - \overline{X})(Y_i - \overline{Y})}{\sqrt{\sum_{i=1}^{N} (X_i - \overline{X})^2} \sqrt{\sum_{i=1}^{N} (Y_i - \overline{Y})^2}} \quad (3)$$

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. (4) and Eq. (5) respectively.

$$\overline{X} = \frac{1}{N}\sum_{i=1}^{N} X_i \quad (4)$$

$$\overline{Y} = \frac{1}{N}\sum_{i=1}^{N} Y_i \quad (5)$$

The range of correlation coefficient between two images is -1 and +1. The value r = 0 indicates no correlation between images, r = +1 indicates positive correlation and r = -1 indicates negative correlation between them. The value of r nearer to 1 represents that two images are more related to each other.

Mean Absolute Error (MAE)

Mean absolute error determines the strength of the algorithm from different attacks. MAE between two images X and Y is given by Eq. (6).

$$MAE = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}|X(i,j) - Y(i,j)| \quad (6)$$

where, |.| indicates absolute value.

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

Scheme	MSE	PSNR	Correlation	MAE
(2,5)	140.8661	26.6767	0.9811	3.4445
(3,5)	55.2582	30.7408	0.9926	2.3370
(4,5)	263.0668	23.9641	0.9652	6.0047
(5,5)	91.8441	28.5343	0.9878	3.7660

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

Original, Share	MAE
G, S_1	101.7515
G, S_2	101.7740
G, S_3	101.7947
G, S_4	101.8057
G, S_5	101.7733

Table 3. Quantitative evaluation metrics for proposed visual secret sharing scheme on 256 × 256 color image

Scheme	MSE	PSNR	Correlation	MAE
(2,6)	699.8336	73.4948	0.9863	11.2567
(3,6)	240.1856	87.4034	0.9953	7.5747
(4,6)	0.001411	64.3281	0.9722	20.4040
(5,6)	325.6165	83.4444	0.9936	11.7053
(6,6)	937.0445	69.6685	0.9816	17.3840

Table 4. Mean absolute error between original color image and share image for n=6

Original, Share	MAE
G, S_1	261.9921
G, S_2	261.9863
G, S_3	262.3787
G, S_4	261.9961
G, S_5	262.5227
G, S_6	262.5243

The quantitative evaluation metrics for the proposed *(k, n)* secret image sharing scheme between original and recovered gray-scale secret images are given in Table 1. The original and reconstructed secret images are more correlated to each other and contrast of the reconstructed image is high for (3, 5) VSS scheme. Also, MSE and MAE are less in (3, 5) scheme compared to other schemes. The MAE between original secret and share images is very large as given Table 2. It represents large randomness in generated shares and unable to leak any secret information from attacks. Hence the strength of the algorithm is observed to be very high and the secrecy gets improved.

Similarly, performance measures of the proposed scheme for 256 × 256 color image are shown in the Table 3. It is observed that (3, 6) VSS scheme have large values of PSNR and correlation between original secret and reconstructed color images compared to other schemes. The MSE and MAE values give the similarity between original and reconstructed color images. Table 4 represents strength of the proposed scheme by comparing MAE between original and share images. These values justify that this scheme never leaks any secret information to different attackers.

The performance of the proposed scheme is compared with other existing schemes as given in Table 5. The proposed method consistency is checked. The performance is compared in terms of pixel expansion, need for Basis matrices, codebook design, hiding, decoding process, contrast and security. The proposed method has strong security features and good contrast 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 scheme with existing schemes

Parameter	Naor and Shamir [3]	Kafri and Keren [4]	Shyu [5]	Wang, Zhang, Ma and Li [17]	Chen and Wu [20]	Proposed
Pixel Expansion	Yes	No	No	No	No	No
Basis matrices	Required	Not required	Not required	Not required	Not required	Not required
Codebook design	Required	Not required	Not required	Not required	Not required	Not required
Hiding	Basis matrices	Random grid	Random grid	Boolean XOR	Boolean XOR	Boolean XOR and Circular right shift
Recovery	Stacking	Stacking	Stacking	Boolean XOR	Boolean XOR	Boolean XOR and Circular left shift
Contrast	Less	Less	Good	Good	Good	Good
Security	Weak	Weak	Weak	Weak	Weak	Strong

CONCLUSION

A secret image sharing scheme based on Boolean operations is proposed for gray-scale and color images along with its performance evaluation. The proposed scheme uses Boolean operations during encoding and decoding processes of given secret image which reduces the computational cost of the algorithm. A distinct authentication id to each share image and circularly 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 fewer computations. This scheme may further extended to multiple secret images having good quality and more security.

REFERENCES

[1] Blakley, G.R., 1979, "Safeguarding cryptographic keys," AFIPS Conference Proceedings, 48, pp. 313–317.
[2] Shamir, A., 1979, "How to share a secret," Communication of the ACM, 22(11), pp. 612–613.
[3] Naor, M., and Shamir, A., 1995, "Visual Cryptography," Proceedings of Advances in Cryptology (EUROCRYPT' 94), (Lecture Notes in Computer Science, 950, pp. 1-12.
[4] Kafri, O., and Keren, E., 1987, "Encryption of pictures and shapes by random grids," Optics Letters, 12, pp. 377–379.
[5] Shyu, S. J., 2007, "Image encryption by random grids", Pattern Recognition, 40, pp. 1014–1031.
[6] Shyu, S.J., 2009, "Image encryption by multiple random grids," Pattern Recognition, 42: pp. 1582–1596.
[7] Chen, T. H., and Tsao, K. H., 2009, "Visual secret sharing by random grids revisited," Pattern Recognition, 42: pp. 2203–2217.
[8] Lin, K.S., Lin, C.H. and Chen, T.H., 2014, "Distortionless visual multi-secret sharing based on random grid", Information Sciences, 288, pp. 330–346.
[9] Yan, X., Wang, S., Niu, X., and Yang, C.N., 2015, "Generalized random grids-based threshold visual cryptography with meaningful shares," Signal Processing, 109 pp. 317–333.
[10] Chao, H.C., and Fan, T.Y., 2017, "XOR-based progressive visual secret sharing using generalized random grids," Displays, 49, 6–15.
[11] Wang, D.S., Song, T., Dong, L., and Yang, C.N., 2013, "Optimal contrast grayscale visual cryptography schemes with reversing," IEEE Transactions on Information Forensics and Security, 8(12), pp. 2059-2072.
[12] Shyu, S.J., and Chen, M.C., 2011, "Optimum pixel expansions for threshold visual secret sharing schemes," IEEE Transactions on Information Forensics and Security, 6(3), pp. 960-969.
[13] Kang, I., Arce, G.R., and Lee, H.K., 2011, "Color extended visual cryptography using error diffusion," IEEE Transactions on Image Processing, 20(1), pp. 132-145.
[14] Chen, Y.C., Horng, G., and Tsai, D.S., 2012, "Comment on Cheating prevention in visual cryptography," IEEE Transactions on Image Processing, 21(7), pp. 3319–3323.
[15] Wang, R.Z., 2009, "Region Incrementing Visual Cryptography," IEEE Signal Processing Letters, 16(8), pp. 659-662.
[16] Wang, Z., Bovik, A.C., Sheikh, H. R., and Simoncelli, E.P., 2004, "Image Quality Assessment: From Error Visibility to Structural Similarity," IEEE Transactions on Image Processing, 13(4), pp. 600-612.
[17] Wang, D., Zhang, L., Ma, N., and Li, X., 2007, "Two secret sharing schemes based on Boolean operations," Pattern Recognition 40, pp. 2776–2785.
[18] Chao, K.Y., and Lin, J.C., 2009, "Secret image sharing: a Boolean-operations-based approach combining benefits of polynomial-based and fast Approaches," International Journal of Pattern Recognition and Artificial Intelligence, 23, pp. 263–285.
[19] Kumar, S., and Sharma, R. K., 2013, "Threshold visual secret sharing based on Boolean operations", Security and Communication Networks.
[20] Chen, C.C., and Wu, W.J., 2014, "A Secure Boolean-based multi-secret image sharing scheme," Journal of Systems and Software, 92, pp. 107–114.
[21] Fathimal, P.M., and Jansi Rani, P.A., 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.
[22] Ratnam V.K. Javvaji, Sreenivasulu Reddy, T., and Ramana Reddy, P., 2017, "A Review on Visual Secret Sharing Schemes," International Journal of Emerging Technology and Advanced Engineering, 7(11), pp. 223–227.