https://doi.org/10.29042/2020-10-2-80-86

Helix (2020) 10 (2): 80-86

Design of Boolean XOR based *(n, n)* Secret Image Sharing Schemes with Contrast and Security Improvement

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

[1,3]Department of Electronics and Communication Engineering, University College of Engineering, Jawaharlal Nehru Technological University Anantapur, Ananthapuramu, Andhra Pradesh, India

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

E-mail: ratnamjvklakshmi@yahoo.co.in, mettu86@yahoo.co.in, prrjntu@gmail.com

Received: 26th January 2020, Accepted: 15th February 2020, Published: 30th April 2020

Abstract

In this research paper, two novel *(n, n)* secret image sharing schemes are proposed in which all share images are used for reconstruction of secret image(s) instead of threshold number of share images. The first proposed *(n, n)* secret image sharing scheme shares single secret image whereas multiple secret images are used for sharing in the second proposed scheme. The random images are generated by applying circular shift operations. The share images are generated by applying Boolean Exclusive-OR (XOR) operations on random images and secret image(s). The XOR operations improve contrast and circular shift operations improve security of the secret image(s). The proposed schemes are suitable for gray-scale and color images. The experimental simulation results and comparison with existing schemes provide consistency and feasibility of proposed schemes.

Keywords

Boolean XOR; Circular Shift; Contrast; Security; Secret Sharing

Introduction

The increased transmission of multimedia content through the internet made the communication easier and inexpensive. However, the security problems are observed in the transmission and storage of the important information. Though the traditional cryptographic techniques provide better security, they suffer from limitations like complex computations, knowledge of key(s) and mathematical awareness in encrypting and decrypting the secret message. The visual cryptography schemes overcome the limitations of the traditional cryptographic schemes. Naor and Shamir [1] introduced visual cryptography concept in which given secret image is divided into n shadow images or share images, and minimum k (for $k \leq n$) number of shares are stacked together at the destination for recovery of the secret image by human eye. The message to be communicated in the visual cryptography is in the form of the digital image. The visual cryptography schemes suffer from limitations like pixel expansion, large memory, poor contrast, shares alignment problems, etc. It is a challenging task to devise secret image sharing schemes to satisfy security, visual quality or contrast, computational complexity, shares alignment problems and additional storage memory requirement.

Various researchers proposed different schemes to share the secret image such as polynomial based scheme [2, 3], random grids [4], Boolean operation based schemes [5], region incrementing [6], tagged visual cryptography [7] and progressive visual cryptography [8]. The contrast of the reconstructed image is average and high computational complexity in these schemes.

The Boolean XOR based secret image sharing schemes solve the problem of poor contrast in the reconstructed secret image and simplifies the encoding-decoding procedures with less number of computations. Boolean based secret image sharing schemes [8-13] are proposed to solve problems related to contrast in recovered secret image. There is a scope to design schemes for improvement in contrast and security of the secret image.

Novel Boolean XOR based *(n, n)* secret image sharing schemes are introduced in this paper. The proposed techniques have advantages like no pixel expansion, no need to design codebook and no Basis matrices required during share images generation. The quality evaluation metrics [14,15] such as correlation, Peak Signal-to-Noise Ratio (PSNR) and Mean Structural SIMilarity index (MSSIM) are used for verification of experimental simulation results in proposed schemes.

The rest of the paper is organized as follows. The second section reviews the related work. The third section introduces the proposed secret image sharing schemes. The experimental results of the proposed schemes and comparison with related schemes are presented in fourth section. Finally, the fifth section gives conclusion and further research.

Related Work

The secret image sharing schemes proposed by researchers suffer from limitations such as more complex computations and lossy recovery [16, 17], non-random shares [18] and threshold security [18, 19]. Earlier schemes proposed by other researchers concentrated mainly on improvement in the pixel expansion value.

Proposed Secret Image Sharing Schemes

A. (n, n) Secret Image Sharing Scheme for Single Secret Image

In this section, a new Boolean XOR based *(n, n)* secret image sharing scheme for single secret image is proposed. The circular shift function [18] is used for generation of distinct random images. The circular shift function is used to generate distinct random images R_{0k} such that $1 \leq k \leq n-1$. The circular shift function shifts circularly the bits of individual random image pixel by a parameter based on the location of the pixel and modulus operation. Also, this parameter depends on the distinct random image number. The security of the secret image is improved by applying circular shift and modulus operations on each pixel of the secret image. The *n-1* distinct random images and the original secret image are used for generation of *n* share images. The Boolean XOR operations are applied to generate share images. These share images are transmitted through communication channel to the destination. The implementation for generation of share images is given in Algorithm 1.

Algorithm 1: Generation of Share images

```
Input: $w \times h$ Secret image G and an integer n, for $n \geq 2$
Output: Share images $S_i$, for $1 \leq i \leq n$
Step 1:  Generation of n-1 individual random images $R_k$,
         $R_k[i, j] \in$ random(255), for $1 \leq k \leq n-1$, $1 \leq i \leq w$ and $1 \leq j \leq h$.
Step 2:  Generation of n-1 distinct random images $R_{0k}$,
         $R_{0k} = F(R_k) = \text{Circular\_shift}(R_k(x, y), (x + y + k) \bmod 8)$, for $1 \leq k \leq n-1$
Step 3:  Generation of n share images
         $S_1 = R_{01}$
         $S_2 = R_{01} \oplus R_{02}$
         $S_3 = R_{02} \oplus R_{03}$
          . . . . . . . .
          . . . . . . . .
         $S_{n-1} = R_{0n-2} \oplus R_{0n-1}$
         $S_n = R_{0n-1} \oplus G$
Step 4:  Output n share images, $S_1, S_2, \ldots\ldots, S_n$
```

The Boolean XOR operations are applied on share images to recover the secret image. All *n* share images are required for recovery of the secret image. The secret image is not reconstructed by using less than *n* share images. The algorithmic implementation for reconstruction of the secret image is given in Algorithm 2 below.

Algorithm 2: Reconstruction of the Secret image

```
Input: n share images $S_1, S_2, \ldots\ldots, S_n$
Output: Reconstructed secret image $G_1$
Step 1:  Recovery of the secret image, $G_1$
         $G_1 = S_1 \oplus S_2 \oplus S_3 \oplus \ldots\ldots\ldots \oplus S_n$
Step 2:  Output reconstructed secret image, $G_1$
```

These share images are look like noisy, meaningless and are unable to leak any information of the original image which improves the security of the secret image. The Boolean XOR operations in the proposed scheme improve contrast of the reconstructed secret image and circular shift operations improve security of the secret image.

B. (n, n) Secret Image Sharing Scheme for Multiple Secret Images

In this section, a new Boolean XOR based *(n, n)* secret image sharing scheme for multiple secret images is proposed. The random images, R_i (for i = 1, 2, 3, 4, ... , *n*) are in the form of random matrices having values between 0 and 255. These random images have same size as the secret images. The circular shift function is applied on all random images R_i to generate distinct random images R_{0i}. The Circular_shift() function is applied on each pixel of the random image $R_i(x, y)$ using circular left shift operation by a shift value of $((x + y + n) \bmod 8)$. The resultant image is another random image R_{0i}. This two-level generation of random images further improves the security of given secret images. The share images S_i are generated by using XOR operations on original secret images G_i and corresponding random images R_{0i}. These share images are transmitted to destination. The algorithmic implementation for generation of share images for the given secret images is given in Algorithm 3.

Algorithm 3: Generation of Share images

```
Input: $w \times h$ Secret images $G_i$, for $1 \leq i \leq n$
Output: Share images $S_i$, for $1 \leq i \leq n$
Step 1:  Generation of individual random images $R_k$, for $1 \leq k \leq n$
         where, $R[i, j] \in$ random(255), $1 \leq i \leq w$ and $1 \leq j \leq h$.
Step 2:  Generation of distinct random images $R_{0i}$, for $1 \leq i \leq n$,
         $R_{0i} = F(R_i) = \text{Circular\_shift}(R_i(x, y), (x + y + i) \bmod 8)$, for $1 \leq i \leq n$
```

```
Step 3:  Generation of n share images
         $S_i = G_i \oplus R_{0i}$, for $i = 1$
         $S_i = G_i \oplus S_{i-1} \oplus S_{i-2} \oplus \ldots \oplus S_1 \oplus R_{0i}$,  for $i = 2, 3, 4, \ldots, n$
Step 4:  Output n share images ($S_1, S_2, \ldots, S_n$)
```

The individual random images R_i, for $1 \le i \le n$, are used to generate distinct random images R_{0i} using circular shift function. The secret images are reconstructed by applying bit-wise XOR operations on these random images R_{0i} and share images S_i. The algorithmic implementation for reconstruction of secret images is given in Algorithm 4.

Algorithm 4: Reconstruction of Secret images

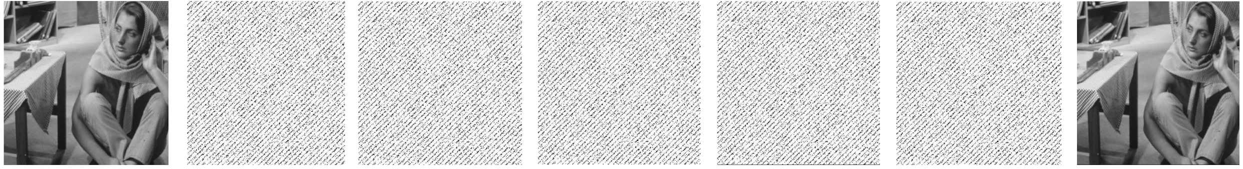
```
Input: Share images $S_i$, for $1 \le i \le n$
Output: Recovered Secret images $G'_i$, for $1 \le i \le n$
Step 1:  Generation of distinct random images $R_{0i}$, for $1 \le i \le n$,
         $R_{0i} = F(R_i) = \text{Circular\_shift}(R_i(x, y), (x + y + i) \bmod 8)$, for $1 \le i \le n$
Step 2:  Reconstruction of n secret images
         $G'_i = S_i \oplus R_{0i}$,   for $i = 1$
         $G'_i = S_i \oplus S_{i-1} \oplus S_{i-2} \oplus \ldots \oplus S_1 \oplus R_{0i}$,  for $i = 2, 3, 4, \ldots, n$
Step 3:  Output n reconstructed secret images ($G'_1, G'_2, \ldots, G'_n$)
```

The novelty of the proposed schemes is the use of circular shift operations in addition to Boolean XOR operations in the share images generation and reconstruction of secret images along with high sharing capacity. The implementation of the proposed schemes is easy because of Boolean operations and symmetric functional use in the generation of share images and reconstruction of secret images.

Results and Discussions

The experimental simulation results, quality evaluation metrics and comparison demonstrate the consistency and feasibility of proposed schemes. All experiments are performed using MATLAB 8.3 with an Intel i3-4000M CPU and 4 GB RAM.

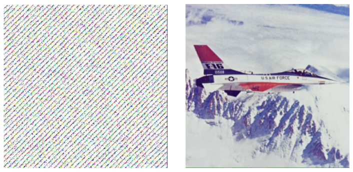
The original gray-scale secret image G chosen here is 'Barbara' as shown in Fig. 1(a) for the proposed (3, 3) secret image sharing scheme. The size of the secret image G is 256 × 256. Fig. 1(b) and Fig. 1(c) shows the distinct random images R_{01} and R_{02} respectively, obtained from the secret image and circular shift operations. The share images S_1, S_2 and S_3 are shown in Fig. 1(d)-(f). The distinct random images and share images are observed to be random and unable to give any information about the secret image. The share images are distributed to participants. The secret image G_1 is reconstructed at the destination by collecting all share images together. The reconstructed secret image is shown in Fig. 1(g). The sizes of distinct random images, share images and reconstructed secret image are same as the original secret image. The Boolean XOR operations are utilized in the proposed scheme enhances visual quality of the reconstructed secret image and the circular shift of each pixel bits to generate distinct random images increases the security of the given secret image.



(a) Original Secret image
(b) Distinct random image1
(c) Distinct random image2
(d) Share image1
(e) Share image2
(f) Share image3
(g) Reconstructed secret image

Fig. 1: Experimental Simulation Results of (3, 3) Secret Image Sharing Scheme for Gray-scale Image

(a) Original Secret image
(b) Distinct random image1
(c) Distinct random image2
(d) Distinct random image3
(e) Share image1
(f) Share image2
(g) Share image3



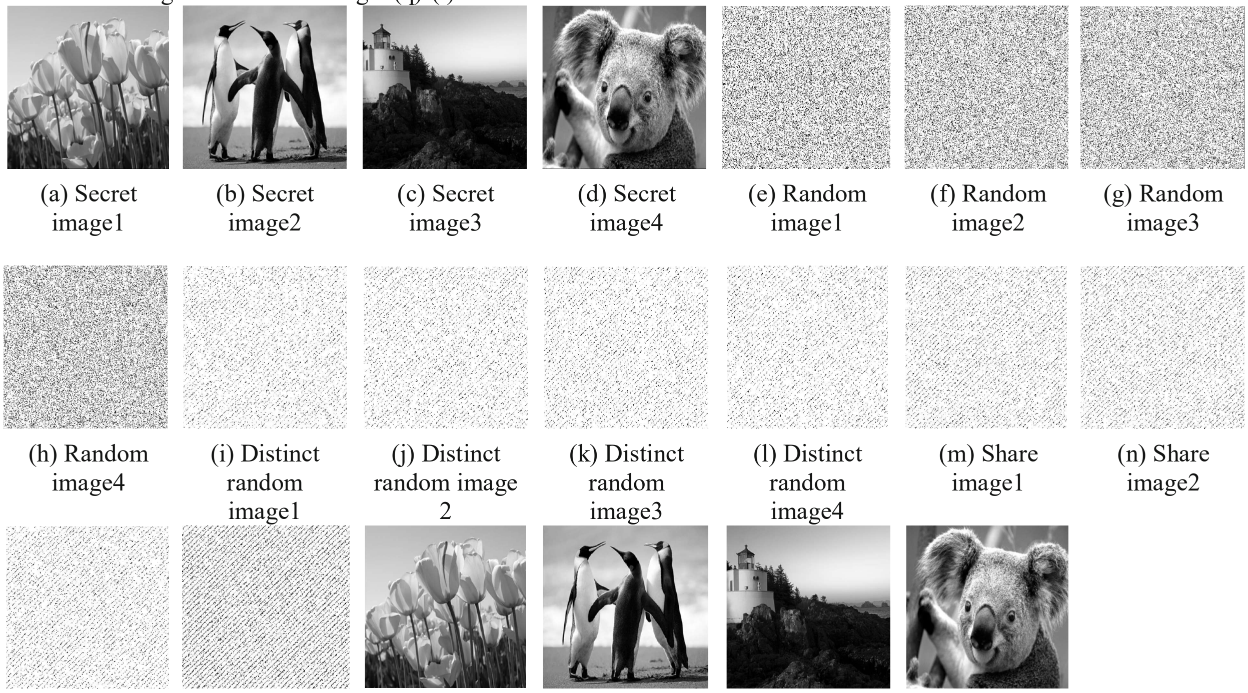
(h) Share image4

(i) Reconstructed secret image

Fig. 2: Experimental Simulation Results of (4, 4) Secret Image Sharing Scheme for Color Image

The experimental simulation results of (4, 4) secret sharing scheme for color image ‘Airplane’ is given in Fig. 2. The original color secret image is shown in Fig. 2(a). The size of the secret image is 256 × 256 × 3. The three distinct random images obtained by circular shifting of pixel bits in original secret image are shown in Fig. 2(b)-(d). The generated four share images are shown in Fig. 2(e)-(h). The image shown in Fig. 2(i) is reconstructed at the destination. It is observed that the security of the secret image is improved and the contrast of recovered secret image is high in the proposed scheme.

The experimental results of (4, 4) multiple secret images sharing scheme for gray-scale images are illustrated in Fig. 3. The original gray-scale secret images G_1, G_2, G_3 and G_4 chosen here are ‘Tulips’, ‘Penguins’, ‘Lighthouse’ and ‘Koala’ respectively as shown in Fig. 3(a)-(d). The size of each secret image is 512 × 512. Fig. 3(e)-(h) shows the random images. The circular shift function is applied on these random images for generation of distinct random images shown in Fig. 3(i)-(l) respectively. The generated share images S_1, S_2, S_3 and S_4 are shown in Fig. 3(m)-(p) are unable to give any information of the secret images. The reconstructed secret images are shown in Fig. 3(q)-(t).



(a) Secret image1

(b) Secret image2

(c) Secret image3

(d) Secret image4

(e) Random image1

(f) Random image2

(g) Random image3

(h) Random image4

(i) Distinct random image1

(j) Distinct random image 2

(k) Distinct random image3

(l) Distinct random image4

(m) Share image1

(n) Share image2

(o) Share image3

(p) Share image4

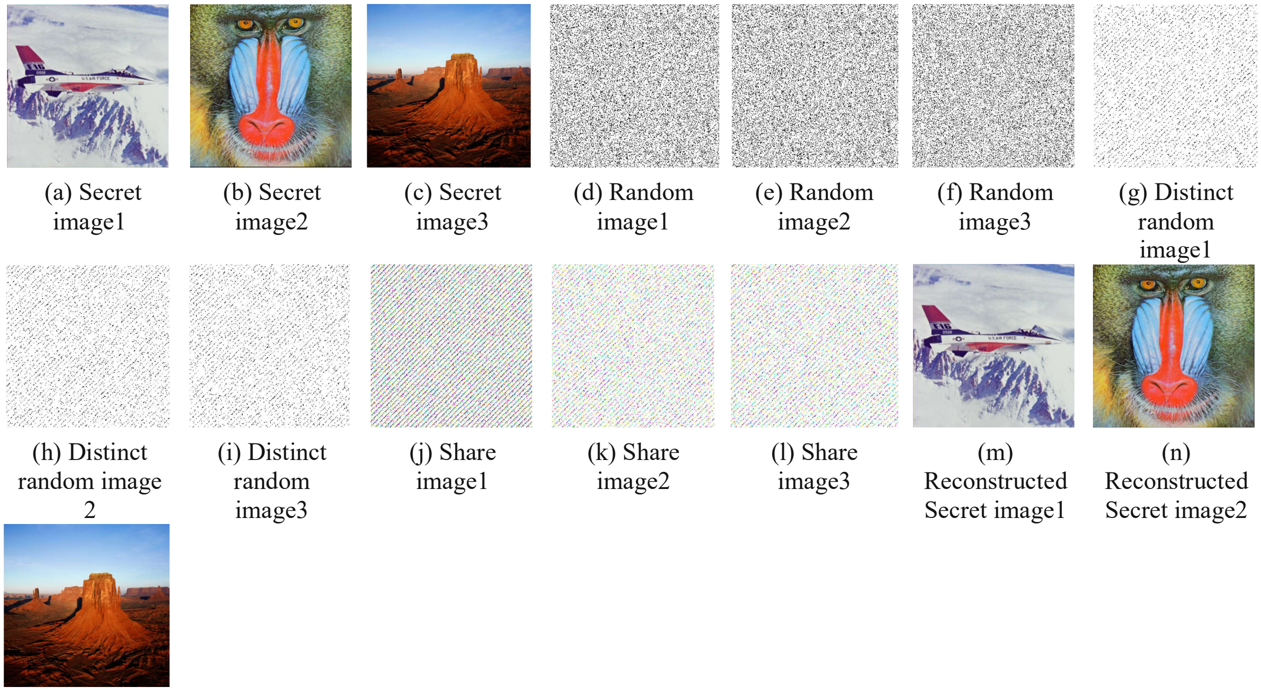
(q) Reconstructed Secret image1

(r) Reconstructed Secret image2

(s) Reconstructed Secret image3

(t) Reconstructed Secret image4

Fig. 3: Experimental Simulation Results of (4, 4) Multiple Secret Images Sharing Scheme for Gray-scale Images



(a) Secret image1

(b) Secret image2

(c) Secret image3

(d) Random image1

(e) Random image2

(f) Random image3

(g) Distinct random image1

(h) Distinct random image 2

(i) Distinct random image3

(j) Share image1

(k) Share image2

(l) Share image3

(m) Reconstructed Secret image1

(n) Reconstructed Secret image2

(o) Reconstructed Secret image3

Fig. 4: Experimental Simulation Results of (3, 3) Multiple Secret Images Sharing Scheme for Color Images

The experimental simulation results of (3, 3) multiple secret images sharing scheme for color images 'Airplane', 'Baboon' and 'Desert' shown in Fig. 4(a)-(c). Each color image has size 512 × 512 × 3. The three random images with same size as original secret images are shown in Fig. 4(d)-(f). The distinct random images, shown in Fig. 4(g)-(i), are generated by circular shifting the random image pixels. Fig. 4(j)-(l) shows the generated random share images. Fig. 4(m)-(o) shows the reconstructed secret images. The XOR operations are used in the proposed scheme to enhance visual quality (contrast) of reconstructed secret images and circular shifting of pixels to enhance security.

The quality evaluation parameters for Fig. 1(g) and Fig. 2(i) are shown in Table 1. The PSNR of reconstructed secret images has infinite values. The correlation and MSSIM of reconstructed secret images are 1. These parameters represent the perfect similarity between original and reconstructed secret images. Hence, the quality parameters confirm that the reconstructed secret images are lossless and have better contrast.

Table 1: Quality Metrics of Reconstructed Secret Image shown in Fig. 1 and Fig. 2

Quality metric	Reconstructed gray-scale secret image (Fig. 1(g))	Reconstructed color secret image (Fig. 2(i))
Correlation	1	1
PSNR	Infinite	Infinite
MSSIM	1	1

The quality evaluation parameters of reconstructed images in Fig. 3 and Fig. 4 are shown in Table 2 and Table 3 respectively. The values of correlation, PSNR and MSSIM of reconstructed secret images by using proposed scheme are one, infinite and one respectively which indicates the lossless reconstruction of the secret images.

Table 2: Quality Metrics of the Reconstructed Secret Images shown in Fig. 3

Quality metric	Reconstructed secret image1	Reconstructed secret image2	Reconstructed secret image3	Reconstructed secret image4
Correlation	1	1	1	1
PSNR	Infinite	Infinite	Infinite	Infinite
MSSIM	1	1	1	1

Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

Table 3: Quality Metrics of the Reconstructed Secret Images shown in Fig. 4

Quality metric	Reconstructed secret image1	Reconstructed secret image2	Reconstructed secret image3
Correlation	1	1	1
PSNR	Infinite	Infinite	Infinite
MSSIM	1	1	1

Table 4: Comparison of Proposed *(n, n)* Schemes with other related Secret Sharing Schemes

Parameter	M. Naor and A. Shamir [1]	A. Shamir [2]	C.C. Thien and J.C. Lin [3]	S.J. Shyu [4]	Y. K. Meghrajani and H.S. Mazumdar [19]	Proposed Schemes
Pixel expansion	Yes	No	No	No	No	No
Basis matrices	Yes	No	No	No	No	No
Codebook design	Yes	No	No	No	No	No
Additional storage space for share images	Required	Not required	Not required	Not required	Not required	Not required
Additional bandwidth for transmission of share images	Required	Not required	Not required	Not required	Not required	Not required
Secret sharing scheme	*(k, n)*	*(k, n)*	*(k, n)*	*(k, n)*	*(n, n)*	*(n, n)*
Randomness	Low	Average	Average	Average	Average	High
Image type	Binary	Gray-scale	Gray-scale	Gray-scale	Gray-scale	Gray-scale and Color
Encoding strategy	Visual cryptography	Polynomial interpolation	Polynomial interpolation	Random grid	Circular shift and Boolean XOR	Circular shift and Boolean XOR
Recovery strategy	Stacking	Stacking	Stacking	Stacking	Boolean XOR	Boolean XOR
Secret recovery	Lossy	Lossy	Lossy	Lossy	Lossless	Lossless
Computational time complexity	Large	Large	Large	Average	Less	Less
Contrast	Poor	Poor	Poor	Average	Average	Good
Security	Less	Average	Average	Average	Moderate	Strong
Alignment problems	Exists	Exists	Exists	Exists	Not exists	Not exists

Table 4 shows the comparison of proposed *(n, n)* secret image sharing schemes with existing schemes. The proposed methods do not require any pixel expansion, code book design and basis matrices for generation of share images. The sizes of share images and reconstructed image are same as the size of the original secret image. Hence, the additional storage space and bandwidth are not required in the proposed scheme. Also, the proposed schemes are suitable for gray-scale and color secret images. The encoding and decoding of the secret image involves Boolean XOR operations and indicates that the computational complexity is very less. The reconstructed secret image is lossless as compared to other secret sharing schemes. The security of the secret image is strong with the proposed schemes because share images do not give any information about the secret image individually due to their high randomness. The contrast and security of the proposed schemes are improved compared to other related schemes. The alignment problems of share images during recovery of the secret image do not exist in the proposed schemes.

Conclusion

Two novel *(n, n)* secret image sharing schemes for sharing of single and multiple secret images are introduced in this paper. The proposed schemes use Boolean XOR and circular shift operations during generation of share images. The secret images are reconstructed by using all share images with minimum computations at the receiver side. The proposed schemes have the advantages of no codebook design, no basis matrices requirement and no pixel expansion. Experimental results indicate that the security and contrast of the recovered secret images are improved in the proposed algorithms. The proposed multiple secret images sharing scheme may further extended to different sized multiple images.

References

[1] M. Naor, A. Shamir. Visual Cryptography. Advances in Cryptology (EUROCRYPTO '94), (Lecture Notes in Computer Science), Vol: 950, A. De Santis, Ed. Berlin, Germany: Springer-Verlag; 1995. p. 1-12.

[2] Adi Shamir, "How to share a secret," *Communication of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[3] Chih-Ching Thien and Ja-Chen Lin, "Secret image sharing," *Computers & Graphics*, vol. 26, pp. 765-770, 2002.

[4] Shyong Jian Shyu, "Image encryption by random grids," *Pattern Recognition*, vol. 40, no. 3, pp. 1014-1031, 2007.

[5] Daoshun Wang, Lei Zhang, Ning Ma and Xiaobo Li, "Two secret sharing schemes based on Boolean operations," *Pattern Recognition*, vol. 40, no. 10, pp. 2776–2785, 2007.

[6] S.J. Shyu, H.W. Jiang. Efficient construction for region incrementing visual cryptography. IEEE Transactions on Circuits and Systems for Video Technology. Vol: 22, No. 5; May 2012. p. 769-777.

[7] X. Wang, Q. Pei, H. Li. A Lossless Tagged Visual Cryptography Scheme. IEEE Signal Processing Letters. Vol: 21, No.: 7; July 2014. p. 853-856

[8] Y.C. Hou, Z.Y. Quan. Progressive visual cryptography with unexpanded shares. IEEE Transactions on Circuits and Systems for Video Technology. Vol: 21, No.: 11; November 2011. p. 1760-1764.

[9] Sachin Kumar and Rajendra K. Sharma, "Threshold visual secret sharing based on Boolean operations," *Security and Communication Networks*, vol. 7, pp. 653-664, 2014.

[10] Xiaotian Wu and Wei Sun, "Extended capabilities for XOR-based visual cryptography," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 10, October, 2014.

[11] Amitava Nag, Sushanta Biswas, Debasree Sarkar and Partha Pratim Sarka, "Secret image sharing scheme based on a Boolean operation," *Cybernetics and Information Technologies*, vol. 14, no. 2, pp. 98-113, 2014.

[12] Shih-Chieh Wei, Young-Chang Hou and, Yen-Chun Lu, "A technique for sharing a digital image," *Computer Standards & Interfaces*, vol. 40, pp. 53–61, 2015.

[13] Priyanka Singh, Balasubramanian Raman, and Manoj Misra, "A (n, n) Threshold Non-expansible XOR based Visual Cryptography with Unique Meaningful Shares," *Signal Processing,* vol. 142, pp. 301–319, January 2018.

[14] Zhou Wang*,* Alan Conrad Bovik*,* Hamid Rahim Sheikh*, and* Eero P. Simoncelli, "Image Quality Assessment: From Error Visibility to Structural Similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600-612, April 2004.

[15] Feng Jiang and Brian King, "A novel quality assessment for visual secret sharing schemes," *EURASIP Journal on Information Security*, no. 1, pp. 1-15, 2017.

[16] Wen-Pinn Fang and Ja-Chen Lin, "Universal share for the sharing of multiple images," *Journal of the Chinese Institute of Engineers,* vol. 30, no. 4, pp. 753-757, 2007.

[17] Ching-Nung Yang, Cheng-Hua Chen and Song-Ruei Cai, "Enhanced Boolean-based multi secret image sharing scheme," *The Journal of Systems and Software*, vol. 116, pp. 22-34, 2016.

[18] Chien-Chang Chen and Wei-Jie Wu, "A Secure Boolean-based multi-secret image sharing scheme," *The Journal of Systems and Software*, no. 92, pp. 107–114, 2014.

[19] Yogesh K. Meghrajani and Himanshu S. Mazumdar*, "*Universal Share for Multisecret Image Sharing Scheme Based on Boolean Operation," *IEEE Signal Processing Letters*, vol. 23, no. 10, pp. 1429-1433, October, 2016.