DOI 10.29042/2018-3588- 3592

Helix Vol. 8(5): 3588- 3592

XOR Based Secret Image Sharing Scheme with Security Improvement

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

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

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

*E-mail: [*1] ratnamjvklakshmi@yahoo.co.in, [2] mettu86@yahoo.co.in, [3] prrjntu@gmail.com*

Received: 19th June 2018, Accepted: 10th July 2018, Published: 31st August 2018

Abstract

A new *(k, n)* natural secret image sharing scheme based on Boolean XOR operation to improve the secret image security is presented in this research paper. A natural secret image is encrypted into *n* meaningless noise-like shares by using a random image of same size as original secret, Boolean XOR operations and circular shifting operations. A distinct identifier is used for each share image by swapping bits of a random number during encoding stage. These share images are transmitted over communication channel. The secret image is reconstructed at the receiving end by using at least *k* or more number of share images with little computations of Boolean XOR operations and circular shifting operations. The proposed scheme is suitable to gray-scale and color images. The experimental results and comparisons give feasibility and consistency of proposed scheme.

Keywords: Boolean XOR Operation; Circular Shift; Contrast; Security; Secret Image Sharing

Introduction

The increase in usage of multimedia data over internet communication may lead security problems in transmitting and storing of certain image data. Cryptographic schemes are required to secure valuable data from hackers. Secret image sharing scheme is one of the cryptographic scheme which is used to secure natural images as well as computer generated art works. Traditional cryptographic techniques have disadvantages such as requirement of an algorithm and remembering some part of the secret while decrypting the secret. The secret image sharing (SIS) schemes does not have these disadvantages. Naor and Shamir [1] introduced the concept of visual cryptography in which secret image is divided into *n* pieces known as share images or shadow images, and minimum *k* number of shares are collected and simply stacked together at the receiving end for reconstruction of the secret image by human visual system in the SIS scheme. The reconstruction process does not require any algorithm or computations to recover the original secret. Hence the number of computations required is drastically reduced in visual cryptography schemes compared to traditional cryptography schemes. The two categories of visual secret sharing schemes are polynomial based secret image sharing scheme (PSIS) and visual cryptography scheme (VCS).

Different VCS schemes in the secret image sharing have been proposed by researchers are random grid based scheme [2], Shamir-Lagrange technique [3, 4], Blakley geometry [5], Chinese Remainder Theorem [6], cellular automata [7], combinational theory [8], essential sharing [9], color image sharing [10], region incrementing [11], progressive visual cryptography [12] and tagged visual cryptography [13]. The poor visual quality is inevitable in classical secret image sharing schemes due to superimposing or stacking of share images. Logical OR operation is the underlying operation in these methods. The low contrast in the reconstructed secret image is observed in these schemes due to logical OR operation in the stacking of share images.

Boolean XOR based SIS schemes enhance the contrast of the recovered secret image compared to earlier suggested methods. Boolean Exclusive-OR (XOR) operation is used in Boolean based secret image sharing schemes and is a bit-wise operation. The contrast of the XOR based secret scheme is improved 2^{k-1} times by comparing with OR based visual cryptography schemes [14]. The computational complexity is very less in Boolean bit-wise operations and is less cost effective. Various schemes [15-20] in Boolean based secret image sharing have been proposed to solve problems related to contrast in recovered secret and alignment of share images during reconstruction process. There is a scope to devise a scheme for improvement in security of the secret image.

A new Boolean XOR based *(k, n)* secret image sharing scheme is introduced in this paper. The proposed technique have merits like no pixel expansion, no need to design codebook during encryption process, no Basis matrices required for generation of share images, wide image format and no alignment problems of share images during reconstruction stage of the secret image.

The rest of the paper is organized as follows. Section II reviews the related work with discussion. The Section III introduces the proposed secret image sharing scheme. The experimental results with corresponding discussions of the proposed scheme and comparison with related schemes is presented in Section IV and conclusion and further research work is provided in Section V.

Related Work

The secret image sharing schemes [14-20] using Boolean operations concentrate on computational complexity problem in the decoding phase of secret reconstruction and provide better contrast in the recovered secret image. The pixel expansion is not involved in the generation of share images in these schemes. The decoding phase requires less number of computations because Boolean XOR operations are required to reconstruct the secret. The alignment problems during reconstruction process is eliminated and the contrast of the reconstructed secret is improved by using Boolean operation based secret image sharing schemes.

Proposed Scheme

In this section, a new Boolean XOR based natural secret image sharing scheme is proposed for gray-scale and color secret images with improved security. Boolean bit-wise Exclusive-OR and circular right shift operations are used for generation of share images. The algorithm 1 gives the generation of share images. A random image is generated having same size of the original secret image. Boolean XOR operation is performed between the secret image and the generated random image. A distinct random identifier x_i is generated for each share image by using a distinct random number through swapping of four most significant bits and four least significant bits. The share images, S_i $(1 \leq i \leq n)$, are obtained by applying circular right shift of resultant XORed image by number of bit positions specified by the identifier. These generated share images are observed to be noise-like meaningless images. Hence these shares never leak any secret information about the secret.

Algorithm 2 gives the reconstruction of the original secret image. The original secret image is reconstructed by using at least k $(k \leq n)$ share images during recovery stage of the secret. The shares S_i $(2 \leq i \leq k)$ are circular left shifted by respective identifier x_i and combined together. The result is bit-wise Boolean XORed with the random image provided by the dealer for recovery of the secret I_1.

An algorithm for generation of n share images is as follows.

Algorithm 1: Share Image Generation

Input: Original Secret image, I
Output: n share images $\{S_1, S_2, S_3, \ldots, S_n\}$
Step 1: Generation of random image

$$R = random(255)$$

Step 2: Combining this random image with secret image

$$C = R \oplus I$$

where, $\oplus$ denotes bit-wise Boolean XOR operation.
Step 3: Dividing C by k
$G = C / k$, where, k is the minimum number of shares for reconstruction of secret and $k \leq n$.
Step 4: Generation of n number of random numbers
$r_i = random\ (255),\ for\ i = 1\ to\ n$
Step 5: Generation of n identifiers
$x_i = [4\text{-}bitLSB(r_i)\ 4bit(MSB(r_i)],\ for\ i = 1\ to\ n$
Step 6: Generation of n share images
$S_i = circularrightshift(G, x_i),\ for\ i = 1\ to\ n$

An algorithm for recovery of the secret image is as follows.

Algorithm 2: Secret image reconstruction
Input: n share images $\{S_1, S_2, S_3, \ldots, S_n\}$
Output: Reconstructed secret image, I_1
Step 1: Combining k share images
$Y = 0$
$Y = Y + circularleftshift(S_i, x_i)\ ,\ for\ i = 1\ to\ n$
Step 2: Reconstruction of secret image

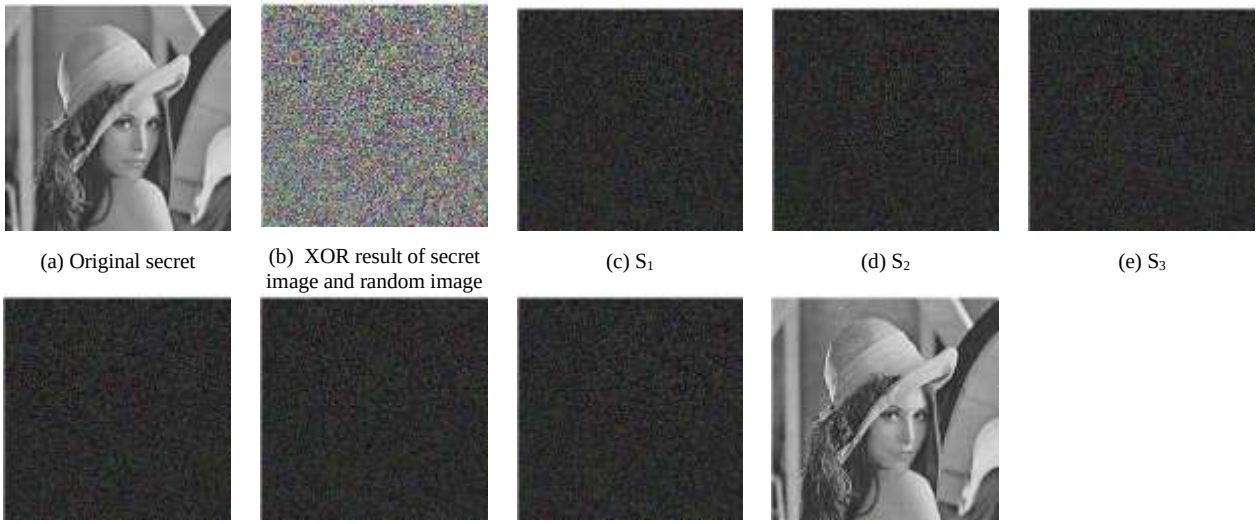
$$I_1 = Y \oplus C$$

The generation of meaningless share images using distinct identifier by swapping bits of distinct random number for each share and using circular shift operations in the algorithm is the novelty in the proposed technique which further improves security of the original image from attacks.

Experimental Results & Discussions

In this section, experimental results, respective discussions and comparison demonstrates consistency and feasibility of the proposed technique. All experiments are performed using MATLAB 8.3.0.532 with an Intel i3-4000M CPU and 4 GB RAM.

Fig. 1 illustrates the experimental results of (3, 6) secret sharing scheme for 256 × 256 size lena gray-scale image. Fig. 1(a) shows original secret image. A random image of size same as original image, i.e., 256 × 256, is generated and bit-wise Boolean XOR operation is applied to original image and random image. Fig. 1(b) shows the resultant image. The generated six share images are shown in Fig. 1(c)-1(h). These generated share images are observed to be random and unable to leak the original secret image information in any manner. The recovered secret image is shown in Fig. 1(i). The security and contrast



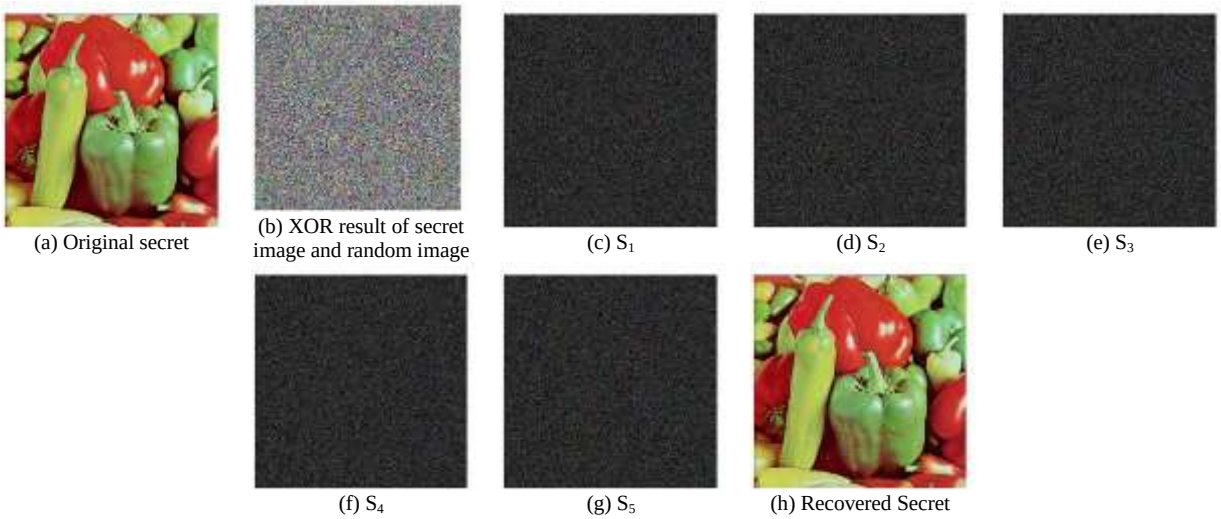
(a) Original secret (b) XOR result of secret image and random image (c) S_1 (d) S_2 (e) S_3

(f) S_4 (g) S_5 (h) S_6 (i) Recovered Secret

Fig. 1. (3, 6) Secret Image Sharing Scheme for 256 × 256 Gray-Scale Lena Image

of the proposed scheme is observed to be improved in this proposed scheme.

Fig. 2 illustrates experimental results of (3, 5) secret sharing scheme for 256 × 256 size peppers color image. The original secret image is shown in Fig. 1(a). A random image of size 256 × 256 is generated and bit-wise Boolean XOR operation is applied to original image and random image. The resultant XORed image is shown in Fig. 2(b). The generated five share images shown in Fig. 2(c)-2(g) are observed to be random and unable to leak the original secret image information. Hence the original secret image security is improved in the proposed scheme. The secret image is revealed by stacking or superimposing any three or more share images. The reconstructed secret image is shown in Fig. 2(h). The contrast of this recovered image is more correlated with original secret. Hence the visual quality of this recovered secret is improved in the proposed technique.



(a) Original secret (b) XOR result of secret image and random image (c) S_1 (d) S_2 (e) S_3

(f) S_4 (g) S_5 (h) Recovered Secret

Fig. 2. (3, 5) Secret Image Sharing Scheme for 256 × 256 Color Peppers Image

Parameter	M. Naor and A. Shamir [1]	S.J. Shyu [2]	C.C. Thien and J.C. Lin [3]	D. Wang, L. Zhang, N. Ma, X. Li [15]	M. Ulutas, V.V. Nabiyev, G. Ulutas and A. Shamir [16]	S. Kumar and R.K. Sharma [18]	J.V.K. Ratnam, P. R. Reddy and T.S. Reddy [19]	Proposed scheme
Pixel expansion	Yes	No	No	No	No	No	No	No
Codebook design	Yes	No	No	No	No	No	No	No
Basis matrices	Yes	No	No	No	No	No	No	No
Image type	Binary	Gray-scale	Gray-scale	Gray-scale	Gray-scale	Color	Gray-scale	Gray-scale and color
Secret sharing scheme	*(k, n)*	*(k, n)*	*(k, n)*	*(n, n+1)*	*(2, n)*	*(k, n)*	*(k, n)*	*(k, n)*
Randomness	Low	Average	Average	Average	Average	Average	High	High
Encoding strategy	Visual cryptography	Random grid	Polynomial	Boolean	Boolean	Boolean	Boolean XOR	Boolean XOR and circular shift
Recovery strategy	Stacking	Stacking	Stacking	Boolean XOR	Boolean XOR	Boolean XOR	Boolean XOR and circular shift	Boolean XOR and circular shift
Secret recovery	Lossy	Lossy	Lossy	Lossy	Lossy	Lossless	Lossless	Lossless
Contrast	Poor	Average	Poor	Average	Average	Good	Good	Good
Security	Low	Average	Average	Average	Average	Average	High	High

Table 1. Comparison of Proposed Scheme with Other Related Schemes

Table 1 shows the comparison of the proposed scheme with other related schemes in terms of pixel expansion, codebook design, basis matrices requirement, image type, secret sharing scheme, randomness, encoding strategy, recovery strategy, secret recovery and security. The proposed scheme requires any *k* or more number of shares to reconstruct the secret by Boolean XOR operations and circular shift operations. Hence there is an improvement in the security and visual quality of the secret with little computations in the recovery phase. The pixel expansion, basis matrices and codebook design are not necessary in the proposed scheme. Also, this scheme is suitable for gray-scale as well as color images.

Conclusion

A new *(k, n)* secret image sharing scheme based on Boolean XOR and circular shift operations is introduced in this paper. The original secret image is reconstructed by using at least *k* or more share images with little computational complexity. The proposed scheme is extended the concept of Boolean XOR operations and has 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 image are improved in the proposed algorithm. The proposed scheme is applicable to both gray-scale and color

secret images. This proposed scheme may further extended to 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] S.J. Shyu. Image encryption by multiple random grids. Pattern Recognition. Vol: 42; 2009. p. 1582–1596.

[3] C.C. Thien, J.C. Lin. Secret image sharing. Computer Graphics. Vol: 26, No: 5; 2002. p. 765-770.

[4] C.C. Chen, C.A. Liu. Tamper-proof secret image sharing scheme for identifying cheated secret keys and shared images. Journal of Electronic Imaging. Vol: 22; 2013.

[5] H.K. Tso. Sharing secret images using Blakley's concept. Optical Engineering. Vol. 47; 2008.

[6] R.Y.V. Subba and B. Chakravarthy. CRT based threshold multi secret sharing scheme. International Journal of Network Security. Vol: 16, No: 4; 2014. p. 249-255.

[7] X. Wu, D. Ou, Q. Liang, W. Sun. A user-friendly secret image sharing scheme with reversible steganography based on cellular automata. Journal of Systems and Software. Vol: 85; 2012. p. 1852–1863.

[8] Z. Liu, M.A. Ahmad, S. Liu. Image sharing scheme based on combination theory. Optical Communication. Vol: 281; 2008. p. 5322–5325.

[9] S.K. Chen. Essential secret image sharing with increasable shadows. Optical Engineering. Vol: 55; 2016.

[10] I. Kang, G.R. Arce, H.K. Lee. Color Extended Visual Cryptography using Error Diffusion. IEEE Transactions on Image Processing. Vol: 20, No.: 1; January 2011. p. 132-145,.

[11] 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.

[12] 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.

[13] 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

[14] C.N. Yang, D.S. Wang. Property Analysis of XOR-Based Visual Cryptography. IEEE Transactions on Circuits and Systems for Video Technology. Vol: 24, No.: 2; February 2014. p. 189-197.

[15] D. Wang, L. Zhang, N. Ma, X. Li. Two secret sharing schemes based on Boolean operations. Pattern Recognition. Vol: 40; 2007. p. 2776–2785.

[16] M. Ulutas, V.V. Nabiyev, G. Ulutas, A. Shamir. A PVSS scheme based on Boolean operations with improved contrast. Proceedings of International Conference on Network and Service Security. IEEE Computer Society Paris. 2009. p. 1-5.

[17] K.Y. Chao, J.C. Lin. Secret image sharing: a Boolean operations based approach combining benefits of polynomial-based and fast approaches. International Journal of Pattern Recognition and Artificial Intelligence. Vol: 23; 2009. p. 263-285.

[18] S. Kumar, R. K. Sharma. Threshold visual secret sharing based on Boolean operations. Security and Communication Networks, 2013. DOI:10.1002/sec.769.

[19] Javvaji V.K. Ratnam, P. Ramana Reddy and T. Sreenivasulu Reddy, "Design of high secure visual secret sharing scheme for gray scale images," IEEE International Conference on Wireless Communications, Signal Processing and Networking 2017 (IEEE WiSPNET 2017), pp. 145–148, March, 2017.

[20] Javvaji V.K. Ratnam, T. Sreenivasulu Reddy, P. Ramana Reddy. Design and performance evaluation of Boolean based secret image sharing scheme. International Journal of Applied Engineering Research. Vol: 13, No. 4; 2018. p. 1827–1832.

