



A NEW SECURITY IMPROVED BOOLEAN XOR OPERATION BASED NATURAL SECRET IMAGE SHARING SCHEME

Javvaji V.K. Ratnam¹, T. Sreenivasulu Reddy²

P. Ramana Reddy³

Research Scholar in JNTUA¹,

Department of Electronics

and Communication Engineering^{1,2,3},

Narasaraopeta Engineering College¹,

Narasaraopet, Andhra Pradesh, India

ratnamjvklakshmi@yahoo.co.in

Sri Venkateswara University²

Tirupati, Andhra Pradesh, India

mettu86@yahoo.co.in²

Jawaharlal Nehru Technological University³

Anantapur, Ananthapuramu, Andhra Pradesh, India

prjntu@gmail.com³

June 20, 2018

Abstract

A new (k, n) natural secret image sharing scheme based on Boolean XOR operation to improve the security of the secret image is presented in this paper. A natural secret image is encoded into n meaningless noise-like share images by using a random image of same size as original secret, simple Boolean XOR and circular shift 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 and circular shift operations. The proposed scheme is suitable to gray-scale and color images. The experimental results and comparison with other related schemes gives the feasibility and consistency of proposed scheme.

Keywords: Boolean XOR operation; Circular shift; Contrast; Security; Secret image sharing

1 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 number of 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 image. Hence the computational complexity is drastically reduced in visual cryptography schemes compared to traditional cryptography schemes. The two major categories of secret image sharing schemes are polynomial based secret image sharing scheme (PSIS) and visual cryptography scheme (VCS).

Different VCS schemes in secret image sharing have been proposed by researchers are random grid based visual secret

sharing 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 visual quality of the reconstructed 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 visual quality of the XOR based secret scheme is improved $2k-1$ 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 to improve 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.

2 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 reconstructed secret image. There is no pixel expansion 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 image is improved further by using Boolean operation based secret image sharing schemes.

3 PROPOSED SCHEME

In this section, a new Boolean XOR based natural secret image sharing scheme is proposed for gray-scale as well as 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. The secret image is Boolean XORed with a random image of size same as that of the original secret image. A distinct random identifier x_i is generated by swapping four least significant bits and four most significant bits of a random number. The share images, $S_i(1 < i < n)$, are generated by applying circular right shift of the 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 secret image. The secret is reconstructed by using at least k ($k \leq n$) share images during recovery stage of the secret. The shares $S_i(2 < i < n)$ 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 given below.

Algorithm 1: Generation of share images

Input: Secret image, I

Output: n share images $S_1, S_2, S_3, \dots, S_n$

Step 1: Generation of random image

$$R = \text{random}(255)$$

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 required for reconstruction of the secret and $k \leq n$.

Step 4: Generation of n number of random numbers

$$r_i = \text{random}(255), \text{ for } i = 1 \text{ to } n$$

Step 5: Generation of n identifiers

$$x_i = [4\text{bit}LSB(r_i).4\text{bit}(MSB(r_i))] , \text{ for } i = 1 \text{ to } n$$

Step 6: Generation of n share images

$$S_i = \text{circularrightshift}(G, x_i), \text{ for } i = 1 \text{ to } n$$

An algorithm for reconstruction of the secret image is given below.

Algorithm 2: Reconstruction of secret image

Input: n share images $S_1, S_2, S_3, \dots, S_n$

Output: Reconstructed secret image, I1

Step 1: Combining k share images

$$Y = 0$$

$$Y = Y + \text{circularleftshift}(S_i, x_i) , \text{ for } i = 1 \text{ to } n$$

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 scheme which further improves the security of the original secret image from attacks.

4 EXPERIMENTAL RESULTS AND DISCUSSIONS

In this section, experimental results, respective discussions and comparison demonstrate the consistency and feasibility of the proposed scheme. 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. The resultant image is shown in Fig. 1(b). 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. The reconstructed secret image is shown in Fig. 1(i). The security and contrast of the proposed scheme is observed to be improved in this proposed scheme.

Fig. 2 illustrates the 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 256×256 size is generated and bit-wise Boolean XOR operation is applied to original image and random image. Fig. 2(b) shows the resultant XORed image. The generated five share images are shown in Fig. 2(c)-2(g). These share images are observed to be random and unable to leak the original secret image information. Hence the security of the secret image is improved in this proposed scheme. The secret image is reconstructed by stacking any three or more share images. The reconstructed secret image is shown in Fig. 2(h). The contrast of this reconstructed image is more correlated with the original secret image. Hence the visual quality of this reconstructed secret is improved in the proposed scheme.

Table 1 shows the comparison of the proposed scheme with

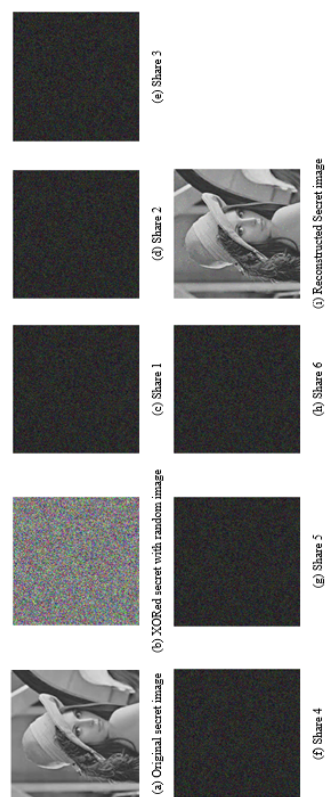


Figure 1: A (3, 6) Secret image sharing scheme for 256×256 gray-scale lena image

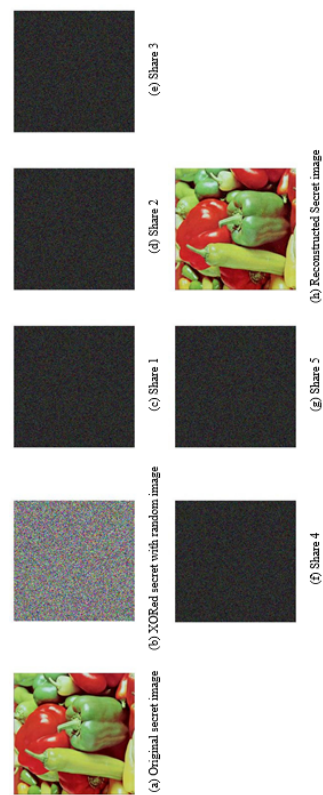


Figure 2: A (3, 5) Secret image sharing scheme for 256×256 color peppers image

Table 1. Comparison of proposed scheme with other related schemes

Parameter	M. Naei and A. Shamir [1]	S.J. Shyu [2]	C.C. Tsien and J.C. Lin [3]	D. Wang, L. Zhang, N. Ma, X. Li [15]	M. Uthair, V.V. Nahiye, G. Uthair and A. Shamir [16]	S. Kumar and R.K. Sharma [18]	J.V.K. Raman, P. K. 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
Basic 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	Boolean
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

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 share images to reconstruct the original secret image by Boolean XOR and circular shift operations. Hence there is an improvement in the visual quality and security of the secret image with little computations in the recovery phase. The pixel expansion, basis matrices and codebook design are not necessary in the proposed scheme. This scheme is suitable to gray-scale as well as color images.

5 CONCLUSION

A new (k, n) secret image sharing scheme based on Boolean XOR and circular shift operations is introduced in this paper. The 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 reconstructed secret image are improved in the proposed algorithm. The proposed scheme is applicable to both gray-scale and color secret images. The proposed scheme may further extended to multiple secret images.

References

- [1] M. Naor and A. Shamir, "Visual Cryptography", Advances in Cryptology (EUROCRYPTO 94), (Lecture Notes in Computer Science), vol. 950, A. De Santis, Ed. Berlin, Germany: Springer-Verlag, pp. 1-12, 1995.
- [2] S.J. Shyu, "Image encryption by multiple random grids", Pattern Recognition, vol. 42, pp. 1582-1596, 2009.
- [3] C.C. Thien and J.C. Lin, "Secret image sharing", Computer Graphics, vol. 26, no. 5, pp. 765-770, 2002.

- [4] C.C. Chen and 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 Blakleys concept", *Optical Engineering*, vol. 47, 2008.
- [6] R.Y.V. Subba and B. Chakraavathy, "CRT based threshold multi secret sharing scheme", *International Journal of Network Security*, vol. 16, no. 4, pp. 249-255, 2014.
- [7] X. Wu, D. Ou, Q. Liang and W. Sun, "A user-friendly secret image sharing scheme with reversible steganography based on cellular automata", *Journal of Systems and Software*, vol. 85, pp. 18521863, 2012.
- [8] Z. Liu, M.A. Ahmad and S. Liu, "Image sharing scheme based on combination theory", *Optical Communication*, vol. 281, pp. 53225325, 2008.
- [9] S.K. Chen, "Essential secret image sharing with increasable shadows", *Optical Engineering*, vol. 55, 2016.
- [10] I. Kang, G.R. Arce and H.K. Lee, "Color Extended Visual Cryptography using Error Diffusion", *IEEE Transactions on Image Processing*, vol. 20, no. 1, pp. 132-145, January 2011.
- [11] S.J. Shyu and H.W. Jiang, "Efficient construction for region incrementing visual cryptography", *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 22, no. 5, pp. 769-777, May 2012.
- [12] Y.C. Hou and Z.Y. Quan, "Progressive visual cryptography with unexpanded shares", *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 21, no. 11, pp. 1760-1764, November 2011.
- [13] X. Wang, Q. Pei and H. Li "A Lossless Tagged Visual Cryptography Scheme", *IEEE Signal Processing Letters*, vol. 21, no. 7, pp. 853-856, July 2014.

- [14] C.N. Yang and D.S. Wang, "Property Analysis of XOR-Based Visual Cryptography", IEEE Transactions on Circuits and Systems for Video Technology, vol. 24, No. 2, pp. 189-197, February 2014.
- [15] D. Wang, L. Zhang, N. Ma, X. Li, "Two secret sharing schemes based on Boolean operations", Pattern Recognition, vol. 40, pp. 27762785, 2007.
- [16] M. Ulutas, V.V. Nabyev, G. Ulutas and 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, pp. 1-5, 2009.
- [17] K.Y. Chao and 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, pp. 263-285, 2009.
- [18] S. Kumar and 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. 145148, March, 2017.
- [20] Javvaji V.K. Ratnam, T. Sreenivasulu Reddy and P. Ramana Reddy, "Design and performance evaluation of Boolean based secret image sharing scheme", International Journal of Applied Engineering Research, vol. 13, no. 4, pp. 18271832, 2018.

