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 Engineering¹,²,³,
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 xi 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 \( S_1, S_2, S_3, ..., S_n \)

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

Step 5: Generation of \( n \) identifiers
\( x_i = \lfloor 4 \text{bit} \text{LSB}(r_i) \rfloor \lfloor 4 \text{bit} \text{MSB}(r_i) \rfloor , \) for \( i = 1 \) to \( n \)

Step 6: Generation of \( n \) share images
\( S_i = \text{circular right shift}(G, x_i) \), for \( i = 1 \) to \( n \)

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

Algorithm 2: Reconstruction of secret image

Input: \( n \) share images \( S_1, S_2, S_3, ..., S_n \)

Output: Reconstructed secret image, \( I_1 \)

Step 1: Combining \( k \) share images

\[
Y = 0 \\
Y = Y + \text{circular left shift}(S_i, x_i) \text{ , for } i = 1 \text{ to } n
\]

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 $\times$ 256 gray-scale lena image.
Figure 2: A (3, 5) Secret image sharing scheme for $256 \times 256$ color peppers image
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Pixel expansion</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Codebook design</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Basic matrices</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Image type</td>
<td>Binary</td>
<td>Gray-scale</td>
<td>Gray-scale</td>
<td>Gray-scale</td>
<td>Gray-scale</td>
<td>Gray-scale</td>
<td>Gray-scale and color</td>
<td></td>
</tr>
<tr>
<td>Secret sharing scheme</td>
<td>$k_e$</td>
<td>$(k, e)$</td>
<td>$(k, e)$</td>
<td>$(k, e)$</td>
<td>$(k, e)$</td>
<td>$(k, e)$</td>
<td>$(k, e)$</td>
<td>$(k, e)$</td>
</tr>
<tr>
<td>Randomness</td>
<td>Low</td>
<td>Average</td>
<td>Average</td>
<td>Average</td>
<td>Average</td>
<td>Average</td>
<td>Average</td>
<td>High</td>
</tr>
<tr>
<td>Encoding strategy</td>
<td>Visual cryptography</td>
<td>Random grid</td>
<td>Polynomial</td>
<td>Boolean</td>
<td>Boolean</td>
<td>Boolean</td>
<td>Boolean</td>
<td>Boolean</td>
</tr>
<tr>
<td>None-way strategy</td>
<td>Stacking</td>
<td>Stacking</td>
<td>Stacking</td>
<td>Boolean XOR</td>
<td>Boolean XOR</td>
<td>Boolean XOR</td>
<td>Boolean XOR and circular shift</td>
<td>Boolean XOR</td>
</tr>
<tr>
<td>Secret recovery</td>
<td>Lower</td>
<td>Lower</td>
<td>Lower</td>
<td>Lower</td>
<td>Lower</td>
<td>Lower</td>
<td>Lower</td>
<td>Lower</td>
</tr>
<tr>
<td>Contrast</td>
<td>Poor</td>
<td>Average</td>
<td>Poor</td>
<td>Average</td>
<td>Average</td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td>Security</td>
<td>Low</td>
<td>Average</td>
<td>Average</td>
<td>Average</td>
<td>Average</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>
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


