International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Enhanced Multi Secret Image Sharing Scheme for Gray and RGB Images

Amit Patel

Department of Computer Science and Engineering, RGUKT, Mylavaram road, Nuzvid 521202, India

Abstract: ***In this paper we proposed a Multi Secret Image Sharing scheme, multi secret image sharing means making multiple shares with multiple secrets such that each share contains the information of all secrets. The proposed algorithm improves the randomness of shares and takes less computation time than the existing one proposed by Chien-Chang Chen and Wei-Jie Wu. Our proposed algorithm uses bit reverse function along with XOR operation to generate shares and to reconstruct the secrets. Experimental results show that this algorithm takes less computation time so that it can be also performed on color images.***

Keywords: Boolean operations, multiple shares, Secret image sharing, Sharing color images, XOR operation**.**

1. Introduction

Security is the primary issue over the Internet as it is a global network. There are so many techniques evolved to preserve data from harmful programs and hackers. Secret sharing techniques protects data by converting them into shares and then reconstructing the secrets from those shares. In single secret sharing technique one secret is divided into k shares. In multi secret sharing technique n secrets are divided into k shares. This paper is all about a multi secret image sharing (MSIS) technique which creates n shares from n secrets.

1.1 Introduction about Images

Broadly images are of three types. Binary, Gray and RGB. Binary Image is a black and white image which contains only zeros and ones in each pixel where zero represents black and one represents white. Gray image contains values in between 0 to 255 in each pixel and those are called as gray levels. Every value corresponds to one gray level (gray shade). Each pixel of RGB Image contains three values namely (r,g,b) where $0 \leq r,g,b \leq 255$. Binary and Gray are two dimensional images and RGB is three dimensional image. So RGB Images takes more computation time than binary and gray. If we decrease the computational time of our algorithm then that can be performed on RGB also.

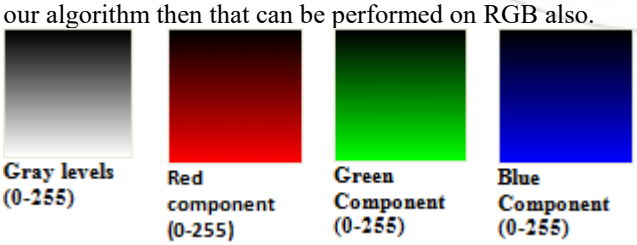


Figure 1: Components of color

Figure 2: Types of images

This paper is structured as follows. Apart from introduction, there are five more sections. Section 2 highlights the review of related works. In section 3 we have defined the problem and in section 4 we outlined implementation details related to the proposed algorithms along with the explanation. Section 5 discusses about the experimental result related to our proposed work and finally we concluded with section 6.

2. Related Work

Due to vast increase in data transmissions, there is a need of secure transmission. These secret image sharing techniques makes data more secure by converting them into shares. In initial days these techniques can be applied on only one image with multiple shares. But now it is extended to multiple images with multiple shares. There are so many algorithms existed but many of them are for single image with multiple shares. Some of them are multiple image with multiple shares but the number of shares are more than the number of image.

Chen and Wu (2011)[2] developed algorithm for multiple secret image sharing using XOR operations. The algorithm uses an extra random image to create shares. In this scheme there are n shared images for n-1 secret images. The algorithm of Chen and Wu secret image sharing scheme is described as follows:

Algorithm 1

1. Assume that $G_i(i = 1,\ldots,n-1)$ and R represent $n-1$ secret images and a random image, respectively.
2. Calculate $B_i = G_i \oplus R\ (i = 1,\ldots,n-1)$.
3. Use Eq. (1) to calculate shared images Si (1)

$$S_1 = B_1$$
$$S_i = B_{i-1} \oplus B_i \quad \text{for } 2 \leq i \leq n-1 \qquad (1)$$
$$S_n = B_{n-1} \oplus G_1$$

Chien-Chang Chen and Wei-Jie Wu[1] implemented Chen and Wu's algorithm by calculating random image from secret images only. But they used BitShift[1] function to calculate random image which takes more computation time. Hence that algorithm is not preferable to compute over RGB images.

Algorithm 2

Sharing Procedure:

1. Assume that G1, G2, . . ., Gndenote n secret images.
2. Use Eq. (2) to calculate a random image R
   $R = F(G_1, \cdots, G_{k-1}, G_k) = F_2(F_1(G_1, \cdots, G_{k-1}, G_k))$
   $= F_2(G_1 \oplus \cdots \oplus G_{k-1} \oplus G_k)$ (2)
   where k = 2 ·Lowerbound(n/2)
3. Acquire the noised secret image N_i by $N_i = G_i \oplus R$, where i = (1, 2,. . ., n).
4. Use below mentioned formula to calculate each shared image S_i from all N_i for participant i.
   $S_1 = N_1$ i=1
   $S_2 = N_2$ i=2
   $S_3 = N_3 \oplus N_2 \oplus N_1$ i=3
   $S_4 = N_4 \oplus N_3 \oplus N_2$ i=4
   …
   $S_n = N_n \oplus N_{n-1} \oplus N_{n-2}$ i=n

Algorithm 3
Recovery Procedure:

1. Use below mentioned formula to calculate each noised image N_i from all S_i for participant i.
   $N_1 = S_1$ i=1
   $N_2 = S_2$ i=2
   $N_3 = S_3 \oplus N_2 \oplus N_1$ i=3
   $N_4 = S_4 \oplus N_3 \oplus N_2$ i=4
   …
   $N_n = S_n \oplus N_{n-1} \oplus N_{n-2}$ i=n
2. Obtain the random image R from the noised secret images $N_1, N_2, \ldots, N_n$ by
   $R = F_2(N_1 \oplus N_1 \oplus \ldots \oplus N_k)$,
   where k = 2 ·Lowerbound(n/2)S
3. Recover all secret images G_i by
   $G_i = N_i \oplus R$.

In our proposed algorithm we have improved the algorithm given by Chien-Chang Chen and Wei-Jie Wu. We have improved the time taken to generate the shares and recover the shares, because the algorithm is taking less time so we can easily apply proposed algorithm on color images as well.

3. Problem Definition

Our proposed algorithm is used to implement a multiple secret image sharing technique with the proposed bit reverse function [8] which increases the randomness of the shares and color depth of images with less computation time. The MSIS technique [8] is defined to meet the following objectives.

- To make less computation time
- Increase the color depth
- Increase the randomness of image

In our proposed algorithm we are using bit reverse function. From the experiments we found that the bit reverse function takes less time as compare to bit shift function, and from the results obtained we have found that bit reverse gives more randomness to the image as compare to bit shift.

4. Proposed Algorithm and Implementation

The proposed scheme uses a random image generating function F to generate the required random image. First calculate the XOR results of images $R_1 = I_1 \oplus I_2 \oplus I_3 \oplus I_4 \oplus \ldots \oplus I_k$. Then R_2 is the bit reverse of R_1. The term R_2 is defined by bit reverse where last 4 bits will be interchanged by first 4 bits to each pixel G(x, y). The objectives of our proposed scheme are to make the algorithm to take less computation, increase the color depth and increase the randomness of the shares. The proposed sharing procedure is illustrated as follows:

4.1 To create shares

Algorithm 4

1. Let us assume $I_1, I_2, I_3, \ldots, I_n$ are input images of RGB Color
2. Calculate First Random Image
   $R_1 = I_1 \oplus I_2 \oplus I_3 \oplus I_4 \oplus \ldots \oplus I_k$ where k=n if n is even, k=n-1 otherwise
3. Calculate Second Random Image
   $R_2 = \text{BitReverse}(R_1)$
4. Calculate Noise images using below formula
   $N_i = I_i \oplus R_2$ ($1 \le i \le n$)
5. Now calculate shares using below formula
   $S_1 = N_1$
   $S_2 = N_2$
   $S_3 = N_3 \oplus N_2 \oplus N_1$
   $S_4 = N_4 \oplus N_3 \oplus N_2$
   …
   $S_n = N_n \oplus N_{n-1} \oplus N_{n-2}$

Fig 3 represents the flow diagram to generate shares from the images, initially we have taken n images and then XOR all images to get random images called R_1 and then apply bit reverse function on image R_1 to get the random image R_2 which will be used for generating the noised images by XORing the i^{th} input image and R_2 to get i^{th} noised image N_i. Then from noised image we will generate the shares by using equation given in the algorithm 4, and Fig 4 shows the experimental result of each step on a set of images.

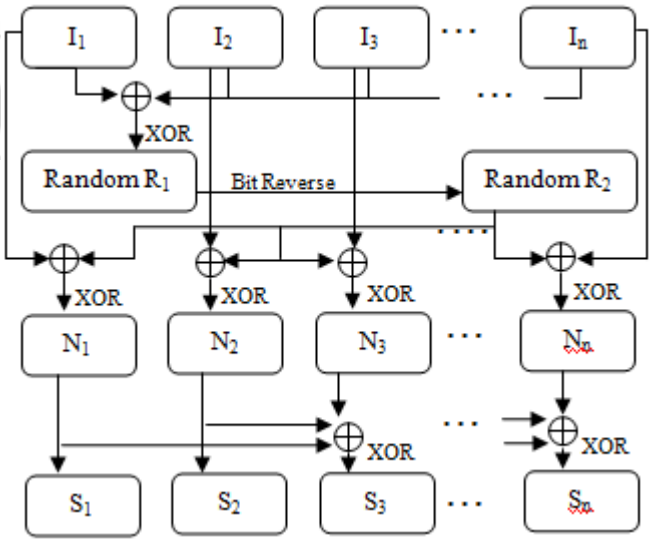


Figure 3: Diagram of procedure to generate the shares

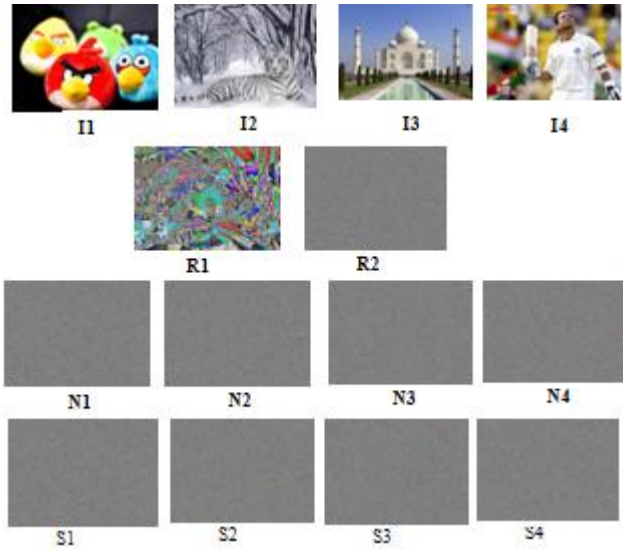


Figure 4: Diagram of flow of generating shares

S1, S2, S3, S4 are the Shares calculated from I1,I2 ,I3, I4 using proposed algorithm

4.2 To reconstruct the secrets

Algorithm 5

1. Let us assume $S_1, S_2, S_3, \ldots, S_n$ are n shares
2. Calculate Noise Images uing below formula
   $N_1 = S_1$
   $N_2 = S_2$
   $N_3 = S_3 \oplus N_2 \oplus N_1$
   $N_4 = S_4 \oplus N_3 \oplus N_2$
   …
   $N_n = S_n \oplus N_{n-1} \oplus N_{n-2}$
3. Calculate First Random Image
   $R_1 = N_1 \oplus N_2 \oplus N_3 \oplus \ldots \oplus N_k$ where k=n if n is even, k=n-1 otherwise
4. Calculate Second Random Image
   $R_2 = \text{BitReverse}(R_1)$
5. Now calculate Secrets using below formula
   $I_i = N_i \oplus R_2 \ (1 \leq i \leq n)$

Fig 5 represents the flow diagram to reconstruct the secrets from the shares, initially we take all n share and using the equation mentioned in algorithm 5 in line 2 recover all the noised images and then XOR all noised images to get random images called R_1 and then apply bit reverse function on image R_1 to get the random image R_2 which will be used for generating the secret images by XORing the i^{th} noised image and R_2 to get i^{th} secret image I_i. Fig 6 shows the experimental result of each step on a set of images.

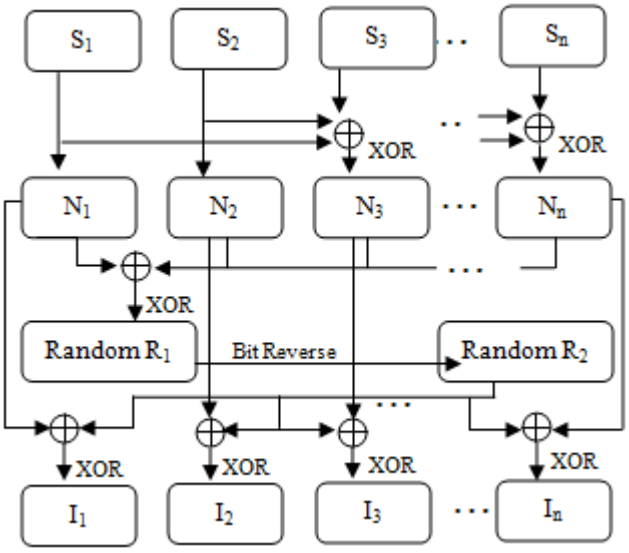


Figure 5: Diagram of procedure to reconstruct the secrets

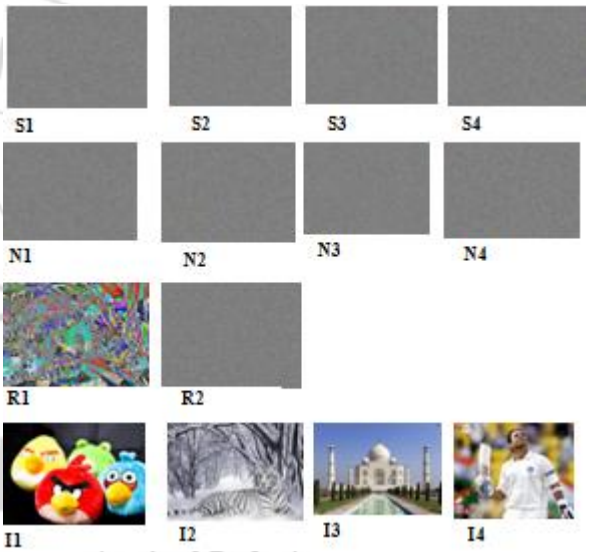


Figure 6: Diagram of flow of reconstructing secrets

I1, I2, I3, I4 are the secrets reconstructed using S1, S2, S3 and S4

4.3 BitReverse function

BitReverse function calculates binary reverse value of each pixel and replaces pixel value with that reversed value, for Example

If pixel value is 1 then binary of that is 0000 0001
Reverse(1) = 1000 0000 = 128

If pixel value is 2 then binary of that is 0000 0010
Reverse(2) = 0100 0000 = 64bles.

Fig 7 shows the result of bit shift and bit reverse on a gray image from the figure we can see that bit reverse provides more randomness to the as compared to bit shift function.

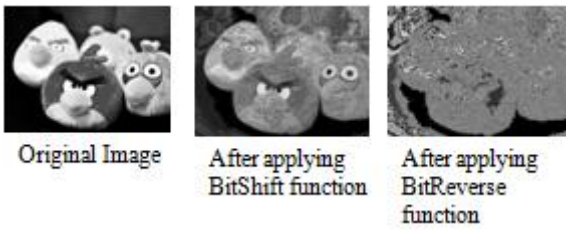


Figure 7: Comparison of Bit shift and bit reverse function Gray images

Fig 8 shows the result of bit shift and bit reverse on a color images from the figure we can see that bit reverse provides more randomness to the as compared to bit shift function.

Figure 8: Comparison of Bit shift and bit reverse function color images

5. Experimental Results

All the experimental results are performed on images of size 1024 x 768 on MATLAB R2012a on a laptop with Intel i3 processer and 4GB RAM. Table 1, Table 2 shows the comparison between Chien and Wu's algorithm and proposed algorithm for creating shares and reconstructing shares for gray images, from the tables we can infer that the proposed algorithm takes less computation time than previous algorithm. Table 3 shows the experimental results on RGB images

Table 1: Time comparison to create shares for Gray images

To create shares	*4 images*	*6 images*	*8 images*	*10 images*	*12 images*
Chien Chang Chen and Wei Jei Wu algorithm	0.695 sec	0.710 sec	0.7114 sec	0.735 sec	0.7441 sec
Proposed algorithm	0.078 sec	0.086 sec	0.094 sec	0.099 sec	0.109 sec

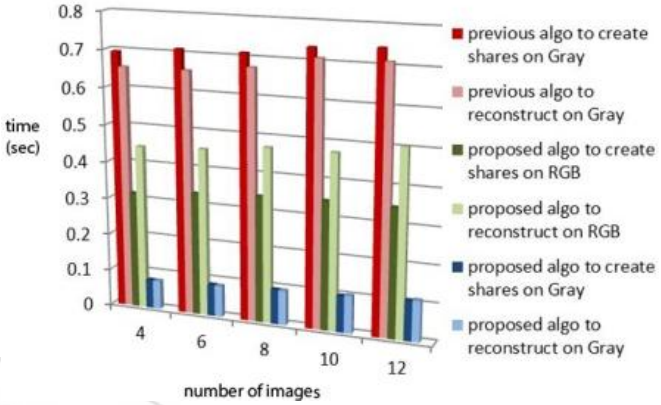
Table 2: Time comparison to reconstruct secrets for Gray images

To Reconstruct secrets	4 images	6 images	8 images	10 images	12 images
Chien Chang Chen and Wei Jei Wu algorithm	0.655 sec	0.656 sec	0.6755 sec	0.709 sec	0.7114 sec
Proposed algorithm	0.078 sec	0.085 sec	0.094 sec	0.102 sec	0.112 sec

Table 3: Results for creating shares and secrets for RGB images

RGB images	4 images	6 images	8 images	10 images	12 images
To create shares	0.316 sec	0.332 sec	0.3420 sec	0.347 sec	0.3480 sec
To reconstruct secrets	0.445 sec	0.453 sec	0.4722 sec	0.474 sec	0.5042 sec

Graph 1 shows the comparison between Chien and Wu's algorithm (previous algo in graph) and proposed algorithm for creating shares and reconstructing shares for Gray and RGB images. Table 4 shows the comparison between Chien and Wu's algorithm and proposed algorithm in terms of recovery type, color depth, function used and time taken to perform the function over one image.



Graph 1: Time comparison for algorithms

Table 4: Comparison in terms of function used and color depth

Name	Recovery type	Colour Depth	Function used	Time taken to perform the function (sec)
Chien-Chang and Wei-Jei Wu (2014)	Lossless	Gray	BitShift	0.6240
The proposed	Lossless	Gray	BitReverse	0.0197
The proposed	Lossless	RGB	BitReverse	0.1015

6. Conclusion

This paper presents the implementation of algorithm proposed by Chien Chang by changing BitShift function with BitReverse function. We have changed that function to increase the randomness of share and to decrease the computational time. The main aim of decreasing computational time is to make algorithm work for RGB images also. We done then experiments over color as well as gray images and results are shown in the previous section.

References

[1] Chen, Chien-Chang, and Wei-Jie Wu. "A secure Boolean-based multi-secret image sharing scheme." Journal of Systems and Software 92 (2014): 107-114.
[2] Chen, T.H, Wu, C.S., 2011. Efficient multi-secret image sharing based on Boolean operations. Singnal Processing 91, 90-97.
[3] Tapasi Bhattacharjee, Jyoti Prakash Singh, Amitava Nag: A Novel (2,n) Secret Image Sharing Scheme, SciVerse ScienceDirect, Procedia Technology 4 (2012) 619 – 623.
[4] Rishiwal, Vinay, and Ashutosh Gupta. "An Efficient Secret Image Sharing Scheme." International e-Conference on Computer Engineering (IeCCE 2012), 2011.

[5] M. Naor, A. Shamir, Visual cryptography, in: Proceedings of the Advances in Cryptology-Eurocrypt '94, Lecture Notes in Computer Science, vol. 950, 1995, pp. 1–12.
[6] Wang, Daoshun, et al. "Two secret sharing schemes based on Boolean operations." Pattern Recognition 40.10 (2007): 2776-2785.
[7] Shyu, Shyong Jian, et al. "Sharing multiple secrets in visual cryptography."Pattern Recognition 40.12 (2007): 3633-3651.
[8] Amit Patel, Kalpana Gangwar, Sai Sudha Melapu. "A Multi Secret Image Sharing Scheme for RGB Images," ICDSP Conference Bangalore 2015.

Author Profile

Amit Patel received the B.Tech degree in Computer Science from Dr. K N Modi Institute of Engineering and Technology in 2012 and M.Tech degree in Artificial Intelligence from School of Computer and Information Sciences, University of Hyderabad in 2014. Now he works as Lecturer in Department of Computer Science in Rajiv Gandhi University of knowledge Technologies Nuzvid.