New Secret Message Sharing Scheme using MSIS Scheme and LSB Algorithm

Amit Patel
Department of Computer Science and Engineering
Rajiv Gandhi University of Knowledge Technologies
Nuzvid, Krishna, India
amtptl93@gmail.com

Sai Sudha Melapu
Department of Computer Science and Engineering
Rajiv Gandhi University of Knowledge Technologies
Nuzvid, Krishna, India
sudhamelapu.au@gmail.com

Abstract— **This paper discuss about a more secure way of sharing the text data by hiding the text data in images by steganography and convert the image into random shares through Multi-Secret Image Sharing scheme. Multi-Secret Image Sharing (MSIS) scheme shares n secret images among n shared images. In this scheme, there are n shares generated from n secrets images and to recover all n secret image we need all n shared images, but if any shared image is lost that will stop the recovery of secret image. The New Secret Message Sharing scheme uses the LSB algorithm which is used to store the secret information in the images and the multi secret image sharing scheme proposed in [2]. From the experimental results it is also found that the proposed scheme provides more randomness to the shares which makes this scheme more secure.**

Keywords—Boolean function; Image sharing; Information sharing; Secret sharing; Steganography.

I. INTRODUCTION

Security has been the major concern over the Internet as it is a global network. There had been many techniques to protect data from intruders such as Cryptography and Steganography [9]. Cryptography is used for secure communication in the presence of third parties by encrypting the data [3]. Steganography ensures more security by hiding the data within other data (image/audio/video) so that no one suspects its existence [4].

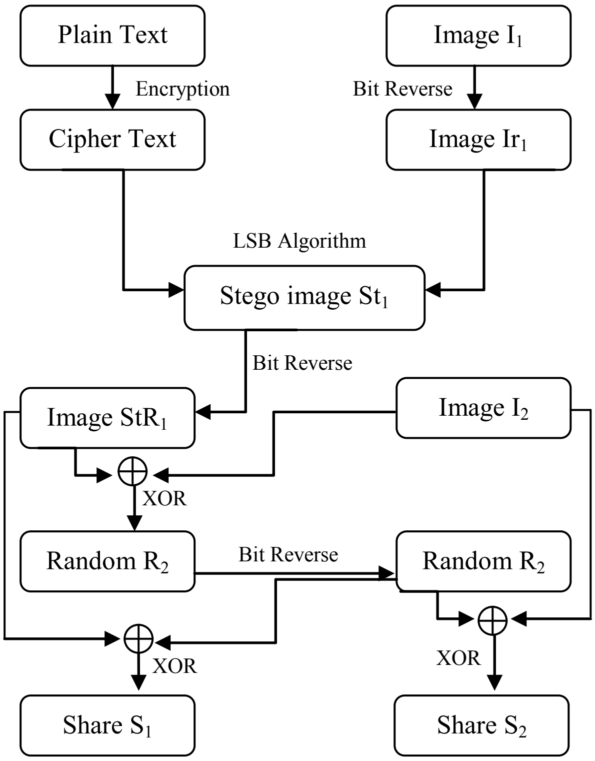
The proposed method uses multi secret image sharing scheme [7] on the stego file (generated by using LSB algorithm [5]) to make it more secure. Secret sharing scheme ensures security to the data by converting them into shares and then reconstructing the secrets from those shares. In Multi Secret Image Sharing scheme [1], multiple secrets are divided into multiple shares such that each share contains the information of all the secrets. In this paper, bit reverse function is included along with XOR operation to bring more randomness in the shares.

This paper is structured as follows. Apart from introduction, there are five more sections. In Section 2, we have explained our New Secret Message Sharing Scheme in detail. In Section 3 we have defined our proposed algorithms for creating shares and for regenerating secrets. Section 4 discusses about the experimental result related to our proposed work and finally we concluded with section 5.

II. NEW SECRET MESSAGE SHARING SCHEME

New Secret Message Sharing (NSMS) scheme is used to share the text data in such a way even if in between someone gets the shared image they cannot find the hidden message. To accomplish this, the two different algorithms, LSB algorithm [5] and Multi Secret Image Sharing scheme [2] are used. The NSMS scheme is consists of Share Generation phase and Message Recovery Phase.

A. Generation of Shares



(a)Generation of Shares

978-1-4673-6680-9/16/$31.00 ©2016 IEEE

As per the proposed method, bit reverse function is applied on the image I_1 which is used for hiding the text. On the resulted image Ir1, LSB technique [6] is applied to create a stego file St_1.On this stego file St_1, again bit reverse function is used to get a StR_1 file. MSIS technique is applied on the StR_1 along with the other Image I_2 for generating the shares.

Bit reverse function calculates the binary reverse value of each pixel and replaces each pixel value with the reverse value. If pixel value is 1 then its 8 bit representation is 00000001 and its bit reverse is represented as 10000000 which is equivalent to 128 in decimal format [2].

Reverse (1) = Reverse (00000001) = 128

Reverse (2) = Reverse (00000010) = 64

The entire procedure for Generation of Shares phase is elaborated in following steps.

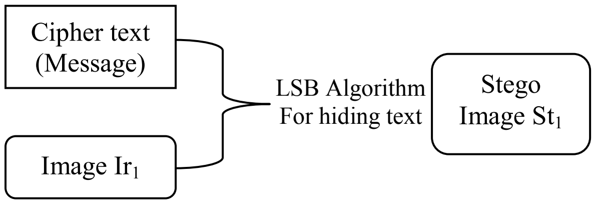
1) Cipher text: Convert the secret text message into cipher text by using encryption algorithm(step1 and step 2 of Create Share phase of the algorithm).

Plain text
Encryption
Cipher text

2) Noisy image(Ir_1): Take the image I_1 and apply bit reverse function to generate noisy image Ir_1, used for hiding the text message .

Image I1
Bit Reverse
Image Ir1

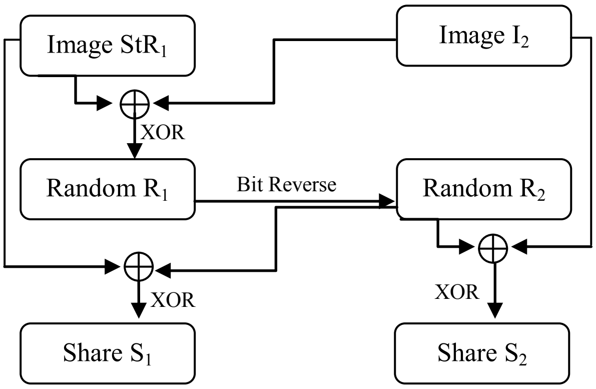
3) Hiding the Cipher text inside the image : Apply LSB algorithm [3] to hide the cipher text inside the bit reversed image Ir_1 .



4) Generating bit reversed Stego Image(StR_1): Take image St_1 and apply bit reverse function to get StR_1.

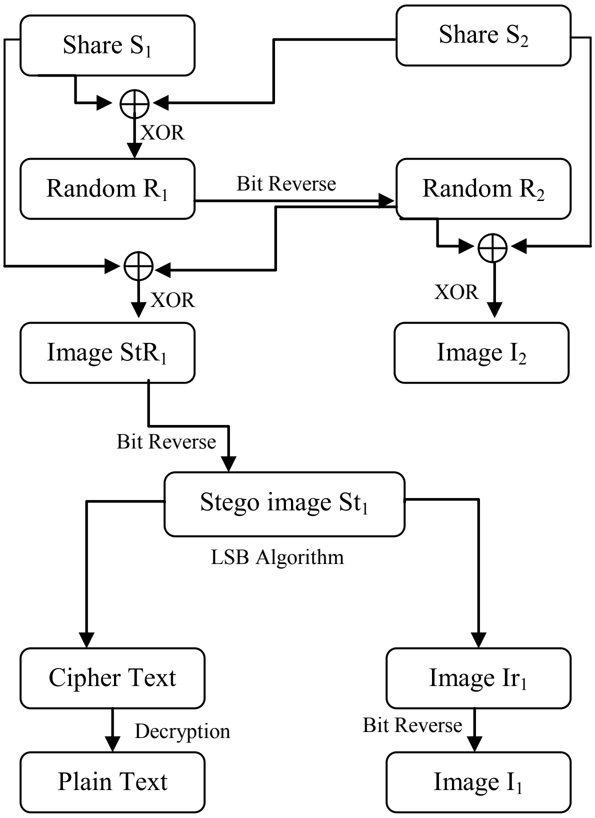
Stego Image St1
Bit Reverse
Image StR1

*5) Multi Secret Image Sharing Technique :*It includes several steps to generate the shares.Initially random image R_1 is generated by applying Exclusive OR in between Image StR_1 and Image I_2. Random image R_1 is bit reversed [2] to generate another random image R_2 which is XORed with image StR_1 to get Share S_1. Share S_2 is generated by performing XOR between image I_2 and random image R_2 [1].



Now these shares will be sent to the receiver. At the receiver side, apply the message recovery phase of the algorithm to get the original text message.

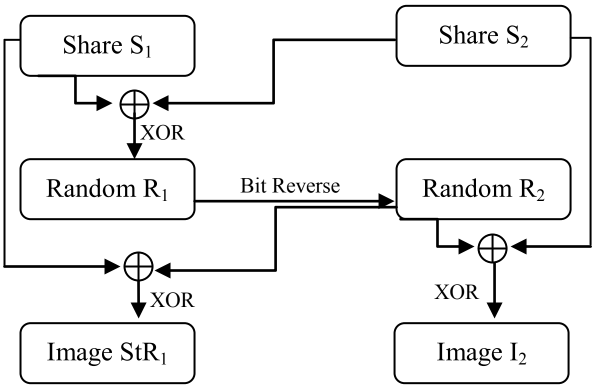
B. Message Recovery



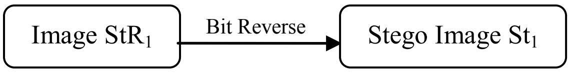
(b) Message recovery

In Message Recovery Phase, combination of LSB and MSIS scheme is applied at the receiver side. It is elaborated in following steps.

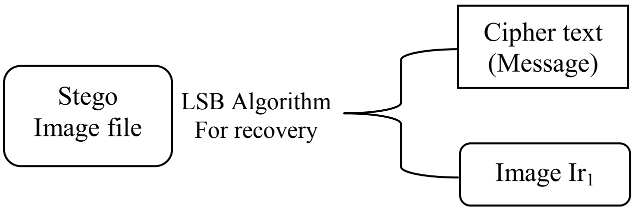
1) Multi secret image sharing technique: Reconstruction of the secret images will be done by shares through generating random image $R_{1,}$ R_1 is bit reversed to get random image R_2. StR_1 is obtained by XOR of R_2 with share S_1 and I_2 is obtained by XOR of R_2 with share S_2 [1].



2) Generation of Stego Image(St_1): Take image StR_1 and perform bit reverse to generate Stego Image St_1 which will be used by LSB algorithm for extracting the hidden message .



3) Extraction of text message: Apply LSB algorithm [3] to extract the encrypted text message from the image St1.



4) Decryption: Perform the decryption using the key provided at the time of encryption on the extracted message from Image Ir_1.

III. ALGORITHM

New Secret Message Sharing Scheme is represented algorithmically in two phases. Those are Generation of Share Phase and Message Recovery Phase. In Generation of shares phase can use any number of images but minimum two images are required for proposed algorithm [1].

A. Create Shares

1. P is the plain text.
2. Perform following steps for encrypting plain text P into cipher text C.
   a) Convert the message string into binary format.
   b) Find the 2's complement of the string.
   c) XOR the 2'complemnt string with the secret key.
   d) Encrypted txt obtained
3. Take cover image I_1.
4. Bitreverse(I_1) = Ir_1.
5. Perform LSB Algorithm [8] on Ir_1 and C to hide the message and the image is called stego image St1.
6. Bitreverse(St_1) = StR_1.(for next step $StR_1 = I_1$)
7. $I_1, I_2, I_3,.., I_n$ are input images of RGB Color
8. 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
9. Calculate Second Random Image
   $R_{2\,=}$ BitReverse(R_1)
10. Calculate Noise images using below formula
    $N_i = I_i \oplus R_2$ ($1 \le i \le n$)
11. Now calculate shares using below formula
    $S_1 = N_1$
    $S_2 = N_2$
    $S_3 = N_3 \oplus N_2 \oplus N_1$
    $S_4 = N_4 \oplus N_3 \oplus N_2$
    …
    $S_n = N_n \oplus N_{n-1} \oplus N_{n-2}$

B. To Recover Secrets

1. Let us assume $S_1, S_2, S_3,\ldots, S_n$ are n shares
2. Calculate Noise Images using 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,

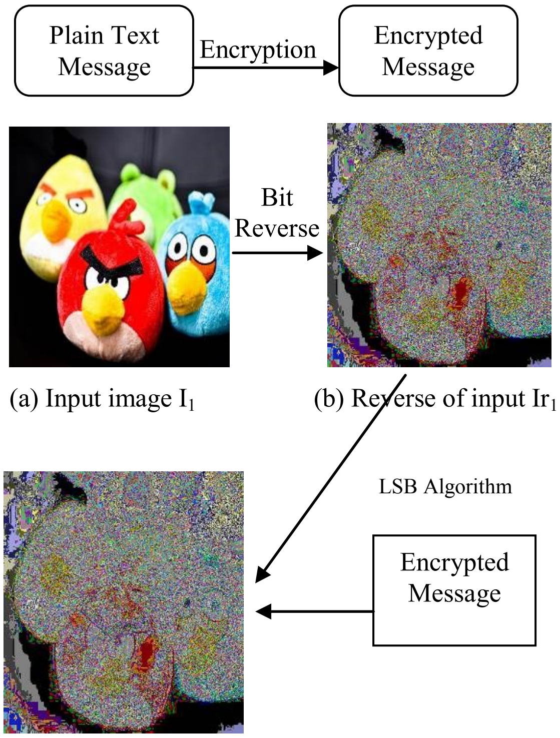
$k = n\text{-}1$ otherwise

4. Calculate Second Random Image
   $R_2 = \text{BitReverse}(R_1)$
5. Now calculate Secrets using below formula
   $I_i = N_i \oplus R_2 \; (1 \leq i \leq n)$
6. Bitreverse(I_1) = St_1.(here I_1 = StR_1)
7. Apply LSB Algorithm [8] on St_1 stego image to extract the hidden message C.
8. Perform the following steps for decrypting the cipher text C to plain text P
   a) The encrypted text is XORed with the secret key used during encryption.
   b) Find the 2's complement of the value obtained after XOR operation.
   c) Plain text P.

IV. EXPERIMENTAL RESULTS

We have done the experiments over the different types of images and different size of images.

Encryption and Share generation Process:



(a) Input image I_1

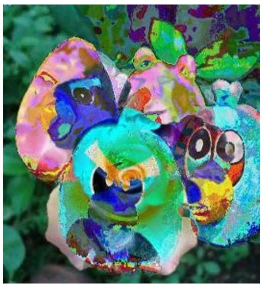
(b) Reverse of input Ir_1

(c) After hiding message St_1

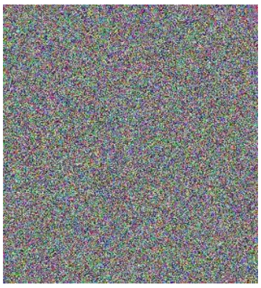
After hiding the message we need to convert this image into random share using MSIS technique.

Bit reverse of St_1 (StR_1)

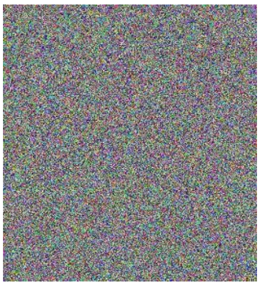
Input image I_2



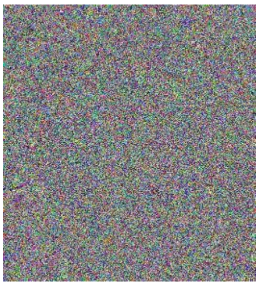
XOR of StR_1 and I_2 (R_1)



Bit reverse of R_1 (R_2)

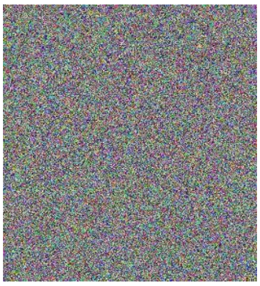


Share S_1

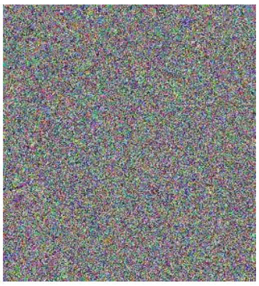


Share S_2

Decryption and Image Recovery Process:

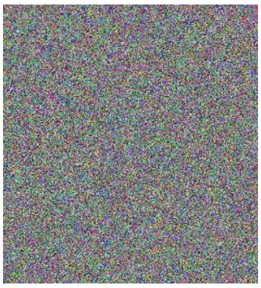


Share S_1



Share S_2

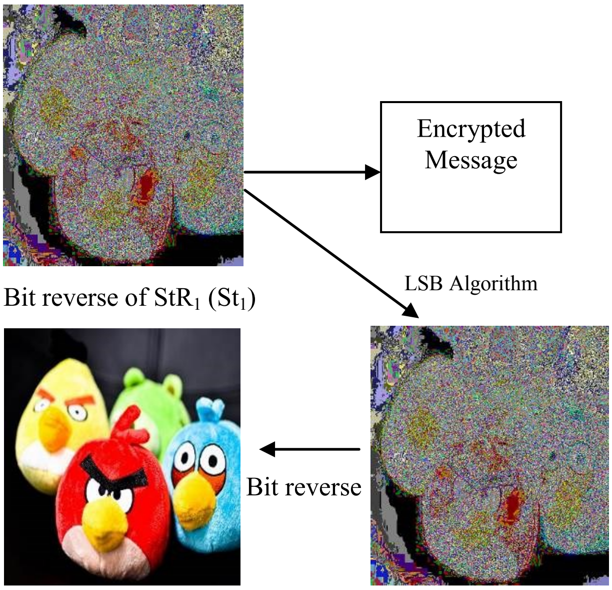
XOR of S_1 and S_2 (R_1)



Bit reverse of R_1 (R_2)

Input image StR_1

Input image I_2



Bit reverse of StR_1 (St_1)

Input image I_1

Image Ir_1

Encrypted Message
Decryption
Plain Text Message

V. CONCLUSION

Cryptography is the science of coding and decoding messages so as to make the message more secure but it does nothing to hide the presence of message whereas Steganography [10] is the art and science of covering information in such a way that its presence is unnoticed. Multi Secret Image Sharing scheme convert multiple secret image into multiple shares to increase randomness such that it cannot be identified easily. The proposed New Secret Message Sharing Scheme combines MSIS scheme and LSB algorithm to make the shares more random and thereby making the data more secure even if it is accessible to any intruder over the network. Our future goal is to modify the algorithm for hiding the data in video files.

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] Amit Patel, Kalpana Gangwar, Sai Sudha Melapu. "A Multi Secret Image Sharing Scheme for RGB Images," unpublished.

[3] Prashanti .G, Sandhya Rani.K, Deepthi.S " LSB and MSB Based Steganography for Embedding Modified DES Encrypted Text", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 8, August 2013, pp.788-799.

[4] Mamta Juneja, Parvinder S. Sandhu, and Ekta Walia,"Application of LSB Based Steganographic Technique for 8-bit Color Images, World Academy of Science, Engineering and Technology, 2009.

[5] Thangadurai, K., and G. Sudha Devi. "An analysis of LSB based image steganography techniques." *Computer Communication and Informatics (ICCCI), 2014 International Conference on*. IEEE, 2014.

[6] Chang, Chin-Chen, Yi-Pei Hsieh, and Chia-Hsuan Lin. "Sharing secrets in stego images with authentication." *Pattern Recognition* 41.10 (2008): 3130-3137.

[7] Shyu, Shyong Jian, et al. "Sharing multiple secrets in visual cryptography."*Pattern Recognition* 40.12 (2007): 3633-3651.

[8] Barhoom, Tawfiq S., and Sheren Mohammed Abo Mousa. "A Steganography LSB technique for hiding Image within Image Using blowfish Encryption Algorithm."

[9] Kumar, B. Ramesh, et al. "Enhanced Approach to Steganography Using Bit planes"." *International Journal of Computer Science and Information Technologies* 3.6 (2012): 5472-5475.

[10] Fridrich, Jiri. "A new steganographic method for palette-based images." *PICS*. 1999.