# More Secure Way of Sharing Secret Text Message

**Amit Patel[1], Sai Prasad Kousika VNH[2]**

[1]Faculty, Department of Computer Science and Engineering, RGUKT,
Mylavaram road, Nuzvid 521202, India

[2]Student, Department of Computer Science and Engineering, RGUKT,
Mylavaram road, Nuzvid 521202, India

**Abstract:** ***The paper is about a more secure way of sharing the text data by hiding the text data in images by steganography (LSB algorithm) and convert the image into random shares through Multi-Secret Image Sharing scheme and sent to the receiver. 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 to recover all n secret image we need all n shared images, but if any shared imaged is lost that will stop the recovery of secret image. The proposed method uses the LSB algorithm which is used to store the secret information in the images and the multi secret image sharing scheme proposed in [3]. 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:** Secret sharing; steganography; stego image; shares; secrets

## 1. Introduction

Security is the primary issue over the Internet as it is a global network. There are so many techniques evolved to protect data from intruders. Cryptography and Steganography [10] are some such methods used for protecting the data over the network. Cryptography is used for secure communication in the presence of third parties by encrypting the data [5]. Steganography ensures more security by hiding the data within other data (image/audio/video) so that no one suspects its existence [5]. In our paper we used LSB algorithm [7] to create a stego file.

Our proposed method uses MSIS scheme on the stego file 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 [3], multiple secrets are divided into multiple shares such that each share contains the information of all the secrets. We have used bit reverse function along with XOR operation to include more randomness in the shares.

This paper is structured as follows. Apart from introduction, there are five more sections. In Section 2 highlights the review of related works and In Section 3, we have explained our New Secret Message Sharing Scheme in detail. In Section 4 we have defined our proposed algorithms for creating shares and for regenerating secrets. 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 message sharing techniques makes data more secure by converting them into image shares. In initial days Cryptography used to send data. But now it can be extended to Steganography where information or a file that has been concealed inside a digital picture [4], video or audio file. If a person views the object in which the information is hidden inside, he or she will have no indication that there is any hidden information. So the person will not try to decrypt the information. Following sub algorithm highlights the two related algorithms in Steganography

### 2.1 LSB Algorithm

LSB (Least Significant Bit) is very efficient algorithm used to embed the information in an image file by altering only least significant bits of a pixel [7]. We can achieve this without any broad change to original colors of image.

**Algorithm 1** (Creating Stego image):

Step1: Read the cover image and text message which is to be hidden in the cover image.
Step2: Convert the text message to binary.
Step3: Calculate LSB of each pixel of image.
Step4: Convert LSB of each pixel of image with one by one converted text bits.
Step5: Write stego file.

**Algorithm 2** (Retrieving data):
Step1: Read the stego file.
Step2: Calculate LSB of each pixel in image.
Step3: Convert each 8-bit binary into single character.

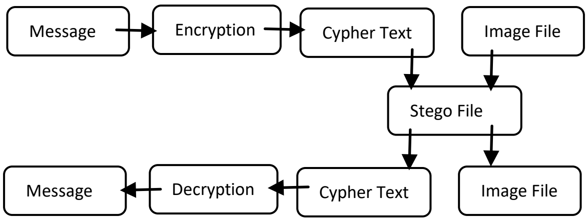


**Figure 1** Block diagram of LSB algorithm

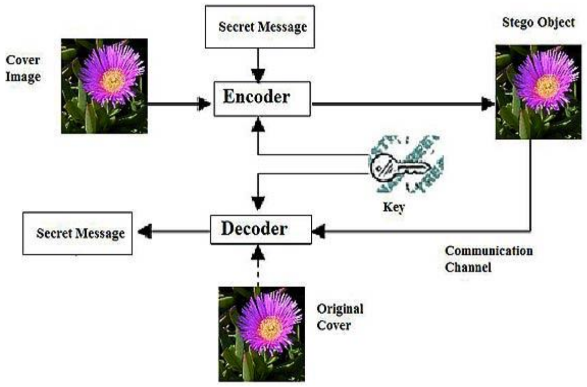


**Figure 2:** Example of LSB algorithm

### 2.2 MSIS Algorithm

MSIS (Multi Secret Image Sharing) means making multiple shares with multiple secrets such that each share contains the information of all secrets [2]. 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

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.

**Algorithm 3** (Creating Shares):

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

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

Chien-Chang Chen and Wei-Jie Wu [2] implemented Chen and Wu's algorithm by calculating random image from secret images only. They used BitShift to function to calculate random image.

**Algorithm 4** (Creating Shares Procedure):

1. Assume that $G_1, G_2, . . ., G_n$ denote 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 Si from all Ni for participant i.

$S_1 = N_1$
$S_2 = N_2$
$S_3 = N_3 \oplus N_2 \oplus N_1$
$S_4 = N_4 \oplus N_3 \oplus N_2$
…
$S_n = N_n \oplus N_{n-1} \oplus N_{n-2}$ i=n

**Algorithm 5** (Share 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 $N_1, N_2, . . ., N_n$ by $R = F_2(N_1 \oplus N_2 \oplus . . . \oplus N_k)$, 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 by combining features of both LSB and MSIS algorithms. We have improved the time taken to generate the shares and recover the shares.

## 3. New Secret Sharing Scheme

Here, we have introduced new algorithm to share the text data in more secure way, even if in between someone gets the shared image they cannot find the hidden message. To accomplish this, the proposed method uses two different algorithms, image based steganography method i.e LSB algorithm [7] and Multi Secret Image Sharing scheme [2].

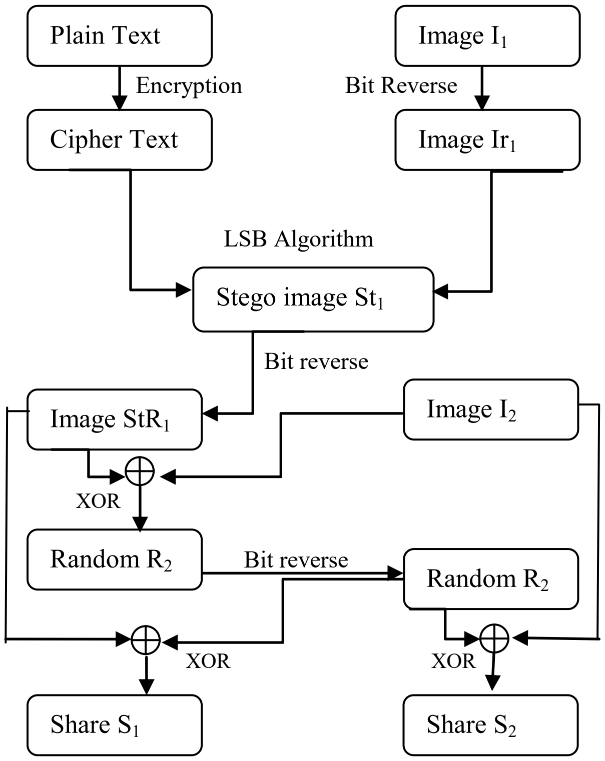


**Figure 3:** Block diagram for MSIS Generation of Shares

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 [7] 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.

### 3.1 Generating Shares

Take the text and encrypt the text message with any cryptographic method and then hide the text message in image $Ir_1$, apply LSB algorithm on encrypted message and image $Ir_1$ to get Stego file $St_1$. $St_1$ is converted to $StR_1$ through bit reverse operation [3]. On image $StR_1$ and image $I_2$, Multi Secret Image Sharing Scheme is used for generating shares which are to be sent to the receiver [9].

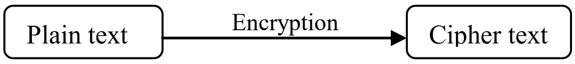
Bit reverse function calculates the binary reverse value of each pixel and replaces each pixel value with the reverse value. If pixel value is 1 then its 8-bit representation is 00000001 and its bit reverse is represented as 10000000 which is equivalent to 128 in decimal format [1].

Reverse (1) = Reverse (00000001) = 128

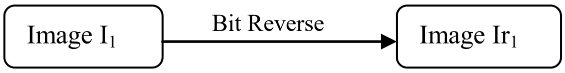
Reverse (2) = Reverse (00000010) = 64

The entire procedure is elaborated in following steps.

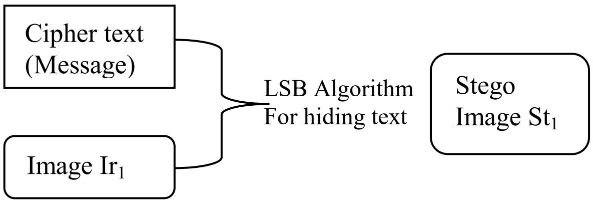
*1) Cipher text:* Convert the secret text message into cipher text by using encryption algorithm (step1 and step 2 of Create Share phase of the algorithm).



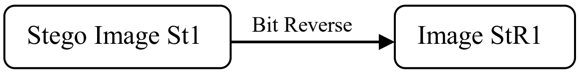
*2) Noisy image ($Ir_1$):* Take the image $I_1$ and apply bit reverse function to generate noisy image $Ir_1$, used for hiding the text message.



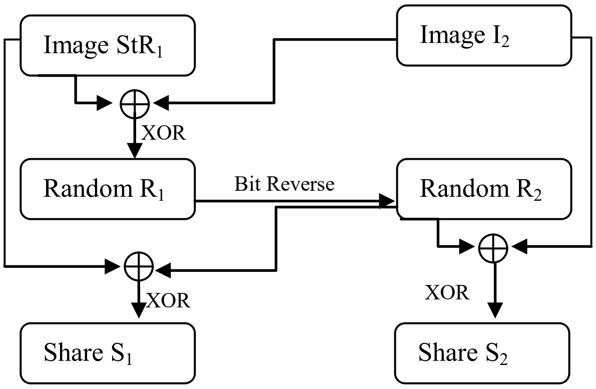
*3) Hiding the Cipher text inside the image:* Apply LSB algorithm to hide the cipher text inside the bit reversed image $Ir_1$.



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



*5) Multi Secret Image Sharing Technique:* This technique includes several steps to generate the shares. Initially random image $R_1$ is generated by using Exclusive OR in between Image $StR_1$ and Image $I_2$. Random image $R_1$ is bit reversed [6] 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.

### 3.2 Message Recovery

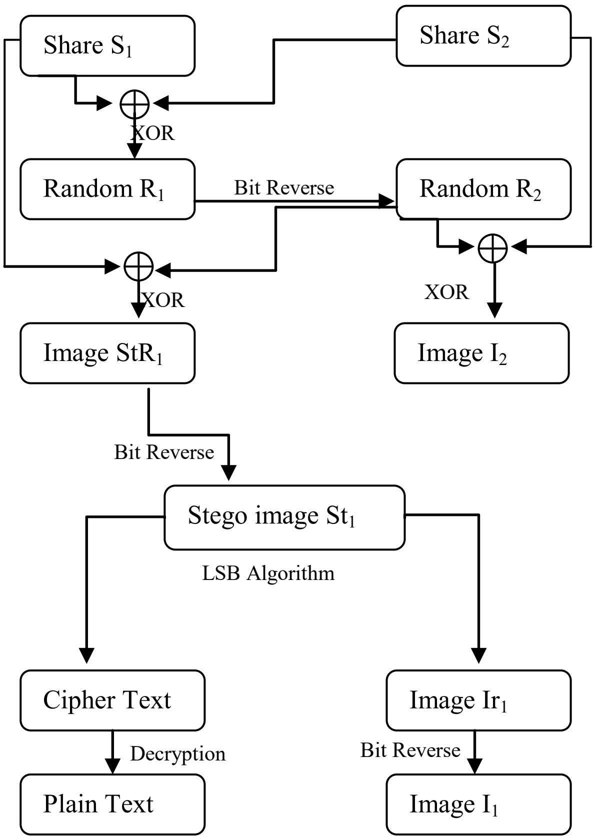
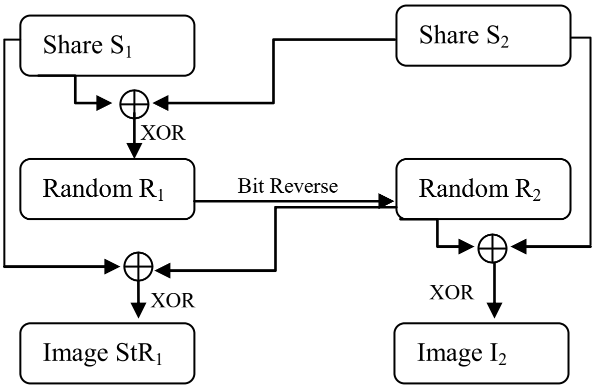


**Figure 4:** Block diagram for MSIS Message recovery

Through Message recovery phase, original message is generated. It also uses combination of both LSB algorithm and MSIS Scheme. It is applied at the receiver side. The entire procedure is elaborated in the following steps.

*1) Multi secret image sharing technique:* This technique includes several steps to reconstruct the secret images from shares. Initially random image $R_1$ is obtained by applying XOR operation between the two shares ($S_1$ and $S_2$) and then bitreverse [6] of $R_1$ is done to obtain the random image $R_2$.

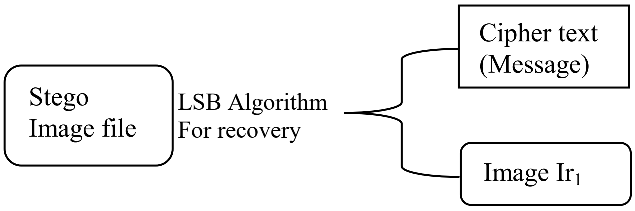
Finally, perform XOR of $R_2$ with share $S_1$ and XOR of $R_2$ with share $S_2$ to generate images $StR_1$ and $I_2$ respectively [1].



*2) Generation of Stego Image($St_1$):* Take image $StR_1$ and perform bit reverse to generate Stego Image [8] $St_1$ which will be used by LSB algorithm for extracting the hidden message

Image $StR_1$
Bit Reverse
Stego Image $St_1$

*3) Extraction of text message:* Apply LSB algorithm [4] 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 $Ir_1$.

Cipher text
Decryption
Plain text

## 4. Problem Definition

Our proposed algorithm is implemented a multiple secret image sharing technique with the proposed bit reverse function [3] and LSB algorithm to make communication of messages more secure. MSIS increases the randomness of the shares and color depth of images with less computation time and LSB hide the message in image [1]. The Proposed algorithm is defined to meet the following objectives.

- Message will be more secure
- To make less computation time
- Increase the randomness of image

In our proposed algorithm we are using MSIS with bit reverse function and LSB algorithm. 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

## 5. Proposed algorithm

New Secret Message Sharing Scheme is represented algorithmically in two phases which 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]. The proposed sharing procedure is illustrated as follows:

### 4.1 Creating Share

**Algorithm 6** (Generating shares with secret message)

```
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 [1] 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
        $R_1 = I_1 \oplus I_2 \oplus I_3 \oplus I_4 \oplus .... \oplus I_k$
        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
        $N_i = I_i \oplus R_2 \ ( 1 \leq i \leq n )$
11.  Now calculate shares using below formula
        $S_1 = N_1$
        $S_2 = N_2$
        $S_3 = N_3 \oplus N_2 \oplus N_1$
        $S_4 = N_4 \oplus N_3 \oplus N_2$
        …
        $S_n = N_n \oplus N_{n-1} \oplus N_{n-2}$
```

### 4.2 To Recover Secrets

**Algorithm 7** (Recovering message from shares)

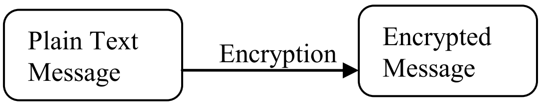
```
1. Let us assume $S_1, S_2, S_3,…, S_n$ are n shares
2. Calculate Noise Images using below formula
       $N_1 = S_1$
       $N_2 = S_2$
       $N_3 = S_3 \oplus N_2 \oplus N_1$
       $N_4 = S_4 \oplus N_3 \oplus N_2$
       …
       $N_n = S_n \oplus N_{n-1} \oplus N_{n-2}$
```

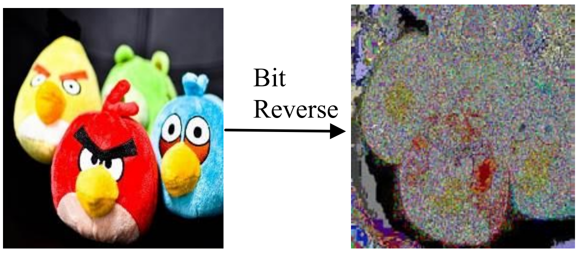
3. Calculate First Random Image
   $R_1 = N_1 \oplus N_2 \oplus N_3 \oplus \ldots \oplus N_k$
   Where k = n if n is even,
   k = n-1 otherwise
4. Calculate Second Random Image
   $R_2 = \text{BitReverse}(R_1)$
5. Now calculate Secrets using below formula
   $I_i = N_i \oplus R_2 \; (1 \le i \le n)$
6. $\text{Bitreverse}(I_1) = St_1$.(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.

## 5. Experimental Results

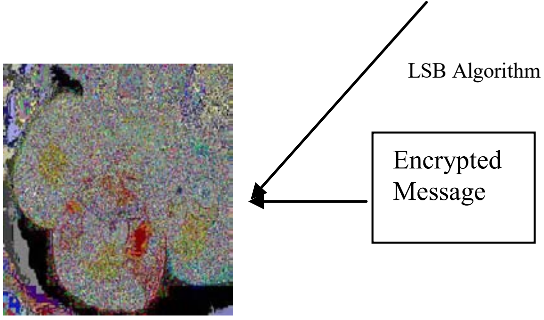
We have done the experiments over the different types of images and different size of images.

### 5.1 Encryption and share generation process





(a) Input image $I_1$ (b) Reverse of input $Ir_1$



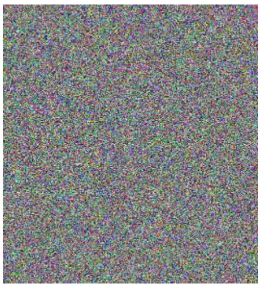
(c) After hiding message $St_1$

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

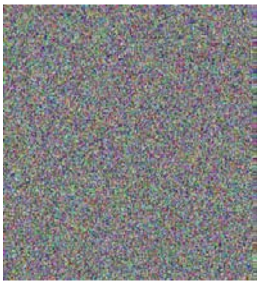
Bit reverse of $St_1$ ($StR_1$)

Input image $I_2$

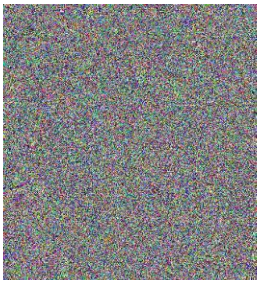
XOR of $I_1$ and $I_2$ ($R_1$)



Bit reverse of $R_1$ ($R_2$)



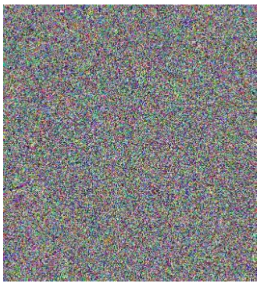
Share $S_1$



Share $S_2$

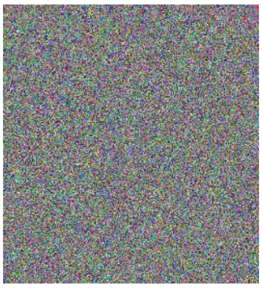
### 5.2 Decryption and Image Recovery Process:

Share $S_1$

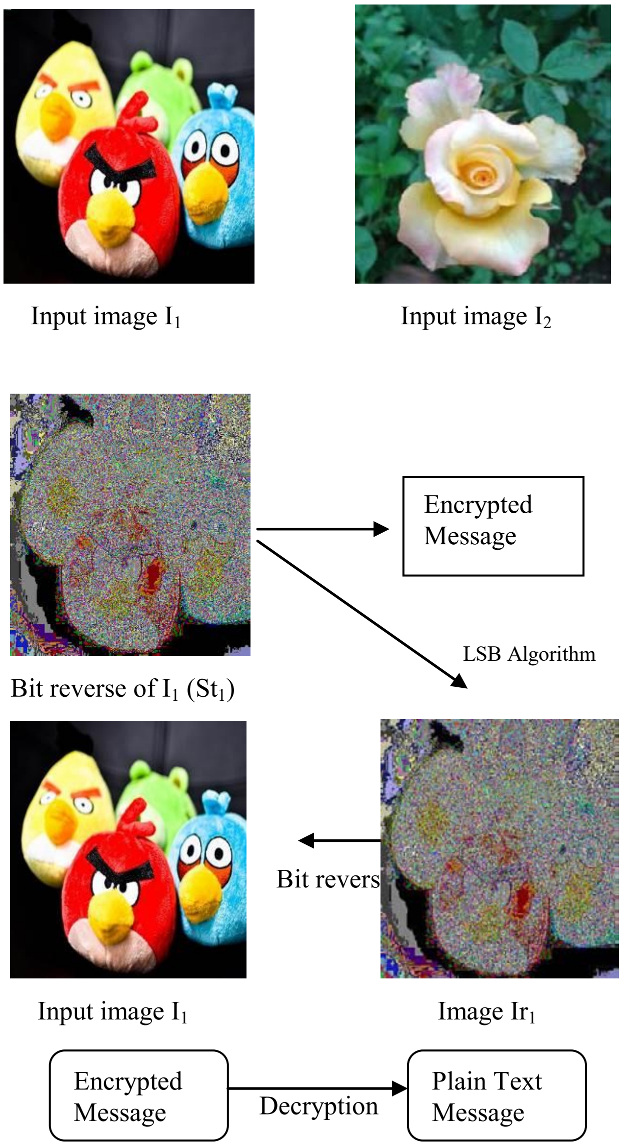


Share $S_2$

XOR of $S_1$ and $S_2$ ($R_1$)



Bit reverse of $R_1$ ($R_2$)



## 6. Conclusion

Cryptography is the science of coding and decoding messages so as to keep these messages secure. It does nothing to hide the presence of message to itself. Steganography [11] 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, this paper discusses the approach we followed to combine all the above mentioned techniques to make the data more secure if it is accessible to any intruder over the network. In proposed New Secret Sharing scheme, encryption algorithm is applied on the secret text to generate cipher text. On this cipher text, image based steganography technique LSB algorithm is used to generate a stego file and finally MSIS scheme converts the images into a random share which is send to the receiver. We are also working on sharing images by using same methods [1]. Our future goal is to modify the algorithm for hiding the data in video files.

## References

[1] Patel, Amit, and Sai Sudha Melapu. "New Secret Message Sharing scheme using MSIS scheme and LSB algorithm." 2016 International Conference on Computer Communication and Informatics (ICCCI). IEEE, 2016.

[2] 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.

[3] Patel, Amit, Kalpana Gangwar, Sai Sudha Melapu. “A Multi Secret Image Sharing Scheme for RGB Images,”2015 International Conference on Digital Signal Processing (ICDSP).

[4] Patel, Amit, Lakshmi Prasanna Mutyala. “Secure way of sharing secret images using LSB and MSIS,” unpublished.

[5] 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.

[6] Patel, Amit. "Enhanced Multi Secret Image Sharing Scheme for Gray and RGB Images." International Journal of Science and Research (IJSR).

[7] 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.

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

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

[10] 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.

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

## 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.

**Sai Prasad KVNH** perusing his final year B.Tech in Department of Computer Science from Rajiv Gandhi University of knowledge Technologies, Nuzvid.