ISSN No. 0976-5697
Volume 8, No. 1, Jan-Feb 2017
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

# Secure Way of Sharing Secret Images Using LSB and MSIS Technique

Amit Patel
Lecturer, Dept. of Computer Science and Engineering
Rajiv Gandhi University of Knowledge and Technologies
Nuzvid, Krishna, India

Lakshmi Prasanna Mutyala
Student, Dept. of Computer Science and Engineering
Rajiv Gandhi University of Knowledge and Technologies
Nuzvid, Krishna, India

***Abstract:*** In this paper we present a new technique for sharing of RGB images. Secret Image Sharing technique distributes the secret information among multiple shares such that these shares altogether is the only way to recover the secret information. In our proposed method RGB image being the secret information will be divided into separate planes. Each single will be stored inside another RGB image by using LSB algorithm. Now to better justify the term Secure, an enhanced MSIS algorithm will be applied on these images to generate the final shares that can be communicated further to the receiver.

***Keywords:*** Cover Images, Stego Images, Secrets, Shares, LSB, MSIS

## I. INTRODUCTION

Steganography is the practice of hiding private or sensitive information within something that appears to be nothing out to the usual. If a person or persons views the object that the information is hidden inside of he /she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information.

An image is an array, or a matrix, of square pixels (picture elements) arranged in columns and rows. An Image can be thought of a two dimensional light intensity function f(x, y), where x and y represent the Cartesian coordinates and the value of the function f at any point (x, y) depends on the brightness and gray level (in black and white image) or RGB value (in colored image) at that point. In imaging science, image processing is any form of signal processing for which the input is an image, such as a photograph or video frame; the output of image processing may be either an image or a set of characteristics or parameters related to the image. Most image processing techniques involve treating the image as a two dimensional signal and applying standard signal processing techniques to it.

In another way we can say that an image is a digital representation of assortment of pixels, like an array. Hence image processing includes

- Acquiring input associated with a digital Image.
- Changing the Image to suit our needs.
- Acquiring information from the Image which is relevant to us. Producing the desired output

### A. *Secret Image Sharing Scheme*

Secret Message Sharing aims to distribute the secret information to several shadow information holders, and we can completely recover the desired information by collecting an enough number of multiple carriers. That is, we can recover the secret based on only some portion of shadow information [4].

Secret Image Sharing [9] is related to the Secret Message Sharing in which each pixel of image will be treated as secret information. Secret image will be used to generate shadow images and required part of these shadow images will be taken in reconstructing the original image. Shadow images will look like some random noise in order to allow no one to get the information about the secret image without permission [4].

This paper is structured as follows. Apart from introduction, there are four more sections. In Section II highlights the related works and In Section III, explain about the proposed algorithms for creating shares and for recovering secrets. Section IV discusses about the experimental result related to our proposed work and finally we concluded with section V.

## II. RELATED WORK

There are many reasons to hide data but they all boil down to the desire to prevent unauthorized persons from becoming aware of the existence of a message. A hidden message is indistinguishable from white noise. Even if the message is suspected, there is no proof of its existence. Most of the newer applications use steganography [10] like a watermark, to protect a copyright on information. Photo collections, sold on CD, often have hidden messages in the photos which allow detection of unauthorized use.

### A. *LSB Based Steganography*

Message will be encoded in image without making drastic changes to the colors in the original image. This can be achieved by changing only least significant bits of a pixel [5].

If suppose R, G and B bytes of original pixel is as below

(r7 r6 r5 r4 r3 r2 r1 r0, g7 g6 g5 g4 g3 g2 g1 g0, b7 b6 b5 b4 b3 b2 b1 b0)

And character (byte) as some bits: c7 c6 c5 c4 c3 c2 c1 c0.

Now these character bits will be placed in LSB positions of R, G and B bytes of pixel accordingly

(r7 r6 r5 r4 r3 c7 c6 c5, g7 g6 g5 g4g3 c4 c3 c2, b7 b6 b5 b4b3 b2 c1 c0)

If we had done this to the example of pixel (225, 100, 100) with character ‘a’, we obtain:

Original pixel = (11100001, 01100100, 01100100)
‘a’ = 01100001

New pixel in bits = (11100011, 01100000, 01100101)
New pixel value = (227, 96, 101)

Notice the new pixel of (227, 96, 101), is almost the same value as the old pixel of (225, 100, 100). There will be no noticeable color difference in the image. To retrieve the message, we can simply extract the appropriate pixels from the RGB values to reconstruct the secret character [7].

### B. *Enhanced Multi Secret Image Sharing Scheme*

This technique is an improvement provided to Chen and Wu’s algorithm [3]. Here bit reversal function [6] has been used in place of bit shift function while generating the random image. With this change the computational time has been improved so it can be preferable even for RGB images

**Algorithm 1**
Sharing Procedure

1. Let us assume I1, I2, I3,.. , In are input images of RGB Color
2. Calculate First Random Image
   R1 = I1 ⊕ I2 ⊕ I3 ⊕ I4 ⊕ ⋯. ⊕ Ik where k=n if n is even, k=n-1 otherwise
3. Calculate Second Random Image
   R2 = BitReverse(R1)
4. Calculate Noise images using below formula
   Ni = Ii ⊕ R2 ( 1 ⩽ i ⩽ n )
5. Now calculate shares using below formula
   S1 = N1
   S2 = N2
   S3 = N3 ⊕ N2 ⊕ N1
   S4 = N4 ⊕ N3 ⊕ N2
   Sn = Nn ⊕ Nn-1 ⊕ Nn-2

**Algorithm 2**
Recovery Procedure

1. Let us assume S1, S2, S3,…, Sn are n shares
2. Calculate Noise Images uing below formula
   N1 = S1
   N2 = S2
   N3 = S3 ⊕ N2 ⊕ N1
   N4 = S4 ⊕ N3 ⊕ N2
   Nn = Sn ⊕ Nn-1 ⊕ Nn-2
3. Calculate First Random Image
   R1 = N1 ⊕ N2 ⊕ N3 ⊕ ⋯ ⊕ Nk where k=n if n is even, k=n-1 otherwise
4. Calculate Second Random Image
   R2 = BitReverse(R1)
5. Now calculate Secrets using below formula
   Ii = Ni ⊕ R2 ( 1 ⩽ i ⩽ n )

## III. PROPOSED ALGORITHM

Image security during communication is needed in various situations like business plan exchanges, personal photos sharing and plans for new inventions etc. This proposed algorithm is used to share an image in a secured manner by storing it inside multiple images and generating shares that can be communicated further.

The proposed algorithm has two phase one encryption that is generation of shares and decryption processes means recovery of image through shares, algorithm are as follows:

### A. *Encryption*

Encryption process involves hiding the secret image inside another RGB image and generating shares for secured communication.

**Algorithm 3**

1. Let Images R,G,B are the respective R,G, and B planes of our RGB secrete image
2. Let I1, I2 and I3 are input images where we are going to hide the above R,G and B planes
3. Suppose R1is any pixel of R image and Ir1, Ig1 and Ib1 are the R,G and B pixels of image I1
   R1= (r7 r6 r5 r4 r3 r2 r1 r0)
   Ir1= (ir7 ir6 ir5 ir4 ir3 ir2 ir1 ir0)
   Ig1= (ig7 ig6 ig5 ig4 ig3 ig2 ig1 ig0)
   Ib1= (ib7 ib6 ib5 ib4 ib3 ib2 ib1 ib0)
4. Hiding of pixel in LSB bits of input images is as follows
   Ir1= (ir7 ir6 ir5 ir4 ir3 **r7 r6 r5**)
   Ig1= (ig7 ig6 ig5 ig4 ig3 **r4 r3 r2**)
   Ib1= (ib7 ib6 ib5 ib4 ib3 ib2 **r1 r0**)
5. Now apply **Algorithm 1** on I1, I2, I3 and generate shares S1, S2 and S3

### B. *Decryption*

The below is the algorithm for recovery of secret image from shares received at the receivers end

**Algorithm 4**

1. Apply **Algorithm 2** on the shares $S_1$, $S_2$ and $S_3$
2. Extract the LSB bits of above generated stego images
   $I_{r1}$= (ir7 ir6 ir5 ir4 **r7 r6 r5**)
   $I_{g1}$= (ig7 ig6 ig5 ig4 ig3 **r4 r3 r2**)
   $I_{b1}$= (ib7 ib6 ib5 ib4 ib3 ib2 **r1 r0**)
   R1= (r7 r6 r5 r4 r3 r2 r1 r0)
3. After extracting all the pixel of individual planes, combine these planes into single RGB image to get

### C. *Overview*

Block diagram representation of the whole process is given below. Once we run the application it will ask to select the operation which we want to perform either encryption or decryption. Based on the selection it will execute the particular function and give the result.

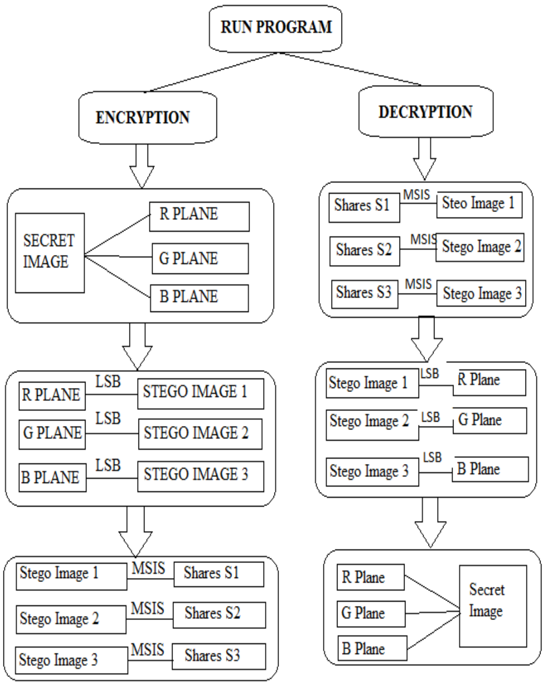


Fig 1. Block diagram of complete process

## IV. EXPERIMENTAL RESULTS

We have done several experiments for few of them results are shown below.

### *A. Encryption*

The template is designed so that author affiliations are

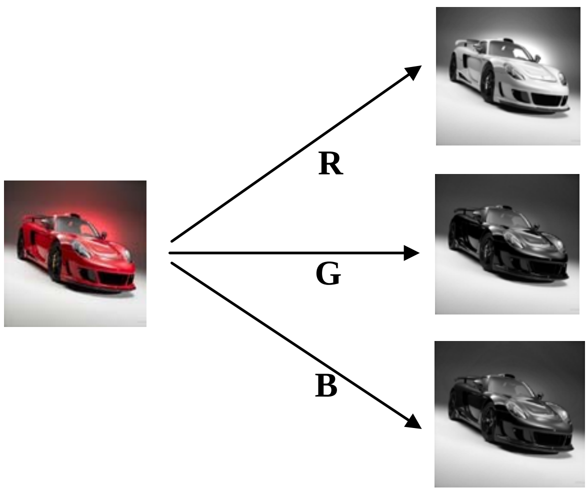


Fig 2. Divison of R G B planes

As depicted in Fig 2, the secret image will get divided into separate planes and these planes will be taken as individual images for the next steps of algorithm

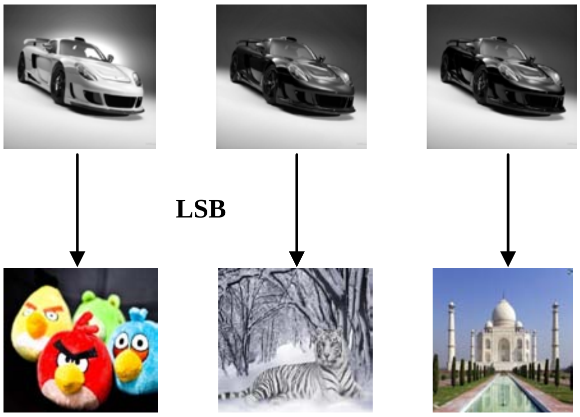


Fig 3. Hiding of planes using LSB algorithm

Each individual plane of our secrete image will be hided inside a RGB image called cover image by using LSB algorithm [2] and stego images [8] will be generates as outputs.

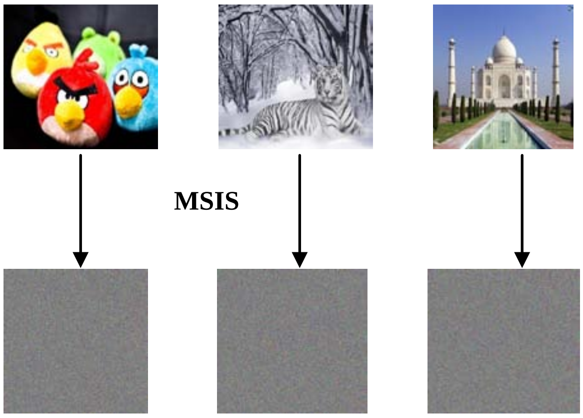


Fig 4. Application of MSIS on cover images

As shown in the figure MSIS algorithm [1] will be applied on stego images and shares that are randomized will be generated as output.

### *B. Decryption*

Decryption is the process for recovery of secret image from shares received at the receivers end.

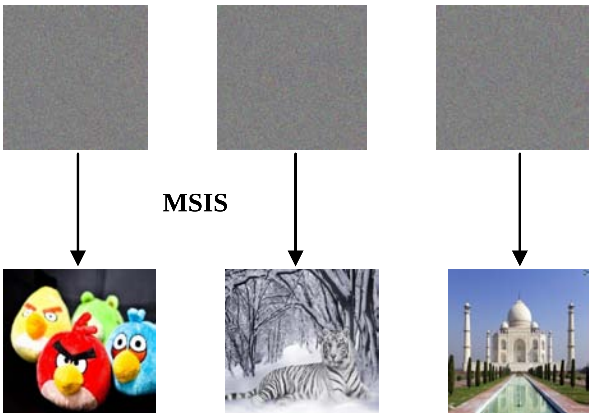


Fig 5. Application of MSIS on shares

 

In the above figure, reverse MSIS algorithm has been applied on shares to get the stego images in which the planes of our original image were hided.

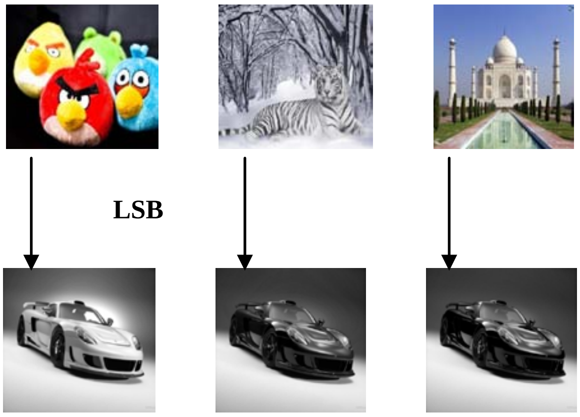


Fig 6. Extraction of planes using LSB algorithm

As depicted from Fig 6, the LSB bits of each stego image have been extracted from the stego images and the image planes have been reconstructed.

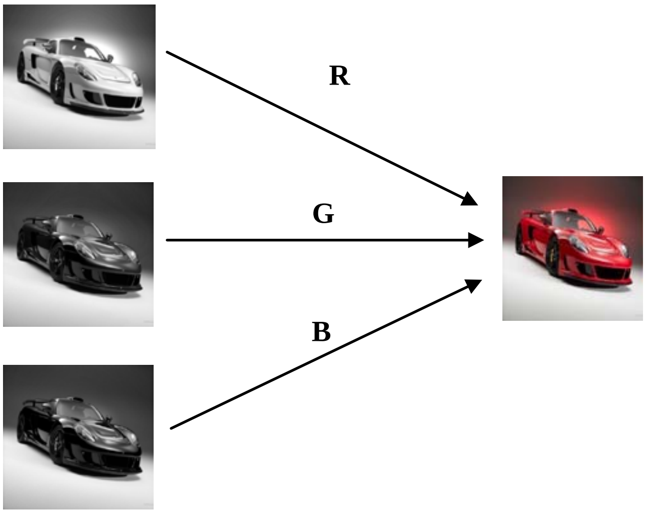


Fig 7. Reconstruction of secret image

The original secret image has been reconstructed from the individual R, G and B planes as shown in the above figure.

## V. CONCLUSION

Steganography is one of the major digital techniques that involve hiding the information inside the image. The purpose of this paper is to share a secret image in a secured manner. Proposed algorithms is about storing an RGB inside other images and generating shares that are quite random. It will become really hard for the intruder to identify the presence of our secret image inside these shares. At the receiver side secret image will be recovered using our decryption algorithm.

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

[4] Amit Patel, Sai Prasad Kousika VNH, "More Secure Way of Sharing Secret Text Message", International Journal of Science and Research (IJSR), https://www.ijsr.net/archive /v5i12/v5i12.php, Volume 5 Issue 12, December 2016, 1563 - 1568.

[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] Amit Patel, "Enhanced Multi Secret Image Sharing Scheme for Gray and RGB Images", International Journal of Science and Research (IJSR), ijsr.net, Volume 5 Issue 2, February 2016, 1867 – 1871.

[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.