# Image Steganography on Second LSB

**Anil Khurana**
Assistant Professor, Electronics and Communication,
Gian Jyoti Instt. of Engg. & Tech.
Shambhu Kalan, Banur, Punjab
E-mail: anil.khurana85@gmail.com

**Abstract**

This paper presents the Image steganography in second Least Significant Bit (LSB) in a grayscale and RGB image. In LSB based Steganography embed the text message or secret message in least significant bits of digital picture and in second LSB the text message or secret messages embedded in second least significant bit of digital picture. In this paper we are showing the results we can obtain from inserting a secret message in second LSB.

**Keywords:** Least Significant Bit (LSB), Mean Square Error (MSE), Signal to Noise Ratio (SNR), Steganography

## I. INTRODUCTION

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" defining it as "covered writing". In image steganography, the information is hidden exclusively in images. The image obtained after insertion of message is called a stego image. Insertion of secret message is done in least significant bit (LSB) or second LSB of the image pixels. Then the stego image formed is having a message which is invisible to human eye. This means that one cannot find the difference between the original image and stego image. The secret message is inserted by using an algorithm and the secret message is obtained from stego image by using reverse algorithm.

## II. METHODS OF STEGANOGRAPHY

### A) LSB STEGANOGRAPHY

LSB is the lowest bit in a series of numbers in binary. e.g. in the binary number: 10110001, the least significant bit is far right 1. The LSB based Steganography is one of the steganographic methods, used to embed the secret data in to the least significant bits of the pixel values in a cover image. e.g. 240 can be hidden in the first eight bytes of three pixels in a 24 bit image.

PIXELS:

| | | |
|---|---|---|
| 00100111 | 11101001 | 11001000 |
| 00100111 | 11001000 | 11101001 |
| 11001000 | 00100111 | 11101001 |

Here if we want to hide 240 in a digital image the first step is to convert 240 into a binary number that is 011110000 then this 9 bit data is replaced by each least significant bit of the pixels of the image.

RESULT:

| | | |
|---|---|---|
| 0010011**0** | 1110100**1** | 1100100**1** |
| 0010011**1** | 1100100**1** | 1110100**0** |
| 1100100**0** | 0010011**0** | 1110100**1** |

240 can be hidden in the first eight bytes of three pixels in a 24 bit image.

B) SECOND LSB STEGANOGRAPHY

Second LSB is next bit in a series of numbers in binary after LSB i.e on second bit from right. e.g in the binary number : 1100110, the second least significant bit is 0

*PIXELS:*

| | | |
|---|---|---|
| *00100110* | 11101001 | 11001001 |
| *00100111* | 11001000 | 11101000 |
| *11001000* | 00100110 | 11101001 |

*240:011110000*

*RESULT:*

| | | |
|---|---|---|
| *0010010**1*** | 1110101**1** | 1100101**0** |
| *1010011**1*** | 1100100**0** | 0110100**1** |
| *0100100**0*** | 0010010**1** | 0110100**1** |

## III. ALGORITHM OF STEGANOGRAPHY

A) SECOND LSB STEGANOGRAPHY

Step 1: Read the cover image and text message, which is to be hidden in the cover image.

Step 2: Convert text message in binary.

Step 3: Rotate Left the binary message

Step 4: Calculate LSB of each pixel of cover image.

Step 5: Replace LSB of the cover image with each bit of secret message one by one.

Step 6: Rotate right each binary pixel.

Step 7: Write stego image.

Algorithm to Retrieve Text Message

Step 1: Read the stego image.

Step 2: Rotate left each binary pixel.

Step 3: Calculate LSB of each pixel of stego image.

Step 4: Retrieve bits and convert each 8 bit into character.

## IV. PERFORMANCE AND RESULTS

Comparative analysis of LSB based and MSB based steganography has been done on basis of parameters like MSE i.e., Mean square error. Both grayscale and colored images have been used for experiments. Mean square error is used to compute how well the methods perform.

The mean squared error between two images $I_1$ (m, n) and $I_2$ (m, n) is:-

$$MSE = \frac{\sum[I_1 (m, n) - I_2 (m, n)]^2}{M*N}$$

LSB Based Steganography for Grayscale Images


Leena.bmp Stego Leena.bmp

MSE = 0.4307


Love.bmp Stego love.bmp

MSE = 0.7832

Second LSB Based Steganography for Grayscale Images


Leena.bmp Stego Leena.bmp

MSE = 2.3019


Love.bmp Stego love.bmp

MSE = 4.7832

## V. CONCLUSION

LSB based steganography embed the text message in LSB of the pixels of cover image whereas Second LSB based steganography embed the text message in second LSB of pixels of cover image. This paper shows the results of second LSB based steganography by calculating Mean square error. MSE computes the error between the cover image and the stego image. If the mean square error is high that means the there is difference between the pixel values of the image then the stego image is not exactly same as the cover image. If the MSE is low then stego image is of good quality and there is less difference between the cover and stego image. Such an image the secret message cannot be observed by human eye so secret information is transferred from source to destination.

**References**

[1] Jamil, T.,"Steganography: The art of hiding information is plain sight", IEEE Potential, 1999.

[2] Francesco Queirolo, Johnson,"Steganography in Images", Fine communication Report, 2002.

[3] K. Sulliavan, O. Dabeer, U. Madhow, B.S. Manjunath, S.Chandrasekaran,"LLRT based detection of LSB hiding", submitted to ICIP, 2003.

[4] O. Dabeer, K. Sulliavan, U. Madhow, S. Chandrasekaran, and B.S. Manjunath,"Detection of hiding in least significant bit", Proceedings of CISS.H, 2003.

[5] Chandramouli, R., Kharrazi, M., Memon,"Image steganography and steganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003.

[6] Deshpande Neeta, Kamalpur Snehal, Daisy Jacobs "Implementation of LSB Stegnography and its Evaluation for various bits", University of Pretoria, South Africa, ISBN, Version 07-04-06, 2004, pp. 173-178.

[7] Neeta Deshpande, Kamalapur Sneha, Daisy Jacobs, "Implementation of LSB Steganography and Its Evaluation for various Bits Digital Information Management", 2006 1st International Conference on 06/01/2007.

[8] Hasan Mathkour, Batool Al-Sadoon,"A new image Steganography techniques", Digital object identifier, version11-18, 2008, pp. 1-4.

[9] Beenish Mehboob, Rashid Aziz Faruqui ,"A Steganography Implementation", IEEE International Symposium on Biometic & Security Technologies, ISBAST 08, 23-24,Islamabad, 2008, pp.1-5.

[10] Mamta Juneja, Parvinder Singh Sandhu, Ekta walia,"Application of LSB based Steganography