

Image Steganography With LSB

Rahul Joshi¹, Lokesh Gagnani², Salony Pandey³

¹ PG Student, KIRC, Kalol

² Asst Prof, KIRC (I.T Department)

³ PG Student, RK UNI, Rajkot

Abstract : The rapid development of data transfer through internet has made it easier to send the data accurate and faster to the destination, but in order to transfer the data securely to the destination without any modifications, there are many approaches like steganography. This paper introduces the concept of steganography using “LSB METHOD”.

Keywords: Carrier Image, Image Steganography, Information Hiding, Least Significant Bit, Steganography

I. INTRODUCTION

The word „Steganography” comes from the Greek steganos (covered or secret) and graphy (writing or drawing) and thus means, literally, covered writing. It is a data hiding techniques, which aims at transmitting a message on a channel where some other kind of information is already being transmitted. The goal of steganography is to hide messages inside the images in such a way that does not allow any “enemy” to even detect that there is a secret message present in the image. Steganography attempts to hide the existence of communication [1]. The basic structure of Steganography is made up of three components:

- i. The Carrier image,
- ii. The Message,
- iii. The Key

The carrier can be a painting, or a digital image. It is the object that will „carry” the hidden message. A key is used to decode/decipher/discover the hidden message. This can be anything from a password, a pattern, a black-light, or even lemon juice.

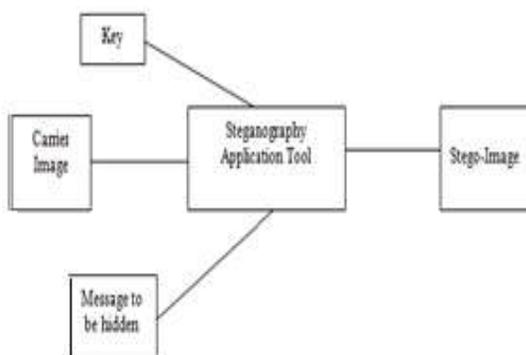


Fig 1. Block Diagram of Steganography

II. LEAST SIGNIFICANT BIT TECHNIQUE

Least significant bit (LSB) insertion is a common and simple approach to embed information in an image file. In this method the LSB of a byte is replaced with an M” s bit. This technique works good for image steganography. To the human eye the stego image will look identical to the carrier image.. For hiding information inside the images, the LSB (Least Significant Byte) method is usually used. To a computer an image file is simply a file that shows different colors and intensities of light on different areas of an image. The best type of image file to hide information inside is a 24 Bit BMP (Bitmap) image. When an image is of high quality and resolution it is a easier to hide information inside image. Although 24 Bit images are best for hiding information due to their size. Some people may choose 8 Bit BMP” s or possibly another image format such as GIF [2]. The reason being is that posting of large images on the internet may arouse suspicion. The least significant bit i.e. the eighth bit is used to change to a bit of the secret message. When using a 24-bit image, one can store 3 bits in each pixel by changing a bit of each of the red, green and blue color components. Suppose that we have three adjacent pixels (9 bytes) with the RGB encoding [3]

```

10010101 00001101 11001001
10010110 00001111 11001011
10011111 00010000 11001011
  
```

When the number 300, can be which binary representation is 100101100 embedded into the least significant bits of this part of the image. If we overlay these 9 bits over the LSB of the 9 bytes above we get the following (where bits in bold have been changed)

```

10010101 00001100 11001000
10010111 00001110 11001011
10011111 00010000 11001010
  
```

Here the number 300 was embedded into the grid, only the 5 bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size.

III. ALGORITHM

1. Select a cover image of size M*N as an input.
2. The message to be hidden is embedded in RGB component only of an image.
3. Use a pixel selection filter to obtain the best areas to hide information in the cover image to obtain a better rate. The filter is applied to Least Significant Bit (LSB) of every pixel to hide information, leaving most significant bits (MSB).
4. After that Message is hidden using Bit Replacement method.

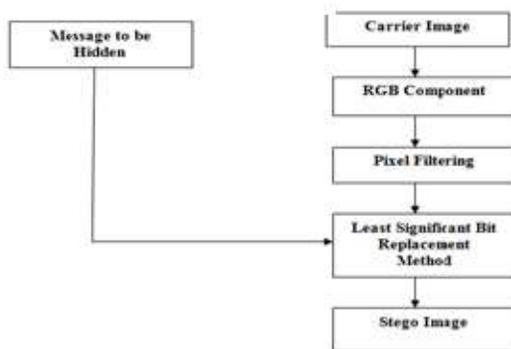


Fig 2. Algorithm of Least Significant Bit

IV.RESULTS

After Implement of this method following parameters are occur using related equation

$$\text{SNR} = 10 \cdot \log_{10} (\text{signal}/\text{noise});$$

Value of SNR display like this

SNR Signal to Noise Ratio

37.4684

Value of PSNR display like this

$$\text{PSNR} = 10 \cdot \log_{10} (\text{peak}^2/\text{MSE});$$

PSNR Peak Signal to Noise Ratio

42.7777

Cover and Stego images display like this



IV. CONCLUSION

This method is very easy to implement .but this method have following disadvantages One of the major disadvantage associated with LSB method is that intruder can change the least significant bit of all the image pixels. In this way hidden message will be destroyed by changing the image quality, a little bit, i.e. in the range of +1 or -1 at each pixel position.

Not immune to noise and compression technique. I will try to solve this disadvantages using enhance or modified LSB method

ACKNOWLEDGMENT

I am very thankful to my guide Prof. Lokesh Ganani for giving me this opportunity to prepare this paper and also thankful to Prof..Hitesh Patel H.O.D of Information Technology Department KIRC KALOL.

REFERENCES

- [1] K.B.Raja, C.R.Chowdary, Venugopal K R, and L.M.Patnaik, " A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images" Department of Computer Science Engineering, Bangalore 2005 IEEE
- [2] V. Lokeswara Reddy, Dr.A.Subramanyam, Dr.P. Chenna Reddy, "Implementation of LSB Steganography and its Evaluation for Various File Formats", *Int. J. Advanced Networking and Applications* 868 Volume: 02, Issue: 05, Pages: 868-872 (2011)
- [3] T Morkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography," in *Proceeding of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sand to South Africa, June/July 2005*