Implementation of LSB-Based Image Steganography Method for Effectiveness of Data Hiding Capacity

Dipak Parikh[1] Prof. Anurag Rishishwar[2] Prof. Manish Trivedi[3]
[1,2,3]RKDF Institute of Science & Technology, Bhopal, Madhya Pradesh

Abstract— Increased use of electronic communication has given birth to new ways of transmitting information securely. Steganography is a science of hiding information by embedding it in some other data called host message. Images are most known objects for steganography. The host message before steganography and stego message after steganography have the same characteristics. The given work is to be done by evaluating it on MATLAB. While evaluation one can calculate SNR, PSNR and BER for individual information Bit for conceal bit and analysis effect on results.

Keywords*:* Steganography, SNR, PSNR, BER

I. INTRODUCTION

Steganography is an art of practice of concealing a message, image or file within another message, image or file. Steganos meaning is "covered, concealed or protected" and graphein meaning "writing". Hidden message may be in invisible ink between the visible lines of private letter. Steganography is an art of hiding some secret message in another message without letting anyone know about presence of secret information except the intended receiver. The message used to hide secret information is known as host message or cover information. Steganography includes concealment of information within computer files. A large redundant bit is present in digital image. Hence digital images are popular cover objects for steganography [2]. A digital image mentioned using 2 -D matrix of color intensities at each grid point. i. e. called pixel. A gray images uses 8 bits while colored uses 24 bits to describe color model e.g. RGB. There are many methods to conceal information inside a cover image. Spatial domain techniques use the pixel gray levels and their color values directly for encoding message bits. These methods are simplest in terms of embedding and extraction complexity. Major drawbacks of these methods are amount of additive noise that creeps in a image which directly affects peak signal to noise ratio and statistical properties of image. Moreover these embedding algorithms are applicable mainly to lossless image compression schemes like TIFF images. LSB (least significant bit) is a major method in spatial domain image steganography. The transform domain methods embed the message in frequency domain of cover image. Spatial domain technique have large capacity and easily detectable. [3], [4]. While frequency based steganography has higher PSNR (peak signal to noise ratio) and is more protected but it is more secure [2] but more complex and requires more calculations. Thus STEGO MESSAGE [9] = HOST MESSAGE + COVER OBJECT (which hides secret message) + STEGO OBJECT (cover object with a message embedded in it).

II. LSB BASED IMAGE STEGANOGRAPHY [8]

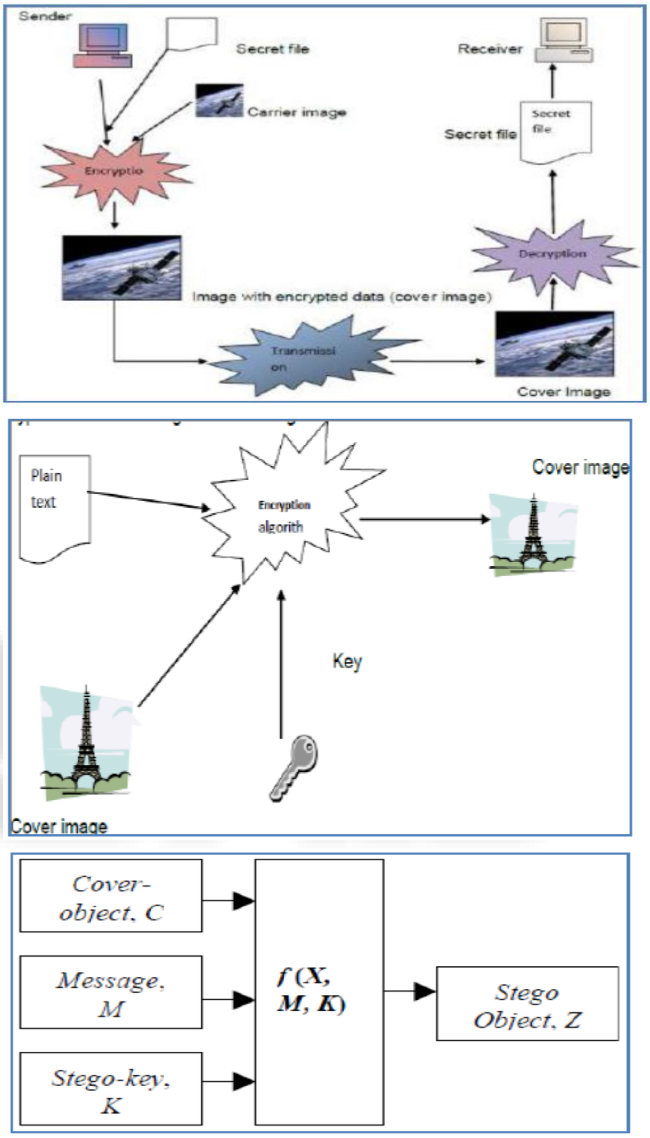

Fig. 1: Block diagram of Steganography

Figure 1 shows the fundamental block diagram of Steganography. The LSB is the lowest significant bit in the byte value of the image pixel. The LSB based image steganography embeds the secret in the least significant bits of pixel values of the cover image (CVR). To illustrate LSB technique, we provide the following example. Suppose the CVR has the following two pixel values:

(0000 1010 0011 0010 0111 0100)
(1111 0101 1100 0011 1100 0111)

Also, from [1] assume that the secret bits are: 101101. After embedding the secret bits, the result pixel values are:

(0000 101**1** 0011 001**0** 0111 010**1**)
(1111 010**1** 1100 001**0** 1100 011**1**)

The bold written bits convey us that the bits were differing from their original value. Only three bits in the cover image were changed. On average about half of the bits in the cover image will be changed when embedding the secret image.

The above LSB method limits the length of the secret message to eighth of the size of the CVR. LSB steganography minimize *n*-bits to increase the capacity of the secret information *n*/8 the size of the CVR. However, increasing *n* disturbs stego-image. In each run, we embed random data in the *n* minimum significant bits, where 1≤*n*≤7. However, we need to introduce the methods to see the resolution and disturbance in images [1].

To measure the imperceptibility of steganography several metrics are used. The metrics indicates how similar (or different) the stego-image compared with CVR.

The following metrics are used in the literature including the work of [5]:

Mean Squared Error (MSE) is calculated by comparing byte by byte of the CVR and Stego-image. The calculation can be expressed as follows:

$$MSE = \frac{1}{M \times N} \sum_{1}^{M} \sum_{1}^{N} \left(f_{ij} - g_{ij} \right)^{2} 2.1$$

Where M, N are the number of rows and columns in the CVR matrix, f_{ij} is the pixel value from CVR, and g_{ij} is the pixel value from the stego-image. Higher value of MSE indicates differences of compared images.

Bit error rate (BER) calculates the actual bit positions of number which are changed in the stego-image compared with CVR.

Peak signal-to-noise ratio measures in decibels the resolution of the stego-image compared with the CVR. The higher PSNR is the better the resolution. PSNR is calculated by following formula:

$$PSNR = 10 \log_{10} \frac{L^{2}}{MSE} \quad 2.2$$

For above LSB of two pixels, we calculate the three metrics and obtain the following values: MSE=0.5, BER=0.0625, PSNR=51.1dB. Various *n*-bit LSB steganography techniques were calculated, where 1≤*n*≤8 using Lena [7] images. The image metrics were calculated for the images across the various LSB experiments.

The result of stego-images is shown in Figure 2-8. Stepwise checking of the images reveals that the disturbance is visible for the stego-image for n≥4. For 8-bit LSB, the image is completely disturbed. The results of the image metrics are tabulated in Table I.

n-bit LSB	SNR	BER	PSNR(dB)
1-bit	96.6594	0	101.9687
2-bit	86.2455	0	91.5548
3-bit	66.9839	0	72.2932
4-bit	56.7356	0	62.0450
5-bit	47.1585	0	52.4678
6-bit	37.4684	0	42.7777
7-bit	27.6675	0	32.9768
8-bit	error	Error	error

Table 1: Image Matrix For Different LSB Method

From the above results of Table I, we conclude following data:

- The metrics for both images are equal.
- The error metrics (MSE and BER) increment quickly with increment of *n*, especially for n≥5.
- The image resolution of PSNR is above 40 dB for 1-bit and 2-bit steganography. For images and video, PSNR ratio between 30dB-50dB is acceptable [6]. Clearly, selecting the appropriate LSB method should balance trade-offs between capacity (i.e., secret size) and imperceptibility (i.e., image distortion) carefully. For our work, we select an LSB method which combines 2-bit and 3-bit as explained below.

III. Simulation Results

The image metrics were calculated for the reproduction of stegoimage. The results show that the produced clown stego-image has better PSNR and small error. Overall, the clown stego-image has similar results to those of Lena images for the 2/3-LSB case. We perform the 1-bit to 7-bit hide data for the input message signal as shown in figure 2-8.

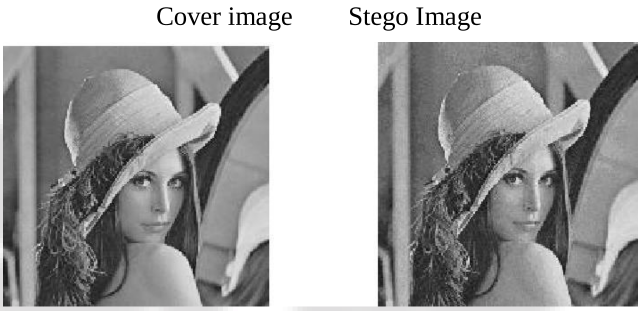

Fig. 2: Stego. For 1-bit hide

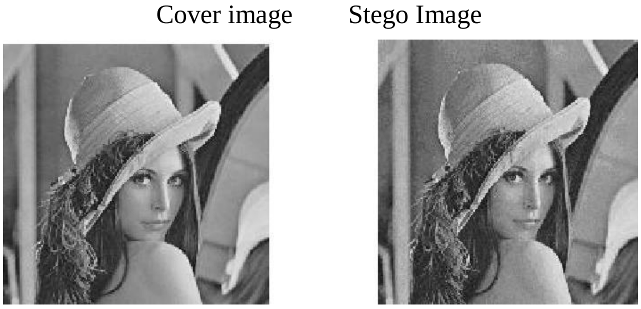

Fig. 3: Stego. For 2-bit hide

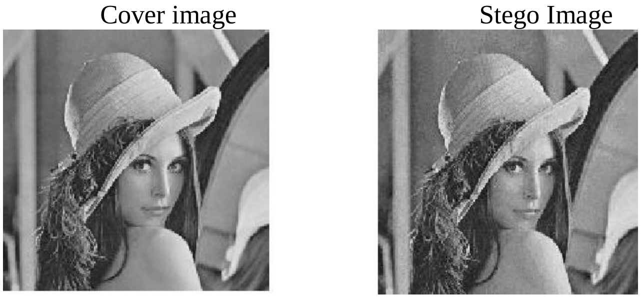

Fig. 4: Stego. For 3-bit hide

Cover image
Stego Image

Fig. 5: Stego. For 4-bit hide

Cover image
Stego Image

Fig. 6: Stego. For 5-bit hide

Cover image
Stego Image

Fig. 7: Stego. For 6-bit hide

Cover image
Stego Image

Fig. 8: Stego. For 7-bit hide

IV. CONCLUSION

In this paper, we have analyzed the performance of different cases of LSB steganography. We may prove that the 2/3-LSB design gives better image resolution and facilitate simple memory access. We also presented the results of test image executed on the hardware implementation. Future work should focus on hardware implementation of more and more complex random-based LSB mechanisms, as well as minimization of the design velocity and power.

REFERENCES

[1] B. Jamil Mohd, S. Abed, T. Al-Hayajneh and S. Alouneh, "FPGA Hardware of the LSB Steganography Method", IEEE Computers, 2012.

[2] T. Morkel, J. Eloff and M. Olivier, "An Overview of Image Steganography," The Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, July 2005.

[3] H. Wang, S. Wang, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, October 2004, Vol. 47, No. 10, pp. 76-82.

[4] E. Walia, P. Jain, Navdeep, "An Analysis of LSB & DCT based Steganography", Global Journal of Computer Science and Technology, April, 2010, Vol. 10, pp. 4-8.

[5] K. Prasad, V. Jyothsna, S. Raju and S. Indraneel, "High Secure Image Steganography in BCBS Using DCT and Fractal Compression," International Journal of Computer Science and Network Security, vol. 10, No.4, April 2010.

[6] "Peak Noise to Signal Ratio". Available: http://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio.

[7] "The image database of the signal" [online]. Available: http://sipi.usc.edu/database/

[8] S. Venkatraman, A. Abrham and M. Paprzycki, "Significance of Steganography on Data Security", Proceeding of the International Conference on Information Technology: coding and computing, 2004.

[9] B.A.Patil, V.A.Chakkarwar, "Review of an improved audio steganographic technique over LSB through random based approach", IOSR Journal of Computer Engineering, Feb 2013, Vol 9, No.1, pp.33-34.