

Enhanced Data Hiding Capacity Using LSB-Based Image Steganography Method

Himanshu Gupta¹, Prof. Ritesh Kumar², Dr. Soni Changlani³

^{1,2,3} *Lakshmi Narain College of Technology & Science, Bhopal, Madhya Pradesh*

Abstract—Steganography is one of the most powerful techniques to conceal the existence of hidden secret data inside a cover object. Images are the most popular cover objects for steganography, and thus the importance of image steganography. This work is only based on simulation on MATLAB. In this work calculate the SNR, PSNR and BER for different message bit for hide bit and analysis effect on the results.

Keywords- Steganography, SNR, PSNR, BER.

I. INTRODUCTION

Steganography is the art of invisible communication by concealing information inside other information. A steganography system consists of three elements: cover-object (which hides the secret message), the secret message and the stego-object (which is the cover object with message embedded inside it.) Given the proliferation of digital images on the internet, and the large redundant bits present in the digital representation of an image, images are the most popular cover objects for steganography [2]. A digital image is described using a 2-D matrix of the color intensities at each grid point (i.e. pixel). Typically, gray images use 8 bits, whereas colored utilizes 24 bits to describe the color model, such as RGB model. The steganography system which uses an image as the cover object is referred to as an image steganography system [2]. There are several techniques to conceal information inside cover-image. The spatial domain techniques manipulate the cover-image pixel bit values to embed the secret information. The secret bits are written directly to the cover image pixel bytes. Consequently, the spatial domain techniques are simple and easy to implement. The Least Significant Bit (LSB) is one of the main techniques in spatial domain image steganography. The transform domain techniques embed the message in the frequency domain of the cover image. Typically, spatial domain techniques are easily detectable [3] and have larger capacity [4]. On the other hand, frequency-based steganography has higher peak signal-to-noise ratio (PSNR) and is more secure [2]. Unfortunately, frequency-based techniques are more complex and require much more computations.

II. LSB BASED IMAGE STEGANOGRAPHY

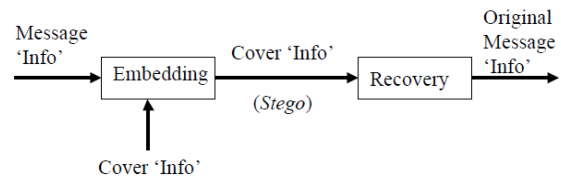


Figure 1: Block diagram of Steganography

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 1011 0011 0010 0111 0101)
(1111 0101 1100 0010 1100 0111)

The underlined bits indicate that the bits were changed from their original value. Only three bits in the cover image were modified. On average about half of the bits in the cover image will be modified when embedding the secret image.

The above LSB method limits the size of the secret data to eighth of the size of the CVR. LSB steganography least n -bits to increase the capacity of the secret information $n/8$ the size of the CVR. However, increasing n distorts stego-image. In each run, we embed random data in the n least significant bits, where $1 \leq n \leq 7$. However, we need to introduce the methods to measure the quality and distortion 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 computed by performing byte by byte comparisons of the CVR and stego-image. The computation can be expressed as follows:

$$MSE = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N (f_{ij} - g_{ij})^2 \quad (1)$$

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 dissimilarity between compared images.

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

Peak signal-to-noise ratio measures in decibels the quality of the stego-image compared with the CVR.

The higher PSNR the better the quality. PSNR is computed using the following equation:

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

For above LSB of two pixels, we compute the three metrics and obtain the following values: MSE=0.5, BER=0.0625, PSNR=51.1dB. Several n -bit LSB steganography techniques were implemented, where $1 \leq n \leq 8$ using Lena [7] images. The image metrics were computed for the images across the various LSB experiments.

The result stego-images are shown in Figure 2-8. Inspecting the images reveal that the distortion is visible for the stego-image for $n \geq 4$. For 8-bit LSB, the image is completely distorted. The results of the image metrics are summarized in Table I.

TABLE I
IMAGE MATRIX FOR DIFFERENT LSB METHOD

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

Examining the results in Table I, we can make the following observations on the data:

The metrics for both images are similar.

• The error metrics (MSE and BER) increases quickly with increased n , especially for $n \geq 5$.

• The image quality indicator 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 carefully balance trade-offs between capacity (i.e., secret size) and imperceptibility (i.e., image distortion). 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 computed for the produced stegoimage. The results show that the produced clown stego-image has good PSNR and small error results. 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.



Figure 2: Stego. For 1-bit hide.



Figure 3: Stego. For 2-bit hide.



Figure 4: Stego. For 3-bit hide.

Cover image

Stego Image



Figure 5: Stego. For 4-bit hide.

Cover image

Stego Image



Figure 6: Stego. For 5-bit hide.

Cover image

Stego Image



Figure 7: Stego. For 6-bit hide.

Cover image

Stego Image



Figure 8: Stego. For 7-bit hide.

IV. CONCLUSION

In this paper, we analyzed the performance of different cases of LSB steganography. We then proposed the 2/3-LSB design which provides good image quality 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 complex random-based LSB mechanisms, as well as optimizing the design speed 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. Jyothisna, 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". [online]. 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/>