An Analysis of Image Steganography Methods

Ms. Shubhangi Hiwe
Dept. of Electronics and Telecommunication Engineering
PVPIT, Bavdhan
University of Pune, Pune, India

Prof. S. I. Nipanikar
Dept. of Electronics and Telecommunication Engineering
PVPIT, Bavdhan
University of Pune, Pune, India

***Abstract*— Steganography means data hiding in images which can be used for covert transmission. This paper presents with hiding text in an image file using Least Significant Bit (LSB) based Steganography, Discrete Cosine Transform (DCT) based steganography, Discrete Wavelet Transform (DWT) based Steganography. Active data concealment ought to end in the extraction of the hidden information from the image with high degree of information integrity. The smallest amount vital bit (LSB) embedding technique suggests that information are often hidden within the least vital bits of image and also the human eye would be unable to note the hidden image within the cover file. The performance and comparison of these three techniques is evaluated on the basis of the parameters like Mean Squared Error (MSE), Peak signal-to-noise ratio (PSNR) and Bit error rate (BER).**

Index terms: Steganography, LSB, DCT, DWT, MSE, PSNR, BER.

I. Introduction

Steganography is the procedure of hiding of a secret message within an ordinary message or image and extracting it to its required destination. Steganography is that the art of invisible communication by concealing information inside different information. The term steganography springs from the Greek and virtually suggests that "covered writing" [1]. A steganography system consists of 3 elements: cover-object (which hides the key message), the key message and therefore the stego-object (which is that the cowl object with message embedded within it.) A digital image is represented employing a 2-D matrix of the color intestines at every grid purpose (i.e. pixel). Typically, grey pictures use eight bits.

The steganography system that uses a picture because the cowl object is remarked as a picture steganography system [2].

The shift from cryptography to steganography is because of that concealing the image existence as stego-images change to implant the key message to hide pictures. Steganography conceptually implies that the message to be transmitted isn't visible to the informal eye. Steganography has been used for thousands of years to transmit knowledge while not being intercepted by unwanted viewers. The most objective of Steganography is especially involved with the protection of contents of the hidden info. Pictures are ideal for information concealment [1, 2] as a result of the big quantity of redundant area is formed within the storing of pictures. In this method, the secret messages are transmitted through unknown cowl carriers in a way that the horribly existence of the embedded messages are not detectable. Carriers embrace images; audio, video, text or the other digitally diagrammatical code or transmission. The hidden message could also be plaintext, cipher text or something which will be diagrammatical as to a small degree stream.

Hiding of data can also be done in the frequency domain. Cover Image is transformed using conventional transformation like DCT, DWT etc. Secret message is embedded in the less significant frequency components of cover image. Mostly frequency domain steganography can be used because of its few applications like it is very secure, undetectable, flexible and has many more techniques for handling of DCT coefficients values.

II. METHODS OF HIDING IN IMAGE STEGANOGRAPHY

For covert communication steganography can be used. The secrete message or information can be embedded into the cover image to obtain the stego image.

There are various methods using which information can be hiding in image steganography. Here different algorithms for proposed embedding and retrieval techniques are discussed.

Almost all data hiding techniques always try to alter immaterial information in the cover image. LSB which means least significant bit insertion is a very common and also a simple approach for embedding the information in a cover image. For example, a simple scheme proposed, is to place the embedding data at the least significant bit of each pixel in the cover image [7, 8, 9]. In steganography, the altered image is called as stego-image. Changing LSB does not change the actual quality of image to human observation but this scheme is sensitive to variety of image processing attacks for example cropping, compression etc. We will be emphasizing more on this technique for the various image formats.

A. The LSB Technique

In the LSB technique of Message hiding, the least significant bit was replaced by the message bit of the secret message. In this paper we evaluated the technique using gray scale images of size 64*64 in which each pixel value was represented with 8 bit representation.

Example:

Let's take an example wherein when the number 300 (representation in binary: 100101100) embedded into the least significant bits of this part of the Cover 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)

1001010**1** 0000110**0** 1100100**0**
1001011**1** 0000111**0** 1100101**1**
1001111**1** 0001000**0** 1100101**0**

After embedding the message into the cover image, the stego image will be obtained, and then this stego image was transformed with the DWT transformation technique so that any hacker can't find where the message was embedded. At the receiver end the inverse DWT is applied, after LSB decryption the original image and message will be obtained. Secrete data can be hide in image the process is called LSB encryption process while retrieving secret data from stego image is called LSB decryption process which is shown in below figure.

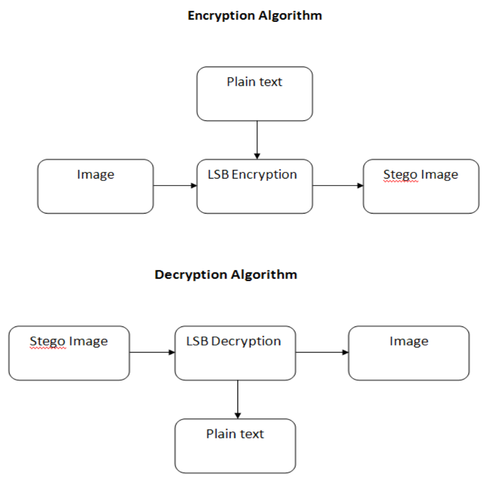

Figure 2.1 LSB Steganography block diagram

1) Algorithm of LSB steganography

1) Embedding

Step1: Read the cover file and text image which need to be hidden in the cover file.
Step2: Convert text message in binary.
Step3: Calculate LSB of each pixels of cover image.
Step4: Replace LSB of cover image with each bit of secret text one by one.
Step5: Get stego image.
Step6: Calculate the mean square Error (MSE), peak signal to noise ratio (PSNR), bit error rate (BER) of the stego image.

2) Extraction

Step1: Read the stego image.
Step2: Calculate LSB of each pixels of stego image.
Step3: Retrieve bits and convert each 8 bit into character.
Step4: Retrieve secret data.

B. Discrete Wavelet Transform (DWT)

The discrete wavelet transform (DWT) is a multiresolution analysis tool with excellent characteristics in the time and frequency domains. The coding efficiency and the quality of image restoration with the DWT are higher than those with the traditional discrete cosine transform.
In Wavelets transformation, the Wavelets are the mathematical functions, defined at a fixed interval. This has an average value of zero which transforms data into different frequency components by representing each component with a resolution matched to its scale.
Here we need to understand the basic idea of the wavelet transform which is to represent any arbitrary function as superposition of a set of such basis functions. Regarding the basic functions which are also called as baby wavelets are acquired from a single prototype wavelet, called as mother wavelet, by dilations or contractions (i.e. scaling) and translations (i.e. shifts).
In DWT steganography secret message can be hidden in cover image this process called encoding while extracting secret data from cover image this process is called decoding.
Detail process of DWT steganography is shown in below figure.

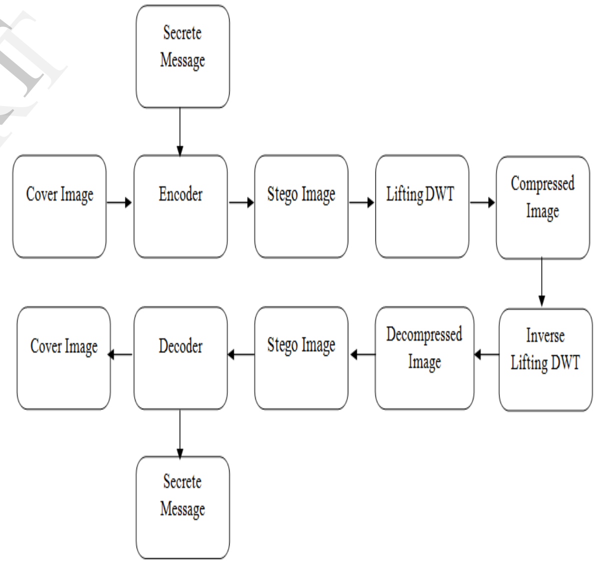

Figure 2.2 DWT Steganography block diagram

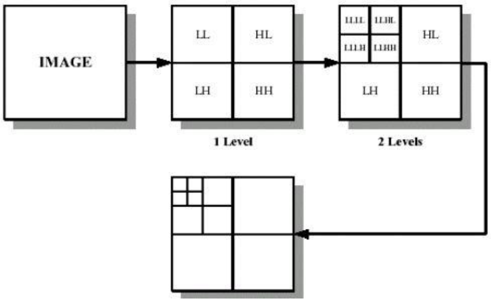

Figure 2.3 2-D DWT for image

1) Algorithm of DWT steganography

1) Embedding

Step1: Read the cover file and text image which need to be hidden in the cover file.
Step2: Convert the text message into binary. Apply 2D-Haar transform on the cover image.
Step3: Obtain the horizontal and vertical filtering coefficients of the cover image. Cover image is added with data bits for DWT coefficient.
Step4: Get stego data.
Step5: Calculate the mean square Error (MSE), peak signal to noise ratio (PSNR), bit error rate (BER) of stego image.

2) Extraction

Step1: Read stego data.
Step2: Obtain the horizontal and vertical filtering coefficients of the cover image. Extract the message bit by bit and recomposing the cover image.
Step3: Convert the data into message vector. Compare it with original message.

C. Discrete Cosine Transform (DCT)

In this DCT based steganography encrypt the text message in least significant bits of the Discrete Cosine (DC) coefficient of digital image.
DCT coefficients are used for JPEG compression. It separates the image into parts of differing importance. It alter signal or image from the spatial domain to the frequency domain. It can separate the image into high, middle and low frequency components.

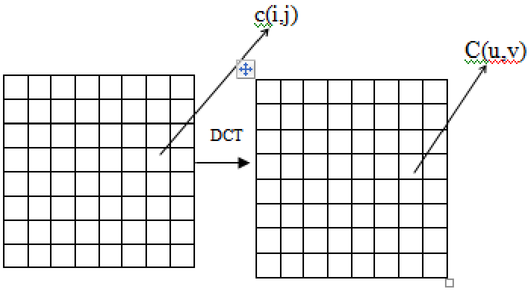

Figure 2.4 Discrete Cosines Transform of an Image

1) Algorithm of DCT steganography

1) Embedding

Step1: Read the cover image.
Step2: Read secret message and convert it in binary.
Step3: The cover image is broken into 8*8 block of pixels.
Step4: Working from left to right, top to bottom subtract 128 in each block of pixels.
Step5: DCT is applied to each block.
Step6: Each block is compressed through quantization table.
Step7: Calculate LSB of each DC coefficient and replace with each bit of secret message.
Step8: Get stego image.
Step9: Calculate the mean square Error (MSE), peak signal to noise ratio (PSNR), bit error rate (BER) of the stego image.

2) Extraction

Step1: Read stego image.
Step2: Stego image is broken into 8*8 block of pixels.
Step3: Working from left to right, top to bottom subtract 128 in each block of pixels.
Step4: DCT is applied to each block.
Step5: Each block is compressed through quantization table.
Step6: Calculate LSB of each DC coefficients.
Step7: Retrieve and convert each 8 bit into character.

III. ANALYSIS

Here we are introducing the methods to measure the quality and distortion in images.

To measure imperceptibility of steganography several metrics are used. To compare stego image and cover results needs a measure of image quality, usually used measures are mean squared error (MSE), peak signal to noise ratio (PSNR) and bit error rate (BER).

1) Mean Squared Error :

Mean Squared Error (MSE) can be calculated by performing byte by byte assessment of the cover file and stego-image. The calculation can be shown as follows:

$$MSE = \frac{1}{M \times N} \sum_1^M \sum_1^N (f_{ij} - g_{ij})^2$$

From above equation M, N are the number of rows and columns in the Cover image (CVR) matrix, fij is the pixel value from CVR, and gij is the pixel value from the stego-image. Higher value of MSE indicates dissimilarity between compared images.

2) Bit Error Rate :

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

3) Peak signal-to-noise Ratio:

Peak signal-to-noise ratio measures in decibels the quality of the stego-image compared with the cover file.
The higher PSNR the better the quality. The PSNR is computed using the following equation.

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

PSNR is a good measure for comparing restoration results for the same image.

IV. RESULT

1) Output result of LSB steganography

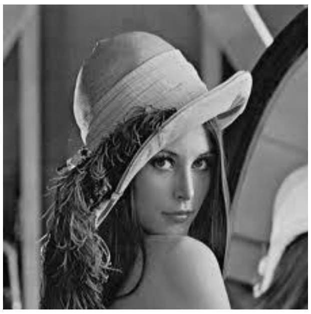

Figure 4.1 Carrier Image

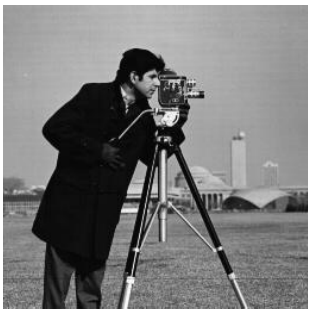

Figure 4.2 Image to hide

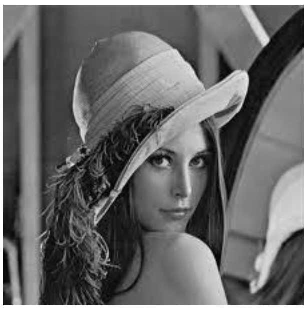

Figure 4.3 Stego Image

2) Output result of DWT steganography

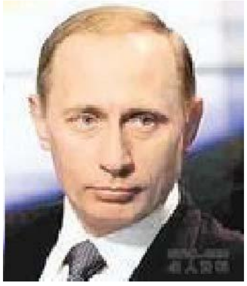

Figure 4.4 Cover Image

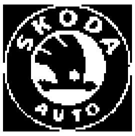

Figure 4.5 Image to hide

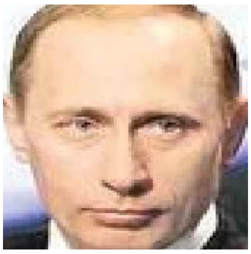

Figure 4.6 Cropped stego image after performing IDWT of embedding process

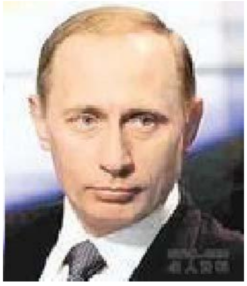

Figure 4.7 Final stego image

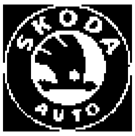

Figure 4.8 Retrieved image

V. CONCLUSION

Steganography is the method of writing hidden message or text in such a way that no one can suspect the existence of message other than sender and intended receiver. In this paper, analysis of LSB, DCT & DWT methods can be successfully implemented and results can be delivered. Comparative analysis of LSB based, DCT based & DWT based steganography has been done on basis of parameters like PSNR, MSE, BER on different images and the results are evaluated. An embedding algorithm is said to be robust if the embedded message can be extracted after the image has been manipulated without being destroyed. DWT is a highly robust method in which the image is not destroyed on extracting the message hidden in it and provides maximum security.

REFERENCES:

[1] Pfitzmann Birgit. Information Hiding Terminology, First International Workshop, Cambridge, UK, Proceedings, Computer Science, 1174. pp. 347-350, May–June.
pp. 61- 76, 1999.

[2] Westfield Andreas and Andreas Pfitzmann, Attacks on Steganographic Systems, Third International Workshop, IH'99 Dresden Germany, October Proceedings, Computer Science 1768.

[3] Moerland, T., "Steganography and Steganalysis", *Leiden Institute of Advanced Computing Science*,Silman, J., "Steganography and Steganalysis: An Overview", *SANS Institute*, 2001 Jamil, T. 18:01, 1999

[4] Wei Zhang,ZheJiang,ZhiyuGao, and YanyanLiu,"An efficient VLSI architecture for Lifting based discrete wavelet transform,"IEEETrans.Circuits and systems,vol.59,NO.3,pp. 158-162,Mar.2012.

[5] G. Xing, J. Li, and Y. Q. Zhang, "Arbitrarily shaped videoobject coding by wavelet," IEEE Trans. Circuits Syst. Video Technol., vol. 11, no. 10,pp. 1135–1139, Oct. 2001.

[6] S. C. B. Lo, H. Li, and M. T. Freedman, "Optimization of wavelet decomposition for image compression and feature preservation," IEEE Trans.Med. Imag., vol. 22, no. 9, pp. 1141–1151, Sep. 2003.

[7] K. K. Parhi and T. Nishitani, "VLSI architecture for discrete wavelet transforms," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 1, no. 2, pp. 191–202, Jun. 1993.

[8] X. X. Qin and M. Wang, "A review on detection of LSB matching steganography," *Inf. Technol. J.*, vol. 9, pp. 1725–1738, 2010.

[9] A. D. Ker, "Locating steganographic payload via WS residuals," in*ACM Proc. 10th Multimed. Secur. Workshop*, 2008, pp. 27–31.

[10] A. D. Ker, "A general framework for the structural steganalysis of LSBreplacement," in *Proc. 7th Inf. Hiding Workshop, ser. Springer LNCS*,
2005, vol. 3727, pp. 296–311.

[11] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB steganography in color and grayscale images," *IEEE Multimedia*, vol. 8, no. 4, pp. 22–28, 2001.

[12] S. Dumitrescu, X.Wu, and Z.Wang, "Detection of LSB steganography via sample pair analysis," *IEEE Trans. Signal Process.*, vol. 51, pp.1995–2007, Jun. 2003.

[13] A. Ker, "Steganalysis of LSB matching in grayscale images," *Signal Process. Lett.*, vol. 12, no. 6, pp. 441–444, Jun. 2005.

[14] J. Fridrich and M. Goljan, "On estimation of secret message length in LSB steganography in spatial domain," in *Secur.,Steganogr. WatermarkingofMultimed. Contents VI, ser. Proc. SPIE*, 2004, vol. 5306,pp. 23–34

[15] www.iosrjournals.org/iosr-jeee/Papers/Vol6-issue1/G0614148.pdf

[16] www.slideshare.netmohit4ugoela-novel-steganographic-technique-based-on-lsb-dct-approach-by-mohit-goel