

# A Steganography Implementation based on LSB & DCT

**Gurmeet Kaur\* and Aarti Kochhar\*\***

\*Department of Electronics and Communication Engineering, CEM Kapurthala.

\*\*Department of Electronics and Communication Engineering, DAVIET Jalandhar

(Received 05 November 2012 Accepted 16 November 2012)

**Abstract**—In recent years, Steganography and Steganalysis are two important areas of research that involve a number of applications. These two areas of research are important especially when reliable and secure information exchange is required. Steganography is an art of embedding information in a cover image without causing statistically significant variations to the cover image. Steganalysis is the technology that attempts to defeat Steganography by detecting the hidden information and extracting. In this paper a comparative analysis is made to demonstrate the effectiveness of the proposed methods. The effectiveness of the proposed methods has been estimated by computing Mean square error (MSE) and Peak Signal to Noise Ratio (PSNR), Processing time, security. The analysis shows that the BER and PSNR is improved in the LSB Method but security sake DCT is the best method.

**Index Terms**— Steganography, Discrete Cosine Transform (DCT), LSB (Least Significant bit).

## I. INTRODUCTION

An important aspect of the modern way of life is communication. Many devices present today have the ability to transmit various information between themselves using different ways of communication, like insecure public networks, different types of wireless networks and the most used: the Internet. In some cases it is needed to keep the information travelling through different kinds of channels secret. Mainly there are two ways of concealing information: cryptography and steganography. Cryptography's main aspect is that the information is somehow distorted, scrambled by the sender using normally an encryption key also known only by the intended receiver who decrypts the message. The problem with cryptography is that a user intercepting the message, although he cannot decrypt it, he might detect that there is encrypted, secret information. On the other hand steganography is able even to

hide this aspect making sure that even the fact that there is secret information, is concealed. Steganography's main aspect is

that it is embedding the secret message into another message. The basic structure of Steganography is made up of three components: the “carrier”, the message, and the key.

## IMAGE STEGANOGRAPHY TECHNIQUES

Based on the analyses of steganography tools' algorithms, we partition these tools into two categories:

- (1). Spatial domain based steganography
- (2) Transform domain based steganography

**Spatial Domain Based Steganography:** Spatial steganography mainly includes LSB (Least Significant Bit) steganography. Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image. The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message.

Pixel: (10101111 11101001 10101000)  
(10100111 01011000 11101001)  
(11011000 10000111 01011001)  
Secret message: 01000001

Result: (10101110 11101001 10101000)  
 (10100110 01011000 11101000)  
 (11011000 10000111 01011001)



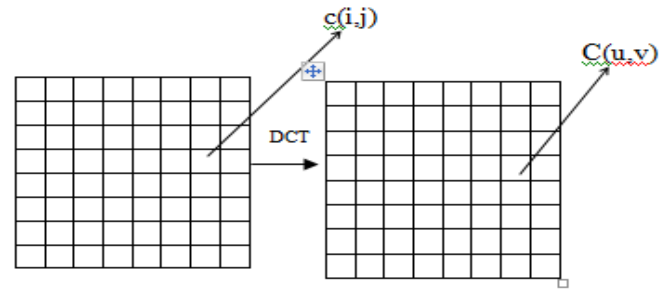
Cover image



stego image

**Transform Domain Based Steganography:** Basically there are many kinds of power level transforms that exist to transfer an image to its frequency domain, some of which are Discrete Cosine Transform, KL Transform and Wavelet Transform.

**The Discrete Cosine Transform (DCT):** This method is used, but similar transforms are for example the Discrete Fourier Transform (DFT). These mathematical transforms convert the pixels in such a way as to give the effect of “spreading” the location of the pixel values over part of the image [5]. The DCT transforms a signal from an image representation into a frequency representation, by grouping the pixels into  $8 \times 8$  pixel blocks and transforming the pixel blocks into 64 DCT.



DCT is used in steganography as- Image is broken into  $8 \times 8$  blocks of pixels. Working from left to right, top to bottom, the DCT is applied to each block. Each block is compressed through quantization table to scale the DCT coefficients and message is embedded in DCT coefficients.

## II.RELATED WORK

Vignesh Kumar Munirajan, Eric Cole, Sandy Ring in Steganography is a means of data hiding in images for covert transmission. Though steganography aims at transmitting images without visual degradation or changes for a naked observer, it cannot dispense with altering spatial and transform level details in order to embed the data [1, 2, 3]. Even though these alterations may not be captured by visual observation, they do manifest themselves for detailed analysis. In this paper we analyze a Fuzzy logic based technique that could be applied

for detaining images with steganography. The images we are looking at are JPEG images and the data. T. Morkel, J.H.P. Eloff, M.S. Olivier[6] give an overview of image steganography, its uses and techniques. It also attempts to identify the requirements of a good steganographic algorithm and briefly reflects on which steganographic techniques are more suitable for which applications.

Ken Cabeen and Peter Gent [1] have discussed the mathematical equations of Discrete Cosine Transform (DCT) and its uses in image compression. Andrew B.

Watson [2] has discussed Discrete Cosine Transform (DCT) technique for converting a signal into elementary frequency component. He developed simple function to compute DCT and show how it is used for image compression. Jessica Fridrich [3] have discussed a reliable and accurate method for detecting least significant bit (LSB) non sequential embedding in digital images. The secret message length is derived by inspecting the lossless capacity in the LSB and shifted LSB plane. Mohesen Ashourian, R.C. Jain and Yo-Sung Ho [4] have proposed a data hiding scheme to embed a signature image in the host image. They selected a gray scale host image of  $512 \times 512$  pixels and signature image of  $256 \times 256$  pixels. They developed image data hiding scheme on dithered quantization and a modified baseline JPEG coding scheme. A test of system performance has been done by JPEG compression, addition of Gaussian noise, and Gaussian and Median filtering of host image. J.R.Krenn [5] has proposed a method to embed message in LSB of DC coefficients of cover image. He proposed a simple pseudo-code algorithm to hide a message inside

Hao-tian Wu, Jiwu Huang [9] in steganographic algorithm is proposed for JPEG Image by modifying the block DCT coefficients. Firstly, an embedding algorithm called LSB+ matching is generated to approximately preserve the marginal distribution of DC coefficients. We further divide the DCT coefficients into four frequency bands, including the direct current (DC), low frequency, middle-frequency, and high-frequency. Via matrix encoding, low data hiding rate and high embedding efficiency are achieved in high-frequency band, while the hiding rate is increased in the middle-frequency and DC bands, and highest in the low-frequency band. In addition, a coefficient selection strategy is employed to make the hidden message less detectable. The proposed algorithm is

implemented on a set of 10000 images and tested with four steganalytic algorithms.

Mamta Juneja, Parvinder Singh Sandhu [11] represented Robust image steganography technique based on LSB (Least Significant Bit) insertion and RSA encryption technique. Steganography is

the term used to describe the hiding of data in images to avoid detection by attackers. Steganalysis is the method used by attackers to determine if images have hidden data and to recover that data. The application discussed in this paper ranks images in a users library based on their suitability as cover objects for some data. By matching data to an image, there is less chance of an attacker being able to use steganalysis to recover the data. Before hiding the data in an image the application first encrypts it. The steganography method proposed in this paper and illustrated by the application is superior to that used by current steganography tools.

Yi-zhen Chen, Zhi Han, Shu-ping Li, Chunhui Lu, Xiao-Hui Yao [13] an improved adaptive steganography algorithm—SVBA algorithm, which fully analyzes the statistical properties and adopts HVS features. SVBA algorithm first divides the image into  $8 \times 8$  blocks and analyzes the mean, variance and entropy value of grey by block, then sets a sensitivity vector for each block with considering HVS features and adjusts the steganography schema dynamically according to the block sensitivity vectors. Simulation experiment results on Matlab7.0 shows this algorithm has a balanced performance on efficiency, capacity, imperceptibility and robustness., Mohammad Javad Khosravi, Samaneh Ghandali [20] novel steganography technique based on the combination of a secret sharing method and wavelet transform is presented. In this method, a secret image is shared into some shares. Then, the shares

and Fletcher-16 checksum of shares are hidden into cover images using an integer wavelet based steganography technique.

### III. MODEL

#### A. Definitions

(i) *Cover image*: It is defined as the original image into which the required information is embedded. It is also termed as carrier image. The information should be embedded in such a manner that there are no significant changes in the statistical properties of the cover image.

(ii) *Stegoimage*: It is an unified image obtained by the combination of the payload and cover image.

(iii) *Perceptibility*: It describes the ability of a third party (not the intended recipient) to visually detect the presence of hidden information in the stego image. The embedding algorithm is imperceptible when used on a particular image if an innocent third party, interested in the content of the cover image, is unaware of the existence of the payload. Essentially this requires that the embedding process not degrade the visual quality of the cover image.

(iv) *Robustness*: It characterizes the ability of the payload to survive the embedding and extraction process, even in the face of manipulations of the stego image such as filtering, cropping, rotating and compression.

(v) *Security*: It is inability of adversary to detect hidden images accessible only to the authorized user. The quality factor can enhance the security of the image. A steganographic image is perfectly secure when statistical data of the cover and stego images are identical.

#### B. Error Analysis:

(i) *Bit Error Rate*: For the successful recovery of the hidden information the communication channel must be ideal but for the real communication channel, there will be error while retrieving hidden information and this is measured by BER. The cover image is represented as cov and stego image as steg in the given equation

$$BER = \frac{1}{|image^{covg}|} \sum_{i=0}^{allpixels} |image^{covg} - image^{steg}|$$

Where  $i$  is the pixel position

(ii) *Mean Square Error*: It is defined as the square of error between cover image and the stego image. The distortion in the image can be measured using MSE.

$$\sum_{i=1}^{allpixels} \sum_{j=1}^{allpixels} \frac{(cov(i,j) - steg(i,j))^2}{N * N}$$

(iii) *Peak Signal to Noise Ratio*: It is the ratio of the maximum signal to noise in the stego image.

$$PSNR = 20 \log_{10} \frac{255}{\sqrt{MSE}}$$

### IV ALGORITHMS OF STEGANOGRAPHY

#### A. Lsb Based Steganography

Algorithm to embed text message:-

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

Step 2: convert the color image into grey image.

Step 3: Convert text message in binary.

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

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

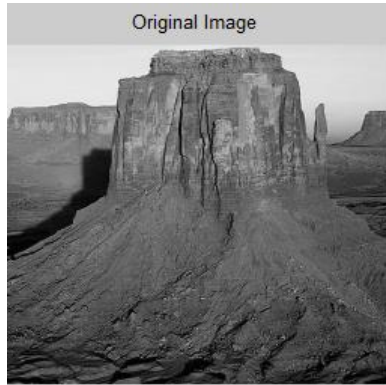
Step 6: Write stego image

Algorithm to retrieve text message:-

Step 1: Read the stego image.

Step 2: Calculate LSB of each pixels of stego image.

Step 3: Retrieve bits and convert each 8 bit into character.



Step 3: The cover image is broken into  $8 \times 8$  block of pixels.

Step 4: Working from left to right, top to bottom subtract 128 in each block of pixels.

Step 5: DCT is applied to each block.

Step 6: Each block is compressed through quantization table.

Step 7: Calculate LSB of each DC coefficient and replace with each bit of secret message. Step 8: Write stego image.

Algorithm to retrieve text message:-

Step 1: Read stego image

Step 2: Stego image is broken into  $8 \times 8$  block of pixels.

Step 3: Working from left to right, top to bottom subtract 128 in each block of pixels.

Step 4: DCT is applied to each block.

Step 5: Each block is compressed through quantization table.

Step 6: Calculate LSB of each DC coefficient



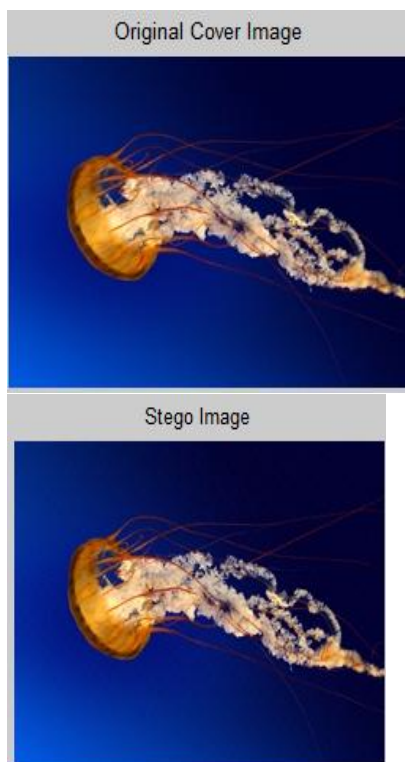
### *B. DCT Based Steganography*

Algorithm to embed text message:-

Step 1: Read cover image.

Step 2: Read secret message and convert it in binary.





## V PERFORMANCE & RESULTS

The analysis of LSB based and DCT based steganography has been done on basis of parameters like PSNR, MSE, Processing time, security. PSNR computes the peak signal to noise ratio, in decibels, between two images. This ratio is used as a quality measurement between two images. If PSNR ratio is high then images are best of quality

Method	Picture name	PSNR	MSE	PROCESSING TIME	SIZE OF COVER IMAGE
LSB	DESERT	51.1109	0.5035	0.133777 seconds	256X256
LSB	JELLYFISH	51.1109	0.4993	0.084754 seconds	256X256
DCT	DESERT	40.6735	5.5684	1.0140 seconds	256X256
DCT	JELLYFISH	39.3983	7.4687	1.3260 seconds	256X256

Table1: simulation results for LSB & DCT Method

Features	LSB	DCT
Invisibility	Low	High
Payload capacity	High	Medium
Robustness against statistical attacks	Low	High
Robustness against image manipulation	Low	Medium
Independent of file format	Low	Medium
PSNR	High	Medium
MSE	Less	Medium

Table 2: Parameters analysis of both steganography methods

## IV. CONCLUSION

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. It is therefore a book on magic. It is emerging in its peak because it does not attract anyone by itself. In this paper aanalysis of LSB & DCT methods has been successfully implemented and results are delivered. The MSE and PSNR of the methods are also compared and also this paper presented a background discussion and implementation on the major algorithms of steganography deployed in digital imaging. From the results it is clear that as PSNR inLSB is the best but as we know that security is much more important in today's communication system. So security wise DCT is the best.

## REFERENCE

- [1] Anil K Jain, "Fundamentals of Digital Image Processing", University of California-Davis, Prentice Hall, 1988
- [2] Ken Cabeen and Peter Gent, —Image Compression and Discrete Cosine Transforml, College of Redwoods.  
<http://online.redwoods.cc.ca.us/instruct/darnold/LAPROJ/Fall98/PKen/dct.pdf>

[3] Chang, C.C., Chen, T.S. and Chung, L.Z., "A steganographic method based upon JPEG and quantization table modification", Information Sciences, 2002, 141(1-2), pp.123-38.

[4]T. Morkel, J.H.P. Eloff , M.S. Olivier,"An Overview of Image Steganography," in *Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005)*, Sandton, South Africa, June/July 2005 .

[5] Ankur M. Mehta, Steven Lanzisera, and Kristofer S. J. Pister, "Steganography 802.15.4 Wireless Communication".

[6] K Suresh Babu, K B Raja, Kiran Kumar K, Manjula Devi T H, Venugopal K R, L M Patnaik,"Authentication of Secret Information in Image Steganography" Microprocessor Applications Laboratory, Indian Institute of Science,Bangalore

[7] Proceedings of the 2006 International Conference on "Intelligent Information Hiding and Multimedia Signal Processing "(IIH-MSP'06)0-7695-2745-0/06 © 2006 IEEE.

[8] Asghar Shahrzad Khashandarag and Naser Ebrahimian, "A new method for color image steganography using SPIHT and DCT, sending with JPEG format", International Conference on Computer Technology and Development, IEEE, 2008

[9] CHEN Zhi-li, HUANG Liu-sheng, YU Zhen-shan, LI Ling-jun and YANG wei, "A Statistical Algorithm for Linguistic Steganography Detection Based on Distribution of Words", 3<sup>RD</sup> International Conference on Availability, Reliability and Security, IEEE, 2008..

[10] K Suresh Babu, K B Raja, Kiran Kumar K, Manjula Devi T H, Venugopal K R, L M Patnaik, "Authentication of Secret Information in Image Steganography" Microprocessor Applications Laboratory, Indian Institute of Science, Bangalore in 2008

[11] Mamta Juneja Parvinder Singh Sandhu, "Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption"2009 International Conference on Advances in Recent Technologies in Communication and Computing.

[12]KokSheik Wong, Xiaojun Qi, and Kiyoshi Tanaka, —A DCT based Mod4 Steganography Method| Signal Processing 87, 1251-1263, 2009.

Z

[13] Yi- Zhen Chen, Zhi Han, Shu-ping Li, Chun-hui Lu, Xiao- Hui Yao , "An Adaptive Steganography Algorithm Based on Block Sensitivity Vectors Using HVS Features " 2010 3rd International Congress on Image and Signal Processing.

[14] James Cane, TheoYi- zhen Chen, Zhi Han, Shu-ping Li, Chun- hui Lu, Xiao- Hui Yao , "An Adaptive Steganography Algorithm Based on Block Sensitivity Vectors Using HVS Feature" 2010 3rd International Congress on Image and Signal Processing.

[15].Adel Almohammad, Gheorghita Ghinea, "Image Steganography and Chrominance Components" 2010 10th IEEE International Conference on Computer and Information Technology (CIT 2010)

[16] Jinsuk Baekl, Cheonshik Kim, Paul S. Fisherl, and Hongyang Cha0, "(N. I) Secret Sharing Approach Based on Steganography with Gray Digital Images." 978-1-4244-5849-3/10/ ©20 1 0 IEEE

[17] Suhaila Abd Halim and Muhammad Faiz Abdullah Sani , "Embedding Using Spread Spectrum ImageSteganography with GF)"Proceedings of the 6th IMT-GT Conference on Mathematics, Statistics and its Applications (ICMSA2010)

[18] Tetsuya Kojima , Yoshiya Horii , "A Steganography Based on CT-CDMA Communication Scheme Using Complete Complementary Codes"arXiv:1001.2623v1 [cs.IT] 15 Jan 2010

[19] T. Morkel, J.H.P. Eloff, M.S. Olivier, "Information and Computer Security Architecture (ICSA) Research Group".

[20]Edward Neuman, —MATLAB Tutorials|, Department of Mathematics, Board of Trustees, Southern Illinois University