An Analysis of LSB & DCT based Steganography

Dr. Ekta Walia [a], Payal Jain [b], Navdeep [c]

GJCST Computing Classification
F.2.1 & G.2.m

***Abstract*- This paper presents analysis of Least Significant Bit (LSB) based Steganography and Discrete Cosine Transform (DCT) based Steganography. LSB based Steganography embed the text message in least significant bits of digital picture. Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover file. Unfortunately, it is vulnerable to even a small image manipulation. Converting an image from a format like GIF or BMP, which reconstructs the original message exactly (lossless compression) to a JPEG, which does not (lossy compression), and then back could destroy the information hidden in the LSBs. DCT based Steganography embed the text message in least significant bits of the Discrete Cosine (DC) coefficient of digital picture. When information is hidden inside video, the program hiding the information usually performs the DCT. DCT works by slightly changing each of the images in the video, only to the extent that is not noticeable by the human eye. An implementation of both these methods and their performance analysis has been done in this paper.**

Keywords- Least Significant Bit (LSB), Discrete Cosine Transform (DCT), Steganography

I INTRODUCTION

Steganography comes from the Greek words Steganós (Covered) and Graptos (Writing). Steganography in these days refers to information or a file that has been concealed inside a digital picture, video or audio file. If a person or persons view the object that the information is hidden inside, he or she will have no idea that there is any hidden information; therefore the person will not attempt to decrypt the information.

[a] Professor, Department of Information and Technology, Maharishi Markandeshwar College of Engineering Maharishi Markandeshwar University, Mullana, Ambala(Haryana)
E-mail: wekta@yahoo.com, Tel No: 91-9416551292[a]
[b] Lecturer, Department of Information and Technology, Maharishi Markandeshwar College of Engineering Maharishi Markandeshwar University, Mullana, Ambala (Haryana)
payaljain2006@gmail.com[b], Tel No: 91-9466742552[b]
[c]Student, Department of Information and Technology, Maharishi Markandeshwar College of Engineering Maharishi Markandeshwar University, Mullana, Ambala(Haryana)

A. Steganographic Techniques

i. Physical Steganography

Physical Steganography has been widely used. In ancient time people wrote message on wood and then covered it with wax. Message was written on the back of postage stamps. Message was written on paper by secret inks.

ii. Digital Steganography

Digital Steganography is the art of invisibly hiding data within data. It conceals the fact that message exists by hiding the actual message. In this, secret data can be hidden inside the image, text, sound clip which can be represented in binary.

iii. Printed Steganography

Digital Steganography output can be in the form of printed documents. The letter size, spacing and other characteristics of a cover text can be manipulated to carry the hidden message. A recipient who knows the technique used can recover the message and then decrypt it.

II METHODS OF CONCEALING DATA IN DIGITAL IMAGE

A. Least Significant Bit (Lsb)

LSB is the lowest bit in a series of numbers in binary. e.g. in the binary number: 10110001, the least significant bit is far right 1.
The LSB based Steganography is one of the steganographic methods, used to embed the secret data in to the least significant bits of the pixel values in a cover image. e.g. 240 can be hidden in the first eight bytes of three pixels in a 24 bit image.

PIXELS:	(00100111 11101001 11001000)
	(00100111 11001000 11101001)
	(11001000 00100111 11101001)
240 :	011110000
RESULT:	(00100110 11101001 11001001)
	(00100111 11001001 11101000)
	(11001000 00100110 11101000)

Here number 240 is embedded into first eight bytes of the grid and only 6 bits are changed.

B. *Discrete Cosine Transform (Dct)*

DCT coefficients are used for JPEG compression. It separates the image into parts of differing importance. It transforms a signal or image from the spatial domain to the frequency domain. It can separate the image into high, middle and low frequency components.

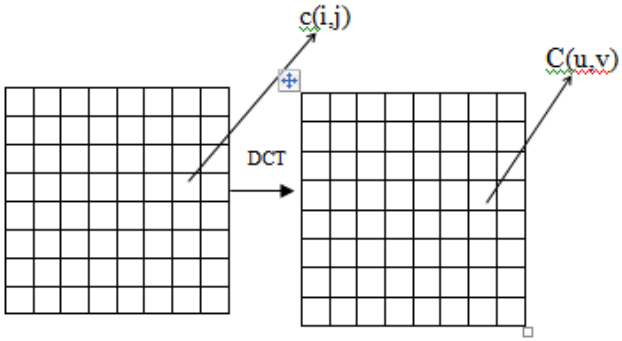


Fig. I Discrete Cosine Transform of An Image

The general equation for a 1D (N data items) DCT is defined by the following equation:

$$C(u) = \alpha(u)\sum_{x=0}^{N-1} f(x)\cos\left[\frac{(2x+1)u\pi}{2N}\right] \quad (1)$$

for u = 0, 1, 2, . . . , N-1.

The general equation for a 2D (*N* by *M* image) DCT is defined by the following equation:

$$C(u,v) = \alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{(2x+1)u\pi}{2N}\right]\cos\left[\frac{(2y+1)v\pi}{2N}\right] \quad (2)$$

for u,v = 0, 1, 2, . . . , N-1

Here, the input image is of size N X M. c(i, j) is the intensity of the pixel in row i and column j; C(u,v) is the DCT coefficient in row u and column v of the DCT matrix.

Signal energy lies at low frequency in image; it appears in the upper left corner of the DCT. Compression can be achieved since the lower right values represent higher frequencies, and generally small enough to be neglected with little visible distortion.

DCT is used in steganography as-

Image is broken into 8×8 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.

III LITERATURE SURVEY

A lot of Research has been carried out on Steganography because it is important to know how much data can be concealed without image distortion. Their description is as follows:

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 et. al [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 512×512 pixels and signature image of 256×256 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 a JPEG image. Ren-Junn Hwang et. al[6] have proposed data hiding based on JPEG technique. They proposed a method of compressing the stego image by lossy compression method to reduce the image size. The receiver then extracts complete data correctly from lossy compressed image.

H. W. Tseng and C. C. Chang *[7]* have proposed a novel high capacity data hiding method based on JPEG. They proposed a method that employs a capacity table to estimate the number of bits that can be hidden in each DCT component so that significant distortions in the Stego-image can be avoided. Youngran Park et. al *[8]* have proposed a new image steganography method to verify whether the secret information had been deleted, forged or changed by attackers. They proposed a method that hides the secret information into special domain of digital image. Neeta Deshpande et. al *[9]* have embedded data in least significant bits of cover image. They explained the LSB embedding technique and presented the evaluation results. Aneesh Jain and Indranil Sengupta *[10]* have proposed a scheme, which hides data in bitmap images, in a way that there is almost no perceptible difference between the original image and new image, and this is also resistant to JPEG compression. M. Chaumont and W. Puech *[11]* have proposed a method to hide the color information in a compressed grey-level image, allow free access to the compressed gray level image, and give color image access only if you own a secret key. KokSheik Wong, Xiaojun Qi, and Kiyoshi Tanaka *[12]* have proposed Mod4 steganography method in discrete cosine transform (DCT) domain. Mod4 is capable of embedding information into both uncompressed and JPEG compressed image. Takayuki Ishida et. al *[13]* have discussed a modified QIM-JPEG2000 steganography which improve the previous JPEG2000 steganography using quantization index modulation (QIM).

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 text message in binary.
Step 3: Calculate LSB of each pixels of cover image.
Step 4: Replace LSB of cover image with each bit of secret message one by one.
Step 5: 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.

B. *DCT Based Steganography*

Algorithm to embed text message:-
Step 1: Read cover image.
Step 2: Read secret message and convert it in binary.
Step 3: The cover image is broken into 8×8 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 8×8 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.
Step 7: Retrieve and convert each 8 bit into character.

V PERFORMANCE & RESULTS

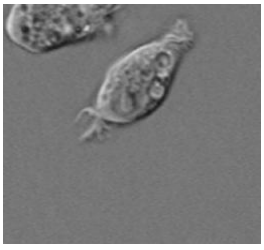
Comparative analysis of LSB based and DCT based steganography has been done on basis of parameters like PSNR. Both grayscale and colored images have been used for experiments. Peak signal to noise ratio is used to compute how well the methods perform.
PSNR computes the peak signal to noise ratio, in 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.

$$PSNR(x,y) = \frac{10\log_{10}(\max(\max(x),\max(y))^2}{|x-y|^2}$$

A. *LSB Based Steganography*

Fig. II Original Cameraman.bmp **Fig III Stego cameraman.bmp**

PSNR between Fig II and Fig III = 51.0870 dB



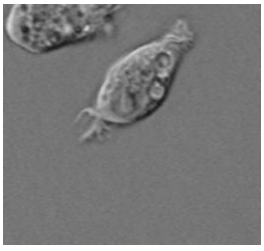
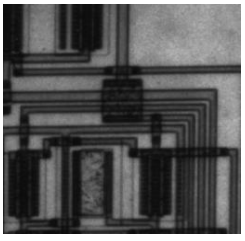


Fig. IV Original cell.bmp **Fig. V Stego cell.bmp**

PSNR between Fig. IV and Fig. V = 49.7214 dB



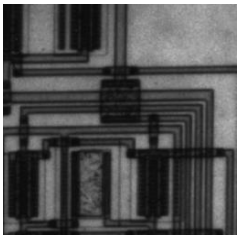


Fig. VI Original circuit.bmp **Fig . VII Stego circuit.bmp**

PSNR between Fig. VI and Fig.VII = 48.3476 dB

i. Using Color Images

Fig .VIII Original army.bmp **Fig. IX Stego army.bmp**

PSNR between Fig VIII and Fig IX =51.0872 dB


Fig .X Original lasercolor.bmp **Fig .XI Stego lasercolor.bmp**

PSNR between Fig X and Fig XI = 51.0881 dB


Fig. XII Original kufte.bmp **Fig. XIII Stego kufte.bmp**

PSNR between Fig XII and Fig XIII = 51.0451 dB

B. DCT Based Steganography

i. Using Grayscale Images


Fig. XIV Original cameraman.bmp **Fig. XV Stego cameraman.bmp**

PSNR between Fig XIII and Fig. XIV = 55.3865 dB


Fig. XVI Original coins.bmp **Fig. XVII Stego coins.bmp**

PSNR between Fig. XVI and Fig. XVII = 55.3049 dB

ii. Using Color Images


Fig. XVIII Original army.bmp **Fig. XIX Stego army.bmp**

PSNR between Fig. XVIII and Fig. XIX = 57.2172 dB


Fig. XX Original ilexvert.bmp **Fig. XXI Stego ilexvert.bmp**

PSNR between Fig. XX and Fig. XXI = 57.0530 dB

VI Conclusion

LSB based steganography embed the text message in LSB of cover image. DCT based steganography embed the text message in LSB of DC coefficients. This paper implements LSB based steganography, DCT based steganography and computes PSNR ratio. PSNR is 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 better of quality. Comparison of LSB based and DCT based stego images using PSNR ratio shows that PSNR ratio of DCT based steganography scheme is high as compared to LSB based steganography scheme for all types of images- (Grayscale as well as Color). DCT based steganography scheme works perfectly with minimal distortion of the image quality as compared to LSB based steganography scheme. Even though the amount of secret data that can be hidden using this technique is very small as compared to LSB based steganography scheme still, DCT based steganography scheme is recommended because of the minimum distortion of image quality.

VII References

1) Ken Cabeen and Peter Gent, "Image Compression and Discrete Cosine Transform", College of Redwoods. *http://online.redwoods.cc.ca.us/instruct/darnold/LAPROJ/Fall98/PKen/dct.pdf*

2) Andrew B. Watson, "Image Compression Using the Discrete Cosine Transform", NASA Ames Research Center , Mathematica Journal, 4(1), p.81-88,1994
3) Jessica Fridrich, Miroslav Goljan, and Rui Du, "Detecting LSB Steganography in Color and Gray-Scale Images", Magazine of IEEE Multimedia, Special Issue on Multimedia and Security, pp.22-28, October-December 2001.
4) Mohesen Ashourian, R.C. Jain and Yo-Sung Ho, *"Dithered Quantization for Image Data Hiding in the DCT domain"*, in proceeding of IST2003, pp.171-175, 16-18 August, 2003 Isfahan Iran.
5) J.R.Krenn, "Steganography and Steganalysis", January 2004.
6) Ren-Junn Hwang, Timothy K. Shih, Chuan-Ho Kao, *"A Lossy Compression Tolerant Data Hiding Method Based on JPEG and VQ."* Journal of Internet Technology Volume 5(2004).
7) Hsien – Wen Tseng and Chin – Chen Chang, " High Capacity Data Hiding in JPEG Compressed Images", Informatica, Volume 15 , Issue 1 (January 2004) 127-142, 2004,0868-4952
8) Youngran Park, Hyunho Kang, Kazuhiko Yamaguchi and Kingo Kobayashi, "Integrity Verification of Secret Information in Image Steganography", Symposium on Information Theory and its Applications, Hakodate, Hokkaido, Japan, 2006.
9) Neeta Deshpande, Kamalapur Sneha, Daisy Jacobs, "Implementation of LSB Steganography and Its Evaluation for various Bits" Digital Information Management, 2006 1st International Conference on. 06/01/2007; DOI: 10.1109/ICDIM.2007.369349
10) Aneesh Jain, Indranil Sen Gupta, "A JPEG Compression Resistant Steganography Scheme for Raster Graphics Images", TENCON 2007 - 2007 IEEE Region 10 Conference, vol.2
11) M. Chaumont and W. Puech, "DCT-Based Data Hiding Method To Embed the Color Information in a JPEG Grey Level Image", 14th European Signal Processing Conference (EUSIPCO 2006), Florence, Italy, September 4-8, 2006, copyright by EURASIP
12) KokSheik Wong, Xiaojun Qi, and Kiyoshi Tanaka, "A DCT based Mod4 Steganography Method" Signal Processing 87, 1251-1263, 2007.
13) Takayuki Ishida, Kazumi Yamawaki, Hideki Noda, Michiharu Niimi, *"Performance Improvement of JPEG2000 Steganography Using QIM"*, Department of System Design and Informatics, Journal of Communication and Computer, ISSN1548-7709, USA, Volume 6, No. 1(Serial No. 50), January 2009.
14) Edward Neuman, "MATLA B Tutorials", Department of Mathematics, Board of Trustees, Southem Illinois University,
15) [15] Rafael C. Gonzalez, Richard E. Woods, "Digital Image Processing", 2nd Edition.