International Journal of Emerging Trend in Engineering and Basic Sciences (IJEEBS)
I *SSN (Online)* 2349-6967
Volume 2 , Issue 1(Jan-Feb 2015), PP31-36

Least Significant Bit (LSB) and Discrete Cosine Transform (DCT) based Steganography

Smruti Ranjan Gouda
(Dept. Of computer Science & Engineering, Asst. Professor, Gandhi Group of institutions, Berhampur, India)

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. 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 :- Steganographic Techniques, DCT.

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.

1.1 History

1- In 440 BC, Herodotus mentions two examples of Steganography in The Histories of Herodotus. Demeratus sent a warning about a forthcoming attack to Greece by writing it on a wooden panel and covering it in wax**.** And other of Histiaeus, who shaved the head of his most trusted slave and tattooed a message on it. After his hair had grown the message was hidden.
2- During World War II, invisible inks were used to conceal information in seemingly standard, innocuous memos or letters. Common sources for invisible inks are milk, vinegar, fruit juices and urine. Each one of these substances darkens when heated and was especially effective during this time due to the fact that the sources were always readily available.
3- In the Second World War the Microdot technique was developed by the Germans. Information, especially photographs, was reduced in size , Extremely difficult to detect.
4- Although steganography is an ancient subject, the modern formulation of it is often given in terms of theprisoner's problem proposed by Simmons where two inmates wish to communicate in secret to hatch an escape plan. All of their communication passes through a warden who will throw them in solitary confinement should she suspect any covert communication. The warden, who is free to examine all communication exchanged between the inmates, can either be passive or active. A passive warden simply examines the communication to try and determine if it potentially contains secret information. If she suspects a communication to contain hidden information, a passive warden takes note of the detected covert communication, reports this to some outside party and lets the message through without blocking it. An active warden, on the other hand, will try to alter the communication with the suspected hidden information deliberately, in order to remove the information.

II. TECHNIQUES

2. Steganography Techniques :

2.1 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.

2.2 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.

2.3 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.

III. METHODS

3.Methods of concealing data in digital image :

3.1 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:
(0010011**1** 1110100**1** 1100100**0**)
(0010011**1** 1100100**0** 1110100**1**)
(1100100**0** 0010011**1** 1110100**1**)

binary will be : **011110000**
RESULT:
(0010011**0** 1110100**1** 1100100**1**)
(0010011**1** 1100100**1** 1110100**0**)
(1100100**0** 0010011**0** 1110100**0**)

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

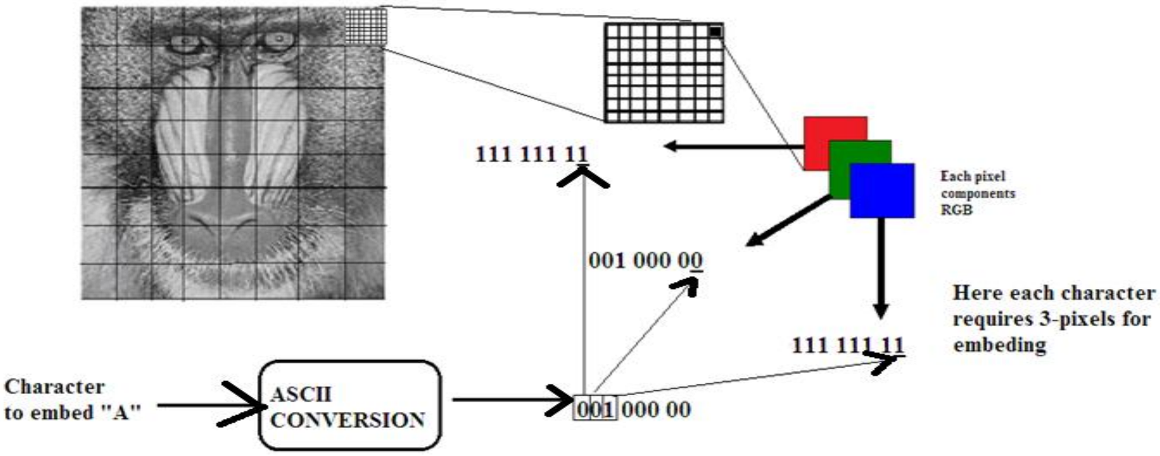

Fig 1: Ascii Conversion Of Data

3.2 Algorithm to retrieve text message

1. Read the stego image.
2. Calculate LSB of each pixels of stego image.
3. Retrieve bits and convert each 8 bit into character.

3.2.1 Embedding 1Bit

In this method the secrete data will be converted into binary and each LSB of the pixels of the cover image will be converted into either 0 or 1 according to the secrete data. Let us illustrate this by using an image called monkey.jpg and the secrete data which is to be embedded is ‘A’.

3.2.2 Embedding 2 Bit

We can embed the secrete data to the 2 LSB bits of the pxel. Let us illustrate with the following diagram as below.

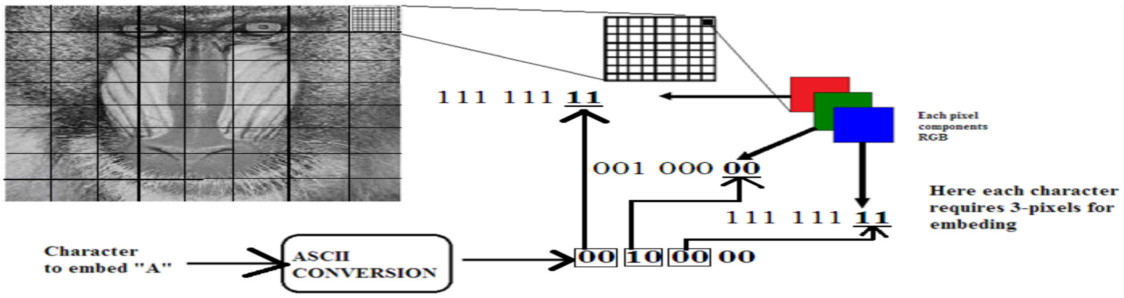

Fig 2: Embedding 2 Bit

3.2.3 Embedding 3 Bit

We can embed the secrete data to the 4 LSB bits of the pixel. Let us illustrate with the following diagram as below.

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.

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

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

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

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

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

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.

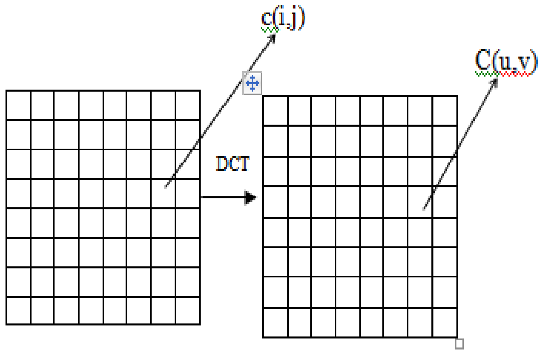

Fig 3: Discrete Cosine Transform of An Image

3.3 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.

3.4 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.

4 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.

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

A. LSB Based Steganography

B.

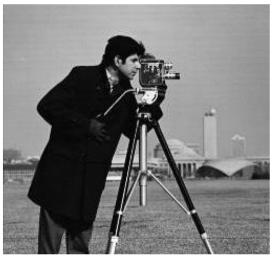

Fig. I Original Cameraman.bmp   Fig II Stego cameraman.bmp

PSNR between Fig I and Fig II = 51.0870 dB

Using Color Images

Fig .III Original army.bmp   Fig. IV Stego army.bmp

PSNR between Fig III and Fig IV =51.0872 dB

B DCT Based Steganography

Using Grayscale Images

Fig. V Original cameraman.bmp Fig. VI Stego cameraman.bmp

PSNR between Fig V and Fig. VI = 55.3865 dB

Using Color Images

Fig. VII Original army.bmp Fig. VIII Stego army.bmp

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

REFERENCE

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.