IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 2, Apr-May, 2014
ISSN: 2320 – 8791 (Impact Factor: 1.479)
www.ijreat.org

Digital Image Steganography Techniques: Case Study

Santosh Kumar.S[1], Archana.M[2]

[1]Department of Electronicsand Communication Engineering, Sri Venkateshwara College of Engineering, Bengaluru, Karnataka, India

[2]Department of Mathematics, S.J.C Institute of Technology, Chickballapur, Karnataka, India

Abstract

Now a days the secured transmission of the data over the communication channel is very essential. Two techniques are available to achieve this goal: cryptography and steganography. Steganography is the science of embedding information into the cover image viz., text, video and image (payload) without causing statistically significant modification to the cover image. This paper deals with hiding text in an image file using Least Significant Bit (LSB) based Steganography, Discrete Cosine Transform (DCT) based Steganography and Discrete Wavelet Transform (DWT) based steganography. The LSB algorithm is implemented in spatial domain in which the payload bits are embedded into the least significant bits of cover image to derive the stego-image whereas DCT & DWT algorithm are implemented in frequency domain in which the stego-image is transformed from spatial domain to the frequency domain and the payload bits are embedded into the frequency components of the cover image. The performance and comparison of these three techniques is evaluated on the basis of the parameters MSE, PSNR, NC, processing time, Capacity& Robustness.

Keywords: *Digital Image Steganography, LSB Steganography, Steganography.*

1. Introduction

Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called Steganography. Steganography is the art and science of invisible communication. This is accomplished through hiding the information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing” [1] defining it as “covered writing”. In image steganography the information is hidden exclusively in images as shown in the Fig. 1.

There are different techniques to implement steganography namely Least Significant Bit (LSB), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) technique. There are two types of domains in which steganography is implemented i.e. spatial domain & frequency domain [2]. In spatial domain, processing is applied directly on the pixel values of the image whereas in frequency domain, pixel values are transformed and then processing is applied on the transformed coefficients. LSB technique is implemented in spatial domain while DCT & DWT technique are implemented in frequency domain.

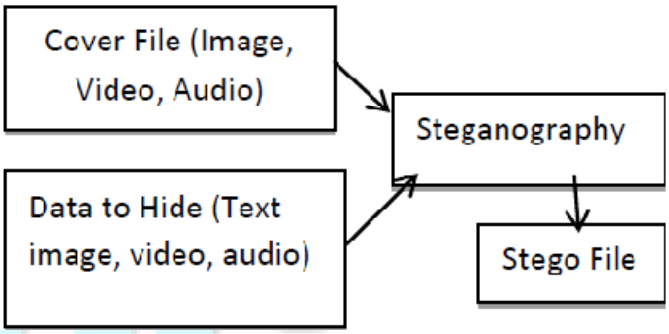

Fig. 1 The process of hiding data

2. Review on Literature

Steganography is used to achieve the secured transmission of the data by embedding the secret information in the image.

2.1 Least Significant Bit Substitution Technique (LSB):

The most well-known steganographic technique in the data hiding field is least-significant-bits (LSBs) substitution. This method embeds the fixed-length secret bits in the same fixed length LSBs of pixels. Although this technique is simple, it generally causes noticeable distortion when the number of embedded bits for each pixel exceeds three.

Several adaptive methods for steganography have been proposed to reduce the distortion caused by LSBs substitution. For example, adaptive methods vary the number of embedded bits in each pixel, and they possess better image quality than other methods using only simple LSBs substitution. However, this is achieved at the cost of a reduction in the embedding capacity.

Consider an 8-bitgrayscale bitmap image where each pixel is stored as a byte representing a gray scale value. Suppose the first eight pixels of the original image have the following gray scale values [3]:

11010010
01001010
10010111
10001100
00010101
01010111
00100110
01000011

To hide the letter C whose binary value is 10000011, we would replace the LSBs of these pixels to have the following new gray scale values:

11010011
01001010
10010110
10001100
00010100
01010110
00100111
01000011

Note that, on average, only half the LSBs need to change. The difference between the cover (i.e. original) image and the stego image will be hardly noticeable to the human eye. However, one of its major limitations is small size of data which can be embedded in such type of images using only LSB. LSB is extremely vulnerable to attacks. LSB techniques implemented to 24 bit formats are difficult to detect contrary to 8 bit format.

2.1.1 Algorithm to embed text message

- Read the cover image and text message which is to be hidden in the cover image.
- Convert text message in binary.
- Calculate LSB of each pixels of cover image.
- Replace LSB of cover image with each bit of secret message one by one.
- Write stego image,
- Calculate the Mean square Error (MSE), Peak signal to noise ratio (PSNR) of the stego image.

2.1.2 Algorithm to retrieve text message

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

2.2. Discrete Cosine Transform technique (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 as shown in the Fig. 2. It can separate the image into high, middle and low frequency components. In low frequency sub-band, much of the signal energy lies at low frequency which contains most important visual parts of the image while in high frequency sub-band, high frequency components of the image are usually removed through compression and noise attacks. So the secret message is embedded by modifying the coefficients of the middle frequency sub-band, so that the visibility of the image will not be affected. The general equation for a 1D (N data items) DCT is defined by the following equation:

$$C(u) = a(u)\sum_{i=0}^{N-1} x_i \cos\left(\frac{(2i+1)u\pi}{2N}\right) \quad (1)$$

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

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

$$C(u,v) = a(v)\sum_{i=0}^{N-1}\left[a(u)\sum_{i=0}^{N-1} x_i\left(\frac{(2i+1)u\pi}{2N}\right)\right] X \left(\frac{(2i+1)v\pi}{2N}\right) \quad (2)$$

Where 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. DCT is used in steganography as Image is broken into 8×8 blocks of pixels. Working from left to right, top to bottom, 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.

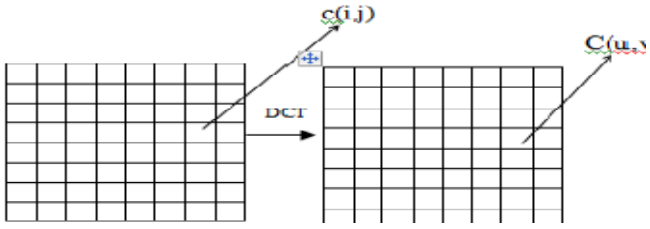

Fig. 2 Discrete Cosine Transform of an Image.

2.2.1Algorithm to embed text message

- Read cover image.
- Read secret message and convert it in binary.
- The cover image is broken into 8×8 block of pixels.
- Working from left to right, top to bottom subtract 128 in each block of pixels.
- DCT is applied to each block.
- Each block is compressed through quantization table.
- Calculate LSB of each DC coefficient and replace with each bit of secret message.
- Write stego image.
- Calculate the Mean square Error (MSE), Peak signal to noise ratio (PSNR) of the stego image.

2.2.2Algorithm to retrieve text message

- Read stego image.
- Stego image is broken into 8×8 block of pixels.
- Working from left to right, top to bottom subtract 128 in each block of pixels.
- DCT is applied to each block.
- Each block is compressed through quantization table.
- Calculate LSB of each DC coefficient.
- Retrieve and convert each 8 bit into character.

2.3 Discrete Wavelet Transform technique (DWT)[4]

The frequency domain transform we applied is Haar-DWT, the simplest DWT. A 2-dimensional Haar-DWT consists of two operations: One is the horizontal operation and the other is the vertical one. Detailed procedures of a 2-D Haar-DWT are described as follows:

- At first, scan the pixels from left to right in horizontal direction. Then, perform the addition and subtraction operations on neighboring pixels. Store the sum on the left and the difference on the right as illustrated in Fig. 3.
- Repeat this operation until all the rows are processed. The pixel sums represent the low frequency part (denoted as symbol L) while the pixel differences represent the high frequency part of the original image (denoted as symbol H).

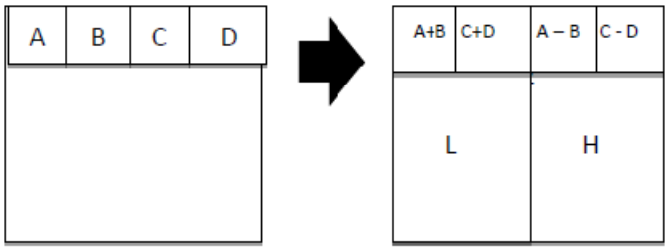

Fig 3: The horizontal operation on first row

- Secondly, scan the pixels from top to bottom in vertical direction. Perform the addition and subtraction operations on neighboring pixels and then store the sum on the top and the difference on the bottom as illustrated in Fig. 4. Repeat this operation until all the columns are processed. Finally we will obtain 4 sub-bands denoted as LL, HL, LH, and HH respectively. The LL sub-band is the low frequency portion and hence looks very similar to the original image. The whole procedure described is called the first-order 2-D Haar-DWT.

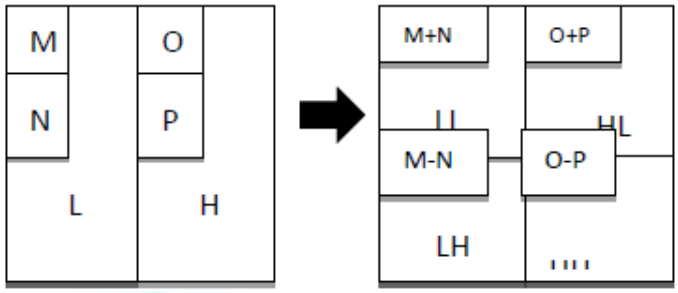

Fig 4: The vertical operation

2.3.1 Algorithm to retrieve text message

- Read the cover image and text message which is to be hidden in the cover image.
- Convert the text message into binary. Apply 2D-Haar transform on the cover image.
- Obtain the horizontal and vertical filtering coefficients of the cover image. Cover image is added with data bits for DWT coefficients.
- Obtain stego image.
- Calculate the Mean square Error (MSE), Peak signal to noise ratio (PSNR) of the stego image.

2.3.2 Algorithm to retrieve text message

- Read the stego image.
- Obtain the horizontal and vertical filtering coefficients of the cover image.

- Extract the message bit by bit and recomposing the cover image.
- Convert the data into message vector. Compare it with original message.

3. Evaluation of Image Quality

For comparing stego image with cover results requires a measure of image quality, commonly used measures are Mean Squared Error, Peak Signal-to-Noise Ratio and capacity.

3.1 Mean-Squared Error:

The mean-squared error (MSE) between two images $I_1(m, n)$ and $I_2(m, n)$ is:

$$MSE = \frac{\sum_{M,N}[I_1(M,N) - I_2(M,N)\,]}{M * N} \qquad (3)$$

M and N are the number of rows and columns in the input images, respectively.

3.2 Peak Signal-to-Noise Ratio:

Peak Signal-to-Noise Ratio (PSNR) avoids this problem by scaling the MSE according to the image range:

$$PSNR = 10log_{10}\frac{256^2}{MSE} \qquad (4)$$

PSNR is measured in decibels (dB). PSNR is a good measure for comparing restoration results for the same image.

3.3 Capacity

It is the size of the data in a cover image that can be modified without deteriorating the integrity of the cover image. The Steganography embedding operation needs to preserve the statistical properties of the cover image in addition to its perceptual quality. Therefore capacity depends on total number of bits per pixel and number of bits embedded in each pixel. Capacity is represented by bits per pixel (BPP) and the Maximum Hiding Capacity (MHC) in terms of percentage.

3.4 Domain Type (DOM)

DOM is either Spatial (S) or Transform (T). The techniques that use transform domain hide information in significant areas of the cover images and may be more complex for attackers.

3.5 Normalized Coefficient (NC)

Correlation is one of the best methods to evaluate the degree of closeness between the two functions. This measure can be used to determine the extent to which the original image and stego image remain close to each other, even after embedding the data.

4. Result

Comparative analysis of LSB based, DCT based & DWT based steganography has been done on basis of parameters like PSNR, MSE, NC, Processing time, Robustness and Capacity on different images and the results are evaluated. If PSNR ratio is high then images are of best quality. The text hidden in the cover image is “hello how r u”. The three techniques are implemented in MATLAB. Two images are taken on which Steganography is implemented. These two images are first converted into gray scale and then the various steganography techniques are implemented on it. The images are firstly converted into gray scale because the shades of gray changes very gradually between the palette entries. This increases the ability to hide information. The original image is shown below.

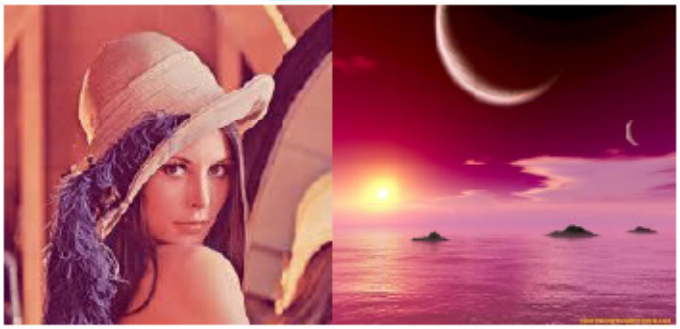

Fig. 5 Original Images

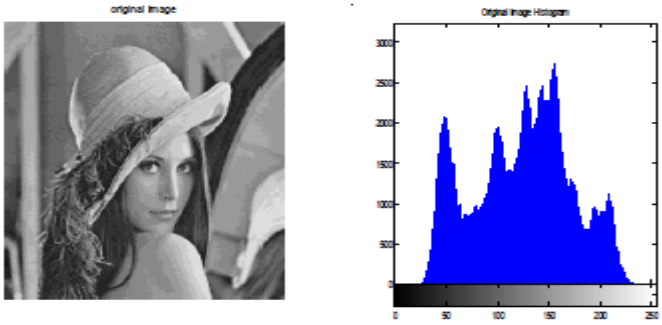

Fig.6 Lena and its histogram

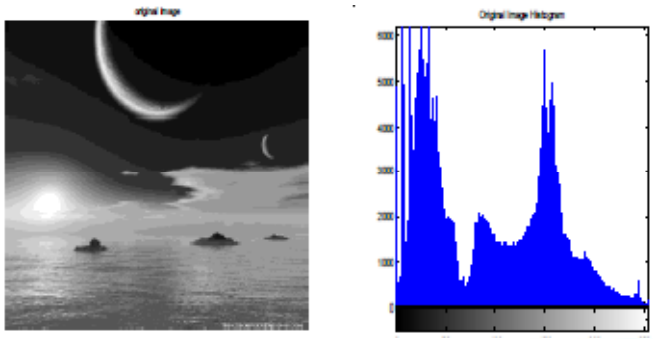

Fig. 7 View and its histogram

4.1 LSB Substitution Technique

The LSB Substitution technique is implemented on the two images and various parameters are evaluated. The Stego images are shown in Fig 8 and Fig. 9. The values of various parameters are shown in Table 1.

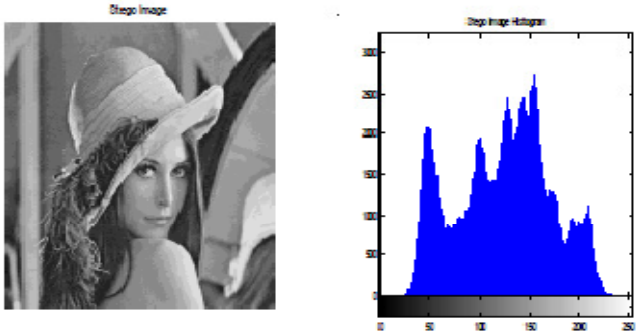

Fig 8: Stego Lena image and its histogram for LSB substitution

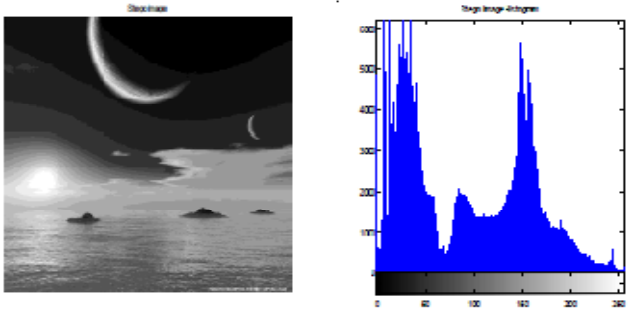

Fig 9: Stego View image and its histogram for LSB substitution

Table 1: Parameters of LSB substitution

Images	MSE	PSNR(db)	NC	Processing Time(sec)
Lena	0.000228	84.534	1	1.316234
View	0.000133	86.881	1	1.357199

4.2 DCT Substitution technique

The DCT Substitution technique is implemented on the two images and various parameters are evaluated. The Stego images are shown in Fig 10 and Fig 11. The values of various parameters are shown in Table 2.

Table 2: Parameters of DC substitution

Images	MSE	PSNR(db)	NC	Processing Time(sec)
Lena	0.00107	77.822	.9964	1.687751
View	0.04701	61.409	0.8163	1.885138

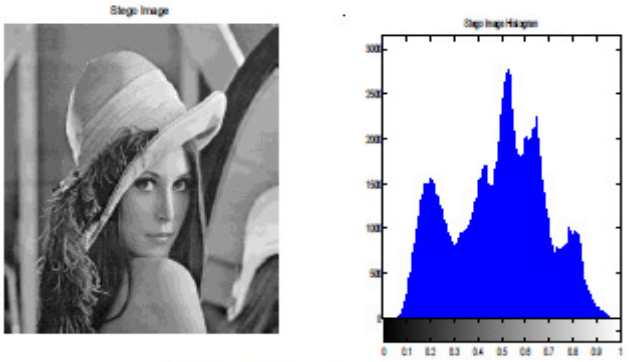

Fig 10: Stego Lena image and its histogram for DCT

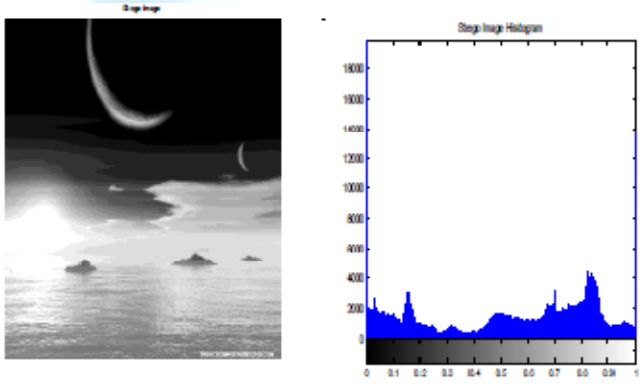

Fig 11: Stego View image and its histogram for DCT

4.3 DWT Substitution technique

The DWT Substitution technique is implemented on the two images and various parameters are evaluated. The Stego images are shown in Fig 12 and 13. The values of various parameters are shown in Table 3.

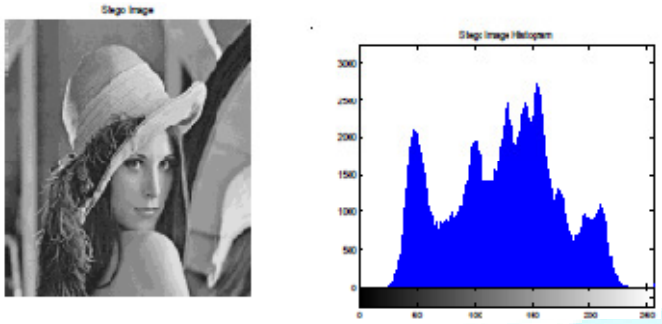

Fig 12: Stego Lena image and its histogram for DWT substitution

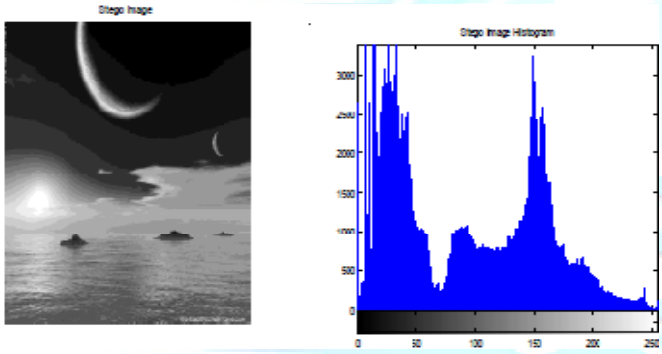

Fig 13: Stego View image and its histogram for DWT substitution

Table 3: Parameters of DWT substitution:

Images	MSE	PSNR(db)	NC	Processing Time(sec)
Lena	186.920	25.4142	0.9984	2.458673
View	186.920	186.920	186.920	186.920

5. 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. It is therefore a book on magic. It is emerging in its peak because it does not attract anyone by itself. In this paper, analysis of LSB, DCT & DWT 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.

Table 4 Parameters analysis of steganography methods:

Features	LSB	DCT	DWT
Invisibility	Low	High	High
Payload Capacity	High	Medium`	Low
Robustness against image manipulation	Low	Medium	High
PSNR	High	Medium	Low
MSE	Low	Medium	High

The PSNR shows the quality of image after hiding the data. PSNR ratio of LSB based Steganography scheme is higher than Frequency domain based Steganography scheme for all types of images Gray scale as well as Color. DCT based Steganography scheme works perfectly with minimal distortion of the image quality in comparison to LSB based Steganography. Even though the amount of secret data that can be hidden by using this technique is smaller as compared to LSB based Steganography, DCT based Steganography scheme is being recommended by us as it ensures minimum distortion of image quality. LSB insertion is more vulnerable to even the most harmless and usual transformations. Whereas, in DWT Based Steganography, coefficients in the low frequency sub-band could be preserved unaltered for improving the image quality. This is due to the different characteristics of DWT coefficients in different sub-bands. Since the most essential portion (the low frequency part) remains unchanged, when the secret messages are embedded in the high frequency sub-bands corresponding to the edges portion of the original image, PSNR is being recommended.

References

[1]. Moerland, T., "Steganography and Steganalysis", *Leiden Institute of Advanced Computing Science.*

[2]. Chen Ming, Zhang Ru, NiuXinxin, Yang Yixian, "Analysis of Current Steganography Tools: Classifications & Features" , International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'06),IEEE- 0-7695-2745-0/06 $20.00 © 2006.

[3]. Vijay KumarSharma, Vishalshrivastava, "A Steganography Algorithm for Hiding Images by improved LSB substitution by minize detection." Journal of Theoretical and Applied Information Technology, Vol. 36 No.1, ISSN: 1992-8645, 15th February 2012.

[4]. Po-Yueh Chen and Hung-Ju Lin, "A DWT Based Approach for Image Steganography",International Journal of Applied Science and Engineering 4, 3: 275-290, 2006.

[5] Chen Ming, Zhang Ru, NiuXinxin, Yang Yixian, "Analysis of Current Steganography Tools: Classifications & Features" , International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'06),IEEE- 0-7695-2745-0/06 $20.00 © 2006.

[6] AneeshJain,IndranilSen. Gupta, "A JPEG Compression Resistant Steganography Scheme for Raster Graphics Images",IEEE-1-4244-1272-2/07/$25.00©2007.