Image Steganography Using DCT and DWT

Nicky Saxena
Department of Computer Science
Inderprastha Engineering College, Ghaziabad, UP, India

Gaurav Agrawal
Department of Computer Science
Inderprastha Engineering College, Ghaziabad, UP, India

Abstract- Image Steganography is the science of hiding the information for secure communication between parties like audio, video, text, images etc. It transmits data by actually hiding the existence of the message so that a hacker or any unauthorized party cannot detect the transmission of message and hence cannot try to decrypt it. For securely communicate information between parties or locations it is not an easy task, considering the possible attacks or unintentional changes that can occur during communication. Encryption is a technique which is used to protect secret information from unauthorized access. The presence of encrypted information can also entice a potential attacker to launch an attack on the secure communication. This paper based on the comparison between the paper, uses image steganography, a technology for hiding information in other information, to facilitate secure communication using DCT and DWT. By use of Steganography one can communicates with secret data as an appropriate multimedia carrier, e.g., image, audio, and video files. It is the process of embedding secret data/message in the cover image without significant changes to the cover image.

Keywords: Spatial Domain, Frequency Domain, Least Significant Bit, Discrete Cosine Transformation, Discrete Wavelet Transform.

I. INTRODUCTION

IJIET Steganography is the art of hiding information. It includes hiding an image, a text file, an audio, video and even an executable program inside age a without "cover" distorting in the cover image. It involve a large number and widely used of applications. Steganography and Cryptography are close to each other but, it is different from cryptography. Cryptography scrambles a message such that to produce something that looks scrambled. The main objective of cryptography is to secure and authenticate communications by changing the data into a form so that it cannot be understand by an eavesdropper.

Steganography is a type of hidden communication that the Greek words stegano or "covered" and graphos or "to a scheme of secret writing where a paper mask with holes is used. The user needs to write his secret message in such holes after placing the mask over a blank sheet of paper. Then remove the mask to fill in the blank parts of the page and in this way the message appears as innocuous text. Another story of a Greek Historian who applied ancient steganography for convey the message secretly to the recipient Herodotus (485-525 BC) is the first Greek historian. His great work, The Histories, is the story of the war between the huge Persian Empire and the much smaller Greek city states. Herodotus recounts the story of Histaiaeus, who wanted to encourage Aristagoras of Miletus to revolt against the Persian king. In order to securely convey his plan, Histaiaeus shaved the head of his messenger, wrote the message on his scalp, apparently carting nothing contentious, and could travel freely. Arriving at his destination, he shaved his head and pointed it at the recipient.

The performance of steganography system can be measured using several properties like statistical undetectability of the data which is the most important property, shows how difficult it is to be determining the existence of a hidden message. Other measures associated with the steganographic techniques are capacity, which is the maximum information that can safely embedded in a work without having statistically detectable objects and robustness, which refers to how well the steganographic system resists the extraction of hidden data. Communication of secret information is a critical factor in information technology that continues to create challenges over challenges with increasing levels of sophistication. In this modern world expectations are becoming strong that one can travel the world jeopardizing the confidentiality of secret information. In these situations where the involved parties are spatially separate, the security of secret networks and additional security mechanisms should be incorporated. This factor can be strengthening by using steganography as the main purpose of this technique is to hide the secret and confident data from the intruders.

Image Steganography's main aim is image to behind secretly an image so the id main purpose of this research paper is to use the different steganography techniques like DCT and DWT to hide an image and comparison the band to obtain the better result. Here we are trying to compare the two band of DWT in which an image can be hidden so that distortion can be reduced.

II. Proposed Algorithm

2.1 Steganography Model

A basic Steganography model contain two image one is cover image and other is secret image which is to be hide behind cover image and one key which is used to encrypt the secret image. Now we start the procedure by taking cover image, key and message and apply the algorithm which gives stego image as a result of the process. The process of embedding can be defined as:

Let I represents the cover image, and S is the stego image. Let R be a Stego-Key and let E be the message that the sender wishes to send. Then E_E represents an embedded message and E_I represents the extracted message.

$$E_E : I \, \Theta R \, \Theta E \rightarrow S \qquad (1)$$

$$E_I :((I,\ r, \epsilon\, I, e))r \,\epsilon\, R,\ e\, \epsilon \approx E\ e, \qquad (2)$$

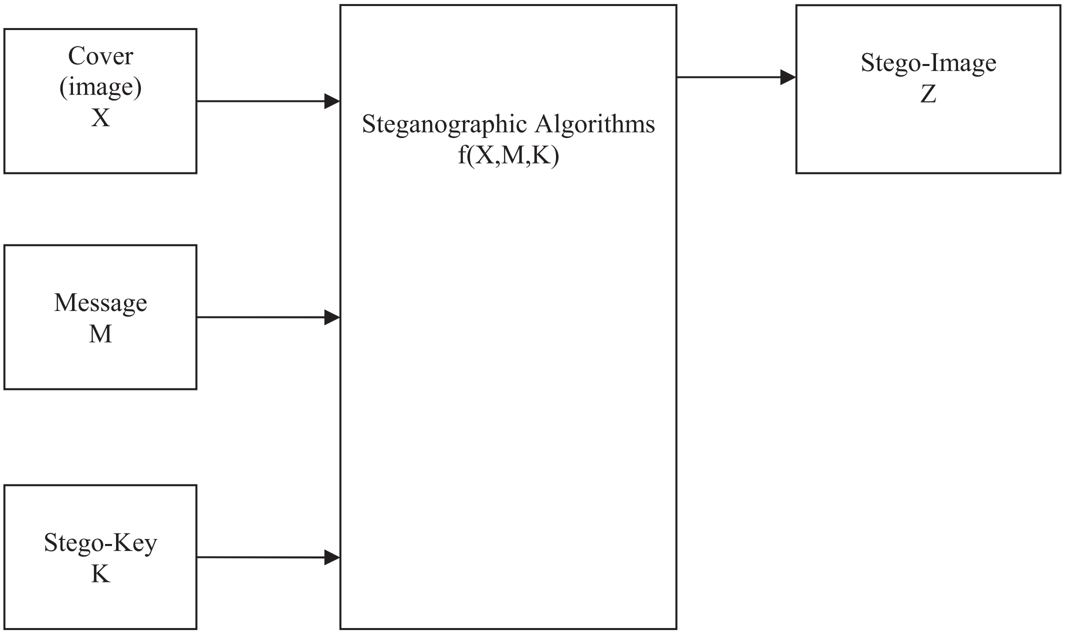


Figure 1. Steganographic Encoder

2.2. Steganographic Techniques-

Steganographic Techniques are divided into two domains: Spatial Domain and Frequency domain. In Spatial domain the processing is directly applied on the pixels values of an image, which involves modification on cover image and the secret image whereas in Frequency domain first pixel values are transformed and ten on that transformed coefficients we apply the process.

2.2.1. Spatial Domain

The term Spatial domain refers to the image plane itself in this we do direct manipulation of pixels in an image. It is aggregate of pixels composing an image. Spatial domain processes will be denoted as:

S (a, b) = T [f (a, b)] (3)

Where f (a, b) is the input image, S (a, b) is the processed image. T is an operation on f, defined over some neighborhood of (a, b). It involves the coding at Least Significant Bit (LSB) Levels.

2.2.1.1. Least Significant Bit (LSB)

LSB includes the embedding of secret message or data at the bits which having minimum weighting so that the original pixel cannot be affected or it can also be defined as in this each pixel of an image is transformed into binary value and data is hidden in to least significant position of the binary value of the pixels of an image so that integrity of cover image can't be In this LSB for embedding a message, a cover image is partitioned into non-overlapping blocks of two consecutive pixels. In each pixel a different value is calculated from the values of two pixels then that different value is replaced by a new value to embed a value of secret message. It is called as LSB replacement.

Let us consider an 8-bitrayscale bitmap image where each pixel is stored as a byte representing a gray scale value. Suppose the first 8 pixels of the original image have the following ray scale values:
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
Here, only half the LSBs need to change. The difference between the cover image and the stego image will be hardly noticeable to the human eye. One of its major limitations is Ease of extraction or it is only good for small size data which can be embedded in easily. It is extremely vulnerable to attacks.

2.2.2. Frequency Domain

Frequency domain is processed to overcome the shortcoming of LSB i.e. weak resistance to attacks. In tis pixel values are transformed and on that transformed coefficients processing is applied. It includes Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Discrete Fourier Transform (DFT). In this paper we are using DCT and DWT transforms.

2.2.2.1. Discrete Cosine Transform (DCT)

Discrete Cosine Transform transforms a signal or image from spatial domain to frequency domain. It separates the image in to parts of differing importance and divides 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.

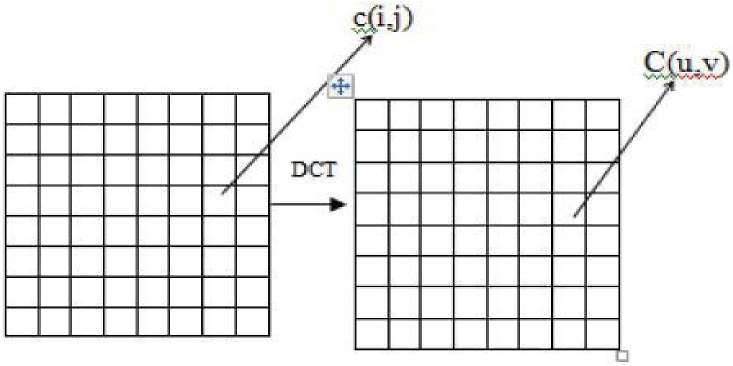


Figure2. DCT

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

$$C(u, v) = \alpha(v) \sum_{i=0} \sum_{i=0} f(i, j) \cos \quad 2N \quad \cos \quad 2N$$

Where

$$\alpha(u) = \frac{1}{N} \quad \text{For u=0;}$$

$$\alpha(u) = \overline{} \; 2 \quad \text{For u=1, -1;2, 3, 4… N}$$

And the corresponding inverse 2D DCT transform is as follows:

$$f(i, j) = \sum_{i=0}^{N-1} \sum_{i=0}^{N-1} \alpha(u)\alpha(v)C(u, v) \cos \quad \frac{\pi(2i+1)u}{2N} \cos \frac{\pi(2j+1)}{2N}$$

DCT is used in steganography is defined by following steps:

- The input image is of size N×M matrix
- f (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.
- In most images, much of the signal energy lies at low frequencies; they appear in upper left column of the DCT.
- The lower right values represent higher frequencies and are of less visual importance.
- The DCT input is an 8×8 array of integers. This array from 0 to 255.
- The output array of DCT coefficients contains, integers, these can range from 1024 to1023.

2.2.2.2. Discrete Wavelet Transform (DWT)

DWT is a linear transformation that operates on a data vector whose lant is an inteer power of 2, transforming it into numerically different vectors of the same length. It is a tool that separates data into different frequency components and then studies each component wit solution matced to its scales. DWT is computer wit cascade of filters i.e. Low and High pass filters. Here H and L denote and High and Low pass filters respectively.

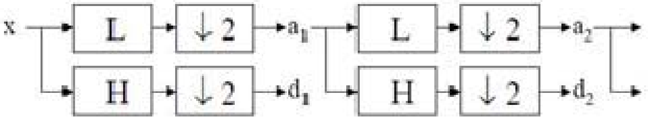
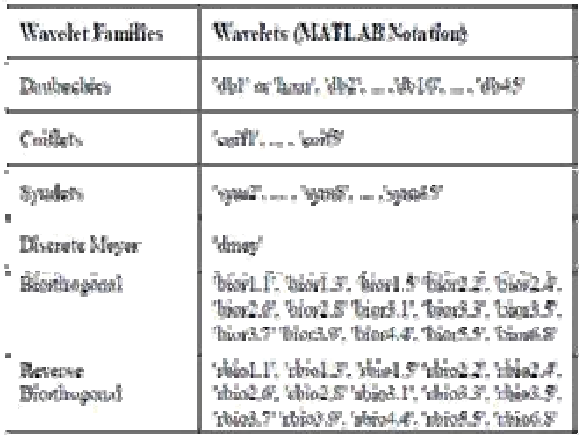


Figure3. Discrete Wavelet Transform

The use of wavelet in an image steganography model lies in the fact that the wavelet transform clearly separates the high frequency and low frequency information on a pixel by pixel basis. DWT is used for digital images. Depending upon the application we are using Haar wavelet, as it is the simplest possible wavelet. It is not continuous and therefore not differentiable. This property can be an advantage for the analysis of the signals. There are various wavelet families with different features. Table 1 show the peak signal to noise ratio of performance of our proposed method of watermarked image and original image with various watermark image, where our watermarked images peak signal to noise ratio has a better performance than others.

Table -1 Wavelet Families



Wavelet Families	Wavelets (MATLAB Notation)
Daubechies	'db1' or 'haar', 'db2', ... ,'db10', ... , 'db45'
Coiflets	'coif1', ... , 'coif5'
Symlets	'sym2', ... , 'sym8', ... ,'sym45'
Discrete Meyer	'dmey'
Biorthogonal	'bior1.1', 'bior1.3', 'bior1.5' 'bior2.2', 'bior2.4', 'bior2.6', 'bior2.8' 'bior3.1', 'bior3.3', 'bior3.5', 'bior3.7' 'bior3.9', 'bior4.4', 'bior5.5', 'bior6.8'
Reverse Biorthogonal	'rbio1.1', 'rbio1.3', 'rbio1.5' 'rbio2.2', 'rbio2.4', 'rbio2.6', 'rbio2.8' 'rbio3.1', 'rbio3.3', 'rbio3.5', 'rbio3.7' 'rbio3.9', 'rbio4.4', 'rbio5.5', 'rbio6.8'

DWT is applied on an image using Haar wavelet, in this the low frequency wavelet coefficient are generated by averaging the two pixel values and high frequency coefficients are generated by taking half of the difference of the same two pixels. The four bands obtained are Approximate Band (LL), Vertical band (LH), Horizontal Band (HL), and Diagonal Band (HH). The Approximation Band consists of low frequency wavelet coefficients, which contain significant part of the spatial domain. The other bands also called as detail bands consists of high frequency coefficients, which contain the edge details of the spatial domain image.

2.2. Proposed work

The procedure we applied is as follows:

1. We take one cover image and decompose in to three color planes i.e. Red, Green, and Blue.
2. On that each plane we apply DWT and divide tam in to four sub band.
3. (a) Then we apply DCT on HH band of Red plane.

   (b) And also on HL band of Red plane.
4. Information of secret binary image is dispersed separately in to selected high frequency component using the session based pseudo random 2D sequence.
5. After embedding bit of secret image in to red plane inverse transform is applied to get back the plane in spatial domain.
6. Finally each plane is concatenated to get color stego image.

III. Experiment and Result

The result of the proposed algorithm is as follows:

(a) (b) (c) (d)

Figure 4. (a) Original image (b) R Plane (c) G Plane (d) B Plane

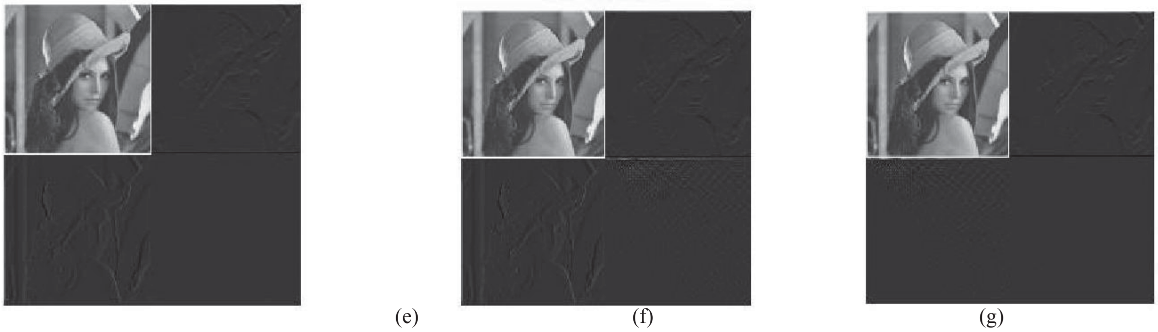


Figure 5. (a) DWT of R Plane (b) DCT of HH band (c) DCT of HL band

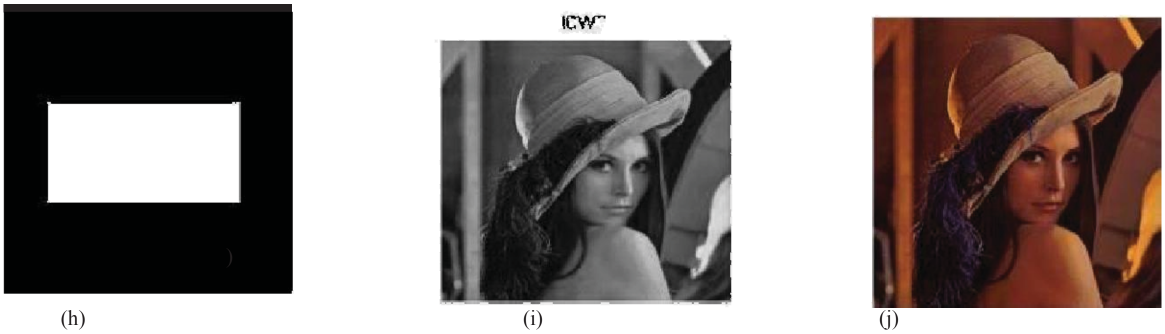


Figure 6. (h) Secret Image (i)Image after Embedding (j) Stego Image

IV.CONCLUSION

It measures the quality of an image. This is basically a performance metric and is used to determine the transparency of the stego image with respect to the input or cover image.

Psnr =10 log10 (255*255/mse) Where

Mean Square Error is the difference between two images. Mse=sum ((im1 (:)-im2 (:)). ^2)/prod (size (im1));

Here,

PSNR between cover image and stego image, when image is embedded in HH band is 47.0285

PSNR between cover image and stego image, when image is embedded in HL band is 33.8707

In this approach embedding is done in frequency domain to secure the secret data which is to be hiding. Here we are showing the comparison between the two bands which give better quality stego image after embedding. In this we hide the secret image in HH band and in HL band and make comparison on basis of PSNR value so it show that HH band is good an give better result than HL band as PSNR after embedding image in HH band is good than image embedded in HL band.

REFERENCES

[1] Stuti Goel, Arun Rana, Manpreet Kaur.: Comparison of Image Steganography Techniques. International Journal of Computers and Distributed Systems Vol. No.3, Issue I, April-May 2013. www.ijcdsonline.com.

[2] Alan Anwer Abdulla.: Combining of Spatial and Frequency Domain Transformation With The Effect of Using and Non-Using Adaptive Quantization for Image Compression. IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 6, November 2010 ISSN (Online): 1694-0814.www.IJCSI.org.

[3] Shahana T.: An Enhanced Security Technique for Steganography Using DCT and RSA. International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 7, July 2013. www.ijarcsse.com.

[4] Tanmay Bhattacharya, Nilanjan Dey, S. R. Bhadra Chaudhuri.: A Session based Multiple Image Hiding Technique using DWT and DCT. International Journal of Computer Applications (0975 –8887) Volume 38–No.5, January 2012.

[5] Shikha Sharda, Sumit Budhiraja.: Image Steganography: A Review. International Journal of Emerging Technology and Advanced Engineering, ISO 9001:2008 Certified Journal, Volume 3, Issue 1, January 2013). www.ijetae.com.

[6] H S Manjunatha Reddy, K B Raja.: HIGH CAPACITY AND SECURITY STEGANOGRAPHY USING DISCRETE WAVELET TRANSFORM. International Journal of Computer Science and Security (IJCSS), Volume (3): Issue (6).

[7] Hemalatha S, U Dinesh Acharya, Renuka A, Priya R. Kamath.: A SECURE COLOR IMAGE STEGANOGRAPHY IN TRANSFORM DOMAIN. International Journal on Cryptography and Information Security (IJCIS), Vol.3, No.1, March 2013..

[8] D. Kunder, "Multi-resolution Digital Watermarking Algorithms and Implications for Multimedia Signals", Ph.D. thesis, university of Toronto, Canada, 2001.

[9] P. Tay and J. Havlicek, "Image Watermarking Using Wavelets", in *Proceedings of the 2002 IEEE*, pp. II.258 – II.261, 2002.

[10] P. Kumswat, Ki. Attakitmongcol and A. Striaew, "A New Approach for Optimization in Image Watermarking by Using Genetic Algorithms", *IEEE Transactions on Signal Processing*, Vol. 53, No. 12, pp. 4707-4719, December, 2005.