International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:268
Vol.3, No.4, April 2014 DOI:10.15693/ijaist/2014.v3i4.8-12

Comparison Between DCT and DWT Steganography Algorithms.

Jay Desai
PG Student/Dept. of CSE
Manipal University, Karnataka, India

Hemalatha S
Assistant Professor/Dept. of CSE
Manipal University, Karnataka, India

Shishira SR
PG Student/Dept. of ISE
NMAMIT,Karnataka,India

***Abstract*— Steganography is an important area of research in recent years involving a number of applications. It is the science of embedding information into the cover image without causing statistically significant modification to the cover image. In this paper we propose an image Steganography that can verify the reliability of the information being transmitted to the receiver. This paper is based on the comparison of the DCT and DWT method. DCT and DWT algorithm are implemented in frequency domain in which the cover image is transformed from spatial domain to the frequency domain and the secret image is embedded into the frequency components of the cover image. The performance and comparison of these two techniques is evaluated on the basis of the parameters MSE, PSNR, processing time and capacity.**

Index terms – Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Steganography, MSE, PSNR.

I. INTRODUCTION

The growing possibilities of modem communications need the special means of security especially on computer network. The network security is becoming more important as the number of data being exchanged on the Internet increases. Therefore, the confidentiality and data integrity are required to protect against unauthorized access. The rapid growth of internet usage over high bandwidth and low cost computer hardware has propelled the explosive growth of steganography [1]. Steganography hides the secret message within the host data set and its presence is imperceptible and is to be reliably communicated to a receiver [2]. Steganography has evolved into a digital strategy of hiding a file in some form of multimedia, such as an image, an audio file or even a video file [3]. The objective of steganography is hiding the payload (embedded information) into the cover image such that the existence of payload in the cover image is imperceptible to the human beings [4]. There are different techniques to implement steganography namely least significant bit (LSB), discrete cosine transform (DCT) & discrete wavelet transform (DWT) technique. There are two types of domains in which steganography is implemented i.e. spatial domain & frequency domain [5]. 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. In this paper we compare two frequency domain techniques DCT and DWT.

A. 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

.

B. 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.

II. BACKGROUND

A. Discrete Cosine Transform (DCT)

DCT coefficients are used for JPEG compression [6] [7]. 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.

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 [8]. 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:

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

Where u = 0, 1, 2…….N-1

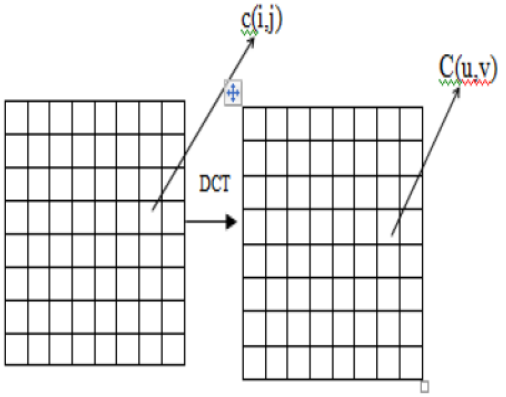

Figure 1. Discrete Cosine Transform of an Image

The general equation for 2D DCT is defined by the following equations

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

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 [10] - 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.

B. Discrete Wavelet Transform

Discrete Wavelet transform (DWT) [10] is a mathematical tool for hierarchically decomposing an image. It is useful for processing of non-stationary signals. The transform is based on small waves, called wavelets, of varying frequency and limited duration. Wavelet transform provides both frequency and spatial description of an image. Unlike conventional Fourier transform, temporal information is retained in this transformation process. Wavelets are created by translations and dilations of a fixed function called mother wavelet. This section analyses suitability of DWT for image watermarking and gives advantages of using DWT as against other transforms. For 2-D images, applying DWT corresponds to processing the image by 2-D filters in each dimension. The filters divide the input into four non-overlapping multi-resolution sub-bands LL1, LH1, HL1 and HH1. The sub-band LL1 represents the coarse-scale DWT coefficients while the sub-bands LH1, HL1 and HH1 represent the fine-scale of DWT coefficients. To Obtain the next coarser scale of wavelet coefficients, the sub-band LL1 is further processed until some final scale N is reached. When N is reached we will have 3N+1 sub-bands consisting of the multi-resolution sub-bands LL_N and LH_x, HL_x and HH_x where x ranges from 1 until N. Due to its excellent spatio frequency localization properties, the DWT is very suitable to identify the areas in the host image where a watermark can be embedded effectively. In general most of the image energy is concentrated at the lower frequency sub-bands LLx and therefore embedding watermarks in these sub-bands may degrade the image significantly. Embedding in the low frequency sub-bands, however, could increase robustness significantly. On the other hand, the high frequency sub-bands HHx include the edges and textures of the image and the human eye is not generally sensitive to changes in such sub-bands. This allows the watermark to be embedded without being perceived by the human eye.

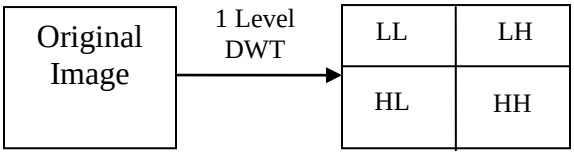

Figure 2. Discrete Wavelet transform of Image

C. Image Quality Measures

(i) Mean Square Error: The MSE is the cumulative squared error between the compressed and the original image.

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - k(i,j)]^2 \quad (3)$$

(ii) Peak Signal to Noise Ratio (PSNR): PSNR is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel (dB) scale.

$$PSNR = 20\ log_{10}\ \frac{255}{\sqrt{MSE}} \quad (4)$$

(iii) 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 & 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.

III. Algorithms of Steganography

A. DCT Based Steganography:

(i) Algorithm to embed secret image:
Step1: Read cover and secret image.
Step2: Cover image and secret image are broken into 8×8 block of pixels.
Step3: Working from left to right, top to bottom subtract 128 in each block of pixels.
Step 4: DCT is applied to each block of cover and secret image.
Step5: Divide each pixel value of secret image with 1000, so this value becomes small.
Step6: Replace middle frequency sub-band coefficients of cover image block with smaller value which is derived through step 5.
Step7: Apply inverse DCT to each block of cover image and combine each block.
Step8: Write stego image.

(ii) Algorithm to retrieve secret image:-
Step1: Read stego image.
Step2: Stego image is broken into 8×8 block of pixels.
Step3: Working from left to right, top to bottom subtract 128 in each block of pixels.
Step 4: DCT is applied to each block of stego image.
Step5: Retrieve middle frequency sub-band coefficients value.
Step6: Multiply 1000 with each value which is derived in step 5.
Step7: Generate image from the value which is derived from step6.
Step 8: Apply inverse DCT on image which is generated in step 7.
Step 9: Write secret image.

B. DWT Based Steganography

(i) Algorithm to embed secret image:
Step1: Read the cover image and secret image which is to be hidden in the cover image.
Step2: Obtain single level 2D DWT of the cover-image C and secret-image S.
Step3: The resulting transformed matrix consists of four sub-bands CLL, CHL, CLH and CHH and SLL, SHL, SLH and SHH obtained by transforming images C and S respectively.
Step4: Divide SLL, SHL and SLH with 1000, so these values become small.
Step5: Replace coefficients, CHH with SLL, CHL with SHL and CLH with SLH values, which is derived Step4.
Step6: Apply Inverse DWT on cover image.
Step7: Write stego image.

(ii)Algorithm to retrieve secret image:-
Step1: Read stego image.
Step2: Apply 2D dwt on stego image ST.
Step3: The resulting transformed matrix consists of four sub-bands STLL, STHL, STLH and STHH
Step4: Retrieve SLL from STHH, SLH from STLH and SHL from STHL and make SHH values to zeroes.
Step5: Combine SLL, SLH, SHL and SHH.
Step6: Apply 2D inverse DWT.
Step7: Write secret image.

IV. Experimental Result

The algorithms are tested in MATLAB. The result with cover image and secret image are shown. Original cover and secret image are shown in Figure 3 and Figure 4 respectively. Moon is hidden in Clock. The cover image size is 512x512 and secret image size is 160x160. Comparative analysis DCT based & DWT based steganography has been done on basis of parameters like PSNR , MSE , processing time and Capacity on images shown in figure (3) and figure (4) and the results are evaluated. If PSNR ratio is high then images are of best quality.

Figure 3. Cover Image

Figure 4. Secret Image

DCT Technique

Figure 5. Stego Image

Figure 6. Decrypted Secret Image

With DCT techniques, PSNR value between cover image and stego image is 44.2224 DB and PSNR value between secret image and decrypted secret image is INF means both images are same, Processing time for this algorithm is 3.34 seconds and capacity of secret image is 8 times smaller than cover image.

DWT techniques

Figure 7. Stego Image

With DWT techniques, PSNR value between cover image and stego image is 40.7728db and PSNR value between secret image and decrypted secret image is 32.4252, processing time of this algorithm is 0.9650 second and maximum size of secret image is equal to cover image.

9] N

Figure 8. Secret Image

V. CONCLUSION

The Steganography is covert communication to protect confidential information. Here we presented a comparative study of DCT and the DWT Methods. Both come under transform domain analysis. Both the methods have good imperceptibility and also Robustness against statistical attacks. But as we know the major aim of the Steganography is to increase the robustness against attacks and also to increase the payload capacity.

Result shown that decrypted secret image and stego image quality for DCT algorithm is better compared to DWT algorithms, while in the case of capacity and processing time, DWT are good compared to DCT.

REFERENCES

[1] J.R. Krenn, "Steganography and Steganalysis", January 2004.

[2] Anil K Jain, "*Fundamentals of Digital Image Processing*", University of California-Davis, Prentice Hall, 1988

[3] K.B.Raja, C.R.Chowdary, Venugopal K R, L.M.Patnaik, "A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images", IEEE-0-7803-9588-3/05/$20.00 ©2005.

[4] 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" .

[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] NageswaraRaoThota, Srinivasa Kumar Devireddy, "Image Compression Using Discrete Cosine Transform", Georgian Electronic Scientific Journal: Computer Science and Telecommunications, No.3 (17), 2008.

[7] Dr. EktaWalia, Payal Jain, Navdeep, "An Analysis of LSB & DCT based Steganography",Global Journal of Computer science & technology, Vol. 10 Issue 1 (Ver 1.0), April 2010.

[8] K.B.Shiva Kumar, K.B.Raja, R.K.Chhotaray, Sabyasach iPattnaik, "Coherent Steganography using Segmentation and DCT",IEEE-978-1-4244-5967-4/10/$26.00 ©2010.

[9] NageswaraRaoThota, Srinivasa Kumar Devireddy, "Image Compression Using Discrete Cosine Transform", Georgian Electronic Scientific Journal: Computer Science and Telecommunications, No.3 (17), 2008.
[10] 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.

Authors Profile

Jay Desai received the **B.E.** degree in Information Technology from A.D Patel Institute of Technology, Vallabh Vidyanagar, Gujarat, India in 2011.Currently pursuing **M.Tech** in Computer Science and Engineering in Manipal Institute of Technology, Manipal, India. His research interest includes Information Security, Image Processing, and Data Structures.

Hemalatha S Currently working as Asssociate Professor in Manipal Institute of Technology, Manipal, Karnataka. Her research interest includes Computer Architecture, Organization, Assembly Language Programming, Logic Design, Cryptography, and Information Security.

Shishira S R received the **B.E.** degree in Computer Science and Engineering from Srinivas Institute of Technology, Mangalore, VTU Belgaum, Karnataka, India in 2012. Currently pursuing **M.Tech.** in Computer Network and Engineering in NMAM Institute of Technology, Nitte, Karnataka, India. Her Research interest includes Network Security,Communication Networks,Mobile Ad hoc networks.