International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Review of Transform Domain Techniques for Image Steganography

Sudhanshi Sharma[1], Umesh Kumar[2]

[1, 2]Governemt Mahila Engg. College, Ajmer, India

Abstract: ***In highly digitalized word, internet plays a very important role in communication. If the data in communication is confidential, then information security becomes an essential issue. Steganography is one of the technique by which we can hide data into data. Thus Steganography can keep the contents of a message secret as well as existence of the message secret. Steganography uses two kind of domain for hiding the data: spatial domain (based on pixel value) and transform domain (based on frequency components). In this paper we review the two approaches of transform domain i.e. DCT & DWT for Steganography. The performance and comparison of these two techniques is measured on the basis of the parameters PSNR, MSE, Robustness & Capacity.***

Keywords: Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Mean Square Error (MSE), Peak Signal-To-Noise Ratio (PSNR), Steganography

1. Introduction

Now a day's use of computer is increasing day by day. Computers help convert analog data into digital data before storing and/or processing on it. Meanwhile, the internet develops and becomes an important medium for digital communication. Despite being a fully open communication media, the internet fetched not only comfort but also few hazards. If the information to be communicated is secret, it is easy for some sly users to illegally copy, damage or alter the data on the internet. Hence information security becomes a crucial matter. Several data hiding techniques have developed on the purpose of data hiding. One of them is Steganography. [1]

Steganography is kind of information hiding technique. Steganography hides the secret message within the host data set and its presence is imperceptible and is to reliable communicated to a receiver. Steganography has developed as a digital process of hiding information with a multimedia (cover) object like an audio file, an image or a video file. The goal of Steganography is hiding the embedded data (payload) into the cover object in order that the presence of data in the cover object is imperceptible to the human eyes. [2]

In this paper we are concern about image Steganography. Image Steganography is a type of Steganography in which we use an image as a cover object. The reason behind taking an image as a cover medium is that images are more common things that we share on internet. Hence it has very less probability to get attention of anyone that there can be a secret message behind the (cover) image. By using an image as a cover object we can conceal text or image as secret data behind it.

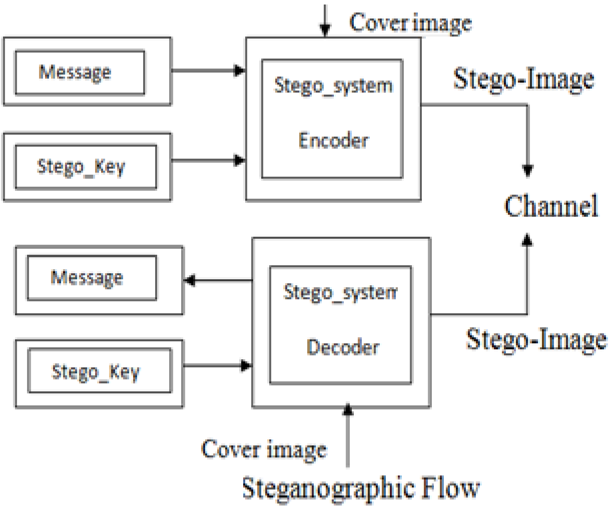


Figure 1: Steganographic Flow

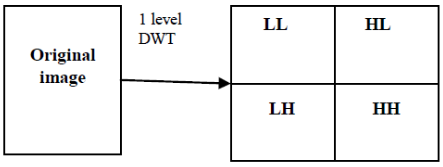
We can work with an image in two types of domain. These are following:-

Spatial Domain: - Spatial domain techniques directly deal with pixels of image. The pixel values are altered to get desired enhancement. Spatial domain techniques like the logarithmic transforms, power law transforms, histogram equalization, are based on the direct manipulation of the pixels in the image. Spatial techniques are particularly useful for directly altering the values of individual pixels and hence the overall contrast of the entire image. But they usually enhance the whole image in a uniform manner which in many cases produces undesirable results. It is not possible to selectively enhance edges or other required information effectively.[3]

Transform domain: - Transformation or frequency domain techniques are based on the manipulation of the orthogonal transform of the image rather than the image itself. Transformation domain techniques are suited for processing the image according to the frequency content. The principle behind the frequency domain methods of image enhancement consists of the computing a 2-D discrete unitary transform of the image, for instance the 2-D DFT, manipulating the transform coefficients by an operator M, and then performing the inverse transform. The orthogonal transform of the image has two components magnitude and phase. The magnitude consists of the frequency content of the image. The phase is used to restore the image back to the spatial domain. The usual transform domain enables operation on the frequency content of the image, and therefore high frequency content such as edges and other subtle information can easily be enhanced.[3]

2. Background

Discrete Wavelet Transform (DWT): - It 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 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 transform process. Wavelets are created by translations and dilations of a fixed function called mother wavelet. This section analyses suitability of DWT for image Steganography and gives advantages of using DWT as against other transform. When we perform discrete wavelet transform on 2-D images, then the image is process by 2-D filters in both dimensions. These filters decompose the input image into four parts. These parts are non-overlapping multi-resolution sub-bands LL_1, LH_1, HL_1 and HH_1. The sub-band LL_1 shows the coarse-scale Discrete Wavelet Transform (DWT) coefficients and remaining sub-bands as LH_1, HL_1 and HH_1 indicate fine-scale of DWT coefficients. To procure the next coarser scale of wavelet coefficients, further DWT apply on sub band LL_1 until we get N level of it. When N is achieved that time than we will have 3N+1 multi-resolution sub bands consisting of LL_N and LH_Y, HL_Y and HH_Y where Y varies from 1 until N. Because of its great spatial-frequency localization attribute, the DWT is very appropriate to recognize the region in the host image where we can hide a secret message effectively. Usually most of the image energy is stored at lower frequency sub $LL_{X;}$ so Steganography in these sub-bands may put down the quality of image. However, embedding in low frequency sub-bands could increase robustness. In contrast, the high frequency sub-bands represents the edges and textures of an image. Usually people do not notice slight changes in above, so high frequency sub bands is more suitable for embedding without being notice by the human eye.[4]



Discrete Cosine Transform (DCT): - The DCT is a approach for transforming a signal into elementary frequency components. It shows an image as a summation of sinusoids of varying frequencies and magnitudes. For an input image x, we can calculate the DCT coefficients of the transformed output image y, by using Eq. 1. In the following equation x, is an input image possess N x M pixels, y(u,v) is DCT coefficient in u^{th} row & v^{th} column of the DCT matrix and x(m,n) is the intensity of the pixel in m^{th} row & n^{th} column of image matrix.

$$y(u,v)=\sqrt{\frac{2}{M}}\sqrt{\frac{2}{N}}\,\alpha_u\alpha_v\sum_{u=0}^{M-1}\sum_{v=0}^{N-1}x(m,n)$$

$$\cos\frac{(2m+1)u\pi}{2M}\cos\frac{(2n+1)v\pi}{2N}\ (1)$$

Where α_u and α_v are given by:

$$\alpha_{u=}\begin{cases}\dfrac{1}{\sqrt{2}}\ u=0\\ 1\ u=1,2\ldots\ldots N-1\end{cases}$$

$$\alpha_{v=}\begin{cases}\dfrac{1}{\sqrt{2}}\ v=0\\ 1\ v=1,2\ldots\ldots N-1\end{cases}$$

The image is recreated by applying inverse DCT operation according to Eq. 2:

$$y(u,v)=\sqrt{\frac{2}{M}}\sqrt{\frac{2}{N}}\,\alpha_u\alpha_v\sum_{u=0}^{M-1}\sum_{v=0}^{N-1}x(m,n)$$

$$\cos\frac{(2m+1)u\pi}{2M}\cos\frac{(2n+1)v\pi}{2N}\ (2)$$

The standard block-based Discrete Cosine Transform divides an image into non-overlapping blocks and implements DCT on each block. As a result it provides three frequency sub bands: low, mid & high. DCT based Steganography depends on two characteristics: - The first is that most much of the energy of any signal consist by low frequency sub band, which accommodate an essential visual part of an image. The second attribute is that high frequency component of any image are often abstain from noise attacks and compression.[4]

3. Algorithm of Steganography

DWT Based Steganography:

Algorithm to implant secret text message:-

Step 1: Study the cover image and secret text message which is to be conceal in the cover image.

Step 2: Transform the secret text message into binary. 2D-Haar transform perform on the cover image.

Step 3: Find filtering coefficients of the cover image in horizontal and vertical direction. Cover image is attached with data bits for DWT coefficients.

Step 4: Get stego image.

Step 5: Determine the Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) of the stego image.

Algorithm to regain secret text message:-

Step 1: Study the stego image.

Step 2: Find out the horizontal and vertical filtering coefficients of the cover image. Retrieve the secret message bit by bit and recompose the cover image.

Step 3: Translate data into message vector. Differentiate it with original message.[5]

DCT Based Steganography:

Algorithm to implant secret text message:-
Step 1: Study cover image.
Step 2: Study secret message and transform the message in binary form.
Step 3: The cover image is divide into 8x8 blocks of pixels.
Step 4: Operating from left to right and top to bottom for subtract 128 in each block of pixel.
Step 5: DCT is perform to each block of pixel.
Step 6: Each block is compressed by using quantization table.
Step 7: Compute LSB of each DC coefficient and swap with each bit of secret message.
Step 8: Create stego image.
Step 9: Evaluate the Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) of the stego image.

Algorithm to regain secret text message:-
Step 1: Study stego image.
Step 2: Stego image is divide into 8x8 blocks of pixels.
Step 3: Functioning from left to right, top to bottom subtract 128 in each block of pixels.
Step 4: DCT is perform to each block.
Step 5: Each block is compressed through quantization table.
Step 6: Analyse LSB of each DC coefficient.
Step 7: Get back and translate each 8 bit into character.[5]

4. Evaluation of Image Quality

For differentiate stego image with cover image we need some measures of image quality, usually Peak Signal to Noise Ratio, Mean-Squared Error and Capacity are use to evaluate the quality of an image.

Mean-Square Error: The mean-square error (MSE) between two Image I1(m,n) and I2(m, n) is denote as:

$$MSE = \sum_{M,N} [I1(m,n) - I2(M,N)]^2$$

Here M and N show the number of rows and columns in image matrix of input images, respectively.

Peal Signal to Noise Ratio: PSNR remove this problem by using the MSE according to the range of image:

$$PSNR = 10\log_{10}\frac{256^2}{MSE}$$

PSNR is calculated in decibels (db). PSNR is a fine measure for evaluating restoration results for the same image.

Capacity: Capacity is the size of data in a cover image which can be altered without degrade the quality of the cover image. The embedding operation of Steganography desires to protect the statistical properties of the cover image besides its perceptual quality. Thus capacity of an image lies on total number of bits per pixel and number of bits implanted in each pixel. Unit of capacity is bits per pixel (bpp) and in terms of percentage it calculated as Maximum Hiding Capacity (MHC).

Type of Domain (DOM): DOM can be two types either Transform (T) or Spatial(S). The technique that uses transform domain to hide data in considerable region of the cover images may be more difficult for attackers. [6]

5. Result & Conclusion

Comparative analysis of DWT based & DCT based Steganography has been perform on the basis of parameters like PSNR, MSE, Robustness and Capacity on two images and the results are analyzed. If PSNR ratio is high then quality of images are best. [7]

DCT Transform Technique

(a) Mig (b) Atelidae

Table 1: DCT Transform Technique

COVER IMAGE	PSNR(db)	MSE(db)
MIG	55.6473	.420896
ATELIDAE	58.3766	.30740

DWT Transform Technique

(a) Mig (b) Atelidae

Table 2: DWT Transform Technique

COVER IMAGE	PSNR(db)	MSE(db)
MIG	44.76	1.4741
ATELIDAE	44.96	1.4405

Table 3: Parameters Analysis of Steganography Methods

Features	DCT	DWT
Invisibility	High	High
Payload capacity	Medium	Low
Robustness against image manipulation	Medium	High
PSNR	High	Low
MSE	Low	High

6. Conclusion

Steganography is a technique of writing secret message such a way that no one can doubt for the existence of the message apart from the sender and considered recipient. In this paper, we compare two image Steganography techniques by using DCT & DWT through MSE and PSNR. We have presented background discussion of DCT & DWT, algorithm of Steganography and parameters for evaluation of image quality after embedding the data. From the results, we get the conclusion that PSNR of DCT is higher than DWT techniques. It shows that DCT gives best quality of image. If the embedded message can be retrieved properly from the cover image without being destroyed, then embedding algorithm is called robust. DWT is more robust method for extracting the message without being destroyed. It gives maximum security.

References

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

[2] Jay Desai, Hemalatha S, Shishira Sr, "Comparison between DCT and DWT Steganography Algorithms", International Journal of Advanced Information Science and Technology (IJAIST), Vol.24, No.24, April, 2014.

[3] Snehal O. Mundhada, V.K. Shandilya, "Spatial and Transformation Domain Techniques for Image Enhancement", International Journal of Engineering Science and Innovative Technology (IJESIT), Volume 1, Issue 2, November 2012.

[4] Navnidhi Chaturvedi, Dr. S. J. Basha, "Comparison of Digital Image Watermarking Methods DWT & DWT-DCT on the Basis of PSNR", International Journal of Innovative Research In Science, Engineering and Technology, Vol. 1, Issue 2, December 2012.

[5] Gurmeet Kaur and Aarti Kochhar, "Transform Domain Analysis of Image Steganography", International Journal for Science and Engineering Technologies with Latest Trends" 6(1): 29-37, 2013.

[6] Vanita T. Anjalin D Souza, Rashmi B. And Sweeta Dsouza, "Review on Steganography Latest Significant Bit Algorithm and Discrete Wavelet Transform Algorithm", International Journal of Innovative Research in Computer and Communication Engineering, Vol.2, Special Issue 5, October 2014.

[7] Stuti Goel, Arun Rana, Manpreet Kaur, "A Review of Comparison Techniques of Image Steganography", IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE), Volume 6, Issue 1, Pp 41-48, May-Jun, 2013.