ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

Review on Transform Domain Steganographic Techniques (DCT & DWT)

Dipalee Borse, ShobhanaPatil

Asst. Professor, Dept of CS, Dr.D.Y. Patil ACS College, Pimpri, India

ABSTRACT: Due to malicious changes & abolition of secret data, the security of information is very crucial. Steganography is becoming increasingly popular in areas of Information security. Steganography is used to hide the existence of secret data while transmitting through an untrusted channel. Steganography can be implemented in different spatial & frequency domains. This paper has the review on frequency domain steganographic techniques such as Discrete cosine transform (DCT) and Discrete wavelet transform (DWT).

KEYWORDS: DCT, DWT, frequency domain, Security, Steganography.

I. INTRODUCTION

The use of internet as a communication media is increasing exponentially day by day. Information hiding techniques can be used to preclude the malicious modification, use or obliteration of the secret data. Information Security is process of keeping information secure, protecting its accessibility, integrity, and secrecy.

Steganography is process of the hiding of a secret data within another media such as image, so that the presence of the hidden message is indiscernible. Steganalysis is reveals the secret data form stego media. The word *steganography* restraints the greek words *steganos* means "protected/covered", and *graphie*means "writing". It was first used in 1499 by Johannes Trithemius. In digital steganography digital images, video, audio, DNA, Protocol, etc., are used as a cover media to hide the secret information Figure below shows the general process of steganography:

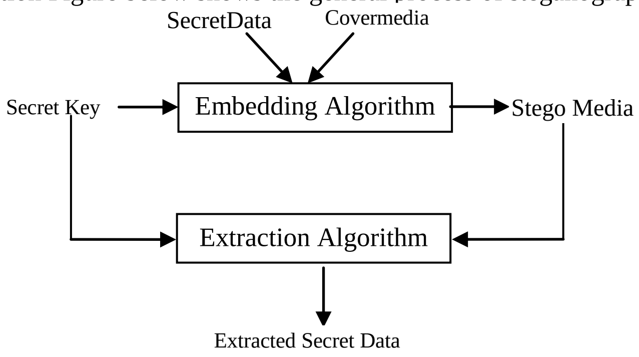


Figure 1: Process of steganography

Steganographic Techniques

Steganography techniques can be classified into following domains.

A. Substitution or Spatial Domain

B. Transform Domain

C. Statistical

D. Distortion

E. Cover Generation

Spatial domain, directly alter bits in the image pixel values in hiding data. In Distortion Techniques, decoder functions to check for differences between the original cover image and the distorted cover image in order to restore the secret message. The encoder adds a sequence of changes to the cover image. So, information is described as being stored by signal distortion. Statistical Techniques are vulnerable to rotating, cropping, scaling attacks and also all the watermarking attacks. Cover Generation Technique is used to generate a cover image for secret communication.

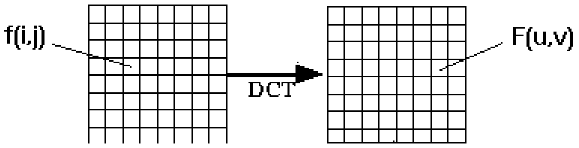
In Transform Domain Technique, Various transformations are used on the image to hide information in it. The process of embedding data in the frequency domain of a signal is sturdier than embedding principles that operate in the time domain. Most of the strong steganographic systems today operate within the transform domain Transform domain techniques is advantageous than spatial domain as they hide information in those areas of the image which are not affected in compression, cropping, or other image processing techniques. Transform domain techniques may outrun lossless and lossy format conversions.

The next sections covers overview of Transform domain (Discrete Cosine Transform & Discrete wavelet transform), Literature Survey and Conclusion.

II. OVERVIEW OF DCT AND DWT

A. Discrete Cosine Transform:

DCT commonly used for multimedia image/video compression. The discrete cosine transform (DCT) helps separate the image into parts with respect to the image's visual qualityi.e. high, low & middle frequency components. The DCT transforms a signal or image from the spatial domain to the frequency domain.



A DCT is a finite sequence of data points in terms of a sum of cosine functions oscillating at different frequencies. DCTs are equivalent to DFTs of roughly twice the length, operating on real data with even proportion and computationally quite simpler than FFT.Much of the signal energy in image lies at low frequencies which appear in the upper left corner of the DCT. The lower right values represent higher frequencies which are small enough to be neglected with little visible distortion.

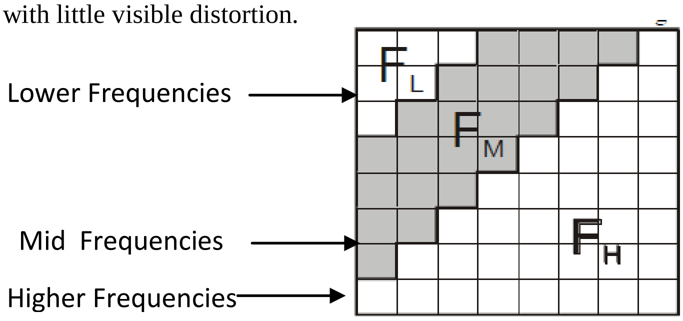


Fig. DCT Regions

1D Dct:

For N data items 1D DCT is defined by:

$$F(u) = \left(\frac{2}{N}\right)^{\frac{1}{2}} \sum_{i=0}^{N-1} \Lambda(u).cos\left[\frac{\pi.u}{2.N}(2i+1)\right] f(i)$$

And the corresponding inverse 1D DCT transform is simple $F^{-1}(u)$, i.e.:

$$\begin{aligned} f(i) &= F^{-1}(u) \\ &= \left(\frac{2}{N}\right)^{\frac{1}{2}} \sum_{u=0}^{N-1} \Lambda(u).cos\left[\frac{\pi.u}{2.N}(2i+1)\right] F(u) \end{aligned}$$

where

$$\Lambda(\xi) = \begin{cases} \frac{1}{\sqrt{2}} & \text{for}\xi = 0 \\ 1 & \text{otherwise} \end{cases}$$

2D DCT:

For 2D N by M image 2D DCT is defined:

$$\begin{aligned} F(u,v) &= \left(\frac{2}{N}\right)^{\frac{1}{2}} \left(\frac{2}{M}\right)^{\frac{1}{2}} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} \Lambda(u) \cdot \Lambda(v). \\ & cos\left[\frac{\pi \cdot u}{2 \cdot N}(2i+1)\right] cos\left[\frac{\pi \cdot v}{2 \cdot M}(2j+1)\right] \cdot f(i,j) \end{aligned}$$

And the corresponding ‘inverse’ 2D DCT transform is simple $F^{-1}(u,v)$, i.e:

$$\begin{aligned} f(i,j) &= F^{-1}(u,v) \\ &= \left(\frac{2}{N}\right)^{\frac{1}{2}} \sum_{u=0}^{N-1} \sum_{v=0}^{M-1} \Lambda(u) \cdot \Lambda(v). \\ & cos\left[\frac{\pi.u}{2.N}(2i+1)\right] \cdot cos\left[\frac{\pi \cdot v}{2 \cdot M}(2j+1)\right] \cdot F(u,v) \end{aligned}$$

where

$$\Lambda(\xi) = \begin{cases} \frac{1}{\sqrt{2}} & \text{for}\xi = 0 \\ 1 & \text{otherwise} \end{cases}$$

Performing DCT for Steganography: To embed the data in image consider a cover image of MxN& the data is to be concealed. First divide the image in 8x8 blocks. & perform 2D DCT on each block. This will generate a matrix of DCT Coefficients. The lower right coefficients represent higher frequencies which are negligible. So in next step quantization is applied on each 8x8 block to compress the block. Then LSB of DCT coefficients are replaced with data bits (that are to be hidden). Perform Inverse DCT on each resulting block. Then combine all blocks to form a stego image.

B. Wavelet Transform

The wavelet transform is different in merit function than other transform techniques. Wavelet transform uses functions that are localized in both the real and Fourier space. Generally, the wavelet transform can be expressed by the following equation:

$$F(a,b) = \int_{-\infty}^{\infty} f(x)\, \psi^*_{(a,b)}(x)\, \mathrm{d}x$$

Where the * indicates the complex conjugate symbol and function ψ is any function. Wavelet transform is in fact an infinite set of various transforms.

Discrete Wavelet Transform: In mathematics or functional analysis, a **discrete wavelet transform** (DWT) is any wavelet transform for which the wavelets are discretely sampled. It captures both frequency *and* location information (location in time) that means it provides time –frequency representation. It is implementation of the e wavelet transform using a discrete set of the wavelet scales and translations following some defined rules. Actually, this transform decomposes the signal into mutually orthogonal set of wavelets or its implementation for the discrete time series sometimes called discrete-time continuous wavelet transform. The wavelet can be constructed from a scaling function which describes its scaling properties. The restriction that the scaling functions must be orthogonal to its discrete translations implies some mathematical conditions on them which are mentioned every where.e.g.Dilation equation is

$$\phi(x) = \sum_{k=-\infty}^{\infty} a_k \phi(Sx - k)$$

WhereS is a scaling factor (usually chosen as 2). The area between the function must be normalized and scaling function must be orthogonal to its integer translations, i.e

$$\int_{-\infty}^{\infty} \phi(x)\, \phi(x+l)\, \mathrm{d}x = \delta_{0,l}$$

As after applying more conditions we get result of these equations which is nothing but finite set of coefficients $\mathbf{a_k}$which define scaling function and wavelet. The wavelet is obtained from the scaling function as N where N is an even integer. The set of wavelets then forms an ortho normal basis that is use to decompose the only signal.

Working of discrete wavelet transform: In brief, Time domain signal is passed through various Low pass filters and high pass filters. these filter our out high frequency and low frequency portions of the signal .this procedure is repeated, each time some part of the signal corresponding to some frequencies being removed from the signal.

Steps:

1. if we have a signal which has frequencies up to 1000 Hz. Divide it in two parts by passing the signal from a high pass and a low pass filter which results in two different versions of the same signal: portion of the signal corresponding to 0-500 Hz(low pass portion), and 500-1000 Hz(high pass portion).
2. We can choose any version that is either low pass portion or high pass portion or both and repeat the steps above. This process is called Decomposition.
3. After these steps we get bunch of signals that actually represents the same signal but actually all corrsosponding to different bands.
4. We can put them all together and plot on 3 d graph where one axis represents time, second represents frequency and third represents amplitude.

Haar-DWT: Secret messages are embedded in the high frequency coefficients resulted from Discrete Wavelet Transform. Coefficients in the low frequency sub-band are conserved unchanged to improve the image quality. Mathematical operations like addition, Subtraction are performed on the secret messages before embedding. These mechanisms provide better security than previous stenography. Haar DWT is the simplest frequency domain transform. it consist of two operations. One is horizontal operation and another is vertical.

Procedure of Haar DWT:

1. At start, scan the pixels from left to right in horizontal direction.
2. Perform the addition and subtraction operations on neighboring pixels.
3. Store the sum on the left and the difference on the right as below

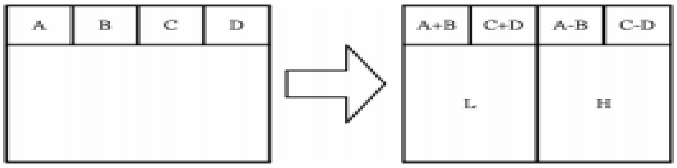


Fig: Horizontal operation

This step is repeated until all the rows are processed. The pixel sums represent the low frequency part here it is denoted L while the pixel differences represent the high frequency part of the original image here denoted as H.

4. Again, scan the pixels from top to bottom in vertical direction. Perform the addition and subtraction operations on neighbouring pixels and then store the sum on the top and the difference on the bottom as below.

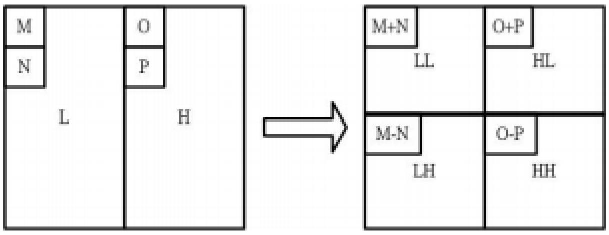


Fig: Vertical Operation

This step is repeated until all the Columns are processed. At end, this mechanism gives four sub-bands denoted as LL, HL, LH, and HH.The LL sub-band is the low frequency section and looks very similar to the original image.

III. LITERATURE REVIEW

In [1] authors proposed method provides a combination of frequency domain DCT and LSB technique of spatial domain steganography to hide a data The image is compressed using DCT then DCT coefficients are arranged by zigzag scan pattern. Data bits are obscured by altering the LSB of elements of zigzag array.After embedding data zigzag array is again converted into 8×8 block. These blocks are dequantized and inverse DCT is performed. All 8×8 blocks are combined to form the stego image which is then sent to receiver. For extraction the reverse process is applied. It is a way to mask a secret message in an image without corrupting the image quality and to provide better resistance against steganalysis process.

In [2] Walia*et. al.* has done comparative analysis of LSB based and DCT based steganography on basis of parameters like PSNR (peak signal to noise ratio). PSNR ratio of DCT based steganography scheme is high as compared to LSB based steganography scheme for Greyscale as well as Color images). DCT works with minimal distortion of the image quality as compared to LSB steganography. The amount of secret data hidden using this technique is very small as compared to LSB but DCT based steganography scheme gives minimum distortion of image quality.

In [3] the author has compared DCT coefficients replacement method with the JSTEG algorithm (precise copy of LSB method in spatial domain). However the data embedding capacity in replacement algorithm is less than the JSteg algorithm, PSNR ratio for all of the images, in replacement algorithm is greater than the JSteg.

In [4] Hardik patel and Preeti dave has introduced a steganographic technique based on DCT. In this method certain number of bits replaced in a carrier image so the receiver must know number of bits replaced in a carrier image, number of bits stored for secret image data, the size of secret image and a key matrix. The key matrix indicates position where the bits of stego image are stored. Without these parameters it is difficult to retrieve the secret image from the stego image.

In [5], Author has proposed a method, where cover image is cropped and that cropped part works as a key at decoding side which improved security. In this method, data is embedded within skin area of image.to implement this skin tone detection, DWT and LSB matching algorithm is used.A skin detector can be used that converts a given pixel into an appropriate color space and then a skin classifier to label the pixel whether it is a skin or a non-skin pixel. Author has used HSV as color image of RGB color space can be converted into HSV color spaceeasily. Theauthor has used 2D DWT and variable sized LSB insertion method, in which secret message bit is embedded at the rightmost bit of pixel value as it does not affect original pixel value. In embedding process, skin detection is performed to find the skin area of image which is used as cover. Skin area detected of an image is then cropped to hide the data within limited skin pixel place. Then to improve the quality of an image, histogram equalization has been performed. Pseudo key is generated for encryption followed by DWT tool and then secret data is embedded using LSB matching mechanism. Author has used OPA (optimization pixel adjustment)to reduce the distortion, generated by applying LSB; .OPA improved the quality of the stego image.as in the next step inverse DWT is performed and then image is constructed called as stego image with secret data. Extraction process was the exact reverse of embeddingprocess. Proposed method is better in terms of PSNR.

In [6,] Author has proposed a steganography method for digital image that explores skin tone area in image. In this method, skin tone is detected. Final step in skin detection is to define decision rule that differentiate between skin and non-skin pixels. They have used RGB color space and masking & filtering mechanism. Masking was done by covering non skin area with black mask and filtering was done by replacing the white regions that skin area in binary image with skin area in cover image. ROI is selected to embed the message. It is segmented 2 D Haar wavelet is applied to ROI. The sub band is selected for embedding. After that inverse DWT is applied to get stego image. But decoding is not exact inverse of encoder. This has increased the security and robustness of algorithm. Authors have implemented IDWT on encoder end but not on decoder end. This is very important feature that increases the robust ness of algorithm.

In [7], thispaper, a new DWT difference based method of stenography. this is based on idea of the Bhattacharyya and Sanyal‘s Transformation. Group of 8x8 DWT coefficients four seed pixels are selected and each pixel is embedded its 3x3 neighbourhood. DWT difference between twosomes of neighbouring pixel is calculated for each block that is called as seed. Certain Arithmetic operation is applied to map a pair of binary bits with the help of computed difference. Haar Discrete wavelet transform is applied to get four components like approximation coefficient matrix, as well as coefficient matrix along vertical horizontal and diagonal. Then these components are divided into 8x 8 blocks. This is followed by normalizing coefficients. For each 8 x8 block, four seed pixels are identified so that their neighbor of 3 x3 should not overlap. Then extraction of 3 x 3 seed block is done. As per the binary representation of each secret character, 2 bits secret data are mapped in the DWT coefficients with the help of message bit, its decimal equivalent DWT difference and magnitude of DWT coefficients. Once mapping is over, fractional components of DWT coefficients are restored. Then 8 x 8 blocks are merged. Apply inverse DWT to get stego image. It is secured method relative entropy distance is low between stego image and cover image.

In [8], Author has used integer wavelet transform as it maps an integer data set into another integer data set. In DWT, filters have floating point coefficients. If we truncate floating point values of the pixels that should be integers may reason the loss of the hidden information that leads the failure in data hidingTo overcome this, when the input data is integer (as in digital images), the output data will no longer be integer which doesn't allow perfect reconstruction of the input image and hence no loss of information via forward and inverse transform. In inverse wavelet transform, the LL sub band appears to be a close copy with smaller scale of the original image .while in the DWT the LL sub band is distorted. Authors not only used simple IWT but also lifting scheme to obtain integer wavelet transform due to some arithmetic operation. The proposed embedding algorithm reads cover image into 2 D decimal array. Cover image is divided into 8 x 8 blocks which are non-overlapping. These blocks are transformed into 2 D Harr wavelet transform that results in LLI, LHI, HLI, HHI.this is followed by calculating hiding capacity. Bits are embedded in randomly selected coeficients.OPA is applied for adjusting pixel value. Then inverse transform is applied to get stego image. Extracting algorithm is reverse of embedding algorithm.This algorithm increases the hiding capacity. Secret data is hidden in a random order using a secret key .this is known both sender and receiver.

In [9] this paper, 2 D DWT is performed on a gray level cover image of size M × N. Before encoding, Huffman encoding is done on the secret messages or image. Each bit of Huffman code of secret message or image is embedded in the high frequency coefficients caused from DWT. Preserving the wavelet coefficients in the low frequency sub-band; quality of an image is improved.The embedding of secret message starts with decomposition of cover image using Haarwavelet.Then Huffman encoding is applied on the 2 D secret image into one D bit stream. Huffman code is decomposed into 3-bits blocks and formed a decimal value ranging from 0 to 7. one sub-band is selected to replace bit for embedding the secret message. if we have coefficients matrix of the selected sub-band, 3 least significant bits of wavelet coefficients is replaced by the 3 bits of Huffman encoded bit stream in the form of 3 bit block Bi. Then IDWT is applied to get stegoimage.extraction is reverse of embedding. Security is maintained as the secret message or image cannot be extracted without knowing Huffman table and decoding rules.

In [10] this paper, DWT is applied on cover image to get 4 bands .Again DWT is applied on HH band to get the next rougher scale of coefficients that result in another level of sub-bands as LL2, HL2, LH2 and HH2. LL2 band is selected to embed the secret because hiding in the approximate band will result in a better extraction of the secret at thei.e. receiver side. For LL2 level top left corner, 5 LSB are replaced by 5 MSB of secret image pixel. And this step is repeated till n times as size of secret image is n*then inverse DWT is applied to get stego image. Extraction procedure is reverse of above.Advantage of proposed method is when the stego is passed over the network, and then an invader may acquire the stego image and can try to image to alter the secret hidden behind it. The algorithm is robust to various kinds of stego attacks.

IV. CONCLUSIONS

In above paper we have studied different transform domain steganographic methods. In Transform domain we focused on two major techniques are Discrete cosine transform and Discrete wavelet Transform. DCT in image processing is mainly used for compression of JPEG image. With steganography it provides greater security but the data embedding capacity is less than spatial domain techniques.DWT in image processing is used to decompose the cover image to get the four frequency bands where in the high frequency band maximum data is embedded. This gives maximum data embedding capacity and security used in steganography.

REFERENCES

[1] Singla, Deepak, and RupaliSyal. "Data Security Using LSB & DCT Steganography in Images." *International Journal Of Computational Engineering Research* 2 (2013): 359-364.

[2] Walia, Ekta, Payal Jain, and NavdeepNavdeep. "An analysis of LSB & DCT based steganography." *Global Journal of Computer Science and Technology* 10.1 (2010).

[3] Sheisi, Hossein, JafarMesgarian, and MostafaRahmani. "Steganography: Dct Coefficient Replacement Method and Compare WithJSteg Algorithm." *International Journal of Computer and Electrical Engineering* 4.4 (2012): 458-462.

[4] Patel, Hardik, and Preeti Dave. "Steganography Technique Based on DCT Coefficients." *International Journal of Engineering Research and Applications* 2.1 (2012): 713-717.

[5] Swati Kumravat, "An Efficient Steganographic Scheme Using Skin Tone Detection and Discrete Wavelet Transformation", International Journal of Computer Science & Engineering Technology (IJCSET), ISSN : 2229-3345 ,Vol. 4 No. 07 Jul 2013

[6] SunitaBarve, "Efficient and Secure Biometric Image Stegnography using Discrete Wavelet Transform", International Journal of Computer Science & Communication Networks,Vol 1(1), 96 ISSN:2249-5789

[7] Souvik Bhattacharyya and GautamSanyal "A Robust Image Steganography using DWTDifference Modulation (DWTDM)",I. J. Computer Network and Information Security, 2012, 7, 27-40

[8] S.Jayasudha,"Integer Wavelet Transform Based Steganographic Method Using OpaAlgorithm",International Journal Of Engineering And ScienceIssn: 2278-4721, Vol.2, Issue 4 (February 2013), Pp 31-35.

[9] Amitava Nag, SushantaBiswas, DebasreeSarkar&ParthaPratimSarkar,"A Novel Technique for Image Steganography Based on DWT andHuffmanEncoding",International Journal of Computer Science and Security, (IJCSS), Volume (4): Issue (6)

[10] AayushiVerma, RajshreeNolkha, Aishwarya Singh andGarimaJaiswal ,"Implementation of ImageSteganography Using 2-Level DWT Technique",International Journal of Computer Science and Business InformaticsISSN: 1694-2108 | Vol. 1, No. 1. MAY 2013 1

[11] N.F. Johnson and S. Jajdodia," Exploring steganography: Seeing the Unseen", IEEE computer, pp. 26-34, 1998.

[12] HediehSajedi,"Recent advances in Steganography", www.intechopen.com, ISBN 978-953-51-0840-5

[13] C. P. Sumathi,T. Santanamand G.Umamaheswari, "A Study of Various Stenographic Techniques Used for Information Hiding", International Journal of Computer Science & Engineering Survey, Vol.4, December 2013.

[14] Stefan Katzenbeiser& Fabien A.P.Petitcolas(1999), "Information Hiding Techniques for Steganography and Digital Watermarking", Artech House, Computer Security series, Boston, London.

[15] Abbas Cheddad, Joan Condell, Kevin Curran and Paul McKevitt, "Digital Image Steganography: Survey and Analysis of Current Methods", Signal processing, volume 90, Issue 3, March2010, pages 727-752.

BIOGRAPHY

Dipalee Borse is a Assistant Professor in the Computer Science Department, Dr.D.Y. Patil ACS college, Pimpri, Pune. She received MSC(CS) degree in 2009 from NMU, Jalgaon, MS, India. Her research interests are Steganography, Information Security

Shobhana Patil is a Assistant Professor in the Computer Science Department, Dr.D.Y. Patil ACS college, Pimpri, Pune. She received MSC(CS) degree in 2007 from SPPU, Pune , MS, India. Her research interests are Steganography, Information Security

DOI: 10.15680/IJIRCCE.2015. 0312093