International Journal Of

Recent Scientific Research

ISSN: 0976-3031

Volume: 7(3) March -2016

A REVIEW OF IMAGE STEGANOGRAPHY BASED ON DISCRETE WAVELET TRANSFORM

Rajendraprasad K and Narasimha V. B

THE OFFICIAL PUBLICATION OF
INTERNATIONAL JOURNAL OF RECENT SCIENTIFIC RESEARCH (IJRSR)
http://www.recentscientific.com/ recentscientific@gmail.com

ISSN: 0976-3031

Available Online at http://www.recentscientific.com

International Journal of Recent Scientific Research
Vol. 7, Issue, 3, pp. 9195-9201, March, 2016

International Journal of Recent Scientific Research

REVIEW ARTICLE

A REVIEW OF IMAGE STEGANOGRAPHY BASED ON DISCRETE WAVELET TRANSFORM

Rajendraprasad K and Narasimha V. B

[1]Department of Informatics, Osmania University, Hyderabad, Telangana, India
[2]Department of CSE, Osmania University, Hyderabad, Telangana, India

ARTICLE INFO

Article History:

Received 06th December, 2015
Received in revised form 14th January, 2016
Accepted 23rd February, 2016
Published online 28th March, 2016

Keywords:

Steganography, Wavelet Transformation, DWT, DCT

ABSTRACT

Image steganography is considered as method hiding information and secret communication of potential computer users over the internet. From the past time to present time security of confidential information is always an important issue. The main purpose of stegnography is to hide the existence of the message so that it becomes difficult for attacker to detect it. The discrete wavelet transform is used to embed the secret into the cover image and the inverse transform is used to recover the secret. In this technique provides robustness, better image quality and authentication ability. The stress is laid to improve the authentication ability of the secret image.

INTRODUCTION

The main purpose of Steganography is to hide the data into another data such as hiding data in other text or image file. Steganography hide the information in such away that only sender and receiver can know it. The two concepts that are closely related to Steganography are watermarking and fingerprinting that is mainly used for protection of property. Research in Steganography has been gain due to the lack in cryptographic system. Secret image sharing is a technique to prevent a secret from malicious modification, destruction and unauthorized disclosure by splitting the secret into several shares and recovering the secret from sufficient shares [1].

Usually images are ideal for information hiding because a large amount of redundant space is created in the storing of images. The secret is transmitted through the hidden media in such a manner that the very existence of the secret becomes undetectable and thereby unnoticed to the naked eye. Steganography means concealed writing. Steganography refers to the hiding of a secret behind the camouflage images. For hiding the data, there exist a variety of different techniques, but the proposed scheme uses the discrete wavelet transform to hide the data in the cover image and thereby shows promising results. The steganography techniques must satisfy:

A. The integrity of the hidden message after it has been embedded inside the cover object must be correct.
B. The cover object must remain unchanged or almost unchanged to the naked eye [2]. Generally image steganography is method of information hiding into cover-image and generates a stego- image. This stego-image then sent to the other party by known medium, where the third party does not know that this stego-image has hidden message. After receiving stego-image hidden message can simply be extracted with or without stego-key (depending on embedding algorithm) by the receiving end [21]. Basic diagram of image steganography is shown in Figure 1 without stego- key, where embedding algorithm required a cover image with message for embedding procedure. Output of embedding algorithm is a stego-image which simply sent to extracting algorithm, where extracted algorithm unhides the message from stego-image.

Corresponding author:* **Rajendraprasad K
Department of Informatics, Osmania University, Hyderabad, Telangana, India

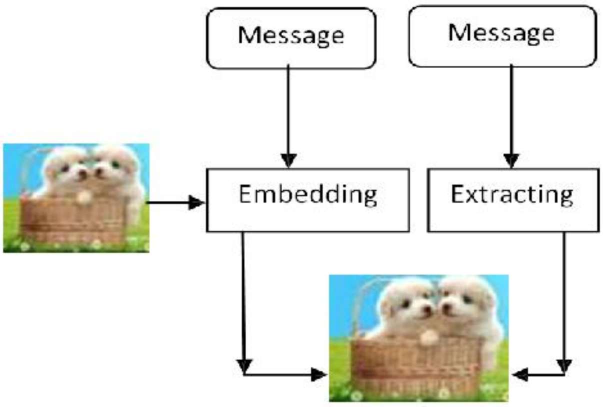


Fig1 Image Steganograph

There are many versions of spatial steganography, all directly change some bits in the image pixel values in hiding data. Least significant bit (LSB)- based steganography is one of the simplest techniques that hides a secret message in the LSBs of pixel values without introducing many perceptible distortions. Changes in the value of the LSB are imperceptible for human eyes. Spatial domain techniques are broadly classified into:

1. Least significant bit (LSB)
2. Pixel value differencing (PVD)
3. Edges based data embedding method (EBE)
4. Random pixel embedding method (RPE)
5. Mapping pixel to hidden data method
6. Labeling or connectivity method
7. Pixel intensity based method
8. Texture based method
9. Histogram shifting methods

Transform Domain Technique*:* This is a more complex way of hiding information in an image. Various algorithms and transformations are used on the image to hide information in it. Transform domain embedding can be termed as a domain of embedding techniques for which a number of algorithms have been suggested [17]. The process of embedding data in the frequency domain of a signal is much stronger than embedding principles that operate in the time domain. Most of the strong steganographic systems today operate within the transform domain Transform domain techniques have an advantage over spatial domain techniques as they hide information in areas of the image that are less exposed to compression, cropping, and image processing. Some transform domain techniques do not seem dependent on the image format and they may outrun lossless and lossy format conversions. Transform domain techniques are broadly classified into:International Journal of Advanced Science and Technology Vol. 54, May, 2013 117

1. Discrete Fourier transformation technique (DFT).
2. Discrete cosine transformation technique (DCT).
3. Discrete Wavelet transformation technique
4. (DWT).
5. Lossless or reversible method (DCT)
6. Embedding in coefficient bits

Distortion Techniques: Distortion techniques need knowledge of the original cover image during the decoding process where the 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 [18]. Using this technique, a stego object is created by applying a sequence of modifications to the cover image. This sequence of modifications is use to match the secret message required to transmit [19].The message is encoded at pseudo- randomly chosen pixels. If the stego-image is different from the cover image at the given message pixel, the message bit is a "1." otherwise, the message bit is a "0." The encoder can modify the "1" value pixels in such a manner that the statistical properties of the image are not affected. However, the need for sending the cover image limits the benefits of this technique. In any steganographic technique, the cover image should never be used more than once. If an attacker tampers with the stego-image by cropping, scaling or rotating, the receiver can easily detect it. In some cases, if the message is encoded with error correcting information, the change can even be reversed and the original message can be recovered [20].

Masking and Filtering: These techniques hide information by marking an image, in the same way as to paper watermarks. These techniques embed the information in the more significant areas than just hiding it into the noise level. The hidden message is more integral to the cover image. Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image.

Advantages of Masking and filtering Techniques

1. This method is much more robust than LSB replacement with respect to compression since the information is hidden in the visible parts of the image.

Disadvantages of Masking and filtering Techniques

1. Techniques can be applied only to gray scale images and restricted to 24 bits.

In [1] authors have proposed an adaptive least significant bit spatial domain embedding method. This method divides the image pixels ranges (0-255) and generates a stego-key. This private stego- key has 5 different gray level ranges of image and each range indicates to substitute fixed number of bits to embed in least significant bits of image. The strength of proposed method is its integrity of secret hidden information in stego-image and high hidden capacity. The limitation is to hide extra bits of signature with hidden message for its integrity purpose. It also proposed a method for color image just to modify the blue channel with this scheme for information hiding. This method is targeted to achieve high hidden capacity plus security of hidden message.

Yang *et al.*, in [2] proposed an adaptive LSB substitution based data hiding method for image. To achieve better visual quality of stego-image it takes care of noise sensitive area for embedding. Proposed method differentiates and takes advantage of normal texture and edges area for embedding. This method analyzes the edges, brightness and texture masking of the International Journal of Advanced Science and Technology Vol.

54, May, 2013 118 cover image to calculate the number of k-bit LSB for secret data embedding. The value of k is high at non-sensitive image region and over sensitive image area k value remain small to balance overall visual quality of image. The LSB‟s (k) for embedding is computed by the high-order bits of the image. It also utilizes the pixel adjustment method for better stego-image visual quality through LSB substitution method. The overall result shows a good high hidden capacity, but dataset for experimental results are limited; there is not a single image which has many edges with noise region like „Baboon.tif‟.

In [3] anthers have proposed LSB based image hiding method. Common pattern bits (stego-key) are used to hide data. The LSB‟s of the pixel are modified depending on the (stego-key) pattern bits and the secret message bits. Pattern bits are combination of MxN size rows and columns (of a block) and with random key value. In embedding procedure, each pattern bit is matched with message bit, if satisfied it modifies the 2nd LSB bits of cover image otherwise remains the same. This technique targets to achieve security of hidden message in stego-image using a common pattern key. This proposed method has low hidden capacity because single secret bit requires a block of (MxN) pixels.

In [4] author proposed a Pixel value difference (PVD) and simple least significant bits scheme are used to achieve adaptive least significant bits data embedding. In pixel value differencing (PVD) where the size of the hidden data bits can be estimated by difference between the two consecutive pixels in cover image using simple relationship between two pixels. PVD method generally provides a good imperceptibility by calculating the difference of two consecutive pixels which determine the depth of the embedded bits. Proposed method hides large and adaptive k-LSB substitution at edge area of image and PVD for smooth region of image. So in this way the technique provide both larger capacity and high visual quality according to experimental results. This method is complex due to adaptive k generation for substitution of LSB.

In [5] authors proposed a method of Multi-Pixel Differencing (MPD) which used more than two pixel to estimate smoothness of each pixel for data embedding and it calculate sum of difference value of four pixels block. For small difference value it uses the LSB otherwise for high difference value it uses MPD method for data embedding. Strength is its simplicity of algorithm but experimental dataset is too limited.

In [6] author proposed another pixel value differencing method, it used the three pixels for data embedding near the target pixel. It uses simple k-bit LSB method for secret data embedding where number of k-bit is estimated by near three pixels with high difference value. To retain better visual quality and high capacity it simply uses optimal pixel adjustment method on target pixels. Advantage of method is histogram of stego-image and cover-image is almost same, but dataset for experiments are too small.

In [7] authors have introduced a high capacity of hidden data utilizing the LSB and hybrid edge detection scheme. For edge computation two types of canny and fuzzy edges detection method applied and simple LSB substitution is used to embed the hidden data. This scheme is successful to embed data with higher peak signal to noise ratio (PSNR) with normal LSB based embedding. The proposed scheme is tested on limited images dataset. This method is not tested on extensive edges based image like„ Baboob.tif‟.

Madhu *et al.*, in [8] proposed an image steganography method, based on LSB substitution and selection of random pixel of required image area. This method is target to improve the security where password is added by LSB of pixels. It generates the random numbers and selects the region of interest where secret message has to be hidden. The strength of method is its security of hidden message in stego-image, but has not considers any type of perceptual transparency. An image steganographic method of mapping pixels to alphabetic letters. It maps the 32 letters (26 for English alphabetic and other for special characters) with the pixel values. Five (5) bits are required to represent these 32 letters and authors have generated a table where 4 cases design to represent these 32 letters. According to that table, each letter can be represented in all 4 cases. It utilizes the image 7 MSB (Most Significant Bits) (27 = 128) bits for mapping. Proposed method maps each 4- case from the 7 MSB‟s of pixel to one of the 32- cases in that table. These 4-cases increase the probability of matching. This algorithm keeps the matching pattern of cover-image which is then used for extracting data from the stego-image. Proposed method does not required any edge or smoothness computations but secret data should be in the form of text or letter for embedding.

In [10], authors have introduced a data hiding technique where it finds out the dark area of the image to hide the data using LSB. It converts it to binary image and labels each object using 8 pixel connectivity schemes for hiding data bits. This method required high computation to find dark region its connectivity and has not tested on high texture type of image. Its hiding capacity totally depends on texture of image.

In [16] a novel lossless or reversible data hiding scheme for binary images is proposed. JPEG2000 compressed data is used and the bit-depth of the quantized coefficients are also embedded into some code-blocks. Proposed data embedding method is useful for binary images not for gray or color images.

Babita *et al.*, in [11] uses 4 LSB of each RGB channel to embed data bits, apply median filtering to enhance the quality of the stego image and then encode the difference of cover and stego image as key data. In decoding phase the stego-image is added with key data to extract the hidden data. It increases the complexity to applying filtering and also has to manage stego-key. Proposed scheme has high secret data hiding capacity.

In [12] author have proposed a pixel indicator technique with variable bits; it chooses one channel among red, green and blue channels and embeds data into variable LSB of chosen channel. Intensity of the pixel decides the variable bits to embed into cover image. The channel selection criteria are sequential and the capacity depends on the cover image channel bits. Proposed method has almost same histogram of cover and stego-image.

Hamid *et al.*, in [13] have proposed a texture based image steganography. The texture analysis technique divides the texture areas into two groups, simple texture area and complex texture area. Simple texture is used to hide the 3-3-2 LSB (3 bits for Red, 3 bits for Green, 2 bits for Blue channels) method. On the other hand over complex texture area 4 LSB embedding technique is applied for information hiding. The above method used the both (2 to 4 LSB for each channel) methods depending on texture classification for better visual quality. Proposed method has high hidden capacity with considering the perceptual transparency measures e.g PSNR etc.

M. Chaumont *et al.,* in [14] have proposed a DCT based data hiding method. It hides the color information in a compress gray-level image. It follows the color quantization, color ordering and the data hiding steps to achieve image steganography. The purpose of method is to give free access to gray-level image to everyone but restricted access of same color images to those who have its stego-key. It has high PSNR plus with noticeable artifact of embedding data.

K. S. Babu *et al.*, in [15] proposed hiding secret information in image steganography for authentication which is used to verify the integrity of the secret message from the stego-image. The original hidden message is first transformed from spatial domain to discrete wavelet transform (DWT); the coefficients of DWT are then permuted with the verification code and then embedded in the special domain of the cover image.

Proposed Scheme

Wavelets are signals which are local in time and scale and generally have an irregular shape. A wavelet is a waveform of effectively limited duration that has an average value of zero. The term „wavelet" comes from the fact that they integrate to zero; they wave up and down across the axis. Many wavelets also display a property ideal for compact signal representation: orthogonality. This property ensures that data is not over represented. A signal can be decomposed into many shifted and scaled representations of the original mother wavelet. A wavelet transform can be used to decompose a signal into component wavelets. Once this is done the coefficients of the wavelets can be decimated to remove some of the details. Wavelets have the great advantage of being able to separate the fine details in a signal. Very small wavelets can be used to isolate very fine details in a signal, while very large wavelets can identify coarse details. In addition, there are many different wavelets to choose from. Various types of wavelets are: Morlet, Daubechies, etc. [9, 10]. One particular wavelet may generate a more sparse representation of a signal than another, so different kinds of wavelets must be examined to see which is most suited to image compression. A wavelet function Ψ(t) has two main properties,

$$\int_{-\infty}^{0} \Psi(t)dt = 0$$

That is, the function is oscillatory or has wavy appearance.

$$\int_{-\infty}^{0} |\Psi(t)|^2 dt < \infty$$

That is, the most of the energy in Ψ(t) is confined to a finite duration.

Discrete Wavelet Transformation

The proposed compression technique with pruning proposal based on discrete wavelet transform (DWT). The proposed technique first decomposes an image into coefficients called sub-bands and then the resulting coefficients are compared with a threshold. Coefficients below the threshold are set to zero. Finally, the coefficients above the threshold value are encoded with a loss less compression technique. The compression features of a given wavelet basis are primarily linked to the relative scarceness of the wavelet domain representation for the signal. The notion behind compression is based on the concept that the regular signal component can be accurately approximated using the following elements: a small number of approximation coefficients (at a suitably chosen level) and some of the detail coefficients.

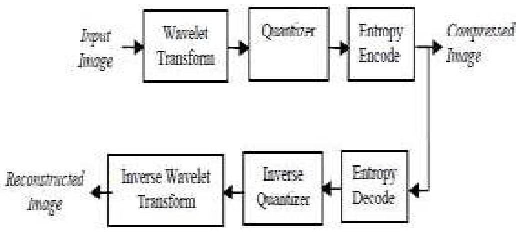


Fig2 Wavelet transform based compression.

The steps of the proposed compression algorithm based on DWT are described below:

I. Decompose

Choose a wavelet; choose a level N. Compute the wavelet. Decompose the signals at level N.

II. Threshold detail coefficients

For each level from 1 to N, a threshold is selected and hard thresholding is applied to the detail coefficients.

III. Reconstruct

Compute wavelet reconstruction using the original approximation coefficients of level N and the modified detail coefficients of levels from 1 to N. The prerequisite to the proposed technique is that cover image and the secret image should have the same size.

In general, the proposed technique consists of these phases: (a) embedding phase, (b) authentication phase, (c) extraction phase, (d) restoration phase.

Embedding Phase

In the embedding phase, the secret message signal is embedded into the cover image using the Haar DWT. Fig.1 shows the embedding procedure being followed. Initially, the cover image is used and Haar wavelet transform is applied to it. A 2- dimensional Haar-DWT consists of two operations: one is the horizontal operation and the other is the vertical one. Before embedding the secret into the cover image, the message signal is distorted by applying randomization. The technique of randomization scatters the secret throughout the whole surface so that the secret cannot be easily identified [10]. Further the result of Haar wavelet transform and message signal is combined in order to get the resulting stego image. The embedding is such that first the visual quality of the results has no serious downtrend, and second it is difficult to recognize that any data is hidden in the stego images. The embedding procedure satisfies both of these requirements [11].

Authentication Phase

In the authentication phase, the dealer can verify whether the stego images provided by the owner are tampered or not [12]. The verification procedure involves that if the secret has been tampered then during the extraction phase, the dealer would not be able to retrieve the original secret. The proposed technique enhances the data security by secret sharing. Instead of hiding data directly into the cover image pixels, the proposed technique embeds data in the form of scattered pixels.

Extraction Phase

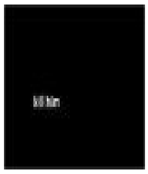
In the extraction phase, the secret has to be recovered from the stego image received by the receiver. The extraction procedure being followed. The cover image is decomposed into multi- resolution subbands [13]. The inverse DWT is applied to the stego image. The subbands of the cover image and stego image are subtracted in order to retrieve the secret. Thresholding is performed in order to regain the pixels which have been tampered due to noise addition. During the extraction phase, the stego image and the cover image are taken to recover the secret.

Restoration Phase

Digital images are easily corrupted by noise during transmission [1]. Firstly, identify unreliable bits i.e. the bits that have been altered in order to tamper the secret of each pixel in the embedded image by detecting noise in the stego image. Secondly, it determines corrupted pixels. For each corrupted pixel, the value of the corrupted pixels is corrected by adjusting the tampered bits. Restoration implies recovering the secret without any noise.

The cover image and the payload image. After the embedding phase, the resultant stego image appears named as wimage.fits. The fits format is better than JPG as it stores the thresholding values in terms of double, not as an 8-bit digit.

a)Cover Image



b) loaded Image

c) Stegno Image

fig3

The results are demonstrated in. Some noise is put onto the image of Fig.3 (a), as an intended attack to the image, yielding the noisy image of Fig.3 (c) which is then authenticated by the proposed technique. The secret is not retrieved when it has been altered [8]. So a blank image appears authenticating that the secret has been tampered.

Comparison of DCT Vs DWT

The Discrete Cosine Transform (DCT) algorithm is well known and commonly used for image compression. DCT converts the pixels in an image, into sets of spatial frequencies. It has been chosen because it is the best approximation of the Karhunen_loeve transform that provides the best compression ratio [5]. The DCT work by separating images into the parts of different frequencies. During a step called Quantization, where parts of compression actually occur, the less important frequencies are discarded, hence the use of the lossy. Then the most important frequencies that remain are used retrieve the image in decomposition process. As a result, reconstructed image is distorted.

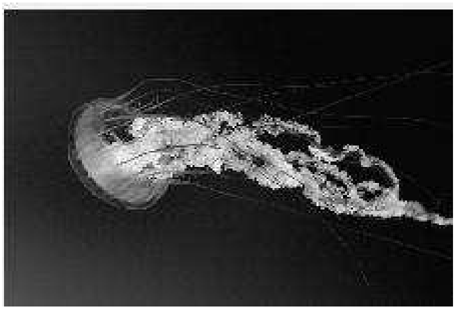


Fig 3 d Original image

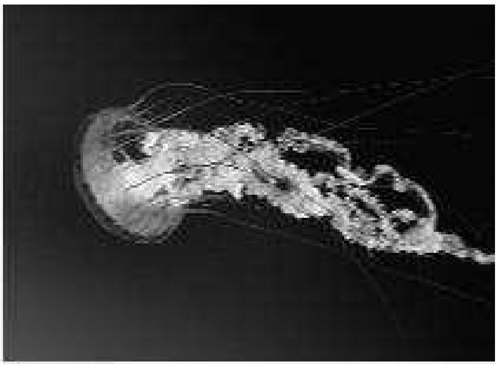


Fig 3e Compressed image of DCT Wavelet

Transform has become an important method for image compression. Wavelet based coding provides substantial improvement in picture quality at high compression ratios mainly due to better energy compaction property of wavelet transforms [8]. Wavelets are functions which allow data analysis of signals or images, according to scales or resolutions. The DWT represents an image as a sum of wavelet functions, known as *wavelets*, with different location and scale. It represents the data into a set of high pass (detail) and low pass (approximate) coefficients.

The input data is passed through set of low pass and high pass filters. The output of high pass and low pass filters are down sampled by 2.The output from low pass filter is an approximate coefficient and the output from the high pass filter is a detail coefficient [9]. This procedure is one dimensional (1-D) DWT. but in this research work we are using two dimensional (2-D) DWT. In case of in two directions, both rows and columns. The outputs are then down sampled by 2 in each direction as in case of 1-D DWT [8]. Output is obtained in set of four coefficients LL, HL, LH 2-D DWT, the input data is passed through set of both low pass and high pass filter and HH. The first alphabet represents the transform in row where as the second alphabet represents transform in column. The alphabet L means low pass signal and H means high pass signal. LH signal is a low pass signal in row and a high pass in column. Hence, LH signal contain horizontal elements. Similarly, HL and HH contains vertical and diagonal elements, respectively [10].

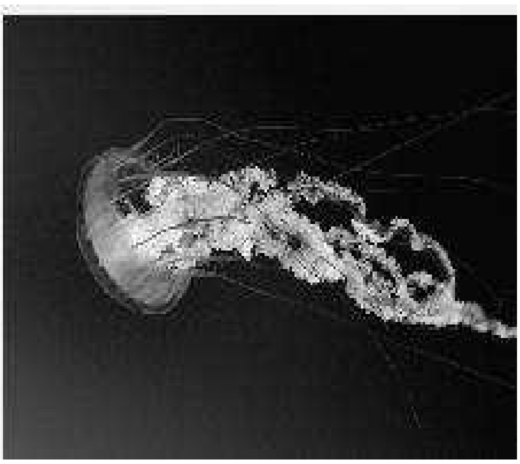


Fig3.f Original image

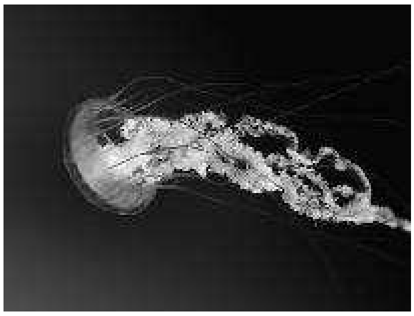


Fig.3.g compressed Image of DWT

We are comparing the images which are compressed by applying DCT and DWT using MATLAB. Figure4 and Figure5 shows peak signal to noise ratio graph of DCT and DWT, Figure6 and figure7 shows bit error rate graph of DCT and DWT, TABLE 1 shows peak signal to noise ratio, bit error rate, compression ratio, Mean square error and time of the compressed images of DCT and DWT.

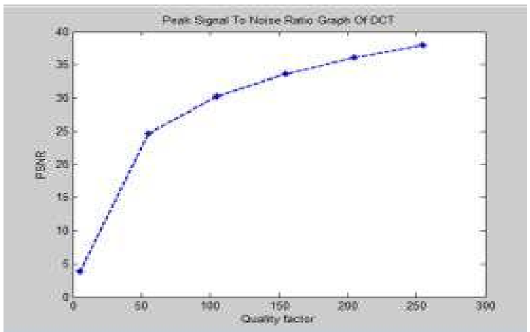


Fig4 PSNR graph of DCT

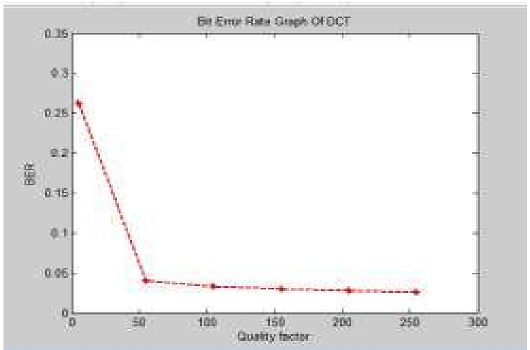


Fig5 BER graph of DCT

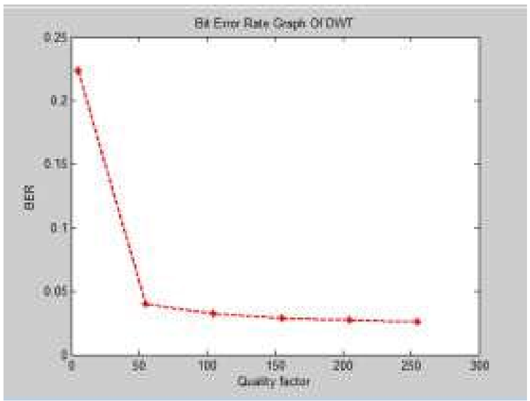


Fig6 PSNR graph of DCT

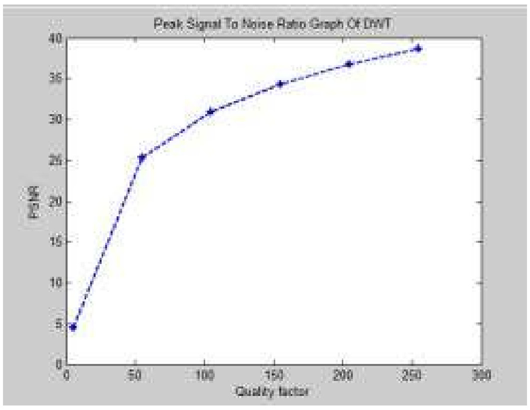


Fig.*7* BER graph of DWT

	DCT	DWT
Comparison Ratio	20.1763	20.3955
PSNR	0.0263	38.6309
MSE	10.3820	8.9123
BER	37.9680	0.0259
TIME	7.4121	3.5139

CONCLUSION

In this paper As steganography becomes widely used in computing, there are issues that need to be resolved. the secret image sharing scheme in the DWT domain as related to image science. A new and efficient secret image sharing technique for embedding the secret messages into images without producing any major changes. it has been seen that this technique is better than technique in terms of image quality and tampering results. Embedding capacity of this technique is much better than the existing techniques in the frequency domain such as DCT. Beside this technique provides robustness which can avoid various image attacks, noise addition. Hiding secret data into the transform domain.

References

1. Dulce R. Herrera-Moro, Raúl Rodríguez-Colín, Claudia Feregrino-Uribe "Adaptive Steganography based on textures",17th International Conference on Electronics, Communicationsand Computers (CONIELECOMP'07).
2. YildirayYalman 1 , FeyziAkar 2 and Ismail Erturk "Contemporary Approaches to the Histogram Modification
3. Blossom Kaur, Amandeep Kaur, Jasdeep Singh "Steganographic Approach For Hiding Image In Dct Domain", *International Journal of Advances in Engineering & Technology*, July 2011.
4. Xuefeng Wang Zhen Yao Chang-Tsun Li "A Palette-Based Image Steganographic Method Using Colourquantisation", Image Processing, 2005. ICIP 2005. IEEE International Conference on 11-14 Sept. 2005
5. Souvik Bhattacharyya, Gautam Sanyal "Study and analysis of quality of service in different image based steganography using Pixel Mapping Method(PMM)", *International Journal of Applied Information Systems* (IJAIS) – ISSN : 2249-0868
6. Foundation of Computer Science FCS, New York, USA Volume 2– No.7, May 2012 – www.ijais.org [6] M.Shobana, R.Manikandan "Efficient Method For Hiding Data By Pixel Intensity", M.Shobana *et al.* / *International Journal of Engineering and Technology* (IJET), Vol 5 No 1 Feb-Mar 2013
7. K. Naveen BrahmaTeja, Dr. G. L. Madhumati, K. Rama Koteswara Rao "Data Hiding Using EDGE Based Steganography", *International Journal of Emerging Technology and Advanced Engineering* (ISSN 2250-2459, Volume 2, Issue 11, November 2012).
8. Hemalatha S., U Dinesh Acharya, Renuka A. and Priya R. Kamath"An Integer Wavelet Transform Based Steganography Technique for Color Images", *International Journal of Information & Computation Technology*. ISSN 0974-2239 Volume 3, Number 1 (2013), pp. 13-24.
9. Vijay Kumar and Dinesh Kumar "Performance evaluation of DWT based image steganography", Advance computing conference (IACC), 2010 IEEE 2nd International.
10. H. Motameni, M. Norouzi, M. Jahandar, and A. Hatami "Labeling Method in Steganography", World Academy of Science, Engineering and Technology *International Journal of Computer, Information Science and Engineering* Vol:1 No:6, 2007.
11. W. Zhang, S. Wang, and X. Zhang, "Improving embedding efficiency of covering codes for applications in steganography," IEEE Communications Letters, vol. 11, pp. 680–682, August 2007.

****

How to cite this article:

Rajendraprasad K and Narasimha V. B.2016, A Review of Image Steganography Based on Discrete Wavelet Transform. *Int J Recent Sci Res.* 7(3), pp. 9195-9201.

ISSN 0976-3031
9 770976 303009 >