Volume 5, No. 5, May 2014
Journal of Global Research in Computer Science
REVIEW ARTICLE
Available Online at www.jgrcs.info
ISSN-2229-371X

A STUDY OF STEGANOGRAPHY TECHNIQUES USING DISCRETE WAVELET TRANSFORM

Pratap Chandra Mandal
Asst. Prof., Department of Computer Application
B.P.Poddar Institute of Management & Technology
Kolkata, West Bengal, India
pcmandal9@gmail.com

***Abstract*—**Steganography is the science that involves communicating secret data in an appropriate multimedia carrier .The goal here is always to conceal the very existence of the embedded data .Unlike the space domain approaches, secret messages are embedded in the high frequency coefficients resulted from Discrete Wavelet Transform. Coefficients in the low frequency sub-band are preserved unaltered to improve the image quality.In this paper a detailed survey of existing and newly proposed steganographic techniques has been discussed.

Keywords- Digital image ,steganography, spatial domain, frequency domain, DWT

I. INTRODUCTION

Steganography is the art of hiding information through original files in such a way that the existence of the message cannot be known. The term steganography is comes from Greek word Steganos, which means, "Covered Writing". Now a day a lot of applications are Internet-based and in some cases it is desired that the communication be made secret. There are two techniques are available to achieve this goal. One is cryptography, where the sender uses an encryption key to encrypt the message, this encrypted message is transmitted through the insecure public channel, and decryption algorithm is used to decrypt the message. The reconstruction of the original message is possible only if the receiver has the decryption key. The second method is steganography, where the secret message is inserted in another medium.

The original files can be referred to as cover image. A stego-key is used for hiding process to restrict detection and/or recovery of the embedded data. Steganography differs from cryptography. The purpose of cryptography is to secure communications by changing the data into a form that cannot be understood. Steganography techniques, on the other hand, hide the existence of the message itself, which makes it difficult for a third person to find out where the message is. Sometimes sending encrypted information may draw attention, while invisible information will not.Both techniques can be used together to better protect information. In this case, even if steganography fails, the message cannot be recovered because a cryptography technique is used as well. The cracking of steganographic messages is called steganalysis. The purpose of steganalysis is to identify the information and determining that whether or not they have hidden messages encoded into them and if possible, extract the hidden information [1].

Design of a steganographic system can be categorized into spatial domain methods and transform domain methods .In spatial domain, the processing is applied on the image pixel values . In the transform domain method, the first step is to transform the cover image into frequency domain. Then the transformed coefficients are processed for hiding the secret information. However, methods of this type are computationally complex. Steganography methods using DCT , DWT, DFT come under this category

.

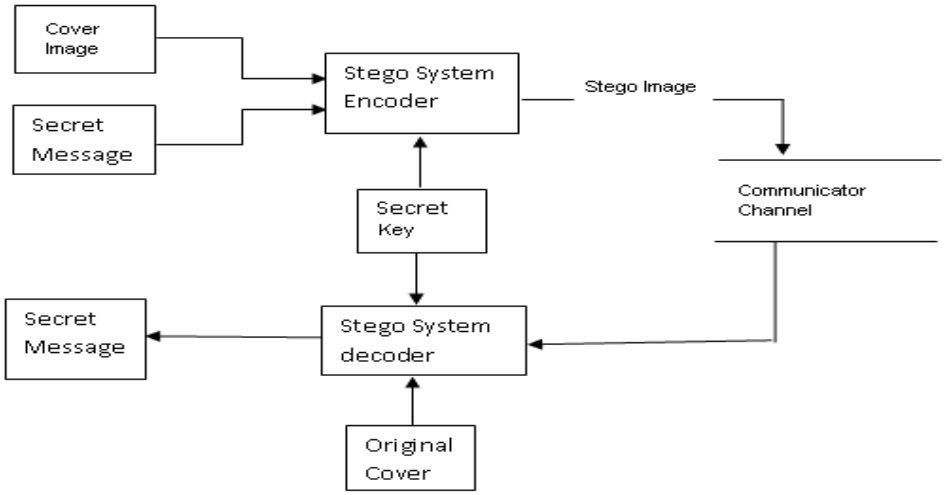

Figure 1: Steganography System

II. INFORMATION-HIDING SYSTEM FEATURES

An information-hiding system is characterized by three different aspects that contend with each Other. They are capacity, security, and robustness. Capacity means, the amount of information that can be hidden in the cover medium, security to an eavesdropper's inability to detect hidden information, and robustness to the amount of modification the stego medium can withstand before an adversary can destroy hidden information [3]. Information hiding relates to both watermarking and steganography. A watermarking system's primary goal is to achieve a high level of robustness-that is, it should be impossible to remove a watermark without degrading the data object's quality. Steganography, on the other hand, strives for high security and capacity, but often entails that the hidden information is fragile.

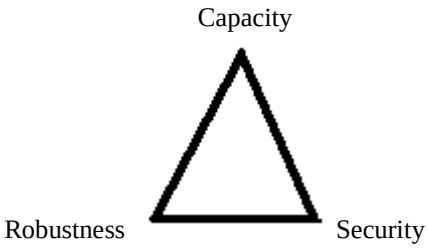

Figure 2 : Information hiding system features

III. DIFFERENT KINDS OF STEGANOGRAPHY

The four main categories of file formats that can be used for steganography are:
I. Text
II. Images
III. Audio
IV. Protocol

I. Text steganography: Hiding information in text is the most important method of steganography.The method was to hide a secret message in every nth letter of every word of a text message. After booming of Internet and different type of digital file formats it has decreased in importance. Text stenography using digital files is not used very often because the text files have a very small amount of redundant data.

II. Image steganography: Images are used as the popular cover objects for steganography. A message is embedded in a digital image through an embedding algorithm, using the secret key. The resulting stego image is send to the receiver.On the other side, it is processed by the extraction algorithm using the same key. During the transmission of stego image unauthenticated persons can only notice the transmission of an image but can't guess the existence of the hidden message.

III. Audio steganography: Audio stenography is masking, which exploits the properties of the human ear to hide information unnoticeably. An audible, sound can be

inaudible in the presence of another louder audible sound .This property allows to select the channel in which to hide information.[4]

IV. Protocol steganography: The term protocol steganography is to embedding information within network protocols such as TCP/IP. We hide information in the header of a TCP/IP packet in some fields that can be either optional or are never used.

IV. STEGANOGRAPHIC TECHNIQUES

There are two basic types of steganography: spatial steganography, transform steganography.

I. Spatial Domain Technique: 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. To our human eye, changes in the value of the LSB are imperceptible. Embedding of message bits can be done either sequentially or randomly. Least Significant Bit (LSB) replacement, LSB matching, Matrix embedding and Pixel value, differencing are some of the spatial domain techniques.

II. 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. [2]. 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 LSB 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 :

1. Discrete Fourier transformation technique (DFT).
2. Discrete cosine transformation technique (DCT).
3. Discrete Wavelet transformation technique (DWT).

V. DISCRETE WAVELET TRANSFORM

Discrete Wavelet Transform is used for digital images. Many DWTs are available. Depending on the application most appropriate one should be used. To hide text message integer wavelet transform can be used. When DWT is applied to an image it is decomposed into four sub bands: LL, HL, LH and HH.

The LL part contains the most significant features. So if the information is hidden in LL part the stego image can withstand compression or other manipulations. Sometimes distortion may be produced in the stego image and then other sub bands can be used [11].

DWT is becoming more popular and is replacing DCT and DFT in many applications such as compression. DWT has excellent properties, mainly suitable for compression and embedding, as listed below:

1. Decomposition of the signal into different frequency bands by DWT closely matches with the HVS characteristics and this makes it possible to processes the different frequency bands independently
2. The high frequency sub bands in DWT locate the image features such as edges and texture regions, which are less sensitive to HVS characteristics and hence can be used for embedding.
3. In compression, multiresoluton representation property of DWT is suitable for transmission of image and video data.

Because of the above attractive properties we considered the use of Discrete Wavelet Domain for steganography. The decomposition of Lena image by 2 levels of 2D - DWT is shown in Figure 3.

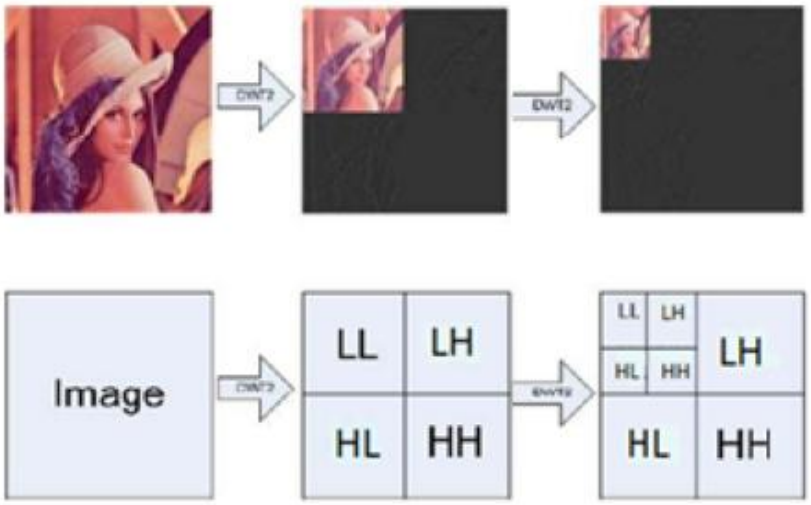

Figure 3 : 1 Level 2D – DWT of Lena Image

VI. TRANSFORMATION TECHNIQUE

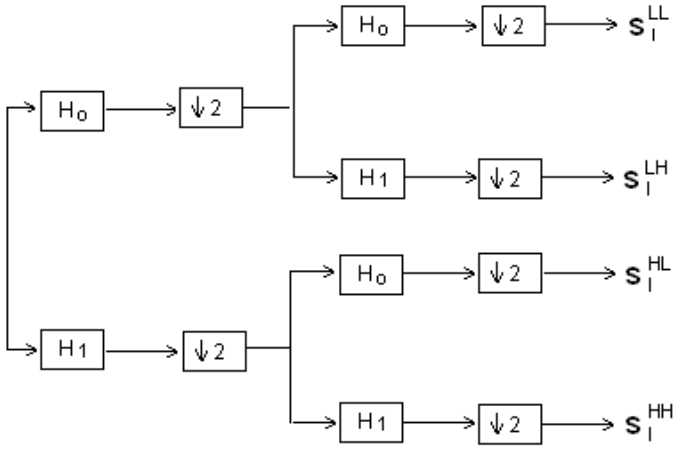

Figure 4: illustration of 1-level 2-d wavelet transformation

For transforming the image into wavelet domain, wavelet filters are applied row wise and then column wise or vice versa, depending on the user's choice. Figure 4 shows 2-D transform of the image. H0 and H1 represents the low-pass and high-pass filters and $\downarrow 2$ Shows the down sampling by two. As shown in figure 4 , first both low-pass and high-pass filters are applies on the image and down sampled column wise to low-pass and high-pass filtered data. The same filters are applied on these data column wise and down sampled row wise to form three detail subbands which correspond to horizontal (LH), vertical (HL) and diagonal (HH) and one approximate (LL) subband. For obtaining next level subbands the same procedure is repeated on the approximate subband of the previous level. For a decomposition of L-levels a total of 3 detail subbands and one approximate subband are obtained. Each as shown in figure 4 is represented by $S_l^{\#}$, where l= {0,1,….,L-1} represents the orientation of the subband.

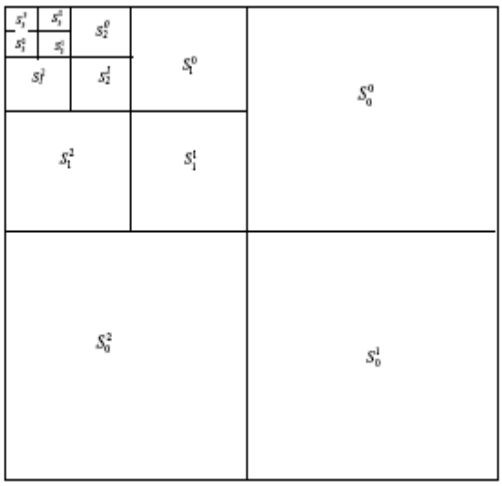

Figure 5 : 4-Level wavelet decomposed image representation.

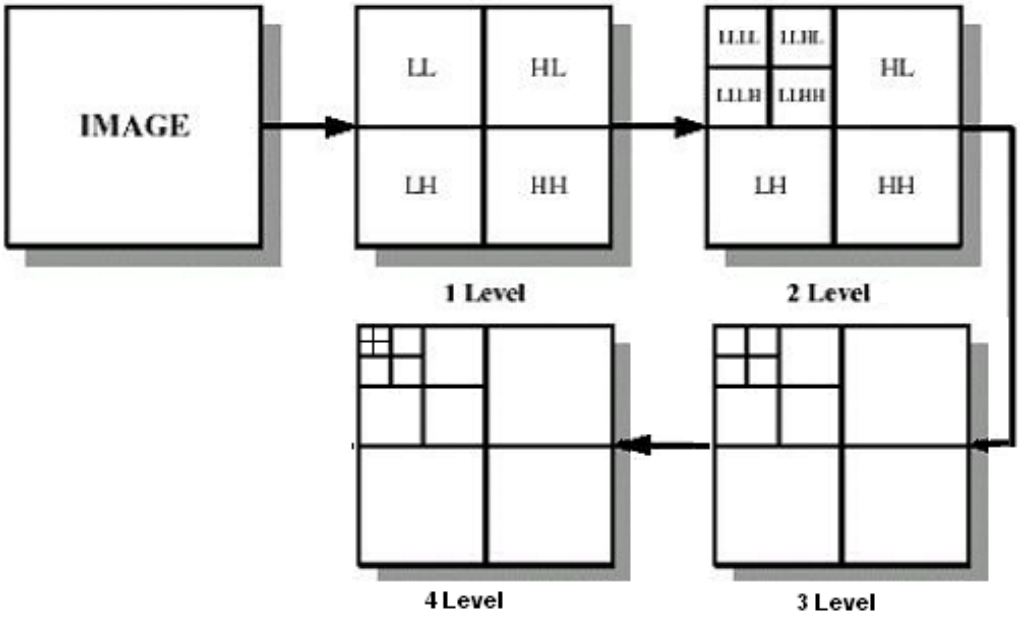

Figure.6: 4 Level Discrete Wavelet Transform

VII. LITERATURE SURVEY

Po-Yueh Chen et al. [6] proposed a new steganography technique which embeds the secret messages in frequency domain. According to different users' demands on the embedding capacity and image quality, the algorithm is divided into two modes and 5 cases. Secret messages are embedded in the high frequency coefficients resulted from Discrete Wavelet Transform. Coefficients in the low frequency sub-band are preserved unaltered to improve the image quality. Some basic mathematical operations are performed on the secret messages before embedding. These operations and mapping table keep the messages away from stealing, destroying from unintended users on the internet and provide satisfactory security.

H S Manjunatha Reddy et al ,[7] In their paper, high capacity and Secured Steganography using Discrete wavelet transform (HCSSD) has proposed. The wavelet coefficients of both the cover and payload are fused into single image using embedding strength parameters alpha and beta. The cover image and payload are preprocessed to reduce the pixel range to ensure the payload is recovered accurately at the destination. This is observed that the capacity and security is increased with acceptable PSNR in the proposed algorithm.

In paper [8] ,the proposed method pre-adjusts the original cover image in order to guarantee that the reconstructed pixels from the embedded coefficients would not exceed its maximum value and hence the message will be correctly recovered. Then, they uses Wavelet transform to transform both the cover image and the hidden message. Wavelet transform allows perfect embedding of the hidden message and reconstruction of the original image .

Elham Ghasemi et al. [9] shows the application of Wavelet Transform and Genetic Algorithm in a novel steganography scheme. They employ a genetic algorithm based mapping function to embed data in Discrete Wavelet Transform coefficients in 4x4 blocks on the cover image. The optimal pixel adjustment process is applied after embedding the message. They utilize the frequency domain to improve the robustness of steganography and, they implement Genetic Algorithm and Optimal Pixel Adjustment Process to obtain an optimal mapping function to reduce the difference error between the cover and the stego-image, therefore improving the hiding capacity with low distortions. Simulation results reveal that the novel scheme outperforms adaptive steganography technique based on wavelet transform in terms of peak signal to noise ratio and capacity, 39.94 dB and 50% respectively.

Amitava Nag et al. [10] presents a novel technique for Image steganography based on DWT. Firstly 2D Discrete Wavelet Transform is performed on a gray level cover image of size M × N and Huffman encoding is performed on the secret messages/image before embedding. Then each bit of Huffman code of secret message/image is embedded in the high frequency coefficients resulted from DWT. Image quality is to be improved by preserving the wavelet coefficients in the low frequency subband. The experimental results shows that the algorithm has a high capacity and a good invisibility.PSNR of cover image with stego-image shows the better results in comparison with other existing steganography approaches.In this paper, the major importance is given on the secrecy as well as the privacy of information.

Hemalatha S et al. [11] provides a novel image steganography technique that hides both image and key in color cover image using Discrete Wavelet Transform (DWT) and Integer WaveletTransform (IWT). There is no visual difference between the stego image and the cover image. The extracted image is similar to the secret image. This is proved by the high PSNR (Peak Signal to Noise Ratio),value for both stego and extracted secret image. In their proposed method, the cover image is 256x256 lena

color image. The secret information is grey scale image of size 128 x128. To transfer the secret image confidentially, the secret image itself is not hidden, instead a key is generated.Then the key is encrypted .The resultant key is hidden in the cover image using Integer Wavelet Transform (IWT). This improves the security and also the capacity can be improved to some extent since the key is compressed.

In paper[12], **Prabakaran Ganesan et al.** proposed a high secure steganography scheme hiding a 256×256 size gray secret image into a 512×512 size gray cover image with different combination of Discrete Wavelet Transform and Integer Wavelet Transform (IWT). Pixel Value Adjustment is first performed on cover image. The secret image values are scrambled by using Arnold transform. The DWT /IWT is applied on both the cover and scrambled secret image. Blending process is applied to both images and compute I DWT/IWT on the same to get the stego image. The extraction model is the reverse process of the embedding model. Different combination of DWT/IWT transform is performed on the scrambled secret image and cover image to achieved high security and robustness. Hybrid transform combination approach and case analysis provided the various hiding environment. Experimental results and case study provided the stego-image with perceptual invisibility, high security and certain robustness.

In paper [13] **Hemalatha S. et al.** proposes a secure color image steganography technique to hide a secret image using the keys.The secret image is hidden by considering the three color components separately. The keys are generated using the corresponding color components and the keys are hidden in the respective color components of the cover image. Using the keys the secret image can also be extracted. Integer Wavelet Transform is used to hide the keys. Experimental results shows better Peak Signal to Noise Ratio (PSNR), which is a measure of security compared to other existing color image steganography techniques. In their technique the secret information is hidden in the middle bit-planes of the integer wavelet coefficients in high frequency sub-bands.

In the paper[14], **Preeti Chaturvedi and R. K. Bairwa** have proposed a data hiding scheme that hides data into the integer wavelet coefficients of an image. The system combines a data hiding technique and the optimum pixel adjustment algorithm to increase the hiding capacity of the system compared to other systems. This method hide secret data in a random order using a secret key only known to both sender and receiver. This method, embeds different number of bits in each wavelet co-efficicient according to a hiding capacity function in order to increasing the hiding capacity without losses of the visual quality of stego image. It minimizes the error difference between original coefficients values and modified values by using the optimum pixel adjustment algorithm.

Figure 7 shows a general representation of the steganography method proposed by Ali Al-Ataby [8] .

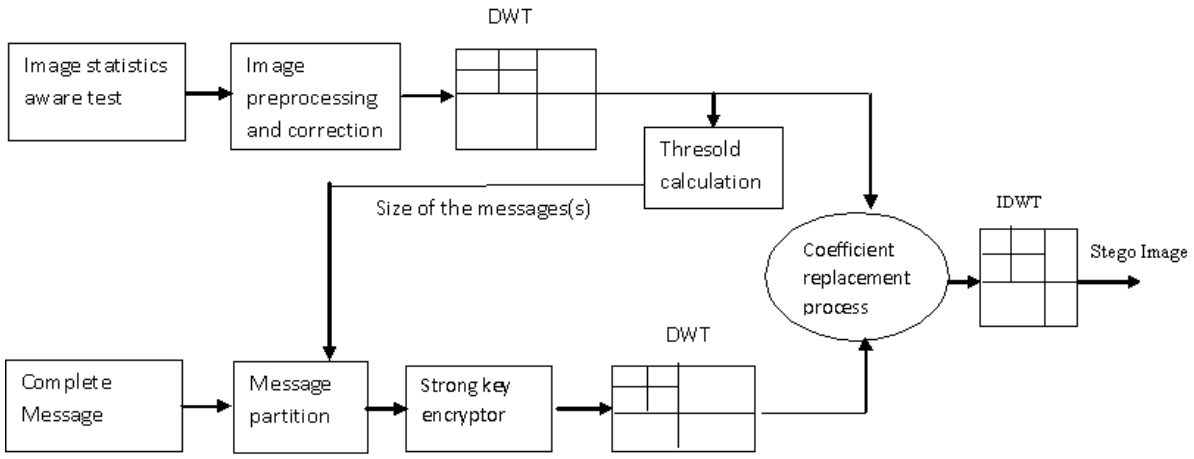

Figure 7 : general representation of the steganography method[8].

Figure 8 : Original Lena Image

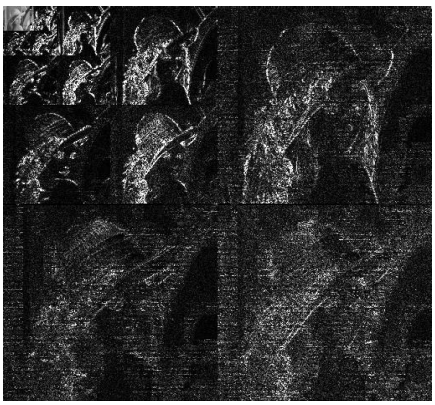

Figure 9 : 4 Level W T Lena Image

Figure 10 : hidden Image

Figure 11: 1 Level WT of hidden image

Figure 12: stego Lena Image

VIII. CONCLUSION

In this paper a survey on the current literature on steganography using Discrete Wavelet Transform. has been done . It presented a background discussion on the major algorithms of steganography deployed in digital imaging. The emerging techniques such as DWT is not too prone to attacks, especially when the hidden message is small. This is because they alter coefficients in the transform domain, thus image distortion is kept to a minimum. Generally these method tend to have a lower payload compared to spatial domain algorithms. There are different ways to reduce the bits needed to encode a hidden message. This explores how these techniques can be implemented in the fields where security of data is the prime concern.

REFERENCES

[1] Ramanpreet Kaur,Prof.Baljit Singh "survey and analysis of various steganographic techniques ", international journal of engineering science & advanced technology, Volume-2 , Issue-3, 561 – 566, May-June 2012.

[2] N. F. Johnson, S. Katzenbeisser. "A Survey of steganographic techniques." in Information Hiding Techniques for Steganography and Digital Watermarking, S.Katzenbeisser and F.Petitcolas, Ed. London: Artech House, 2000,

pp. 43-78

[3] Ali Al-Ataby1 and Fawzi Al-Naima 2 ," A Modified High Capacity Image Steganography Technique Based on Wavelet Transform", The International Arab Journal of Information Technology, Vol. 7 , No. 4 , October 2010

[4] S.C.Katzenbeisser."Principlesof Steganography ."in Information Hiding Techniques for Steganography and Digital Watermarking, S. Katzenbeisser and F. Petitcolas, Ed. London: Artech House, 2000, pp. 43- 78

[5] P. Kruus, C. Scace ,M. Heyman, and M. Mundy. (2003), " A survey o f steganography techniques for image files." Advanced Security Research Journal . [On line] , 5(1), . 41-52.

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

[7] 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)

[8] Ali Al-Ataby1 and Fawzi Al-Naima2 "A Modified High Capacity Image Steganography TechniqueBased on Wavelet Transformography ",The International Arab Journal of Information Technology, Vol.7, No. 4, October 2010.

[9] Elham Ghasemi, Jamshid Shanbehzadeh, Nima Fassihi, High Capacity Image Steganography Using Wavelet Transform and Genetic Algorithm", proceedings of the international multiconference of ngineers and Computer Scientists 2011 Vol I,IMECS 2011,March 16-18,Hong Kong

[10] Amitava Nag , Sushanta Biswas , Debasree Sarkar ,Partha Pratim Sarkar, "A Novel Technique for Image Steganography Based on DWT and Huffman Encoding", International Journal of Computer Science and Security, (IJCSS), Volume (4): Issue (6)

[11] Hemalatha S1, U Dinesh Acharya2, Renuka A3, Priya R. Kamath4," A secure color Image Steganography in transform domain ", International Journal on Cryptography and Information Security (IJCIS), Vol.3, No.1, March 2013

[12] Prabakaran Ganesan and R. Bhavani," A high secure and robust Image steganography using dual wavelet blending model ", Journal of Computer Science 9 (3): 277-284, 2013.

[13] Hemalatha S.1, U Dinesh Acharya2, Renuka A.3 and Priya R. Kamath4," 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

[14] Preeti Chaturvedi1, R. K. Bairwa2 ," An Integer Wavelet Transform Based Steganography Technique for Concealing Data in Colored Images", International Journal of Recent Research and Review, Vol. VII, Issue 1, March 2014

[15] Abbas Cheddad , Joan Conde ,Kevin Curran, PaulMcKevitt "Digital Imagesteganography : Surveand analysisof currentmethods", Signal Processing 90 (2010) 727–752

