IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
nCORETech
LBS College of Engineering, Kasaragod
Vol. 3, Special Issue 1, February 2016

# Image Steganography Using Discrete Wavelet Transform – A Review

**Tushara M[1], K. A. Navas[2]**

M. Tech Scholar, Dept of Electronics & Communication Engineering, LBS College of Engineering, Kasaragod, India[1]

Principal, LBS College of Engineering, Kasaragod, India [2]

**Abstract**: Steganography is the art and science of hiding information. Steganography methods are categorised into spatial domain and transform domain methods. Transform domain methods are gaining importance as they provide better security compared to spatial domain methods. Among the other transform domain steganography techniques, techniques that use discrete wavelet transform are becoming increasingly popular because DWT has excellent properties suitable for embedding. This paper presents a review on steganography techniques that use discrete wavelet transform.

**Keywords:** Digital image steganography, spatial domain, frequency domain, DWT.

## I. INTRODUCTION

Steganograpy involves hiding information in a cover media which may be text, image, audio or video. In image steganography the cover media used is image. The image obtained after hiding data is called stego image. The term steganography is formed from two greek words, 'stegano' which means covered and 'graph' which means writing. Two techniques that make secret communication possible are cryptography and steganography. Cryptography is concerned with protecting the contents of the message whereas steganography conceals the existence of the message. Both cryptography and steganography can be used together to improve security.

Three different aspects that charaterise steganography systems are: capacity, imperceptibility and security. Capacity is the maximum number of bits that can be hidden in the cover image without effecting its visual quality. Imperceptibility means that the process of data embedding should not make any perceivable alterations to the cover image. Security means steganalysers should not be able to detect hidden data.

Steganography techniques are basically categorised into spatial and transform domain techniques. In spatial domain techniques, data embedding is done in the image pixel values. In transform domain techniques, the image is first converted to frequency domain and secret data are embedded in the transform coefficients. Such techniques include those which use transforms like DCT, DFT and DWT. Transform domain techniques are computationally more complex compared to spatial domain techniques.

This paper presents a study of transform domain steganography techniques that use DWT. Section II provides an introduction about the basic concepts of DWT. In section III a discussion on few steganography techniques that make use of DWT is presented. The conclusion derived from the study is presented in the last section.

## II. DISCRETE WAVELET TRANSFORM

The wavelet transform describes a multi-resolution decomposition process in terms of expansion of an image onto a set of wavelet basis functions. DWT has its own excellent space frequency localization property. The DWT splits the signal into high and low frequency parts. The high frequency part contains information about the edge components, while the low frequency part is split again into high and low frequency parts. The high frequency components are usually used for steganography since the human eye is less sensitive to changes in edges.

In two dimensional applications, for each level of decompositions, first perform the DWT in the vertical direction, followed by the DWT in the horizontal direction. After the first level of decomposition, there are four sub-bands: LL1, LH1, HL1 and HH1. For each successive level of decomposition, the LL sub-bands of the previous level is used as the input. To perform second level decomposition, the DWT is applied to LL1 band which decomposes the LL1 band into four sub-bands: LL2, LH2, HL2 and HH2. Figure 1 shows the three phase decomposition of an image using DWT.

Discrete wavelet transform is used in digital images. On applying DWT, the image is decomposed into four sub-bands: LL, LH, HL and HH. The LL part contains most important details about the image. Embedding in LL part makes stego image resistant to various attacks but can lead to distortions in stego image.

Some of the properties that make DWT based steganography techniques more popular compared to other transform based techniques are:

IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
nCORETech
LBS College of Engineering, Kasaragod
Vol. 3, Special Issue 1, February 2016

(i) Decomposition of the signal into different frequency bands by DWT closely matches with the human visual system (HVS) characteristics and this makes it possible to process the different frequency bands independently
(ii) 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.

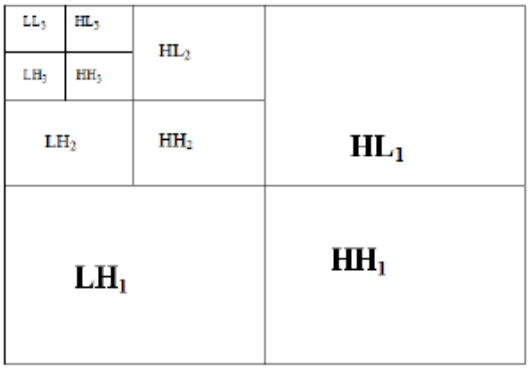


Fig.1 Three phase decomposition using DWT

## III.DWT BASED STEGANOGRAPHY TECHNIQUES

Various works have been done in the field of steganography using DWT. A few of these techniques are studied and analysed here.

A. High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm
Ghasemi et al. [1] presented a steganography technique that uses wavelet transform and genetic algorithm. A genetic algorithm based mapping function is used 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. Processing in frequency domain improve the robustness of steganography. The use of Genetic Algorithm and Optimal Pixel Adjustment Process results in an optimal mapping function to reduce the difference error between the cover and the stego-image, thereby improving the hiding capacity with low distortions**.**
The proposed method embeds the message in Discrete Wavelet Transform coefficients based on GA and OPAP algorithm and then applied on the obtained embedded image.
Haar Discrete Wavelet Transform: DWT analysis divides signal into two classes (i.e. Approximation and Detail) by signal decomposition for various frequency bands and scales. DWT utilizes two function sets: scaling and wavelet which associate with low and high pass filters orderly. Such a decomposition manner bisects time separability. In other words, only half of the samples in a signal are sufficient to represent the whole signal, doubling the frequency separability.
Haar wavelet operates on data by calculating the sums and differences of adjacent elements. This wavelet operates first on adjacent horizontal elements and then on adjacent vertical elements. One nice feature of the Haar wavelet transform is that the transform is equal to its inverse. Each transform computes the data energy in relocated to the top left hand corner. After each transform is performed the size of the square which contains the most important information is reduced by a factor of 4.
Genetic Algorithm: Genetic Algorithm is a technique which mimics the genetic evolution as its model to solve problems. The given problem is considered as input and the solutions are coded according to a pattern. The fitness function evaluates every candidate solution most of which are chosen randomly. Evolution begins from a completely random set of entities and is repeated in subsequent generations. The most suitable, and not the bests, are picked out in every generation. Use of GA aims to improve the image quality.

Embedding Algorithm: The following steps explain the embedding process:
Step1. Divide the cover image into 4×4 blocks.
Step2. Find the frequency domain representation of blocks by 2D Haar Discrete Wavelet Transform and get four sub-bands LL1, HL1, LH1, and HH1.
Step3. Generate 16 genes containing the pixels numbers of each 4×4 blocks as the mapping function.
Step4. Embed the message bits in k-LSBs DWT coefficients each pixel according to mapping function. For selecting value of k, images are evaluated from k=3 to 6. K equal to 1 or 2, provide low hiding capacity with high visual quality of the stego image and k equal to 7 or 8, provide low visual quality versus high hiding capacity.
Step5. Fitness evaluation is performed to select the best mapping function.

IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
nCORETech
LBS College of Engineering, Kasaragod
Vol. 3, Special Issue 1, February 2016

Step6. Apply Optimal Pixel Adjustment Process on the image.
Step7. Calculate inverse 2D-HDWT on each 4×4 block.

Extraction Algorithm: The extraction algorithm consists of four steps as follows:
Step1. Divide the cover image into 4×4 blocks.
Step2. Extract the transform domain coefficient by 2D HDWT of each 4×4 block.
Step3. Employ the obtained function in the embedding phase and find the pixel sequences for extracting.
Step4. Extract k-LSBs in each pixel.

This technique increase the capacity and the imperceptibility of the image after embedding. Use of GA preserve the local image properties. The OPAP is used to increase the hiding capacity of the algorithm in comparison to other systems. However by this method, the computational complexity is high. The capacity and imperceptibility of image increase simultaneously. Also, the best block size can be selected to reduce the computation cost and to increase the PSNR using optimization algorithms such as genetic algorithm.

B. Wavelet Based ECG Steganography
Ibaida et al. [2] introduced a wavelet-based steganography technique which combines encryption and scrambling technique to protect patient confidential data. This method allows ECG signal to hide its corresponding patient confidential data and other physiological information thus guaranteeing the integration between ECG and the rest.
This technique is a hybrid between two preceding categories. First, it is based on using steganography techniques to hide patient confidential information inside patient biomedical signal. Moreover, the proposed technique uses encryption based model to allow only the authorized persons to extract the hidden data. The patient ECG signal is used as the host signal that will carry the patient secret information as well as other readings from other sensors such as temperature, glucose, position, and blood pressure. The ECG signal is used here because most of the healthcare systems will collect ECG information. Moreover, the size of the ECG signal is large compared to the size of other information.
In this model body sensor nodes will be used to collect ECG signal, glucose reading, temperature, position and blood pressure, the sensors will send their readings to patient's PDA device via Bluetooth. Then, inside the patient's PDA device the steganography technique will be applied and patient secret information and physiological readings will be embedded inside the ECG host signal. Finally, the watermarked ECG signal is sent to the hospital server via the Internet. As a result, the real size of the transmitted data is the size of the ECG signal only without adding any overhead, because the other information are hidden inside the ECG signal without increasing its size. Figure 2 shows the embedding system.

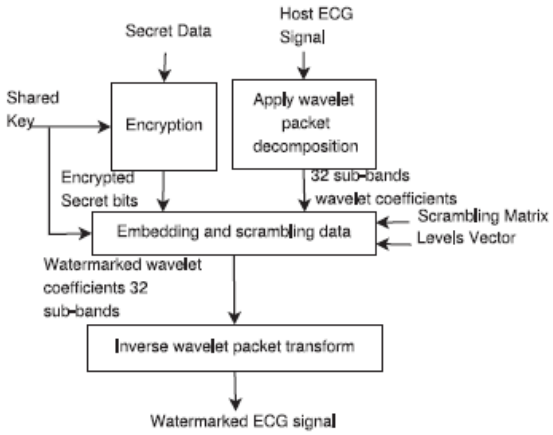

Fig. 2 Block diagram of the sender steganography system

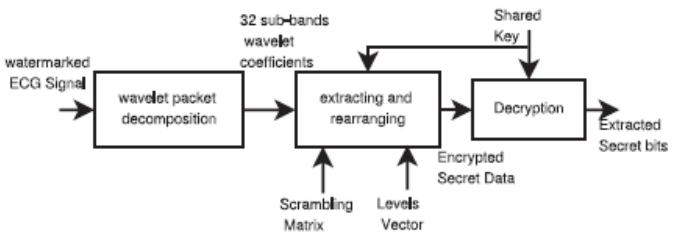

Fig. 3 Block diagram of receiver steganography system

IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
nCORETech
LBS College of Engineering, Kasaragod
Vol. 3, Special Issue 1, February 2016

At hospital server the ECG signal and its hidden information will be stored. Any doctor can see the watermarked ECG signal and only authorized doctors and certain administrative personnel can extract the secret information and have access to the confidential patient information as well as other readings stored in the host ECG signal. Figure 3 shows the extraction process.
This method guarantees minimum acceptable distortion in the ECG signal. It provides high security. This technique slightly affects the quality of ECG signal. However, watermarked ECG signal can still be used for diagnoses purposes.

C. Optimised Image Steganography using Discrete Wavelet Transform
Parul et al. [3] presented a DWT based image steganography method in which the cover image is divided into higher and lower frequency sub-bands and data is embedded into higher frequency sub-bands. Arnold Transformation is used to increase the security.

In this approach DWT is used for decomposing the image into higher and lower frequency sub bands. Secret data is transformed using Arnold transformation. The secrete image is divided into RGB components and embedded into HL sub band of RGB components of cover image respectively.

The cover image is split into its components. DWT is applied on all three components. The secrete images is transformed using Arnold transform and every color component of transformed secrete images are separated. Embed the secrete images components into HL, HH, and LH sub band. Inverse DWT is done to obtain stego image. Recovery procedure is reverse of embedding.

This approach is superior in terms of PSNR and high embedding capacity. Also, the use of Arnold transformation improves security.

D. High Capacity Image Steganography Based on Haar DWT for Hiding Miscellaneous Data
Hamad A. A. et al [4] proposed a high capacity and efficient steganography technique, where binary images, color images, and large text files can be all concealed within a single cover image at the same time using Haar Wavelet transform.

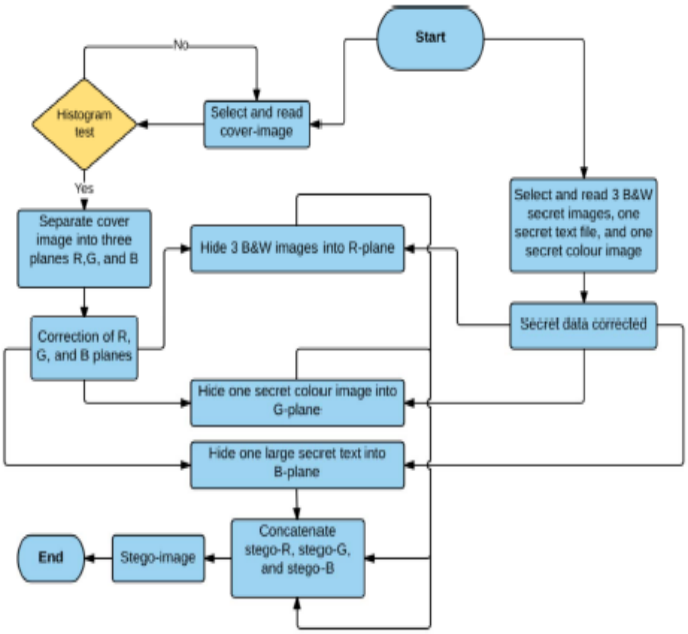


Fig. 4 Encoding process

The Haar DWT is used in this technique to convert the cover image into four sub-bands that are approximation, vertical, horizontal and diagonal coefficients, which represent low-low, high-low, low-high and high-high frequencies respectively. Secret data are corrected and concealed in coefficients other than approximation coefficients by the least significant bit and pseudo random number techniques. Pseudo random number technique is implemented in order to hide B&W secret images as well as secret text file. Once the embedding process is completed, the inverse Haar DWT is applied to form the stego image.

IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
nCORETech
LBS College of Engineering, Kasaragod
Vol. 3, Special Issue 1, February 2016

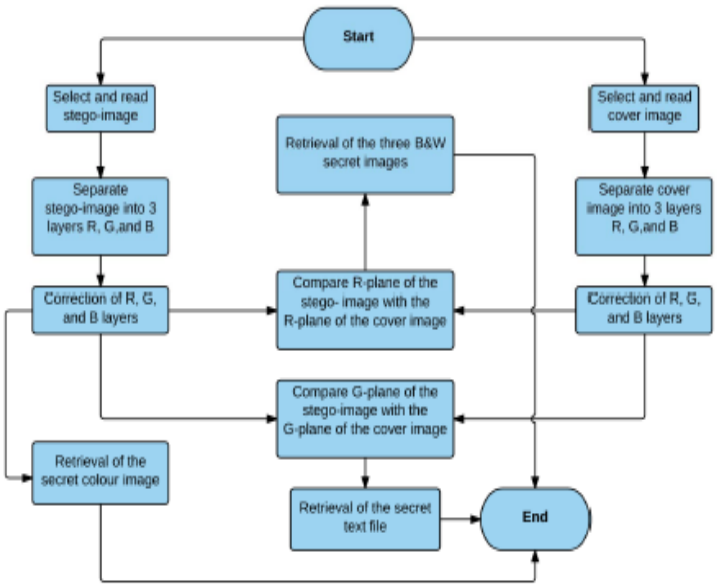


Fig. 5 Decoding process

The proposed steganography techniques provide not only high capacity Capacity values are found to be high except for that of hiding B&W images, since approximation coefficients that represent the low-low frequencies of the Wavelet transform has not been used for hiding process. However, as the capacity increases, PSNR decreases, and MSE increases.

E. Colour Image Steganography Method Based on Sparse Representation

Ahani et al. [5] proposed the use of sparse representation to securely hide a message within non-overlapping blocks of a given colour image in the wavelet domain. All four sub-images of the two-dimensional wavelet transform of two colour bands are used for data embedding without affecting the image perceptibility. Bit error rate of hidden data extraction is reduced to zero by introducing a novel refinement procedure in the proposed algorithm. The refinement procedure introduced solves the hidden bit extraction errors caused by the rounding process, the overflows and the nature of approximation in sparse decomposition.

This algorithm has been proved to outperform several other transform domain steganography methods in the sense of the average PSNR of the stego images generated at the same embedding rates. Besides, this method has been shown to be undetectable by a number of well known powerful image steganalysers.

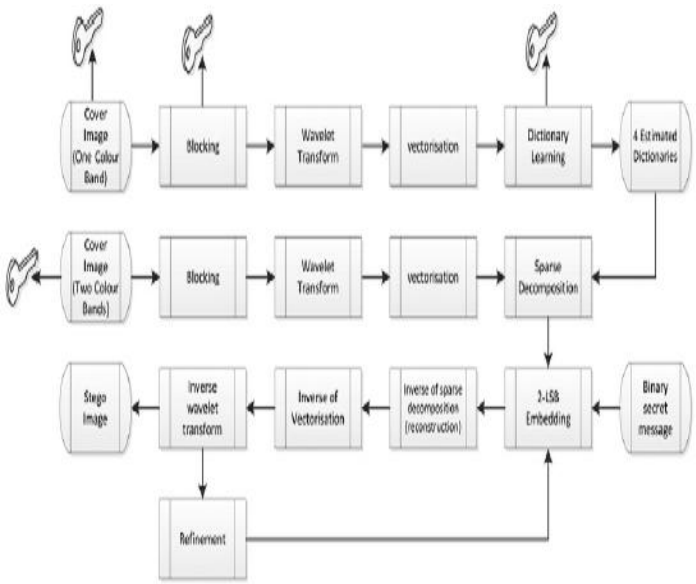


Fig. 6 Block diagram of embedding process

IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
nCORETech
LBS College of Engineering, Kasaragod
Vol. 3, Special Issue 1, February 2016

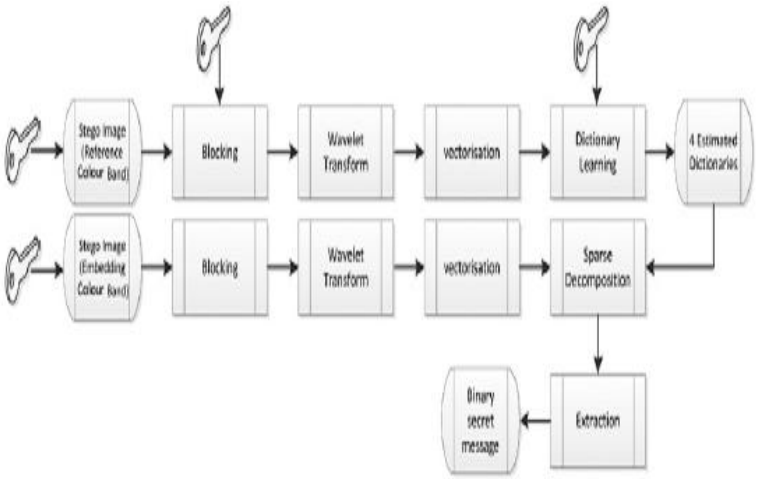


Fig. 7 Block diagram of extraction process

## IV. CONCLUSION

This paper presents a study of few steganography techniques based on DWT. DWT based steganography techniques have proved to be less prone to attacks because the coefficients in the transform domain are altered. Also such techniques cause minimum distortion in image. But these techniques have lower capacity compared to spatial domain techniques.

## REFERENCES

[1] E. Ghasemi, J. Shanbehzadeh, N. Fassihi, "High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm", Proc. IMECS, 2011.
[2] A. Ibaida, I. Khalil, "Wavelet Based ECG Steganography for Protecting Patient Confidential Information in Point-of-Care Systems", IEEE Trans. Of Biomed. Eng., vol. 60, pp. 3322-3330, Dec. 2013.
[3] Parul, Manju, Harish Rohil, "Optimised Image Steganography using Discrete Wavelet Transform", Int. Journal of Recent Development in Eng and Tech., vol. 2, pp. 75–81, Feb. 2014.
[4] Hamad A. A, Ali A, Majid A. A, Waleed A, "High Capacity Image Steganography Based on Haar DWT for Hiding Miscellaneous Data", IEEE Jordan Conf. on Applied Electrical Eng. and Comp. Tech., March 2015
[5] S.Ahani, S. Ghaemmaghami, "Colour Image Steganography Method Based on Sparse Representation", IET Image Process, vol. 9, pp. 496-505, 2015.