A TECHNIQUE TO MITIGATE THE EFFECT OF ATTACKS IN DIGITAL IMAGES

A Thesis Submitted
In Partial Fulfillment of the Requirements
For the Degree of

MASTER OF TECHNOLOGY
(Full Time)

in

COMPUTER SCIENCE & ENGINEERING
(Software Engineering)

by

AKANKSHA SINGH
(Enrollment No. 1150449001)

Under the supervision of
Assistant Professor Mohd. Saif Wajid
Department of Computer Science BBD University, Lucknow

to the

BABU BANARASI DAS UNIVERSITY
LUCKNOW

May, 2017

CERTIFICATE

It is certified that the work contained in this thesis entitled “A Technique To Mitigate The Effect Of Attacks In Digital Images.”, by Akanksha Singh (RollNo.1150449001), for the award of Master of Technology from BabuBanarasi Das University has been carried out under my/our supervision and that this work has not been submitted elsewhere for a degree.

Signature

Mohd. Saif Wajid
Assistant Professor
CSE Department BBDU

ABSTRACT

One of the biggest technological events of the last two decades was the invasion of digital media in an entire range of everyday life aspects. Digital data can be stored efficiently and with a very high quality, and it can be manipulated very easily using computers. Furthermore, digital data can be transmitted in a fast and inexpensive way through data communication networks without losing quality. Digital media offer several distinct advantages over analog media. The quality of digital audio, images and video signals are better than that of their analog counterparts. Editing is easy because one can access the exact discrete locations that need to be changed. Copying is simple with no loss of fidelity and a copy of a digital media is identical to the original. With digital multimedia distribution over World Wide Web, Intellectual Property Right (IPR) are more threatened than ever due to the possibility of unlimited copying. One solution would be to restrict access to the data using some encryption technique. However encryption does not provide overall protection. Once the encrypted data are decrypted, they can be freely distributed or manipulated. The above problem can be solved by hiding some ownership data into the multimedia data, which can be extracted later to prove the ownership. This idea is implemented in bank currency notes. In bank currency notes, a watermark is embedded which is used to check the originality of the note. The same "watermarking" concept maybe used in multimedia digital contents for checking the authenticity of the original content. So, A ***Watermarking is adding an "ownership" information in multimedia contents to prove the authenticity***. This technology embeds a data, an unperceivable digital code, namely the watermark, carrying information about the copyright status of the work to be protected. Continuous efforts are being made to device an efficient watermarking schema but techniques proposed so far do not seem to be robust to all possible attacks and multimedia data processing operations. Considering the enormous financial implications of copyright protection, there is a need to establish a globally accepted watermarking technique. The

sudden increase in watermarking interest is most likely due to the increase in concern over IPR. Today, digital data security covers such topics as access control, authentication, and copyright protection for still images, audio, video, and multimedia products. A pirate tries either to remove a watermark to violate a copyright or to cast the same watermark, after altering the data, to forge the proof of authenticity.

Generally, the watermarking of still image, video, and audio demonstrate certain common fundamental concepts. Numerous watermarking applications reported in the literature depend on the services we wish to support. Thus watermarking techniques may be relevant in various application areas including Copyright protection, Copy protection, Temper detection, Fingerprinting etc. Based on their embedding domain, watermarking schemes can be classified either as Spatial Domain (The watermarking system directly alters the main data elements, like pixels in an image, to hide the watermark data) or Transformed Domain (the watermarking system alters the frequency transforms of data elements to hide the watermark data). The latter has proved to be more robust than the spatial domain watermarking.

To transfer an image to its frequency representation, one can use several reversible transforms like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), or Discrete Fourier Transform (DFT).. Each of these transforms has its own characteristics and represents the image in different ways. Watermarks can be embedded within images by modifying these values, i.e. the transform domain coefficients. In case of spatial domain, simple watermarks could be embedded in the images by modifying the pixel values or the least significant bit (LSB) values. However, more robust watermarks could be embedded in the transform domain of images by modifying the transform domain coefficients. In 1997 Cox et.al presented a paper “Secure Spread Spectrum Watermarking for Multimedia” , one of the most cited paper (cited 2985 times till April’ 2008 as per Google Scholar search), and after that most of the research efforts are based on this work. Even though spatial domain based techniques can not sustain most of the common attacks like compression, high pass or low pass filtering etc., researchers present spatial domain based techniques too. Since, financial implications of some of the application areas like fingerprinting and copyright protection are very high and till now no successful algorithm seem to be available to prevent illegal copying of the multimedia contents, the primary goal of this thesis work is chosen to develop watermarking schemes for images (which are stored in spatial domain as well as transformed domain) which can sustain the known attacks and various image manipulation operations.

This thesis resolves the following issues:

- To study and analyze the various watermarking techniques which exist and to develop an inference from them.
- To generate a novice algorithm to implement data hiding in image data using DWT Transform technique.
- Algorithm development using various wavelet filters like daubechies, coiflets and symlets.
- Testing and performance evaluation of the technique based on various factors like Peak to Signal Noise Ratio (PSNR), Mean Square Error(MSE) etc.

Digital watermarking is the act of hiding a message related to a digital signal (i.e. an image, song, video) within the signal itself. It is a concept closely related to steganography, in that they both hide a message inside a digital signal. Watermarking has a number of uses in security, authentication and registration purposes. Image Watermarking is a widely sought after research area and many researchers have done extensive study on various aspects of digital image watermarking. Out of those techniques DWT based techniques are quite popular. In this research work a novel algorithm has been presented for Digital Image Watermarking, which uses the DWT technique to perform Watermark embedding and extraction process. The wavelet filter are of many kinds and erstwhile research have been mostly carried on ‘haar’ and ‘daubechies’ wavelet filter.

In this research work, ‘symlets’ and ‘coiflet’ filters have been used. A comparative study of results in terms of PSNR and MSE with other filters is also available to give a better reasoning and insight.In this research work, the various watermarking techniques were discussed extensively to understand the state of the art of Digital image Watermarking. A number of methods such as Least Significant Bit(LSB) Watermarking, DCT based Watermarking and DWT based Watermarking have been presented in brief in the survey of the state of the art literature. The various watermarking models have also been thoroughly studied to come to have a better understanding of the domain. Further, the Wavelet domain and wavelet based watermaking is special importance to the context of this research works thus the various terms related to wavelet, wavelet analysis, multiresolution analysis etc. has been discussed. Another important aspect of this research work is to deploy various kinds of wavelet filters for performing the watermark. Thus, a number of wavelet filters have been studied and presented in this work.

A comparative analysis of results in terms of MSE and PSNR is shown which gives the conclusion that symlet filter based algorithm is the best in terms of performance.The future research work can be centered around validating the findings of this research work by including a larger set.

Acknowledgements

I express my sincere gratitude towards my guide Prof. Mohd. SaifWajid for his constant help, encouragement and inspiration throughout the project work. Also I would like to thank our Head of Department,Dr. Reena Srivastava for her able guidance and for providing all the necessary facilities, which were indispensablein the completion of this project.

I take this opportunity to express my hearty thanks to all those who helped me in the completion of my project work. I am very grateful to the authors of various articles on the Internet, for helping me become aware of the research currently ongoing in this field.

I am very thankful to my parent for their constant support.. Last, but not the least, I would like to thank my classmates for their valuable comments, suggestions and unconditional support.

Table of Contents

List of Tables

List of Figures

List of Symbols, Abbreviations and Nomenclature

AbbreviationDescription	
AWGN	Additive White Gaussian Noise
AGN	Additive Gaussian Noise
BER	Bit Error Rate
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DIW	Digital Image Watermarking
HH	Horizontal Highs/vertical Highs
HL	Horizontal Highs/vertical Lows
IQM	Image Quality Measure
JPEG	Joint Photographic Experts Group
LH	Horizontal Lows/vertical Highs
MSE	Mean Square Error
PSNR	Peak Signal-To-Noise Ratio
RGB	Red-Green-Blue

CHAPTER 1

INTRODUCTION

Digital watermarking is the act of hiding a message related to a digital signal (i.e. an image, song,video) within the signal itself. It is a concept closely related to steganography, in that they both hide a message inside a digital signal. However, what separates them is their goal. Watermarking tries to hide a message related to the actual content of the digital signal, while in steganography the digital signal has no relation to the message, and it is merely used as a cover to hide its existence.Watermarking has been around for several centuries, in the form of watermarks found initially in plain paper and subsequently in paper bills.The increasing amount of research on watermarking over the past decade has been largely driven by its important applications in digital copyrights management and protection.One of the first applications for watermarking was broadcast monitoring. It is often crucially important that we are able to track when a specific video is being broadcast by a TV station. This is important to advertising agencies that want to ensure that their commercials are getting the air time they paid for. Watermarking can be used for this purpose. Information used to identify individual videos could be embedded in the videos themselves using watermarking, making broadcast monitoring easier.Another very important application is owner identification. Being able to identify the owner of a specific digital work of art, such as a video or image can be quite difficult. Nevertheless, it is a very important task, especially in cases related to copyright infringement. So, instead of including copyright notices with every image or song, we could use watermarking to embed the copyright in the image or the song itself.Transaction tracking is another interesting application of watermarking. In this case the watermark embedded in a digital work can be used to record one or more transactions taking place in the history of a copy of this work. For example, watermarking could be used to record the recipient of every legal copy of a movie by embedding a different watermark in each copy. If the movie is then leaked to the Internet, the movie producers could identify which recipient of the movie was the source of the leak.

1.1 Watermarking Properties:

Every watermarking system has some very important desirable properties. Some of these properties are often conflicting and we are often forced to accept some trade-offs between these properties depending on the application of the watermarking system.

The first and perhaps most important property is effectiveness. This is the probability that the message in a watermarked image will be correctly detected. We ideally need this probability to be 1. Another important property is the image fidelity. Watermarking is a process that alters an original image to add a message to it, therefore it inevitably affects the image’s quality. We want to keep this degradation of the image’s quality to a minimum, so no obvious difference in the image’s fidelity can be noticed.

The third property is the payload size. Every watermarked work is used to carry a message. The size of this message is often important as many systems require a relatively big payload to be embedded in a cover work. There are of course applications that only need a single bit to be embedded. The false positive rate is also very important to watermarking systems. This is the number of digital works that are identified to have a watermark embedded when in fact they have no watermark embedded. This should be kept very low for watermarking systems.

Lastly, robustness is crucial for most watermarking systems. There are many cases in which a watermarked work is altered during its lifetime, either by transmission over a lossy channel or several malicious attacks that try to remove the watermark or make it undetectable. A robust watermark should be able to withstand additive Gaussian noise, compression, printing and scanning, rotation, scaling, cropping and many other operations.

1.2 State of the Art:

Cover medium can be any multimedia content like digital images, audio files or video files. The main motive of steganography is to hide the existence of communication [1]. To understand the concept of steganography let us consider an example of two friends want to communicate in secret manner. Alice wants to send some secret information to his friend Bob. Alice starts by writing a letter to his friend describing his recent summer camp experiences. After he finished writing, Alice replaces the ink with the milk and writes down the secret message in between the inked lines of his letter. After sometime when milk dries, the secret message becomes invisible to human visual system. To see the hidden secret message bob try to heat the paper above the candle. This heating process reveals the hidden secret message. This is an example of steganography. Steganography, watermarking and cryptography are the three fields which are closely related to each other and belong to same family i.e. Security.

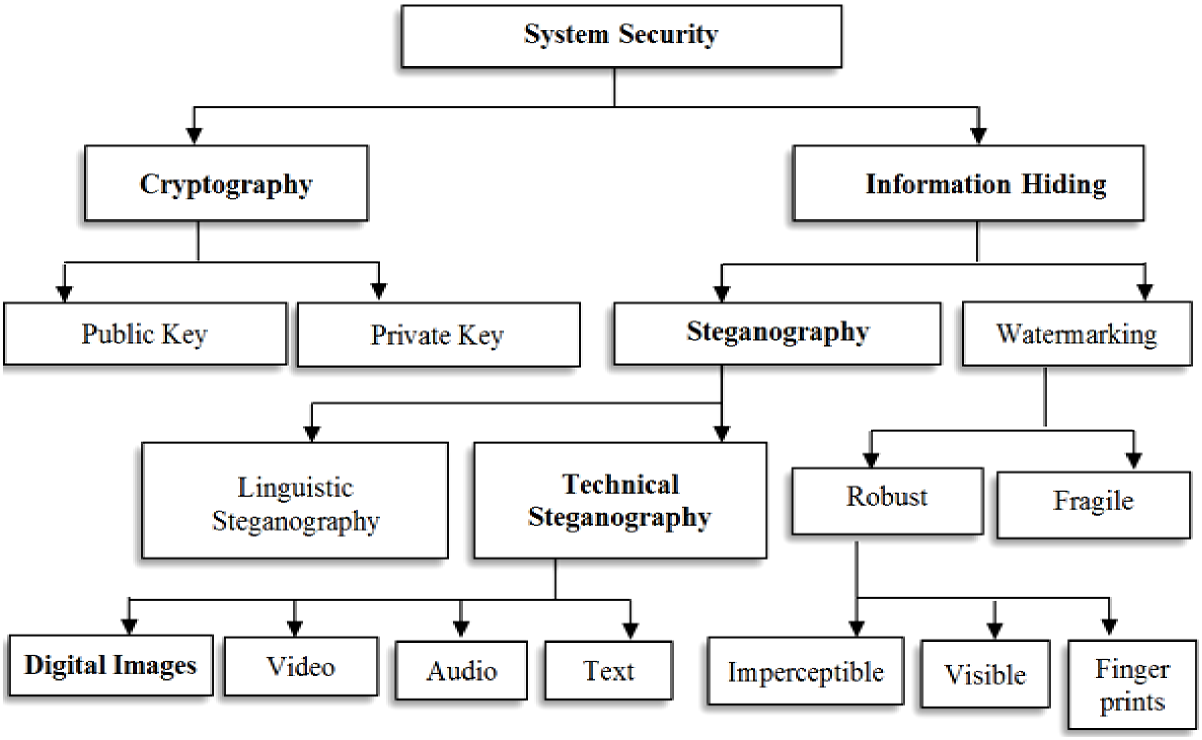


Fig 1.1: Taxonomy of Cryptography

In spatial domain steganography techniques secret information is directly embedded in pixel values i.e. pixels are directly altered to store secret messages. Basically these techniques are very simple but have greater impact then other techniques.

LSB substitution algorithm is simplest form of algorithm in which LSBs of the cover image is modified according to the secret message. It is simple yet effective technique of embedding secret data into images. Each pixel is of 8 bits in case of Gray scale images. Color RGB images use 24 bits to store color information each 8 bits for Red, Green and Blue components. The Advantages of this algorithm is simplicity and high perceptual efficiency. It can also achieve high embedding capacity but this algorithm is sensitive to image manipulations such as cropping, scaling and rotations, Lossy compression and addition of noise. There are number of variations of this algorithm including Edge and texture masking of cover image to determine the number k bits of LSBs for data embedding [3], Adaptive LSB algorithm based on brightness, optimized LSB algorithm using cat swarm and genetic algorithm [4,5], image steganography based on histogram modifications [6,7] etc. This research work mainly focuses on LSB steganography algorithm, so the rest of all the algorithms available in the literature will not be discussed in detail. Pixel Value Differencing is another technique sub divides the cover image into non overlapping blocks consisting of two connecting pixels. This technique hides the data by altering the difference between two connected pixels. High difference in the cover image pixel value allows the higher alterations. Area of the pixel decides the hiding capacity of this technique for example if edge area is chosen then the difference is high in between the connecting pixels, where as in smooth areas, difference is low. So, ideal choice is to select edge areas to embed the secret message that is having more embedding capacity. Stego image produced by this technique has more quality and has better imperceptibility results [8].

Grey Level Modification technique the data is mapped by applying some modifications to the gray values of the image pixels. This technique will not hide or embed data, instead it map the data by using some mathematical functions. Set of pixels are selected for mapping using this mathematical function. It uses the concept of odd and even numbers for mapping the data in cover image. High hiding capacity and low computational are some advantages of this technique [9].

Prediction based Steganography technique pixel values are predicted with the help of predicator. This technique removes the loopholes of other techniques which directly embed the secret data into pixel values. In order to improve hiding capacity and visual quality it uses prediction error values (EV). EVs are altered to hide the secret data. It consists of two steps, namely prediction step and entropy coding. In prediction step predicators are used to determine the pixel values of a cover image and in the second step entropy coding of prediction error values is done.

Quantization Index Modulation(QIM) is a technique of spatial domain steganography in which secret information is embedded in cover image by modulating an index with embedded information and after that quantization process is applied to the host signal with associated quantizers. This technique has number of advantages such as high embedding capacity and is highly robust technique. Transform domain steganography techniques are the most complex way to embed the secret data in the cover image. Any image in digital form is made up of high and low frequency components. Digital image can have smooth and edge (sharp) areas. Smooth areas represent low frequency whereas high frequency is represented by edge or sharp areas of the cover image. Changes done in low frequency areas can easily be visible to human eyes. So it is not possible to embed equal amount of secret information in all the regions. It has number advantages over the spatial domain methods of steganography such as it is more robust against compression, image processing and cropping and these methods are less prone to attacks. These techniques are not dependent upon image file format. Transform domain steganography techniques are broadly classified into following types:

Discrete wavelet transformation techniques divides the cover image into four sub bands where higher band represent finer details and lower band has more important information. Entropy coders locate the transform coefficients and encode them. DWT technique has extra edge over DCT that it offers efficient energy compaction than DCT without any blocking artifacts after the process of coding. DWT has multi-resolution nature that make it best fit for scalable image coding. There are several other types of transforms that can applied with DWT such as integer transform, curvelet transform, contourlet transform, dual tree DWT etc.

Discrete Cosine Transformation Technique: Discrete cosine transformation is very famous steganography techniques which is best suited for JPEG images. JPEG images are widely used over the internet and have lossy nature of compression. DCT is extensively used for image and video compression. Every block of DCT is quantized with the help of quantization table of JPEG. Quantized coefficients are used to embed the secret message. Afterward coding methods are applied such as Huffman coding. In this technique high frequency regions are better for information hiding as they often become zero after the process of quantization. Hence it is not necessary to modify the coefficient value if the embedded data is zero. JSteg/ JPHide, F5, YASS (Yet another steganographic scheme) and outguess are some of the DCT steganography tools.

In frequency domain watermarking, the cover data is considered as communication medium. The watermark is considered as a signal that is passed through this medium. In frequency domain watermarking the cover medium is converted to frequency domain before adding the watermark. After the insertion of the watermark, the medium is inversely transformed to get the watermarked medium in the spatial domain. The watermark inserted in the frequency domain ensures high level of security. The watermark is spread in such a way that the position of the watermark in not known. Moreover, watermark destruction brings severe degradation to the watermarked medium. The most popular methods in this domain are DCT and DWT. Nowadays a number of researchers have focused their research on these two methods. Cox proposed a non-blind watermarking technique. The technique is based on using spread spectrum for inserting a watermark in DCT domain [10]. A Gaussian random sequence is used as a watermark. The watermark is inserted imperceptibly in a spread spectrum-like fashion. The technique proposed was robust to majority of geometric and common signal processing attacks like compression, analog-to digital and digital-to-analog conversion etc. But the major limitation of the technique is that it requires the original image to register it against the transformed watermarked image. Harrak et al. proposed a watermarking technique in [11]. In wavelet based methods an image is decomposed into different sub-bands. A wavelet based watermarking technique is proposed. In this technique every watermark bit is embedded in various frequency bands. The technique spread the watermark information in large spatial regions of the cover medium. The technique is able to survive the frequency based attacks for example removing the high frequency areas through low-pass filter, and the removal of high-pass details in JPEG compression. The technique is also resistant against the time based attacks like rotation and pixel shifting. This technique is not imperceptible because of using a fix watermarking level for the whole image. The technique proposed by Huang is a blind technique in which the original image is not required at the time of detection [12]. In this technique, HVS is used to insert the watermark in wavelet domain. In this method four adjacent coefficients after conversion to wavelet domain are grouped. Watermark is then added to the average of these four adjacent coefficients

1.3 **Problem Statement:**

Data Hiding or Steganography represents an important paradigm in software engineering. Several kinds of steganography methods exist for images but they are not intelligent to differentiate between redundant and non-redundant information in the data.

Some of the key concerns while developing any watermarking technique are Robustness and immunity against attacks, additive Gaussian noise, compression, printing and scanning, rotation, scaling, cropping, false positive rate and Degradation of the image’s quality. This research work aims at analyzing the various wavelet filters and their ability to mitigate the above mentioned effects. Digital Image Watermarking techniques using the DWT approach has been considered for analysis purpose in this research work. Majority of research done previously in Image Watermarking using DWT has been on ‘haar’ wavelet filter only thus a comparative analysis of various kinds of other wavelet filters has been envisaged in this research work, so as to give a critical analysis in this fields and also suggest other available filter techniques for watermarking.

1.4 Objective:

The key objectives of this research work are as below:

Some of the key concerns while developing any watermarking technique are Robustness and immunity against attacks, additive Gaussian noise, compression, printing and scanning, rotation, scaling, cropping, false positive rate and Degradation of the image’s quality.

The main objective is to analyse the various watermarking techniques and to develop a robust algorithm to mitigate the effect of attacks like compression ,additive noise and cropping.

1.5 Methodologies:

- The proposed work in this thesis will be implemented in MATLAB Software using various functions available in Image Processing Toolbox and Wavelet Toolbox.
- The Discrete Wavelet Transform will be used as the transform technique to convert the images from spatial domain to frequency domain.
- The general process flow diagram as mentioned in Figure 2 will be used as building block to proceed with the implementation.

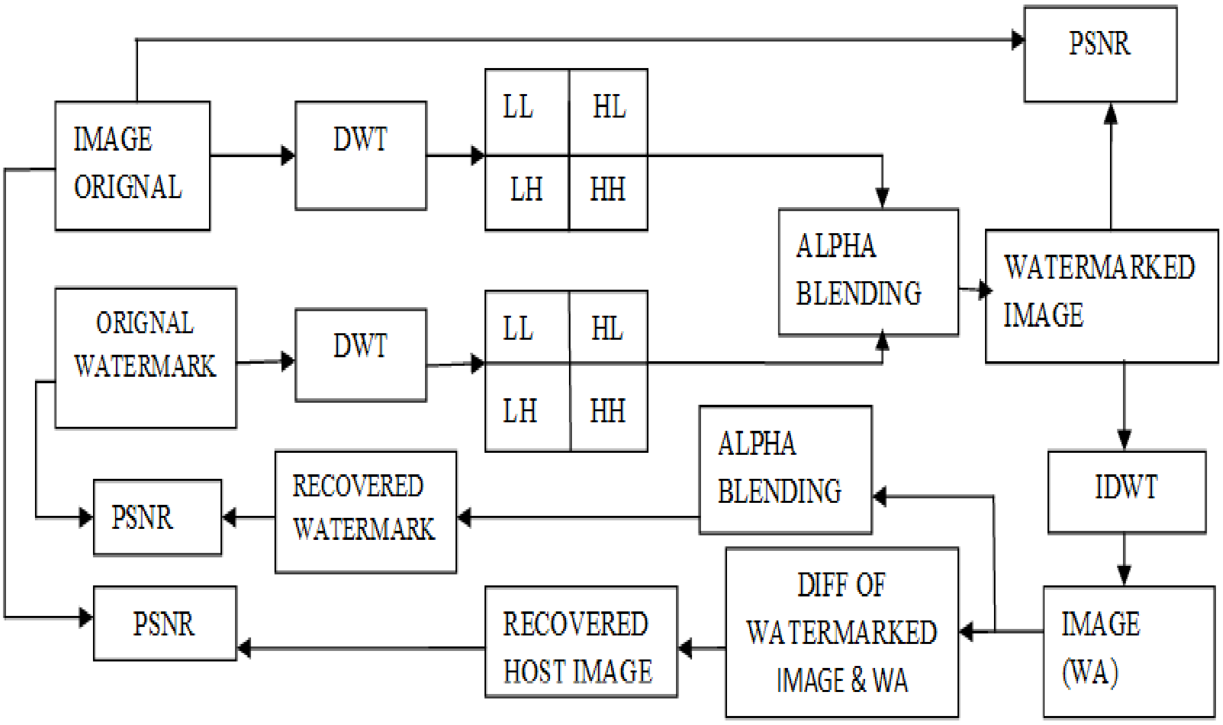


Figure 2: Process Flow Diagram

1. **Watermark Embedding:**

In this process firstly the gray scale host image is taken and 2D DWT (Discrete Wavelet Transform)is applied to the image which decomposes image into four components low frequency approximation, high frequency diagonal, low frequency horizontal ,low frequency vertical components. In the same manner DWT is also applied to the watermark image which is to be embedded in the host image. The wavelet used here is the wavelets of daubechies. The technique used here for inserting the watermark is alpha blending. In this technique the decomposed components of the host image and the watermark which are obtained by applying DWT to both the images are multiplied by a scaling factor and are added. During the embedding process the size of the watermark should be smaller than the host image but the frame size of both the images should be made equal. Since the watermark embedded in this paper is perceptible in nature or visible, it is embedded in the low frequency approximation component of the host image.

Alpha blending:

According to the formula of the alpha blending the watermarked image is given by:

WMI=k*(LL1) +q*(WM1) (1)

WMI=Watermarked image

LL1=low frequency approximation of the original image WM1=Watermark. k, q-Scaling factors for the original image and watermark respectively.

1. **Watermark Extraction:**

In this process the steps applied in the embedding process are applied in the reverse manner. The Inverse discrete wavelet transform is applied is applied to the watermarked image .Now the result obtained is subtracted from the watermarked image and in this way the host image is recovered. The watermark is recovered from the watermarked image by using the formula of the alpha blending.

Alpha Blending:RW=(WMI - k*LL1)

RW=Recovered watermark, LL1=Low frequency approximation of the original image, WMI=Watermarked image

An example of Watermarking approach is as shown in the below figure using a standard test image ‘baboon.jpg’. As shown in the figure there are two steps-one the watermark embedding and the other extraction of the watermark. As shown in the Figure the image obtained after watermarking contains the watermark image embedded and is not visible as such. Its only available when the watermarked image is passed through the Watermark Extractio Algorithm.

CHAPTER 2

LITERATURE REVIEW

The data hiding represents a useful example to the construction of a hypermedia document or image, which are very less convenient to manipulate. The aim of the steganography is to hide the message/image in the source image by some key techniques or methods and cryptography is a process to hide the message content in the image. The main objective is to hide a message inside an image keeping its visible properties and the source image as close to the original image. The most common methods to make these changes is usage of the least-significant bit (LSB) produced through masking, filtering and transformations on the source image.

According to visibility, there are two types of digital watermarking: visible and invisible. In a visible watermarking, data is visible in the image or video. Usually the information is a text message or a company logo which recognizes the owner of the media. Most television channels have logos that indicate that the information on the specific channel is protected. Nobody is allowed to use this data without permission from the channel that owns the data. The logo means a visible watermark that can be added [11]. An invisible watermarking is information added to a digital multimedia object such as a text, audio, image, or video. An object that contains an “invisible watermark” should look like the original object. One of the most important applications of an “invisible watermark” is copyright protection. It is useful as a way of recognizing the author, creator, owner, and authorized client of a document or information [12].

2.1 Understanding Images

As a matter of fact, a computer manipulates images as a group of picture elements called pixels. Each pixel represents a stream of binary numbers that express the pixel’s intensity or color [11]. According to the color, images can be categorized into two kinds of images. One is a grayscale image, in which each pixel has 8 bits (1 byte) and the second is color image, in which each pixel has 24 bits (3 bytes). The 8- bit image has 256 different gray palettes (2^8=256). This type of image will be displayed as a black-and-white picture (0 refers to black and 255 is white). A 24-bit image consists of three fundamental colors: “red, green, and blue” (RGB); each pixel is represented by three bytes. Each byte refers to the intensity of the three main colors RGB, respectively. This type of image has good quality, and the number of palettes is more than 16 million (2^{24}) different color [13].

According to extensions, images are divided into many types such as JPEG (Joint Photographic Experts), BMP (Bitmap), PNG (Portable Network Graphics), GIF (Graphics Interchange Format), TIFF (Tagged Image File Format), and etc. Most of these extensions use RGB format to show intensity of pixel color. The web page programming such as Hypertext Markup Language (HTML) uses RGB, where each two hexadecimal digits represent one primary color. This means each pixel has six hexadecimal digits. For example, the color yellow can be created by a full amount of red color (decimal 255, hex FF); the full amount of green, the pixel's value will be "#FFFF00" in the hexadecimal system number [13]. Images are of different sizes, which depend totally on the number of pixels and also on the number of bits in each pixel. The size of an 8-bit gray image consists of resolution 320 by 240 pixels which is equal to 75 Kilobytes (320*240 bytes), while the size of an image with a full color (24-bit RGB) is going to be 225 Kilobytes [14]. It is necessary to reduce image file sizes when transmitting via the internet. For this purpose many compression methods were developed over recent years. The two most popular types of compression are lossy and lossless compression, which are widely used in image processing. Compression processes are especially useful in BMP, GIF, and JPEG file image types [6, 14]. Lossy compression scheme uses by JPEG images this technique try to expand the file near to the size of original file [12]. On the other hand, lossless compression is a scheme that uses to rebuild the original image by applying some software. GIF and 8-bit BMP are two types of images which use for this scheme [14].

2.2 Watermarking

Watermarking is a concept closely related to steganography, in that they both hide a message inside a digital signal. However, what separates them is their goal. Watermarking tries to hide a message related to the actual content of the digital signal, while in steganography the digital signal has no relation to the message, and it is merely used as a cover to hide its existence. Watermarking has been around for several centuries, in the form of watermarks found initially in plain paper and subsequently in paper bills. However, the field of digital watermarking was only developed during the last 15 years and it is now being used for many different applications. There are several ways in which we can model a watermarking process. These can be broadly classified in one of two groups. The first group contains models which are based on a communication-based view of watermarking and the second group contains models based on a geometric view of watermarking.

2.2.1 Communication-based models:

Communication based models describe watermarking in a way very similar to the traditional models of communication systems. Watermarking is in fact a process of communicating a message from the watermarking embedder to the watermarking receiver. Therefore, it makes sense to use the models of secure communication to model this process. In a general secure communication model we would have the sender on one side, which would encode a message using some kind of encoding key to prevent eavesdroppers to decode the message if the message was intercepted during transmission. Then the message would be transmitted on a communications channel, which would add some noise to the noise to the encoded message. The resulting noisy message would be received at the other end of the transmission by the receiver, which would try to decode it using a decoding key, to get the original message back. This process can be seen in the below figure 2.1.

In general, communication-based watermarking models can be further divided into two sub-categories. The first uses side-information to enhance the process of watermarking and the second does not use side-information at all. The term side-information refers to any auxiliary information except the input message itself, that can be used to better encode or decode it. The best example of this is the image used to carry the message, which can be used to provide useful information to enhance the correct detection of the message at the receiver.

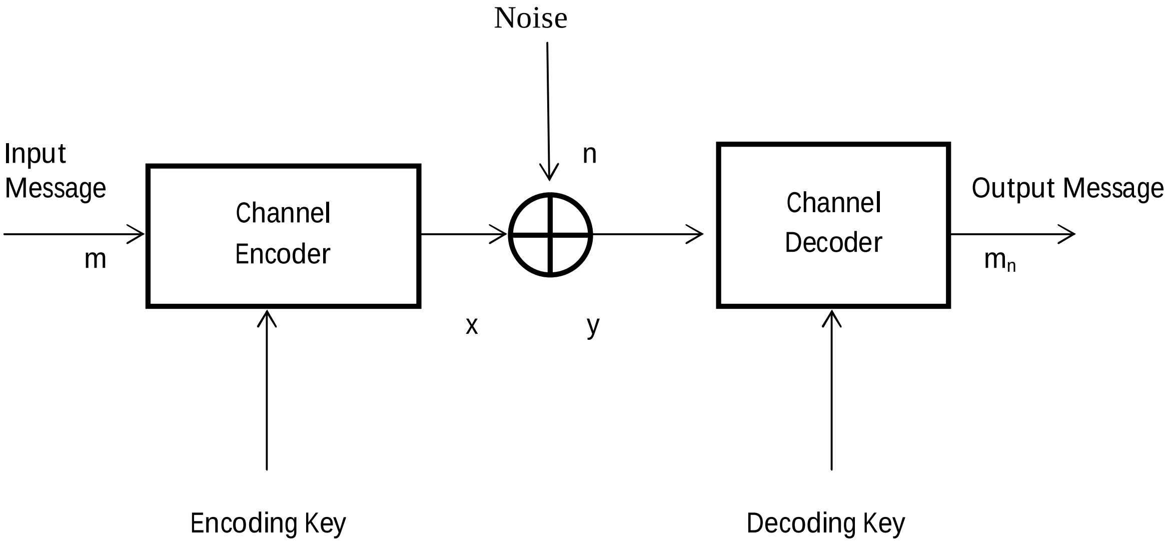


Fig 2.1: Communication model

It is often useful to think of watermarking in geometric terms. In this type of model, images, watermarked and un-watermarked, can be viewed as high-dimensional vectors, in what is called the media space. This is also a high-dimensional space that contains all possible images of all dimensions. For example a 512 X 512 image would be described as a 262144 elements vector in a 262144-dimensional space.

2.1.2 Geometric based Models:

Geometric models can be very useful to better visualize the watermarking process using a number of regions based on the desirable properties of watermarking. One of these regions is the embedding region, which is the region that contains all the possible images resulting from the embedding of a message inside an un-watermarked image using some watermark embedding algorithm. Another very important region is the detection region, which is the region containing all the possible images from which a watermark can be successfully extracted using a watermark detection algorithm. Lastly, the region of acceptable fidelity contains all the possible images resulting from the embedding of a message into an un-watermarked image, which essentially look identical to the original image. The embedding region for a given watermarking system should ideally lie inside the intersection of the detection region and the region of acceptable fidelity, in order to produce successfully detected watermarks that do not alter the image quality very much.

An example of a geometric model can be seen in Figure 2.2. Here we can see that if mean square error (MSE) is used as a measure of fidelity, the region of acceptable fidelity would be an n-dimensional sphere centered on the original un-watermarked image, with a radius defined by the largest MSE we are willing to accept for images with acceptable fidelity. The detection region for a detection algorithm based on linear correlation would be defined as a half space, based on the threshold used to decide whether an image has a watermark embedded or not. Note that the diagram is merely a projection of an n-dimensional space into a 2d space.

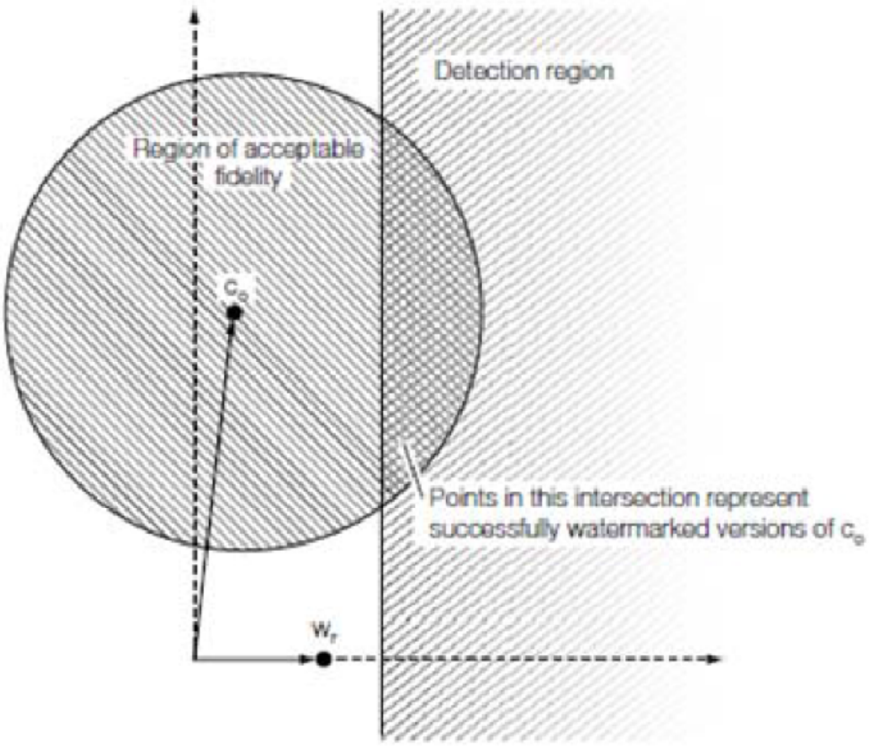

Detection region
Region of acceptable fidelity
c_o
Points in this intersection represent successfully watermarked versions of c_o
w_r

Fig 2.2: The region of acceptable fidelity

When thinking about complex watermarking systems, it is sometimes more useful to consider a projection of the media space into a possibly lower-dimension marking space in which the watermarking then takes place as usual. This projection can be handled more easily by computers because of the smaller number of vector elements and can be possibly expressed by block-based watermarking algorithms which separate images into blocks instead of operating on a pixel basis.As described earlier, some communication-based watermarking models do not take advantage of the channel side-information. In this kind of models, the image is simply considered as another form of channel noise that distorts the message during its transmission. This can be seen in Figure 2.3. The watermark embedder encodes a message using a watermark encoder and a key. This is then added to the original image and transmitted over the communication channel which adds some noise. The watermark detector at the other end receives the noisy watermarked image and tries to decode the original image using a key.

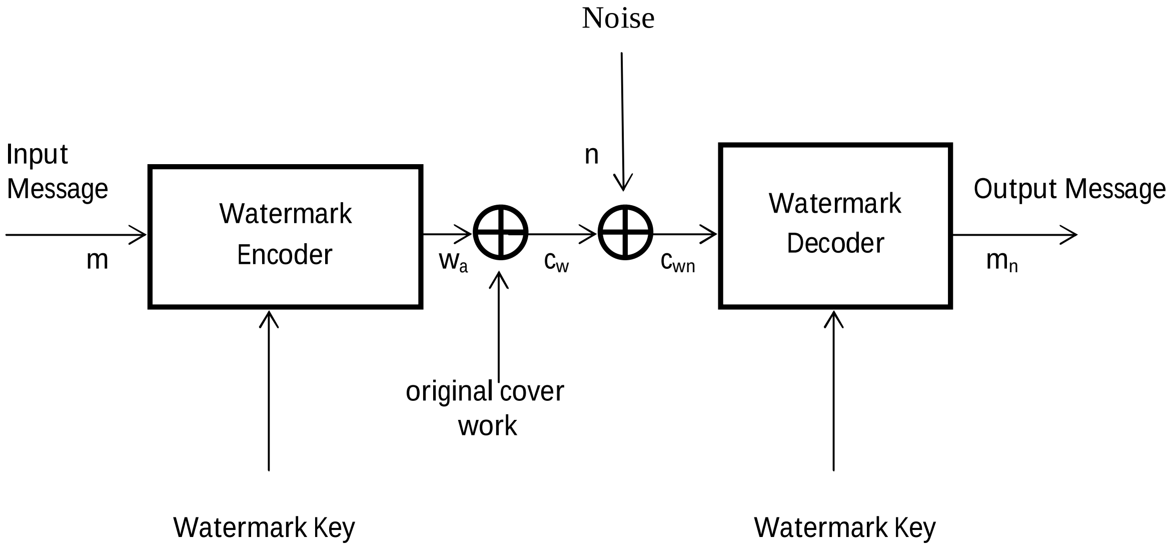


Fig 2.3 : Watermarking Steps

2.3 Blind embedding and linear correlation detection

This system is an example of blind embedding, which does not exploit the original image statistics to embed a message in an image. The detection is done using linear correlation. This system is a 1-bit watermarking system, in other words it only embeds one bit (a 1 or 0) inside the cover image. The algorithm for the embedder and the detector is as follows:

2.3.1 Embedder:

1. Choose a random reference pattern. This is simply an array with the same dimensions as the original image, whose elements are drawn from a random Gaussian distribution in the interval [-1, 1]. The watermarking key is the seed that is used to initiate the pseudo-random number generator that creates the random reference pattern.
2. Calculate a message pattern depending on whether we are embedding a 1 or a 0. For a 1, leave the random reference pattern as it is. For a 0, take its negative to get the message pattern.
3. Scale the message pattern by a constant α which is used to control the embedding strength. For higher values of α we have more robust embedding, at the expense of losing image quality. The value used at the initial experiment was α = 1.
4. Add the scaled message pattern to the original image to get the watermarked image.

2.3.2 Detector:

1. Calculate the linear correlation between the watermarked image that was received and the initial reference pattern that can be recreated using the initial seed which acted as the watermarking key.
2. Decide what the watermark message was, according to the result of the correlation. If the linear correlation value was above a threshold, we say that the message was a 1. If the linear correlation was below the negative of the threshold we say that the message was a 0. If the linear correlation was between the negative and the positive threshold we say that no message was embedded.

An example of the embedding process can be seen in Figure 2.4. The top left image is the original image, the bottom left image is the reference pattern and the watermarked image resulting from embedding a 1, with α=1, is seen on the right. As we can see, there is no perceptual difference between the original and the watermarked image.

2.3.3 Watermark Extraction:

The Watermark Extraction process is almost the opposite of the detection process. The Watermarked image is passed through the key algorithm and the embedded watermark is retrieved from it.

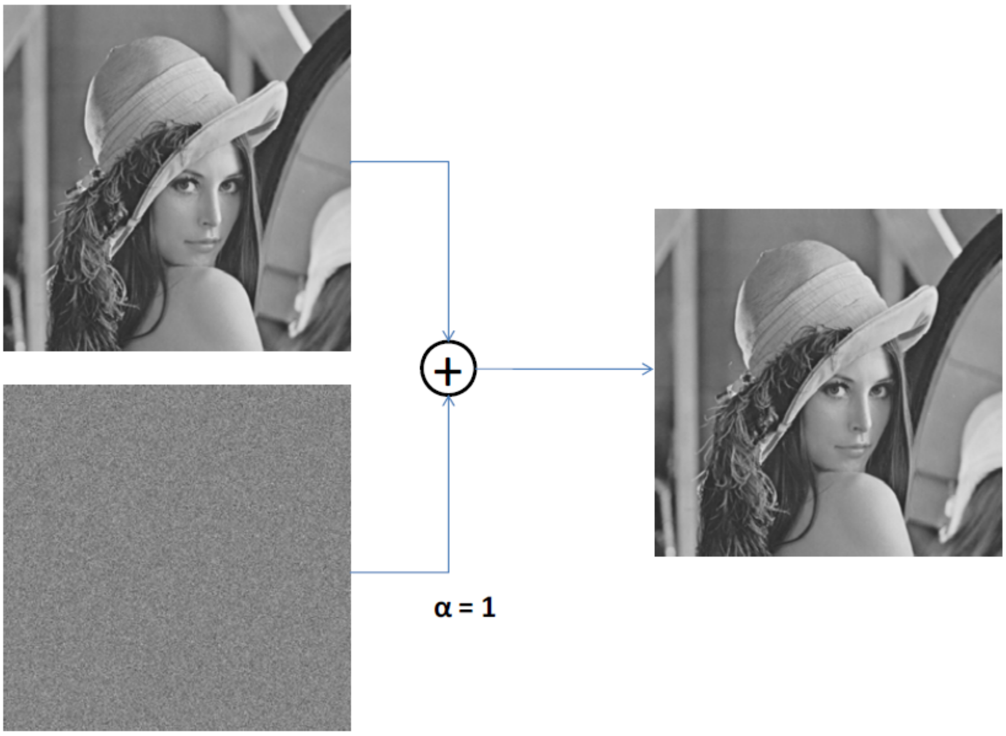


Fig 2.4: Watermark Embedding

2.4 Spatial Domain Watermarking

There are many algorithms using original data, such as video, image, audio, and text, to hide specific information like logos or personal signatures in a spatial domain. In other words, if the original data is an image, processing would be into the pixel values without changing the data into another domain. The widest and simplest method in spatial domain is Least Significant Bit (LSB), which is replacing the first bit in each pixel by information that intends to hide [15].

2.4.1 Least Significant Bit Watermarking

LSB is the one of the oldest and simplest algorithms that allows users to hide their information using spatial domain . The human eye cannot recognize the difference that occurs in the two first bits in each pixel. In other words, the change in the least significant bit does not affect the image’s quality. 24-bit images have three LSB because each RGB channel has its own LSB [13]. This provides users with more storage capacity to embed the information that is necessary to hide. For example, two pixels of an RGB image color will provide six bits for watermarking. To encode a message (100111) in RGB image needs two LSB pixels [15].

RGB Pixel 1 (R: 00010101 G: 11001100 B: 11101100)

RGB Pixel2 (R: 11011111 G: 00010001 B: 11001001)

To hide the same message (100111) in a gray-scale image six LSB pixels are needed.

Pixel1: 10010101 Pixel2: 00001100 Pixel3: 11001000

Pixel4: 10011111 Pixel5: 00010001 Pixel6: 11001011

2.4.2 Frequency Domain Watermarking

This is also called transform domain, because the original data changes from spatial to frequency domain. The most common frequency methods are Discrete Fourier Transformation (DFT), Discrete Wavelet Transformation (DWT), and Discrete Cosine Transformation (DCT). For example, an 8-bit image with a 256 by 256 resolution can be transformed into frequency watermarking using DWT. The result of this processing would be four small images, each of them with a 128 by 128 resolution. Moreover, four images will have different frequency ranges from low to high because each of them has different coefficients for others. The main advantage of using frequency domain watermarking is that it is robust for many kinds of signal manipulations when sending data via the Internet. Also, it resists of many noises that attack embedded information [2].

2.4.3 Discrete Cosine Transform

The DCT is a very popular transform function used in signal processing. It transforms a signal from spatial domain to frequency domain. Due to good performance, it has been used in JPEG standard for image compression. DCT has been applied in many fields such as data compression, pattern recognition, image processing, and so on.

The DCT transform and its inverse manner can be expressed as follows[30]:

$$X_C(k_1, k_2) \underline{\underline{\Delta}} \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} 4x(n_1, n_2) \cos \frac{\pi k_1}{2N_1}(2n_1+1) \cos \frac{\pi k_2}{2N_2}(2n_2+1),$$

For,

$$(k_1, k_2) \in [0, N_1-1]x[0, N_2-1], Otherwise, X_C(k_1, k_2) \underline{\underline{\Delta}} 0.$$

As an image transformed by the DCT, it is usually divided into non-overlapped m x m block. In general, a block always consists of 8x8 components. The block coefficients are shown in figure 2.5. The left-top coefficient is the DC value while the others stand for AC components. The zigzag scanning permutation is implied the energy distribution from high to low as well as from low frequency to high frequency with the same manner.

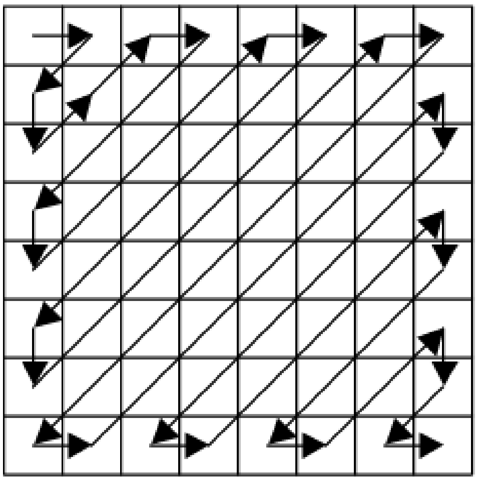
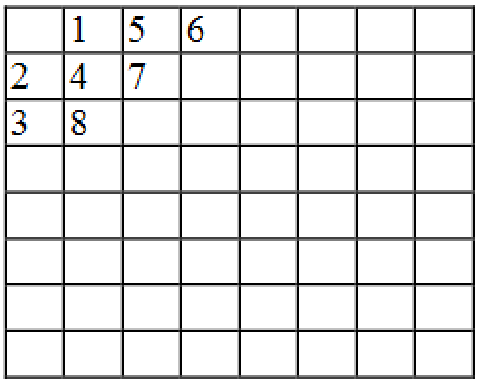


Fig 2.5: DCT block Coefficient and Zigzag

The human eyes are more sensitive to noise in lower-frequency band than higher frequency. The energy of natural image is concentrated in the lower frequency range. The watermark hidden in the higher frequency band might be discarded after a lossy compression. Therefore, the watermark is always embedded in the lower-band range of the host image that transformed by DCT is perfect selection. The lower-band coefficients of DCT block are described as in Figure 2.6.



	1	5	6				
2	4	7					
3	8						

Fig 2.6: 8 lower band coefficients

2.4.4 Discrete Wavelet Transform

It is a tool to transform the signal or data from one domain which is a spatial to another domain which is afrequency. In the frequency domain the signal splits into the two half one of them is high frequency and another is low frequency. Then each of them is going to divide again into high and low frequency that four different parts of signal [16]. Four parts or sub bands of decomposed signal are LL, LH, HL and HH frequencies which are low-low, low-high, high-low and high-high frequencies [10]. Low frequency is the same of original signal and other parts are more details of signal they are not exact data as original one, so we can change or remove depends on the technique that we using. The reconstruction process is the opposite of decomposition process that means the four bands of divided data have to be mixed again to recover the original data. Sometimes we do more than one level of decomposition depends on the algorithm that we use. Low-low frequency band will be used in case we do second decomposition. In case of reconstruction the last level of decomposition will used first which is an exact opposite direction [14]. DWT is the multiresolution description of an image the decoding can be processed sequentially from a low resolution to the higher resolution. In this the low frequency signals are located in the frequency domain while high frequency signals are located in the pixel domain. Wavelets have their energy concentrated in time and are well suited for the analysis of the transient, time varying signals. The 2D wavelet transform decomposes an image into lower resolution approximation image(LL) as well as horizontal(HL),vertical(LH) and diagonal(HH) detail components. The perceptible watermark should be embedded in the low frequency region while the imperceptible watermark should be embedded in the high frequency region. Figure 2.7 shows the architecture of the watermarking model based on digital watermarking. In this the Discrete wavelet transform is applied to the original image and the watermark separately. After this the watermark is embedded in the image using the alpha blending technique. For the recovery of the watermark and the original image the IDWT(Inverse Discrete Wavelet Transform) is applied to the watermarked image and the both images are recovered.

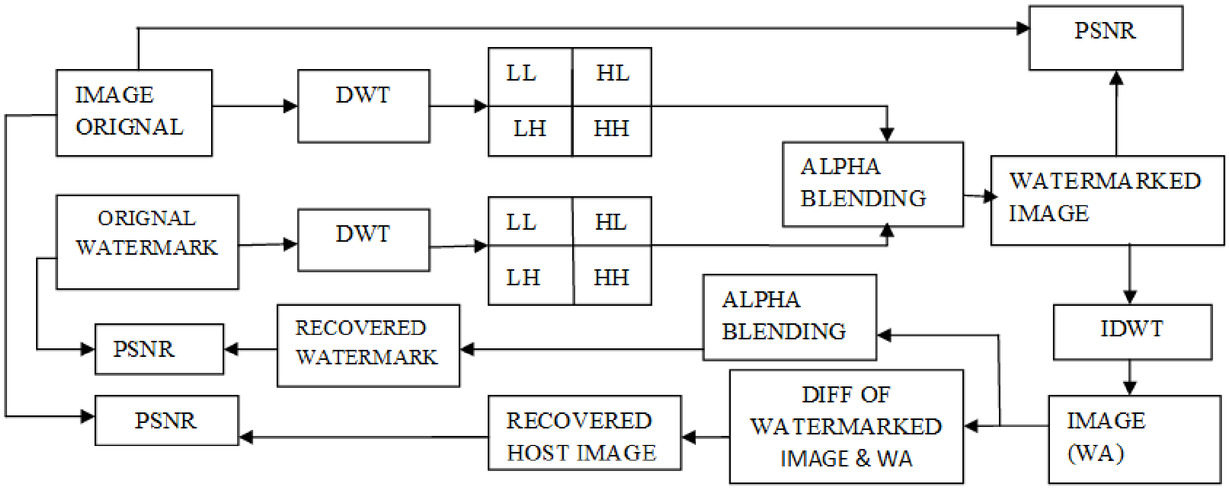


Fig 2.7: Architecture of DWT base Watermarking Technique[20]

Watermark Embedding: In this process firstly the gray scale host image is taken and 2D DWT (Discrete Wavelet Transform) is applied to the image which decomposes image into four components low frequency approximation, high frequency diagonal, low frequency horizontal ,low frequency vertical components. In the same manner DWT is also applied to the watermark image which is to be embedded in the host image. The wavelet used here is the wavelets of daubechies. The technique used here for inserting the watermark is alpha blending [20]. In this technique the decomposed components of the host image and the watermark which are obtained by applying DWT to both the images are multiplied by a scaling factor and are added. During the embedding process the size of the watermark should be smaller than the host image but the frame size of both the images should be made equal. Since the watermark embedded in this paper is perceptible in nature or visible, it is embedded in the low frequency approximation component of the host image.

Alpha blending:

According to the formula of the alpha blending the watermarked image is given by:

WMI=k*(LL1) +q*(WM1) 2.2

WMI=Watermarked image

LL1=low frequency approximation of the original image WM1=Watermark. k, q-Scaling factors for the original image and watermark respectively.

Watermark Extraction: In this process the steps applied in the embedding process are applied in the reverse manner. The Inverse discrete wavelet transform is applied is applied to the watermarked image .Now the result obtained is subtracted from the watermarked image and in this way the host image is recovered. The watermark is recovered from the watermarked image by using the formula of the alpha blending.

Alpha blending

RW=(WMI - k*LL1) 2.3

RW=Recovered watermark, LL1=Low frequency approximation of the original image, WMI=Watermarked image

2.5 Characteristics feature of Data Hiding Techniques

- **Robustness** to attacks can embedded data exist manipulation of the stego medium in an effort to destroy, or change the embedded data.
- **Perceptibility** does embedding message distort cover medium to a visually unacceptable level.
- **Tamper Resistance** Beyond robustness to destruction, tamper-resistance refers to the difficulty for an attacker to alter a message once it has been embedded in a stego image.[13]
- **Capacity** how much information can be hidden with relative to the change in perceptibility.

CHAPTER 3

WAVELET ANALYSIS

The analysis of a non-stationary signal using the Fourier Transform or the Short Time Fourier Transform, does not give satisfactory results. Better results can be obtained using wavelet analysis. One advantage of wavelet analysis is the ability to perform local analysis. Wavelet analysis is able to reveal signal aspects that other analysis techniques miss, such as trends, breakdown points, discontinuities, etc. In comparison to the STFT, wavelet analysis makes it possible to perform a multiresolution analysis.

3.1 Multiresolution Analysis:

The time-frequency resolution problem is caused by the Heisenberg uncertainty principle and exists regardless of the used analysis technique. For the STFT, a fixed time-frequency resolution is used. By using an approach called multiresolution analysis (MRA) it is possible to analyze a signal at different frequencies with different resolutions. The change in resolution is schematically displayed in Fig. 3.1.

For the resolution of Fig. 3.1 it is assumed that low frequencies last for the entire duration of the signal, whereas high frequencies appear from time to time as short burst. This is often the case in practical applications. The wavelet analysis calculates the correlation between the signal under consideration and a wavelet function f(t). The similarity between the signal and the analyzing wavelet function is computed separately for different time intervals, resulting in a two dimensional representation. The analyzing wavelet function f(t) is also referred to as the mother wavelet.

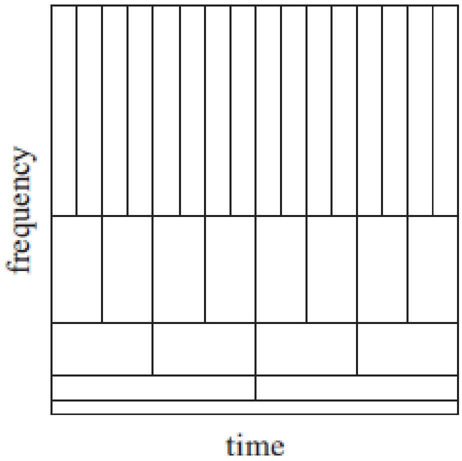


Fig 3.1: Multiresolution time-frequency plane

A wavelet function f(t) is a small wave, which must be oscillatory in some way to discriminate between different frequencies.The wavelet contains both the analyzing shape and the window. Fig. 3.2 shows an example of a possible wavelet, known as the Morlet wavelet. For the CWT several kind of wavelet functions are developed which all have specific properties.

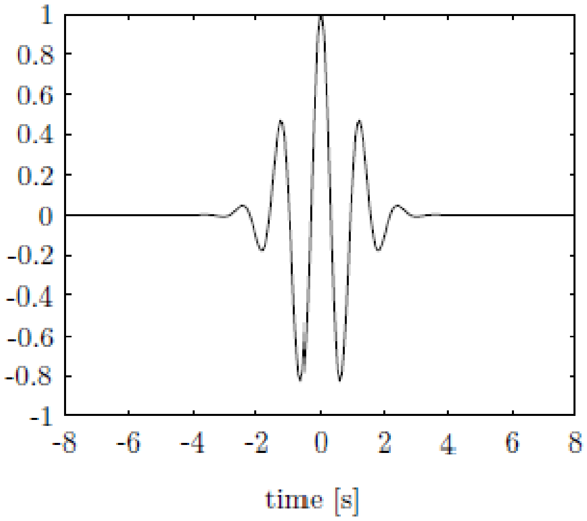


Fig 3.2: A Sample Wavelet

3.2 Discrete Wavelet Transform

The discrete wavelet transform (DWT) uses filter banks for the construction of the multiresolution time-frequency plane. The DWT uses multiresolution filter banks and special wavelet filters for the analysis and reconstruction of signals.

A filter bank consists of filters which separate a signal into frequency bands. An example of a two channel filter bank is shown in Fig. 3.3. A discrete time signal x(k) enters the analysis bank and is filtered by the filters L(z) and H(z) which separate the frequency content of the input signal in frequency bands of equal width. The filters L(z) and H(z) are therefore respectively a low-pass and a high-pass filter. The output of the filters each contains half the frequency content, but an equal amount of samples as the input signal. The two outputs together contain the same frequency content as the input signal, however the amount of data is doubled. Therefore downsampling by a factor two, denoted by ↓ 2, is applied to the outputs of the filters in the analysis bank. Reconstruction of the original signal is possible using the synthesis filter bank.

In the synthesis bank the signals are upsampled (↑ 2) and passed through the filters $L^{'}$(z) and $H^{'}$(z). The filters in the synthesis bank are based on the filters in the analysis bank. The outputs of the filters in the synthesis bank are summed, leading to the reconstructed signal y(k). The different output signals of the analysis filter bank are called subbands, the filter-bank technique is also called subband coding.

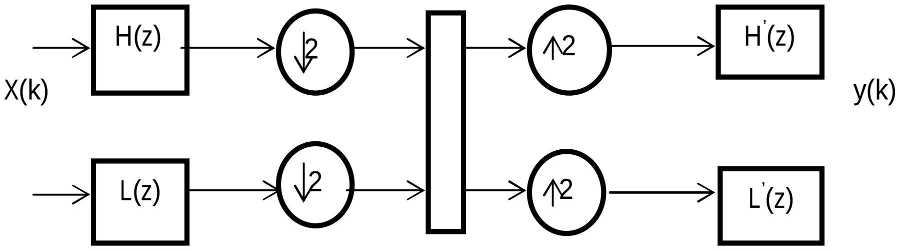


Fig 3.3: A two channel Filter Bank

3.2.1 Down and Up Sampling

The low- and high-pass filters L(z) and H(z) split the frequency content of the signal in half. It therefore seems logical to perform a down-sampling with a factor two to avoid redundancy. If halfof the samples of the filtered signals cl(k) and ch(k) are reduced, it is still possible to reconstruct the signal x(k) [22]. The down-sampling operation (↓2) saves only the even-numbered components of the filter output, hence it is not invertible. In the frequency domain, the effect of discarding information is called aliasing. If the Shannon sampling theorem is met, no loss of information occurs [21]. The sampling theorem of Shannon states that down sampling a sampled signal by a factor M produces a signal whose spectrum can be calculated by partitioning the original spectrum into M equal bands and summing these bands [23]. In the synthesis bank the signals are first upsampled before filtering. The up sampling by a factor two (↑2) is performed by adding zeros in between the samples of the original signal. Note that first down sampling a signal and then upsampling it again will not return the original signal.

3.3 Wavelet functions

For the DWT special families of wavelet functions are developed. These wavelets are compactly supported, orthogonal or biorthogonal and are characterized by low-pass and high-pass analysis and synthesis filters. Some generally used families for the DWT are discussed in this section.

3.3.1 Daubechies:

The Daubechies familiy is named after Ingrid Daubechies who invented the compactly supported orthonormal wavelet, making wavelet analysis in discrete time possible. The first order Daubechies wavelet is also known as the Haar wavelet, which wavelet function resembles a step function.

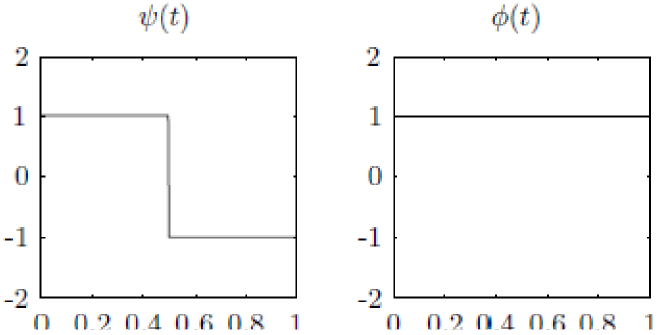


Fig 3.4: Haar Wavelet(db1)

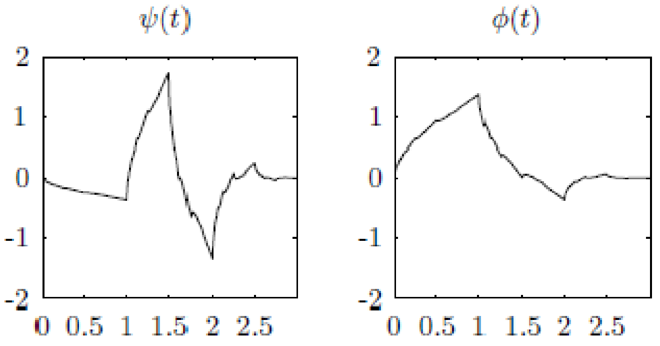


Fig 3.5: db2 wavelet and scaling function

3.3.2 Coiflets

Coiflets are also build by I. Daubechies on the request of R. Coifman. Coifman wavelets are orthogonal compactly supported wavelets with the highest number of vanishing moments for both the wavelet and scaling function for a given support width. The Coiflet wavelets are more symmetric and have more vanishing moments than the Daubechies wavelets.

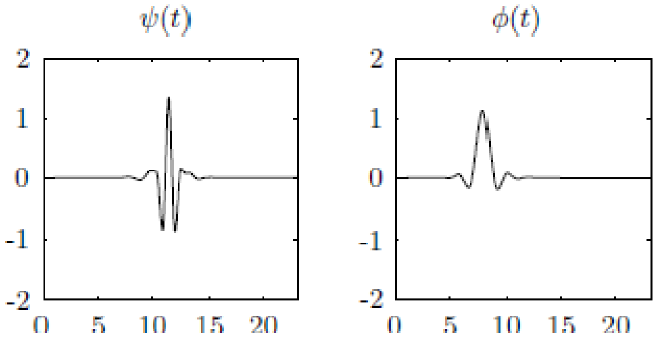


Fig 3.6: Coiflet wavelet and scaling function

3.3.3 Symlets

Symlets are also orthogonal and compactly supported wavelets, which are proposed by I. Daubechiesas modifications to the db family. Symlets are near symmetric and have the least asymmetry. The associated scaling filters are near linear-phase filters. The properties of symlets are nearly the same as those of the db wavelets.

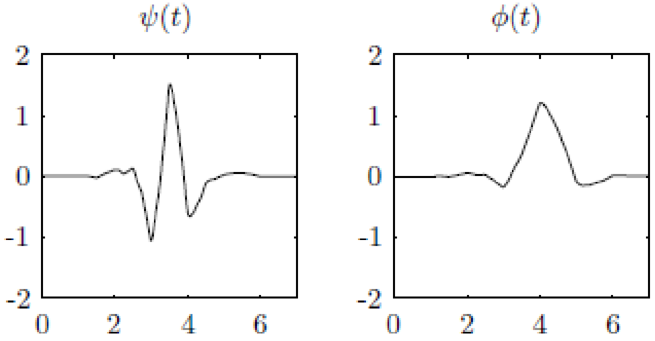


Fig 3.7: Symlet Wavelet and scaling function

Table 3.1: Comparison of Wavelet Filters for use in Image

Wavelet Family	Type	Characteristic	Window Type	Coefficient	Implementation Cost
HAAR	**Orthonormal**	Conceptually simple, memory efficient, exactly reversible	**Non Overlapping**	Two scaling and wavelet function coefficients	**Cheap**
Daubechies	**Orthogonal**	Smoother and compact	**Overlapping**	Four wavelet and scaling coefficients	**Costly than Haar**
Coiflets	**Orthogonal**	Higher computational overhead, smoother wavelet and increased capabilities in several image-processing techniques	**Highly overlapped**	Six scaling and wavelet function coefficients	**More Costly**
Symlets	**Symmetrical wavelets**	Modified Duabechies	**Overlapped**	Two scaling and wavelet function coefficients	**Cost Effective**

The above table 3.1 shows the comparison of various types of wavelet filters.

CHAPTER 4

PROPOSED WORK

Wavelet Transform is one of the widely used techniques nowadays by the researchers working in the image processing domain. The discrete wavelet transform has been used in a number of research works of late related to image compression, image de-noising, image watermarking, image fusion etc. In this research work, the usage of Discrete Wavelet Transform for the purpose of Image Watermarking has been envisaged. The algorithm used here uses discrete Wavelet Transform technique to convert the original image i.e. the input image from spatial domain to transform domain. As has been observed during the literature survey of a number of scholary articles, mainly ‘haar’ wavelet has been used in the research work. The other types of wavelets like duabechies, coiflets and symlets find little or no significance in the works earlier. Thus an important aspect of this research work is to use the other wavelet filters namely coiflet and symlet in implementing the Watermarking.

The following points the key aspects of the proposed work:

- Wavelet Transform or Discrete Wavelet Transform is one of the widely used techniques for image processing applications and is used in this project.
- Watermarking algorithm using DWT technique will be implemented using various kinds of wavelet filters such as haar, coiflet and symlet.
- The performance of the developed methodology with different kinds of filters will be compared on the basis of several performance characteristics viz. PSNR and MSE.

4.1: Algorithm Used

Input Cover Image

Preprocess for type and size

Apply 2D-DWT using different filters viz. db1, sym1.

Select subband for Watermarking.

Find out weight factor S(i,j) for HH subband.

Generate Watermark Key Image

PERFORM EMBEDDING

$$Y = cv + c*abs(cv)*N \tag{4.1}$$

where cv is the DWT coefficient in which the embedding is done, c is the watermark weight, N is the size of hidden image

Perform Inverse DWT.

The watermarked image is obtained

PERFORM EXTRACTION

Read in the watermarked image.

Perform DWT.

Obtain Coefficients of Hidden message, using below equation:

$$cc=abs(cv1/N) \tag{4.2}$$

where cc is hidden message, cv1 is the coefficients of DWT and N is watermark size

4.2 Performance Parameters

The degree of distortion of image can be measured by using mean square error (MSE) and peak signal-to-noise ratio (PSNR). Both MSE and PSNR are used because they represent the grey value error of the whole image. All the pixels of an image are equally important. With the use of PSNR or MSE, gray-value difference between corresponding pixels of the original image and the pixels of distorted image are considered. All the pixels of an image are independent of their neighbor pixels. Therefore, pixels at different position have different effect on human visual system. Mean Square Error could be estimated in one of numerous approaches to quantify the contrast between values implied by an evaluation and correct quality being certified

The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error.

Lower the value of MSE lowers the error.

$$\mathrm{MSE}=\frac{1}{MN}\sum_{i=1,j=1}^{M,N} I(\mathrm{i,j})^2 - \mathrm{C}(\mathrm{i,j})^2 \qquad (4.3)$$

Where M,N represent the width and height pixel values I is original image and C is compressed image.

PSNR is expressed in terms of the logarithmic decibel scale because many signals have a very wide dynamic range. ThePSNR is used as a measure of quality of reconstruction after a number of image processing applications. In such case the signal is the original data, and the noise is the error.

In some cases, reconstruction may appear to be closer to the original than another, even though it has a lower PSNR (a higher PSNR would normally indicate that the reconstruction is of higher quality).

The PSNR values are calculated using the following equation:

PSNR=10log10 ((2*n-1)2)/MSE (4.4)

where n represents the no. of bits per pixel.

4.3 Tools Used

The algorithm described in the above chapter has been implemented in MATLAB software version MATLAB7.10, R2010a. The below section gives a description of the MATLAB software.

4.3.1 MATLAB :

MATLAB stands for Matrix laboratory and is a high-performance language for technical computing. It integrates computation, visualization, and programming in an easy-to-use environment where problems and solutions are expressed in familiar mathematical notation.

4.3.2 MATLAB Simulator

The name MATLAB stands for Matrix Laboratory. MATLAB was originally made to provide easy access to matrix software developed by the LINPACK and EISPACK projects. Today, MATLAB engines incorporate the LAPACK and BLAS libraries, embedding the state of the art in software for matrix computation.

MATLAB is an interactive system whose basic data element is an array that does not require dimensioning. This allows you to solve many technical computing problems, especially those with matrix and vector formulations, in a fraction of the time it would take to write a program in a scalar non interactive language such as C or Fortran.In industry, MATLAB is the tool of choice for high-productivity research, development, and analysis.MATLAB has evolved over a period of years with input from many users. In university environments, it is the standard instructional tool for introductory and advanced courses in mathematics, engineering, and science.

4.3.3 Key Features :

- Mathematical functions for linear algebra, statistics, Fourier analysis, filtering, optimization, numerical integration, and solving ordinary differential equations**.**
- High-level language for numerical computation, visualization, and application development.
- Interactive environment for iterative exploration, design, and problem solving.
- Built-in graphics for visualizing data and tools for creating custom plots.
- Tools for building applications with custom graphical interfaces.
- Functions for integrating MATLAB based algorithms with external applications and languages such as C, Java, .NET, and Microsoft Excel.
- Development tools for improving code quality and maintainability and maximizing performance.

4.3.4 Architecture of MATLAB System :

The MATLAB system consists of five main parts:

- **Development Environment :**

It includes the MATLAB desktop and Command Window, a command history, an editor and debugger, and browsers for viewing help, the workspace, files, and the search path. This is the set of tools and facilities that help you use MATLAB functions and files. Many of these tools are graphical user interfaces.

- **The MATLAB Mathematical Function Library :**

This is a vast collection of computational algorithms ranging from elementary functions, like sum, sine, cosine, and complex arithmetic, to more sophisticated functions like matrix inverse, matrix eigen values, Bessel functions, and fast Fourier transforms.

- **The MATLAB Language :**

This is a high-level matrix/array language with control flow statements, functions, data structures, input/output, and object-oriented programming features. It allows both “programming in the small” to rapidly create quick and dirty throw-away programs, and “programming in the large” to create large and complex application programs.

- **Graphics :**

MATLAB has extensive facilities for displaying vectors and matrices as graphs, as well as annotating and printing these graphs. It includes high-level functions for two-dimensional and three-dimensional data visualization, image processing, animation, and presentation graphics. It also includes low-level functions that allow you to fully customize the appearance of graphics as well as to build complete graphical user interfaces on our MATLAB applications.

- **The MATLAB Application Program Interface :**

This is a library that allows you to write C and Fortran programs that interact with MATLAB. It includes facilities for calling routines from MATLAB (dynamic linking), calling MATLAB as a computational engine, and for reading and writing MAT-files.

4.3.5 Strengths :

- MATLAB combine nicely calculation and graphic plotting.
- MATLAB is relatively easy to learn.
- MATLAB may behave *as* a calculator or as a programming language .
- MATLAB is optimized to be relatively fast when performing matrix operations.
- MATLAB does have some object-oriented elements.
- MATLAB is interpreted (not compiled), errors are easy to fix.

4.3.6 Usage in Research

MATLAB has been used as the programming tool for implementation of the proposed algorithm. MATLAB contains a number of built in functions which can be easily called in our own program to perform their desired functionalities.

The following toolboxes and the functions related to them are relevant to programming used in this thesis:

- Image Processing Toolbox
- Wavelet Toolbox
- Graphics Library

CHAPTER 5

SYSTEM IMPLEMENTATION AND ANALYSIS

This chapter presents an implementation detail of the research work. The invisible watermark for different kinds of images is generated and embedded inside the cover image. This ensures image security while it is transferred over the internet. The images as explained in Chapter 2 can exit in various formats such as .jpg, .bmp., .png etc. The Discrete Wavelet transform technique will be used to transform these image from their original spatial domain to frequency domain. The watermark generated then would be inserted into one of the frequency bands in the DWT subbands. The detailed architecture of the watermark embedding and extraction is explained in this chapter. This framework will then be implemented and a prototype simulation of the framework has to be performed in the upcoming chapters.

5.1 System Architecture:

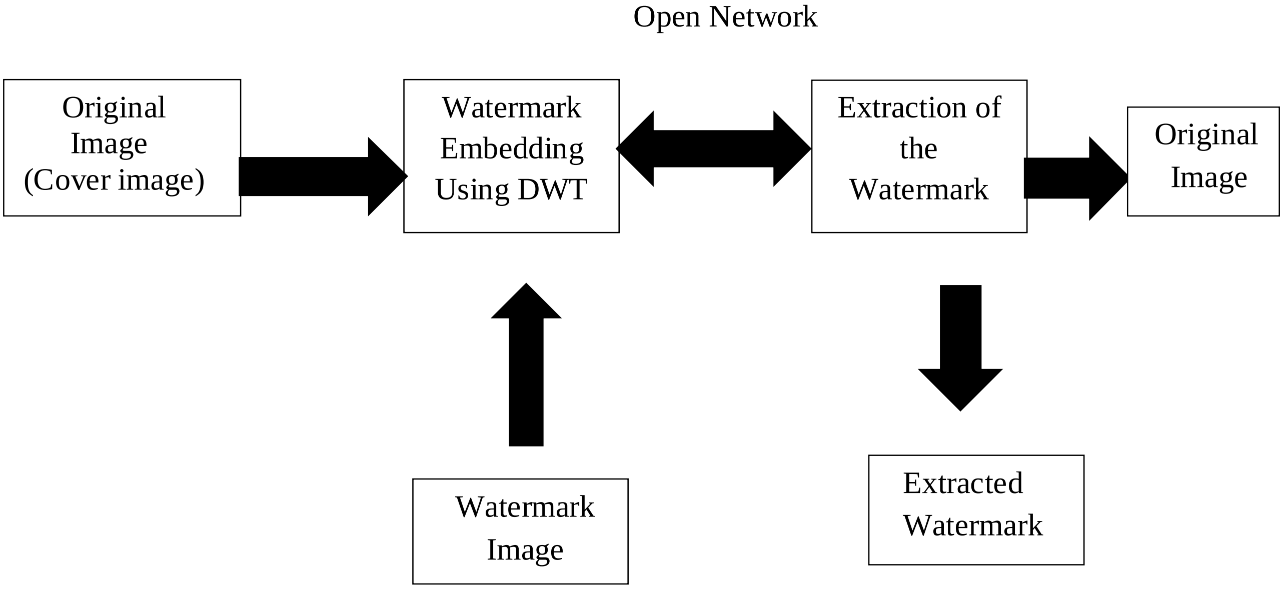

Open Network
Original Image (Cover image)
Watermark Embedding Using DWT
Extraction of the Watermark
Original Image
Watermark Image
Extracted Watermark

Fig 5.1: System Architecture

Figure 5.1 shows the general block diagrammatic representation of the watermarking procedure. The key elements are explained as below:

1. Embedding Process:

   The embedding process consists of embedding the above obtained patient information in the cover image. The cover image also called as original image is the medical image resulting from medical scan of the patient. For this research, various standard images available on the internet have been used. The result of the embedding process is the watermarked image which contains the hidden message behind the original cover image. This image can now be sent over the network.

2. Extraction Process:

   The extraction process is implemented at the receiver side to find out the hidden watermarked image containing the hidden information. If the hidden image is obtained either partially or fully it validates the authenticity of the image and at the same time gives valuable information about the patient’s medical diagnosis at the sender end.

5.2 Watermark Embedding:

The watermark embedding procedure is the most important part in the system architecture. It is required to save the watermark so as to maintain the perceptibility of the image within acceptable limits. The below diagram shows, the stepwise description of the embedding algorithm used in this research work.

Algorithm:

Step1 : Read the image into the system. The image is originally obtained from internet source. The images are available in various formats of compression such as .png(portable network graphics), .jpg(Joint photographic expert group) etc. we have chosen .png image types and of size 256x256. These images when brought to the system are available in true color format, even if they appear having only gray, black and white shades but system reads them as a true color image only, having mxnxp structure. So the next step involves converting it to a suitable format.

Step2: The image read in above is converted to a grayscale format.

Step 3: The watermark image to be embedded i.e. the image form is available in .bmp format is converted to the same size as that of the image i.e 256x256.

Step 4: The next step is to calculate the 2-D Discrete Wavelet Transform of the original image or the cover image. The DWT method has been used which has a lot of advantages over other methods. Discrete wavelet transformation(DWT) techniques divides the cover image into sub bands where the higher bands represent finer details and lower bands generally have more important information. Entropy coders locate the subband coefficients and encode them. DWT technique has an edge over DCT that it offers efficient energy packing than DCT without blocking the artifacts after the process of coding. DWT has a multi-resolution based nature that make it best fit for scalable image coding.

The result of this step is the division of the spatial domain image into a frequency domain sub bands. A 2D-DWT results into four sub bands as shown in the below figure 5.2.

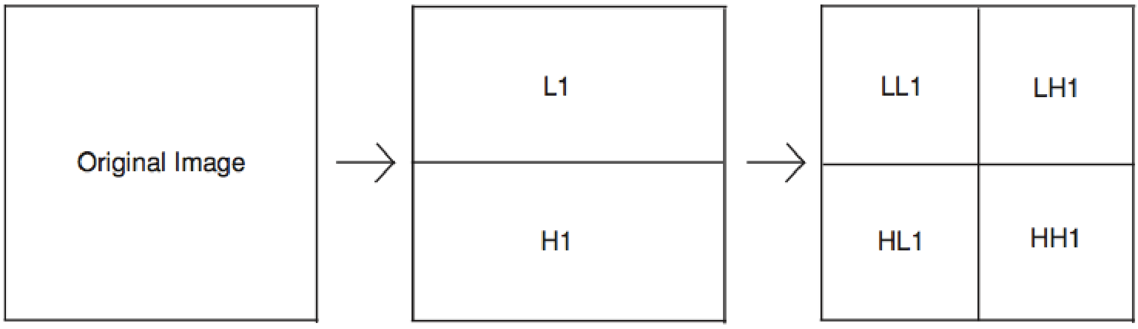


Fig 5.2 : 2D-DWT subbands

The sub bands thus obtained are LL1 which stands for low-low frequency, LH1 for low-high frequency, HL1 for high-low frequency and HH1 for high-high frequency respectively. These bands contain the frequency transform information of the image. As described earlier the high frequency band contain less redundant information and can be our region of interest to place the watermark image inside these high frequency components.

The wavelet transform uses wavelet filters to find out the frequency coefficients. In this algorithm daubechies1 filter has been used.

Step 5: The watermark image is embedded in one of the high frequency subband. For this research work results, the HL i.e high-low frequency component has been chosen. The embedding process id done using the below equation:

Y= cv + c*abs(cv).* N (5.1)

where cv is the DWT coefficient in which the embedding is done, c is the watermark weight, N is the size of hidden image

This generates new coefficients with the embedded information of the hidden image.

Step 6: The inverse discrete Wavelet Transform(IDWT) is performed on the above sub bands to convert the frequency domain image information to spatial domain pixel information. This completes the embedding process.

5.3 Watermark Extraction

.The extraction process is basically to be employed at the receiving end of such a kind of system as shown in figure 3.1. The image is obtained over the network and is sent to the extraction algorithm, which performs the extraction process on this received image and if it is possible to extract the hidden image, then image can be assumed to be authentic.

Algorithm:

Step 1: Read in the image obtained at the receiver end. This image is actually the watermarked image which apart from what appears outside as similar to the original cover image but it must contain the embedded watermark as well.

Step2: 2-D DWT is performed on this image to obtain conversion from spatial domain to the frequency domain and to get the frequency sub bands of this image. The wavelet filter used at the embedding stage is daubechies 1. The same filter is used to perform the 2-D DWT on the image, yet again.

Step 3: The coefficients obtained from the above step, which contain the watermark image is the high low band. Thus it is extracted from the DWT transform to obtain the frequency domain transform, using the following equation:

cc=abs(cv1./N); (5.2)

where cc is hidden message, cv1 is the coefficients of DWT and N is watermark size.

5.4 Results and Discussion:

Extensive experiments have been performed on a number of images to analyze the working of the algorithm. Several standard test images such as boat, baboon, Lena, peppers, couple, cameramen etc are referred to in the present paper for watermark embedding and watermark detection. The technique is not limited to the use these cover images but we have used them as they are standard images widely used by other researchers working on watermarking. They all are gray scale images with size 256x256. All the images are watermarked using the best evolved expression.

The below portion shows the obtained results on Baboon image:

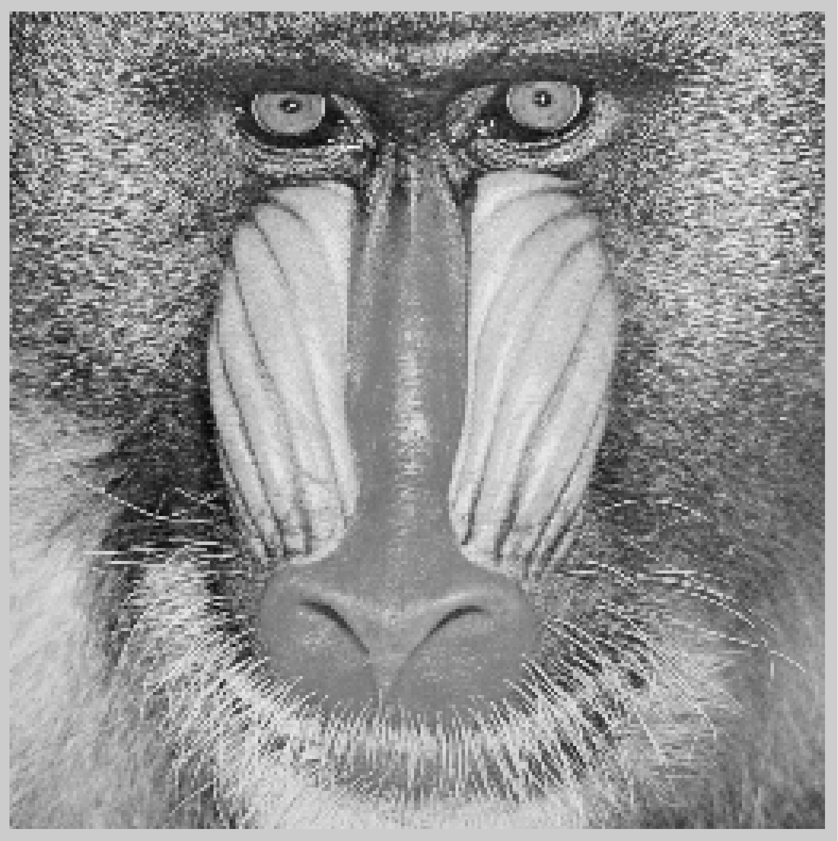


Fig 5.3: Original Image

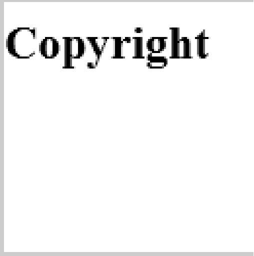


Fig 5.4: Key Image (Hidden Image)

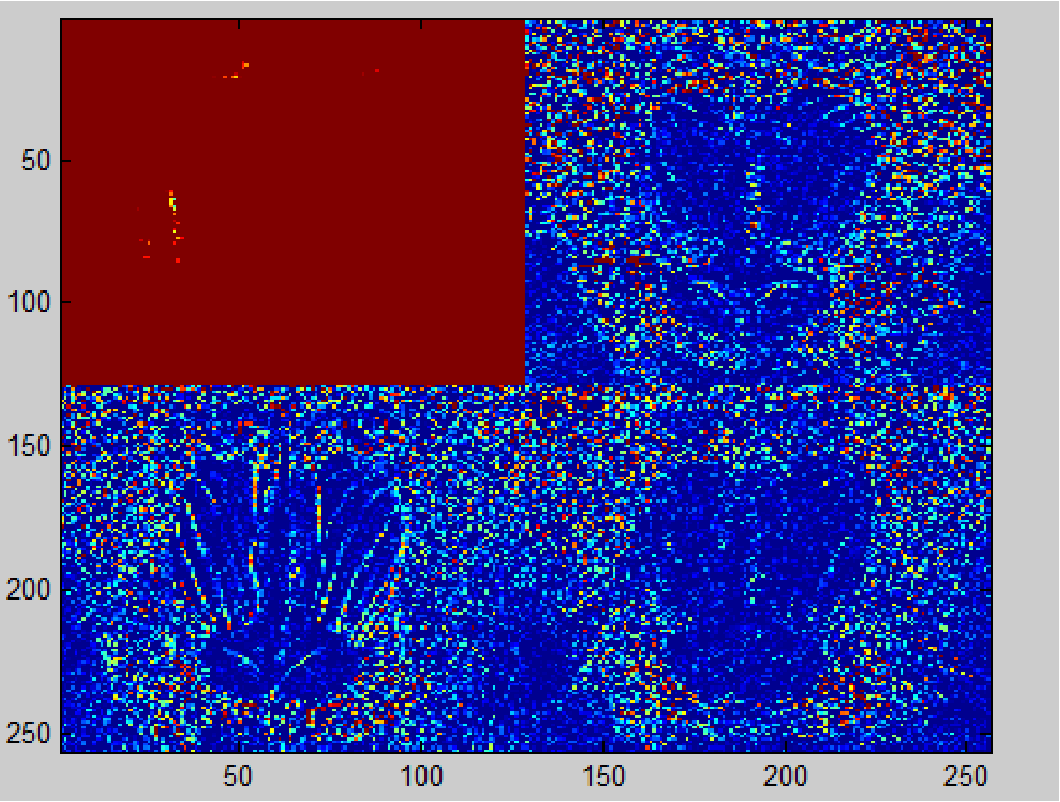


Fig 5.5: Image after 2D-DWT

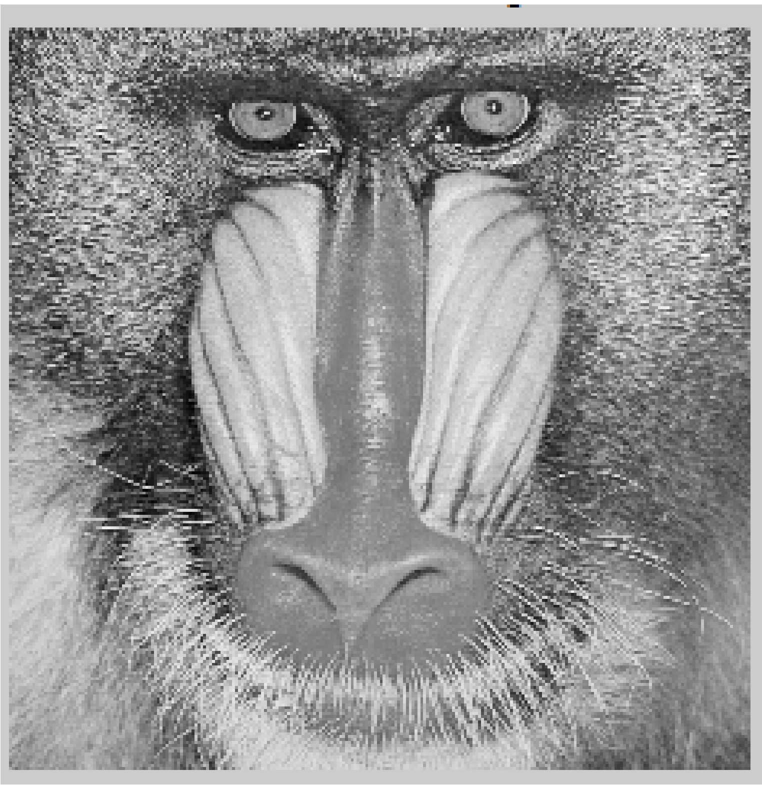


Fig 5.6: Watermarked Image

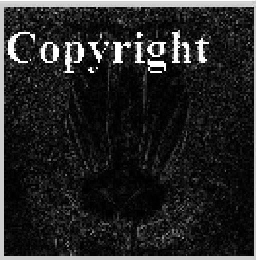


Fig 5.7: Retrieved Watermark

The above figure shows the various parts of the implementation. Figure 5.3 shows the original image of baboon. Figure 5.4 shows the key image. Figure 5.5 shows the watermarked image which is watermarked using the best evolved expression. There is no perceptual distortion in the watermarked image which shows the high imperceptibility of the proposed technique. . Figure 5.7 shows the retrieved watermark under no attacks, which proves that the proposed method is able to learn the spatial distribution of the baboon image.

The results obtained from other test images viz. boat, peppers and lena are as shown below. Since the hidden image is same, as in the above case so it is excluded and the results of other steps are only shown for other images.

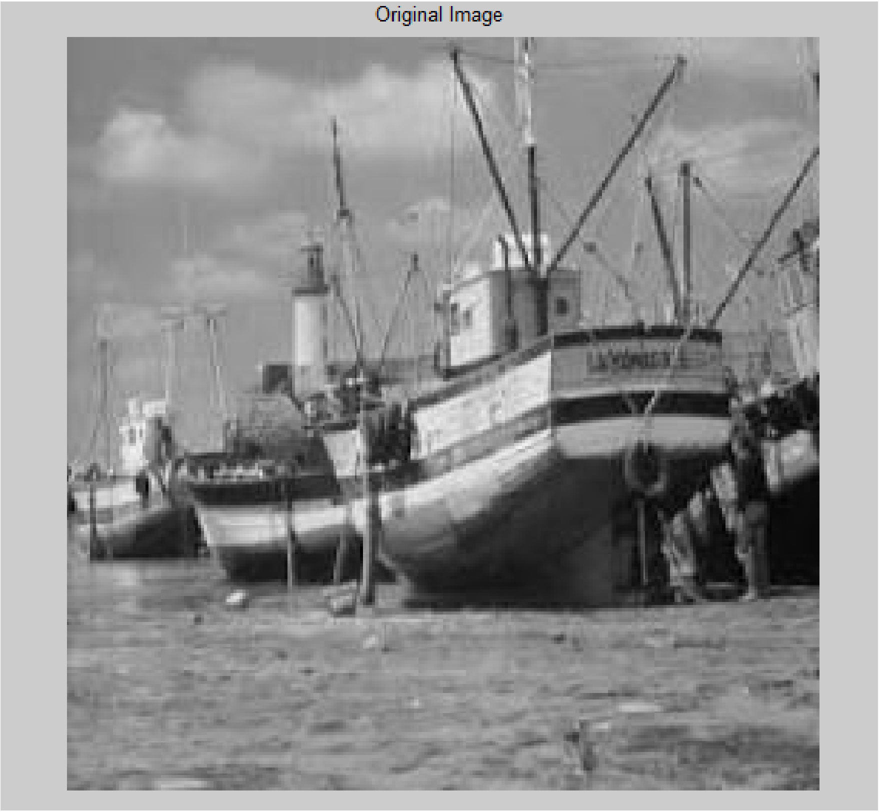


Fig 5.8: Original Image(Boat)

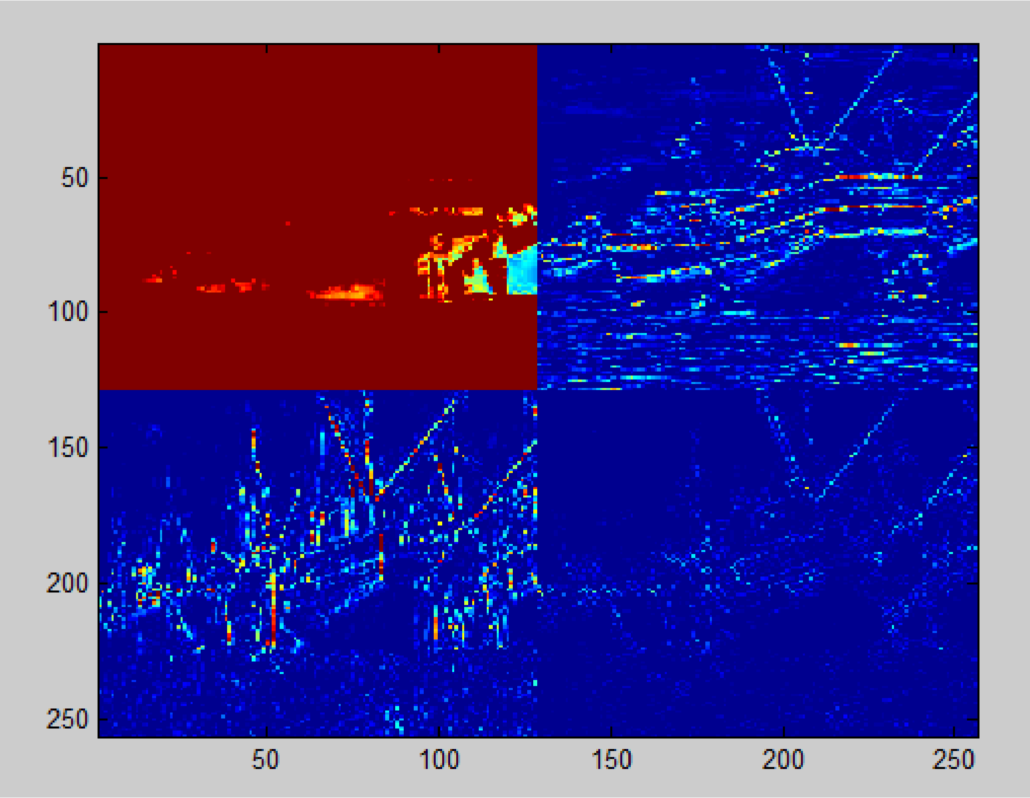


Fig 5.9: Image after 2D-DWT

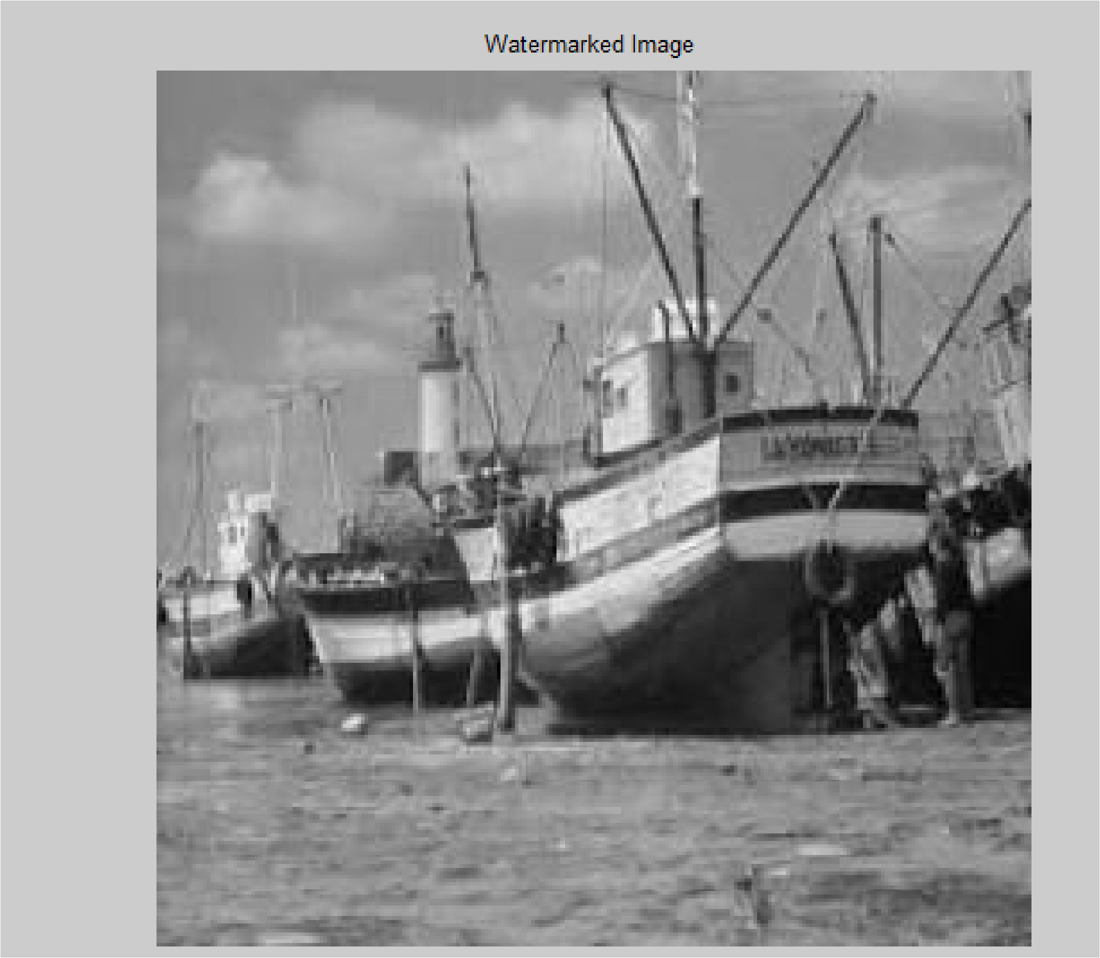


Fig 5.10: Watermarked Boat Image

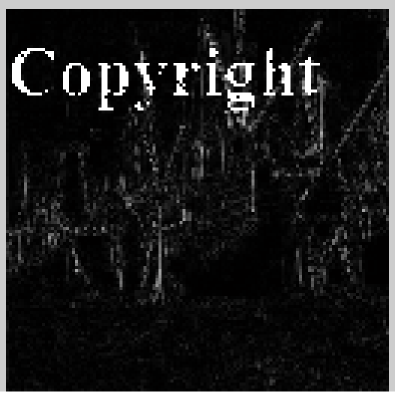


Fig 5.11: Extracted Watermark

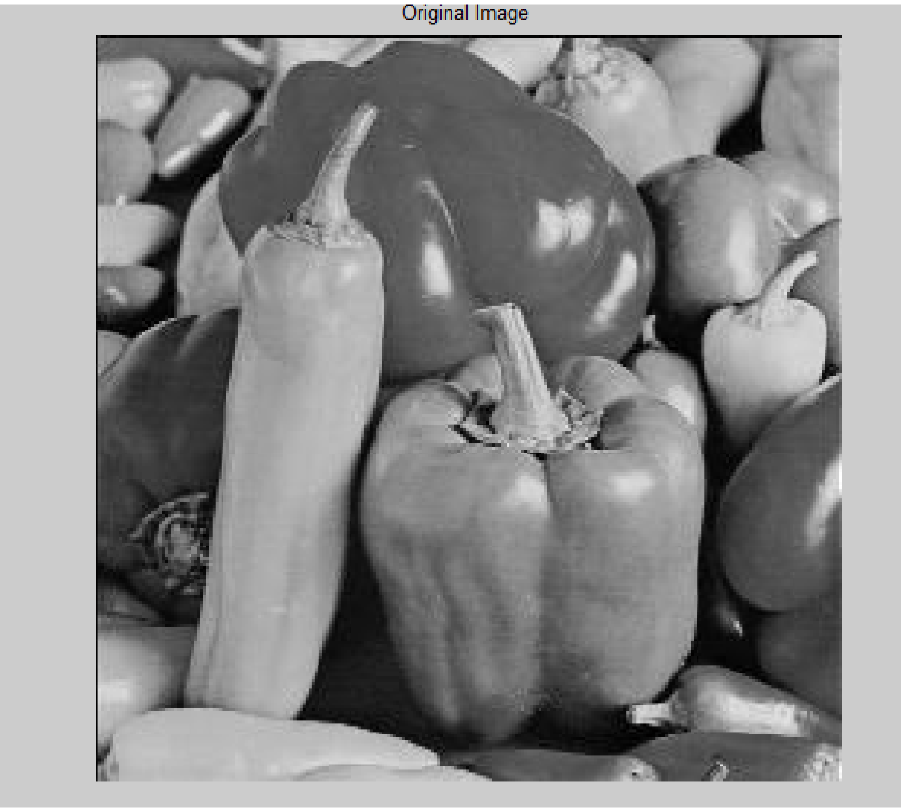


Fig 5.12: Original Image(Peppers)

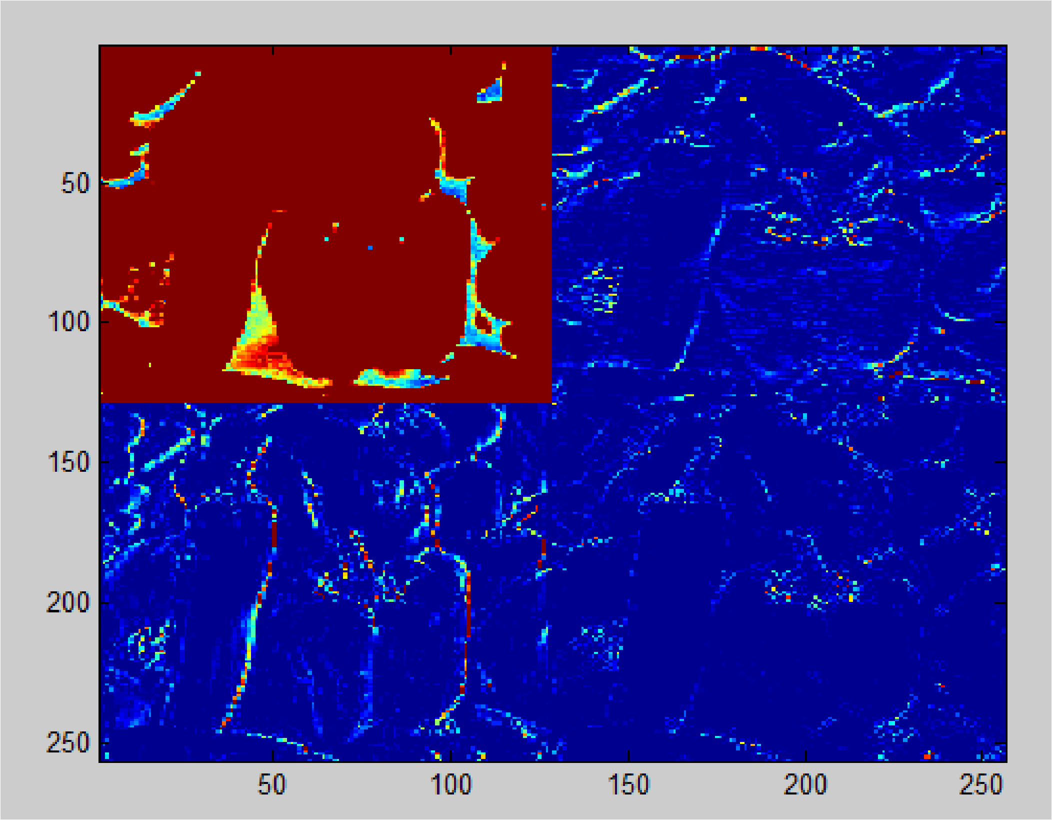


Fig 5.13: Image after DWT(Peppers)

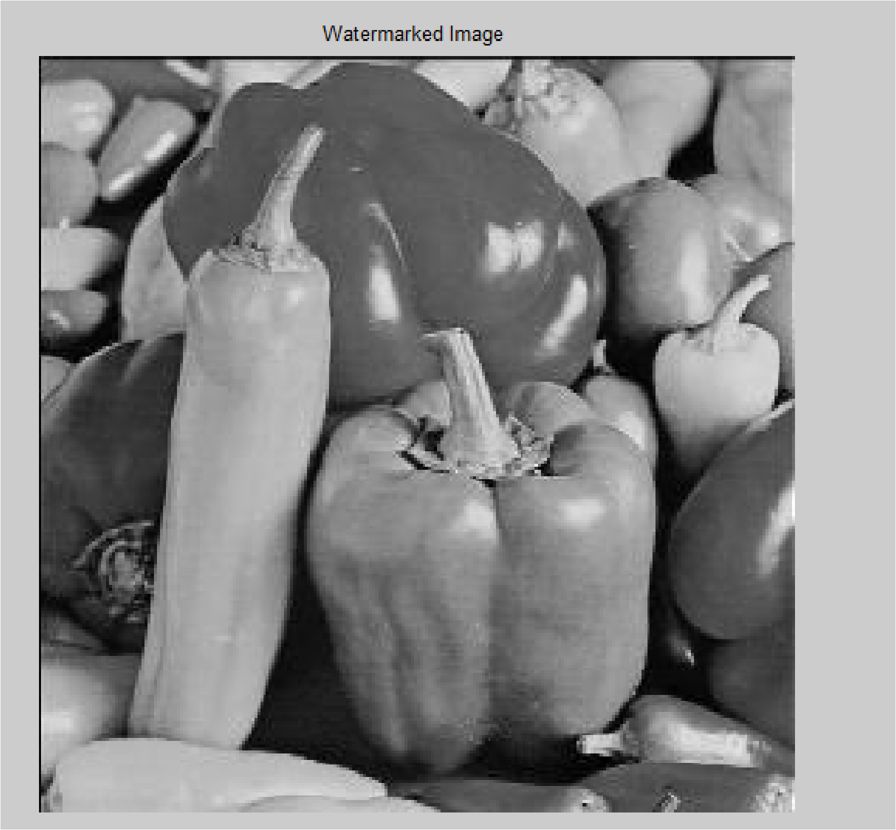


Fig 5.14: Watermarked Image

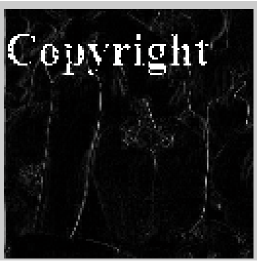


Fig 5.15: Retrieved Watermark

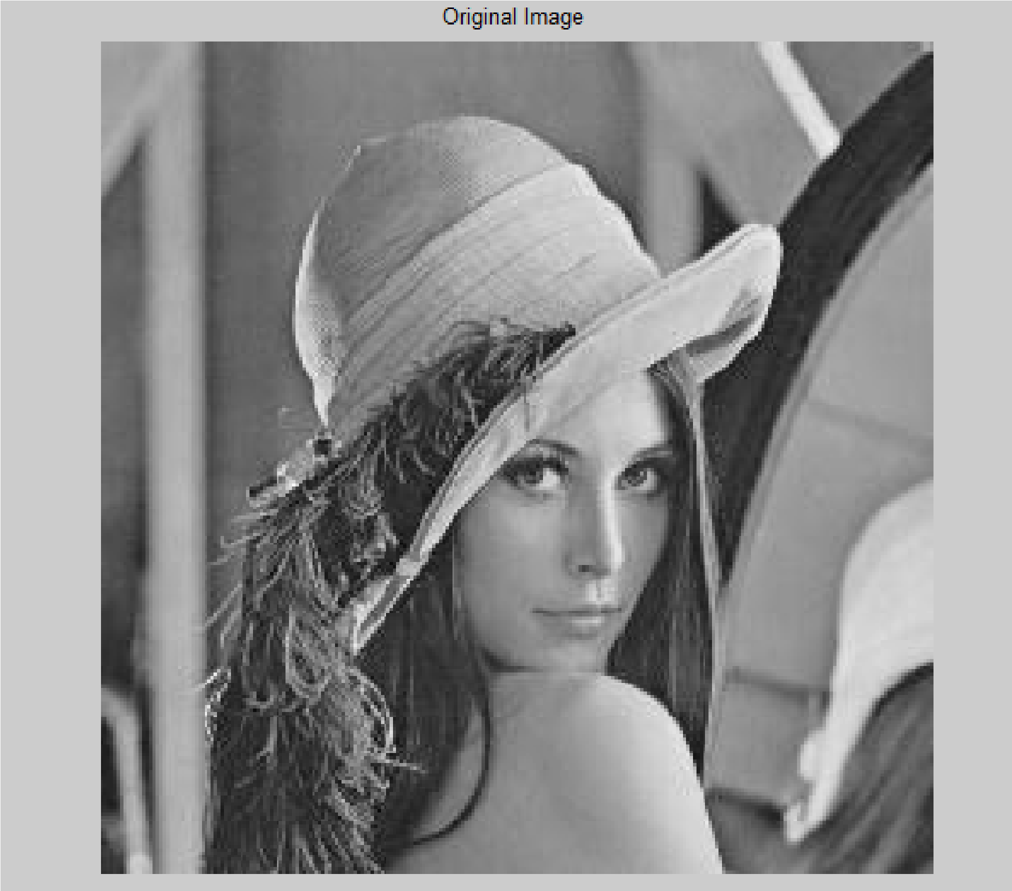


Fig 5.16: Original Image(Lena)

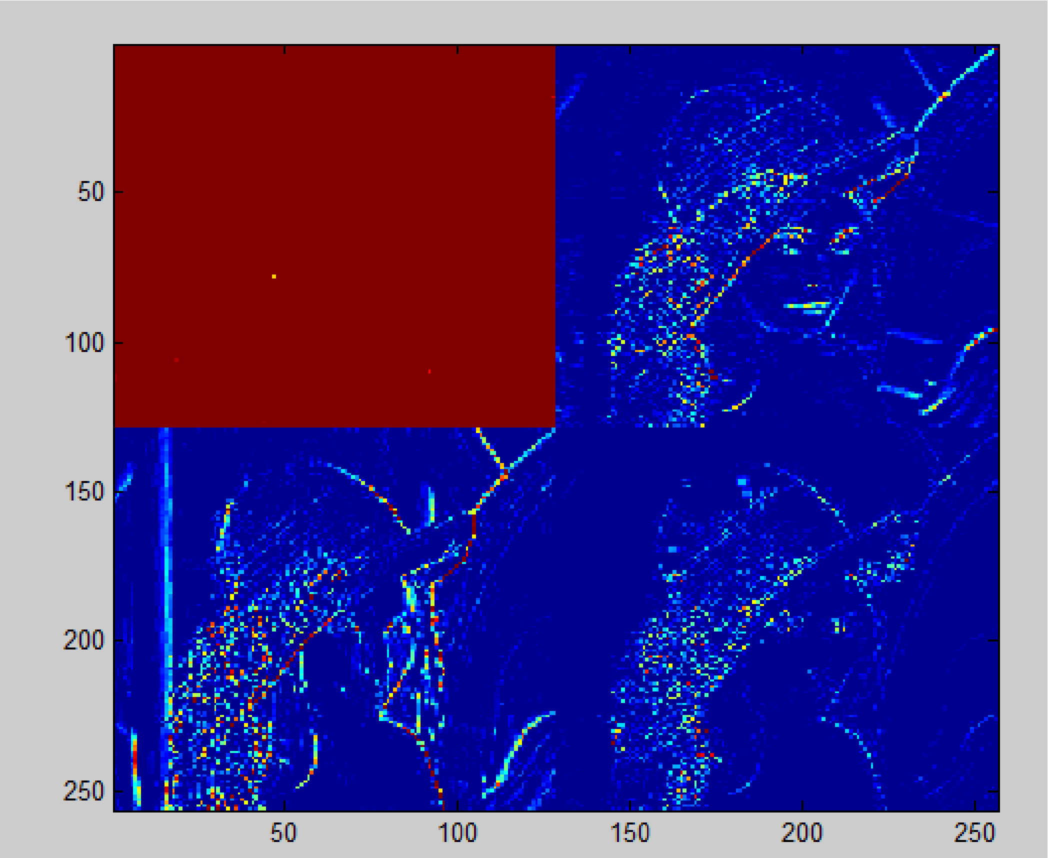


Fig 5.17: Image after 2D-DWT

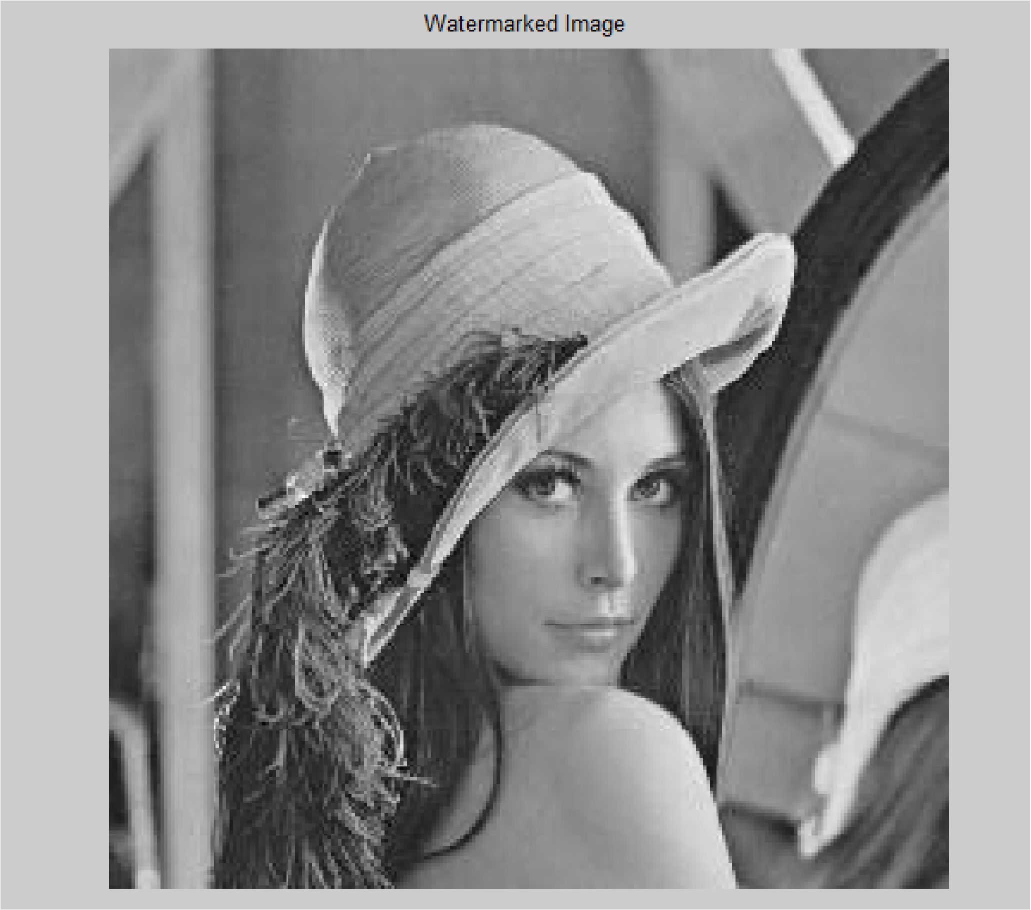


Fig 5.18: Watermarked Image

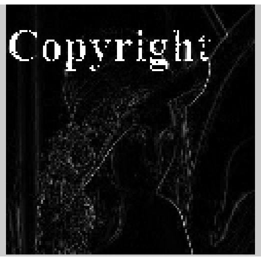


Fig 5.19: Retrieved Watermark

The below table represents the values of PSNR and MSE for various images.

Table 5.1:Comparative Results for Baboon Image

Filter Used	**MSE**	**PSNR**
HAAR(DB1)	80.7402	66.9129
SYMLET	79.4937	67.0685
COIFLET	80.0438	66.9995

Table 5.2: Comparative Results for Boat Image

Filter Used	**MSE**	**PSNR**
HAAR(DB1)	38.9263	74.2086
SYMLET	38.3553	74.3564
COIFLET	38.3842	74.3488

Table 5.3: Comparative Results for Pepper Image

Filter Used	MSE	PSNR
HAAR(DB1)	27.3578	77.7353
SYMLET	25.3977	78.4787
COIFLET	25.3234	78.0580

Table 5.4: Comparative Results for Pepper Image

Filter Used	MSE	PSNR
HAAR(DB1)	26.5616	78.0306
SYMLET	25.2895	78.5214
COIFLET	25.5326	78.4257

CONCLUSION

This research work presents a novel approach towards Digital Image Watermarking. Digital Image Watermarking has important role in image authentication and registration and is an integral part of various applications. In this work, the various watermarking techniques were discussed extensively to understand the state of the art of Digital image Watermarking. A number of methods such as Least Significant Bit(LSB) Watermarking, DCT based Watermarking and DWT based Watermarking have been presented in brief in the survey of the state of the art literature. The various watermarking models have also been thoroughly studied to come to have a better understanding of the domain. Further, the Wavelet domain and wavelet based watermaking is special importance to the context of this research works thus the various terms related to wavelet, wavelet analysis, multiresolution analysis etc. has been discussed. Another important aspect of this research work is to deploy various kinds of wavelet filters for performing the watermark. Thus, a number of wavelet filters have been studied and presented in this work.

A discussion on Wavelet transform and wavelet filters gives a thorough insight into the wavelet technology which can be greatly useful to better understand the wavelet terminology. The proposed method based on 2D-DWT technique has been implemented and tested on a number of standard test images and the results show a high level of perceptibility of Watermarked Image and the retrieved hidden image. The method was implemented using haar, symlet and coiflet filters. A comparative analysis of results in terms of MSE and PSNR is shown which gives the conclusion that symlet filter based algorithm is the best in terms of performance.

FUTURE WORK

The future research work can be centered around validating the findings of this research work by including a larger set of images. Further, the present work can be extended with higher levels of wavelet analysis. Another modification in research idea could be to include Artificial intelligence, Fuzzy logic or Neural Network to select the redundant and non-redundant information form the watermark to achieve better performance.

REFERENCES

[1]. M. Kim, D. Li and S. Hong, “A Robust Digital Watermarking Technique for Image Contents based on DWT-DFRNT Multiple Transform Method”,International Journal of Multimedia and Ubiquitous Engineering,Vol.9, No.1 (2014), pp.369-378.

[2]. Brijesh B. Mehta, Udai Pratap Rao,” A Novel approach as Multi-place Watermarking forSecurity in Database”,Int'l Conf. Security and Management | SAM'11 |.

[3]. Nameer N. EL-Emam,”Hiding a Large Amount of Data with High Security Using Steganography Algorithm”,Journal of Computer Science 3 (4): 223-232, 2007

[4]. Dipesh Agrawal and Samidha Diwedi Sharma,” Analysis of Random Bit Image Steganography Techniques”, International Journal of Computer Applications (0975 – 8887)International Conference on Recent Trends in engineering & Technology – 2013.

[5]. Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt,”Digital Image Steganography: Survey and Analysis of Current Methods”, Signal Processing, Volume 90, Issue 3, March 2010, Pages: 727-752\

[6]. Anil Kumar and Rohini Sharma,”A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique”,International Journal of Advanced Research in Computer Science and Software Engineering,Volume 3, Issue 7, July 2013.

[7]. Ramadhan Mstafa and Christian Bach,”Information Hiding in Images Using Steganography Techniques”,2013 ASEE Northeast Section Conference, Norwich University, March 14-16, 2013.

[8]. ISO/IEC 14495-1**,** ITU T.87, “Information technology - Lossless and near-lossless compression of Continuous tone still images," 1999.

[9]. M. J. Weinberger, G. Seroussi, and G. Sapiro, "LOCO-I: A low complexity, context-based, lossless image compression algorithm," in *Proc. DCC'SG,* (Snowbird, Utah, USA), pp. 140-149, Mar. 1996.

[10]. I. Ueno and F. Ono. "Prouosed modification of LOCO-I for its improvement of the performance." ISOIIEC JTCl/SC29/WGl doc. N297. Feb. 1996.

[11]. M. 'J. Weinbeiger, G. Seroussi, and G. Sapiro. ISO/IEC JTCl/SC29/WGl docs. N341, N386, N412 (1996).

[12]. M. J. Weinberger, G. Seroussi, G. Sapiro, and E. Ordentlich, "JPEG-LS with limited-length code words." ISO/IEC JTCl/SC29/WGl doc. N538**,** July 1997.

[14] Yu, Y.-H., Chang, C.-C., & Lin, I.-C. “A new steganographic method for color and grayscale image hiding. Computer Vision and Image Understanding”, 107(3), 183-194. doi: 10.1016/j.cviu.2006.11.002, 2007

[15]Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. *Signal Processing, 90*(3), 727-752,2007

[16] Min-Jen, T., & Jung, L. (2011, 6-9 Nov. 2011). The quality evaluation of image recovery attack for visible watermarking algorithms. Paper presented at the Visual Communications and Image Processing (VCIP), 2011 IEEE.

[17] H.Harrak,T.D. Hien & Y. Nagata, Z.Nakao,” DCT Watermarking Optimization by Genetic Programming”, Volume 35 of the series Advances in Soft Computing pp 347-351.

[18] Chun-Hsiang Huang, Chih-Hao Shen & Ja-Ling Wu,” Fidelity-Controlled Robustness Enhancement of Blind Watermarking Schemes Using Evolutionary Computational Techniques”, Volume 3304 of the series Lecture Notes in Computer Science pp 271-282

[19] Min-Jen, T., & Jung, L ,“The quality evaluation of image recovery attack for visible watermarking algorithms”, Paper presented at the Visual Communications and Image Processing (VCIP), 2011 IEEE, (2011, 6-9 Nov. 2011).

[20] Akhil Pratap Singh and Agya Mishra,”Wavelet Based Watermarking On Digital Image”,Indian Journal of Computer Science and Engineering,Vol 1 No 2, 86-91.

[21] B. de Kraker. A numerical-experimental approach in structural dynamics. Technical report, Eindhoven University of Technology, Department of Mechanical Engineering, 2000.

[22] G. Strang and T. Nguyen. Wavelets and Filter Banks. Wellesley-Cambridge Press, second edition, 1997. ISBN 0-9614088-7-1.

[23] M.G.E. Schneiders. Wavelets in control engineering. Master’s thesis, Eindhoven University of Technology, August 2001. DCT nr. 2001.38.

APPENDICES

I. APPENDIX – CODE FOR SETTING OF IMAGES.

Vtest1

```
a=imread('imw.png');
b=rgb2gray(a);
b=a;imshow(b)%imshow(b);
b(45:135,108:135,:)=255;
b(:,108:135,:)=255;
b(45:135,:,:)=255;
imshow(b);
%test=b;
test=b;
```

II. APPENDIX -CODE USING COIFLET FILTER

```
im-coif-

clc;close all;clear all;

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

img  = imread('peppers.png'); %Get the input image
img  = rgb2gray(img);      %Convert to grayscale image
img  = double(img);
c = 0.001; %Initialise the weight of Watermarking

figure,imshow(uint8(img)),title('Original Image');
[p q] = size(img);figure;

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%

%Generate the key
vtest1;
n=double(test);
N=n(1:130,1:130);
figure,imshow(uint8(N)),title('Key');

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

%Computing the Wavelet Transform

[Lo_D,Hi_D,Lo_R,Hi_R] = wfilters('coif1');%Obtain the fiters associated with
haar
[ca,ch,cv,cd] = dwt2(img,Lo_D,Hi_D);     %Compute 2D wavelet transform

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%
```

```
%Perform the watermarking
y = [ca ch;cv cd];
figure;image(y)
Y1= cv + c*abs(cv).* N; %mbedding message into the image;

Y11=[ca ch;Y1 cd];

p=size(Y1,1);q=size(Y1,1);
for i=1:p
for j=1:q
        nca1(i,j) = Y11(i,j);
        ncv1(i,j) = Y11(i+p,j);
        nch1(i,j) = Y11(i,j+q);
        ncd1(i,j) =  Y11(i+p,j+q);
end
end


%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%

%Display the Watermarked image
wimg1 = idwt2(nca1,nch1,ncv1,ncd1,Lo_R,Hi_R);


figure,imshow(uint8(wimg1)),title('Watermarked Image');
imwrite(uint8(wimg1),'wm.jpg');


%extraction of message
wimg11=imread('wm.jpg');
[ca1,ch1,cv1,cd1] = dwt2(wimg11,Lo_D,Hi_D);
cc=abs(cv1./N);
%diff = imabsdiff(cv1,cv);
figure,imshow((cc));title('Extracted Watermark');
mse=mean(mean(img-double(wimg1))).^2% computing mse
psnr=10*log(255*255/mse)
```

III. APPENDIX -CODE USING SYMLET FILTER

```
im-sym-

clc;close all;clear all;

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

img  = imread('peppers.png'); %Get the input image
img  = rgb2gray(img);      %Convert to grayscale image
img  = double(img);
c = 0.001; %Initialise the weight of Watermarking
```

```
figure,imshow(uint8(img)),title('Original Image');
[p q] = size(img);figure;

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%

%Generate the key
vtest1;
n=double(test);
N=n(1:131,1:131);
figure,imshow(uint8(N)),title('Key');

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

%Computing the Wavelet Transform

[Lo_D,Hi_D,Lo_R,Hi_R] = wfilters('sym4');%Obtain the fiters associated with
haar
[ca,ch,cv,cd] = dwt2(img,Lo_D,Hi_D);     %Compute 2D wavelet transform

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%

%Perform the watermarking
y = [ca ch;cv cd];
figure;image(y)
Y1= cv + c*abs(cv).* N; %mbedding message into the image;

Y11=[ca ch;Y1 cd];

p=size(Y1,1);q=size(Y1,1);
for i=1:p
for j=1:q
        nca1(i,j) = Y11(i,j);
        ncv1(i,j) = Y11(i+p,j);
        nch1(i,j) = Y11(i,j+q);
        ncd1(i,j) =  Y11(i+p,j+q);
end
end


%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%

%Display the Watermarked image
wimg1 = idwt2(nca1,nch1,ncv1,ncd1,Lo_R,Hi_R);


figure,imshow(uint8(wimg1)),title('Watermarked Image');
imwrite(uint8(wimg1),'wm.jpg');
```

```
%extraction of message
wimg11=imread('wm.jpg');
[ca1,ch1,cv1,cd1] = dwt2(wimg11,Lo_D,Hi_D);
cc=abs(cv1./N);
%diff = imabsdiff(cv1,cv);
figure,imshow((cc));title('Extracted Watermark');
mse=mean(mean(img-double(wimg1))).^2% computing mse
psnr=10*log(255*255/mse)
```

LIST OF PUBLICATIONS

International journal

- Akanksha Singh and Mohd.Saif Wajid “A Watermarking Approach in DWT Domain using **S**YMLET and COIFLET Filters” IJARIIT international journal of advance research , ideas and innovations in technology (volume 3, Issue 3), india, May 2017.

CURRICULUM VITAE

AKANKSHA SINGH

OBJECTIVE

- To enhance the goodwill of institution and to build a career in teaching and research work ,which will help me to explore myself fully and realize my potential.

E.Mail I.D : akankshasingh9495@gmail.com

ADDRESS : B-5 , Sector-C , Aliganj ,Lucknow**.**

EDUCATIONAL QUALIFICATIONS

- Pursuing M. Tech. in Computer Science & Engineering (S.E) from BBDU Lucknow.
- B.Tech . in Computer Science & Engineering (72%) from Rameshwaram Institute of Technology and Management , Lucknow .Year of passing : 2012.
- Central Board of Secondary Education Certificate(65%) from Navyuga Radiance Lucknow. Year of passing : 2003.
- High School Certificate (HSC) (62%) from CMS , Lucknow. Year of passing : 2001.

M.TECH THESIS

- A Technique To Mitigate The Effect Of Attacks In Digital images.

PUBLICATIONS

- Akanksha Singh and Mohd.Saif Wajid "A Watermarking Approach in DWT Domain using **S**YMLET and COIFLET Filters" IJARIIT international journal of advance research , ideas and innovations in technology (volume 3, Issue 3), india , May 2017.

DECLARATION

- I Akanksha Singh , hereby declare that the information furnished above are truee and correct to the best of my knowledge and belief.