# `DIGITAL WATERMARKING TECHNIQUE ON FINGERPRINT IMAGE

A Dissertation submitted in fulfillment of the requirements for the Degree

of

## MASTER OF ENGINEERING

*in*

## Electronic Instrumentation & Control Engineering


*Submitted by*

Nisha Chugh
801351014

*Under the Guidance of*
Dr. Sunil Kumar Singla

Assistant Professor, EIED


**2015**


**Electrical and Instrumentation Engineering Department**

**Thapar University, Patiala**

***(Declared as Deemed-to-be-University u/s 3 of the UGC Act., 1956)***

**Post Bag No. 32, Patiala – 147004 Punjab (India)**

# DECLARATION

I hereby certify that the work which is presented in dissertation entitled, "**Digital Watermarking Technique on Fingerprint Image**", in partial fulfillment of the requirements for the award of the degree of **Master of Engineering in Electronics Instrumentation & Control**, submitted to Electrical & Instrumentation Engineering Department of Thapar University, Patiala is as authentic record of my own work carried under the supervision of **Dr. Sunil Kumar Singla**. It refers others researcher's work which are duly listed in the reference section. The matter contained in this dissertation has not been submitted, neither in part nor in full to any other degree to any other university or institute except as reported in text and references.

Place: Thapar University, Patiala

Date: 14-07-15

**(Nisha Chugh)**

**Roll No.: 801351014**

It is certified that the above statement made by the student is correct to the best of my knowledge and belief.

14/7/2015

**(Dr. Sunil Kumar Singla)**

**Assistant Professor**

Electrical & Instrumentation Engineering Department

Thapar University, Patiala

Date: 14-07-15

***Countersigned by:***

**Dr. Ravinder Agarwal**

Head

Electrical & Instrumentation Engineering Department

Thapar University, Patiala

**Dr. S.S. Bhatia**

Dean (Academic Affairs)

Thapar University, Patiala

# ACKNOWLEDGEMENT

First of all, I would like to express my gratitude to **Dr. Sunil Kumar Singla, Assistant Professor,** Electrical and Instrumentation Engineering Department, Thapar University Patiala for his patient guidance and support throughout this report. I am truly very fortunate to have the opportunity to work with him. I found his guidance to be extremely valuable.

I express my sincere gratitude to **Dr. Ravinder Agarwal, Head of the Department** as well as PG coordinator, **Nirbhowjap Singh, Assistant Professor**, Electrical and Instrumentation Engineering Department.

I would like to thank **Mr. Atul Sharma, Research Scholar,** EIED Department and the entire faculty and staff of Electrical and Instrumentation Engineering Department and my friends who devoted their valuable time and help me in all possible ways towards successful completion of this work. I also thank all those who have contributed directly or indirectly to this work.
Lastly, I would like to thank my parents for their continuous love and encouragement.

Nisha Chugh

**(Nisha Chugh)**

**Roll No.: 801351014**

Place: Thapar University, Patiala

Date: 14-07-15

# TABLE OF CONTENTS

**TOPIC** **PAGE NO**

# TABLE OF CONTENTS (continued)

# LIST OF TABLES

# LIST OF FIGURES

# NOMENCLATURE

| | |
|---|---|
| DWT | Discrete Wavelet Transform |
| DCT | Discrete Cosine Transform |
| PSNR | Peak Signal To Noise Ratio |
| MSE | Mean Square Error |
| FOR | Fitness of recovery |

# Abstract

In this age of automated world, the protection of data is of utmost importance. Digital watermarking is one of the probable solution along with steganography for claiming the ownership. While in steganography, data is always hidden but in watermarking, it can be visible or invisible. Digital watermarking is a technique of hiding the digital watermark, which is a low energy signal, in the image, video or audio signal, in a blind or non-blind way. This dissertation presents a Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) based blind watermarking technique that securely embeds a letter image in the fingerprint image to enhance the security level. DCT, DWT and Different levels of DWT are compared in terms of Peak Signal to noise ratio and fitness factor. The analysis of watermarked image under the salt & pepper and JPEG compression attacks has been carried out to find out the robustness of the system. DWT gives much better result than DCT and in the DWT, as the level of transform increases, imperceptibility of the watermarked image is increased in such a way that it can cheat the human vision easily on the other hand robustness get decreased, fitness factor of the extracted watermark is not good enough as it was in the previous level. It is concluded that there has to be a tradeoff between the robustness and imperceptibility of the watermark. Apart from imperceptibility and robustness, average elapsed time for embedding and extraction has also been compared between DCT and various levels of DWT and results shows that DCT take more time than DWT and time get reduced as the level of DWT increases.

# CHAPTER 1

# INTRODUCTION

## 1.1 Introduction

Due to the advent of internet, it is possible to create and deliver the contents like image, real time audio and video in digital form. An important issue is the protection of rights and assurance of security of all the contributors. This has lead the researchers to take interest in developing new security mechanisms. Digital Watermarking is one of the potential solution for claiming the ownership [1].

Watermarking is old technique as it is the descendant of steganography, which has been in extant for many years. Steganography is the hiding of secret data within other cover message so that the existence of data will not be noticed. Some of the techniques like invisible ink, word spacing patterns in a printed document etc have been used since the times of ancient Greek civilization. But Steganography is dissimilar with digital watermarking in many aspects. Firstly, digital watermarks may be visible or invisible that is, it need not always to be hidden on the other hand Steganography is always hidden. So, visible watermarks are not to be examined as Steganography. Secondly, Robustness is the important factor in digital watermarking. But still, Watermarking is examined as a precise technique of steganography where the secrete message called watermark is embedded in the host message in such a way that it may or may not be captured by human eye. If it is visible to human eye then called visible watermarking and if it is invisible, called blind watermarking. The most common examples of watermarking includes specific patterns in currency notes which are only visible after a certain process, logos present in the printed text documents and many more. This is the watermarking in physical objects.

Digital watermarking is alike to watermarking real entity except that the digital watermarking technique is used for digital content instead of real entity. In digital watermarking, low energy signal called watermark is embedded in the host signal in this way that it is difficult for the human eye to perceive it [2]. Host signal may be image, video, audio or text document in digital set-up. The digital watermarking system essentially consists of embedding and extraction as

shown in Fig1.1. The watermark embedder embeds a watermark in the host signal which is called embedding and watermark extractor extract the watermark signal from the watermarked image. A special vital force named, secret key is used during embedding and extraction of watermark. This secret key is very personal which is only known to the programmer or the authorized parties which ensures the authentication of the watermark. Further, channel may be prone to attacks So, it must be flexible to the attacks so that if attacks are performed on the image, watermark not get lost from the watermarked image.

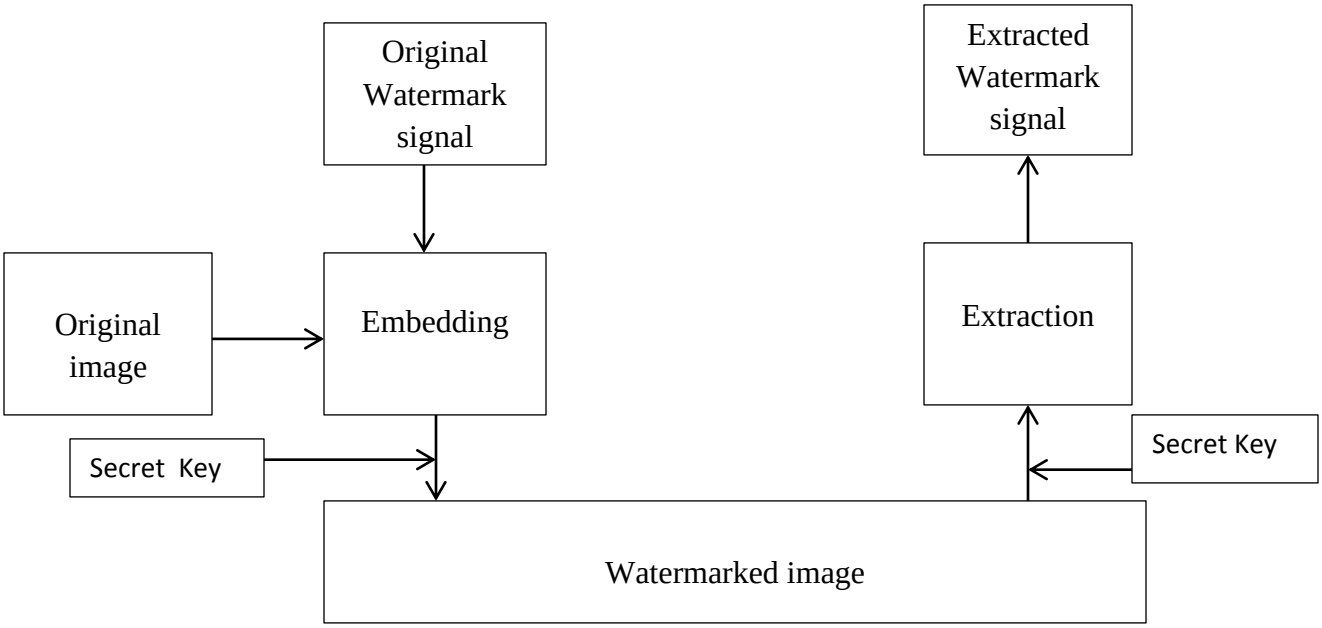



Fig 1.1: Digital Watermarking System [2]

Watermarking of fingerprint images is used to secure central databases from which fingerprint images are sent to intelligence agencies for identification purposes. So, if the fingerprint that is received is falsely matched to someone else due to some incidental/intentional tampering, then the extracted watermark plays an important role to justify weather the fingerprint is of same person or not [3]. Therefore invisible watermark in the fingerprint images plays an important role and in this project, complete work is done on the various images in a way that watermark which may be name, voter id number, pan card number or any particular identification proof of the

person is embed in the fingerprint after that that particular watermark is extracted from the watermarked image.

### 1.2 Classification Of Digital Watermarks

The digital watermarks are classified as shown in Fig 1.2

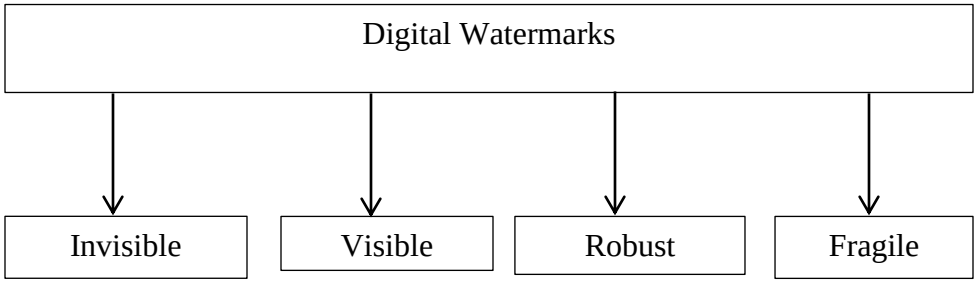
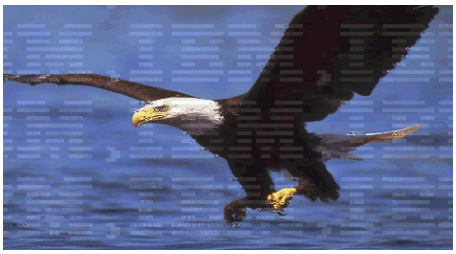



Fig 1.2: Types of Watermarks [4]

**(i) Invisible Watermark:** Watermarks that is unseen to the user and there is almost no difference between the output and input image which mean that the watermarked image is almost similar to the original image [4] Invisible watermarking is more robust to signal processing as compared to the visible one. The invisible watermark is shown in Fig 1.3 (a).

**(ii) Visible Watermark:** These Watermarks can be clearly seen by the viewers. There is difference between the output and the input image which mean that the watermarked image is not similar to the original image [4] It cannot withstand with the various attacks. The invisible watermark is shown in Fig 1.3 (b).


(a)



(b)

Fig 1.3: (a) Invisible Watermark (b) Visible Watermark [5]

**(iii) Fragile Watermark:** These watermarks are very sensitive and can be easily destroyed with very few modifications in the watermarked signal.

**(iv) Robust Watermark:** Those watermarks which cannot be easily broken as they are resilient to the various attacks and the signal processing operations.

### 1.3 Requirements of Digital Watermarking

The requirements of digital watermarking are [2, 6, 7]:-

**(i) Imperceptibility:** Transparency is the important feature of digital watermarking. Watermark should be embedded in such a way that it must not be visible to the viewers that is imperceptible so as not to cheapen the image quality [2].

**(ii) Robustness:** It is defined as "ability to detect the watermark from the watermarked image after various signal processing operations like signal enhancement, geometric image operations and noise filtering" [7]. Watermark should be robust means it must not get demolished as a result of intentional or unintentional signal processing operations or attacks like JPEG, salt and pepper attacks, speckle attacks etc.

**(iii) Security:** Another important requirement of watermark is its security. Watermark must be secret enough that it cannot be detectable by an unauthorized parties that is it must be accessible only to authorized parties [2]. This security up to a great extent is achieved by secret key which is used during embedding and extraction [6].

**(iv) Readability:** A watermark should convey as much information as possible. Extraction of the watermark is used to identify the ownership of the fingerprint.

### 1.4 Applications of Digital Watermarking

The applications of digital watermarking are [2]:-

**(i) Ownership Assertion:** Watermarks can be used for ownership assertion. Watermark signal can be embedded using the secret key in the original image and then the watermarked image can be publicized So that if anyone claims of the ownership, then the owner of the image can prove his ownership.

**(ii) Digital Fingerprinting:** It is a method to recognize the holder of the digital content [2]. Since the fingerprint if the two persons cannot be same but it seems to be same sometime. Therefore, the name of person, his age etc can be added in the form of watermark in the fingerprint so that to recognize it later it is needed.

**(iii) ID Security:** Various information like passport number, name of the person, date of birth of the person etc can be embedded in the photo that appears on the ID so that to compare it with the written text whenever it is required just by extracting the information from photo [7].

**(iv) Broadcast Monitoring:** Fragile watermark is used to verify the content whether it is really broadcasted or not which was supposed to be broadcasted.

**(v) Content Archiving:** Watermarking can be used to insert digital object identifier serial number to help archive digital contents like images, audio and video [2].

**(vi) Meta-data Insertion:** A common example of the meta-data insertion is that of Medical – rays which store patient records like patient name, age and many other relevant things [6].

**(vii) Tamper Detection:** Fragile type of watermark is used for that particular purpose in such a way that if the embedded fragile watermark is get degraded presence of tamper is indicated.

**(viii)** Watermarking technique can also be used in various purposes like source tracking, software crippling, screen casting, video authentication etc.

### 1.5 Problem Formulation

Watermarking is a technique of hiding digital data in a digital image to decrease identity theft. The objectives of this dissertation are:-

(i) To Embed the watermark in the fingerprint image using technique DCT and DWT.

(ii) To analyze the different noise attacks such as salt & pepper etc on the watermarked image.

(iii) To Compare the effect of DCT and various levels of DWT on watermarking.

### 1.6 Organisation of Thesis

(i) Chapter 2 discuss the literature survey of various papers based on the watermarking techniques.

(ii) Chapter 3 explains the various watermarking techniques available and the algorithm adopted in this work.

(iii) Chapter 4 includes the discussions and results.

(iv) Chapter 5 gives the conclusion and future scope of the work.

# CHAPTER 2
# LITERATURE REVIEW

A lot of work has been done in the past in the field of image watermarking. Review relevant literature is given below:

**Hsieh et al. [1]** introduced a multi-resolution wavelet transform in order to hide the digital watermark so that it is resistant to lossy image compression attacks .Qualified significant wavelet tree (QSWT) which is derived from the Embedded zero tree wavelet (EZW) technique is used to embed and extract the recognizable watermark into an image. QSWT includes the relationships of DWT coefficients and spatial information into consideration in the experimental set up. This method is robust to JPEG compression attacks, sharpening, blurring.

**Potdar et al. [2]** presented a survey of digital watermarking techniques. They discussed the requirements and application of digital watermarking in our day to day life. Various types of watermarks like Pseudo-Random Gaussian Sequence, Binary image or grey scale image watermarks which can be embedded and extracted are discussed. They also gave a comparison between DCT, DWT and DFT. By comparison it shows that DCT is robust to Low Pass filtering, brightness, contrast but it is resistant to various geometrical attacks like scaling, rotation and cropping on the other hand DWT is robust to JPEG, Speckle and salt & pepper attacks and DFT, since it is RST invariant, therefore it is robust to scaling, rotation and translation than DCT and DWT which is not RST invariant.

**Chouhan et al. [3,11]** introduced a Robust Digital Watermarking scheme which is based on Discrete Wavelet Transform (DWT) for fingerprint authentication. A highly uncorrelated, zero mean, two dimensional PN random sequence is generated to embed and extract the watermark. A secret seed is used to generate that PN random sequence which can be further used to extract the watermark. Various attacks like salt & pepper, speckle noise, Gaussian noise, various geometrical attacks like cropping are also performed in order to prove the robustness of the watermark. Comparison between DCT and DWT-DCT with the same algorithm is also

performed to prove that DWT is better than DCT and DWT-DCT as its fitness factor is very good.

**Song et al. [4]** introduced a various surveys in watermarking techniques. It includes the classification of various watermarks like visible, invisible etc. It talks about the spatial and transform domain. Spatial domain in which embedding in done in image pixels on the other hand in transform domain embedding done in frequency domain. It talks about various transform techniques like DWT, DCT, DFT and find that DWT is having various advantages over DCT and DFT. Four attacks like Sharpen, Histogram etc are also performed to show the results.

**Zebbich et al. [6]** introduced a new scheme to embed the watermark in the biometric images like fingerprint image. It says that every biometric image having its interested region which gives the pertinent information of the image. So, it explains the embedding of watermark in that particular interested region which will retain the concealed facts from the segmentation technique which normally discard the unusable background and interested region remains unchanged. It also provide good imperceptibility and robustness. In this Paper, the proposed scheme also upgrade the performance which gives better detection of watermark. The purposed scheme is applied to the biometric images, specially fingerprint images which is universally used biometric data. As all know, The watermarking is done in basically in either spatial domain or transform domain, transform domain gives better result, in transfer domain , various fields are common: DWT, DCT and DFT. But in this paper DFT and DWT is used which gives much better result than the existing techniques. Various attacks are also performed just to check its robustness and purposed method gives better result.

**Chopra et al. [8]** introduced basic model of watermarking technique stages and its classification. It also explains the watermarking attacks like what type of attacks to be performed on the watermarked image like simple, Detection-disabling, ambiguity attacks etc. This paper works on Spatial domain in which it used LSB technique. Watermark is embedded in the Least significant bit of the image through the watermarking technique and then extraction is done. MSE and PSNR are the parameter which is used to compare the original and the watermarked image just to show the imperceptibility. Various noises like salt and pepper noises , Gaussian noises, poison

noises are applied in the form of attacks just to show the robustness of the image. It is concluded that there is trade-off between imperceptibility and robustness in the technique.

**Lee et al. [9]** introduced a method of watermarking technique that use random mapping function.It's main focus is make watermarking technique more robust than existing LSB technique. In this paper, random coordinate of the cover image is being secured just to increase the robustness of the watermark. The result of the purposed technique shows that the quality of the watermarked image is far better than the existing LSB technique.

**Sridhar et al. [18]** introduced the compression of images using wavelet transform. It discuss about the lossy and loseless compression operation sequences and conclude that the loseless image compression techniques are having low compression ratio whereas lossy compression attacks have high compression ratio. It further tells about wavelet transform, explains its properties like multi-resolution property and also talks about its fast computation then it comes to explain the various wavelet families like Haar wavelets, Daubechies wavelets, Symlet wavelets, coiflet wavelets and bi-orthogonal wavelets. Then perform operations of wavelets on high detailed image, medium detailed images, low detailed images and color images and concludes various results like Daubechies family wavelet Db8 produced highest PSNR for medium detailed image and for color images, Bi-orthogonal family wavelet and symlet family produced better PSNR and compression ratios.

**Vatsa et al. [20]** introduced protection of fingerprint and face template using watermarking. Face template is used as watermark which is to be embed in the fingerprint and this watermarking technique includes both DWT and LSB. According to this DWT is resistant to frequency attacks and LSB based watermarking technique is resistant to geometrical attacks. So, this algorithm provides the advantages of both DWT and LSB. It perform various attacks like JPEG, Gaussian noise, Median filter, gamma etc and concludes that algorithm gives good fitness factor after the extraction of watermark. At last it also compares the results with LSB and DWT with the results obtained by the combination of both that is DWT and LSB.

**Al-Haj [21]** introduced a digital watermarking using DWT-DCT. This combination is used because DWT and DCT can compensate for the drawbacks of each other. It also explains the

DCT and DWT in a very fruitful manner. In this first, DWT is applied to the image to split it into different sub-bands, then a particular sub-band is selected then DCT is applied on that selected sub-band. Watermark is embed in that particular sub-band, then inverse DCT is again applied , then inverse DWT is applied to obtain the watermarked image. Then extraction is done by the use of correlation and watermark is extracted. Then PSNR and fitness factor is calculated to prove the imperceptibility and the robustness of the watermarking.

**Safabakhsh et al. [22]** introduced the digital watermarking on static images using frequency domain. In this, innovative based approach with the Human Visual Characteristics is used to develop the watermarking algorithm. Firstly, 3-level DWT is applied on an image to get the various sub-bands. Then, entropy based method is used to select the DWT coefficients and watermark is embedded with the help of PN sequence and HVS then inverse DWT is applied to obtain the watermarked image. At last attacks are performed and correlation is used to separate the watermark from the watermarked image. PSNR between the original and the watermarked imaged is find out to check the imperceptibility and similarity is find out between the original and the extracted watermark to check the robustness.

**Jain et al. [23]** introduced the method to hide a fingerprint in an image. In this, computation of ROC curves of many individuals is done. Eigen- face coefficients of the users face which act as watermark is used to clarify the cover fingerprint image. It is make sure that the due to the watermarking, features for the matching not get changed due to the encoding and decoding process. . As a consequence, the verification accuracy is based on decoded watermarked fingerprint images is very similar to that with original fingerprint images.

**Kim et al. [24]** introduced wavelet based digital Watermarking using level-threshold thresholding. In this, pixel value of all the sub-bands, which is achieved by applying DWT on an image, are used in order to embed the watermark in the whole image. Gaussian distribution random sequence vector is used as watermark in the paper. Level-thresholding scheme is used to select the pixel value in which watermark is embedded. Vector projection method is used to extract the watermark. PSNR values between lena image and watermarked lena image is compared and various attacks like wavelet compression attacks are performed on the watermarked image to examine the robustness of the image.

**Zebbiche et al. [25]** introduced a technique to protect the fingerprint minutiae data using in the fingerprint images using watermarking which provide security to both the data and images. In this paper, at first, conversion of minutiae data to the binary data is done then DWT is applied to an host image and compute the locations of the pixel value where watermark is to be embedded and arrange it in the decreasing order and embed the watermark in each sub-band using quantization technique. IDWT is done to get the watermarked image. Now, extraction of watermark is done by knowing the location of the pixel values where watermark was embedded. PSNR values are calculated and various attacks are performed on the image to check the robustness of the watermark.

**Alkhathami et al. [26]** introduced the technique to embed two watermark in fingerprint images. In this, two watermarks are embedded in an fingerprint image. It basically compare the minutiae points before and after embedding the watermark. First, extract the minutiae points of the fingerprint image then DCT is used to divide the fingerprint image into 8*8 blocks and then check the block where there is no minutiae points and then SHA2 is used to embed the first watermark which is unique identification number of the person. Second watermark which is gray scale image is added as second watermark in the whole image then perform inverse DCT. Then extraction of minutiae points are again of the watermarked image in order to make the comparison. Here watermarking is basically done to check whether the image is being attacked or not.

**Ganic et al. [27]** introduced the watermarking technique based on the DWT and SVD. This paper describes the classification of watermarking schemes. In this paper, DWT is applied on the image and split the image into four sub-bands and Singular Value Decomposition is applied to the each sub-band. Then apply SVD to the watermark image and combine the watermark with the original image using the modification of singular values and at last inverse DWT is done to achieve the watermarked image. Now, in order to extract the watermark, DWT is applied to the watermarked image and then SVD is applied to each band to extract the singular points thereby reconstruct the watermark. It concludes that the SVD is the better way of embedding and extracting the watermark as it is resistant to different attacks also like salt and pepper, Speckle attacks, cropping etc.

**Jabade et al. [28]** introduced an inclusive review of the watermarking techniques. It discussed the various applications of digital watermarking like copyright protection, broadcast monitoring, tamper detection etc. This paper also gave a review on various attacks and attributes like fidelity, robustness, pay load etc. It also discussed the Discrete Wavelet transform and its advantages over DCT. Various parameters to show the imperceptibility and robustness were also discussed. Different kinds of wavelet like Haar, Bi-orthogonal, Complex etc were also reviewed. Apart from that various techniques were examined like SVD, ICA, SVM, GA in this paper.

**Lu et al. [29]** introduced a technique for embedding and extracting the watermark in an image. It gave a review on the earlier vector quantization technique which is used only for the copyright security. It presented a novel multipurpose digital image watermarking method based on the multistage vector quantizer structure, which can be used for both image verification and copyright protection. In the embedding process, different techniques are used to form different VQ stages in which robust and semi-fragile watermark are embedded. Watermark is extracted accordingly. It shows that this technique gives better results than previous Vector quantization technique.

**Gunsel et al. [30]** introduced two method to embed the watermark in the fingerprint image. In the first method, various features are extracted so that to prevent the watermarking regions. Watermarking encoding and decoding techniques are used in first method. On the other hand, Second method uses a feature adaptive watermarking technique which is used before feature extraction. The difference between both of them is that in the first technique feature is extracted later while in the second case feature is extracted before. The similarity between them is that both of the techniques not require the original image to extract the watermark. It is concluded that first method is also used for colored images by using the standard deviation and gradient magnitude method and both techniques are resistant to the cropping attacks and it is also concluded that in both the cases watermark is embedded in the fingerprint images without changing the various features associated with them.

**Noore at al. [31]** introduced a technique to embed the watermark in the fingerprint image. In this paper, texture regions of the fingerprint image are selected in which watermark is embedded using the Discrete Wavelet Transform. Various texture features are extracted to embed the watermark and adjustments in that region does not affect the perceptibility of the fingerprint

image that means it maintain the imperceptibility and therefore reserved the minutiae details of the fingerprint. Automatic fingerprint identification system is used in order to determine the high matching scores which confirmed the probity of the fingerprint image. Pixel based metrics and human visual system metrics is used to determine the degree of similarity between original and extracted watermark. This technique is also resistant to various attacks.

# CHAPTER 3

# Watermarking Techniques and Adopted Algorithm

## 3.1 Various Techniques Used for Watermarking

Watermarking may be done in spatial and frequency domain. In spatial domain, Least significant bit (LSB) watermarking technique is normally used on the other side in the frequency domain, Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) is used for watermarking method. LSB watermarking technique, DWT and DCT are explained below.

### 3.1.1 LSB Watermarking Technique

It is very simple technique based on the changes of the pixel value. Each image pixel is indicated by the values ranging from 0-255 and in which MSB is the most significant bit which is the first bit to the left and LSB is the least significant bit which is the first bit to the right [8, 9, 10]. In LSB watermarking technique, Watermark is embedded in the LSB region.

Let take an example of LSB Based watermarking technique:

Image:

10100111 00110100 00011001 00111000 ...

Watermark:

0 1 1 0 ...

Watermarked Image:

10100110 00110101 00011001 00111000 ...

But this LSB based watermarking techniques are having various drawbacks like it cannot survive with various attacks [9, 37]. Due to its various disadvantages scientists shifted to transform domain in which DCT and DWT are mostly used for this technique.

### 3.1.2. DCT Based Watermarking Technique

Digital Watermarking techniques can be done in spatial and frequency domain. Previous work were concentrated on spatial domain. But now focus is shifted to frequency domain as it is more robust than in spatial domain. Frequently used frequency domain transform includes Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT) and Discrete Fourier Transform

(DFT). DCT is a fourier related transform which uses only real numbers and it is very popular because most of the compression techniques develop in DCT domain [36,38]. In DCT, Image can be easily broken into various frequency bands which make it suitable for image watermarking. It can survive against various attacks like filtering, noising etc. But due to its various disadvantages like blocking artifacts, DWT is further used to get fine results [21].

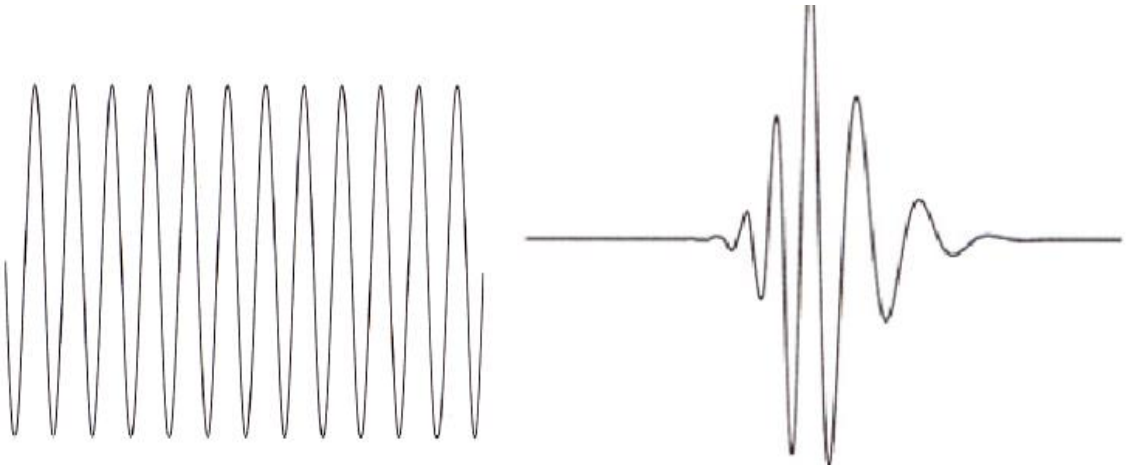
### 3.1.3. DWT based Watermarking Technique

Discrete Wavelet Transform is mostly used due to its various advantages like it has multi resolution characteristics, gives better compression ratio [11]. Therefore, both DCT and wavelet based digital watermarking is used in this project, just to prove that DWT give better result. Parameters like peak signal to noise ratio, fitness factor, average elapsed time for embedding and extraction are being compared by applying discreet cosine transform and discrete wavelet transform. In this dissertation English alphabet as a watermark has been used but any static image can be used in the fingerprint image for authentication purpose..

## 3.2 Introduction to Wavelets

A wave is a repeatedly vibration which is generated by the energy transfer. On the contrary, wavelets are the isolated waves whose energy is condensed in space or time and are best fitted for temporary or transient signals. Wavelets can also be defined as the mathematical functions that break the message to various distinct frequency components so that to study each component separately with a resolution matched to its scale [14]. The basic idea to use wavelet is that to examine the data with the scale. Wavelets also satisfy certain mathematical demands. Now, It depend on the what kind of window we are using like if we use large window then large features can be seen on the other hand if we use small window then small features can be examined. So it makes to all kind of features we want which make them interesting [12].

Now, wavelets technique adopted a wavelet prototype function which is defined as mother wavelet. Very tighten, narrow, high-frequency category of the prototype is used for the temporal analysis on the other hand enlarge, widen, low-frequency category of the prototype is used for the frequency analysis. Wavelets are widely used in various functions like to remove the noise, to enhance the image etc [13,14].`Fig 3.1 shows the demonstration of wave.



(a) (b)

Fig 3.1: Demonstration of (a) a wave (b) a wavelet

### 3.2.1 Wavelet Families

Mother Wavelet is used for transformation of waves and for this mother wavelet needs some basic function. Mother wavelet is responsible for the features of the wavelet transform as it is the only one which develops the all wavelet function. Therefore, choice of mother wavelet is very important and it must be chosen according to the requirements. Various type of wavelet functions like Haar, Daubechies, Coiflet, Symlet are available and Haar is the oldest one therefore any introduction starts from Haar otherwise Daubechies is widely used and also called Maxflat wavelet [40]. Fig 3.2 shows the various wavelet functions which are widely used in the image watermarking techniques and other methods. In this project, all the wavelets like Haar, Daubechies, Coiflet, symlet was applied on the developed technique just to check the difference obtained in the results [41]. In this work, after applying the various wavelets, it is concluded that it doesnot make a large effect to choose different wavelets as it gives approximately the same result. Keeping eye on this research, Haar wavelet is the finally applied in the proposed technique just because of the reason that it is simple and widely used and take less time in comparison to all others mother wavelet functions. All the wavelets are explained in the next page in detail.

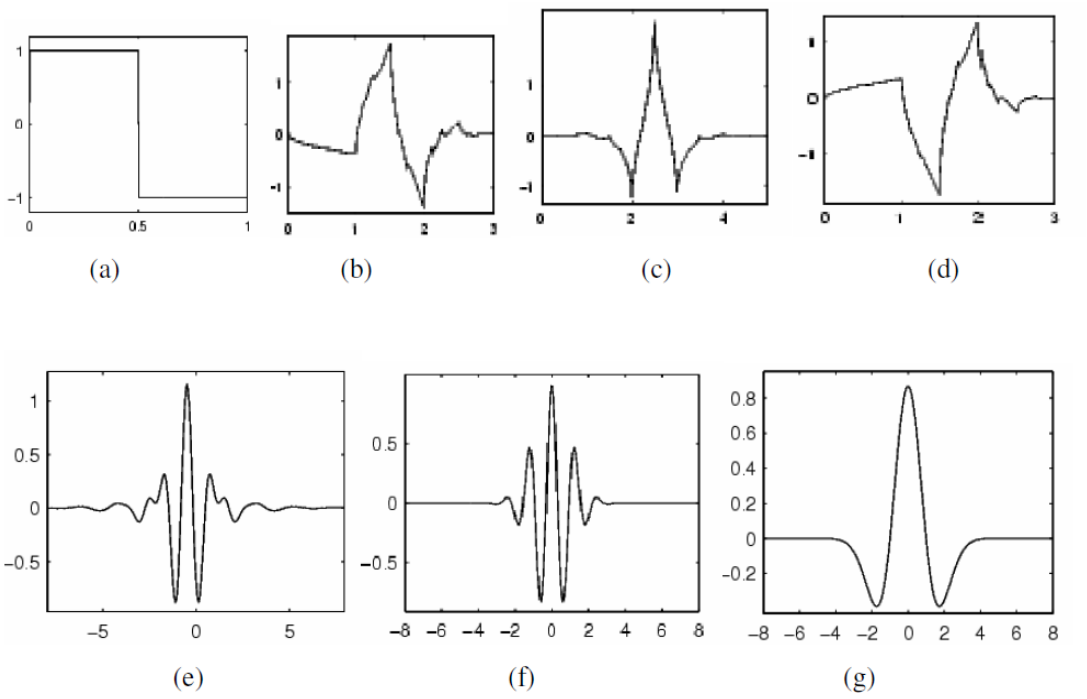



Fig 3.2: Wavelet families (a) Haar (b) Daubechies4 (c) Coiflet1 (d) Symlet2 (e) Meyer (f) Morlet (g) Mexican Hat [42].

### (i) Haar wavelet

It is used as it is fast, simple, memory efficient and having the ability to reconstruct the signal perfectly. Haar matrix proposed in 1909 by Alfred haar which is the simplest possible wavelet and very fast transform. It is a sequence of rescaled "square shaped" functions which together form wavelet families [11]. Haar wavelet function and scalinf function is described mathematically in th next page which gives the idea that how haar wavelet works.

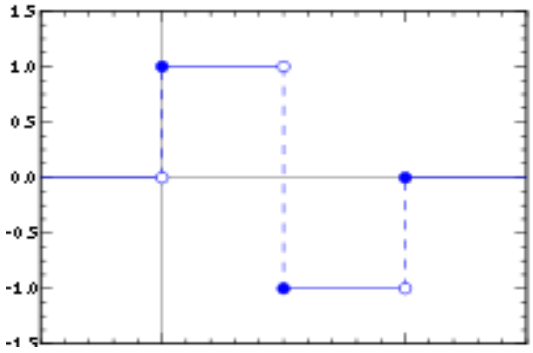


Fig 3.3: The Haar wavelet [11]

The Haar wavelet's mother wavelet function $\psi(t)$ can be described as [11]:

$$\psi(t) = \begin{cases} 1 & 0 \le t < 1/2, \\ -1 & 1/2 \le t < 1, \\ 0 & otherwise \end{cases} \quad (2.1)$$

Its scaling function $\phi(t)$ can be defined as [11]:

$$\phi(t) = \begin{cases} 1 & 0 \le t < 1, \\ 0 & otherwise \end{cases} \quad (2.2)$$

**(ii) Daubechies wavelet**

It is having the four wavelet and scaling function. The scaling coefficients are [15] :

$$H0 = 1 + \sqrt{3}/4\sqrt{2} \quad (2.3)$$

$$H1 = 3 + \sqrt{3}/4\sqrt{2} \quad (2.4)$$

$$H2 = 3 - \sqrt{3}/4\sqrt{2} \quad (2.5)$$

$$H3 = 1 - \sqrt{3}/4\sqrt{2} \quad (2.6)$$

Scaling function is applied to the incoming data. If the real data is having M values then scaling function is given the wavelet transform step in order to determine the M/2 flat values.

The wavelet function coefficients are given as [15]:

$$G0 = H3 \quad (2.7)$$

$$G1 = -H2 \quad (2.8)$$

$$G2 = H1 \quad (2.9)$$

$$G3 = -H0 \quad (2.10)$$

The Scaling function is calculated as [15]:

$$p[i] = H0s[2i] + H1s[2i+1] + H2s[2i+2] + H3s[2i+3] \quad (2.11)$$

The Wavelet function is calculated as [15]:

$$d[i] = G0s[i] + G1s[2i+1] + G2s[2i+2] + G3s[2i+1] \quad (2.12)$$

Scaling and wavelet function value is to be calculates at each and every step. Therefore its index will get increased by two at every step and other values are generated for the further calculations.

In case of forward transform, I will be increases upto n-2 and same in the case of inverse transform [15].In this there is edge problem arises which is to be solved and it can be solved various methods like Zeros can be used to fill the blank space but then one problem arise that it can generate the significant error doe to the extra zeros produced in it. Now other method to reduce that problem is to assume that it is mirrored at the corners. The next way to reduce is Gram-Schmidt orthogonalization which will determine the scaling and wavelet function which is to applied at the corners.

**(iii) Coiflet Wavelet**

It is designed such that they are having scaling functions with vanishing moments. It is symmetric in nature as it is having N/3-1 and wavelet functions having N/3 moments. It is having various properties like symmetric, orthogonal, bi orthogonal. It is to supposed that in coiflet wavelet both scaling and wavelet functions are to be normalized by $1/\sqrt{2}$. The mathematical equation is given by [16]:

$$B_k = (-1)^k C_{N-1-k} \tag{2.13}$$

Where,

K=coefficient index

B=wavelet coefficient

C=scaling coefficient

N=wavelet index

**(iv) Symlet wavelet**

These are also a part of wavelet families and it is just the extended version of Daubechies wavelet. It is also having various properties like it is symmetris, orthogonal.

**(v) Meyer Wavelet**

It is part of wavelet families having orthogonal properties or u can say that it is an orthogonal wavelet and its wavelet and scaling function is defined below.

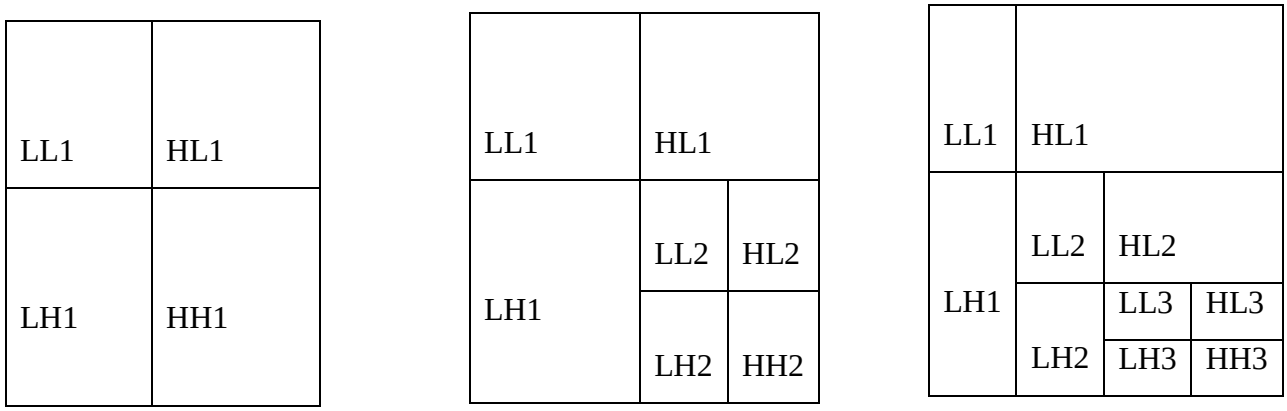
$$\mu(w)=\begin{cases} \frac{1}{\sqrt{2\pi}}\sin\left(\frac{\pi}{2}v\left(\frac{3|w|}{2\pi}-1\right)\right)e^{\frac{jw}{2}} & if\ \frac{2\pi}{3}<|w|<\frac{4\pi}{3} \\ \frac{1}{\sqrt{2\pi}}\cos\left(\frac{\pi}{2}v\left(\frac{3|w|}{2\pi}-1\right)\right)e^{\frac{jw}{2}} & if\ \frac{4\pi}{3}<|w|<\frac{8\pi/3}{3} \\ 0 & otherwise \end{cases} \tag{2.14}$$

$$V(x)= \begin{cases} 0 \ if \ x < 0, \\ x \ if \ 0 < x < 1, \\ 1 \ if \ x > 1 \end{cases} \quad (2.15)$$

After studying various wavelets like Daubechies, Symlet, Coiflet, Haar, Mexican Hat etc it is to be examined that haar wavelet is very simple and very easy to use and far away from various critical problems therefore keeping eye on all this, in this project haar wavelet is used in our algorithm.

**3.3 Discrete Wavelet Transform**

Wavelet Transform, gives a time-frequency description of the signal, is a advanced approach commonly used in de-noising, compression, watermarking etc. Discrete Wavelet Transform, based on pyramidal coding, is a type of wavelet transform which requires less computation time and resource [3]. DWT basically decompose the image into three spatial direction i.e. horizontal, vertical, diagonal which shows that it shows the anisotropic property of the HVS more precisely. In DWT, various digital filtering approaches like low pass and high pass filtering is successively used to split the signal into various bands as shown in the Fig 3.4 [18] LL1, HL1, LH1, HH1 are the four sub-bands, obtained by applying 1-level DWT Transform. The LL1/LH1/HL1/HH1 band can be further split in the same manner, which produce more sub-bands [21]. This can be extended to 2nd level, 3rd level which results for the DWT transform. Sub-bands obtained by high pass filtering gives detailed information and its magnitude is small on the other hand sub-bands obtained by low pass filtering produce coarse approximations and its magnitude is very large.




1st level DWT 2nd level DWT 3rd level DWT



Fig 3.4: Different levels of DWT transform [17]

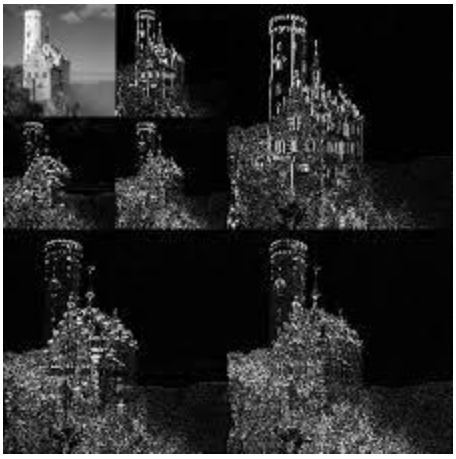


Fig 3.5: The three layer decomposition of the image [9]

The image shown in Fig 3.5 is a pyramid which firstly decompose into 1 level DWT which separates the high and low level frequencies of the images then it further decompose one of its levels (LL/HL/LH/HH) to 2 level DWT which again separates its low and high frequency present in that particular level. After 2 level, 3 level DWT is applied to further separate the low and high frequency components.

DWT can be expressed mathematically as [18]:

$$Y_{high}[k]=\sum_n x[n].h[2k-n] \quad (2.3)$$

$$Y_{low}[k]=\sum_n x[n].g[2k-n] \quad (2.4)$$

Where, x is the original signal passed through the series of filters with an impulse response.

### 3.3.1 Advantages of DWT OVER DCT

The advantages of DWT over DCT are [21,24]:

(i) It avoid blocking phenomenon as it doesn't require division of input coding into blocks.

(ii) It provide good localization in both domains.

(iii) DWT introduces inherent scaling.

(v) DWT have higher decorrelation and energy compression efficiency.

(vi) Less information lost in DWT of Original Image than DCT.

(vii) Temporal and spectral properties of audio, video signals may also be examined with the help of DWT. It is based on wavelets whose frequency is varied and timing is limited on the other hand this in not possible in DCT.

### 3.4 Watermark Embedding and Extraction Algorithm

The embedding and extraction of watermark has been explained in section 3.4.1 and 3.4.2.

#### 3.4.1 Embedding Algorithm

Text image used as watermark is embedded in fingerprint image. Secret key is used to generate random sequence of the size of sub-band (HL/LH) which is added to the original sub-band in order to generate the new sub-band which is shown in the block diagram is Fig 3.6.

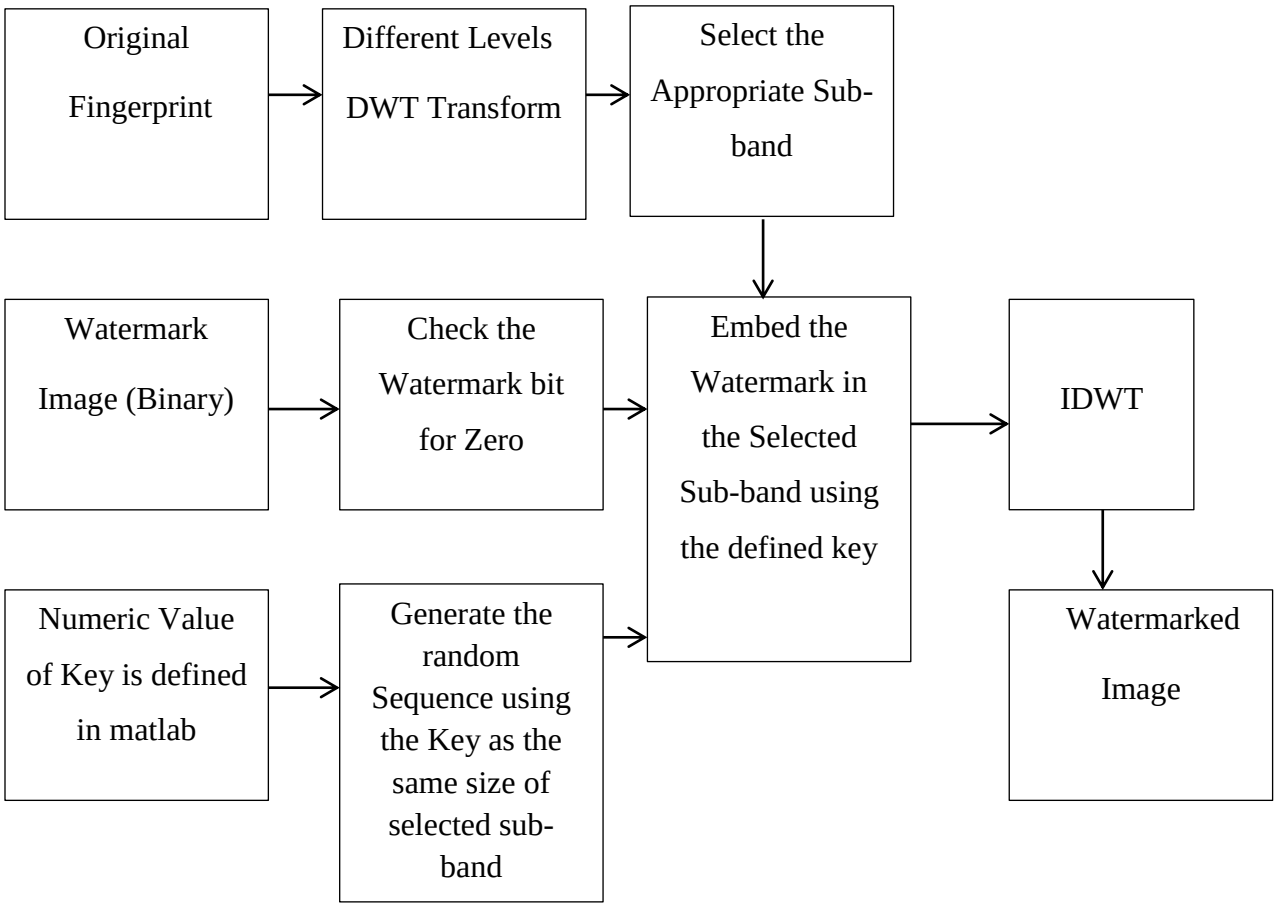



Fig 3.6: Watermark Embedding Block Diagram

**Algorithm:-**

**Step 1:** Transform the original image using either1-level, 2-level or 3-level DWT transform. Select the HL1 and LH1 bands in case of 1-level DWT transform and HL2 &LH2 in case of 2-level DWT transform and similarly in case of 3-level .

**Step 2:** Two dimensional random sequence is generated of the size selected sub-bands (HL1/HL2/HL3) and (LH1/LH2/LH3) using the appropriate key in order to embed the watermark in the original image.

**Step 3:** If watermark bit=0, embed the random sequence in the select sub-bands (HL1/HL2/HL3) and (LH1/LH2/LH3) with the watermark amplification factor k.

If Watermark bit=0,

(HL1/HL2/HL3) = (HL1/HL2/HL3) + k*Rn1; Rn1 and Rn2 are the generated random

(LH1/LH2/LH3) = (LH1/LH2/LH3) + k*Rn2; sequence for HL&LH.

Else,

(HL1/HL2/HL3) = (HL1/HL2/HL3) ;

(LH1/LH2/LH3) = (LH1/LH2/LH3) ;

**Step 4:** Perform the IDWT to obtain the watermarked image.

## 3.4.2 Extraction Algorithm

Secret key used in the embedding of watermark, is further used to extract the watermark from the watermarked image. Various noises in the form of attacks are also applied on the watermarked image in order to check the robustness. Complete algorithm of extraction of watermark is discussed in the next page. This extraction algorithm gives better results for DWT than DCT and in DWT, 1$^{st}$ level result gives more accuracy that means it extract the watermark in a proper manner that it was embedded in the embedding algorithm on the other hand watermark strength get reduced as we goes to the 2$^{nd}$ and the 3$^{rd}$ level. Algorithm is shown in Fig 3.7.

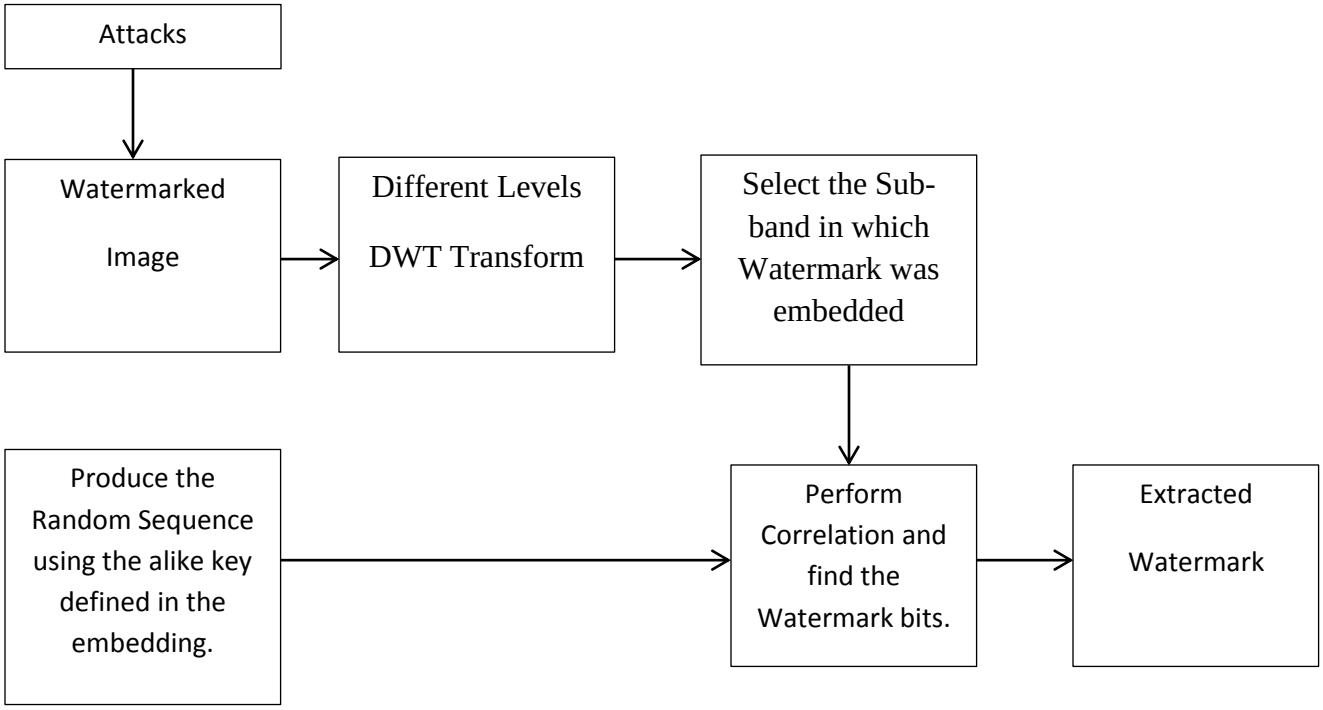



Fig 3.7: Watermark Extraction Block Diagram

## Algorithm:-

**Step 1:** Apply either1-level, 2-level or 3-level DWT transform on the attacked watermarked image depending upon level selected while embedding. Attacks like Salt & pepper, Speckle can be performed .

**Step 2:** Two dimensional Random sequence of the size of the selected sub bands(HL1/HL2/HL3) and (LH1/LH2/LH3) is generated using the identical key that was utilized in the embedding process and also select the watermarked sub bands (HL1/HL2/HL3) or (LH1/LH2/LH3) in which watermark is embedded.

**Step 3:** Calculate the similarity between generated random sequences and the selected sub band using the Correlation function.

**Step 4:** Calculate the mean correlation and compare each correlation value with the mean correlation.

If correlation value > mean(correlation)

Watermark bit=0;

Else

Watermark bit=1;

This process continues till all of the bits are recovered.

# CHAPTER 4

# RESULTS AND DISCUSSIONS

## 4.1 Performance Parameters

Parameter such as peak signal to noise ratio is used to compare the original and watermarked image and Fitness of Recovery has been used for comparison between original and extracted watermark.

**4.1.1 Peak Signal to Noise Ratio (PSNR):-** It is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. It is expressed in terms of logarithmic decibel scale.

MSE = (1/(J*K))*sum(sum((Y-Z).^2))

PSNR = 20*log(max(max(Y)))/((MSE)^0.5)

Where,

MSE=Mean Square error

J and K are the size of original fingerprint image

Y is the original fingerprint image and,

Z is the watermarked image.

**4.1.2 Fitness of recovery:-** 100*Correlation factor

Where, Correlation factor is the correlation between the original and the extracted watermark.

## 4.2 RESULTS

This section explains the results obtained by applying the algorithm on thirty sample images

Various fingerprint images (thirty in total) of different persons with specifications 8-bit depth and size 296×560 pixels at 1 dpi and watermark of size 38 × 31 are taken to apply the algorithm. Fig 4.1 (a) shows the sample watermark image and Fig 4.1 (b) shows sample fingerprint images. Further, results of embedding the watermark in fingerprint image in the form of watermarked images and extracted watermark images are shown in the results. Apart from the images, Result section also contained the tables which include the comparison results of PSNR, fitness factor, average elapsed time for embedding and extraction with DCT and various levels of DWT.

(a)

| | | | | |
|---|---|---|---|---|
|  Image 1 |  Image 2 |  Image 3 |  Image 4 |  Image 5 |
|  Image 6 |  Image 7 |  Image 8 |  Image 9 |  Image 10 |

| | | | | |
|---|---|---|---|---|
|  Image 11 |  Image 12 |  Image 13 |  Image 14 |  Image 15 |
|  Image 16 |  Image 17 |  Image 18 |  Image 19 |  Image 20 |
|  Image 21 |  Image 22 |  Image 23 |  Image 24 |  Image 25 |

| | | | | |
|---|---|---|---|---|
|  |  |  |  |  |
| Image 26 | Image 27 | Image 28 | Image 29 | Image 30 |

(b)

Fig 4.1: (a) Watermark image of size (38×31) pixels (b) Original fingerprints (296×560) pixels

Fig 4.2 shows the watermarked images with corresponding PSNR for DCT, 1st level DWT, 2nd level DWT and 3rd level DWT for image 1.

| DCT | 1st level DWT | 2nd level DWT | 3rd level DWT |
|---|---|---|---|
|  |  |  |  |
| PSNR=14.0193 | PSNR=15.3961 | PSNR=22.8467 | PSNR=26.9982 |

Fig 4.2: Watermarked images with corresponding PSNR for DCT and different levels of DWT for image 1

Fig 4.3 shows the extracted watermarks (without attacks) with corresponding fitness of recovery for DCT, 1st level DWT, 2nd level DWT, 3rd level DWT for image 1.

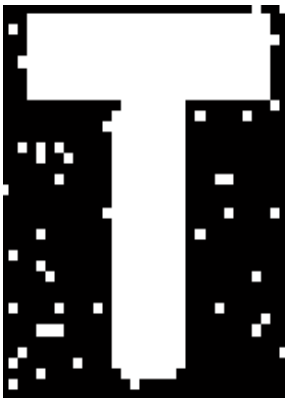
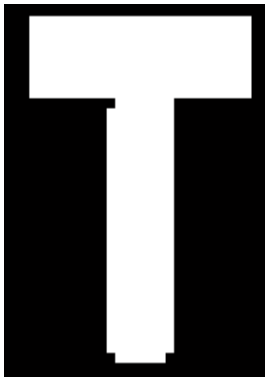
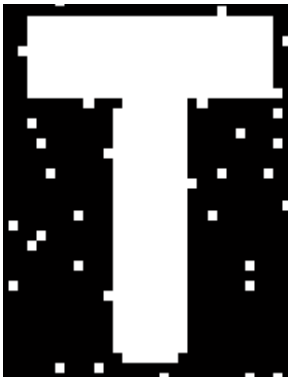
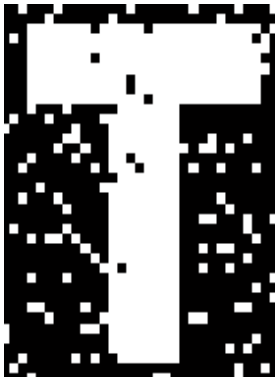
| DCT | 1st level DWT | 2nd level DWT | 3rd level DWT |
|---|---|---|---|
|  |  |  |  |
| Fitness factor=92.289 | Fitness factor=100 | Fitness factor=94.130 | Fitness factor=81.601 |

Fig 4.3: Extracted Watermarks (Without Attacks) with corresponding Fitness of Recovery for DCT and different DWT levels for image 1

Fig 4.4 shows the watermarked images with corresponding PSNR for DCT, 1st level DWT, 2nd level DWT and 3rd level DWT for image 2.

| DCT | 1st level DWT | 2nd level DWT | 3rd level DWT |
|---|---|---|---|
|  |  |  |  |
| PSNR=14.8357 | PSNR=16.1333 | PSNR=23.2899 | PSNR=27.4144 |

Fig 4.4: Watermarked images with corresponding PSNR for DCT and different levels of DWT for image 2

Fig 4.5 shows the extracted watermarks (without attacks) with corresponding fitness of recovery for DCT, 1st level DWT, 2nd level DWT, 3rd level DWT for image 2.

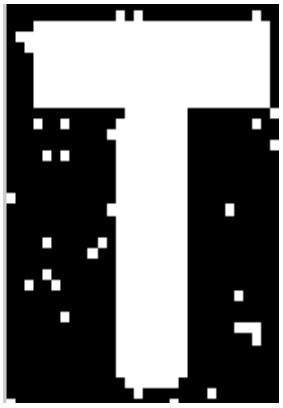
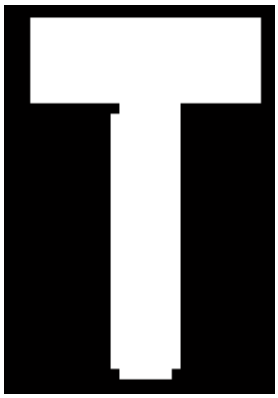
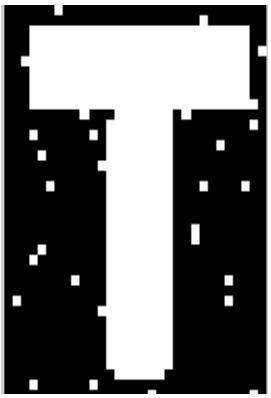
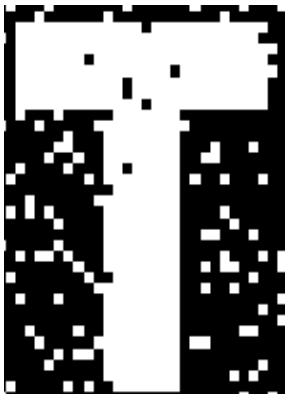
| DCT | 1st level DWT | 2nd level DWT | 3rd level DWT |
|---|---|---|---|
|  |  |  |  |
| Fitness factor=93.623 | Fitness factor=100 | Fitness factor=94.813 | Fitness factor=81.519 |

Fig 4.5: Extracted Watermarks (Without Attacks) with corresponding Fitness of Recovery for DCT and different DWT levels for image 2

Fig 4.6 shows the watermarked images with corresponding PSNR for DCT, 1st level DWT, 2nd level DWT and 3rd level DWT for image 3.

| DCT | 1st level DWT | 2nd level DWT | 3rd level DWT |
|---|---|---|---|
|  |  |  |  |
| PSNR= 15.2468 | PSNR=16.3889 | PSNR=23.5034 | PSNR=27.654 |

Fig 4.6: Watermarked images with corresponding PSNR for DCT and different levels of DWT for image 3

Fig 4.7 shows the extracted watermarks (without attacks) with corresponding fitness of recovery for DCT, 1st level DWT, 2nd level DWT, 3rd level DWT for image 3.

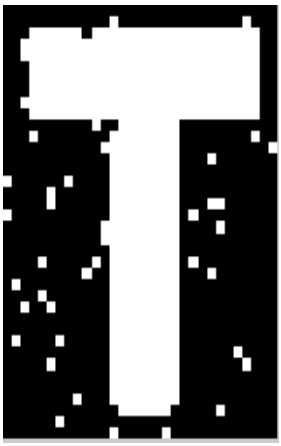
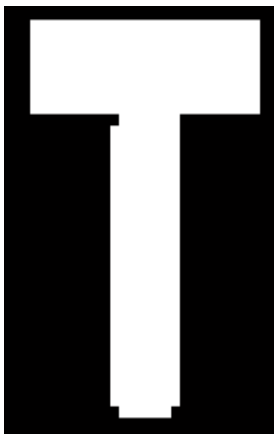
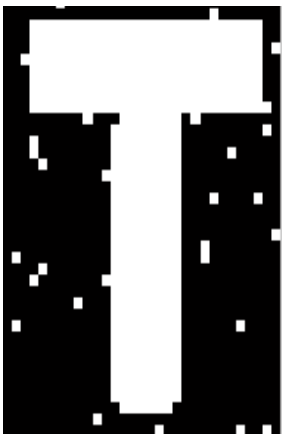
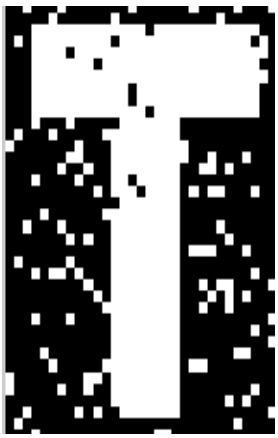
| DCT | 1st level DWT | 2nd level DWT | 3rd level DWT |
|---|---|---|---|
|  |  |  |  |
| Fitness factor=92.587 | Fitness factor=100 | Fitness factor=94.813 | Fitness factor=81.306 |

Fig 4.7: Extracted watermarks (without attacks) with corresponding Fitness of recovery for DCT and different DWT levels for image 3

Fig 4.8 shows the watermarked images with corresponding PSNR for DCT, 1st level DWT, 2nd level DWT and 3rd level DWT for image 4.

| DCT | 1st level DWT | 2nd level DWT | 3rd level DWT |
|---|---|---|---|
|  |  |  |  |
| PSNR= 14.2208 | PSNR=16.3100 | PSNR=23.1153 | PSNR=27.2668 |

Fig 4.8: Watermarked images with corresponding PSNR for DCT and different levels of DWT for image 4

Fig 4.9 shows the extracted watermarks (without attacks) with corresponding fitness of recovery for DCT, 1st level DWT, 2nd level DWT, 3rd level DWT for image 4.

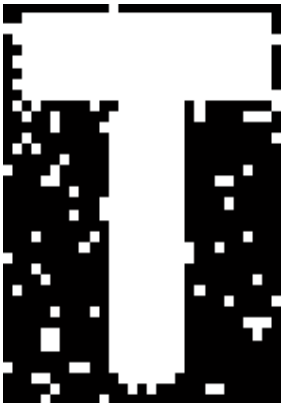
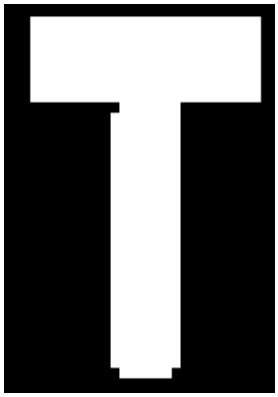
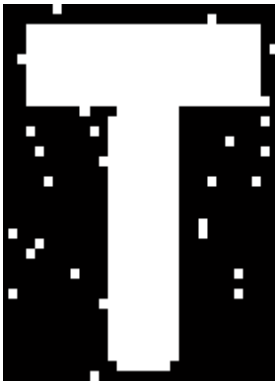
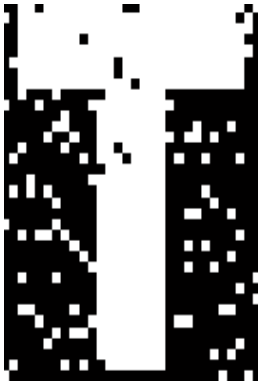
| DCT | 1st level DWT | 2nd level DWT | 3rd level DWT |
|---|---|---|---|
|  |  |  |  |
| Fitness factor=86.308 | Fitness factor=100 | Fitness factor=94.642 | Fitness factor=81.453 |

Fig 4.9: Extracted watermarks (without attacks) with corresponding Fitness of recovery for DCT and different DWT levels for image 4

Fig 4.10 shows the watermarked images with corresponding PSNR for DCT, 1st level DWT, 2nd level DWT and 3rd level DWT for image 5.

| DCT | 1st level DWT | 2nd level DWT | 3rd level DWT |
|---|---|---|---|
|  |  |  |  |
| PSNR= 15.6767 | PSNR=16.3798 | PSNR=23.8748 | PSNR=28.0263 |

Fig 4.10: Watermarked images with corresponding PSNR for DCT and different levels of DWT for image 5

Fig 4.11 shows the extracted watermarks (without attacks) with corresponding fitness of recovery for DCT, 1st level DWT, 2nd level DWT, 3rd level DWT for image 5.

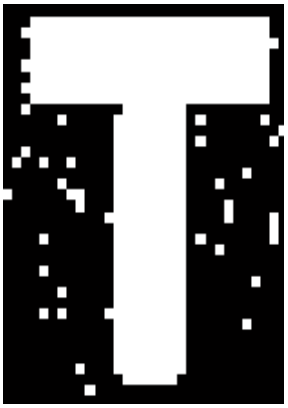
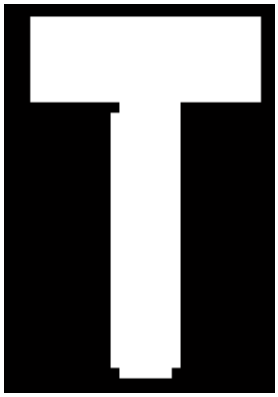
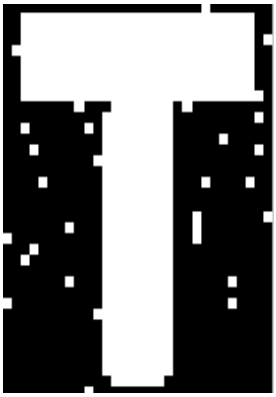
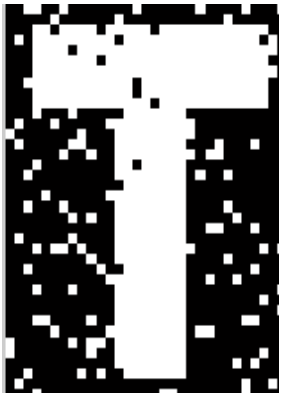
| DCT | 1st level DWT | 2nd level DWT | 3rd level DWT |
|---|---|---|---|
|  |  |  |  |
| Fitness factor=92.953 | Fitness factor=100 | Fitness factor=93.961 | Fitness factor=80.881 |

Fig 4.11: Extracted watermarks (without attacks) with corresponding Fitness of recovery for DCT and different DWT levels for image 5

Fig 4.12 shows the watermarked images with corresponding PSNR for DCT, 1st level DWT, 2nd level DWT and 3rd level DWT for image 6.

| DCT | 1st level DWT | 2nd level DWT | 3rd level DWT |
|---|---|---|---|
|  |  |  |  |
| PSNR= 14.3864 | PSNR=16.2616 | PSNR=23.2466 | PSNR=27.3981 |

Fig 4.12: Watermarked images with corresponding PSNR for DCT and different levels of DWT for image 6

Fig 4.13 shows the extracted watermarks (without attacks) with corresponding fitness of recovery for DCT, 1st level DWT, 2nd level DWT, 3rd level DWT for image 6.

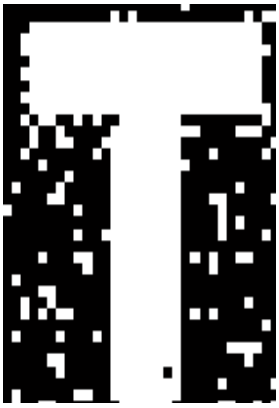
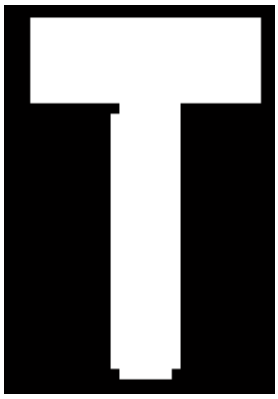
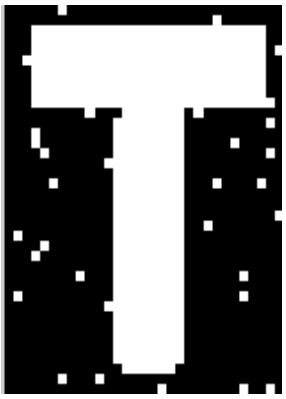
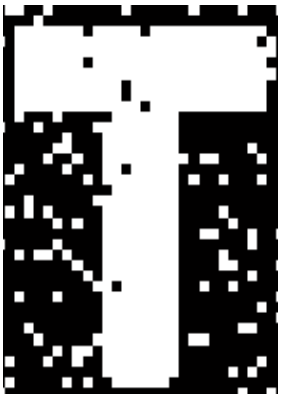
| DCT | 1st level DWT | 2nd level DWT | 3rd level DWT |
|---|---|---|---|
|  |  |  |  |
| Fitness factor=81.868 | Fitness factor=100 | Fitness factor=94.301 | Fitness factor=81.813 |

Fig 4.13: Extracted watermarks (without attacks) with corresponding Fitness of recovery for DCT and different DWT levels for image 6

Fig 4.14 shows the watermarked images with corresponding PSNR for DCT, 1st level DWT, 2nd level DWT and 3rd level DWT for image 7.

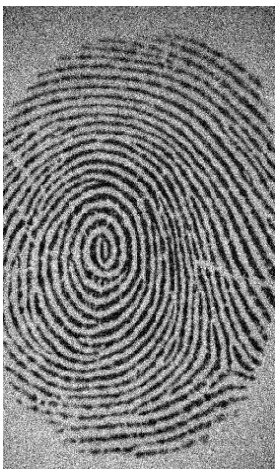
| DCT | 1st level DWT | 2nd level DWT | 3rd level DWT |
|---|---|---|---|
|  |  |  |  |
| PSNR= 14.4233 | PSNR=15.1158 | PSNR=23.1593 | PSNR=27.3018 |

Fig 4.14: Watermarked images with corresponding PSNR for DCT and different levels of DWT for image 7

Fig 4.15 shows the extracted watermarks (without attacks) with corresponding fitness of recovery for DCT, 1st level DWT, 2nd level DWT, 3rd level DWT for image 7

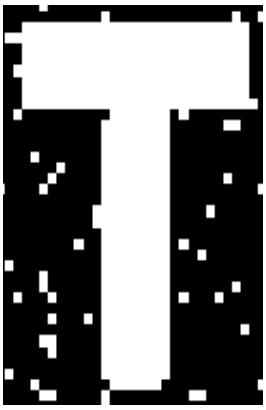
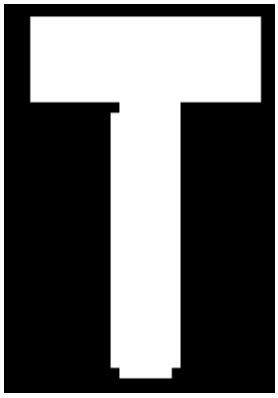
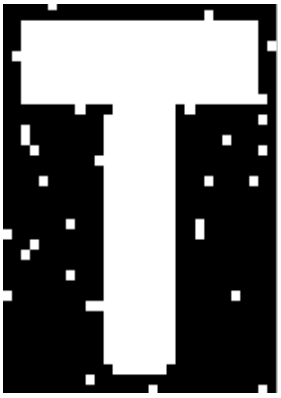
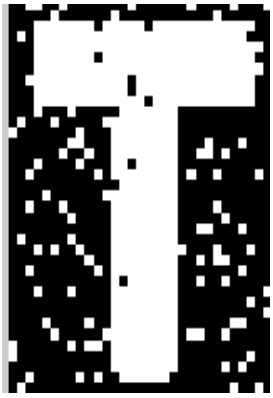
| DCT | 1st level DWT | 2nd level DWT | 3rd level DWT |
|---|---|---|---|
|  |  |  |  |
| Fitness factor=91.633 | Fitness factor=100 | Fitness factor=94.471 | Fitness factor=81.813 |

Fig 4.15: Extracted watermarks (without attacks) with corresponding Fitness of recovery for DCT and different DWT levels for image 7

Fig 4.16 shows the watermarked images with corresponding PSNR for DCT, 1st level DWT, 2nd level DWT and 3rd level DWT for image 8.

| DCT | 1st level DWT | 2nd level DWT | 3rd level DWT |
|---|---|---|---|
|  |  |  |  |
| PSNR= 14.2639 | PSNR=16.1889 | PSNR=23.1593 | PSNR=27.3103 |

Fig 4.16: Watermarked images with corresponding PSNR for DCT and different levels of DWT for image 8

Fig 4.17 shows the extracted watermarks (without attacks) with corresponding fitness of recovery for DCT, 1st level DWT, 2nd level DWT, 3rd level DWT for image 8.

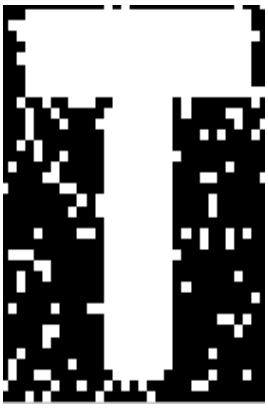
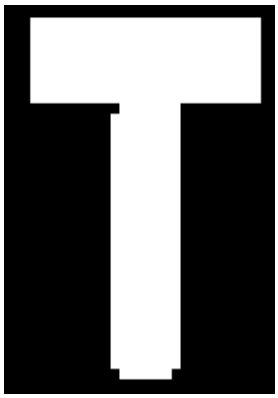
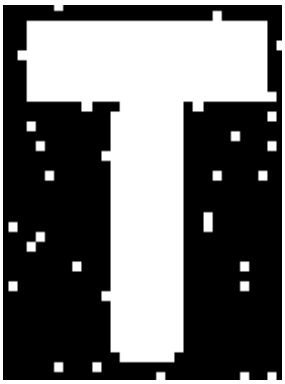
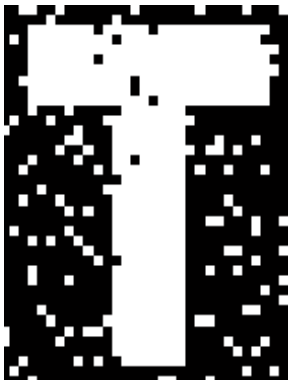
| DCT | 1st level DWT | 2nd level DWT | 3rd level DWT |
|---|---|---|---|
|  |  |  |  |
| Fitness factor=82.510 | Fitness factor=100 | Fitness factor=94.471 | Fitness factor=81.601 |

Fig 4.17: Extracted watermarks (without attacks) with corresponding Fitness of recovery for DCT and different DWT levels for image 8

Fig 4.18 shows the watermarked images with corresponding PSNR for DCT, 1st level DWT, 2nd level DWT and 3rd level DWT for image 9.

| DCT | 1st level DWT | 2nd level DWT | 3rd level DWT |
|---|---|---|---|
|  |  |  |  |
| PSNR= 14.9362 | PSNR=16.5810 | PSNR=23.5873 | PSNR=27.7388 |

Fig 4.18: Watermarked images with corresponding PSNR for DCT and different levels of DWT for image 9

Fig 4.19 shows the extracted watermarks (without attacks) with corresponding fitness of recovery for DCT, 1st level DWT, 2nd level DWT, 3rd level DWT for image 9.

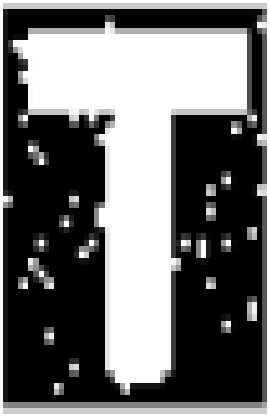
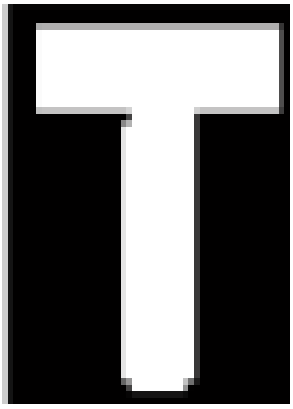
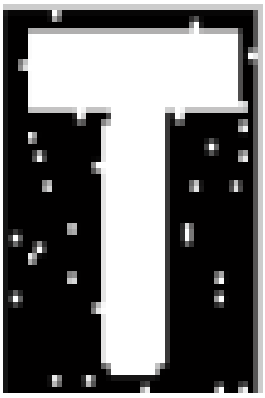
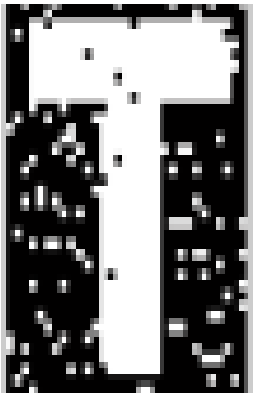
| DCT | 1st level DWT | 2nd level DWT | 3rd level DWT |
|---|---|---|---|
|  |  |  |  |
| Fitness factor=92.125 | Fitness factor=100 | Fitness factor=94.301 | Fitness factor=82.617 |

Fig 4.19: Extracted watermarks (without attacks) with corresponding Fitness of recovery for DCT and different DWT levels for image 9

Fig 4.20 shows the watermarked images with corresponding PSNR for DCT, 1st level DWT, 2nd level DWT and 3rd level DWT for image 10.

| DCT | 1st level DWT | 2nd level DWT | 3rd level DWT |
|---|---|---|---|
|  |  |  |  |
| PSNR= 15.1374 | PSNR=16.9821 | PSNR=23.7527 | PSNR=27.9042 |

Fig 4.20: Watermarked images with corresponding PSNR for DCT and different levels of DWT for image 10

Similarly, the algorithm is applied to all the sample images and comparison between DCT and various levels of DWT with corresponding PSNR and fitness factor have been made and is given in Table 1.

Table 1: Comparison of PSNR values and Fitness factor (without attacks) for all sample images

| Image No. | PSNR (db) | | | | Fitness Factor | | | |
|---|---|---|---|---|---|---|---|---|
| | DCT | DWT | | | DCT | DWT | | |
| | | 1st level | 2nd level | 3rdlevel | | 1st level | 2nd level | 3rd level |
| 1. | 14.0193 | 15.3961 | 22.8467 | 26.9982 | 92.2894 | 100 | 94.1309 | 81.6012 |
| 2. | 14.8357 | 16.1333 | 23.2899 | 27.4414 | 93.6235 | 100 | 94.8139 | 81.5195 |
| 3. | 15.2468 | 16.3889 | 23.5034 | 27.6549 | 92.5875 | 100 | 94.8139 | 81.3066 |
| 4. | 14.2208 | 16.3100 | 23.1153 | 27.2668 | 86.3082 | 100 | 94.6425 | 81.4538 |
| 5. | 15.6767 | 16.3798 | 23.8748 | 28.0263 | 92.9532 | 100 | 93.9613 | 80.8813 |
| 6. | 14.3864 | 16.2616 | 23.2466 | 27.3981 | 81.8689 | 100 | 94.3010 | 81.8136 |
| 7. | 14.4233 | 15.1158 | 23.1593 | 27.3108 | 91.6333 | 100 | 94.4715 | 81.8136 |
| 8. | 14.2639 | 16.1889 | 23.1593 | 27.3108 | 82.5103 | 100 | 94.4715 | 81.6012 |
| 9. | 14.9362 | 16.5810 | 23.5873 | 27.7388 | 92.1251 | 100 | 94.3010 | 82.6174 |
| 10. | 15.1374 | 16.9821 | 23.7527 | 27.9042 | 89.7033 | 100 | 94.6425 | 82.7660 |
| 11. | 14.5048 | 16.6718 | 23.2899 | 27.4414 | 86.4587 | 100 | 94.4715 | 82.1943 |
| 12. | 14.0412 | 16.0301 | 22.8920 | 27.0435 | 84.3153 | 100 | 94.6425 | 82.4058 |
| 13. | 14.4604 | 16.8408 | 23.0267 | 27.1782 | 89.7033 | 100 | 94.3010 | 82.3211 |
| 14. | 13.6970 | 15.5238 | 22.6163 | 26.7678 | 88.7596 | 100 | 94.8139 | 82.5547 |
| 15. | 14.1114 | 16.0081 | 22.8920 | 27.0435 | 90.8221 | 100 | 94.4715 | 82.7039 |
| 16. | 14.3305 | 16.6521 | 23.2031 | 27.3546 | 84.5282 | 100 | 94.8139 | 82.7927 |
| 17. | 14.2360 | 15.3674 | 23.0267 | 27.1782 | 92.4550 | 100 | 94.3010 | 81.8971 |
| 18. | 14.3694 | 15.3679 | 23.1593 | 27.3108 | 86.7609 | 100 | 94.4715 | 81.0939 |
| 19. | 14.1607 | 15.7563 | 23.0267 | 27.1782 | 84.9687 | 100 | 94.1309 | 80.7341 |
| 20. | 14.2451 | 15.5762 | 22.9821 | 27.1336 | 92.7867 | 100 | 94.4715 | 79.8571 |
| 21. | 14.1104 | 15.5643 | 22.8011 | 26.9526 | 93.9613 | 100 | 95.1582 | 81.8136 |
| 22. | 15.3763 | 16.4926 | 24.1139 | 28.2654 | 89.9450 | 100 | 94.3010 | 81.1768 |
| 23. | 14.1956 | 16.0533 | 23.0711 | 27.2226 | 90.1804 | 100 | 94.4715 | 81.0939 |
| 24. | 14.7483 | 15.9674 | 23.7893 | 27.4569 | 89.3404 | 100 | 94.7485 | 87.2485 |
| 25. | 15.0851 | 15.8136 | 22.7845 | 27.8456 | 94.9858 | 100 | 94.2345 | 81.4196 |
| 26. | 14.4513 | 16.6480 | 24.6536 | 27.1234 | 89.7033 | 100 | 97.1245 | 81.0654 |
| 27. | 14.3065 | 16.3499 | 21.7485 | 27.4569 | 83.0055 | 100 | 97.7498 | 21.7489 |
| 28. | 14.3822 | 16.5665 | 23.2031 | 27.3546 | 87.5223 | 100 | 94.1309 | 82.1735 |
| 29. | 14.2898 | 15.8537 | 23.1593 | 27.3108 | 83.9454 | 100 | 94.6425 | 82.3859 |
| 30. | 14.4619 | 16.6702 | 23.3331 | 27.4845 | 92.7845 | 100 | 94.4715 | 82.7660 |

On analyzing the Table 1, it can be concluded that PSNR and fitness factor of DWT is more than that of DCT. SO DWT is better method and as the level of DWT go on increasing, PSNR go on increasing while fitness factor go decreasing.

Table 2 shows comparison between DCT and various levels of DWT with corresponding average elapsed time for embedding and extraction for all 30 images.

Table 2: Comparison of average elapsed time for embedding and extraction (without attacks) for all sample images

| Image No. | Average Elapsed Time for Embedding (sec) | | | | Average Elapsed Time for Extraction (sec) | | | |
|---|---|---|---|---|---|---|---|---|
| | DCT | DWT | | | DCT | DWT | | |
| | | 1st level | 2nd level | 3rdlevel | | 1st level | 2nd level | 3rd level |
| 1. | 7.6915 | 5.6176 | 3.7581 | 1.6523 | 10.2836 | 3.8086 | 1.3873 | 0.8536 |
| 2. | 7.3181 | 4.0082 | 2.1146 | 1.5452 | 21.1712 | 3.8157 | 1.2978 | 0.8074 |
| 3. | 6.8222 | 3.7199 | 2.1229 | 1.7827 | 10.9436 | 3.9889 | 1.3107 | 0.8202 |
| 4. | 6.8913 | 3.8780 | 2.0521 | 1.6631 | 10.0101 | 3.9459 | 1.3422 | 0.8088 |
| 5. | 6.3117 | 3.5414 | 2.0953 | 1.6157 | 10.4434 | 4.0109 | 1.3235 | 0.8163 |
| 6. | 6.1709 | 3.6701 | 2.0592 | 1.6377 | 10.7708 | 4.0225 | 1.2855 | 0.8199 |
| 7. | 6.3297 | 3.6681 | 2.0768 | 1.5603 | 10.745 | 3.9239 | 1.2710 | 0.8244 |
| 8. | 6.3915 | 4.1559 | 2.0979 | 1.5446 | 10.4149 | 3.8838 | 1.3384 | 0.7962 |
| 9. | 6.4429 | 3.4702 | 2.0113 | 1.6145 | 11.067 | 3.9569 | 1.2909 | 0.8199 |
| 10. | 6.2156 | 3.7042 | 2.0870 | 1.6472 | 10.832 | 3.9906 | 1.3554 | 0.8215 |
| 11. | 6.9046 | 3.4496 | 1.9758 | 1.6216 | 11.0480 | 3.9036 | 1.3378 | 1.1205 |
| 12. | 6.5088 | 3.5805 | 2.1275 | 1.6063 | 11.1036 | 3.9262 | 1.2891 | 0.7863 |
| 13. | 6.2255 | 3.4801 | 2.1026 | 1.6648 | 10.9197 | 3.8644 | 1.3315 | 0.7974 |
| 14. | 6.5623 | 3.6608 | 1.9862 | 1.6007 | 11.7193 | 3.9208 | 1.2678 | 0.7985 |
| 15. | 6.5989 | 3.5039 | 2.2054 | 1.6007 | 10.8893 | 3.8838 | 1.2968 | 0.8529 |
| 16. | 6.2842 | 3.6437 | 2.0162 | 1.8886 | 10.5222 | 3.8976 | 1.2574 | 0.8072 |
| 17. | 6.2795 | 3.5034 | 2.0033 | 1.5868 | 11.3656 | 4.2409 | 1.3166 | 0.8282 |
| 18. | 6.9595 | 3.5069 | 2.0271 | 1.5490 | 10.9384 | 3.8870 | 1.2516 | 0.8677 |
| 19. | 6.3818 | 3.6765 | 2.0542 | 1.6019 | 10.7604 | 3.8562 | 1.3046 | 0.8429 |
| 20. | 8.5716 | 3.4605 | 1.9721 | 2.0568 | 10.7429 | 3.8564 | 1.2647 | 0.8195 |
| 21. | 7.3417 | 3.5115 | 2.0488 | 1.7556 | 14.6325 | 3.9164 | 1.2339 | 0.8316 |
| 22. | 7.3220 | 3.4973 | 1.9408 | 1.6542 | 14.2275 | 3.9353 | 1.2537 | 0.7955 |
| 23. | 7.4209 | 3.4391 | 2.0963 | 1.6372 | 14.1956 | 4.1783 | 1.3123 | 0.8760 |
| 24. | 7.6151 | 3.4410 | 1.7485 | 1.2360 | 14.1809 | 4.0279 | 1.7845 | 0.7891 |
| 25. | 6.6300 | 3.5399 | 2.9678 | 1.7845 | 12.5473 | 3.9443 | 1.6987 | 0.6587 |
| 26. | 6.4814 | 3.5416 | 2.0564 | 1.9687 | 12.4318 | 3.9236 | 1.7498 | 0.6358 |
| 27. | 7.0163 | 3.4665 | 2.7489 | 1.3648 | 11.8581 | 3.8668 | 1.6598 | 0.9874 |
| 28. | 7.2558 | 3.5181 | 2.1099 | 1.6824 | 11.9650 | 3.9088 | 1.2451 | 0.8475 |
| 29. | 7.0129 | 3.5563 | 2.0105 | 1.4955 | 11.4885 | 4.0022 | 1.2553 | 0.8082 |
| 30. | 6.6641 | 3.5327 | 2.0046 | 2.2311 | 11.6053 | 3.8518 | 1.3112 | 0.7895 |

From the above table, it has been observed that the embedding and extraction time for DCT is more than that of DWT. Moreover, as the level of the DWT increases, the embedding and extraction time decreases.

The salt and pepper and Jpeg Compression noise attacks has been applied on the system and their effect on the system has been analyzed as given in Table 3 and Table 4.

Table 3: Comparison of fitness factor and average elapsed time for embedding and extraction (salt and pepper attacks) for all sample images

| Image No. | Fitness Factor | | | | Average Elapsed Time for Extraction (sec) | | | |
|---|---|---|---|---|---|---|---|---|
| | DCT | DWT | | | DCT | DWT | | |
| | | 1st level | 2nd level | 3rdlevel | | 1st level | 2nd level | 3rd level |
| 1. | 40.0260 | 100 | 92.8414 | 81.9614 | 9.6091 | 3.7174 | 1.1846 | 0.784 |
| 2. | 45.7934 | 100 | 93.9878 | 81.6884 | 9.6372 | 3.7492 | 1.1795 | 0.755 |
| 3. | 54.8839 | 99.9874 | 91.8912 | 80.4554 | 9.6528 | 3.7205 | 1.1837 | 0.934 |
| 4. | 42.9124 | 100 | 92.7874 | 81.2397 | 10.1097 | 3.7244 | 1.2097 | 0.812 |
| 5. | 60.5139 | 100 | 92.5654 | 79.2136 | 9.8084 | 3.7368 | 1.1999 | 0.884 |
| 6. | 43.1135 | 100 | 92.1174 | 80.2578 | 9.8947 | 3.7769 | 1.1857 | 0.965 |
| 7. | 40.9155 | 99.2641 | 91.7247 | 80.7824 | 9.7362 | 3.7626 | 1.1955 | 0.747 |
| 8. | 39.3547 | 100 | 94.1278 | 81.3648 | 11.0145 | 3.7757 | 1.2045 | 0.765 |
| 9. | 43.6171 | 100 | 93.7814 | 79.6574 | 9.7094 | 3.7348 | 1.2037 | 0.755 |
| 10. | 43.4802 | 100 | 92.7541 | 80.9858 | 9.8322 | 3.7852 | 1.1898 | 0.785 |
| 11. | 48.1861 | 98.2112 | 91.4784 | 78.4157 | 9.6851 | 3.7845 | 1.1364 | 0.2358 |
| 12. | 47.1425 | 99.7415 | 92.4187 | 73.1648 | 9.1474 | 3.9548 | 1.1457 | 0.9674 |
| 13. | 42.8574 | 100 | 94.7841 | 82.4781 | 9.4784 | 3.7418 | 1.3259 | 0.5698 |
| 14. | 46.1245 | 100 | 90.4187 | 79.4561 | 9.4785 | 2.7486 | 1.3489 | 0.5264 |
| 15. | 40.2145 | 99.4158 | 92.7418 | 83.1457 | 10.1248 | 3.4561 | 1.7498 | 0.7849 |
| 16. | 47.2145 | 98.4178 | 97.4187 | 76.7489 | 9.1464 | 3.7419 | 1.6354 | 0.9675 |
| 17. | 42.1457 | 99.1487 | 93.4784 | 79.1478 | 9.7418 | 3.7952 | 1.9875 | 0.1298 |
| 18. | 61.7415 | 100 | 97.1547 | 78.1789 | 11.4572 | 3.4159 | 1.5498 | 0.7894 |
| 19. | 52.1497 | 97.4154 | 93.4785 | 79.7498 | 9.3648 | 3.7419 | 1.2698 | 0.1598 |
| 20. | 54.1278 | 99.1487 | 90.4578 | 80.7468 | 10.4789 | 3.4568 | 1.7418 | 0.3658 |
| 21. | 54.7414 | 100 | 92.1478 | 81.4986 | 11.3612 | 3.7418 | 1.9635 | 0.1547 |
| 22. | 40.5897 | 100 | 92.4781 | 82.7489 | 9.1457 | 3.9875 | 1.5987 | 0.9635 |
| 23. | 42.7415 | 98.1457 | 93.4781 | 79.5698 | 9.7485 | 3.7419 | 1.5789 | 0.8745 |
| 24. | 40.1478 | 100 | 91.7487 | 80.1359 | 9.3214 | 3.7469 | 1.3697 | 0.9658 |
| 25. | 52.1478 | 100 | 92.4718 | 87.1598 | 10.7892 | 3.6529 | 1.7448 | 0.7894 |
| 26. | 60.7498 | 99.4178 | 92.7487 | 79.4298 | 9.7456 | 3.7498 | 1.0235 | 0.1598 |
| 27. | 45.1245 | 100 | 90.1478 | 80.4985 | 8.1568 | 3.6245 | 1.0256 | 0.4598 |
| 28. | 43.8754 | 98.1475 | 93.4796 | 81.4789 | 10.7468 | 3.4896 | 1.4782 | 0.1578 |
| 29. | 42.1987 | 99.4784 | 92.7485 | 78.4527 | 11.4578 | 3.7419 | 1.4187 | 0.6398 |
| 30. | 50.1648 | 100 | 94.4598 | 79.4152 | 9.1289 | 3.6589 | 1.9685 | 0.2458 |

Table 4: Comparison of fitness factor and average elapsed time for embedding and extraction

(Jpeg Compression attacks) for all sample images

| Image No. | Fitness Factor | | | | Average Elapsed Time for Extraction (sec) | | | |
|---|---|---|---|---|---|---|---|---|
| | DCT | DWT | | | DCT | DWT | | |
| | | 1st level | 2nd level | 3rdlevel | | 1st level | 2nd level | 3rd level |
| 1. | 35.7485 | 92.5348 | 85.9645 | 76.4453 | 10.1458 | 3.8451 | 1.1968 | 0.741 |
| 2. | 36.7458 | 94.8645 | 87.8912 | 78.5621 | 11.2357 | 3.7452 | 1.1844 | 0.796 |
| 3. | 36.1485 | 93.8415 | 87.8995 | 79.8469 | 9.2569 | 3.7698 | 1.19556 | 0.946 |
| 4. | 38.7495 | 93.8279 | 87.9565 | 78.2348 | 11.5698 | 3.8759 | 1.1967 | 0.812 |
| 5. | 34.1258 | 92.8565 | 86.2385 | 76.2145 | 10.256 | 3.8466 | 1.1899 | 0.848 |
| 6. | 39.7849 | 93.2532 | 85.6596 | 78.2569 | 9.5698 | 3.9863 | 1.1872 | 0.965 |
| 7. | 37.1452 | 94.4179 | 86.8265 | 79.1447 | 9.5678 | 3.7482 | 1.1957 | 0.796 |
| 8. | 36.1542 | 95.1749 | 88.1935 | 78.4187 | 9.8459 | 3.7657 | 1.1799 | 0.778 |
| 9. | 38.1235 | 91.4586 | 85.4598 | 77.9696 | 10.2365 | 3.7388 | 1.6535 | 0.775 |
| 10. | 39.4587 | 95.7896 | 86.7465 | 78.9687 | 9.1564 | 3.7859 | 1.1894 | 0.796 |
| 11. | 38.4578 | 90.2569 | 84.1598 | 75.1265 | 11.5689 | 3.1548 | 1.1578 | 0.7891 |
| 12. | 40.1236 | 91.5498 | 83.2569 | 72.1985 | 9.2365 | 3.9654 | 1.1698 | 1.2564 |
| 13. | 39.5489 | 90.2569 | 87.1569 | 72.3366 | 10.2569 | 3.1235 | 1.2569 | 0.1478 |
| 14. | 38.5689 | 91.1489 | 86.1587 | 75.1298 | 11.2569 | 3.2548 | 1.9685 | 0.2365 |
| 15. | 34.5689 | 92.2569 | 89.2569 | 75.1489 | 12.2548 | 3.5698 | 1.3698 | 0.9874 |
| 16. | 38.2569 | 93.4569 | 87.1569 | 76.2389 | 9.2365 | 3.4152 | 1.4587 | 0.8596 |
| 17. | 40.5869 | 92.4879 | 86.1547 | 77.4259 | 9.2589 | 3.4987 | 1.9685 | 0.1478 |
| 18. | 41.4578 | 91.5987 | 83.2569 | 70.1548 | 10.1587 | 3.6598 | 1.2365 | 0.3698 |
| 19. | 39.4166 | 93.4569 | 83.1549 | 71.2698 | 10.2569 | 3.4578 | 1.7896 | 0.2547 |
| 20. | 39.4589 | 90.4598 | 86.1236 | 75.1236 | 10.5698 | 3.1548 | 1.1365 | 0.2485 |
| 21. | 40.1256 | 92.5698 | 89.1247 | 76.2598 | 11.2569 | 3.9685 | 1.4598 | 0.6987 |
| 22. | 41.1578 | 93.7895 | 86.2569 | 78.2548 | 11.3698 | 3.4598 | 1.1254 | 0.2456 |
| 23. | 39.2569 | 92.7498 | 84.1549 | 76.2563 | 9.6235 | 3.1478 | 1.2365 | 0.2987 |
| 24. | 37.1245 | 91.9658 | 83.7415 | 78.4512 | 9.5698 | 3.6589 | 1.1254 | 0.2365 |
| 25. | 39.2569 | 90.2369 | 86.2365 | 74.2563 | 10.235 | 3.1478 | 1.1547 | 0.2541 |
| 26. | 41.1265 | 91.5698 | 85.1247 | 79.2541 | 10.256 | 3.2698 | 1.1985 | 0.2589 |
| 27. | 39.4159 | 92.4569 | 84.4569 | 76.1258 | 9.3654 | 3.4569 | 1.1256 | 0.3698 |
| 28. | 38.7596 | 91.2659 | 86.2541 | 78.2452 | 10.236 | 3.1478 | 1.1236 | 0.3657 |
| 29. | 41.5987 | 91.5698 | 81.2654 | 79.5632 | 11.2365 | 3.6987 | 1.1254 | 0.1598 |
| 30. | 40.2569 | 91.4985 | 82.1569 | 78.2562 | 9.2563 | 3.1569 | 1.2398 | 0.1547 |

From the Table 3 & 4, it has been observed that as attacks are applied on the watermarked images, fitness factor get reduced for both DCT and DWT but attacks have great impact on DCT than DWT. Moreover on DWT, impact of attacks increases as we increase the level of DWT.

### 4.3 Quantitative Performance Evaluation:-

This section presents the quantitative performance of the evaluation results of PSNR, Fitness Factor, average elapsed time for embedding and extraction. Fig 4.21 shows the relationship between PSNR with DCT and various levels of DWT.

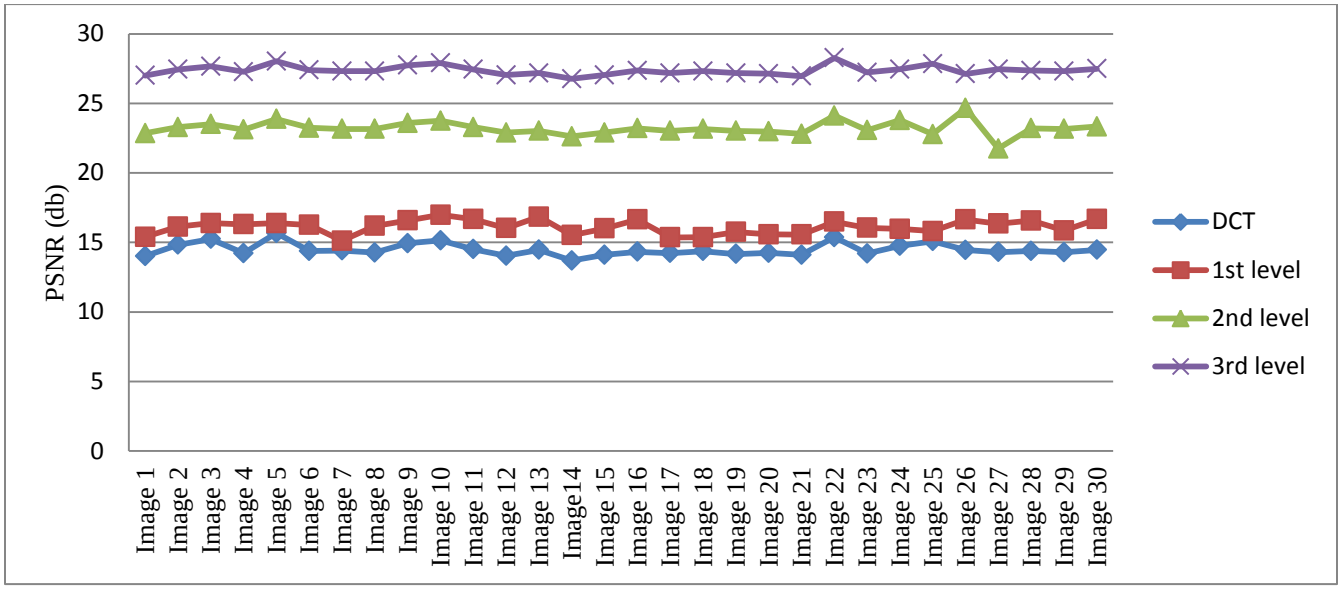



Fig 4.21: Relationship between PSNR and DCT and Various levels of DWT

Fig 4.22 shows the relationship between fitness factor with DCT and various levels of DWT without performing attacks.

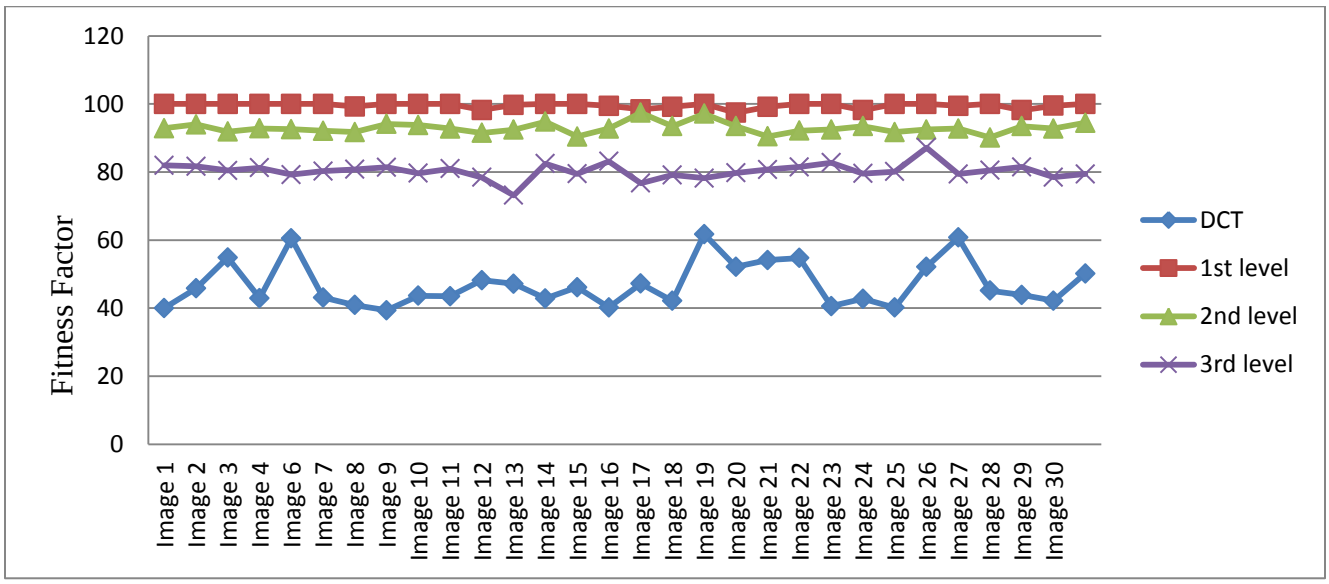



Fig 4.22: Relationship between Fitness Factor and DCT and various levels of DWT (without attacks)

Fig 4.23 shows the relationship between average elapsed time for embedding with DCT and various levels of DWT.

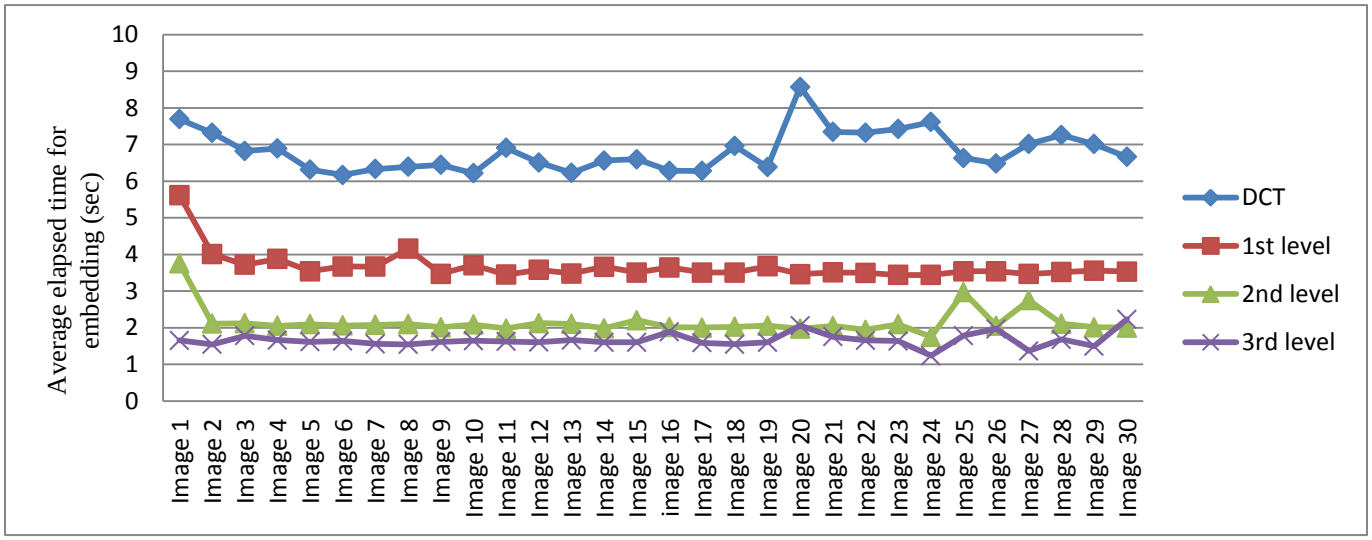



Fig 4.23: Relationship between Average elapsed time for embedding and DCT and various levels of DWT

Fig 4.24 shows the relationship between average elapsed time for extraction with DCT and various levels of DWT without performing attacks.

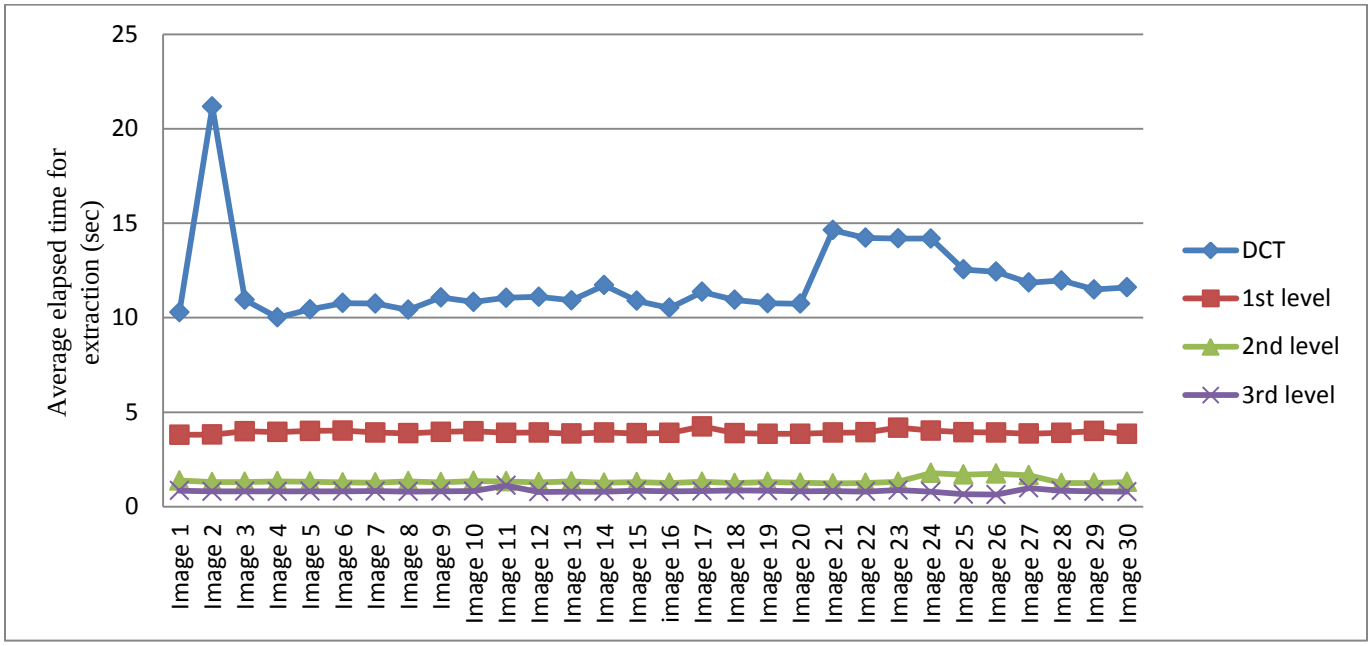



Fig 4.24: Relationship between Average elapsed time for extraction and DCT and various levels of DWT

(without attacks)

Fig 4.25 shows the relationship between fitness factor with DCT and various levels of DWT after applying salt and pepper attacks.

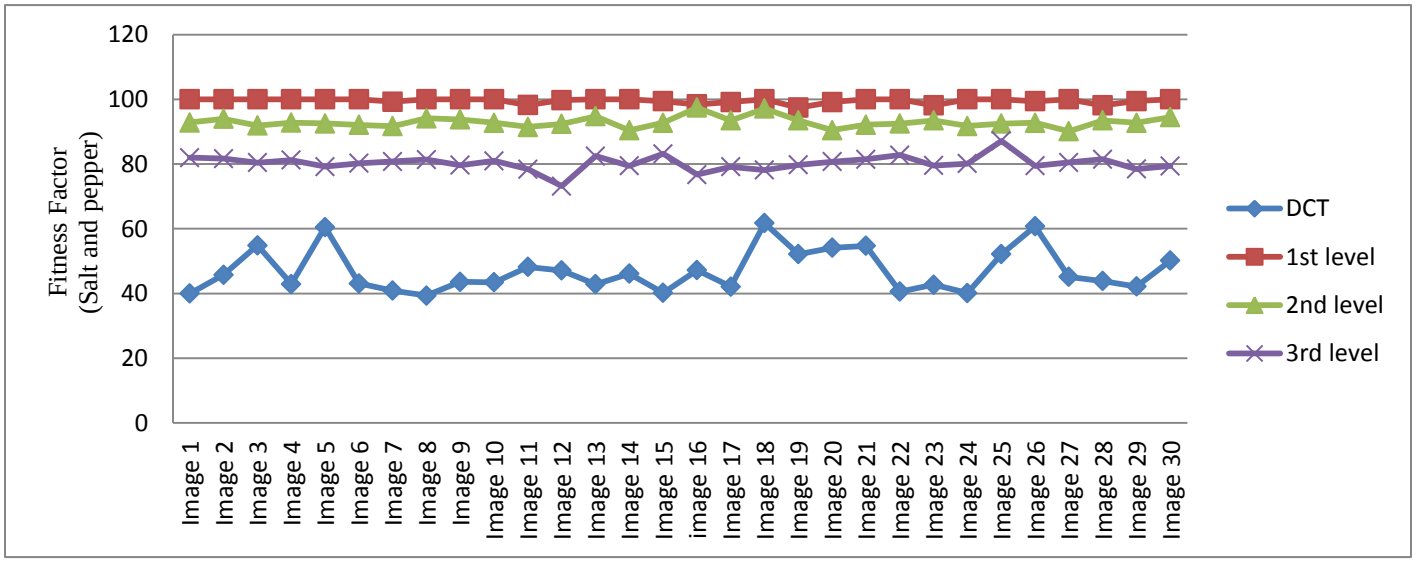



Fig 4.25: Relationship between Fitness Factor and DCT and levels of DWT (salt and pepper attacks)

Fig 4.26 shows the relationship between average elapsed time for extraction with DCT and various levels of DWT after applying salt and pepper attacks.

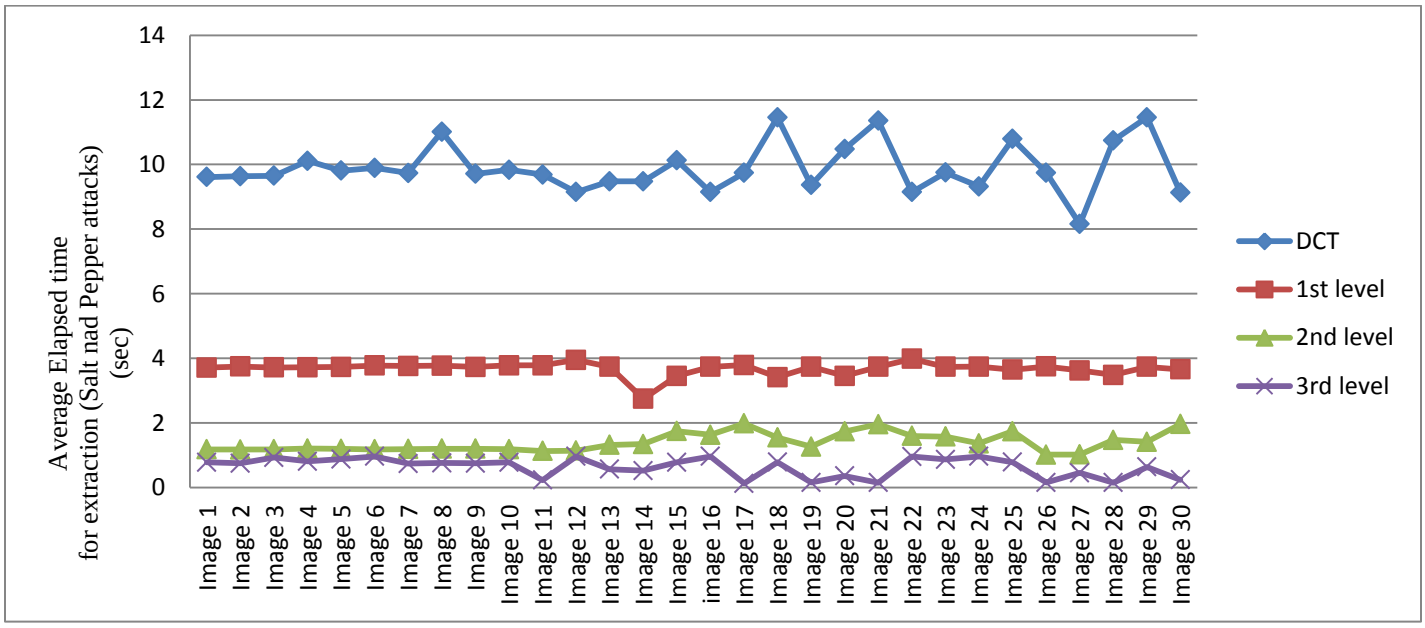



Fig 4.26: Relationship between Average elapsed time for extraction and DCT and various levels of DWT (salt and pepper attacks)

Fig 4.27 shows the relationship between fitness factor with DCT and various levels of DWT after applying Jpeg Compression attacks.

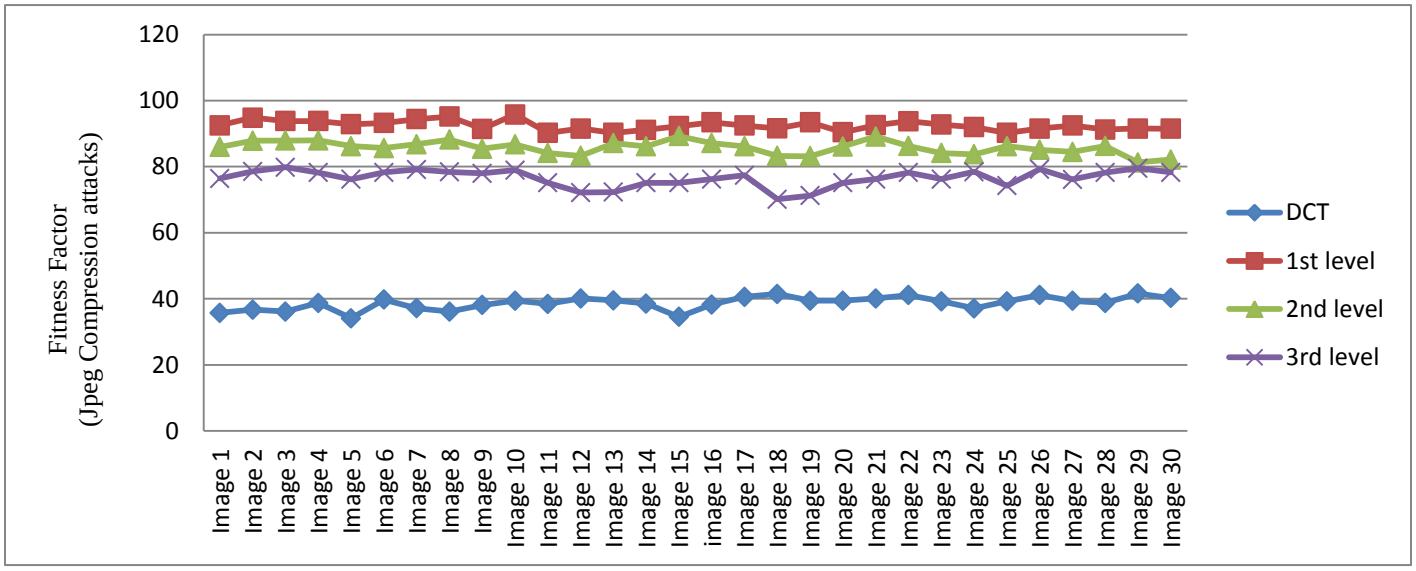



Fig 4.27: Relationship between Fitness Factor and DCT and various levels of DWT

(Jpeg Compression attacks)

Fig 4.28 shows the relationship between average elapsed time for extraction with DCT and various levels of DWT after applying Jpeg Compression attacks.

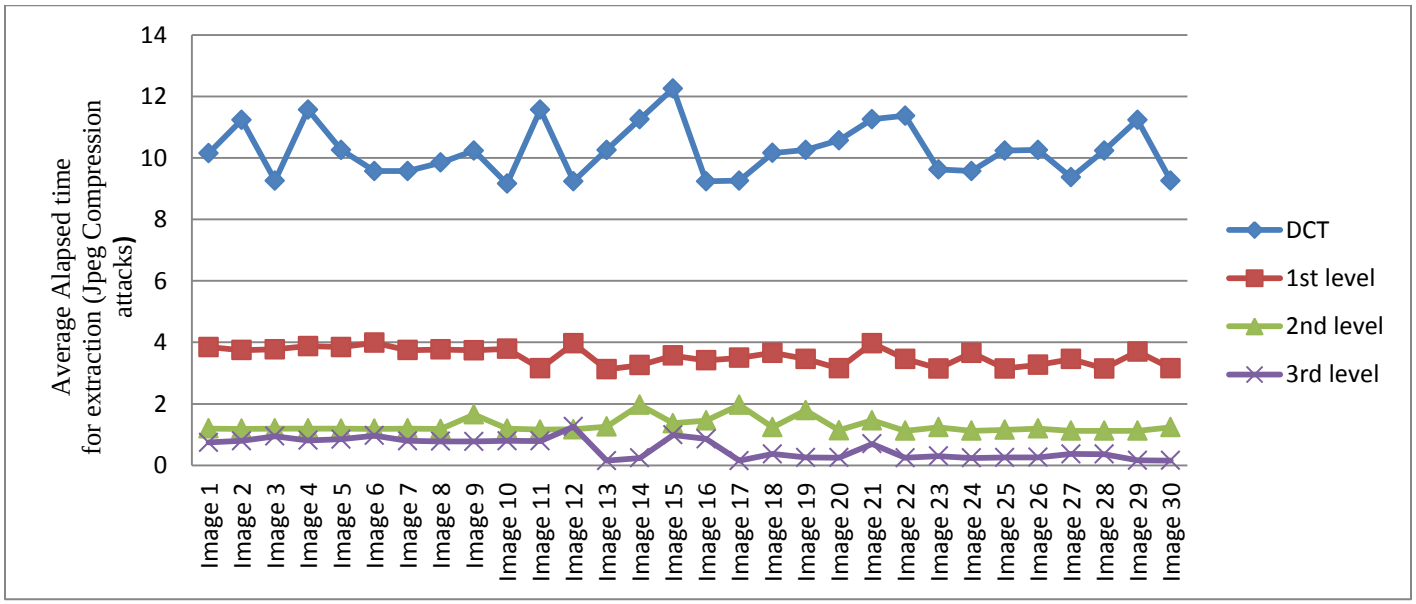



Fig 4.28: Relationship between Average elapsed time for extraction and DCT and various levels of DWT

(Jpeg Compression attacks)

From the above all results and quantitative performance evaluation, it can be seen how DCT and various levels of DWT varies with PSNR, Fitness Factor and average elapsed time for embedding and extraction. It can be concluded from the above graphs and Tables that DWT gives much better results than DCT in all aspects on the other hand in DWT, parameters changes as level of DWT changes.

# CHAPTER 5

# CONCLUSION & FUTURE SCOPE

## 5.1 Conclusion

Digital Watermarking is a data hiding technique in which confidential digital message is masked in the digital signal. Digital watermark which is a secret message should be embedded in perfect location to make it secure, imperceptible and highly robust. Digital Watermarking can be done in spatial and transform domain. Earlier it was done in spatial domain, but now the work has been shifted to transform domain due to various disadvantages in spatial domain. In this dissertation, digital watermark is embedded in fingerprint image by applying Discrete Cosine transform and Discrete Wavelet Transform Techniques. This work compares the peak signal to noise ratio (PSNR) for both of the transform techniques. It is concluded that PSNR is good for DWT in comparison to DCT and moreover, in DWT, PSNR increases as the level of DWT increases which shows that imperceptibility increases with the level of DWT. Fitness factor has also been compared by applying various noises in the form of attacks like salt and pepper, Jpeg Compression for both techniques and which concludes that fitness factor is very high for DWT as compared to DCT and in DWT, fitness factor decreases as the level of DWT is increased which shows robustness decreases. Comparison of average elapsed time for embedding and extraction has also done which concludes that DCT take more time than DWT and in DWT, time get decreased as the level of DWT increases. So, it is concluded at last that DWT gives much better results than DCT in all aspects due to various disadvantages of DCT like block phenomenon, low compression ratio, high information lost, unable to analyze both spectral and temporal properties simultaneously etc. Moreover, a tradeoff has examined between the imperceptibility and robustness.

## 5.2 Future Scope

In future, work can be further extended in the following directions

(i) Embedding of English alphabet as a watermark has been implemented. It can be further improved by adding various details like age, voter-id card etc in the fingerprint image.

(ii) Various different encryption techniques can be applied on watermark before embedding it in the fingerprint image just to provide the security of watermark itself.

(iii) Work implemented on static signal. This can be extended to non-stationary signals like video, audio.

# REFERENCES


[1] M. S. Hsieh, D. C. Tseng & Y. H. Huang, "Hiding digital watermarks using multi resolution wavelet transform,"*On Industrial Electronics, IEEE Transactions*, 2001, 48(5), pp. 875-882.

[2] V. M. Potdar, S. Han & E. Chang, "A survey of digital image watermarking techniques," *On Industrial Informatics, 3rd IEEE International Conference*, August, 2005, pp. 709-716.

[3] R. Chouhan, A. Mishra & P. Khanna , "Wavelet-based robust digital watermarking scheme or fingerprint authentication," *In Proceedings of International Conference on Intelligent Computational Systems (ICICS)* , July, 2011, pp. 29-33.

[4] C. Song, S. Sudirman & M. Merabti, "Recent Advances and Classification of Watermarking Techniques in Digital Images," *In Proceedings of Post Graduate Network Symposium*, June, 2009.

[5] Watermark Image. Available at http://www.google.co.in/webhp?sourceid=chromeinstant

&uin=1@ie=UTF8#q=visible%20watermamrk%20images. Accessed on 20/10/2014.

[6] K. Zebbiche & F. Khelifi, "Region-based watermarking of biometric images: Case study in fingerprint images," *On International Journal of Digital Multimedia Broadcasting,* 2008.

[7] X. Y. Wang & H. Zhao, "A novel synchronization invariant audio watermarking scheme based on DWT and DCT. *Signal Processing*," *On IEEE Transactions*, 2006, 54(12), pp. 4835-4840.

[8] D. Chopra, P. Gupta, B. C. Gaur Sanjay & A. Gupta, "Lsb Based Digital Image Watermarking For Gray Scale Image," *On IOSR Journal of Computer Engineering (IOSRJCE) ISSN,* 2012. pp. 2278-0061.

[9] J. G. Lee, E. J. Yoon & K. Y. Yoo , "A new LSB based digital watermarking scheme with random mapping function," *In Ubiquitous Multimedia Computing, International Symposium on , IEEE*, October, 2008, pp. 130-134.

[10] N. Chandrakar & J. Bagga, "Performance Comparison of Digital Image Watermarking Techniques: A Survey," *International Journal of Computer Applications Technology and Research*, 2013, 2(2), 126-130.

[11] R. Chouhan, A. Mishra & P. Khanna, P, "Fingerprint Authentication by Wavelet-based Digital Watermarking," *International Journal of Electrical and Computer Engineering (IJECE)*, 2012, 2(4), 519-528.

[12] C. K. Chui, "An introduction to wavelets," *Academic Press*, 2014, vol (1).

[13] A. Graphs, "An introduction to wavelets," *Computational Science & Engineering, IEEE,* 1995, 2(2), pp. 50-61.

[14] A. Habibi," Introduction to wavelets," *In Military Communications Conference, IEEE,* November, 1995, vol(2), pp. 879-885

[15] Daubechies Filter. Available at http://bearcave.com/mis/misl_tech/wavelets/daubechies/. Accessed on 20/05/2015.

[16] Coiflet Filter. Available at https://en.wikipedia.org/wiki/Coiflet. Accessed on 21/05/2015.

[17] Levels of DWT. Available at http://inspirehep.net/record/822532/plots. Accessed on 29/05/2015.

[18] S. Shridhar, P. R. Kumar, & K. V. Ramanaiah, "Wavelet Transform Techniques for Image Compression- An Evaluation," *International Journal of Image, Graphics and Signal Processing (IJIGSP)*, 2014, 6(2), pp.54.

[19] Haar Wavelet. Available at http://en.wikipedia.org/wiki/Haar_wavelet. Accessed on 22/05/2015.

[20] M. Vata, R. Singh, A. Noore, M. M. Houck & K. Morris, "Robust biometric image watermarking for fingerprint and face template protection," *On IEICE Electronics Express*, 2006, 3(2), pp. 23-28.

[21] A. Ali-Haj, "Combined DWT-DCT digital image watermarking", *Journal of computer science*, 2007, *3*(9), pp. 740-746.

[22] R. Safabakhsh, S. Zaboli & A. Tabibiazar, "Digital watermarking on still images using wavelet transform," *In Information Technology, Coding and Computing (ITCC), International Conference, IEEE,* April, 2004, vol (1), pp. 671-675.

[23] A. K. Jain, U. Uludag & R. L. Hsu, "Hiding a face in a fingerprint image," *In Proceedings of International Conferences on Pattern Recognition, 16th International Conference, IEEE,* 2002, vol (3), pp. 756-759.

[24] J. R. Kim & Y. S. Moon, "A robust wavelet-based digital watermarking using level-adaptive thresholding", *In Proceedings of International Conferences on Image Processing, International Conference, IEEE,* October, 1999, vol (2), pp. 226-230.

[25] K. Zebbiche, L. Ghouti, F. Khelifi & A. Bouridane, "Protecting fingerprint data using watermarking," *In Adaptive Hardware and Systems, First NASA/ESA Conference, IEEE,* June, 2006, pp. 451-456.

[26] M. Alkhathami, F. Han & R. Van Schyndel, "Fingerprint minutiae protection using two watermarks," *In Industrial Electronics and Applications (ICI), 8th IEEE Conference,* 2013.

[27] E. Ganic & A. M. Eskicioglu, "Robust DWT-SVD domain image watermarking: embedding data in all frequencies", *In Proceedings of Workshop on Multimedia and Security,* September, 2004, pp. 166-174.

[28] V. S. Jabade & D. S. R. Gengaje, "Literature review of wavelet based digital image watermarking techniques", *International Journal of Computer Applications*, 2011, 31(1), pp. 28-35.

[29] Z. M. Lu, D. G. Xu & S. H. Sun, "Multipurpose image watermarking algorithm based on multistage vector quantization," *Image Processing, IEEE Transactions on*, 2005, 14(6), pp. 822-831.

[30] B. Gunsel, U. Uludag & A. M. Tekalp, "Robust watermarking of fingerprint images," *Pattern Recognition*, 2002, 35(12), pp. 2739-2747.

[31] A. Noore, R. Singh & M. Vatsa, "Enhancing security of fingerprints through contextual biometric watermarking," *Forensic Science International*, 2007, 169(2), pp. 188-194.

[32] R. C. Gonzalez and R. E. Woods, “Digital image processing”, 2002.

[33] A. K. Jain & U. Uludag, “Hiding biometric data”, *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 2003, *25*(11), pp. 494-1498.

[34] J. Fridrich & M. Goljan, “Robust hash functions for digital watermarking." *Information Technology: Coding and Computing, Proceedings, International Conference on*, *IEEE*, 2000, pp.178-183.

[35] J. S. Seo, J. Haitsma, T. Kalker & C. D. Yoo, “A robust image fingerprinting system using the Radon transform,” *Signal Processing: Image Communication*, 2004, 19(4), pp. 325-339.

[36] M. D. Swanson, B. Zhu & A. H.Tewfik, “Transparent robust image watermarking,” *Image Processing, Proceedings., IEEE International Conference on*. *1996,* vol (3), pp. 211-214.

[37] N. Nikolaidis & P. Ioannis, “Robust image watermarking in the spatial domain,” *Signal processing* , 1998, 66(3), pp. 385-403.

[38] B. L. Gunjal & R. R. Manthalkar, “An overview of transform domain robust digital image watermarking algorithms”, *Journal of Emerging Trends in Computing and Information Sciences*, 2010, *2*(1), pp.37-42.

[39] M. Jiansheng, L. Sukang & T. Xiaomei, “A digital watermarking algorithm based on DCT and DWT,” In *International Symposium on Web Information Systems and Applications , May, 2004*, pp. 104-107.

[40] A. Graps, “An introduction to wavelets”, *Computational Science & Engineering, IEEE*, 1995, *2*(2), pp.50-61.

[41] C. K. Chui, “*An introduction to wavelets”*, *Academic press*, 2014, (Vol. 1).

[42] Wavelet Families. Available at http:// www.flickr.com/photos/29488969@N07/2756467125

Accessed on 29/05/2015.

[43] D. Mukherjee, S. Maitra & S. T. Acton, “Spatial domain digital watermarking of multimedia objects for buyer authentication,” *In Multimedia, IEEE Transactions on*, 2004, *6*(1), pp.1-15.

[44] E. Ganic & A. M. Eskicioglu, "Robust DWT-SVD domain image watermarking: embedding data in all frequencies", *In Proceedings of Workshop on Multimedia and Security*, September, 2004, pp. 166-174.

[45] N. Memon & P. W. Wong, "Protecting digital media content," *On Communications of the ACM*, 1998, *41*(7), 35-43.

[46] M. U. Celik, G. Sharma, E. Saber & A. M. Tekalp, "Hierarchical watermarking for secure image authentication with localization," On *Image Processing, IEEE Transactions*, 2002, *11*(6), 585-595.

[47] F. A. Petitcolas, "Watermarking schemes evaluation," On *Signal Processing Magazine, IEEE*, 2000, *17*(5), 58-64.