Wavelet Based Watermarking Technique using Digital Images

Project Report submitted in partial fulfillment of the requirement for the degree of

Master of Technology.

in

Computer Science & Engineering

under the Supervision of

Mr. Amit. Kumar Singh

By

By:-Anum Javeed

Enrollment no: 132221

Jaypee University of Information Technology

Waknaghat, Solan – 173234, Himachal Pradesh

TABLE OF CONTENT

CERTIFICATE

This is to certify that project report entitled "Wavelet Based Watermarking Technique using Digital Images", submitted by Anum Javeed in partial fulfillment, for the award of degree of Master of Technology in Computer Science and Engineering to Jaypee University of Information Technology, Waknaghat, Solan has been carried out under my supervision.

This work has not been submitted partially or fully to any other University or Institute for the award of this or any other degree or diploma.

Signature of Supervisor……..

Name of Supervisor: Mr.Amit Kumar Singh

Designation**:** Assistant Professor

Date**……**

ACKNOWLEGEMENT

Firstly, I would like to thank Allah, the merciful the gracious who has given me the ability and energy to accomplish the thesis work.

Foremost, I would like to express my sincere gratitude to my advisor Mr. Amit Kumar Singh for the continuous support of my thesis study and research, for his patience, motivation, enthusiasm, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better advisor and mentor for my thesis study. Who let me experience the research for Watermarking of Images and practical issues beyond the textbooks patiently corrected my writing and financially supported my research. .

I am extremely grateful to Brig. (Retd).Satya Prakash Ghrera, Professor and Head of the Department of the Computer Science and Engineering, and all other Faculty members Department of Computer Science and Engineering.

I would also like to thank my parents and brother. They were always supporting me and encouraging me with their best wishes.

Signature of the student……

Name of the student: Anum Javeed Zargar

Date……

LIST OF FIGURES

Content Page number

LIST OF TABLES

Content Page number

LIST OF ACRONYMS

DWT	Discrete Wavelet Transform
DCT	Discrete Cosine Transform
SVD	Discrete Fourier Transform
BTC	Block Truncation coding
PSNR	Peak Signal to Noise Ratio
NC	Normalized Correlation
F.C	Fractal Compression
C.R	Compression Ratio

MOTIVATION

As my motivation of doing this project is that watermark provides:

- **Cryptography:** In this technology, sender convert plaintext to cipher text by using encryption key and other side receiver decrypt the cipher to plain text. When key is deciphered cryptography does not know how to handle plain text [1].As plain text can be easily attacked by intruders, and our message will be remain no longer secret

- **Digital image and communication in medicine (DICOM)**: It is a standard for handling storing and printing, transmitting information in medical imaging. The communication protocol use in it is application protocol which uses TCP/IP It includes a header file format definition and network communication protocol. DICOM can be exchanged between two entities that are capable of receiving image and patient data in DICOM format. Image displayed under DICOM standard does not define how image are displayed or annotated. There is a challenge that data which is to be embedded must not affect the quality of image ,which result in wrong diagnosis [2].

- **Copyright Protection:** It has wide variety of applications such as fingerprinting, medical images, data tampering and authentication it has mechanism that prevent data usually digital data from being copied.

- **Stolen images:** With the help of watermark we can easily find stolen images watermark has a property to solve the issues of stolen images , so it was one of my great motivation to choose watermark as my project. Digital watermarking is a technique which provides a best solution to these important issues.

OBJECTIVE

- To study an investigate in detail image watermarking technique in spatial and transform domain. The most prospective techniques among them will be retraced by analysis and simulation for digital image.
- To study software tools for simulation and investigation of the image processing applications.
- To propose a novel technique to improve the robustness without significant degradation of image quality against signal processing attack. To evaluate image quality of the watermarked image by the parameter PSNR and robustness of the extracted watermark by the parameter NC in terms of numerical value.

ABSTRACT

Watermarking is highly demanding in recent times for the protection of multimedia data in network environment from illegal copying, violation of copyright, authentication etc while compression of multimedia signals is essential to save storage space and time to transmit the data. However, the working principles of watermarking and compression seem to be different as perceptual data coding removes inherent redundancy during compression. Compression technique reduces the number of bits in image, but produces better quality of image. Image compression plays very important role in image processing when we want to send large images on the internet. Generally threat to the image is increased on the internet, so compressed image is send to make optimal use of network band-width. Image is easily changed on the internet intentionally or unintentionally. To make sure that the correct image is being delivered at the other end, so we embed watermark to the image .Though watermarking increases the size of the uncompressed image but it has to be done to achieve high degree of robustness. Image storage and transmission have created an important and increasing part for the compression techniques. The main aim of compression is to reduce the number of bits as much as possible, while keeping the pixel resolution and the visual quality of the reconstructed image as close to the original image as possible. The redundancy and similarity among different images make compression easy.

The thesis has been organized into 5 chapters. Each chapter give distinct concept:

Chapter 1 presents general description about digital watermarking, spatial and transform domain technique used in image watermarking, characteristics and recent applications of watermarking.

Chapter 2 discussed several reported technique of wavelet based watermarking for digital images.

Chapter 3 described a wavelet based method for image watermarking using Lossy compression technique. The method is found to robust against known signal processing attacks. The proposed watermarking method using BTC compression technique and

fractal compression technique. The performance of the BTC based compression technique is better than the fractal based technique.

The performance of the wavelet based watermarking technique has also been discussed with lossless compression technique in chapter 4. The method is using Huffman compression technique and found to be robust and imperceptible than the above lossy compression techniques.

Chapter V described the conclusion and future work.

CHAPTER 1

Digital Image Watermarking: An Overview

1. Introduction

Digital watermark referred simply to watermarking, a different pattern of bits inserted into digital images, audio, video, text, it helps to identify the file's copyright information and provide authentication .It is a process that embeds a data called watermark into different multimedia object such that watermark can be extracted or detected later to make an declaration about the object [1].Watermark can be either visible or invisible, as it can be use to protect different type of multimedia objects and data. Watermark can be used to identify both the source and intended recipient. Watermark presence in the image should not easily degrade the quality of image. It should be resistant to different signal processing attacks. Visible watermark can be used for improved copyright protection.. Invisible watermark uses to detect misappropriate images. It can be used as evidence of ownership.

There are three type of Information hiding techniques[1] :

- **Cryptography** is the process of converting information to an unintelligible form so that only the person endorsed with the key can decrypt it. The message which sender wants to send is called as plain text and one received by receiver is cipher text. The process of converting plain text to cipher text is called encryption and from cipher text to plain text is called as decryption. Hence encryption protect data from getting damaged during transmission, but during transmission data is not longer protected. Hence some best methods were designed to offer better security than what cryptography could present. This led to the detection of new technique stenography and watermarking [1]
- **Steganography** is the process of hiding communication The information is hide in a unremarkable cover in such a way that its existence is not known to the attacker. Watermarking is closely related to steganography, but its goal is to achieve high level of robustness means when watermark removed from cover

image quality of image should not be degraded, while as steganography stands for high capacity and security ,even small modification to stego image can destroy it [3].

Watermarking is closely related to steganography, but in watermarking the unseen information is usually related to the host object. Hence it is mainly used for copyright protection and administrator authentication [1].

Watermarks and its different techniques can be divided into various categories according to working domain [4]. It can be spatial domain watermarking and Frequency domain watermarking. Spatial domain methods include Least Significant Bit (LSB), Patch Work, spread spectrum and correlation based technique are simple high capacity but are not robust against common signal processing attacks. Spatial domain is based on gray-level mapping where type of mapping depends on criteria used for enhancement [4].Transform domain method (DFT, DWT, DCT and SVD etc) produces excellent quality of watermarked image by embedding watermark image into different sub-bands using different transformation techniques. The transform domain watermarking is comparatively to a large extent better than the spatial domain watermarking.

1.1 Difference between Steganography, Cryptography and Watermark:

- **Steganography Vs. Cryptography**: The term steganography means "cover writing" whereas cryptography means " secret writing". Cryptography is the study of methods of transferring messages in different form so that only the designed recipients can remove the masquerade and read the message. The message we want to send is called plain text and hidden message is called cipher text. The process of converting a plain text to a secret text is called enciphering or encryption, and the reverse process from secret text to plain text is called deciphering or decryption [1].
- **Steganography Vs. Digital Watermarking:** A watermark focussed on intellectual property right and authentication of digital media and can be supposed as an attribute of the carrier (cover). It may contain information such as

copyright, license, tracking and authorship etc. Whereas in case of steganography, the surrounded message may have nothing to do with the cover image. In steganography an matter of concern is bandwidth for the covert message whereas robustness and imperceptibility is of more concern with watermarking [1].

- **Digital signature Vs. Digital watermark:** There are contradictory viewpoints about the "digital signature". A digital signature is based upon the concept of public key encryption. A private key is used to encrypt a hash version of the image. This encrypted file then forms a unique "signature" for the image since only the entity signing the image has knowledge of the private key used. An associated public key can be used to decrypt the signature. The image under question can be hashed using the same hashing function as used original in cover image. If these hashes match with the original image, then the image is considered as authentic. It is use to validate the authenticity and integrity of a message or original document. A watermark, on the other hand, is a process of trouncing information in a cover image the information should be hidden in such a way that image quality should not be degraded. The watermark allows for verification and authentication of an image. However, a watermark alone is not enough to prove first authorship, since an image could be marked with multiple watermarks. It has also been pointed out in [1] that digital watermarks are well suited for copyright and bank verification. Figure 1 shows different type of watermarking techniques.

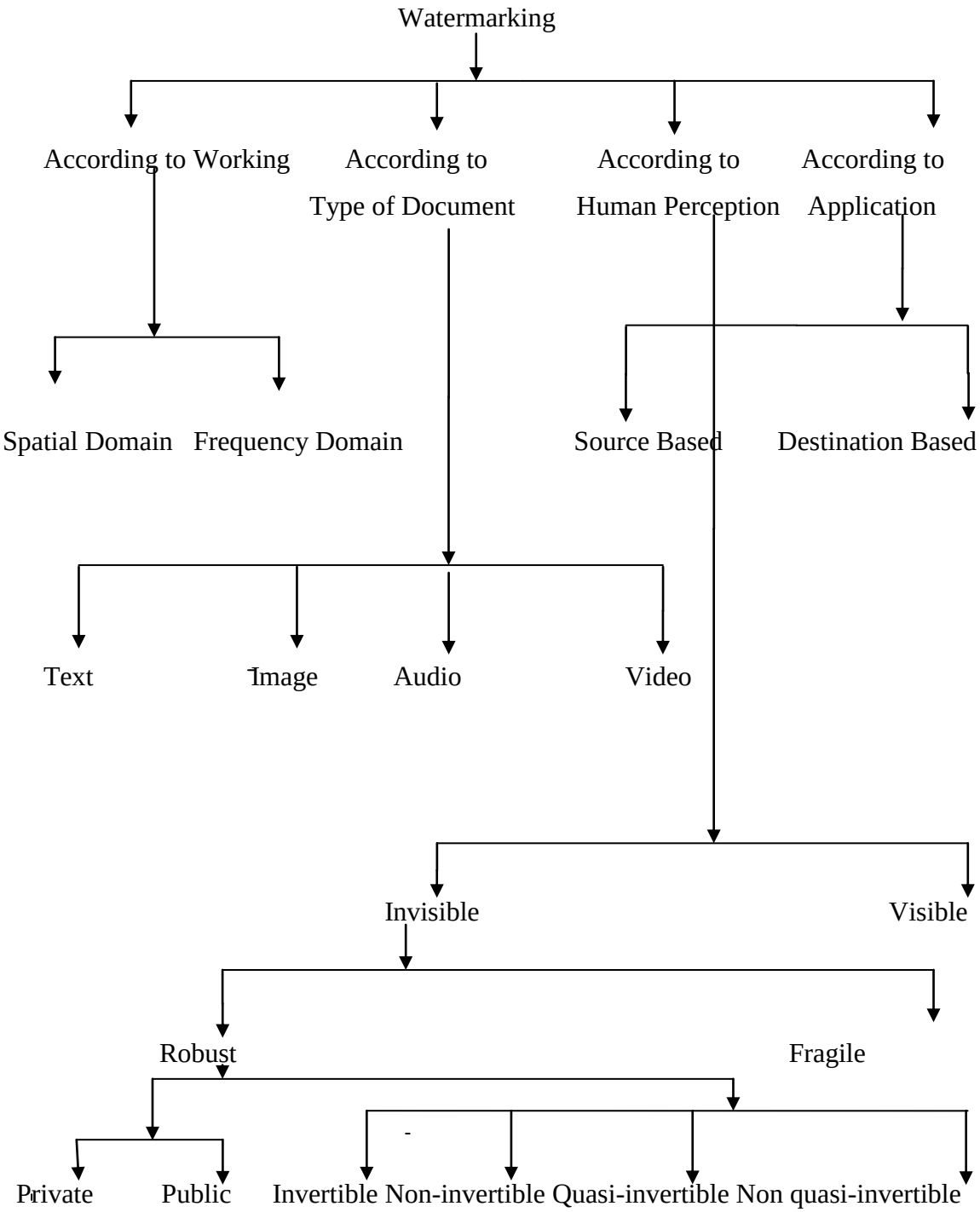


Figure 1: Type of watermarking Technique [1]

1.2 General Frame work for watermarking:

Watermarking is the process that embeds data called a watermark or digital signature or tag or label into a multimedia object such that watermark can be detected or extracted later to make an assertion about the object. The object can be an image or audio or video. A simple illustration of a digital watermark would be a visible "seal" placed over an image to identify the limited rights. However the watermark might contain information in sequence including the identity of the purchaser of a particular copy of the material.

In general, any watermarking scheme (algorithm) consists of three parts.

- The watermark.
- The encoder (insertion algorithm).
- The decoder and comparator (verification or extraction or detection algorithm).

Encoding Process: Lets the cover image be denoted by R, a signature S = s1, s2 and the watermarked image By $R^{'}$. E is an encoder function, it takes an image R and a signature (S) and it generate a new image which is called watermarked image (R') mathematically written as.

$$E(R,S) = R^{'} \quad (1)$$

It should be noted that the signature (S) may be dependent on image (R). In such cases, the encoding process described by Eqn. 1 still holds. Figure 1 illustrates the encoding process [1].

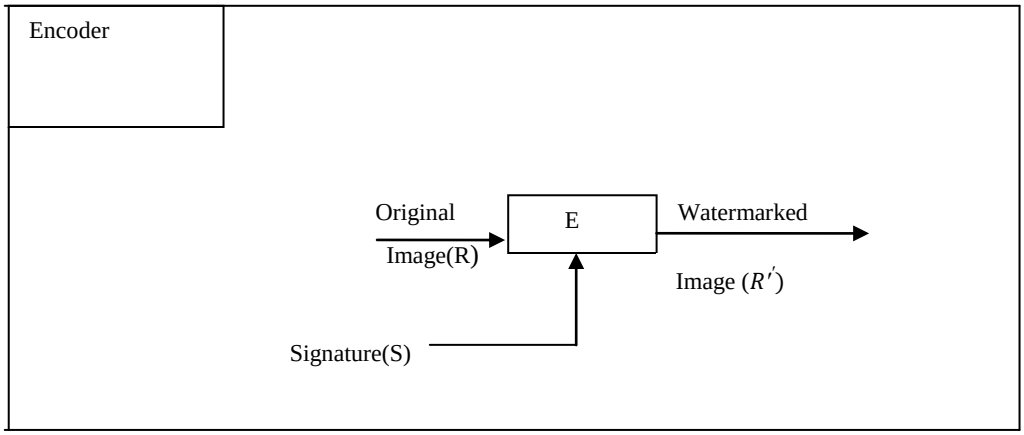


Figure 2: Encoding Process [1]

Decoding Process

A decoder function H takes an image M (M can be any watermarked or un-watermarked image, and possibly corrupted or damaged) whose rights is to be determined and recover a signature $S'$from the image. In this process an extra image R can also be included with the original and un-watermarked version of image M. This is due to the fact that some encoding techniques may use the original images in the watermarking process to provide extra robustness against intentional and unintentional bribery of pixels.Figure 2 illustrates the decoding process Mathematically,

$$E(M,R) = S' \quad (2)$$

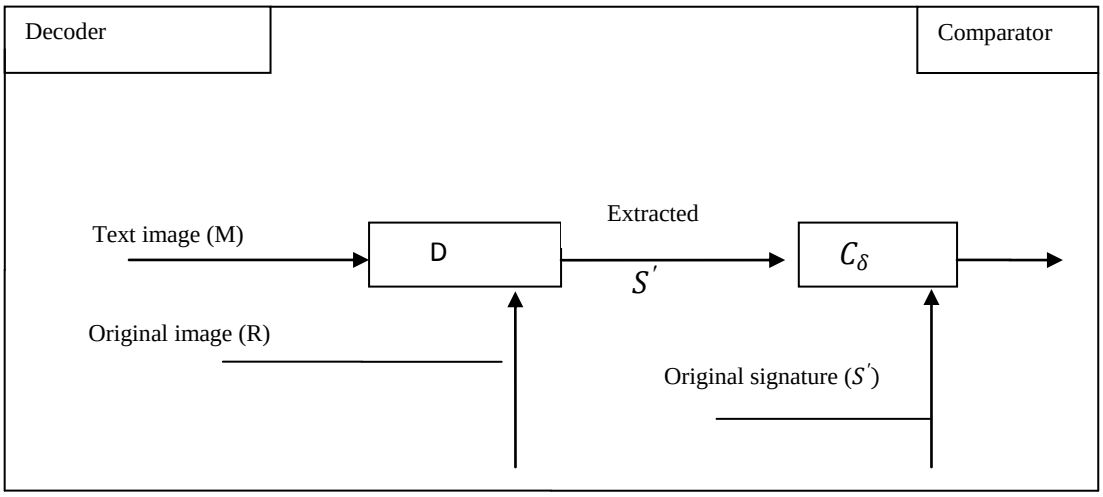


Figure3: Decoding Process[1]

The extracted signature S' will then be compared with the owner signature sequence by a comparator function C_δ and a binary output decision is generated.

1.3 Types of Digital Watermarks:

Watermarking techniques can be divided into four categories according to the type of document to be watermarked [1].

- Image Watermarking
- Video Watermarking
- Audio Watermarking
- Text Watermarking

According to the individual perception, the digital watermark can be divided into three different types as follows.

- Visible watermark
- Invisible-Robust watermark
- Invisible-Fragile watermark
- Dual watermark

Visible Watermark

These watermarks can be seen clearly by the viewer and can also identify the logo or the owner. Visible watermarking technique changes the original signal. The watermarked signal is different from the original signal.

Invisible Watermark

Invisible watermarking refers to adding information in a video or picture or audio as digital data .It is not observable or perceivable, but it can be detected by different ways. It may also be a form or type of secret writing and is used for widespread use. It can be retrieve easily

Invisible watermark can be further divided into three different types:

- Robust Watermark
- Fragile Watermark
- Public and Private watermark

Robust Watermarks

Invisible watermark cannot be manipulated without disturbing the host signal, by robust make it resist to different signal processing attacks. This is very important requirement of a watermark. There are a variety of attacks, intentional (salt and pepper, speckle attack) and intentional attacks which are aimed at destroying the watermark. So, the surrounded watermark should be such that it is resistant to various such attacks. They are designed to resist any manipulations that may be encountered.

Fragile Watermarks

They are designed with very low robustness. They are used to check the consistency of objects. It is use to check any interference done by any other channel. so we can easily detect fraud or any alteration in it. Alteration to an original work that is clearly not noticeable, are nor referred to as watermarks, but as barcodes.

Public and Private Watermark

They are differentiated in accordance with the secrecy requirements for the key used to embed and retrieve watermarks. If the original cover image is not known during the recovery process then it is called a public or a blind watermark and if the original image is known during the recovery process it is called a non-blind watermark or a private watermark.

1.4 Technique of watermarking

There are different digital watermarking techniques in different domain which are categorized as [7].

1.4.1 Spatial Domain Techniques

Spatial domain watermarking slightly modifies the pixels of one or two randomly selected subsets of an image. Modifications might include swapping the low-order bit of

each pixel. However, this technique is not reliable when subjected to normal media operations such as filtering or lossy compression [6]. LSB, Spread spectrum and correlation based technique are some important spatial domain techniques.

Least Significant Bit Coding (LSB)

LSB coding is one of the earliest methods. It can be applied to any figure of watermarking. In this method the LSB of the transport signal is substituted with the watermark. The bits are embedded in a different sequence which acts as the key. In order to recover it back this sequence should be known. The watermark encoder first selects a partition of pixel values on which the watermark has to be embedded. It then embed the information on the LSBs of the pixels from this subset [7]. LSB coding is a very straightforward technique but the robustness of the watermark will be too low. With LSB coding almost forever the watermark cannot be retrieved without a noise component. Many other technique for LSB substitution is used such as MSB of cover image is replace with LSB of watermark.

Spread Spectrum Technique

The watermark should not be placed in unwanted region of the image or its spectrum, since many signal processing attack affect these components. The question is to how to insert a watermark in the significant region of the spectrum .Any spectrum coefficients an be modified, such changes in coefficient of spectrum will be small. This problem can be solved by using spread-spectrum analogy in which frequency part of the image is viewed as communication channel and watermark as a signal which is transmitted through it [10]. In spread-spectrum communication, one transmits a narrowband signal over a wide large bandwidth such that signal energy present in any frequency is not noticeable. Similarly watermark are also transmitted over different frequency, so that if energy is small and will not be noticed. Spreading the watermark throughout the spectrum ensures a large amount of security against intentional or unintentional attack.

Correlation-Based Techniques

In this method a pseudo random noise (PN) with a pattern W(x, y) is added to an image, according to the equation. This method do not perform data-reduction of the feature based techniques ,and is very expensive

IW(x, y) = Watermarked image.

I(x, y) =Original image

k=gain factor

$$T = I(x, y) + k.\ IW(x, y) \quad (3)$$

Increasing k increases the robustness of the watermark at the expense of the quality of the watermarked image[10]. At the decoder the connection between the random noise and the image is found out and if the value exceeds a certain entry value the watermark is detected else it is not.

1.4.2 Frequency Domain Techniques

All signals have a regularity domain representation and in 1822, Baron Jean Baptist Fourier detailed the theory that any real world waveform can be generated by the addition of sinusoidal waves. It produce high quality watermarked image by transforming the original image into the frequency domain by the use of Fourier Transform, Discrete Cosine Transform, Discrete Wavelet Transform. Frequency domain method are more robust as compared to spatial domain. It is a straightforward method

Discrete Cosine Transform (DCT)

It is a process which converts a sequence of data points in the spatial domain to a sum of sine and cosine waveforms with different amplitudes in the frequency domain. A linear combination of m known basis vectors weighted with the m coefficients will result in the original vector[8]. The known basis vectors of transform from this class are “sinusoidal”, which means that they can be represent by sinus bent waves or, in other words, they are strongly restricted in the frequency domain. It is widely used in image compression DCT help image to separate into different parts.DCT is similar to DFT. The difference between DCT and DFT is that DFT applies to complex numbers, while DCT uses just actual numbers. For real input data with even equilibrium DCT and DFT are equivalent. It is

easier and more efficient to regard DCT as set of basis function in the form of input array which can be stored and computed. The DCT basis function are illustrated below.Figure 4 show basis of DCT block function.

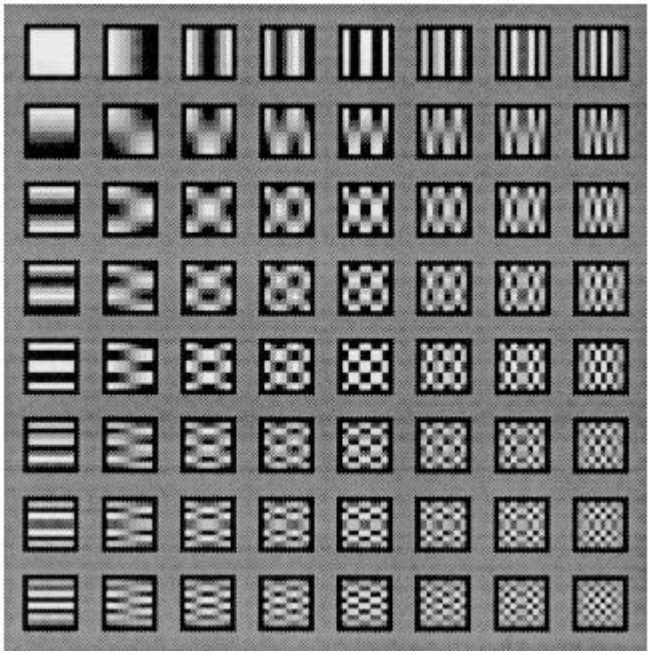


Figure 4: 8X8 example block DCT basis function [8]

Discrete Fourier Transform (DFT)

The Fourier transform is an analysis of global frequency content in the signal. There are applications in digital image processing wherein we need the restricted frequency components. This can be done by using the Short Time Fourier Transform. Then these wavelets are created by translation and dilation of fixed called as mother wavelets.

$$f(y,\propto) = \int_{-\infty}^{\infty} f(r)g(r-\propto)e_{dx}^{-jyx} \quad (3)$$

Where ‘y’ denotes the frequency and ‘alpha’ denotes the position of the window. This equation transforms the signal f(r) in a small window around ‘alpha’ [4]. The STFT is then performed on the signal and local information is extracted. The process can then be repeated iteratively to produce N scale transform.

Discrete Wavelet Transform (DWT)

DWT is a filters based system. It involves decomposition of image into a frequency channel of constant bandwidth. DWT is implemented with multilevel decomposition also. Level wise decomposition is done in different stages of DWT sub-band. At first level Image is decomposed into four different sub bands [9]. LL (Approximation sub-band) LH (Horizontal sub-band), HL (Vertical sub-band), and HH (Diagonal sub-band). The LL sub band can be decomposed further to obtain higher level of decomposition. These sub-bands are formed with the help of Haar-wavelet, basically Haar wavelet are simply considered to pair input values and produce desired output values. DWT also provide protection and confidently against various signal processing attacks. The watermark can also be embedded in the other three sub bands to maintain the quality of image as the LL sub-band is more sensitive to human eye [9].Figure 5 shows first level decomposition of dwt.

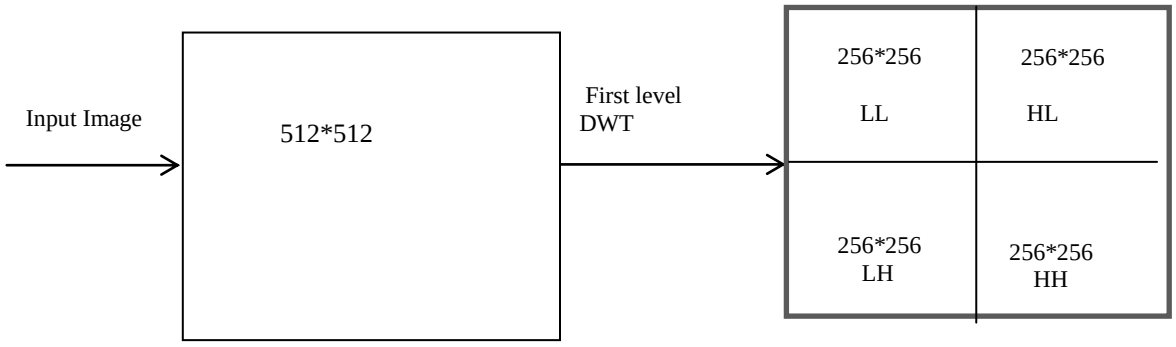


Figure.5 First level decomposition of input image [5].

One of the many advantages over the wavelet transform is that that it is believed to more accurately model aspects of the human visual system (HVS) as compared to other wavelet transform . This allows us to use higher energy watermarks in regions that the HVS is known to be less receptive to, such as the high detail bands {LH, HL, HH)

1.5 Applications of Watermarking:

The important applications of digital watermark are [1]:

- **Copyright Protection:** This is by far the most prominent application of watermarks. With tons of images being exchanged over insecure networks every day, copyright protection becomes a very important issue. Watermarking an image will prevent relocation of copyrighted images.
- **Contents Authentication:** Sometimes the ownership of the contents has to be verified. This can be done by embedding a watermark and providing the owner with a private key which gives him an access to the message. ID cards, ATM cards, credit cards are all examples of documents which require authentication.
- **Broadcast Monitoring:** As the name suggests broadcast monitoring is used to verify the programs broadcasted on different Television channel or radio. It especially helps the advertising the important notices of companies to see if their advertisements appeared for the right duration or not.
- **Content Labeling:** Watermarks can be used to give more information about the
- cover object. This process is named content labeling.
- **Tamper Detection:** Fragile watermarks can be used to detect tampering in an image. If the fragile watermark is degraded in any way then we can say that the image or document in question has been tampered.
- **Digital Fingerprinting:** This is a process used to detect the owner of the content. Every fingerprint will be unique to the owner.
- **Content Protection:** In this protection the content embossed with a visible watermark that is very difficult to remove so that it can be publicly and freely distributed.
- **Confidentiality of Medical data**: In protection of medical field digital watermark provides great security

1.6 Requirements of digital watermarking

The major requirements for digital watermark are [1]:

- **Security:** The security requirement of a watermarking system can differ slightly depending on the application. Watermarking security implies that the watermark should be difficult to remove or alter without damaging the host signal.
- **Imperceptibility:** The imperceptibility refers to the perceptual transparency of the watermark ideally, no visible difference between the watermarked and original signal should exist. A simple way to reduce distortion during watermarking process is embedding the watermark into the perceptually insignificant portion of the host signal. However, this makes it easy for an attacker to alter the watermark information without being noticed.
- **Robustness:** This is by far the most important requirement of a watermark. There are different types of attacks, unintentional (salt and pepper , Gaussian noise, speckle attack) and unintentional attacks which are aimed at destroying the watermark. So, the embedded watermark should be such that it should be resistant to various attacks. Watermark robustness accounts for the capability of the watermark to survive signal manipulations. Apart from malevolent attacks, different signal processing attacks can pose a threat to the detection of watermark, thus making it desirable to design a watermark that can survive those operations.
- **Capacity :** The capacity describes the maximum amount of data that can be embedded into the image to ensure proper recovery of the watermark during extraction.

As these characteristics are trying to hinder each other's effect, so in order to maintain a balance between them I have proposed a technique in term of robustness and imperceptibility**.**

1.7 Attacks

A watermark image is subjected to different type of manipulations and attacks. some intentional such as compression ,salt and pepper and some unintentional such as cropping, filtering etc[5]. Figure 6 shows different type of watermark attacks.

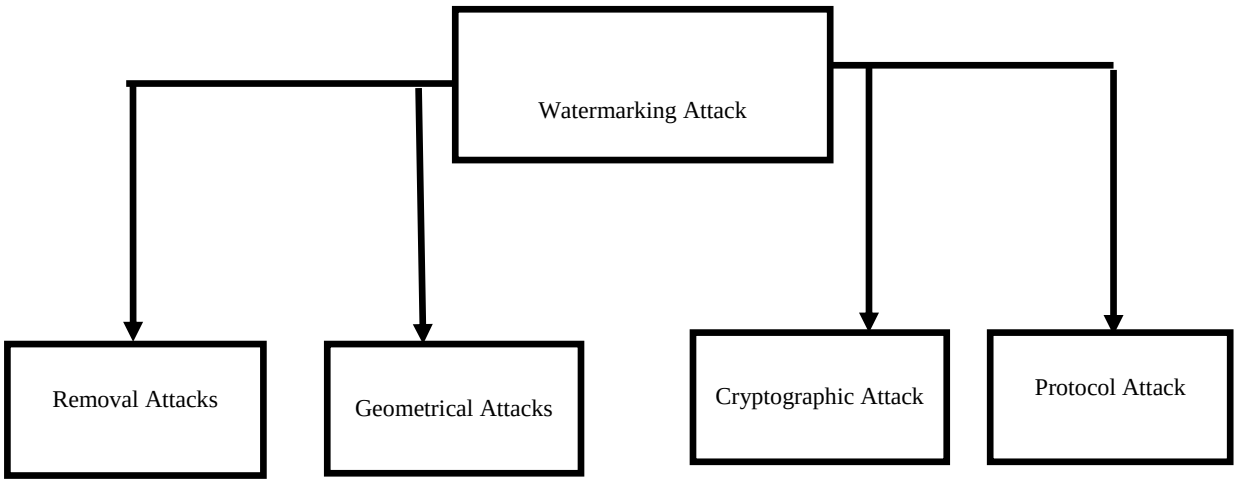


Figure6: Types of Watermark Attacks [5]

1.7.1 Removal Attacks

Removal attacks aim at the complete removal of the watermark information from the watermarked data without affecting the security of the watermarking algorithm (e.g., without the key used for watermark embedding). That is, no processing, , can recover the watermark information from the attacked data. This category includes demodulation, and collusion attacks. They never remove the watermark completely neither damage the watermark. Complicated removal attacks try to optimize operations like denoising or quantization to impair the embedded watermark as much as possible while keeping the quality of the attacked text high enough. Usually, arithmetical models for the watermark and the original data are exploited within the optimization process

1.7.2 Geometrical

In contrast to removal attacks, geometric attacks do not actually remove the embedded watermark itself, but intend to degrade the quality of watermark detector synchronization with the fixed information. The detector could recuperate the embedded watermark information when perfect harmonization is obtained back. However, the difficulty of the required harmonization process might be too great to be practical. However, most recent watermarking methods survive these attacks due to the use of special association techniques. Geometric attack is based on modification of histogram. Robustness to global numerical distortion often relies on the use of either a transform-invariant domain.. Robustness to global affine transformation is more or less a solved issue. Therefore, pixels are locally shifted, moved, and rotated without important visual distortion. However, it is worth noting that some recent methods are able to resist this attack.

1.7.3 Cryptographic

Cryptographic attacks aim at cracking the security methods in watermarking schemes and thus finding a way to remove the embedded watermark information or to embed misleading watermarks. A cryptographic attack is a method for finding a way for the security of a cryptographic system by finding a fault in a code, cipher, cryptographic or key management scheme. This process is also called "cryptanalysis". The, application of these attacks is restricted due to their elevated computational complexity.

1.7.4 Protocol

Protocol attacks aim at attacking the entire watermarking object. This can create vagueness with respect to the true civil rights of the data. It has been shown that for exclusive rights protection applications, authentication watermarks need to be not invertible. The requirement of viability of the watermarking technology implies that it should not be possible to extract a watermark from a non-watermarked document.

A solution to this problem might be to make watermarks signal-dependent by using one-way functions. Another protocol attack is the replicate attack. In this case, the objective **is** not to destroy the watermark or damage its detection, but to provide watermark from

watermarked data and duplicate it to some other data, called goal data. The approximate watermark is modified to the local features of the target data to satisfy its imperceptibility. The duplicate attack is applicable when a suitable watermark in the objective data can be produced with neither algorithmic knowledge of the watermarking technology nor knowledge of the watermarking key.

1.7.5 Active & Passive

Attacker removes or plunders the watermark. Attacker just try to identify the watermark.

1.7.6 Collusion

Attacker decodes dissimilar copies with different watermarks and joins them to make one solitary watermark.

1.7.7 Distortive

Attacker applies distortive modification to make the watermark undetectable by any other person & making it unreadable from the receiver end.

CHAPTER 2

Literature Background

Before getting into the details of the different compression and transform techniques variety of researchers and scholars have proposed their working research materials on watermarking that employees different transform techniques like SVD, DCT, DWT and a combination of spatial domain and transform domain techniques etc.
A brief review of current image watermarking methods is presented below

1. Van et al. [11] proposed watermarking technique for digital image In this technique, the LSB watermark is replaced with MSB of digital image. The limitations of the method is highly susceptible to noise, and less resistant to different signal processing attacks, and is easily destroyed when some dissimilar attacks are applied. The factor affecting watermarks are noise and different scaling transform. Gaussian noise, salt and pepper noise degrade image in transmission process

2. K.A.Navas et al. [12] proposed the watermark technique for medical image and with EPR embedded in region of non-interest image by using LSB technique. The advantage of this paper is that it has high capacity and invisibility .

3. Nyanja Dewy et al. [13] proposed a DWT based stenographic technique. Cover image is decomposed into four different sub bands using DWT for the purpose of watermarking. Encoded Secret image is hidden using spiral scanning and alpha blending technique is used in HH band.

4. Maratha et al. [14] proposed a new approach to cover the watermark according to the characteristics of the human visual system (HVS). In contrast to conventional methods operating in the wavelet domain, covering is accomplished pixel by pixel by taking into account the texture and the luminosity content of all the image sub bands. This method is

more strong than other different signal processing attacks but multifaceted than any other transform.

5. Muhammad arsenal et al. [15] proposed a reversible watermarking method using Genetic Algorithm (GA) to solve the optimization problem. An intelligent reversible watermarking approach GA-Rev watermarking method for different medical images is proposed. GA-Rev watermarking method is based on the idea of block-based embedding of watermark using GA and integer wavelet transform (IWT). GA based quick threshold assortment system is applied to improve the imperceptibility for a fixed payload or vice versa. The experimental results show that GA-Rev WM provides significant improvement in terms of imperceptibility for a desired level of payload against the existing approaches.

6. A.kannammal et al. [16] proposed a technique by two-level securities to medical images using watermarking and encryption. Watermarking is performed using wavelet filter banks, which have the capability to expose singularities in different direction. The medical image is taken as watermark and it is embedded in each LH sub band of the original image using LSB watermarking method.. To extract watermark now inverse discrete non-tensor is applied on watermarked embedded image to get watermark image. Watermark is encrypted using symmetric and asymmetric encryption algorithm. For decryption private key is used and LSB is applied to get medical image back**.** The limitation of this paper is that RC4 is better than AES and RSA algorithm**.**

7. Mohammad et al. [17] proposed a fragile watermarking scheme that uses bit budget to detect tamper in medical images, based on hamming code. Hamming code uses parity bits to detect and correct errors in data, and provides images substantiation and verification. The host image is disintegrating into different blocks and verification is performed block wise so that they can easily localize tampers. For security purposes two keys are used to choose pixels that should take part in hamming code. As first key is used to choose 4 pixels of each block of an image and second key is used to select different pixels of an image, so parity bits can be inserted into it. For extraction purpose they have used first key and second key to find received vector R. Hamming code use parity bits to detect and correct errors in data. These parity bits are added actual during encoding

and are removed during decoding. Syndrome vector is used to identify the fault and if it is equal to zero vectors “no errors have occurred”.

8. Akiyoshi Wakatani et al. [18] proposed a technique of embedding signature images into areas other than region of interest. In this paper autograph of person is compressed by progressive coding algorithm which is used as signature information. In this paper signature image with moderate quality can be acquired from clipped image including only part of the ROI.In this paper the most important part of the signature is embedded into pixels nearest to the ROI part. Thus part of the image clipped from the other part of the main image include the ROI can produce the signature image with moderate quality. Haar is the simplest wavelet which is used. Here ROI contain small portion of the signature image.

9. Joan Pupate et al. [19] proposed a new technique based on fractal coding and decoding. It exploits the spatial redundancy within the image relationship among different parts of fractal image. Digital signature is use to modify fractal appearance of the image.IFS exploit the connection between whole image and its part, thus exploiting the similarities that exit between an image and its smaller parts.

10. Fuisal Alturki et al. [20] proposed a fragile digital watermarking technique, which can be used as a digital signature for data authentication and copyright. This technique is suitable for different class of image formats such as png , jpeg or bitmap images. The digital signature is inserted into spatial domain of the image, then the watermark is embedded into transform domain. The tampering in the watermarked image will create errors in the embedded image, the error in the embedded image will be easily detected. The watermark acts as a digital signature which breaks any modification applied to the image. The main disadvantage of this approach is that it is not robust against lossy compression attack and is not resistant to different signal processing attack and does not provide any information about different type of attacks.

11. Russell Mersereuu et al.[21] proposed a wavelet packets-based robust blind watermarking scheme using chaotic encryption .Two different chaotic sequence are

modulated accordingly characters of chaotic system are used for image extraction and encryption. The watermark information is changed into one dimension sequence by arithmetic modulation .They make use of blind extraction because extraction watermark does not need original cover image. The major advantage of this paper is

(1) Good invisibility as they are tested with images having higher PSNR.

(2) Good security, two chaotic sequences are used, one is use to encrypt watermark and other is to extract watermark image.

(3) Good power and good quality of image are used in JPEG compression .

(4) Blind watermark scheme is used because extraction of watermark does not need original cover image. They are resistant to different signal processing attack, and watermark has good invisibility and security. This proposed technique is used in exclusive rights and authentication purpose.

12.Rig Das et al. [22]proposed a novel technique for image steganography based on Huffman encoding. Two 8 bit gray-level images are used one as cover and secret image is used. Huffman encoding is embedded inside the secret message before embedding and each bit of Huffman code of secret message is embedded inside the cover image by swapping the LSB of each pixel intensities of over image. The limitation of this paper must have high capacity and good invisibility.

13. Adiwijaya et al. [23] propose a scheme for medical image which easily help doctors to diagnose the patient. Medical image is divided into two parts ROI and RONI, the LSB pixels of ROI image is compressed with the help of Huffman compression, and then stores in RONI region. A compressed LSB using Huffman will be inserted in the RONI region as twice of LSB's bit. In Table1 summary of different wavelet techniques are described.

Table 1: Summary of existing wavelet based watermarking techniques

	Author name/Year	Technique Used	Watermark Type	Result
1	Ju Lei ,Sui Zhiyuan, Fang Yong/2011	DWT	Text	ElDM use to measure visual distortion
2	Salwa A.k.Mostafa et al	DWT And DWPT	EPR data as Text watermark	MRI1 :PSNR=31.272 BER=0 NC=1
3	K.A.Nawas,S.Arachna Thamphy,and M.sasiku et al/2008	IWT	Image	WPSNR is 53 db which says embedded image is less distorted
4	Deepti Anand ,Niranjan/1998	LSB	Text	CT Scan , MNRMSE=0.0092 Angiogram MNRMSE=0.023
5	Muhammad Arsalan,Sana Ambreen Malik/2011	IWT	Digital Image	Lena SSIM= 0.9940 at Payload 0.1 Babar SSIM=0.9933 at Payload 0.2

6	A.kannammal,S.Subha Rani/2013	LSB	Medical Image	Pepper, PSNR=86.06 NC=1 CV=0.01
7	Mohammad Arabzadeh ,Habibollah Danyali/2010	LSB and Hamming code	Medical Image	MRI PSNR=64.3381 db. CT=64.5022 db. FAR ratio: RI=0%,CT=0%
8	Akiyoshi Wakatani	Haar wavelet	Digital Image	Patterns of division: A:19 db. B:17.87db C:NG

CHAPTER 3

Digital Image Watermarking using Lossy Compression Techniques

The proposed work in my thesis is an algorithm for digital image watermarking based on discrete wavelet transforms (DWT) and block truncation coding (BTC) has been proposed. In the embedding process, the host image is decomposed into first level DWT and the watermark image is compressed by BTC. The compressed watermark is then embedded into the selected sub-band of the host image. The proposed method has been extensively tested against numerous known signal processing attacks and has been found to be robust and highly imperceptible. Further, the performance of the algorithm has been tested with fractal compression technique. The performance of BTC is better than fractal compression in terms of imperceptibility and robustness.

3.1 Block Truncation Coding (BTC)

BTC is a loss compression technique used for gray scale images which was proposed by Delp and Mitchell [27]. In this technique the image is divided into blocks of m pixels and each block is processed separately. The mean value (μ) and the standard deviation (σ) are calculated for each block and first two sample moments are preserved in compression. The original pixels of a block is encoded into a bit plane(A),where pixels with value less than the mean value are set to '0'and those having value greater than are equal to the mean value are set to'1'[27-31].The block is decompressed according to triple(μ,σ, A) .The bit '0' of A is set to b and the bit '1' of A is set to c where b and c are represented as mean and standard deviation and are computed according to equation (1) and (2) and q stands for the number of bits'1' in A.

$$b = \mu - \sigma\sqrt{\frac{q}{m-q}} \tag{4}$$

$$c = \mu + \sigma\sqrt{\frac{m-q}{q}} \tag{5}$$

In this paper BTC is applied on different bands of DWT sub-bands and result are shown below experimentally.

3.1.1 Fractal Compression Technique

Fractal is one of the best methods to describe natural modality in the process of transformation and iteration. Fractal image compression is also called as fractal image programming because compressed images are represented by different transforms. In Fractal compression image is divided into non-overlapping domain blocks [36].This type of relation is closely related to quad-tree decomposition. It resembles parent-child relationship. In it tree like structure is formed. This method is best suited for textures and natural images, where one part of image results other part of the same image [37]. Fractal algorithm converts the parts of fractal image into mathematical data called 'fractal codes 'which are used for recreation of encoded image. It is mathematically represented as iterated function system (IFS)

3.2 Performance Measures: The performance of the watermarking algorithm can be evaluated on the basis of its robustness and imperceptibility. A larger peak signal to noise ratio (*PSNR*) indicates that the watermarked image more closely resembles the original image meaning that the watermark is more imperceptible. Generally, cover image with PSNR value greater than 28 is acceptable [24-26]. PSNR is defined as

$$\text{PSNR}=10 \times log \frac{255\times255}{MSE} \quad (6)$$

Where the mean square error is defined as

$$\text{MSE}=\frac{1}{A\times B}\sum_{i=1}^{A}\sum_{j=1}^{B}\left(C_{ij} - D_{ij}\right) \quad (7)$$

Where C_{ij} is a pixel of the original image of size $A\times B$ and D_{ij} is a pixel of the watermarked image of size $A\times B$,the robustness of the algorithm is determined in terms of correlation factor.

Normalized Correlation: The NC gives a measure of the robustness of watermarking. After extracting the watermark, the normalized correlation (NC) is computed between the original watermark and the extracted watermark using Eq. (5). This is used to predict the existence of the watermark and to measure the correctness of the extracted watermark.

$$NC = \frac{\sum_{i=1}^{A}\sum_{j=1}^{B}(D_{originalij} \times D_{recoveredij})}{\sum_{i=1}^{A}\sum_{j=1}^{B} D2_{recoveredij}} \quad (8)$$

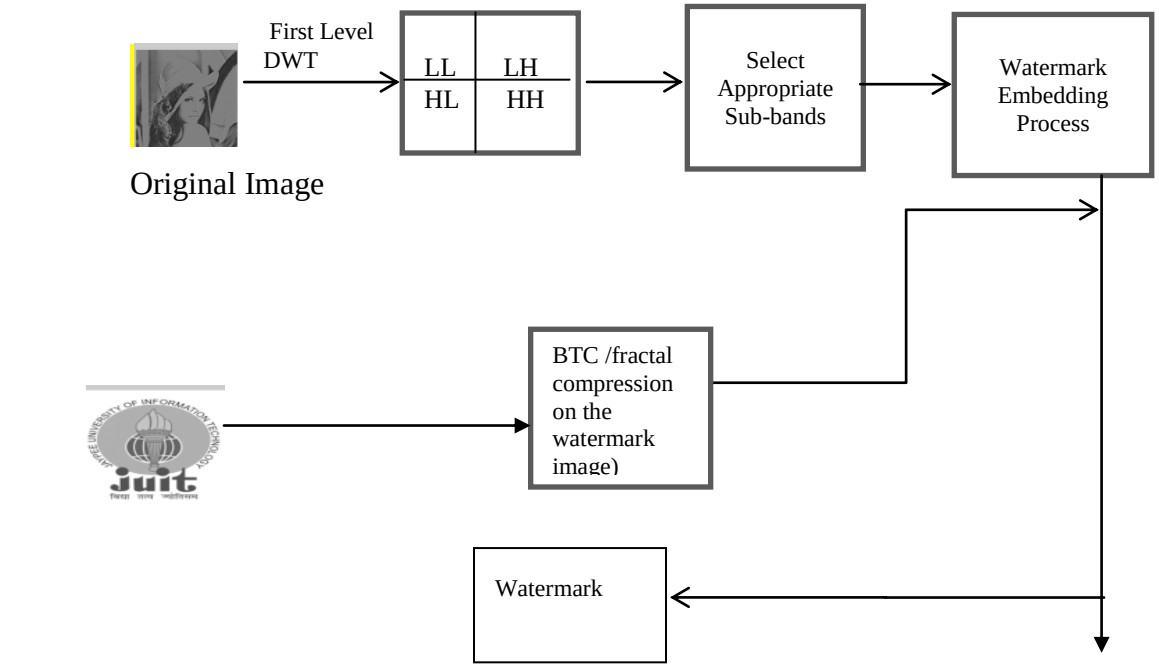
Where $D_{originalij}$ is a pixel of the original watermark of size $A \times B$ and $D_{recoveredij}$ is a pixel of the recovered watermark of size $X \times Y$

3.3 Proposed Algorithm

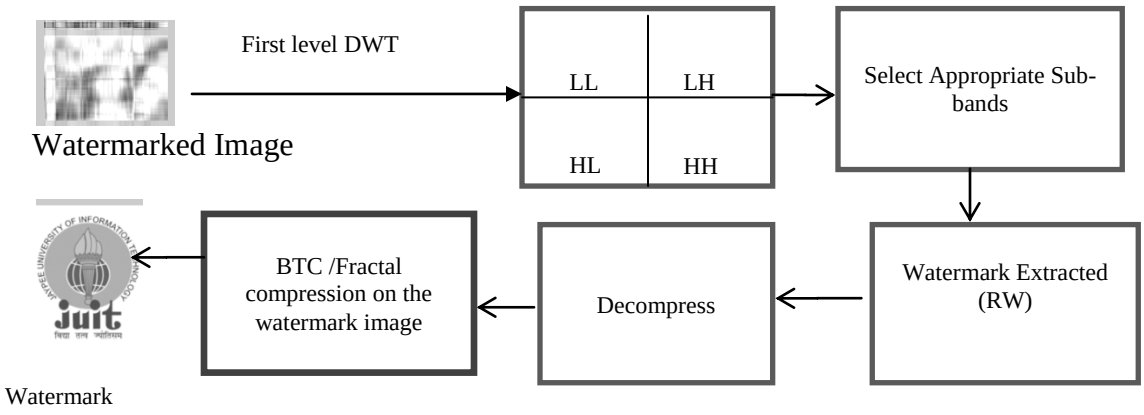
The watermark embedding and extraction method can be shown in Figure 7a and Figure 7b, respectively. The proposed algorithm has two parts: (1) embedding and (2) extraction for image watermark as given below:

a. **Embedding Process**: In the embedding process, the host image is disintegrating into first level DWT. Then any appropriate selected sub-band is taken and watermark image is compressed with the help of BTC and Fractal compression technique. The compressed watermark is then embedded into the selected sub-band of the host image. The embedding between compressed watermark image and host image is done with the help of gain factor $\propto$, which is varied accordingly from 0.1 to 0.9. The proposed method has been extensively tested against numerous known signal processing attacks and has been found to be robust and highly imperceptible

b. **Extraction Process:** The reverse processing of embedding process is us



(a)



(b)

Figure 7: Watermark (a) Embedding and (b) Extraction

3.4 Experimental Results

We have described the performance of combined DWT and BTC based watermarking method. We are using gray scale images of Lung as original image of size 256× 256 and JUIT logo image as watermark of size 256× 256. The image watermark embedding method is based on DWT and BTC Then the comparison of our proposed BTC compression technique is done with fractal compression technique. Figure 8: shows effect of BTC on different type of cover ,watermark image ,watermark compressed, watermarked image.

(a) (b) (c) (d)

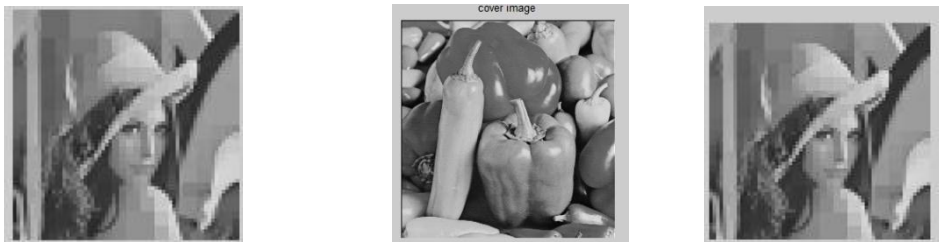
Figure 8 (a)Cover image (b)Watermark Image (c)Watermark compressed with BTC (d)Watermarked Image .

In the above experiment,BTC is a lossy compression technique for and divide image into many non-overlapped blocks, each image is represented by two distinct values.BTC preserves the first and second order moment character of the original image.BTC has to preserve the first and second moment characteristics of the original block.BTC cannot provide coding gain as other compression techniques.BTC have to preserve the moment characteristics of the original image.BTC improves the quality of the image .BTC is approximately good solution for image/video compression with an extremely low complexity. In figure(a) cover image is taken and watermark is compressed with the help of BTC technique. It is a lossy compression technique for gray scale image ,then compressed watermark is embedded into cover image with the help of gain factor which varies from 0.01 to 0.09 .This compressed watermark is tested against different signal processing attack. Figure 9 shows effect of fractal compression on cover image,

watermark image,quadtree decomposition, decompressed watermark image, watermarked image and watermark extracted

(a) (b) (c)

Figure 9 (a)Cover image (b)Watermark image (c) Quad tree decomposition of Watermark Image



(d) (e) (f)

(d) Decompressed watermark Image (e)Watermarked Image (f) Watermark Extracted

The experimental results for fractal compression are performed in mat lab, as it is a loosy compression technique**.** Lossy compression technique used is fractal compression technique. It is a class of data compression algorithms that can be obtained by dividing original grey level image into un overlapped blocks depending on the threshold value of 0.3.Fractals are easily found in nature. They display self-similar structure over an extended, but our limited scale range[30].Example flakes of snow ,clouds ,crystals and mountain. In fractal compression, image is divided into number of different square blocks called range. Further the image is divided into bigger square blocks, called domain blocks ,which are usually four times larger than the range block[31].It is valuable due to high Compression ratio. It permit reconstruction of original data, and try to reduce compression rate, the decoded part of image is independent of the reconstructed of the image quality. when using Fractal compression technique watermark is compressed, by lossy compression technique and then embedded into cover image using different gain

factors. The watermarked image is obtained should be dead set against different signal processing attacks. Lossless compression data provide reconstructed image same as original image.JPEG is a lossless compression technique.

Table 2: Performance of the method at different gain factor without any attack.

Gain Factor(k)	PSNR	NC
0.1	52.56	0.94
0.3	51.4	0.96
0.5	49.5	0.97
0.7	46.56	0.99
0.9	44.38	1

In Table 2 gain factor k is varied from 0.2 to 9. We have implemented proposed algorithm in MATLAB. The performance of the proposed algorithm is evaluated in terms of imperceptibility and robustness against various signal processing attacks. The PSNR is used to measure the quality of the watermarked image. However, robustness of the extracted watermark is measured by NC. The maximum PSNR has been obtained at gain factor 0.1. However, the maximum NC value has been obtained at gain factor 0.9. We have found that the larger the gain factor, stronger will be the robustness and smaller the gain factor better will be the image quality.

Table 3: Performance of PSNR method at different gain factor and different sub-band

Gain Factor (K)	PSNR				NC
	LL	LH	HL	HH	HH
0.1	33.52	33.15	34.92	38.45	0.97
0.2	32.15	30.13	31.19	34.34	0.98
0.3	28.83	29.84	29.81	30.14	0.99

In Table 3, PSNR value for different sub-bands are calculated at different gain-factors The highest PSNR value is 38.45 obtained at HH sub-band with gain-factor 0.1 and the NC of HH(sub-band) is taken. The maximum NC in HH sub-band is 0.99 obtained at gain-factor 0.3, showing that our method is robust and PSNR decreases with increase in Gain factor.

Table 4: Performance of the proposed method between different block size, PSNR, and NC at constant gain factor=0.1

Block size	PSNR	NC
2*2	44.25	0.96
4*4	41.1	0.97
6*6	37.04	0.98
8*8	35.12	1

In table 4 it is clearly shown that on keep gain factor constant and having different block size, PSNR decreases and robustness increases. The highest PSNR value is 44.25 obtained at block size 2*2, and highest NC value 1 is obtained at block size $8 * 8$., which is equal to 1.

Table 5: Comparison between BTC and Fractal compression of our proposed algorithm

Gain Factor(k)	BTC Compression		Fractal Compression	
	PSNR	NC	PSNR	NC
0.1	39.17	0.95	33.14	0.84
0.4	36.15	0.96	28.87	0.87
0.7	33.43	0.98	27.87	0.90

In table 5 it is clearly shown that on increasing block size PSNR decrease in case of BTC and Fractal compression. It is observed that BTC provide better result when compared to Fractal compression technique. These compression techniques provide better results and better performance in terms of image quality. This way we can demonstrate how our BTC compression technique is better than any other compression technique.

Table 6: Performance of NC at LL sub-bands against different attacks at gain-factor 0.01

Attacks	NC
Brightness attack	0.94
Rotation attack	0.93
Contrast attack	0.96
Salt and Pepper	0.95
Gaussian Noise	0.93

In Table 6 Performance of NC value on LL sub-band at constant gain factor when different attack is applied. The maximum value of NC is 0.96 and is obtained in case of Contrast attack when gain factor is 0.01.

3.5 Performance analysis of the proposed method for different attacks

Salt and Pepper

Salt and pepper noise is a form of noise which is sometimes seen on different images. It occurs in the form of white and black pixels. An efficient noise reduction method for this type of noise is a median filter or morphological filter[34]. For reducing the effect of salt –pepper noise, but not both ,a contra-harmonic mean filter can be effective. In this way embedded watermark is exposed into salt and pepper noise with.

X=imnoise ('Y',salt & pepper',D) where Y' is the watermarked image

adds "salt and pepper" noise to the image Y,where D is the noise density. Here D varies from 0.2 to 0.9, and we can easily see the effect in image. Figure 10 shows the effect of salt and pepper noise on the watermarked image.

Figure10: Effect of salt and pepper noise on watermarked image

Speckle Noise

Speckle is a granular ‘noise’ that exist in and degrade the quality of images which are in the form of active radar, synthetic aperture radar (SAR) images, medical ultrasound and optical tomography images.

Speckle noise occur in form of a common phenomena called as speckle. It occurs due to interference of the returning wave from their sources at the transducer aperture. These are basically scattered signal add coherently, i.e. they are added constructively and destructively depending on the different phase of different wavelets. The mean gray level of local area is increased. Speckle noise in case of SAR is serious, causing difficulties for images to interept.It is caused by coherent processing of backscattered signal. At times speckle contain practical information, when it is associated with laser speckle and dynamic speckle, where changes are measured in time. . Figure 9 shows the effect of speckle attack on the watermarked image.

Figure 11: Effect of speckle noise on watermarked image

Rotation attack

This attack try to destroy the synchronizations of the watermark detectors and the watermarking, even a slight rotation may change the detection of watermarks. Resize of rotation attack is based on the combination of the Zernike moments and singular value decomposition (SVD) [34].This may cause partitioning of DWT and decompose SVD to lower frequency components. Due to rotation attacks image is rotation through different angles, by using syntax imrotate (I1, different angles ‘loose’, bilinear)

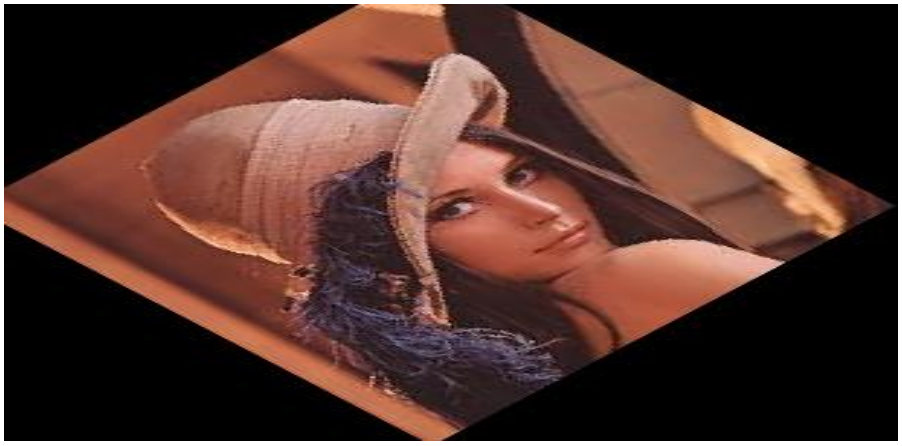


Figure12: Rotation done at an angle of 45 degree

Figure13: Rotation done at an angle of 75 degree

Due to rotate attack image is rotated through different angles in which we want

3.6 Conclusion

In this technique, we proposed a new approach for digital image watermarking. The DWT and BTC are proficient techniques used for watermarking so there combination makes a very attractive watermarking technique. Due to the excellent properties of DWT, the DWT is suitable to identify the area in the cover image where watermark can be embedded easily. One of the best properties of BTC are that larger blocks allow greater compression, and quality gets reduced with increase in block size due to the property of this algorithm. So, the proposed hybrid technique improves the robustness and imperceptibility as compared DWT and BTC individually. The main properties of the proposed work can be identified as follows: (1) In the proposed method we have embedded compressed watermark into different sub-bands of host image and desired results are obtained. (2) The image quality of traditional BTC is used for configurations of high coding gain, where the energy-preserving property is exploited to effectively remove the false contour and blocking effect inherently exist in BTC images.(3) BTC uses a two-level nonparametric quantizes that adapt to basic properties of image. This quantizes produces high-quality quality of images that appear to enhance data rates of 2.5 bits/picture element. (4) BTC based watermarking technique is better than Fractal based compression technique in terms of robustness and watermarked image quality. Moreover, the efficiency can also be improved by replacing the high and low means with the maximum and minimum value of block size of BTC.

We would like to further improve our performance, which will be reported in future Communication. One of the efficient properties of BTC that larger blocks allow greater compression, and quality gets reduced with increase in block size due to the property of this algorithm. So, the proposed hybrid technique improves the robustness and imperceptibility as compared DWT and BTC individually. The main properties of the proposed work can be identified as follows: (1) In the proposed method we have embedded compressed watermark into different sub-bands of host image and desired results are obtained. (2) The image quality of traditional BTC is used for configurations of high coding gain, where the energy-preserving property is exploited to effectively remove the false contour and blocking effect inherently exist in BTC images.(3) BTC uses a two-level nonparametric quantizes that adapt to basic properties of image. This quantizes produces good quality of images that appear to enhance data rates of 2.5 bits/picture element. (4) BTC based watermarking technique is better than Fractal based compression technique in terms of robustness and watermarked image quality. Moreover, the efficiency can also be improved by replacing the high and low means with the maximum and minimum value of block size of BTC.

Chapter 4

Digital Image Watermarking using Lossless Compression Techniques

The proposed work in my thesis is an algorithm for digital image watermarking based on discrete wavelet transforms (DWT) and Huffman coding has been proposed. In the embedding process, the host image is decomposed into first level DWT and the watermark image is compressed by Huffman. The compressed watermark is then embedded into the selected sub-band of the host image. The proposed method has been extensively tested against numerous known signal processing attacks and has been found to be robust and highly imperceptible.

4.1 Introduction

A Watermark embeds an imperceptible signal to audio, video and image for variety of purpose including copyright protection and violation. However, the working principles of watermarking and compression seem to be different as perceptual data coding removes inherent redundancy during compression. Image Compression is a well known topic that codes picture into fewer amounts of data. There are two kind of image compression techniques: Lossless and Lossy Image. Lossless image compression are error-free coding methods .It can decompressed into one which is the original image .Since lossless compression keep all the information in image ,the size of the compressed results are not reduced so much. Most common examples of lossless compression are Huffman compression, arithmetic compression, run length coding etc. Lossy image compression techniques produce results with little distortion and image obtained from decompressing is not same as the original one [34]. Most common example of lossy compression are BTC, Fractal compression, JPEG compression. Lossy compression is use to compress multimedia data especially in streaming of data and used in internet telephone. Whereas lossless is used in text and data files, Compression plays very important role in image processing when we want to send large images on the internet [35]. Generally threat to the image is increased on the internet, so compressed image is send to make optimal use

of network band-width. However, the image can be distorted on open channel. To make sure that the correct image is being delivered at the receiver end, so we embed watermark to the image. Image storage and transmission have created an important and increasing part for the compression techniques. The main aim of compression is to reduce the number of bits as much as possible, while keeping the pixel resolution and the visual quality of the reconstructed image as close to the original image as possible. The redundancy and similarity among different images make compression easy.

4.2 Huffman Compression

Huffman coding algorithm is one of the best Known algorithms for lossless data compression. In Huffman the code must have a prefix property, that code of one symbol should not be a prefix of another code. Huffman's algorithm is a greed approach, by greedy approach we mean, it is an algorithm that follows the problem solving heuristic of making the local optimal choice at each stage with the hope of finding global optimal prefix-free binary codes[36].

Huffman's algorithm is based on the idea that a variable length code should be used for smallest code words and longest codeword for the least likely symbols. Due to this technique the average code length is reduced .The algorithm assign code words to particular symbols by constructing a binary code tree of that symbol. Each symbol of alphabet is a leaf of the coding tree. The code of a given symbol represents a exclusive path from the root to that leaf ,with 0 or 1 added[37].The leaf which is on the left side of the root of Huffman binary tree is 0,and leaf which is on the right side of the root of Huffman binary tree is 1 and is assigned to it along the path. In this paper Huffman is applied on different bands of DWT sub-bands and result are shown below experimentally. Huffman's algorithm constructs a binary coding tree in a greedy fashion, starting with the leaves and repeatedly merging the two nodes with the smallest probabilities [36]. Then further merge two more nodes with probability more than the previous node merged. A priority row is used as the main data structure to store the nodes. The root will have probability of highest symbol along the path

The pseudo code appears below.

Algorithm 1: Huffman Coding

Step1: Input: Array E[1...n] of numerical frequencies or probabilities.

Step2: Output: Binary coding tree with n leaves that has minimum expected code length for E Huffman (E[1...n])

Step3: S = empty binary tree

Step4: Q = priority queue of pairs (i, E[i]), i = 1...n, with f as comparison key

Step5: for each r = 1...n − 1

Step6: i = extract Min(Q)

Step7: j = extract Min(Q)

Step8: E[n + r] = E[i] + E[j]

Step9: insert Node(S, M + r) with children i, j

Step10: insert Rear (Q,(n + r, E[n + k]))

Step11: return T

4.3 Huffman Encoding.

Huffman codes solve the problem of finding an favourable codebook for an arbitrary probability distribution of different symbols .In Huffman coding ,a compressed string of symbols will be the message of particular code and its alphabet will be the original or message alphabet. The compressed output will consist of different symbols.

A code is called as string of output symbols associated with a message symbol and a codebook will be set of all codes associated with all symbols in the message alphabet. A. Huffman's algorithm produce optimal code for symbol-by symbol coding with the probability of symbol known, it is not optimal when the probability of symbol is not known ,as there might exist many equivalent codebooks, none will have a less length normal than average code length. Huffman coding is a "variable –length codes" really means variable –integer-length codes. Huffman in his landmark 1952 paper [38] give the procedure to build optimal variable length codes given an arbitrary frequency distribution for a finite alphabet. They make the codebook favourable. The condition to be fulfilled is as follows:

(a) No code should be prefix of another code.

(b) No auxiliary information is required to be delimiter between codes.

The Huffman encoding algorithm starts by constructing a list of all the alphabet symbols in descending order of their probabilities. It then constructs, from the bottom, a binary tree with a symbol at every leaf. This is done in different steps, where at each step two symbols with the less probabilities are combined, similarly then next two are added with less frequency than the previous one, so in this way they are added to the top of the partial tree, deleted from the list of tree, and replaced with an supplementary symbol representing the two original symbols [25]. When the list is reduced to just one auxiliary symbol (representing the entire alphabet), the tree is complete. The tree is then traverse to determine the code words of the symbols.

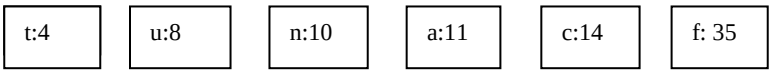
4.4 Huffman Decoding

Before starting the compression of a data file, the encoder has to determine the particular codes which have to be decoded. It does that based on the probabilities of different frequencies of occurrence of the symbols. The probabilities or different frequencies of symbols have to be written separate, as side information, on the output, so that any Huffman decoder will be able to decode the data easily. This is easy, because the frequencies are represented in the form of integers and the probabilities can be written in the form of decimal. It normally adds just a few little hundred bytes to the output. It is also possible to write the different variable-length codes themselves on the output, but this may be problem, because the codes have different sizes and different frequencies. It is also possible to even write the Huffman tree on the output [39], but this may requires more space than the usual space required by just few frequencies for decoding. . In any case, the decoder must know what is at the beginning of the compressed file, read it, and construct the Huffman tree for that particular alphabet. Only then it is possible for reader to read and decode the rest of its input. The algorithm for decoding the Huffman is simple as compared to other lossless compression techniques. Start at the source edge of the tree and read the first bit off the input (which is the compressed file). If it is zero, follow the base edge of the tree; if it is one, follow the peak edge of the tree. Read the subsequent bit and move another edge toward the leaves of the tree. When the decoder arrives at a leaf,

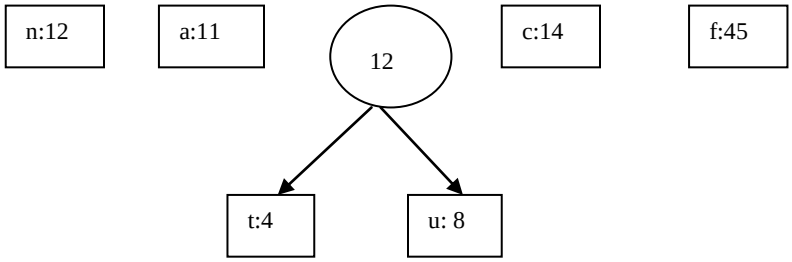
it will automatically finds there the original, uncompressed symbol, which is in the form of ASCII symbols and that code is emitted by the decoder. The process starts again at the origin with the next bit to encounter.

4.5 How does it work

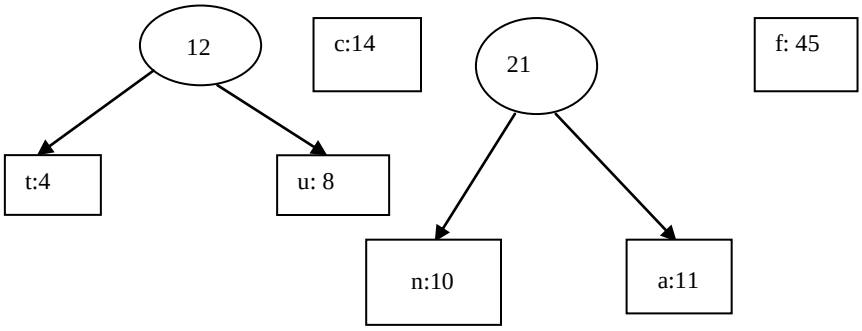
Assume a file that contains 100 characters built out of 6 different letters with the following frequency [27]. ‘f’: 35, ‘a’: 11, ‘n’: 10, ‘c’: 14, ‘u’: 8 and ‘t’: 4 The Huffman algorithm creates a Huffman Tree as follows:



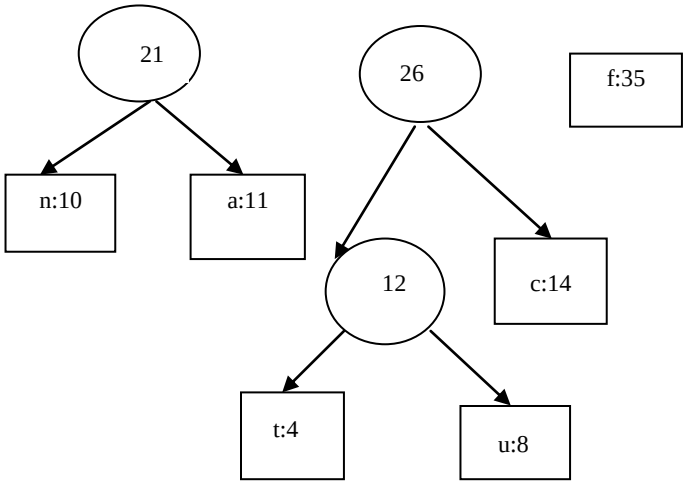
(a)



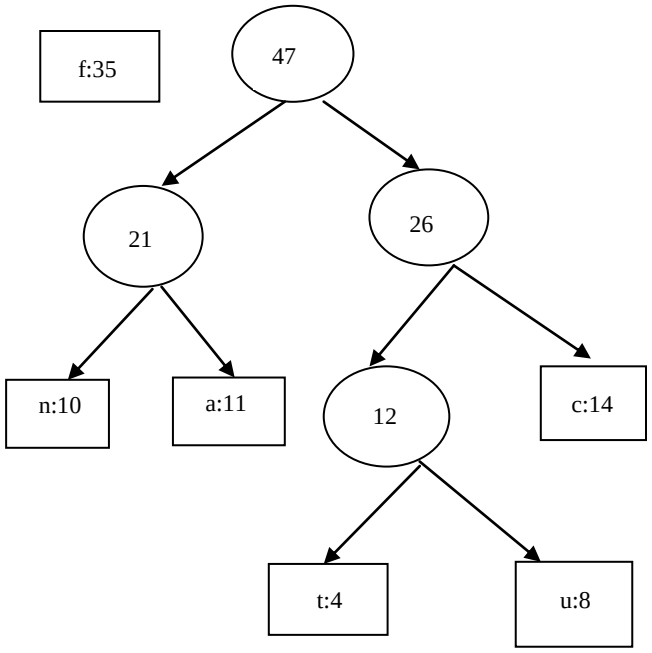
(b)



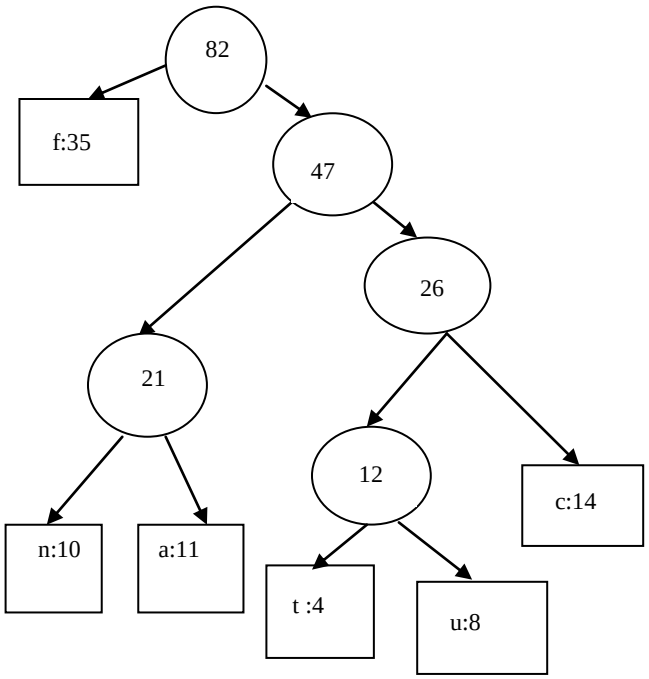
(c)



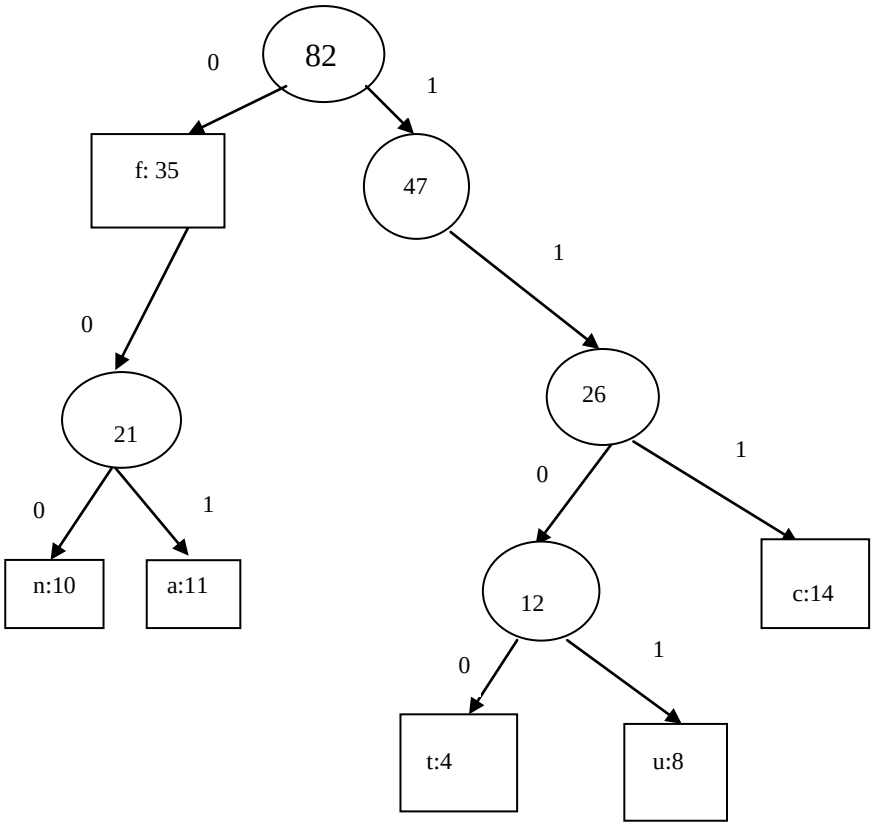
(d)



(e)



(f)



(g)

Figure: 14 Huffman Principle (a) Initial (b) First iteration (c)Second iteration(d)Third iteration(e)Fourth iteration (f)Fifth iteration (g) Sixth iteration

This way we construct Huffman codes. An edge connecting an internal node with its children is labelled "0''if it is an edge to the left child ,and "1",if it is an edge to the right child .The Huffman code for a character c is the sequence of edges connecting the root to the leaf for that characters.

Therefore, we encode it follow:

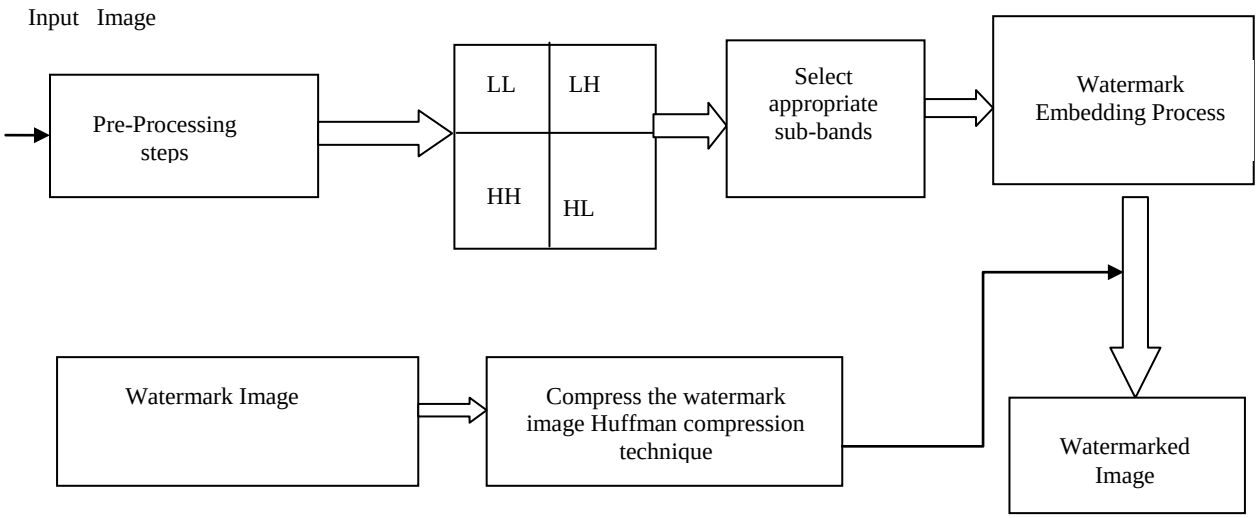
F: 0
a: 101
n: 100
c: 111
u: 1101
t: 1100

The compression ratio can be calculated as follows .We start with the ASCII encoding. Every character in the encoding process requires 8 bits .Thus a text containing 1000 characters has a size of 8000 bits or 1000 bytes. Thus number of bits required using the Huffman code is 35*1+11*3+10*3+14*3+8*4+4*4=35+33+30+42+32+16=1,504 bytes which yield a compression ratio of 27%

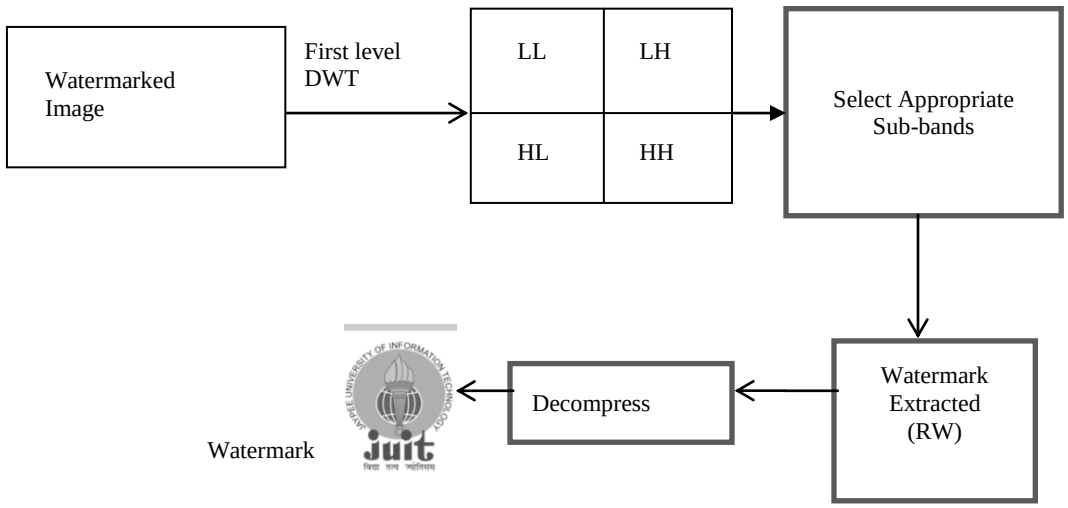
4.6 Proposed Algorithm

The watermark embedding and extraction method can be shown in Figure 12a and Figure 12b, respectively. The proposed algorithm has two parts: (1) embedding and (2) extraction for image watermark as given below:

a. **Embedding Process**: In the embedding process, the host image is decomposed into first level DWT. Then any appropriate selected sub-band is taken and watermark image is compressed with the help of Huffman compression technique. The embedding between compressed watermark image and host image is done with the help of gain factor∝, which is varied accordingly from 0.1 to 0.7. The proposed method has been extensively tested against numerous known signal processing attacks and has been found to be robust and highly imperceptible
b. **Extraction Process:** The reverse processing of embedding process is used for the extraction of watermark image.



(a)



(b)

Figure 15: Watermark (a) Embedding and (b) Extraction process

.

4.7 Performance Metrics

The performance of a lossless image compression algorithm can be specified in terms of compression efficiency and complexity. Compression efficiency is measured by the compression ratio or by the bit rate .Compression ratio is the size of the original to the compressed image, and bit-rate is the number of bits that are processed per unit time, is required by the compressed image. For example a 256×256 medical image is taken ,8-bit per pixel imae requires $256\times 256 = 65536 \times 8\text{bits} = 65{,}536$ bytes when stored in uncompressed form. If the compression image requires 32769 bytes, then the compression ratio is given by 65536÷32769=1.9.

4.8 Experimental Results and analysis

We have described the performance of combined DWT and Huffman based watermarking method. We are using gray scale images of medical image as original image of size 512×512 and JUIT logo image as watermark of size 256×256. The image watermark embedding method is based on DWT and Huffman .Figure 16 shows cover image, watermark image, watermarked image and extracted watermark

(a) (b) (c) (d)

Figure 16(a) Cover image (b) Watermark (c) Watermarked Image (d) Extracted Watermark**.**

The experimental results for Huffman compression are performed in mat lab, lossless compression technique is used**.** Lossless compression technique used is Huffman compression technique. It is a type of data compression algorithms that allows original data to be reconstructed from the compressed data without any lost in data.It permit reconstruction of original data ,and try to improve compression rate. The embedding between compressed watermark image and host image is done with the help of gain

factor∝, which is varied accordingly from 0.1 to 0.9.. The watermarked image is obtained which is resistant against different signal processing attacks.

Table 7: PSNR and NC performance of the proposed method at different gain factor without any attack.

Gain Factor(k)	PSNR	NC
0.1	52.56	0.94
0.3	51.4	0.96
0.5	49.5	0.97
0.7	46.56	0.99
0.9	44.38	1

In Table 7 gain factor k is varied from 0.1 to 9. We have implemented proposed algorithm in MATLAB. The performance of the proposed Huffman algorithm is evaluated in terms of imperceptibility and robustness against various signal processing attacks. The PSNR is used to measure the quality of the watermarked image. However, robustness of the extracted watermark is measured by NC. The highest PSNR is 52.56 has been obtained at gain factor 0.1. However, the highest NC value is 0.99 has been obtained at gain factor 0.9. We have found that the larger the gain factor, stronger will be the robustness and smaller the gain factor better will be the image quality. On increase the gain Factor image quality get distorted.

Table 8: PSNR and NC performance of the proposed method at different gain factor and using different sub-band

Gain Factor (K)	PSNR				NC
	LL	LH	HL	HH	LH
0.1	36.52	33.15	32.92	30.45	0.97
0.2	30.15	30.13	30.19	29.34	0.98
0.3	29.83	29.84	29.81	27.14	0.99

In Table 8, PSNR value for different sub-bands are calculated at different gain-factors The highest PSNR value is 36.92 obtained at LH sub-band with gain-factor 0.1 and the NC of LH(sub-band) is taken. The highest value of NC is 0.99 obtained in LH obtained as compared to different sub-bands at gain-factor 0.1, 0.2, 0.3.The highest NC value is

obtained at gain factor 0.3 in LH sub-band. Showing that our method is more robust and imperceptible as PSNR decreases with increase in Gain factor.

Table 9: NC performance of proposed method at LH sub-bands against different attacks and gain-factor 0.01

Attacks	NC
Brightness attack	0.94
Rotation attack	0.93
Contrast attack	0.95
Salt and Pepper	0.96
Gaussian Noise	0.93

In Table 9 Performance of NC value on LH sub-band at constant gain factor when different attack is applied. The highest value of NC is 0.96 obtained in case of Salt & pepper attack when gain factor is 0.01.

Table 10: PSNR and Compression Ratio of proposed method at LH sub-band at gain-factor 0.01.

Different Image	PSNR	Compression Ratio
Brain Image	28.21	1.78
Lung Image	29.14	2.01
MRI Image	37.14	3.92

In Table 10 Performance of PSNR and Compression ration value on LH sub-band at constant gain factor 0.1 is applied. The highest value of compression ratio is 3.92 obtained in case of MRI image whose PSNR is high and compression ratio. The lowest compression ratio is 1.78 obtained in case of Brain Image. means brain image take less time to compress than any other two image. Rate of compression of brain image is better than all other images.

Table 11: Comparison between Huffman, BTC and Fractal compression of our proposed algorithm.

Gain Factor(k)	BTC Compression		Huffman Compression		Fractal Compression	
	PSNR	NC	PSNR	NC	PSNR	NC
0.1	34.17	0.90	45.14	0.95	29.14	0.84
0.4	31.15	0.94	43.24	0.97	28.87	0.87
0.7	30..43	0.96	41.14	0.98	27.87	0.90

In table 11 it is clearly shown that on increasing gain factor PSNR decrease in case of Huffman, BTC and Fractal compression. The results of BTC and Fractal have been experimentally shown in [36]. It is observed that Huffman provide better result when compared to BTC and Fractal compression technique. As Huffman is a lossless compression technique. The compressed image will be exactly same as original image. Without any loss of data or pixels of image These compression techniques provide better results and performance in terms of image quality. This way we can show how our Huffman compression technique is better than any other compression technique. The highest value of PSNR is 45.14 at gain-factor 0.1 obtained in case of Huffman compression and highest value of NC is 0.90 obtained in case of Huffman compression at gain factor of 0.98

Table 12: Comparison between Huffman and Fractal compression ratio of our proposed algorithm at different images, at constant gain factor 0.1[36].

Images	Huffman Compression	Fractal Compression
	C.R	C.R
Brain	1.23	10.19
Lena	2.01	11.87
Lung	2.98	12.87

In table 12 ,it is clearly shown that compression ratio is better in case of lossless compression technique ,we have used Huffman compression, and have take different image and calculated its compression ratio, and compression ratio is better in terms of

Huffman compression technique when applied on medical image, means lossless image take less time to compress than lossy compression technique, so there is no loss of data in case of lossless technique means original image will be same as reconstructed image[41].The highest value of C.R is obtained in case of Lung image which is 12.87 and lowest in Brain image which is 1.23,means Huffman compressed has less compression ratio as compared to other compressions.

4.9 Performance analysis of the proposed method for different attacks

Salt and Pepper

Salt and pepper noise is a form of noise which is sometimes seen on different images. It o occurs in the form of white and black pixels[34-36]. An efficient noise reduction method for this type of noise is a median filter or morphological filter. For reducing the effect of salt – pepper noise, but not both ,a contra-harmonic mean filter can be effective. In this way embedded watermark is exposed into salt and pepper noise with.

X=imnoise (Y', salt & pepper',D) where Y' is the watermarked image

adds "salt and pepper" noise to the image Y,where D is the noise density. Here D varies from 0.2 to 0.9,and we can easily see the effect in image. Figure 14 shows the effect of salt and pepper noise on the watermarked image.

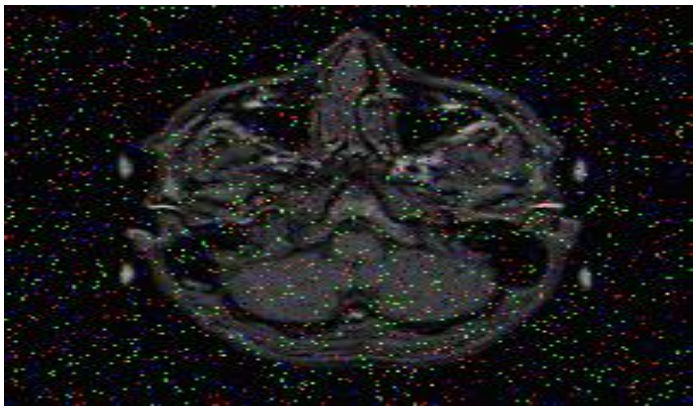


Figure17. Effect of salt and pepper noise on watermarked image

Speckle Noise

Speckle is a granular ‘noise’ that exist and degrade the quality of images which are in the form of active radar, synthetic aperture radar (SAR) images, medical ultrasound and optical tomography images.

Speckle noise occur in form of a common phenomena called as speckle. It occurs due to interference of the returning wave from their sources at the transducer aperture. These are basically scattered signal add coherently, i.e. they are added constructively and destructively depending on the different phase of different wavelets. The mean gray level of local area is increased[37]. Speckle noise in case of SAR is serious, causing difficulties for images to intercept. It is caused by coherent processing of backscattered signal. At times speckle contain useful information, when it is associated with laser speckle and dynamic speckle, where changes are measured in time. . Figure 15 shows the effect of speckle attack on the watermarked image.

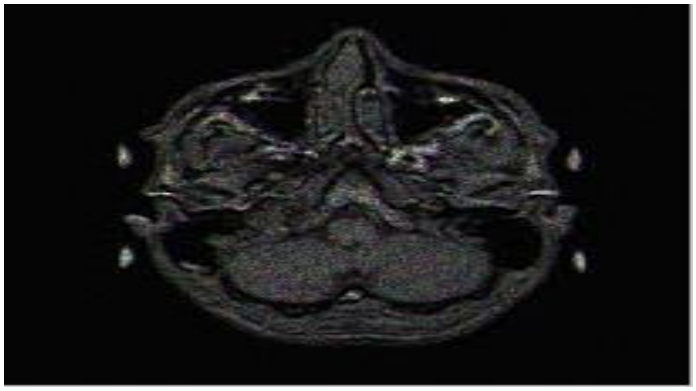


Figure18. Effect of speckle attack on watermarked image

Rotation attack

This attack try to destroy the synchronizations of the watermark detectors and the watermarking, even a slight rotation may change the detection of watermarks. Resize of rotation attack is based on the combination of the Zernike moments and singular value decomposition (SVD)[38].This may cause partitioning of DWT and decompose SVD to lower frequency components[39]. Due to rotation attacks image is rotation through different angles, by using syntax imrotate (I1, different angles ‘loose’, bilinear). Figure 16 and 17 shows when watermarked images are rotated through different angles.

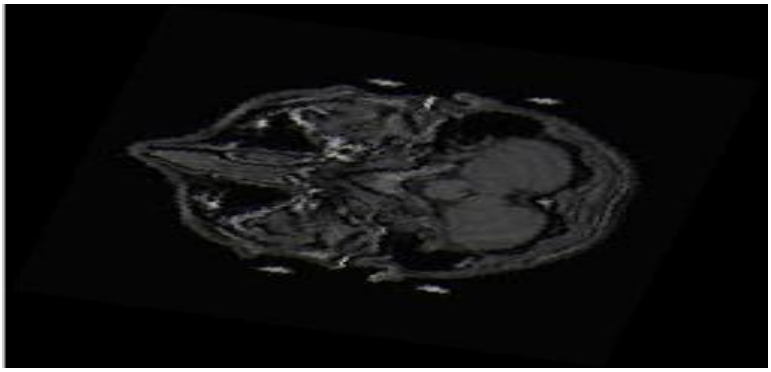


Figure19: Rotation done at an angle of 75 degree

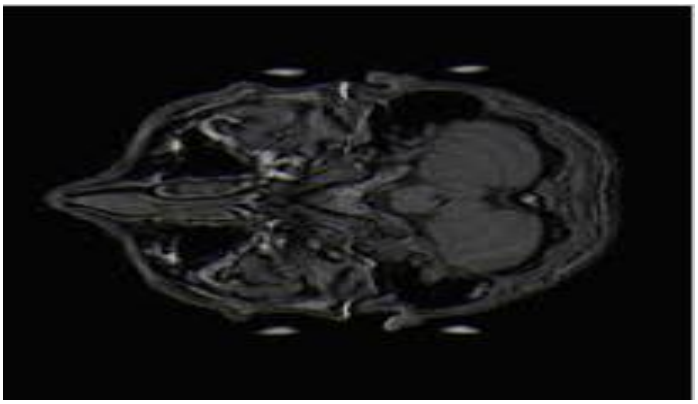


Figure20: Rotation done at an angle of 90 degree

Due to rotate attack image is rotated through different angles in which we want them to rotate.

4.10 Conclusion

In this technique, we proposed a new approach for digital image watermarking. The DWT and Huffman are efficient techniques used for watermarking so there combination makes a very good watermarking technique. Due to the excellent properties of DWT, the DWT is suitable to identify the area in the cover image which is suitable for embedding watermark. One of the efficient properties of Huffman that it has less compression ratio,

and quality gets reduced with increase in gain factor due to the property of this algorithm. So, the proposed hybrid technique improved the robustness and imperceptibility as compared to BTC and fractal based compression techniques. The main properties of the proposed work can be identified as follows: (1) In the proposed method, we have embedded compressed watermark into different sub-bands of host image and desired results are obtained as watermark is compressed to embed more information which is useful in medical application.(2)Huffman coding is based on the particular frequency occurrence of a data item(pixel in images). It uses a lower number of bits to encode the data that occurs more frequently. Based on various applications such as medical applications, where the pixel of any data is more important, so any distortion in the received data may cause the wrong diagnoses both lossy and lossless have importance at their own places. Lossy is use to compress different multimedia data and text such as audio, video and still images.

Chapter 5
Conclusion and Future Work

In proposed approach a new technique for digital image watermarking is used. The DWT and compression are efficient techniques used for watermarking .Due to excellent of DWT we can embed watermark in any of the DWT sub-band and will monitor the change in NC, PSNR of desired image. To further improve robustness and imperceptibility will try to add different compression to our watermark so our image quality will be more better on different gain factors. However, the working principles of watermarking and compression seem to be different as perceptual data coding removes inherent redundancy during compression. Image Compression is a well known topic that codes picture into fewer amounts of data. There are two different kinds of image compression techniques: Lossless and Lossy Image. Lossless image compression are error-free coding methods .It can decompressed into one which is the original image .Since lossless compression keep all the information in image ,the size of the compressed results are not reduced so much. Most common examples of lossless compression are Huffman compression, arithmetic compression, run length coding etc. Lossy image compression techniques produce results with little distortion and image obtained from decompressing is not same as the original one. In chapter 3, two lossy compression techniques are applied on watermark namely BTC and Fractal compression. In BTC compression, it is a lossy compression and is applied block wise on watermark making use of different gain factors and providing better image quality in term of robustness and imperceptibility and resistant to different signal processing attack. The other lossy compression applied on watermark to compress it and embed it on desired sub-band of cover image is Fractal compression, It is also lossy compression technique for digital images based on fractals. It is like parent child relationship**.** In chapter 4 Lossless compression technique is used ,by lossless means original image is same as reconstructed image, the aim of lossless compression is to reduce number of bits in image, but maintain image quality and pixel resolution of reconstructed image same as original one. One of the efficient properties of Huffman that it has less compression ratio, and quality gets reduced with increase in gain factor due to

the property of this algorithm. So, the proposed hybrid technique improved the robustness and imperceptibility as compared to BTC and fractal based compression techniques. The main properties of the proposed work can be identified as follows: (1) In the proposed method, we have embedded compressed watermark into different sub-bands of host image and desired results are obtained as watermark is compressed to embed more information which is useful in medical application.(2)Huffman coding is based on the particular frequency occurrence of a data item(pixel in images). It uses a lower number of bits to encode the data that occurs more frequently. Based on various applications such as medical applications, where the pixel of any data is more important, so any distortion in the received data may cause the wrong diagnoses both lossy and lossless have importance at their own places. Lossy compression is use to compress multimedia data such as audio, video, text and still images. It is used for streaming of data and in internet telephony.

For the identity authentication purpose, we will use multiple watermarks in our proposed method. Also, performance of the proposed method will improve in near future.

APPENDIX A

SYSTEM REQUIREMENTS

An operating system is software which manages computer hardware and software resources and provide different services for computer programs. The operating is essential component of the system software in a application of computer system. There are different user-friendly OS available which can be worked on. For my Project I am working on Window 7 (32 bit) ,with Intel® Core(TM)2 Duo CPU T6400 @2.00 GHZ 2.00 GHz, with RAM 2.00 Gb.

Software Requirement:

MATLAB 2013a I am using for the simulation of my project**.**

APPENDIX B

MATLAB:

Matlab is a high –level processing language and interactive environment for numerical computation, revelation and programming. Using Matlab, you can visualize data develop different algorithms, and create models and application .The language tool and different help operations help you to build multiple approaches and reach a best solution in matlab. Matlab is used for wide variety of applications like image and video processing, control system test and measurement, computational finance and biology[42]. The main Key features of Matlab 13 which we have used are

Key Features

- High –level language for numerical computation, revelation and application.
- Interactive environments for produce interactive designs.
- Produce different function for linear algebra, Fourier, statistics, integration and differential equation.
- Built-in graphics for visualizing code quality and maximizing performance of our outputs.
- It is a developmental tool kit for improving our code quality.
- Different Languages are used for integrating Matlab like C, Java.

Desktop Basics:

When you start MATLAB, the desktop appear in its default layout.Figure 17 shows snapshot of mat lab layout.

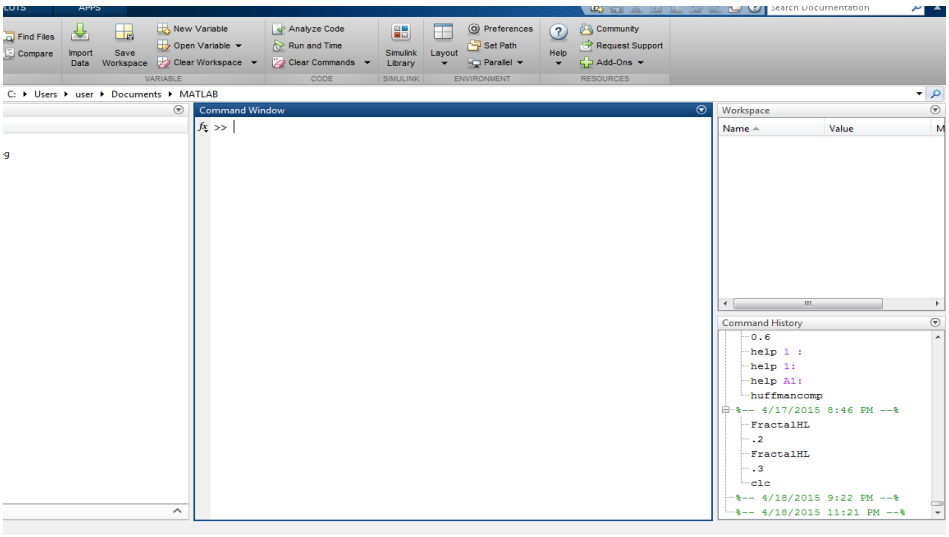


Figure 21: Matlab Layout

The desktop include different panels:

Current Folder: where we access our files

Command Window: Enter commands at the different command lines indicated by the >>

Workspace: Explore data which we have created or imported from our files.

Matlab have different operation in-built like:

Help and Documentation:

All MATLAB functions have supporting documentation that include examples calling different, outputs and calling syntax. There are different ways ,how can we access these documents in command

For the function documentation in a different window other than a main window use the doc command

doc **means**

It displays different function hints and properties .Its syntax is denoted as

mean(

Help mean

Access the full documents by clicking on the help icon.

Matrices and Magic Squares

In the Mat lab environment, a matrix is a rectangular array of different numbers. especially when it is attach to 1-by-1 matrices, which are scalars and with

matrices with one row and one column ,which are represented in the form of vectors. Matlab can store data both numerically and non-numerically .The operations in matlab are designed to be possible as natural[43-44]. Whereas other programming language works with numbers one at a time, so it take lot of processing and computation for data. Matlab work with other matrix quickly and simultaneously. Mat lab has two transpose operators .The apostrophe operator (for example A') perform a conjugate transposition .The flipping of matrix is done diagonally and automatically change the sign of complex component.

Magic Function

Matlab has built-in function which built square of almost any size, that create magic square of almost any size. This function is named magic

B=magic (4)

B=

16 2 3 13

5 11 10 8

9 7 6 12

4 14 15 1

The matrix property is same as other vector properties, and same "magic" properties, the only difference is that middle columns are easily exchanged.

Matrix Operators

Expression use familiar arithmetic and precedence's rule:

+ Addition

_ Subtraction

*** Multiplication**

/ Division

\ Left division

^ Power

' Complex conjugate transpose

( ) Evaluation order

Basic image processing commands in MATLAB:

Digital images, and many other files, are known as matrix in Matlab .Some of the basic image processing commands are given below:

Loading an image:

For loading a particular image ,it is best to put an image in some folder ,with extension on m-file. This way image can be easily loaded through “imread” command.

```
A=imread (‘brain.jpg’)
```

Else if image is in different folder, it should be properly addressed:

```
A = imread(‘C:\Users\User2\D\brain.jpg’);
```

The different formats supported by MATLAB are: gif ,jpg ,bmp, hdf, jpx ,ras ,tif (tiff),pcx ,pbm and xwd. If image is black and white ,then matrix is 2-dimensional.However if there is a colour image, it will be three dimensional which has 3 main colours.Red,Green,Blue.The number of bits need to preserve the value of every pixel is called as “bit depth” of the image. The output class of imread is “logically” for depth of one bit, “uint8” for bit-depth between 2-8,and “uint16” for very high bit depths.

Displaying an image:

The most common command to display an image matrix is “imshow”

```
Imshow (A);
```

This command can depict different matrices with different double values. if the values are not between 0-255 ,it is better to map in this region. This can be simply done by adding an empty matrix to the command. The lowest value of matrix is considered as ‘0’ and highest one is considered ‘255’.With the help of imshow command image is displayed on screen

```
Imshow (A, [ ]);
```

Creating an Image

“Imwrite” is used for creating an image file out of a particular matrix. The image file is created in the same folder with the m-file if no path is given. This command has some useful parameters such as JPEG image compression ratio:

```
Imwrite (A,'wm_brain.bmp','Mode','lossy','Quality', 55,'Bitdepth', 12);
```

Changing colour of image

Rgb2gray changes colour of image from 3 dimensional to 2 dimensional.

Uint8: It converts to 8-bit unsigned integer.

Syntax: Its syntax is int Array=uint8

Due to this syntax, it converts the element of an array into unsigned 8-bit (1-byte) integer of class uint8.

Convert a double array to uint8:

```
my data=uint8(magic(10);
```

PUBLICATION

- Anum Javeed, Amit Kumar Singh "Hybrid Technique for Robust and Imperceptible Image Watermarking in DWT- BTC Domain" International Journal Of Electronic Security and Digital Forensics Inder science (Under Review).

References:

[1] S. P. Smohanty "Digital Watermarking a tutorial review",M.S.Thesis Indian Institute of Science Banglore,1999,pp 1-24.

[2] M. Mustra, K. Delac, and M.Grgic, "Overview of the DICOM Standard", 50th International Symposium ELMAR-2008, September, Zadar, Croatia,pp.39-44.

[3] A. Cheddad, J.Condell and K.Curran . "Digital image steganography: Survey and analysis of current methods." Signal processing Vol 90(3), 2010 pp .727-752.

[4] M. Harem, S. A. K. N El- shimmy, and A S Tolba, F M Abd-el-Kader, H M ELindy, "Wavelet Packets-Based Blind Watermarking for Medical Image Management". Journal on The Open Biomedical Engineering, Vol 4, April 2010,pp. 93–98.

[5] H. Peng, Wang, and J. Wang, "Image watermarking method in multi-wavelet domain based on support vector machines". Elsevier The Journal of Systems and Software, Vol 83, March 2010,pp 1470–1477.

[6] N.Nikolaidis and I Pitas, "Digital Image Watermarking: An Overview", in Proc.IEEE International Conference on Multimedia Computing and Systems, Vol 1, Florence, June 1999, pp 1-6.

[7] F. Hartung, M. Kutter,"Multimedia Watermarking Techniques", Proceedings of IEEE, Vol. 87, (7), July 1999, pp. 1085 – 1103.

[8] A. Watson , "Image Compression Using the Discrete Cosine Transform",Journal on Mathematical Vol4 (1),1994 pp.81-88.

[9] A.K Singh, M. Dave and A. Mohan, "Wavelet Based Image Watermarking: Futuristic Concepts in Information Security", Springer Proceedings of the National Academy of Sciences, India Section A: Physical Sciences Vol 84 (3),June 2014 pp. 345-359.

[10] I. J. Cox, J. Kilian, F. T. Leighton and T. Shamoon, "SecureSpread Spectrum Watermarking for Multimedia,"IEEE Transactions on Image Processing, Vol. 6. (12), 1997, pp. 1673-1687.

[11] V.Schyndel, R.G.Andrew Z.Tirkel, and F. Osborne. "A digital watermark." in IEEE Proc. Image Processing, , Austin, TX Vol. 2, November,1994,pp. 86-90.

[12] K.A.Navas and M. Sasikumar ,"A Benchmark for Medical Image Watermarking", in Proc.IEEE Systems, Signals and Image Processing, and 6th EURASIP Conference

focused on Speech and Image Processing, Multimedia Communications and Service, Maribor,June 2007,pp. 237-240.

[13] D. Nilanjan, S.Samantha, and A. Bardhan Roy, "A Novel Approach of Image Encoding and Hiding using Spiral Scanning and Wavelet Based Alpha-Blending Technique."International Journal of Computer Technology and Applications Vol 2, (6) 2011, pp.1970-1974.

[14] M. Perumal, S, and V. Vijaya Kumar. "A wavelet based digital watermarking method using thresholds on intermediate bit values." International Journal of Computer Applications Vol 15, (3) 2011, pp. 29-36.

[15] M.Arsalan, Sana Malik and A. Khan, "Intelligent reversible watermarking in integer wavelet domain for medical images",ACM Journal of Systems and Software ,Vol 84(4),April 2013,pp .883-894.

[16] A. Kannammal, and S. Subha Rani, "Two Level Security for Medical Images Using Watermarking/Encryption Algorithms", International Journal of Imaging Systems andTechnology,Vol24(1),March,2014,pp.1-10.

[17] J,Edward Delp and O.Robert.Mitchell, "Image Compression using block truncation coding",IEEE Transaction on Communication, Vol 27 (9), 2012,pp.1335-1342.

[18] A.Mohammad and M.Nosoohi**,** "Medical Image Authentication based on Fragile Watermarking using Hamming Code",in Proc.IEEE, Biomedical Engineering (ICBME), Isfahan ,Iran November 2010,pp.1-4.

[19] J.Puate and F.Jordan, "Using fractal compression scheme to embed a digital signature into an image",2009,pp 1-12.

[20] F. Alturki and R. Mersereuu, "Secure Fragile digital watermarking technique for digital images",2001 ,pp.1031-1034.

[21] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," IEEE Transaction on . Multimedia, Vol. 4, (1), March, 2002, pp. 121–128.

[22] R..Das, and Th. Tuithung, "A Novel Steganography Method for Image Based on Huffman Encoding", in Proceedings IEEE on Emerging Trends and Applications in Computer Science (NCETACS), 2012 ,Shillong,pp.14-28.

[23] K.Adwijaya, P. N. Faoziyah and F. P. Perman, "Tamper Detection and Recovery of Medical Image Watermarking using Modified LSB and Huffman Compression",in IEEE Proceedings , Lodz,2013,pp.129-132.

[24] M. Analoui and J. P. Allebach, “Model-based color half toning using direct binary search” in Proc. SPIE, Human Vision, San Jose, CA, Feb. 1992, Vol. 1666, pp.96–108.

[25] Q. Lin and J. P. Allebach, “Color FM screen design using DBS algorithm”, in Proc.SPIE- The International Society for Optical Engineering, Vol. 3300, Jan, 1998, pp. 353–361.

[26] A. U. Agar and J. P. Allebach, “Model-based color half toning using direct binary search,” IEEE Trans. on Image Processing., Vol. 14(12), December 2005 pp.1945–1959.

[27] J. M. Guo, “Improved block truncation coding using modified error diffusion,” Journal Electron. Letters, Vol (44)7, March, 2000 pp. 1269–1275.

[28] J. M. Guo and M. F. Wu, “Improved block truncation coding based on the void-and-cluster dithering approach,” IEEE Trans. Image Process., Vol. 18, (1), January, 2009. pp. 211–213.

[29] S. F. Tu and C. S. Hsu, “A BTC-based watermarking scheme for digital images,” An International Journal on Information & Security, Volume 15(2),2004, pp.216-228 .

[30] M. H. Lin and C. C. Chang, “A novel information hiding scheme based on BTC,” in IEEE Proc. Computer and Information Technology, (CIT), Wuhan, China, September 2004, pp.66–71.

[31] J. Han (2007) “Speeding up Fractal Image Compression Based on Local Extreme Points”, IEEEComputer Society, pp.732-737.

.

[32] E Arnaud. Jacquin, (1993) “Fractal image coding”, in Proc. of IEEE Vol.81, pp. 1451-1465.

[33] H.B.Kekre, K.T. Sarode, S. R Sange(2011) “ Image reconstruction using Fast Inverse Halftone & Huffman coding Technique, IJCA,Vol 27(6), pp.34-40.

[34] M. Aggarwal and A.Narayan “Efficient Huffman Decoding”, IEEE Trans, 2000, pp.936-939.

[35] A. Cheddad, J.Condell, K. Curran, and P.Mc Kevitt. "Digital Image Steganography: Survey and Analysis of Current Methods".ELSEVIER Journal on Signal Processing Vol 90 2010 pp 727-752.

[36] A. Javeed and A. K. Singh “Hybrid Technique for Robust and Imperceptible Image Watermarking in DWT- BTC Domain” International Journal Of Electronic Security and Digital Forensics Inder science(Under Review).

[37] R. Pasco, "Source Coding Algorithms for Fast Data Compression," Ph.D. Thesis, Department of Electrical Engineering, Stanford University, CA,1976.

[38] C. B. Jones, "An Efficient Coding System for Long Source Sequences," IEEE Trans. Info. Theory IT Vol 27, 2007, pp 280-291.

[39]J J. Rissanen, "Generalized Kraft Inequality and Arithmetic Coding," IBMJ. Res. Develop. Vol 20 ,2005, pp 198-203.

[40] G.Glen ,Jr. Langdon,. and J.Rissanen, "A Double Adaptive File Compression Algorithm," IEEE Trans. Commun.Vol 31, 2008, pp 1253-1255.

[41] D. Hanselman and B.Littlefield, Mastering MATLAB® 7, Pearson Education, India 2008.

[42] Z.Wang A.Bovik, A. and E. P Simoncelli "Image quality assessment From error visibility to structural similarity". IEEE Transaction. Image Processing, vol. 13(4),2004, pp. 600-612.