A BLIND IMAGE WATERMARKING SCHEME BASED ON DWT FOR TAMPER DETECTION

A Thesis Submitted
in Partial Fulfilment of the Requirements
for the Degree of

MASTER OF TECHNOLOGY
in
Software Engineering

by

Shruti Agarwal
(1150449009)

Under the Supervision of
Asst. Prof. Namita Srivastava
CSE Department, BBDU

to the
School of Engineering

BABU BANARASI DAS UNIVERSITY
LUCKNOW

May, 2017

CERTIFICATE

It is certified that the work contained in this thesis entitled "**A Blind Image Watermarking Scheme Based on DWT for Tamper Detection**", by Shruti Agarwal (1150449009), for the award of Master of Technology from Babu Banarasi Das University has been carried out under my supervision and that this work has not been submitted elsewhere for a degree.

Date:

Namita Srivastava
Assistant Professor
CSE, BBDU

ABSTRACT

Digital Watermarking is one of the important techniques to secure media files in the domain of data authentication and copyright. It can be defined as hiding digital information in the host data to protect the content from unauthorized users. It is required for content authentication, to prove ownership and to get some copyright-related information. For this paper, my work focuses on Image watermarking among other media types. As it can be assumed that a successful image watermarking approach can be later be applied to videos easily by taking video frames at some instant of time.

Tampering is a problem that has gained importance because of increasing use of digital media on the internet. More the data transmission more is the risk of the original content getting degraded or tampered. Hence the detection followed by restoration is important. Most of the research carried out so far in tamper detection are non-blind or semi-blind techniques, while more recent work includes tamper detection of the image using blind extraction algorithms.

There are lot of methodologies proposed in order to solve this problem. Some of them are schemes focussing on just the watermark extraction using DFT, DCT and some are more robust schemes using DWT as the base algorithm. Each algorithm proposed has advantages and disadvantages over different problem sets. This leads attentions towards developing a more robust and highly imperceptible methodology that is well equipped in detection, and localization of the tamper.

The proposed algorithm uses DWT for watermark embedding and extraction. The extraction algorithm is a blind algorithm, which means the extraction method does not require either the original image or the watermark to extract watermark from the tampered image. The scheme focuses on improving the PSNR of the watermarked images and the detection rate of the tampered images.

In this paper, a blind and informed watermarking approach is proposed. The watermark is built from the original image using the most significant bits method. The approach aims to provide a high robustness and imperceptibility with perfectly tamper detection zone. The original image is divided into blocks and the MSB of each block is inserted into its partner block's LSB. The watermark is embedded into the transfer domain. The proposed algorithm uses DWT for watermark embedding and extraction. The watermarked images are tampered and tested to locate the tampered area in the image. The experimental results prove the imperceptibility and the perfect detection of the tamper zones.

ACKNOWLEDGEMENTS

Over the year it has been my fortune to encounter many people who have given me more of their time, companionship, professional and personal help. I would like to take this opportunity to express my deep sense of gratitude to all who helped me directly or indirectly during this thesis work, without which this indeed, would have been a mammoth task.

I would first of all wish to thank my supervisor, **Mrs. Namita Srivastava**, for being a great mentor and the best advisor I could ever have. Her advice, encouragement and critics are source of innovative ideas, inspiration and causes behind the successful completion of this dissertation. The confidence shown on me by her was the biggest source of inspiration for me. It has been a privilege working with her for last one year.

A humble 'Thank you' Ma'am.

I am highly obliged to all the faculty members of Computer Science and Engineering Department for their support and encouragement. I also thank our dean of School of Engineering, **Prof. (Dr.) Seethalekshmi K.** and H.O.D, CSE Department, **Dr. Reena Srivastava** for providing excellent computing and other facilities without which this work could not achieve its quality goals. I would also like to thank our coordinator, **Mr. Saif Wajid** for full support and guidance whenever I required. I choose this moment to acknowledge their contributions gratefully.

I am, of course, particularly indebted to my parents and my brother for their monumental, unwavering support and encouragement on all fronts. They have truly always there for me, and without them none of this would have been even remotely possible. I would like to take this opportunity to express my deepest gratitude to all those who helped me at different stages during this thesis work.

Shruti Agarwal

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DWT	Discrete Wavelet Transform
HH	High-high sub-band
HL	High-low sub-band
HVS	Human Visual System
JPEG	Joint Photographic Experts Group
LH	Low-high sub-band
LL	Low-low sub-band
MSE	Mean Square Error
NC	Normalized Correlation
PSNR	Peak signal-to-noise ratio
SNR	Signal-to-Noise Ratio
SSIM	Structural Similarity Index Measure

CHAPTER 1

INTRODUCTION

"The Internet is becoming the town square for the global village of tomorrow" Bill Gates (1975-present). The Internet plays host to all aspects of economic and social life. In the recent era, the Internet has become the huge hub of data which are crucial as well as less crucial. IBM claims 90% of the todays data was generated in just the last two years. This is because of the availability of inexpensive sources that generate data like texts, images, videos and audios within no time. Among all types of data, images occupies an effective position since the information that an image carries can be understood way faster than the respective texts. Moreover, the digital documents can be distributes worldwide without much time and effort. And here the role of internet comes into play which aids in real time information delivery. Unlike traditional copying that also degrades the quality of the content, multiple copies can be created of the digital images without lose in quality in a short span. That is no quality loss at basically no cost. Thus, this unlimited duplication of data threatens the intellectual property rights of the content owners. As said there is a much need for technologies that promise to protect their rights.

The crucial data requires more protection and security from the various threats and new attacks that breach the security of ownership. The digital media can be manipulated easily using various image editing software. Copying is simple with no loss of fidelity. A copy of digital media is identical to the original so in no way the owner can claim his rights over his work and prevent it from being used in improper way just by looking at it. Thus the solutions to combat issues of ownership in legal disputes, copyright, copy control, content integrity and intellectual property right protection can be Steganography, Cryptography, Digital Watermarking, Digital Fingerprinting and digital signature.

In cryptography, the data to be secured is encrypted using encoder i.e. the plain text is converted to the cipher text, and is transferred over the transmission channel. A key is provided to the legitimate owner (one who has paid for the content). The receiver on getting the ciphered text decodes it to get the actual message. However encryption does not provide overall protection. The owner is unable to discover how his product is being handled after it has been decrypted by the buyer. Also, once the encrypted data are decrypted, they can be freely distributed and manipulated. A pirate user can distribute numerous copies of the decrypted (unprotected) data. In fact, watermarking can complement encryption. Encryption can protect data during transmission and watermarking can be used afterwards to prosecute copyright infringements.

Steganography is a bit similar to encryption or cryptography. In steganography, the critical data is hidden inside some other content and is transmitted. The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted message arouse interest of the pirates. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

Watermarking can insert a unique mark into every copy of the work like movie, therefore an illegal copy can be traced to the original source, for example to a specific theater. But digital fingerprinting cannot do that, it can only tell you a certain content is very similar to an “original” content. Thus watermarking has a clear advantage for tracing. Whereas a digital signature is a mathematical scheme for demonstrating the authenticity of the digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. But the most effective way for copyright protection and content integrity is digital watermarking.

To begin with a quick background of watermarking is given and then the attention is given to the watermarking requirements that watermarking system must meet, types of watermarking, applications and various attacks on a watermarking system.

The below list contains some standard terms related to digital watermarking which are used throughout the thesis:

- Host Image – The cover image over which the watermark is to be embedded.
- Watermark – Some kind of data embedded to the image for copyright protection and content authentication at the usage by third party.
- Watermark embedding – The process of adding watermark to the host image.
- Watermarked Image – The resultant host image after being embedded with the watermark.
- Tampered Image – The watermarked image which has gone some kind of modifications or alterations.
- Watermark extraction – To retrieve the watermark from the tampered or modified image to verify the source and for content authentication.
- Watermark scheme – Comprises of watermark embedding and watermark extraction.

CHAPTER 2

DIGITAL WATERMARKING

Digital Watermarking is the act of hiding digital information in a carrier signal; the hidden information should but does not need to, contain a relation to the carrier signal. A watermark is embedded to protect the host data and it becomes an integral part of the data, always attached to it wherever the data is transferred. The watermark usually carries the copyright or the ownership information of the content. Though digital watermarking and steganography sounds similar, these two are completely different concepts. In steganography, the hidden data is on the highest priority for sender and receiver whereas in watermarking both the source image and the hidden image, signature or data is on highest priority. The information hidden is used for verifying the authenticity, ensuring data integrity and to protect unauthorized access of the content. It is prominently used for tracing copyright infringements.

The watermark stems from the ancient art of a figure or design incorporated into paper during its manufacture and appearing lighter than the rest of the sheet when viewed in transmitted light for the same purpose. Watermarks have been used on postage stamps, currency and other government documents to discourage counterfeiting. Figure 2.1 shows the perceptible watermark on a sheet of paper. (Image taken from http://www.watermarks.info/todo.htm).

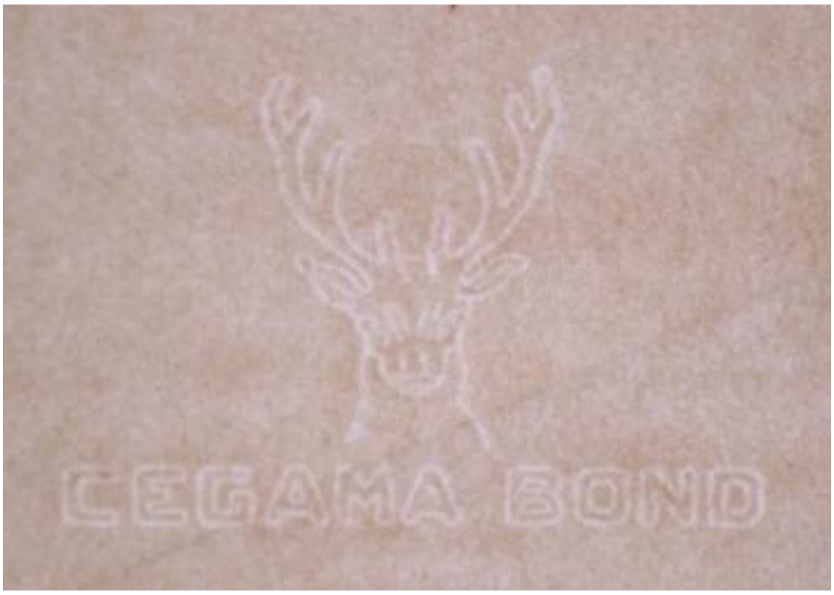


Figure 2.1: Perceptible watermark embedded in a sheet of paper.

With the increasing rate of piracy and copyright proof, digital watermarking has become a good topic of research. For example the music and video industry loses billions of dollars per year due to illegal copying and downloading of copyrighted materials from the Internet [9]. More robust algorithms need to be developed to prevent integrity and authenticity where the integrity shows the content intact from illegal manipulation and the authenticity prove the data originality as sent from the source [13]. Ideally digital watermarks should be hard to notice, difficult to reproduce, and impossible to remove without destroying the medium they protect. Continuous efforts are being made to devise efficient watermarking schemes but techniques proposed so far do not seem to be robust to all possible attacks and various multimedia data processing operations. Basically digital watermarking is gaining so much attention because of sudden increase in threats to intellectual property rights. An illegal user or a pirate tries to modify the original data or host image by either removing the watermark to violate a copyright or cast the same watermark after altering the data in order to forge the proof of authenticity or tries to tamper the image so that it becomes difficult to identify the original.

2.1 The Watermarking Process

The watermarking process can be divided into two parts: watermark embedding and watermark extraction.

2.1.1 Watermark Embedding

Watermark embedding is a process of embedding some bits or a logo or an owner identified image into the host image. Embedding is carried out to enhance the security of the original image and prevent it from being misused. The block diagram in the Figure 2.2 shows the watermark embedding process.

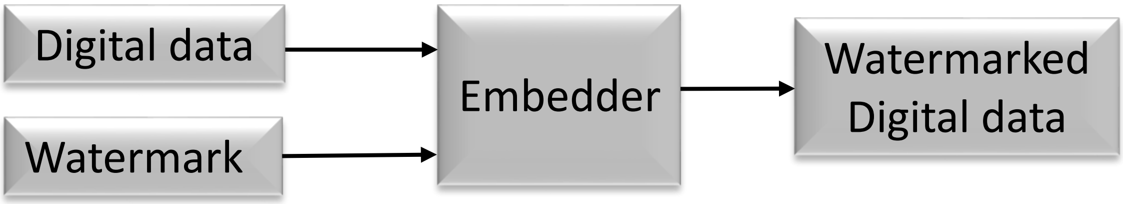


Figure 2.2: Watermark embedding process

The embedder takes two inputs. One is the host image or the cover image in which the watermark has to be embedded. And the other is the watermark that is to be embedded inside the cover image. The watermark can be either a separate image or logo or can also be a part of the host image itself. The output of the embedding system is the watermarked image whose visual quality must not degrade if the watermark inserted is the inviable one. But if it’s a visible watermark then obviously it will affect the visual quality of the host image.

2.1.2 Watermark Extraction

Watermark extraction is the process to retrieve the watermark from the image that may or may not have undergone alterations. The watermark extracted can be used for tracing the source or to solve legal disputes by protecting the copyright of the owner. The watermark that has been extracted can also help in detecting the tampers and thus recover it using the algorithm using which the watermark had been embedded. Thus watermark extraction is a vital part in watermarking process. The Figure 2.3 represents the block diagram of watermark extraction. A key may (or may not) be used to extract watermark from the tampered image.

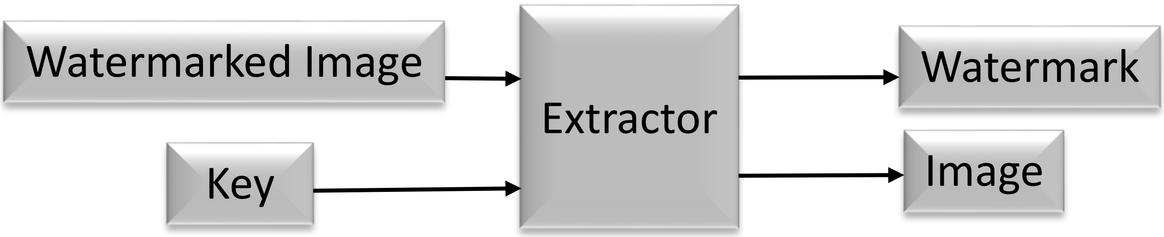


Figure 2.3: Watermark extraction process

The extraction algorithms are of 3 types: blind, semi-blind and non-blind. Each type is discussed in detail in the upcoming sections. Mainly the blind extraction algorithm requires the key for watermark extraction as there is no availability of the host image or the original watermark embedded into the cover image. Further details on extraction algorithms is been discussed in section 6 of this chapter.

2.2 Application Areas of Digital Watermarking

Watermarking technologies can be applied in every digital media where security and owner identification is needed [10]. Among various applications, the focus of my work is on tamper detection application of digital watermarking. Watermarking schemes are useful in the following areas:

2.2.1 Copyright Protection

The purpose of copyright is protecting the creator against infringement. The one who originates the work is the creator of the work. In other words, a person whose mental or creative effort resulted in the finished version of the work is the creator of his work. Copyright arises at the time when the work becomes available to third parties and thus the need for copyright protection which can be effectively done by watermarking the work beforehand.

No formality or legal actions are required to acquire a copyright. Nevertheless, it is good to officially record the date on which the work was created in order to ease the process of detection of illegal modifications and ultimately, protect the copyright. When a work contains a valid copyright, an infringer cannot claim in court that he or she did not know that the work was copyrighted.

If the work is produced by an individual, copyright protection will generally end 70 years after his death. But if a company is regarded as the creator of a work, copyright protection expires 70 years after introduction or publication of the work [ref]. The other use of watermarking for copyright protection can be in broadcasting fields. A channel's video can be shown on another channel without giving credits to the original broadcasted channel. Also without paying the required fees for the copyrighted content. Copyright protection thus provides benefits in the form of economic rights which entitle the creators to control use of their literary and artistic material and to obtain an appropriate economic reward.

2.2.2 Copy Protection

Copy protection is a type of content protection or copy restriction. It is an effort to prevent reproduction of the digital media or any other sort of work mainly due to copyright reasons i.e. to prevent illegal copying. Unauthorized copy and distribution accounted for $2.4 billion in lost revenue in the United States alone in the 1990s. The illegal copying of the data is affecting much to the musical and gaming industry thus there is a serious need for protecting the data from any sort of reproductions. And here, the digital watermarking come into role and ease the tension of the host data owners who are continuously looking for techniques to protect their copyrighted contents. Thus there is a requirement for copying devices to be integrated with the watermark detecting circuitry.

2.2.3 Tamper Detection

Tamper detection is a process that makes unauthorized access to the protected objects easily detected. Seals, markings or techniques like watermarking may be tamper indicating. Tampering is the act to modify the content without notice any change at the destination [13].

Tampering means deliberate alteration or modification to the information or system. Often multiple level of security needs to be address to reduce the risk of tampering. We can make use of digital watermarking to detect tampers in the data. The algorithm used to embed watermark in the data can be traced backward at the destination to figure out whether or not some kind of tamper has been done on the host data. Tamper can be as small as not visible to human eye. For example, the date of diagnosis can be changed for 3 to 8 in a digitized medical test report using any image editing software. Another example can be successfully tampering the car number plate to hide the original car identity. A watermarking system can be embedded in digital cameras to help resolve the issue. If somebody tries to tamper the data, the watermark will get destroyed indicating that the data is tampered. Thus, to prevent such illegal acts a properly watermarked image is required so that any sort of tamper can be detected and thus restored to original. In this thesis we will develop watermark for tamper detection.

2.2.4 Broadcast Monitoring

Broadcast monitoring service automatically monitors network, cable and local TV programs to find what is being shown on TV. It is basically a way to detect whether the paid contents or programs are broadcasted as decided or not. For example, the advertisement companies may want to ensure they are given the exact amount of airtime for which they have paid for. Another example can relate to musicians and actors that they are given enough payment for displaying their work on TV or theatres. The channels want a security that their content is not being copied or recorded and being shown on another websites without their consent. Thus to provide security to such issues a proper system is required. Digital watermarking can be of a lot help in such situations providing knowledge about the misleading behavior of the respective system by putting a unique watermark in each video or audio file prior to broadcast. New items can have a value of over $100,000 per hour, which make them very vulnerable to intellectual property rights violation. Automated broadcast monitoring stations can thus keep full check on which video/audio file has been broadcasted where and how many times.

2.2.5 Fingerprinting

Detecting the watermark from any illegal copy can lead to identify the person who has leaked the original content. Digital Fingerprinting is a technology which enables content owners exercise greater control on their copyrighted content by effective identification, tracking and monitoring across distribution channels while opening additional monetization avenue by exploiting extended value of digital assets. Digital Fingerprints are compact digital impressions extracted from the original content (audio or video) which represents content’s characteristics and have enough details to identify a content variant upon comparison.

If out of number of legal buyers, one start selling the digital media illegally it is very difficult to identify who among many is a threat to the business. Thus if a unique watermark is embedded in each digital copy of the media then it would be easy to identify the faulty by tracing the watermark present in the leaked copy of the media.

2.2.6 Medical Applications

Watermarks can also convey object-specific information to users of the object. For instance, a watermarked digital medical report can help doctors and medical facilities to verify that the reports are not edited by illegal means i.e. they are in their original form and are completely true. Modifications like cropping or scaling can occur. Hence techniques like watermarking are required that are robust to such geometric transformations as medical data of the patients are too crucial to be modified. These medical reports are the only information that describes what further diagnosis is required for the patient.

2.3 Characteristics of Watermarking Schemes

A good watermarking scheme must adhere to the following characteristics.

1) Imperceptibility: In terms of watermarking, imperceptibility represents the invisibility of watermarks to human eyes (regarding the human visual system (HVS)), or if a watermark is an audio clip, it should not be audible to human ears. The watermark embedded into the host should alter the original content till the extent it is not visible to our eyes. The owner of the data would not like his content getting modified for the sake of security. That means the invisible watermarks should not degrade the quality of the content [19] whereas no such limitations with visible watermarks. But in general visible watermarks are more prone to damages and are less robust. Figure 2.4 represents the original image and the watermarked image. By looking at two picture one cannot figure out the difference between both the pictures. This is what imperceptibility of the watermarked image is.

(a) (b)

Figure 2.4: Imperceptibility (a) Original host image and (b) Watermarked image

2) Robustness: Robust watermarking techniques are the ones that can withstand malicious attacks like normal media operation such as filtering, compression; geometrical modifications such as rotation, cropping; addition of noise or color correction. Robustness helps in achieving the target of copyright and ownership issues. Any attempt to remove the watermark from image should severely degrade the image's visual quality. However it depends on the need of the application that whether a robust watermark is required or the fragile watermarking scheme. Fragile watermarks, also called hard authenticate, are designed to detect every possible change in pixel values [1]. Even the slight non-malicious modification in the image would destroy the watermark. That means fragile watermarks are sensitive to modifications. They are good at strict level of integrity check. Medical applications require fragile watermarking schemes as their data is very critical and a patient's life is depended on it. Another type of watermark is semi-fragile watermark. Semi-fragile watermarks are moderately robust and thus provide a "softer" evaluation criterion (authentication with a "degree"). Well suited for content authentication. These lie between robust watermarks and fragile watermarks. Some schemes have been

specifically designed to be compatible with certain distortions, such as JPEG or wavelet compression. To develop a more robust scheme the watermark must be distributed all over the image but this will have its impact on the imperceptibility value of the host image. Thus a good balance has to be maintained between the imperceptibility and the robustness of the watermark.

3) Capacity*:* Storing a watermark needs some space in the image or the video content. But less memory space increases the transmission process's performance [5]. Hence image compression algorithms should be applied but should not affect the visual quality of the original content. The number of bits carried by the watermark could be as low as one bit or several hundred bits. Thus, low bit-rate watermarks are less robust where bit-rate refers to the amount of data a watermark can encode in a signal. Obviously, there is a trade-off between the robustness and the capacity of the watermark [6].

4) Computational Complexity*:* Computational Complexity is another important aspect. The complexity can be calculated either by evaluating the time taken by the embedding and extracting watermark to original image or from watermarked image respectively, or by asymptotic notations of watermarking algorithms. Lesser the time taken by method, more efficient algorithm proves to be.

5) Security*:* Another aspect to consider is the Security of the watermarking scheme. However, it is difficult to quantify and therefore compare how much secure an algorithm is. It can either be yes or no i.e. it is either secure or it is not secure.

6) Key*:* Watermark key is one that is used to embed and extract watermark to and from image. The key identifies the legal owner of the original content, be it an image or a video or any other kind of data. Mainly in case of blind algorithms, the watermark key is very helpful to extract the watermark and thus recover the tampered content and restore it to its original form.

7) Unambiguousness*:* Retrieval of watermark should unambiguously identify the owner. Also, the accuracy of owner identification must not degrade much in the case of an attack. Watermarking the watermarked image is also a major threat as it confuses the extraction system to identify whose watermark was initially present. Also watermarking the watermarked image changes the originally placed watermarked in the data and hence the identification becomes difficult.

2.4 Types of Watermarks

Watermarks can either be blind or informed watermarks. By blind it means that the content of host does not matter. The watermarking schemes can use any other image as the watermark for the host image. But this is not the case with informed watermarking techniques. Informed watermarking techniques use the content from the image as a watermark. These algorithms use region of interest as the watermark. The watermark can be distributed throughout the image keeping the balance between robustness and the imperceptibility factors.

On the basis of application it can be either source-based watermarking or destination-based watermarking. Source-based watermarks are desirable for ownership identification or authentication where a unique watermark identifying the owner is introduced to all the copies of a particular image being distributed and to determine whether the received image has been tampered with. Whereas destination-based watermark is where each distributed copy gets a unique watermark identifying the particular buyer and can be used to trace the buyer in the case of illegal reselling [19].

Watermarks and watermarking techniques can also be divided into different categories depending upon the type of content or document to be watermarked: text watermarking, image watermarking, audio watermarking and video watermarking. To embed a watermark in an image is referred to as image watermarking. Similar is the case with other types of watermarking categories. In this paper focus will be on image watermarking, since it can further be applied to video contents also by taking frames.

2.5 Watermarking Domains

The watermarking techniques can be divided into two main domains: spatial domain and transform domain.

An image is an array or a matrix of square pixels (which are the smallest picture element) arranged in columns and rows. These pixels are as small as small dots on the digital screen. And each pixel carry a numeric value that describes the color that is the level of brightness at that point. Thus, a digital image can be described as a matrix of numbers. The spatial representation of an image is the function of space involving the coordinates x and y. Hence a digital image is a two-dimension array of numbers. This representation of the image is called as spatial representation of the image.

Inserting the watermark into the spatial domain component of the cover image is a direct method that means it slightly modifies one or two pixels of randomly selected subsets of the image. Easy to implement and require less computations. But the problem is that in spatial domain, the watermark is more susceptible to attacks than in transform domain [14].

In transform domain, or what is also called as frequency domain, the magnitude of coefficients are modified while embedding watermark [14]. Hence, watermarking schemes using transform domain have resulted in more robust algorithms.

The basic watermarking techniques in transform domain (also known as frequency domain) are: Discrete Frequency Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). Nowadays, DCT and DWT are the most popular techniques for image compression [5]. DWT gives better compression ratio without losing much information but needs more processing power. While in DCT low processing power is needed but it has block artifacts means loss of some information. Thus frequency domain methods are more robust to malicious attacks. Transform domain techniques are discussed in detail in later chapters.

Other domains include: Radon transform, fractals transform, chirp-Z transform, Hadamard transform, Singular value decomposition (SVD) and Fourier Mellin (FM) transform.

2.6 Extraction Algorithms

On the basis of how the watermark is extracted from the watermarked tampered image, the extraction of the watermark can be: blind [10], semi-blind [19] and non-blind approach.

Blind watermarking or public watermarking does not need the cover signal (the original signal) during the detection process to detect the watermark. Solely the key used during embedding is required for extraction. Whereas in semi-blind approach, the original watermarked image is required for extracting watermark from the received data. In case of non-blind watermarking (also referred to as private watermarking) the original cover signal is required during the detection process. Generally, the non-blind watermarking techniques are robust against image processing attacks.

Developing a blind watermarking scheme is a challenging task as there is no original image or the actual embedded watermark available at the extraction phase to compare the tampered image and figure out what modifications the image has gone through. Thus in this thesis, I develop a blind watermarking scheme as these are more efficient since we do not require to provide the real or original data to the extraction system for the detection of tampers.

2.7 Attacks on Digital Watermarks

In watermarking terminology, an *attack* is any processing that may impair detection of the watermark or communication of the information conveyed in the watermark. The processed watermarked data is then called attacked data. Robustness is an important aspect of any watermarking scheme. Its notion is clear: A watermark is robust if it cannot be impaired without also rendering its carrier (cover, host) data useless. Hence, an attack can only be said to be successful to defeat watermarking scheme if it impairs the watermark beyond acceptable limits while maintaining the perceptual quality of the attacked data.

The literature of watermarking attacks is also huge. The wide class of existing attacks can be divided into four main categories: removal attacks, geometrical attacks, cryptographic attacks and protocol attacks.

2.7.1 Removal attacks

Removal attacks aim at complete removal of a watermark from the cover data. Denoising stems from the idea that watermark can be treated as a noise of some statistical properties. Therefore, it can be estimated from the available copy of watermarked data. Image denoising is mostly based on maximum likelihood (ML) or minimum mean square error (MMSE) criteria. Lossy compression has been shown to have roughly the same influence on noise removal as denoising.

Other attacks in this group are statistical averaging and collusion attacks. Many instances of a given data, each time signed with a different key or different watermark are averaged to compute the attacked data. If the number of available data sets is large enough the embedded watermark may not be detected anymore assuming that on average it will yield zero mean. With the collusion attack, many instances of the same data are available, but this time the attacked data is generated by taking only a small part of each data set and rebuilding a new attacked data set.

2.7.2 Geometrical Attacks

In contrast to the removal attacks, geometrical attacks intend not to remove the embedded watermark itself, but to distort it through spatial or temporal alterations of the stego data. The attacks are usually such that the watermark detector loses synchronization with the embedded information.

Although robustness to global affine transformations is more or less a solved issue, the local random alterations integrated in Stirmark still remains an open problem almost for all techniques. The so-called random bending attack exploits the fact that the human visual system is not sensitive against shifts and local affine modifications. Therefore, pixels are locally shifted, scaled and rotated without significant visual distortions.

2.7.3 Cryptographic and Protocol Attacks

Cryptographic attacks are brute force methods to find the secret information through exhaustive search. Since many watermarking schemes use a secret key it is very important to use keys with a secure length. The protocol attacks aim at general watermarking framework.

To resist watermark inversion, the copyright protection algorithm watermarks need to be non-invertible. Otherwise, an attacker who has a copy of the stego data can claim that the data contains also the attacker's watermark by subtracting his own watermark, thereby creating an ambiguity. Non-invertibility requires that it should not be possible to extract a watermark from non-watermarked image. As a solution, it is proposed to make watermarks signal-dependent by using a one-way function.

2.8 Structure of the Thesis

The rest of the thesis has been organised as follows:

Chapter 3 describes the Literature Survey in the field of image watermarking.

Chapter 4 gives an overview of transform domain techniques.

Chapter 5 describes the Problem Statement i.e. the aim and the objective of the thesis.

Chapter 6 presents the complete detail on Discrete Wavelet Transform

Chapter 7 presents the proposed solution in detail

Chapter 8 gives the simulation results, and

Chapter 9 consist of the conclusion of this thesis.

CHAPTER 3

LITERATURE SURVEY

Within the digital watermarking field, image watermarking has attracted lot of attention among the researchers. That is most of the work is done in case of image watermarking as compared to video or audio watermarking. There can be many reasons for it. First can be the easily availability of the standard images for image processing. There are many standard databases which are available free of cost to the researchers and all varieties of images are available. Second reason can be that it can be assumed that if a watermarking technique is applicable to images then it could be extended to the videos by taking frames of the video at some instant. Some of the related works I have gone through are mentioned below.

In the work of [3], the effects of block sizes on the various attributes of watermarking such as robustness, security, capacity, time taken to embed, visibility and the amount of distortions have been studied. Normally the block-size for watermarking algorithm application is 8 x 8. Discrete Cosine Transform (DCT) of frequency domain is used to break the function into various frequency bands and allows watermark to be easily embedded. From the study it can be derived that as the block-size increases, the robustness and the capacity also increases. The PSNR value of 62-70 dB robust is achieved. But increasing the block-size further the quality of image gets degraded. However, increasing block-size decreases the computational time and also the distortions decreases sharply.

In [4], an imperceptible and a robust combined DWT-DCT digital image watermarking algorithm is described. The algorithm watermarks a given digital image using a combination of the Discrete Wavelet Transform (DWT) and the Discrete Cosine Transform (DCT). Performance evaluation results show that combining the two transforms improved the performance of the watermarking algorithms that are based solely on the DWT transform.

The authors in [5] have presented a DWT based Dual watermarking technique. Both blind and non-blind algorithms are used for copyright protection. The DWT coefficients are primary watermark (logo), are modified using another smaller secondary binary image (sign) and the mid-frequency coefficients of the host image. Since it is an informed watermark, the security increases two-fold. Pseudo-random generator is used to embed watermark randomly in the host image. The method has the ability to withstand cropping, rotation, JPEG compression, scaling and noise integration.

The work in [8] presented a robust image watermarking technique in the frequency domain using Discrete Wavelet Transform (DWT). The watermark embedding is done by tetra-furcating the watermark and is embedded into sub-bands of cover image. The signal-to-noise ratio (SNR) and peak signal-to-noise ratio (PSNR) are calculated to compare the image quality. The Normalized cross-correlation is used to measure the quality of the watermark after extraction. The watermark is divided into four parts and placed in LL_2, HL_2, LH_2 and HH_2 of cover image. The algorithm is applied on gray-scale image and multiresolution property of wavelet transform and wavelet tree-based algorithm is used. The technique is quite efficient to imperceptibility and robust to JPEG compression.

Authors in [14] presented a robust watermarking algorithm based on combined use of Discrete Wavelet transform (DWT) and Singular Value Decomposition (SVD) for protecting real property rights. The watermark is a gray-scale logo image, embedded in a LL and HH blocks of the non-overlapping blocks of the target image by modifying the SVs of the blocks. The main problem with SVD techniques is false-positive detection problem, which is solved by the combined DWT-SVD algorithm in this approach. It is a semi-blind block based watermarking technique to estimate the original coefficients. This work is a way to implement transparent and robust technique.

The work in [15] reflects a hybrid DWT-SVD technique to achieve transparency in accordance with Human Visual System (HVS). DWT and SVD are applied on both the cover and the watermarked image. The horizontal sub-band of the first level DWT of host image is used for higher level decomposition. The SVs of second level horizontal coefficients i.e. LH sub-band of cover image are modified rather than DWT coefficients directly to increase the resistivity against attacks and improve perceptual quality. The PSNR of about 40 dB is gained in this work.

The work in [23] proposes a blind watermarking technique based on Region of Interest (ROI) using Arnold Scrambling. Watermark is generated from the host image itself called informed watermarking. ROI of host image is the watermark image. First level DWT is applied and before embedding, Arnold Scrambling is performed on the approximation coefficients of the watermark as well as the blocks of host image. This results in a robust and secured algorithm for watermarking. To extract watermark the image is divided into 8 by 8 blocks. The results are tested on a gray-scale image.

The paper proposed in [18] presents a robust watermarking algorithm using the features of the host image for watermark generation. The paper also proposes the method to detect the tamper, localize where the tamper has occurred and also recover the alterations. The transform based technique – DWT is used for embedding as well as for extraction of watermark. The original image is partitioned into blocks of size 2x2 and 1D-DWT is applied to produce a watermark which is embedded in four disjoint partitions of the image to enhance the chance of restoration of the image from different cropping attack-based tampers.

The work in [20] presented a novel fragile watermarking scheme using ANN for image recovery. It is a semi-blind technique to extract the watermark and also the watermark is constructed using the features of the image. Thus, it is an informed watermarking algorithm proposed by the authors. The method has a high success ratio in recognizing the types of modifications and provides sufficient evidence.

Some more papers that are best suited for my work have been analyzed and compared as shown in the Table 3.1. In all the following papers, the blind extraction algorithm is used but there is no facility to detect tampers.

Table 3.1: Comparative analysis of the previous schemes

	Wei et al. [1]	**NR et al. [9]**	**M.Vafei et al. [10]**
Host image size	512 x 512	256 x 256	512 x 512
Operating Domain	DWT with quantization	DWT - BPNN	DWT and FNN
Embedding sub-band	LH_1 and HL_1	$LH_{4,}$ HL_4 and HH_4	LH_3 and HL_3
PSNR of watermarked image	42.02	48.12	48.25
Extraction Algorithm	Blind	Blind	Blind
Tamper Detect	No	No	No

CHAPTER 4

WATERMARKING IN TRANSFORM DOMAIN

In this work, transform domain technique is been used since it is more robust to the image processing attacks as said by the various research papers. In transform domain, the host image is first converted to frequency domain and then the coefficients are modified. After modification, the image is again converted back from transform domain to spatial domain i.e. the inverse transform is applied to get the watermarked image. The transform domain techniques commonly used for watermarking are:

- Discrete Fourier Transform (DFT)
- Discrete Cosine Transform (DCT)
- Discrete Wavelet Transform (DWT)
- Fractal Transform

There are various other techniques also such as: Fourier-Mellin transform and Complex Wavelet transform. But these will not be discussed in detail as these are not required for this thesis.

Frequency domain refers to the analysis of mathematical functions or signals with respect to frequency rather than time. A frequency graph shows how much signal lies within each frequency range. A given function or signal can be converted between time and frequency domains with a pair of mathematical operators called transform. Transform domain methods possesses a number of desirable properties:

1) Irregular Distribution*:* The watermark embedded in transform domain is distributed all over the image. This makes difficult for the attacker to extract or completely remove the watermark from the image. After the conversion from transform domain to spatial domain, the embedded data gets distributed over the area of local support.

2) Selected Frequencies*:* Transform domain allows to select the frequency range for embedding process.

The transform domain methods are the perfect example of spread spectrum communication.

4.1 Low Frequency and Mid Frequency

The frequencies of an image can be categorized into low, mid and high frequency components. The low frequency components represent the data that is most visible to human eyes. In fact, we can say that the low frequency and mid frequency components represent the detailed version of the image. Thus schemes that embed watermark in such components of the transform domain are the robust and the compression algorithms hardly affect these frequency areas.

4.2 Energy distribution of transforms

In the DCT transform domain, the energy concentrates in the low frequency regions around the upper-left corner. But in multiresolution DWT transformation, the low frequency components are present in the approximation sub band, also located in the upper-left corner, but the high-frequency components are present in the detailed sub bands at several resolutions. Most energy of the detail sub-bands are located in the edge areas and the textured regions.

4.3 Cost of transforms

The main disadvantage of the transform domain techniques is the computational cost of the algorithm. The spatial domain techniques are easy to compute but at the same time they are not robust to malicious attacks whereas frequency domain techniques are more robust and also the imperceptibility value is high.

CHAPTER 5

PROBLEM DESCRIPTION

Digital watermarking has received a great attention among researchers for securing the data from illegal actions. After studying various papers on Digital Watermarking, it is found that there is a need for a more efficient algorithm for embedding watermark as well as for its extraction. Among various applications of digital watermarking mentioned above, the application that has got least attention is tamper detection. Thus, detecting tampers in the watermarked image that is being attacked is the basis of this paper.

Also there is a scope for a more robust algorithm in transform domain rather than in spatial domain. Thus, in this proposed work the focus will be on Frequency domain technique like Discrete Wavelet Transform (DWT) among various others.

Among the works that has been done on tamper detection, blind watermark extraction for detecting tampers is very rare. So this thesis proposes a tamper detection digital watermarking scheme in blind domain. The goal is to develop a solution for Copyright protection and Owner Authentication in digital images. This paper aims to optimize the trade-off between the twin parameters of image watermarking: imperceptibility and robustness. I, thus propose a DWT-based image watermarking scheme for tamper detection and localization.

CHAPTER 6

DISCRETE WAVELET TRANSFORM

It is well known from Fourier theory that a signal can be expressed as the sum of a, possibly infinite, series of sines and cosines. This sum is also referred to as a Fourier expansion. The big disadvantage of a Fourier expansion however is that it has only frequency resolution and no time resolution. This means that although we might be able to determine all the frequencies present in a signal, we do not know when they are present. To overcome this problem in the past decades several solutions have been developed which are more or less able to represent a signal in the time and frequency domain at the same time. The idea behind these time-frequency joint representations is to cut the signal of interest into several parts and then analyze the parts separately.

The wavelet transform or wavelet analysis is probably the most recent solution to overcome the shortcomings of the Fourier transform. The DWT is highly preferred to overcome the challenge of obtaining a better trade-off between robustness and perceptibility in watermarking problems. It provides both simultaneous spatial localization and frequency spread of the watermark within the host image. In wavelet analysis the use of a fully scalable modulated window solves the signal-cutting problem. The window is shifted along the signal and for every position the spectrum is calculated. Then this process is repeated many times with a slightly shorter (or longer) window for every new cycle. In the end the result will be a collection of time-frequency representations of the signal, all with different resolutions i.e. *multiresolution analysis*. In the case of wavelets we normally do not speak about time-frequency representations but about time-scale representations, scale being in a way the opposite of frequency, because the term frequency is reserved for the Fourier transform.

The wavelet transform is calculated by continuously shifting a continuously scalable function over a signal and calculating the correlation between the two. When discrete wavelets are used to transform a continuous signal the result will be a series of wavelet coefficients, and it is referred to as the wavelet series decomposition.

Wavelet transform decomposes a signal into set of basic functions called wavelets. Wavelets are obtained from a single prototype wavelet y(t) called mother wavelet by dilations and shifting.

$$\psi_{a,b}(t) = \frac{1}{\sqrt{a}}\psi(\frac{t-b}{a})$$

where *a* is the scaling parameter and *b* is the shifting parameter.

Wavelet analysis is carried out to divide the signal into:

- Approximation signal
- Detailed sub-signals.

Approximation signal (LL band) consists of the low frequencies of the signal and shows the general trend of the pixel values. Thus, this sub-band of image decomposition looks very much like that of the original image but with degraded quality i.e. the edges are not sharply defined.

Detailed signals are further divided into 3 sub-bands:

- Low-high (LH) band
- High-low (HL) band
- High-high (HH) band.

These consists of high frequencies of the signal. LH band represents horizontal frequencies, HL band shows vertical frequencies and HH band represents diagonal frequencies of the image or signal. Thus an image is decomposed into four sub-bands.

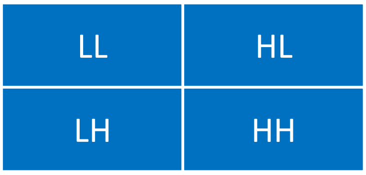


Fig. 6.1: The 4 sub-bands of DWT decomposition

The LL sub-band contains maximum image energy. So, decomposing as well as embedding to this level is robust but perceptive. On the other hand, the higher frequency HH sub-band is less sensitive to human eye. It contains the texture and edge information of an image. Data hidden to this band is not robust enough to image filtering. The watermark can easily be destroyed by attacks like JPEG compression. Also, any change in vertical sub-band components can be perceived quite easily than to horizontal components.

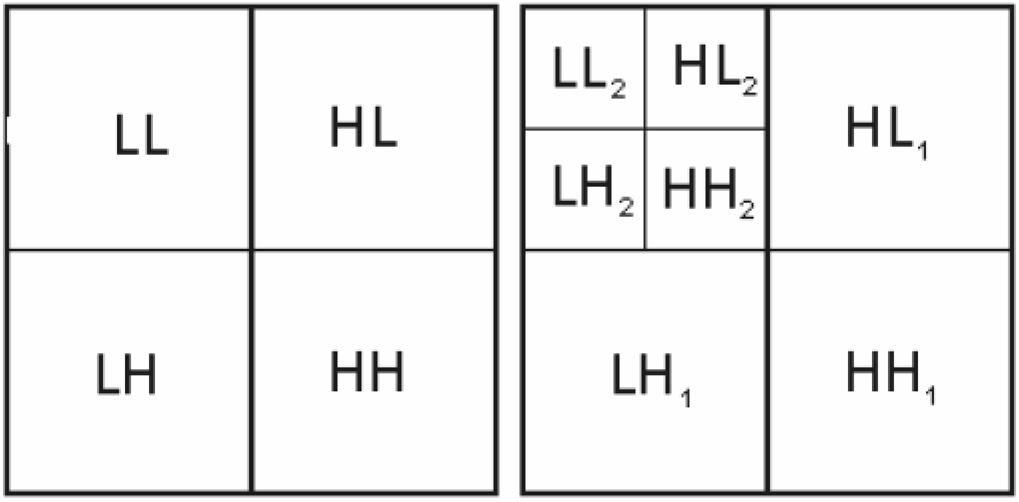


Figure 6.2: 1-scale and 2-scale 2D Discrete Wavelet Transform

To understand the basic idea of DWT focus on the one dimensional signal. A signal is split into parts, high frequencies and low frequencies. The edge components of the signal are largely placed in the high frequency part. The low frequency part is again split into two parts of high and low frequency. This process continues until the signal is entirely decomposed as needed by an application.

For watermarking applications, generally not more than five decompositions are computed. Figure 6.2 shows 2 level decomposition of the signal through a block diagram. Moreover, from the decomposed signal the original signal (or the image) can be reconstructed. This reconstruction process is called as inverse DWT transform.

For most of the signals, the low-frequency content is the significant part. This part is what is called as approximation sub-band as described above as this band gives the signal its identity. On the other hand, the high frequency content may contain a lot of noises that is the data that is usually irrelevant. If we talk about audio signals, removing the high frequency components, do changes the voice but still one can figure out what is being said. Similarly is the case with the digital images. If we remove high frequency bands from the image, the image gets blurry, but still by looking at the image one can figure out what objects are being displayed in the image or what information the image is providing. Figure 6.3 represents the 2-level decomposition on the Lena image. (Image taken from http://www.novagraaf.com/en/services/).

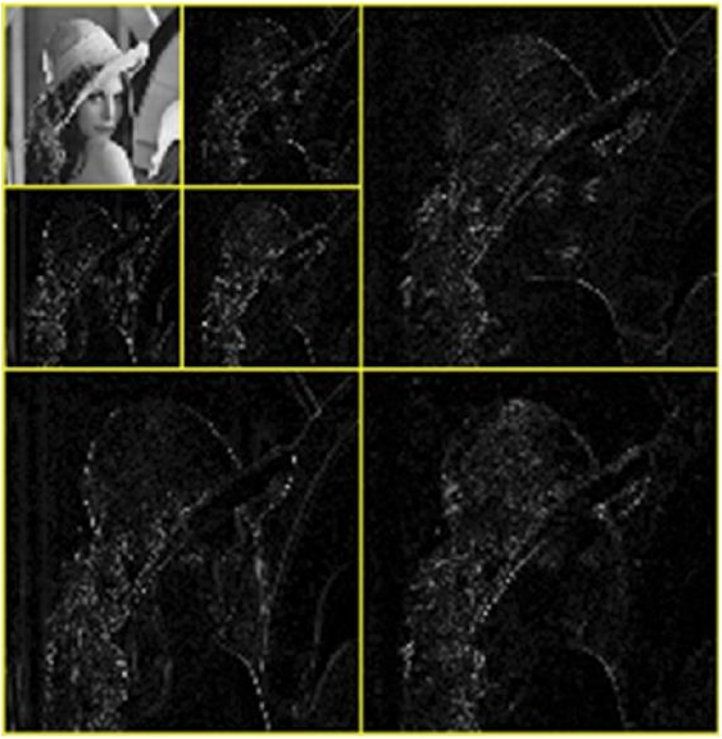


Figure 6.3: 2-level decomposition on the Lena

DWT is very efficient for image compression. If sub-signal is very small i.e. it can be set to zero then the compression ratio increases. This method is very efficient for signals having high frequency for short durations.

For computational simplicity, DWT is performed using Haar wavelet in this paper.

CHAPTER 7

PROPOSED SCHEME

The proposed method attempts to provide better security, imperceptibility and robustness against the various attacks. This technique is a blind scheme which embeds the watermark using DWT and extraction is done to detect the tamper. The watermark used for embedding is extracted from the host image itself. There are 2 distinct phases:

- watermark embedding and
- watermark extraction.

7.1 Watermark Embedding

The watermark preparation is done by block mapping sequence as done in [18]. The images taken in this paper are of size 512 x 512. The image is divided into blocks of 2 x 2 pixels. The steps of watermark generation are as follows:

1. Each 2 X 2 non-overlapping blocks are decomposed using DWT yielding the 4 sub-bands – LL, LH, HL and HH bands. The watermark is generated from the coefficient of the LL sub-band.
2. The image is divided into 2 halves, A and B. Let upper half be A and the lower half be B.
3. Partner blocks of part A are located at the same position in part B and vice versa.
4. The representative information of block A will be the 3 MSBs of LL sub-band of A. Similarly from block B also the watermark can be generated.
5. The DWT is performed on the mapping block to extract the LL, LH, HL and HH sub-bands.
6. The watermark is embedded by changing the 3 LSBs of the coefficient of the LL sub-band.
7. After embedding, apply IDWT to obtain the block in the spatial domain.
8. Thus, the pixels of the mapping block gets modified using the information from the partner block and the watermark gets embedded into the image.

Figure 7.1 shows the block diagram of watermark embedding algorithm of the proposed scheme.

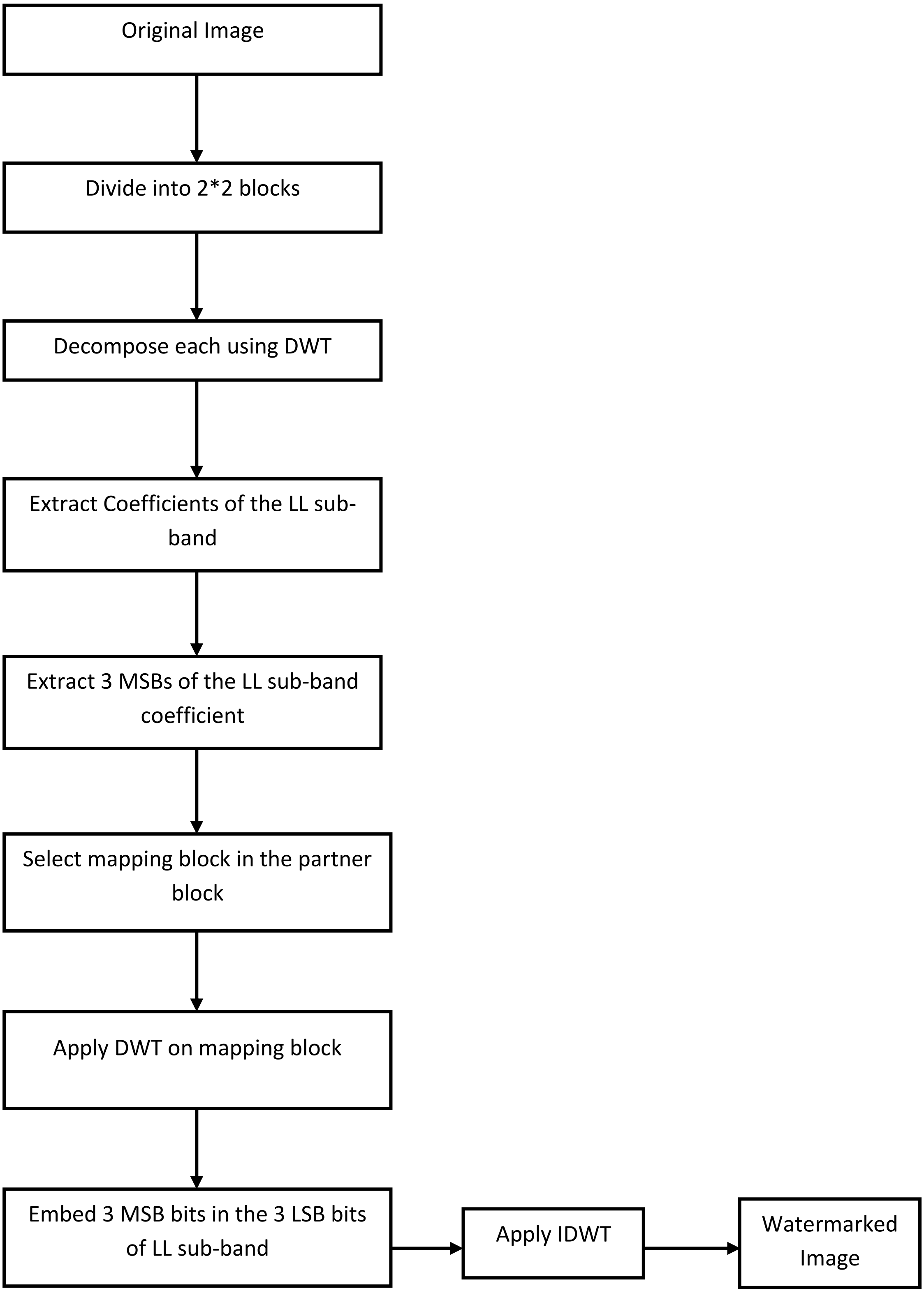

Original Image
Divide into 2*2 blocks
Decompose each using DWT
Extract Coefficients of the LL sub-band
Extract 3 MSBs of the LL sub-band coefficient
Select mapping block in the partner block
Apply DWT on mapping block
Embed 3 MSB bits in the 3 LSB bits of LL sub-band
Apply IDWT
Watermarked Image

Figure 7.1: Block diagram of the proposed watermark embedding algorithm

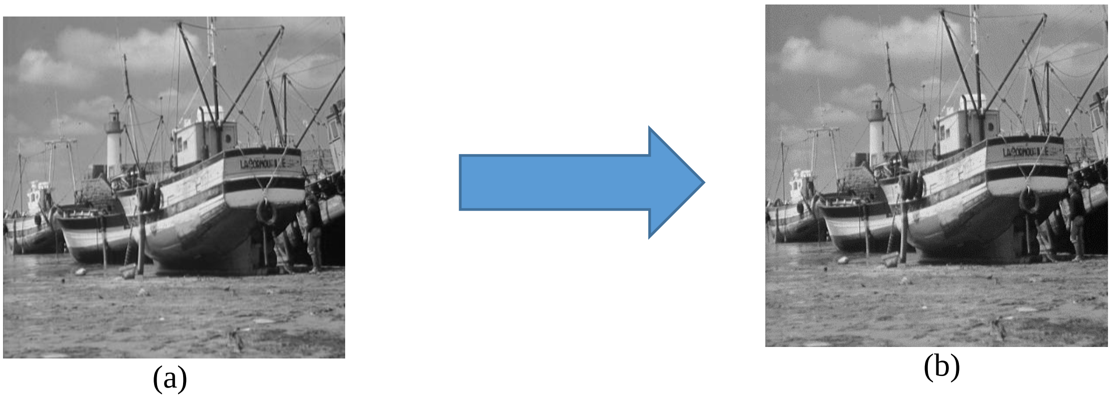


Figure 7.2: Result of Watermark Embedding: (a) original host image and (b) watermarked image with PSNR of 48.10

7.2 Watermark Extraction

Finally the tamper detection is being carried out. The extraction process is the inverse of the embedding process. The tampered area can be detected from the distorted watermarked image without using the host and the watermark images. The block diagram of watermark extraction algorithm is shown in Figure 7.3. The steps for watermark extraction algorithm are as follows:

1. Divide the tampered watermarked image into 2 x 2 blocks.
2. Apply the first-level DWT on each block using the Haar wavelet.
3. For each block, extract the 3 LSB bits of the LL sub band of DWT decomposition.
4. Compare these 3 MSB bits of the block with the 3 LSB bits of the partner block.
5. If all bits compared are same then mark the block valid else mark the block invalid.
6. Also check for neighborhood blocks. If at least 6 neighbors of an invalid are valid then mark this invalid block as valid.
7. Hence the tampered blocks are marked and detected.

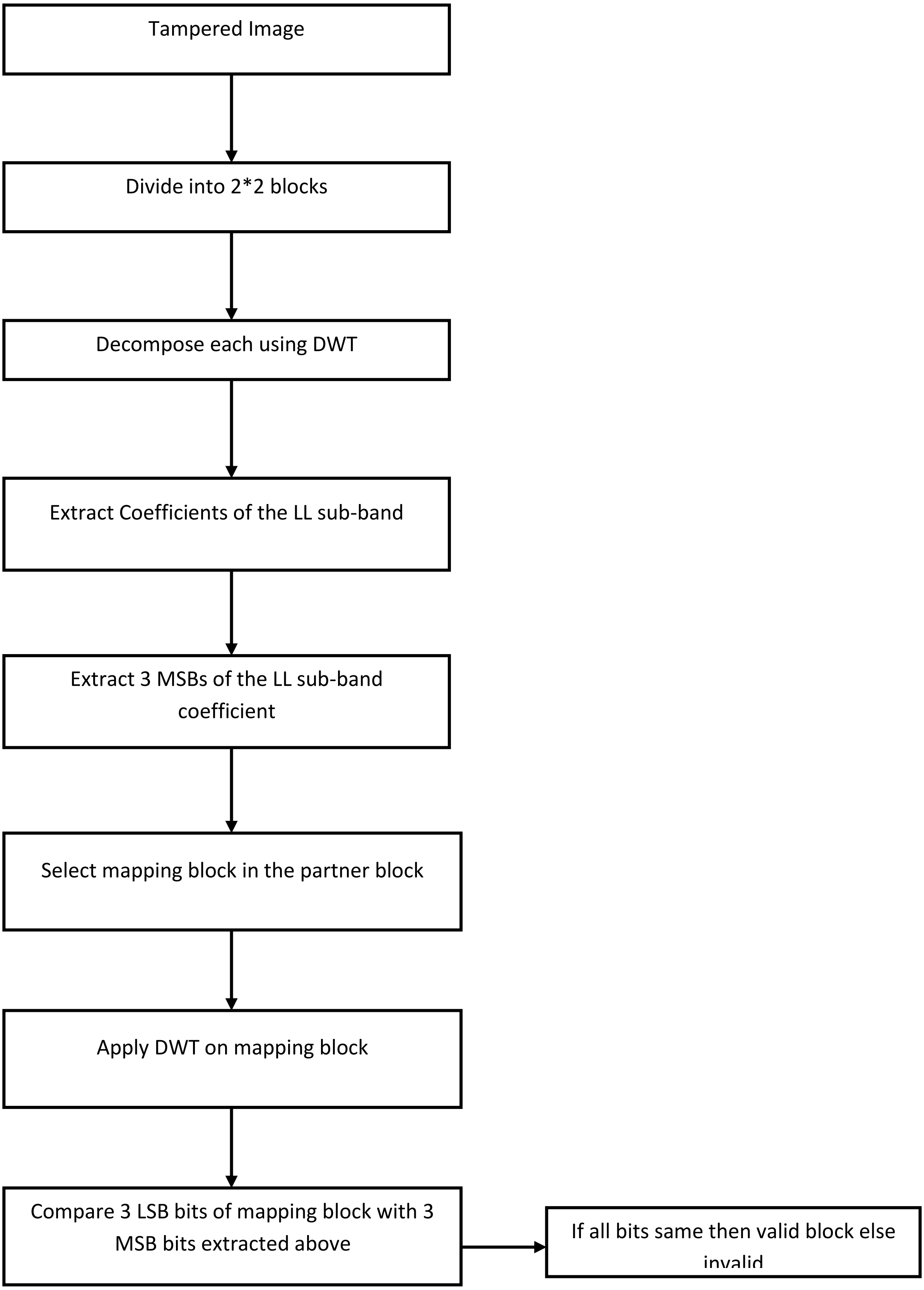

Tampered Image
Divide into 2*2 blocks
Decompose each using DWT
Extract Coefficients of the LL sub-band
Extract 3 MSBs of the LL sub-band coefficient
Select mapping block in the partner block
Apply DWT on mapping block
Compare 3 LSB bits of mapping block with 3 MSB bits extracted above
If all bits same then valid block else invalid

Figure 7.3: Block diagram of proposed extraction algorithm

CHAPTER 8

RESULTS AND EXPERIMENTAL ANALYSIS

To verify our approach efficiency, the performance of the proposed algorithm is tested on eight different gray scale images of size 512 x 512 pixels, namely Lena, Airplane, Boat, Cameraman, Elaine, Missile Vehicle, Walkbridge and Peppers. The image is divided into 2 by 2 blocks. Thus we have 65536 blocks in total, on which watermark is applied. The wavelet used for DWT is Haar wavelet. The performance and feasibility of the proposed scheme is examined through tests carried out over USC-SIPI [24], the image database used in base paper [18], which is a collection of digitized images available and maintained by University of Southern California. One more database used for tests is mentioned in this [25].

The proposed scheme and the previous works, used for comparison, have been implemented using MATLAB 9.0 (R2016a) on a system running on Windows 8 (64 bits) with Intel Core i5 CPU and 4GB RAM.

In the following section, we evaluate the performance of our approach regarding two watermarking requirements: the quality of watermarked image and tamper zones detection.

8.1 Imperceptibility analysis

Peak Signal to Noise Ratio (PSNR) is used for measuring quality of the watermarked image. The mean squared error (MSE) is needed to calculate the PSNR value. The MSE and PSNR are defined as follows:

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}|I_1(i,j) - I_2(i,j)|^2$$

$$PSNR = 20 * log_{10}\left(\frac{255}{sqrt(MSE)}\right)$$

where M and N is the number of pixels in each row and column of the image, respectively; I_1 and I_2 are the host and the watermarked images, respectively; 255 is the maximum value for the pixels values in our images which are 512 by 512 grayscale images.

Imperceptible watermarks are invisible to naked eyes i.e. human eye cannot determine the visible difference between the host image and the watermarked image. In the proposed scheme, the imperceptibility of the watermark has been examined for a wide range of images in terms of PSNR. For the watermarked images, greater values of PSNR justify the imperceptibility of the watermark. Fig. 8.1 shows the original images of Lena, Airplane, Boat, Cameraman, Elaine, Missile Vehicle, Peppers and Walkbridge and Fig. 8.2 shows their respective watermarked images. The PSNR values of the watermarked images are given in the Table 8.1.

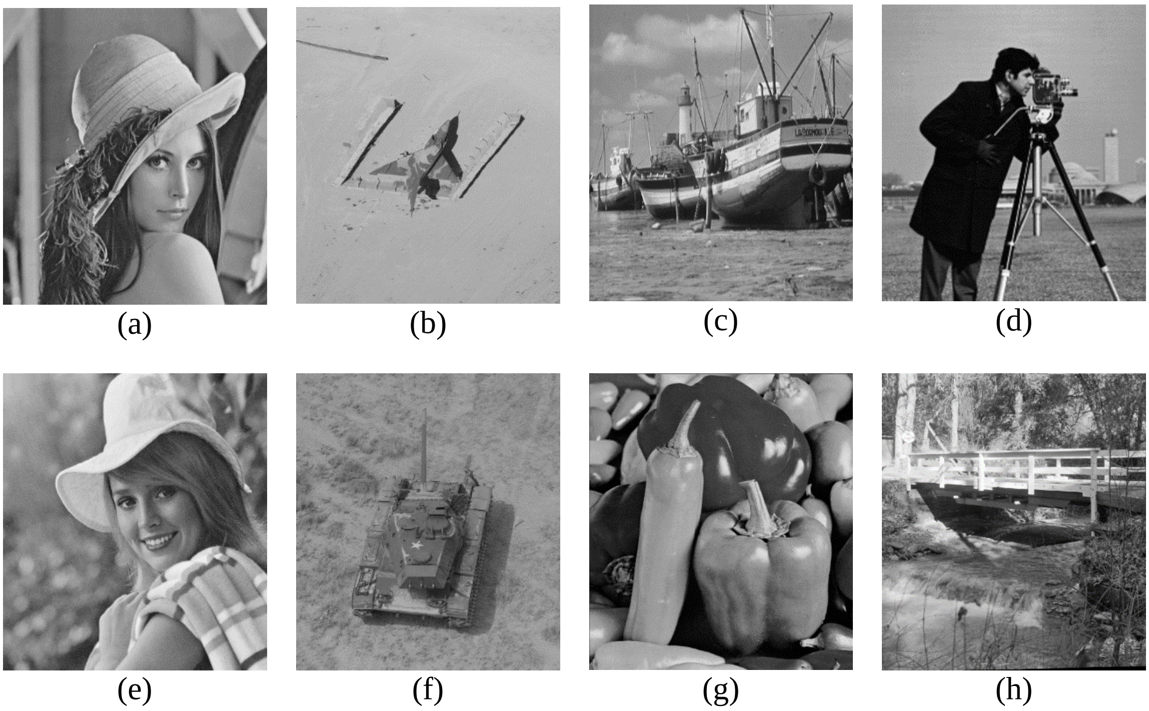
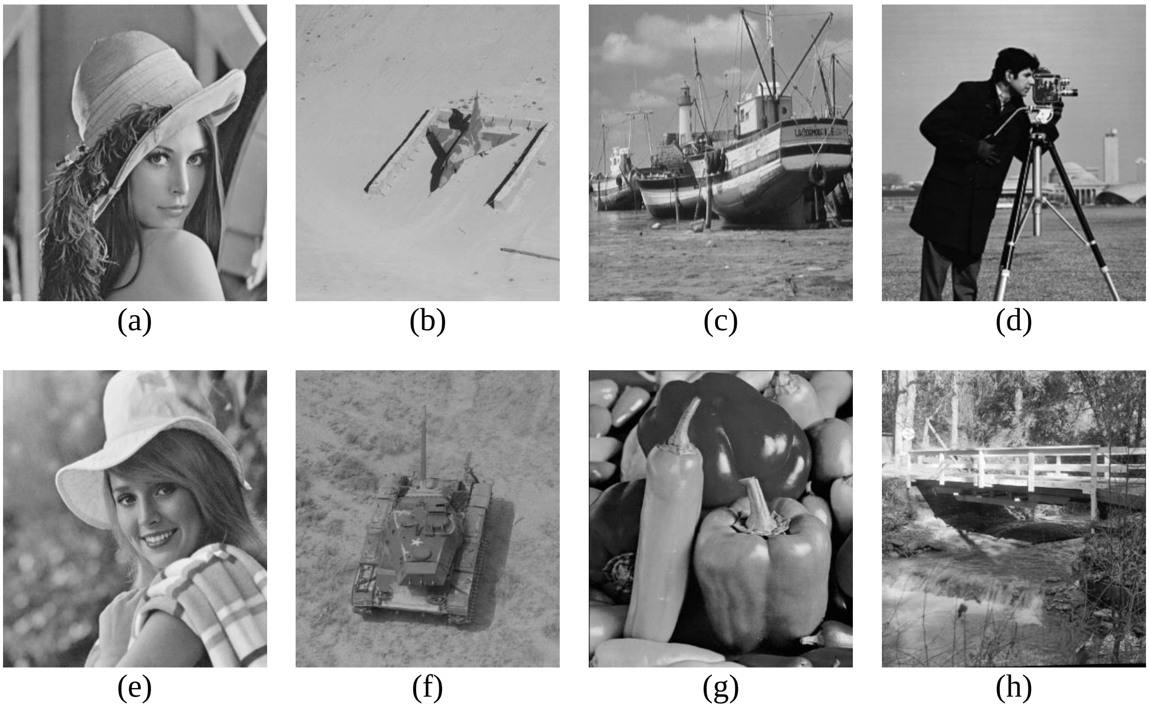


Figure 8.1: Original images: (a) Lena, (b) Airplane, (c) Boat, (d) Cameraman, (e) Elaine, (f) Missile Vehicle, (g) Peppers and (h) Walk Bridge.

From Fig. 8.1 and 8.2, it is clear that there is no visual difference between the original and watermarked images, and the proposed algorithm provides high degree of imperceptibility.



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

(e) (f) (g) (h)

Figure 8.2: Watermarked images: (a) Lenna (PSNR = 48.13), (b) Airplane (PSNR = 46.70), (c) Boat (PSNR = 48.10), (d) Cameraman (PSNR = 47.76), (e) Elaine (PSNR = 48.10), (f) Missile (PSNR = 49.02), (g) Peppers (PSNR = 47.63) and (h) Walkbridge (PSNR = 48.48).

Table 8.1: PSNR values of watermarked images

Image	PSNR (in dB)
Lena	48.13
Airplane	46.70
Boat	48.10
Cameraman	47.76
Elaine	48.10
Missile Vehicle	49.02
Peppers	47.63
Walkbridge	48.48

Table 8.2: Comparison of PSNR of watermarked images

Image name	Size	PSNR (in dB)	
		Ref. [18]	Proposed
Lena	512 x 512	41.44	48.13
Boat	512 x 512	41.32	48.10
Peppers	512 x 512	41.39	47.63

From the Table 8.2, it is clearly visible that as compared with the previous work [18] our proposed work is giving better results in terms of imperceptibility of the watermarked image.

Another criteria to measure the imperceptibility of the watermarked images is SSIM. SSIM measures the similarity or dissimilarity between two images. For a watermarked image, greater value of SSIM close to unity is best.

The SSIM index between two images I_1 and I_2 as described in [18] is computed using the following equation:

$$SSIM(I_1, I_2) = \frac{(2\mu_{I_1}\mu_{I_2} + C_1)(2\sigma_{I_1 I_2} + C_2)}{({\mu_{I_1}}^2 + {\mu_{I_2}}^2 + C_1)({\sigma_{I_1}}^2 + {\sigma_{I_2}}^2 + C_2)}$$

where μ, σ, and σ^2 denote average, variance and covariance respectively. And C_1 and C_2 are constants.

The SSIM value of the proposed and the one in the [18] are compared in table 8.3. The comparison shows that the SSIM index of the proposed is better than that in [18]. The SSIM index of all the 8 grayscale images used in this paper are tabulated in table 8.4.

Table 8.3: The comparison of SSIM index of the proposed scheme with previous scheme

Image name	Size	SSIM	
		Ref. [18]	Proposed
Lena	512 x 512	0.93	0.994
Boat	512 x 512	0.95	0.996
Peppers	512 x 512	0.93	0.995

Table 8.4: SSIM index of watermarked images

Image	SSIM
Lena	0.994
Airplane	0.991
Boat	0.996
Cameraman	0.991
Elaine	0.996
Missile Vehicle	0.996
Peppers	0.995
Walkbridge	0.999

8.2 Payload

The payload is the size of the watermark hidden in the image in terms of number of bits per pixel (bpp). In the proposed work, the size of the watermark is the function of the image size and the block size. The block size used is 2 x 2 and the images are of size 512 x 512.

The payload can be represented as:

$$\left(\frac{MN}{block\ size}\right) number\ of\ watermark\ bits$$

where, M x N is the size of the image.

8.3 Performance against Tampering

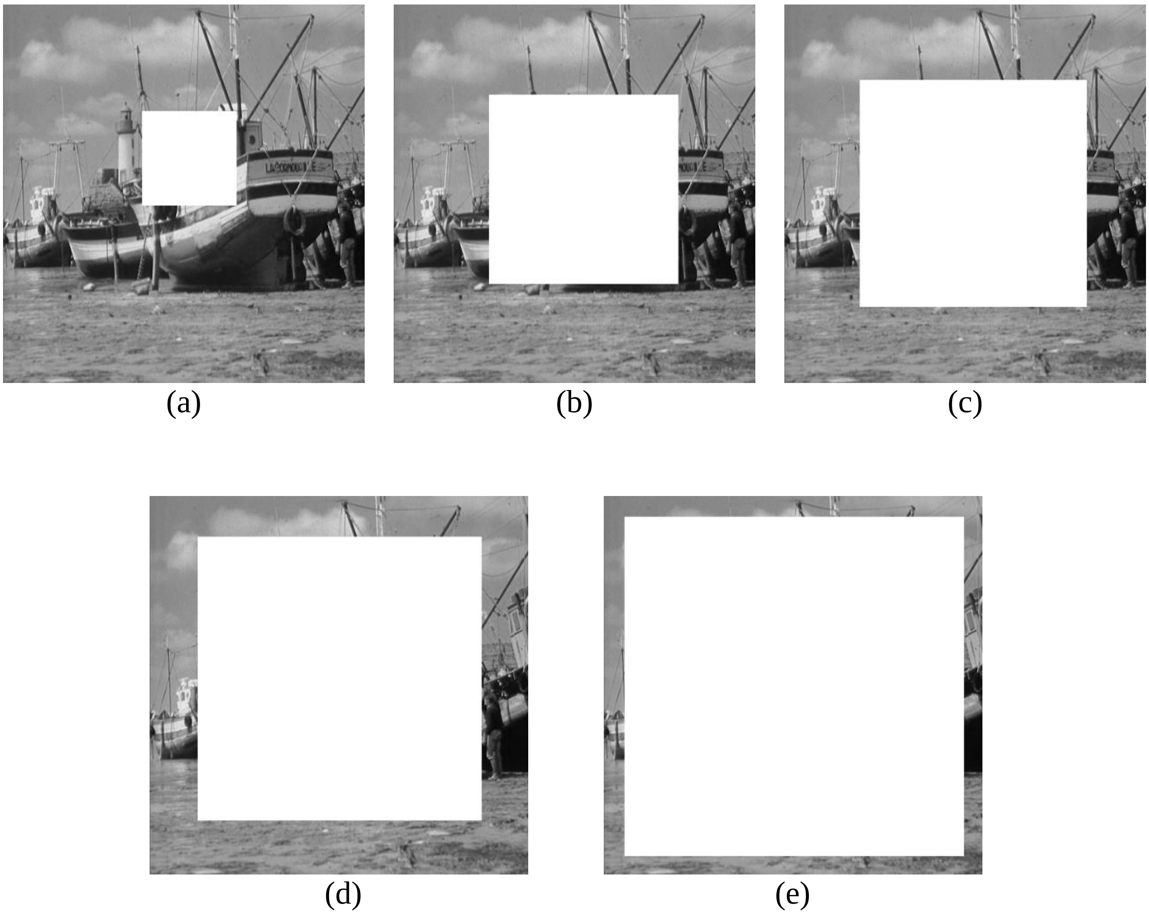
To evaluate the effectiveness of the proposed scheme, the watermarked image is tampered through different type of tampers.

The different ways of tampering can be:

1) Direct cropping which can be divided into two sub-parts: (a) cropping as a whole (a chunk is been removed from the image) or (b) multiple cropping (multiple blocks which may or may not vary in size are removed).

2) Object Manipulation i.e. a particular object is manipulated or removed from the image either as a block or unevenly leaving some part behind.

Both the above ways of tampering have been done and results are analyzed. In case of direct cropping, the various different percentages of tamper are applied and checked. Some are shown in the Figure 8.3.

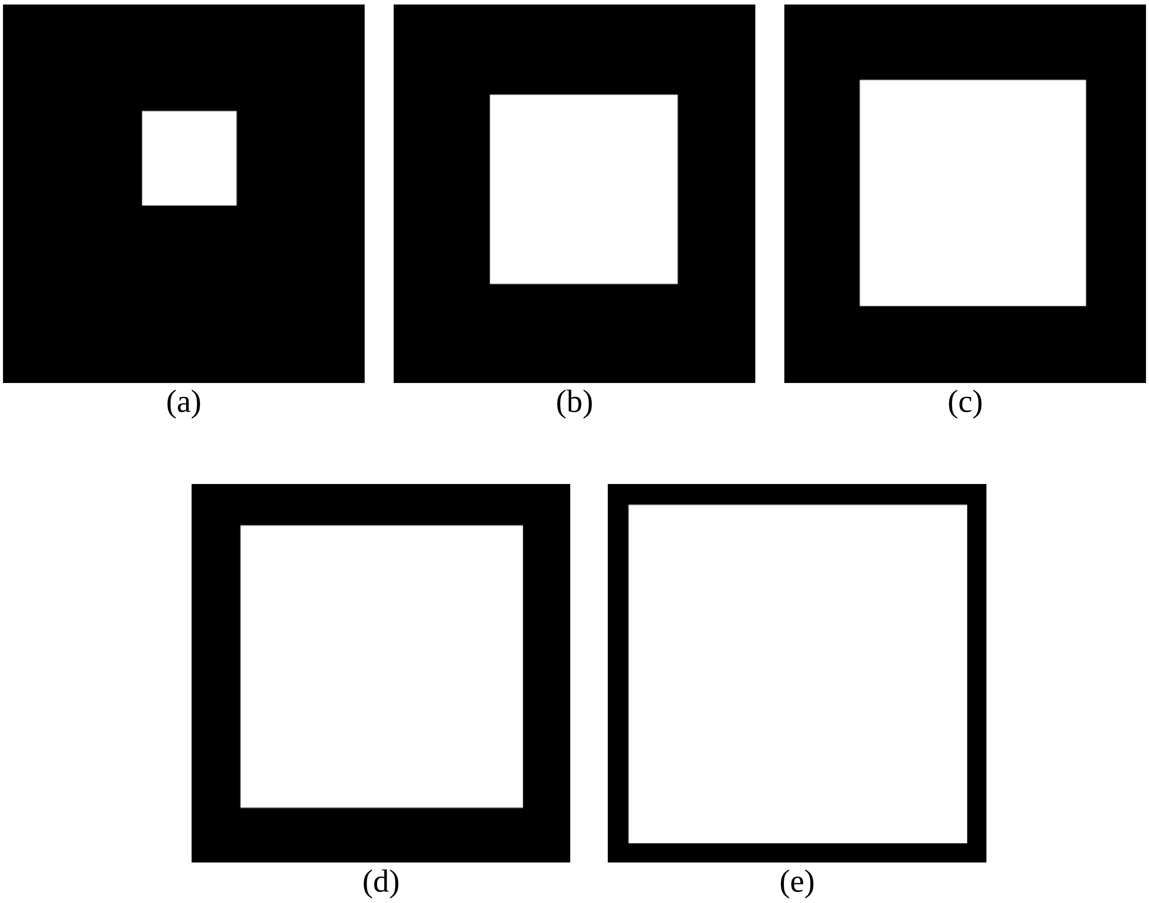


(a) (b) (c)

(d) (e)

Figure 8.3: Tampered watermarked image (a) tampered by 25% (b) tampered by 50% (c) tampered by 60% (d) tampered by 75% (e) tampered by 90%

Figure 8.3 shows the tampering by direct cropping. The images are tampered as a whole by 25%, 50%, 60%, 75% and 90%. The detection of the tampering is shown is Figure 8.4. The tampered area is marked white and the rest of the image which has not undergone tampering is black. Hence Figure 8.4 represents the difference between the original watermarked image and the tampered image. By the results, it can be derived that the proposed algorithm is 100% efficient in detecting the direct cropping tampering when the image is cropped as a whole in one chunk.


(a) (b) (c)

(d) (e)

Figure 8.4: Tamper detection of images of Figure 8.3.

Another way of tampering is directly cropping the image but this time carrying out multiple crop on the image. Figure 8.5 shows how a boat image has undergone multiple cropping. And Figure 8.6 represents the crop detection of images tampered in Figure 8.5. The results prove that the proposed scheme is very well able to detect and localize the multiple cropping tampers.

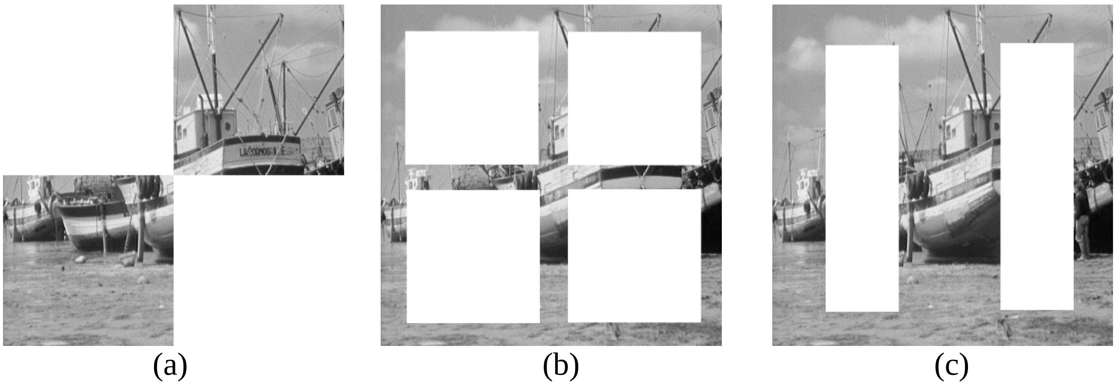


Figure 8.5: Tampered watermarked image by multiple cropping

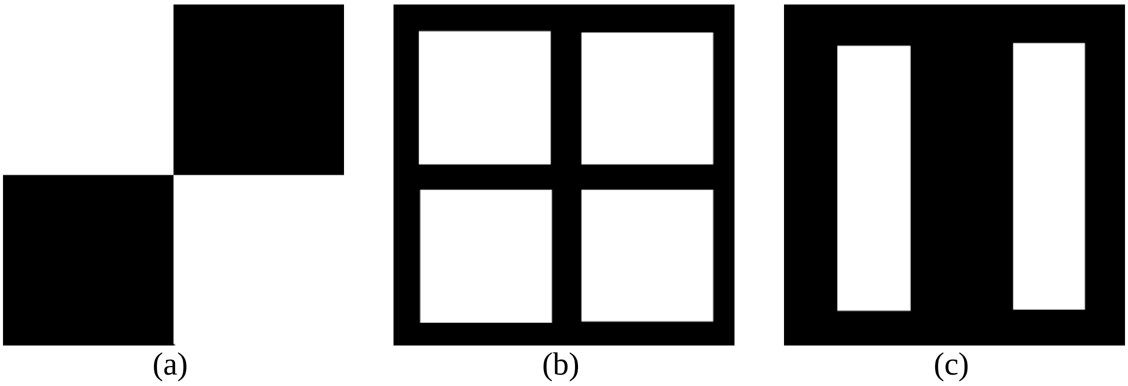
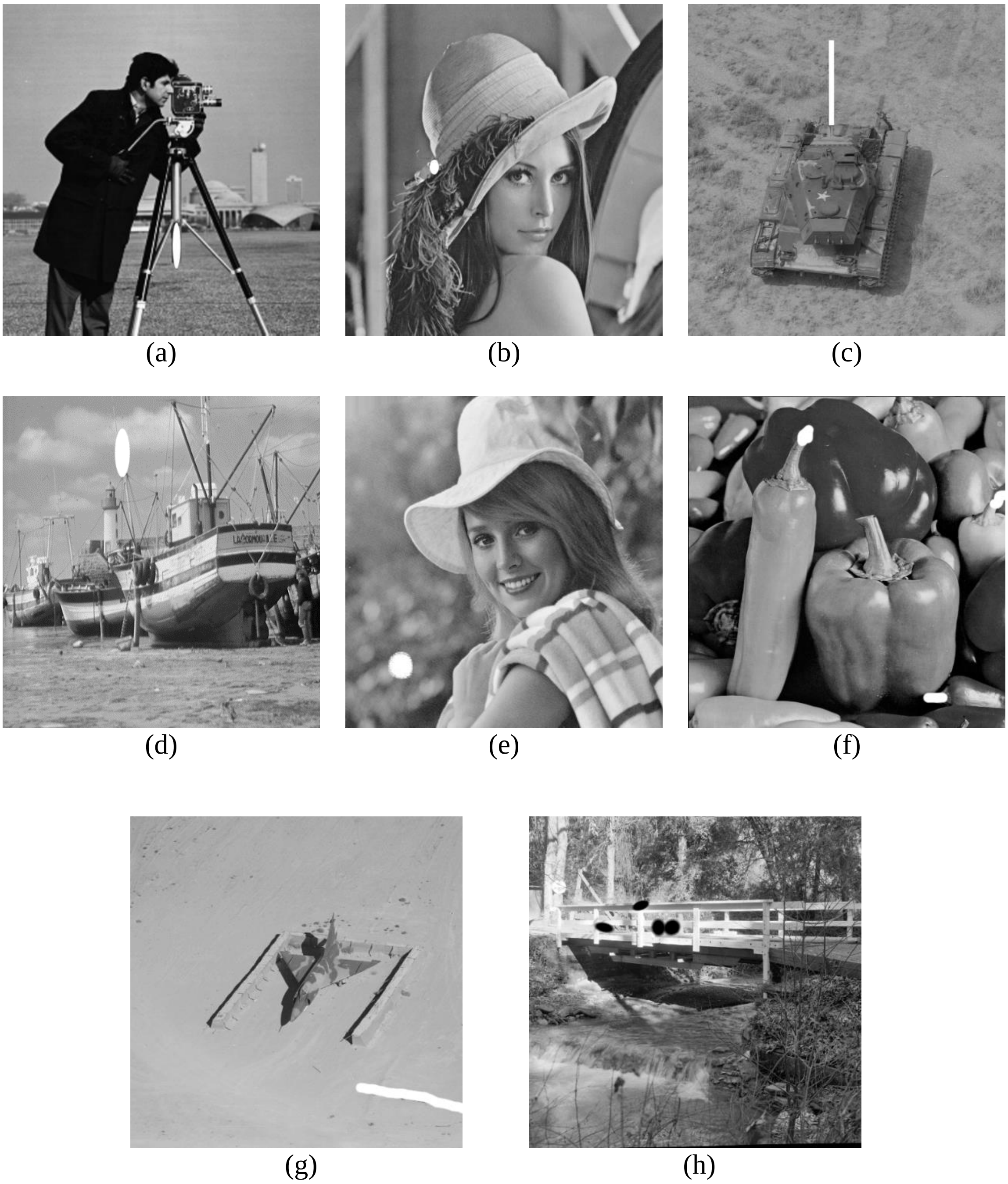


Figure 8.6: Corresponding tamper detection of Figure 8.5 (a) (b) (c)

The tampering of different images by object manipulation is represented in figure 8.7. And the Figure 8.8 shows the corresponding tamper detection.

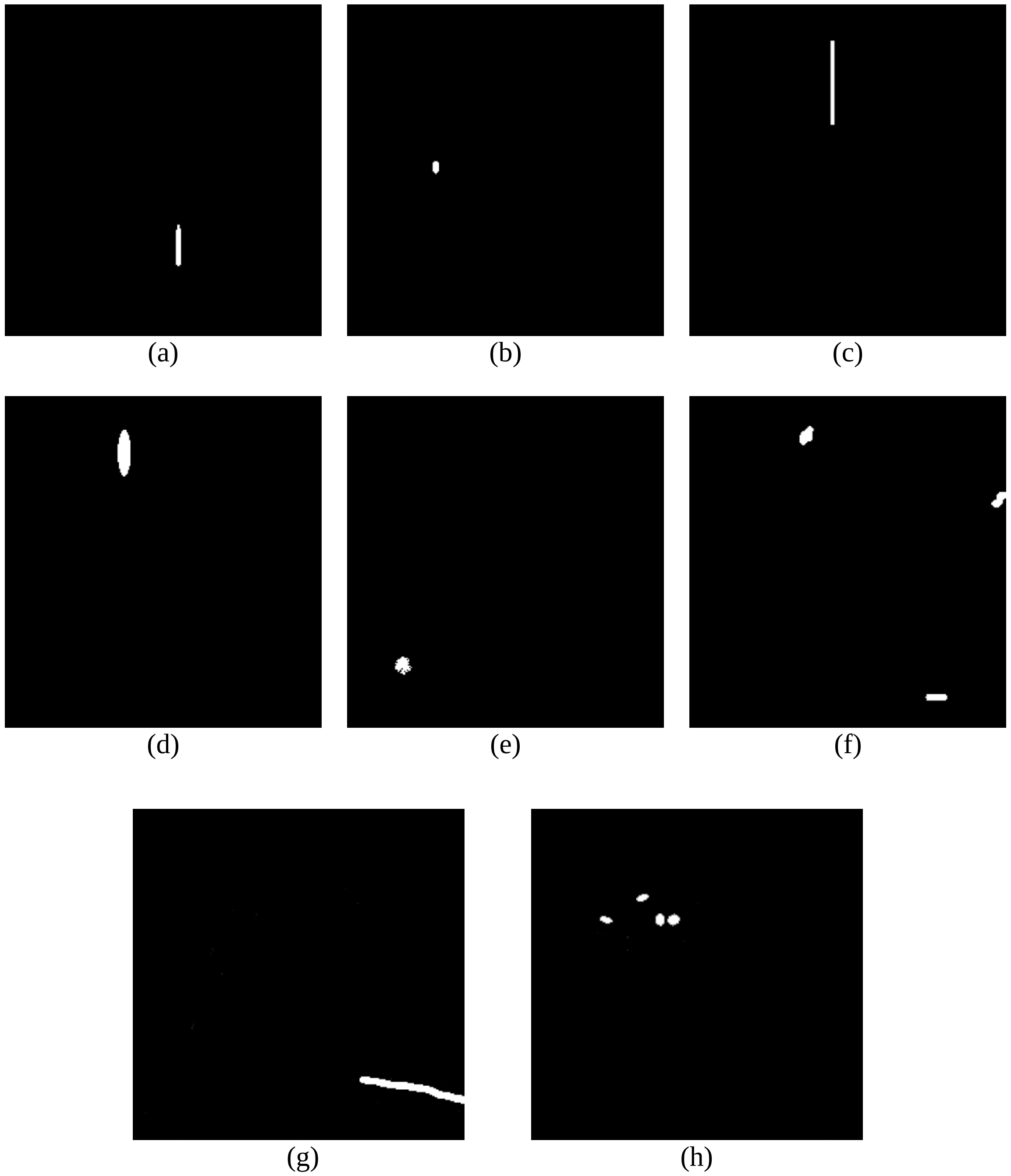
Hence all the above results prove that the proposed algorithm performs well and is successful in detection direct cropping, cropping as a whole, multiple cropping and tamper by object manipulation with an improved imperceptibility of the watermarked images as compared with [18].


(a) (b) (c)

(d) (e) (f)

(g) (h)

Figure 8.7: Tampered watermarked image by object manipulation (a) Cameraman (b) Lena (c) Missile Vehicle (d) Boat (e) Elaine (f) Peppers (g) Airplane and (h) Walkbridge.



(a) (b) (c)

(d) (e) (f)

(g) (h)

Figure 8.8: Difference between the watermarked images and corresponding tampered watermarked images in Figure 8.7.

CHAPTER 9

CONCLUSION

A blind watermarking approach is presented in this thesis. The scheme is operating in the transform domain. The watermarking is done by embedding data from the image to the image itself. Thus a sort of informed watermarking is presented in this thesis. The results of this thesis are compared with that of [18] as the paper presented in [18] is also based on a blind watermarking tamper detection scheme.

The images are watermarked by extracting MSB bits and embedding them to LSB bits of the mapping block. As the results shows, the proposed algorithm improves the quality of the watermarked images. The imperceptibility values of the watermarked images are quite high when compared to the work in [18]. Thus this approach has addressed the watermarked image quality issue (imperceptibility).

Furthermore, the extraction phase presents the tamper detection. To verify results for tamper detection, the watermarked images have been made to undergo various types of tampering and the detection results are checked. The tampering of the images are done using Adobe Photoshop CS6. This technique can detect and discover perfectly the tampered zone after applying the malicious modifications. From the achieved experimental results it can be concluded about the efficiency of the algorithm.

In future work, the scheme can be extended to recover tampers and thus build original image. This work focusses on image watermarking, but further works can extend this scheme for video or audio watermarking.

REFERENCES

[1] *Wei-Hung Lin, Yuh-Rau Wang*, 2009. A blind watermarking method using maximum wavelet coefficient quantisation, Expert Systems with Applications, Vol. 36, 11509-11516.

[2] *Samir Kumar and Shilpi Saha*, 2010. Security on fragile and Semi-fragile watermarks authentication. Int. journal of Computer Applications, Vol. 3(4).

[3] *A. T. Akinwale, M. O. Agbaje, O. Folorunso*, 2010. Effect of Block Sizes on the Attributes of Watermarking Digital Images. International Journal of Nonlinear Science, Vol. 9(3), 358-366.

[4] *AC Suthar, AM Kothari, RS Gajre*, 2010. Performance Analysis of Digital Image Watermarking Technique – Combined DWT–DCT over individual DWT, International Journal of Advanced Engineering & Applications, page- 177.

[5] *Shikha Tripathi, Nishanth Ramesh*, 2010. A DWT based Dual Image Watermarking Technique for Authenticity and Watermark Protection. Signal & Image Processing: An International Journal (SIPIJ), Vol.1 (2).

[6] *Anilkumar Katharotiya, Swati Patel, Mahesh Goyani*, 2011. Comparative Analysis between DCT & DWT Techniques of Image Compression. Journal of Information Engineering and Applications, Vol. 1(2).

[7] *Jiri Fridrich, Miroslav Goljan*, 2011. Comparing robustness of watermarking techniques.

[8] *G. Yamuna and N. Mohananthini*, 2012. A Robust Image Watermarking Scheme Based Multiresolution Analysis. I. J. Image, Graphics and Signal Processing, Vol. 4(11), 9-15.

[9] *Dr. S. Varadarajan and Nallagarla Ramamurthy*, 2012. The Robust Digital Image Watermarking Scheme with Back Propagation Neural Network in DWT Domain, International conference on Modelling.

[10] *H. Mahdavi and M. Vafei*, 2013. A new robust blind watermarking method based on Neural Networks in Wavelet Transform Domain. World Applied Sciences, Journal 22(11).

[11] *H. Pourghassem, M. Vafaei and Mahdavi-Nasab*, 2013. A New Robust Blind Watermarking Method Based on Neural Networks in Wavelet Transform Domain. World Applied Sciences Joural, Vol. 22(11), 1572-1580.

[12] *K. S. Bapat and Radhika v. Totla*, 2013. Comparative Analysis of Watermarking in Digital Images Using DCT & DWT. Int. Journal of Scientific and Research Publications, Vol. 3(2).

[13] *Lalit Kumar Saini, Vishal Shrivastava*, 2014. A Survey of Digital Watermarking Techniques and its Applications, IJCST, Vol. 2(3).

[14] *Ali Farzan, Mohammad Ali Balafar and Sedigeh Razavi Babakalak*, 2014. A new DWT-SVD based robust watermarking scheme for real property rights. ISSN: 2252-5459 (online).

[15] *Anuva Chowdhury, Md. Shahjamal*, 2014. A new DWT-SVD Based Image Watermarking Technique by utilizing the features of Human Visual System.

International Journal of Research in Computer Engineering and Electronics, Vol. 3(6), ISSN 2319-376X.

[16] *Lamri Laouamer, Muath AlShaikh*, 2015. Robust watermarking scheme and tamper detection based on threshold versus intensity, Journal of Innovation in digital ecosystems, Vol. 2, 1-12.

[17] *Pooja Kulkarni, Shraddha Bhise, Sadhana Khot*, 2015. Review of Digital watermarking Techniques. Int. Journal of Computer Applications, Vol. 109(16).

[18] *Dipabali Sarkar, Jayeeta Sarkar, Kheyali Sarkar, Sukalyan Som, Sarbani Patil, and Kashinath Dey*, 2015. A DWT-based Digital Watermarking Scheme for Image Tamper Detection, Localization, and Restoration, Springer India.

[19] *Subhayan Roy Moulick, Siddharth Arora, Prasanta K.Panigrahi*, 2015. Reliable SVD based Semi-blind and Invisible Watermarking Schemes.

[20] *Yu-Cheng Fan and Yu-Yao Hsu*, 2015. Novel Fragile Watermarking Scheme using an Artificial Neural Network for Image Authentication. Applied Mathematics & Information Sciences – An International Journal.

[21] *Hamid A. Jalab and Yahya AL-Nabhani*, 2015. Robust Watermarking algorithm for digital images using discrete wavelet and probabilistic neural network. Journal of King Saud University, pgs – 393-401.

[22] *Ms. Mahua Pal*, 2016. A survey on digital watermarking and its Application, Int. journal of Advanced Computer Science and Applications, Vol. 7(1).

[23] *Ali Aghagolzadeh and Razieh Keshavarzian*, 2016. ROI based robust and secure image watermarking using DWT and Arnold map. Int. Journal of Electronics and Communications (AEU), pages – 278-288.

[24] USC-SIPI image database: Available at http://sipi.usc.edu/database. Accessed on 1 April 2017.

[25] Image database: Available at http://www.imageprocessingplace.com. Accessed on 1 April 2017.

CERTIFICATE OF THESIS SUBMISSION FOR EVALUATION

1. Name: ………………………………………………………………………...…………..

2. Enrollment No.: ……………………………………………………………………..

3. Thesis title: ………………………………………………………………….………..

……………………………………………………………………………………..………

………………………….………………………………………...…………………..

4. Degree for which the thesis is submitted: ……………………………………………

5. Faculty of the University to which the thesis is submitted

……………………………………………………………………………………….……

6. Thesis Preparation Guide was referred to for preparing the thesis. YES NO

7. Specifications regarding thesis format have been closely followed. YES NO

8. The contents of the thesis have been organized based on the guidelines. YES NO

9. The thesis has been prepared without resorting to plagiarism. YES NO

10. All sources used have been cited appropriately. YES NO

11. The thesis has not been submitted elsewhere for a degree. YES NO

12. Submitted 2 spiral bound copies plus one CD. YES NO

(Signature of the Candidate)

Name: …………...…..…………………

Roll No: ……………….………………

Enrollment No.: ……………………..……

CERTIFICATE OF FINALTHESIS SUBMISSION

1. Name: ……………………………………………………………………...…………..

2. Enrollment No.: ……………………………………………………………………….

3. Thesis title: ……………………………………………………………….………..

……………………………………………………………………………………..………

……………………………….……………………………………...………………..

4. Degree for which the thesis is submitted: ………..…………………………………

5. School (of the University to which the thesis is submitted)
.…………………………………………………………………………………………

6. Thesis Preparation Guide was referred to for preparing the thesis. YES NO

7. Specifications regarding thesis format have been closely followed. YES NO

8. The contents of the thesis have been organized based on the guidelines. YES NO

9. The thesis has been prepared without resorting to plagiarism. YES NO

10. All sources used have been cited appropriately. YES NO

11. The thesis has not been submitted elsewhere for a degree. YES NO

12. All the corrections have been incorporated. YES NO

13. Submitted 4 hard bound copies plus one CD. YES NO

(Signature(s) of the Supervisor(s))

Name(s): …………..………………….

(Signature of the Candidate)

Name: ……..…………………….

Roll No ……………..……………

Enrollment No.: …….……………

CURRICULUM VITAE

Shruti Agarwal
M.Tech (Computer Science & Engineering)

Contact No. : - +918604620928
E-mail:- shrutiagarwallko@gmail.com

CAREER OBJECTIVE

To evolve as a successful *Computer Science Engineering* professional by utilizing my technical skills to the fullest and contribute towards industry's growth with innovative software technologies.

ACADEMIC PROFILE

Qualification	Board/University	Year	Percentage/CGPA
M.Tech (Computer Science – Software Engineering)	BBD University	2015-2017	9.07/10
B.Tech (Computer Science Engineering)	AMITY University	2011-2015	7.09/10
Intermediate (P.C.M)	ISC Seth M.R. Jaipuria School	2011	86.83%
High School	ICSE Seth M.R. Jaipuria School	2009	89.57%

PROFESSIONAL PROJECTS

- M.Tech thesis in the area of Digital Image Processing, entitled "**A Blind Image Watermarking Scheme Based on DWT for Tamper Detection**".

- JAVA based-project in a team of 4 members for the fulfillment of graduation degree.
  - **Project Title** :- **Individual Identity Recognition System**

- Underwent training in ANDROID at **TRAINEDGE CONSULTANCY,** Hazratganj, Lucknow.
  - **Project Title** :- **Mystery Doors**
  - **Duration** :- two Months (1st May'14 to 1st july'14)

  Profile: This is a user friendly gaming app where every stage is contained with new concepts.

- Underwent training in PHP at **NIIT Limited,** Hussainganj, Lucknow.
  - **Project Title** :- **College Networks**
  - **Duration** :- one Month (10th May'13 to 10th june'13)

  Profile: This is a college website with login, chat options.

- Underwent training in JAVA at **NIIT Limited,** Hussainganj, Lucknow.

- **Project Title** :- **Duke's Soccer League**
- **Duration** :- one Month (20th May'12 to 20th june'12)

Profile: Activities like register league, enter player details are available in this website.

TECHNICAL PROFICIENCIES

Operating Systems	Windows 7, Windows 8
Database	MySQL
Programming languages	C, C++, JAVA
Web Technologies	HTML,CSS
IT Technologies	Android
Software & Productivity Tools	Eclipse, NetBeans, Macromedia Dreamweaver, MySQL Workbench, MS-office-Word, MS-office-PowerPoint

CURRICULAR INITIATIVES & ACCOMPLISHMENTS

- Merited with scholarships for my diligent performance in academics for the session 2011-2012 and 2012-2013.
- Ranked 1st in my batch in PHP online exam at NIIT.
- Actively participated in various sports activities at school level.
- Executive Member of sports team in Seth M.R. Jaipuria School.
- Received proficiency certificate for my competitive workshop in Chemical Science in the year 2010.
- Participated in Social Awareness Program.
- I have been a participant in my School Orchestra for the four consecutive years 2007, 2008, 2009 and 2010.

INTERPERSONAL SKILL

- Self-Confident and honest.
- Ability to work and win with the Team.
- Ability to cope up with different situations.
- Optimistic, committed performer and a quick learner.
- Punctual, disciplined and sincere.

PERSONAL PROFILE

Father's Name	:-	Ajay Agarwal
Mother's Name	:-	Anjana Agarwal
Permanent Address	:-	287/2, Kayam Khera, Moti Nagar, Lucknow
Date of Birth	:-	16th December 1993
Languages Known	:-	English & Hindi. Novice in German.
Nationality	:-	Indian
Interest	:-	Internet browsing, listening music, exploring technical softwares.

Place: LUCKNOW