IMAGE SECURITY ENHANCEMENT BY SEMI FRAGILE WATERMARKING APPENDED WITH UNSHARP MASKING

A thesis submitted towards the partial fulfilment of the requirements
for the award of degree of

MASTER OF ENGINEERING
IN
ELECTRONICS AND COMMUNICATION

Submitted by

Alice Ghai

Roll No. 801461001

Under the guidance of

Dr. Ankush Kansal

Assistant Professor

Department of Electronics & Communication Engineering

Thapar University, Patiala-147001

Punjab, India

JULY 2016

DECLARATION CERTIFICATE

I, **Alice Ghai (801461001)** hereby declare that the work which is being presented in the dissertation entitled "**Image security enhancement by semi fragile watermarking appended with unsharp masking**", by me in partial fulfillment of the requirement for the award of the degree of Masters of Engineering in Electronics and Communication submitted in Electronics and Communication Department of Thapar University, Patiala is an authentic work carried out under the supervision and guidance of **Dr. Ankush Kansal (Assistant Professor)**, ECED.

To the best of my knowledge, the content of this project report does not form a basis for the award of any previous degree to anyone else.

Alice Ghai

Date: 8/7/16

Alice Ghai

Place: Patiala

801461001

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

Dr. Ankush Kansal
Assistant Professor (ECED)
TU, Patiala

Countersigned By:

Dr. Sanjay Sharma
Head of Department
ECED, Thapar University
Patiala, 147001

Dr. S.S. Bhatia
Dean of Academic Affairs
ECED, Thapar University
Patiala, 147001

ACKNOWLEDGEMENT

To discover, analyse and to present something innovative is to endeavour on an ungraded path towards and unexplored destination is an onerous adventure unless one gets a true torch bearer to show the right path. I would have never accomplished in completing my work without the cooperation, encouragement and help provided to me by different people. I am getting short of words to reveals my deep regards. I take this opportunity to express my subtle sense of gratitude and respect to all those who supported me through thesis duration. I acknowledge with gratitude and modesty my deficit to **Dr. Ankush Kansal (Assistant Professor)** Electronics& Communication Engineering Department, Thapar University Patiala under whose direction I had the privilege to complete my thesis. I am really very fortunate to have the opportunity to work with him.

I convey my candid thanks to **Dr. Sanjay Sharma (Head of Department),** PG coordinator, **Dr.Amit Kumar Kohli (Associate Professor**) entire faculty and staff of Electronics and Communication Engineering Department for their encouragement and cooperation.

I would like to thank my parents for their years of obstinate love and encourage, they have always desired the finest for me and I admire their determination and sacrifice. Above all I render my thanks to the Almighty who bestowed self-confidence, capability and strength in me to bring this work to completion and not letting me down at the time of dilemma. I am greatly obliged to all my friends, who have amicably applied themselves to the task of helping me with abundant moral support and esteemed suggestions helped in successful completion of the present study.

Alice Ghai

Roll no. 801461001

ABSTRACT

In present era of secure communication, various authentication techniques are usedto protect or to resolve the copyright integrity of audio, video and multimedia data files. Digital watermarking is one of the most efficient ways to protect the digital properties of multimedia files in which the original data files to be transferred are embedded with some specific information which is hard to detect and remove. The watermark should be embedded into the host image in a way that it should not degrade the quality of the original watermarked image. Digital image watermarking finds applications in varied areas like defence, medical science, intellectual property right and entertainment.Watermarked digital image is transmitted or stored.There are many promising modifications, such as cropping an image, lossy compression of the information or adding noises. So protections against such attacks should be required. In the proposed semi fragile watermarking technique LBP (Local Binary Pattern) is used for embedding watermark. Besides being able to detect all the malicious changes that affect the quality of watermarked image, it is tolerant to image compression which is essential to transmit images over the network.

In this research work, a framework for enhancement of watermarked image quality using LBP (Local Binary Pattern) watermarking and image enhancement is proposed by unsharp masking.Overall the image quality is enhanced as the PSNR calculated using LBP alone is 45.0398 and using proposed algorithm the value has improved to 66.2204.Moreover, the proposed method is robust against some commonly used image processing operations suchcompression, contrast, noise, tampering and crop attack providing PSNR of 56.6190, 50.0969, 51.0631, 41.0486 and 43.6339 respectively with MSE of 0.0560, 0.3336, 0.2245, 0.7674 and 0.6781also when compared with the traditional method there is improvement of 22.7620% in PSNR when subjected to additive noise attack, 23.8817% improvement in PSNR when subjected to contrast adjustment, compression with 18.651% improvement in PSNR under compression attack.. This technique provides good results against cropping and tampering attacks along with improvement in PSNR of 32.223% and 32.9692% respectively with least computational cost.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVATIONS

DCT	Discrete cosine transform
DWT	Discrete wavelet transform
DFT	Discrete frequency transform
HH	Diagonal high frequency band of 1level DWT
HL	Horizontal high frequency band of 1level DWT
HVS	Human Visual System
ICA	Independent Component Analysis
IDCT	Inverse Discrete Cosine Transform
IDWT	Inverse Discrete Wavelet Transform
JPEG	Joint Photographic ExpertsGroup
LSB	Least Significant Bit
MSB	Most Significant Bit
SVD	Single Value Decomposition
RST	Rotation, Scaling and Translation
PSNR	Peak Signal to Noise Ratio
MSE	Mean square error
SSIM	Structural similarity index
LBP	Local binary pattern

CHAPTER 1
INTRODUCTION

1.1 PREAMBLE

Information transmitted through images is regarded to be much more efficient and trustworthy as people tend to understand the pictorial information much more immediately and easily marking significant advantage over text and sound. An image is a two-dimensional functions $f(x, y)$, where x and y are spatial (plane) coordinates and the value of $f(x, y)$ at some pair of coordinates (x, y) is termed as the intensity or gray level of the image at that point [1]. An image contains a lot of information and can be monochromatic or colored. Pixels commonly show heights, gray levels, colors, opacities etc. A pixel is a basic unit of a colored or monochromatic image on a computer display or in a computer generated image. Digital image formation is the foremost step in any digital image processing application which consists basically of an optical system such as a sensor and a digitizer [2].Owed to the modern evolution in cyber automation and development of veritable immense pace, circuitry supervises all over therefore the security of discrete appeased are essential. Eventually, the security and protection of everyone's production has become a difficult task. So holding the preservation of digital watermarked expression i.e. text, audio image and video has accepted appreciable attention. In digital watermarking system, infiltrator tries to apply some malicious attacks to change the ownership of the digital media. The watermarking has been scheduled as a relevant solution for copyright protection approach for digital data which embed a tide mark with some extra information about the digital media without visibly altering them. Attacks applied on watermarked information can also be non-malicious like compression, smoothing/blurring etc. that are not performed intentionally, rather they attack the watermarked information during transmission over network or storage. Apart from this, there exist many malicious attacks like Rotation, Scaling and Translation (RST) attacks, flipping, cropping and affine transformation or can be signal transform attacks such as compression and noise addition that are performed intentionally [3]. Digital water marking approach consists of two parts and these are embedding and recovery and

algorithms. In the embedding algorithm, the watermark is embedded in digital media with a unique algorithm and this watermark is reclaimed from the watermarked image by extracting algorithm. The most basic and simple approach of watermark insertion is to deposit the watermark into the least significant bit of the prime image. Local Binary Pattern (LBP) is a transparent yet very productive texture operator which labels picture element of an image and neighborhood of each pixel selects a threshold value that considers the results as a binary number. This method is an example for spatial domain technique, which precisely modifies the intensities of a few chosen pixels [4].To restore the quality of image lost due to watermarking linear unsharp masking [13]is incorporated. It is a method for augmenting the perceptual quality of an image by highlighting its high-frequency components. It is an application concentrating on enhancing end contrast to boost nature of the picture.

1.2 IMAGE PROCESSING

Processing an image is equivalent to processing a signal for which image act as an input is an image, and the turn out of this operation is an altered image or a list of criterion put successively as a model in many situations. Processing an image determines the image in two ranges and utilizes assured image refining modes. It generally refers to digital image processing, but both analog and optical which are also image processing's are also possible [1]. The acquisition of images that is generating the input image in the first place is termed as imaging. It is an exercise of any algorithm, which takes input as an image and at the same time returns output as an image. Owed to the modern evolution in cyber automation and development of veritable immense pace, circuitry supervises all over, security of discrete appeased are essential. Therefore, security and protection of everyone's production has become a difficult task. So holding the preservation of digital watermarked expression i.e. text, audio image and video has accepted appreciable attention [2]. This Includes:

- Image correction and manipulation
- Image compression
- Image enhancement
- Image display and printing
- Feature detection.

1.3 Digital Image Processing

A digital image is a two-dimensional image illustrated as a fixed set of digital standards, called pixels or picture elements. Pixel values commonly show gray levels, heights, colors, opacities etc.Digitization signifies that a digital image approximates an original scene [5].Digital image processing refers to the manipulation of images using a digital computer. A picture in digital form is nothing but the collection of row and column points called as matrix. Row and column classify the point in the image and its corresponding value determines the gray level at that point. Image processing procedures could be placed at three points. At the lowest level are those methods which deal straight with the raw, probably noisy pixel values, with denoising and edge detection being noble examples. In the intermediate are procedures which exploit low level marks for additional means, such as segmentation and edge linking. At the maximum level are those approaches which attempt to abstract semantic meaning from the data delivered by the lower levels [6]. The simple components of a digital image processing scheme comprise of image acquisition, storage module, processing stage and display. Images produced using a scanner or cameras are digitized to produce digital images.

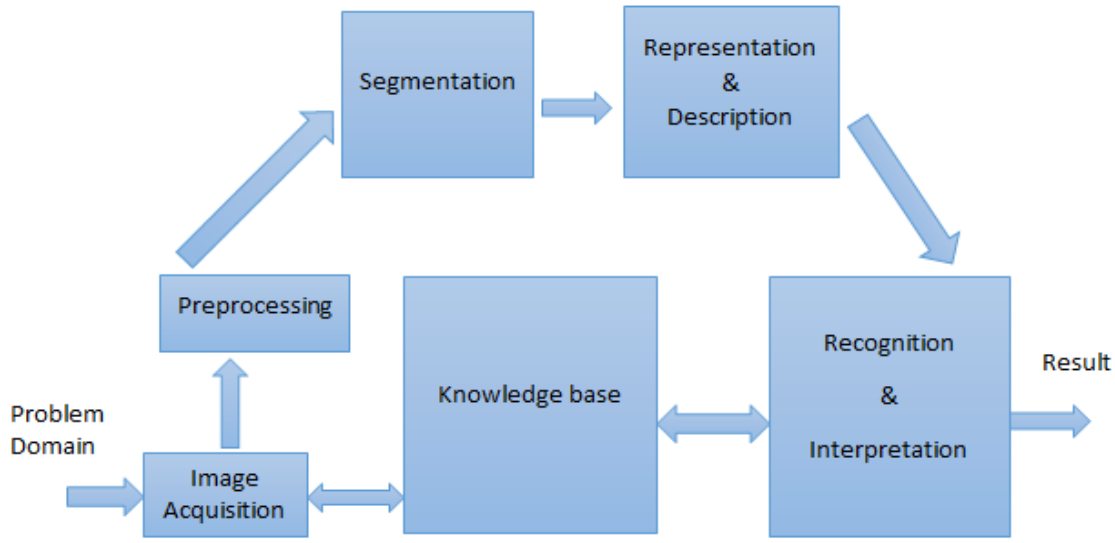


Figure 1.1Digital image processing system [2]

Digital image processing targets on two major tasks:-

- Advancement of pictorial information for human interpretation.
- Processing the image data for transmission, storage and representation for sovereign machine perception.

Digital image processing is the employ of computer algorithms to implement image processing on the digital images. Digital tide marking is a well-equipped technique for attaining content integrity security by inserting the secret data into the picture [7]. The tide marking applications include copyright associated applications, content authentication presentations, forensic and fighting applications. The objective of image verification is to offer a technique to validate the image and guarantee the truthfulness of that image but not to secure the insides from imitative or taken. The way to understand this feature is to embed the authentication tide mark into the digital image by means of a tide marking technique. In the situation of the image being tampered, it can be noticed easily because the pixel values of the embedded data would alter and could not match with the original pixel values [4].

1.4 Watermarking

Watermarking is a microscopic process in which a pattern of bits is embedded with image, which is being transferred or shared. Thus, the image is completely protected and authenticated to owner [5].It involves hiding useful information pertaining to the owner or content creator for data authentication and copyright purpose. The user who knows the algorithm only can use that specified data. Digital watermarking is used for proof of ownership copying prevention authentication purpose. Watermarking technique are characterized based on persuaded properties like robustness, transparency, security, capacity, inevitability [6]. A watermark is an unknown signal added to images that can be removed later to mark some confirmation around the host image. The main point is to discover the balance amongst the features such as robustness to numerous attacks, security and invisibility. Generally, for less intensity watermark better invisibleness is achieved and so it is necessary to select the optimum intensity to embed the watermark. [7].

The generalized block diagram of typical image watermarking scheme is shown in figure 1.2. It comprises watermark embedder and watermark extractor. The inputs to the

watermark embedder are watermark, the input data and the secret key. The purpose of this secret key is to improve the security of watermarking scheme. The output of the watermarking embedder is the watermarked content [10]. The inputs to the watermark extractor are the watermarked image, the secret key(similar as used at the time of embedding) and confine on the method, the original cover content or the watermark. A watermark detector includes a two-step procedure. The first step triggers watermark extraction that exercise one or extra pre-process to extract a vectortermed as extracted watermark.

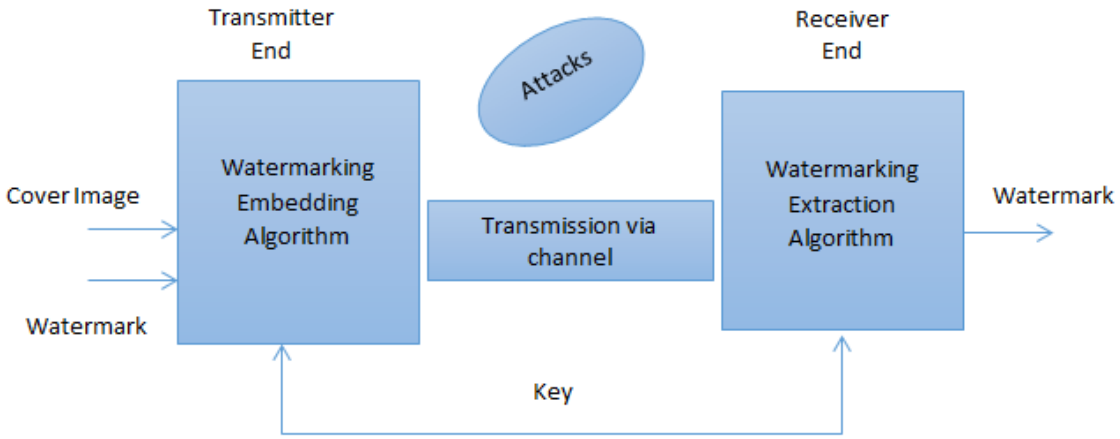


Figure 1.2 Generalized block diagram of typical image watermarking system [7].

Then the second step continues to determine whether the extracted watermark is the identical as the original watermark or not. This procedure usually includes comparing the extracted watermark with the original also named reference watermark [7]. The outcome could be certain kind of confidence measurement representing how likely the original watermark exists in the content.

1.4.1 Watermarking process

Digital image watermarking technique has two parts, namely watermark embedding algorithm and watermark extraction algorithm. Watermarking system performs these steps. In embedding, the watermark signal is produce by procedure that accepts host and data to be impose. Then this signal is capture or transmitted to other user [9]. If another user performs any alteration on watermarked signal then it is coin as attack. There may be

various available attacks on an image. To extract the watermark from image the algorithm is applied to the bombarded signal. This is termed as detection. During transmission, if there is no modification then the watermark is still commenced and it can be derived [10].

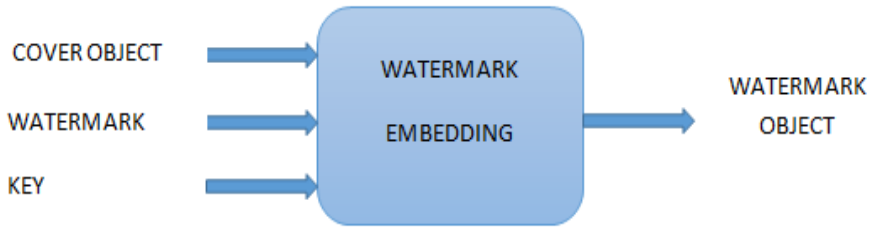


Figure 1.3 (a) Digital watermarking embedding

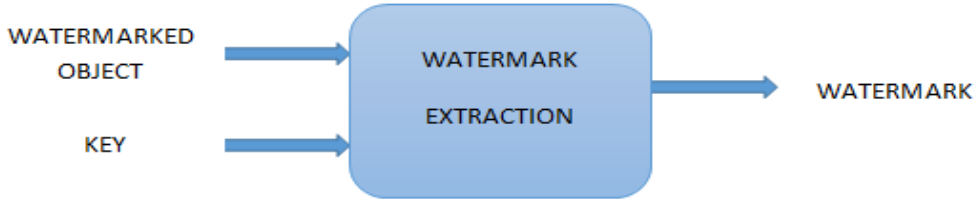


Figure 1.4 (b) Digital watermarking extraction

Three different steps namely embedding, attack and detection are usually worn to perform watermarking. The watermark embedding algorithm embeds watermark in original cover image giving watermarked image. The watermarked image is transmitted via communication media like internet or mobile phone. In watermark extraction algorithm, the watermark is extracted from watermarked image. The extracted watermark is compared with original watermark for authentication. Watermarking is a procedure of secure data from threats, in which holder identification (watermark) is combined with the digital media at the transmitter end and at the receiver end this owner identification is used to distinguish the authentication of data. This method can be applied to all digital media styles such as image, audio, video and documents [8]. Watermark can be embedded either one in spatial or frequency domain. The added watermark signal frequently modifies the host image in an irreversible manner and may mask delicate

details. The watermark can be hidden in the digital data both visibly or invisibly. For a strong watermark embedding, a good watermarking procedure is desirable to be applied.

1.5 Characteristics of watermarking

There are abounding characteristics that watermarking is maintaining are described as:

Invisibility

An embedded watermark is not noticeable. Invisible watermark is buried in the content [11]. Generally, for less intensity watermark better invisibleness is achieved and so it is necessary to select the optimum intensity to embed the watermark. Enlarged robustness requires a tougher embedding, which in turn decreases the pictorial quality of the images. An approved authority only can reveal it as it provides security for the data to be transmitted.

Computational Complexity and data payload

Computational complexity points the bulk of time watermarking procedure takes to decode and encode. To assure security and efficacy of watermark, more calculating complexity is required [9].Data payload is also termed as capacity of watermarking. It is the superlative information that can be latent without lowering image quality. It can be appraised by the quantity of latent data [12].

Robustness

Piracy assails or image processing could not influence the embedded watermark. Even if the striking watermark is withdrawn, there is the invisible one as the substitute. The visible watermark is introduced into the original image while the microscopic watermark is added to it [11].

Fidelity

Fidelity can be regarded as a measure of emotional transparency or imperceptibility of watermark. It denotes the resemblance of watermarked and un-watermarked images. Watermarking should not introduce noticeable noise as it lessen mercenary rate of the watermarked image [13].

Protection and copyright

A tidemark must conceal as well as requisite but insignificant regarding an illegal purchaser. It must exclusively be ponder able beyond atheist socialites. Here the concern acts as a protection along with tide mark which is commonly accomplished beyond the application regarding cryptographic openers [14]. Like knowledge protection methods, the specification regarding mainframe watermark procedures have to broadcast to all. Therefore, generating unrefined watermark with inevasible is a major issue. Watermarking can be used to protect redistribution of copyrighted material over the entrusted network like Internet or peer-to-peer networks [15].

Attacks

Generally, a watermark should be secret and should only be accessible by authorized parties. If the watermark is damaged or corrupted that, is if a person makes any modification on that, it indicates the presence of tampering and hence, the digital content cannot be trusted [13]. This requirement is referred to as security of the watermark and it must be robust to these manipulations. Watermark attacks are grouped into four categories based on their purpose as Simple attack, Detection-disabling attack, Ambiguity attack and Removal attack.

Non-perceptibility and Verifiability

Watermark is not visible to individual eye or not be witnessed by ears of individual, espial be perceived over exceptional mutating or devoted orbits and should abide regarding capability to contribute entire as well as dependable affirmation as the claim regarding consumed-assured knowledge commodity [16].

1.6 CLASSIFICATION OF WATERMARKING TECHNIQUES

The digital image watermarking algorithms can be classified into various techniques on the basis of criteria mentioned below.

- Human perception
- Embedding domain
- Watermark detection process
- Nature of watermark

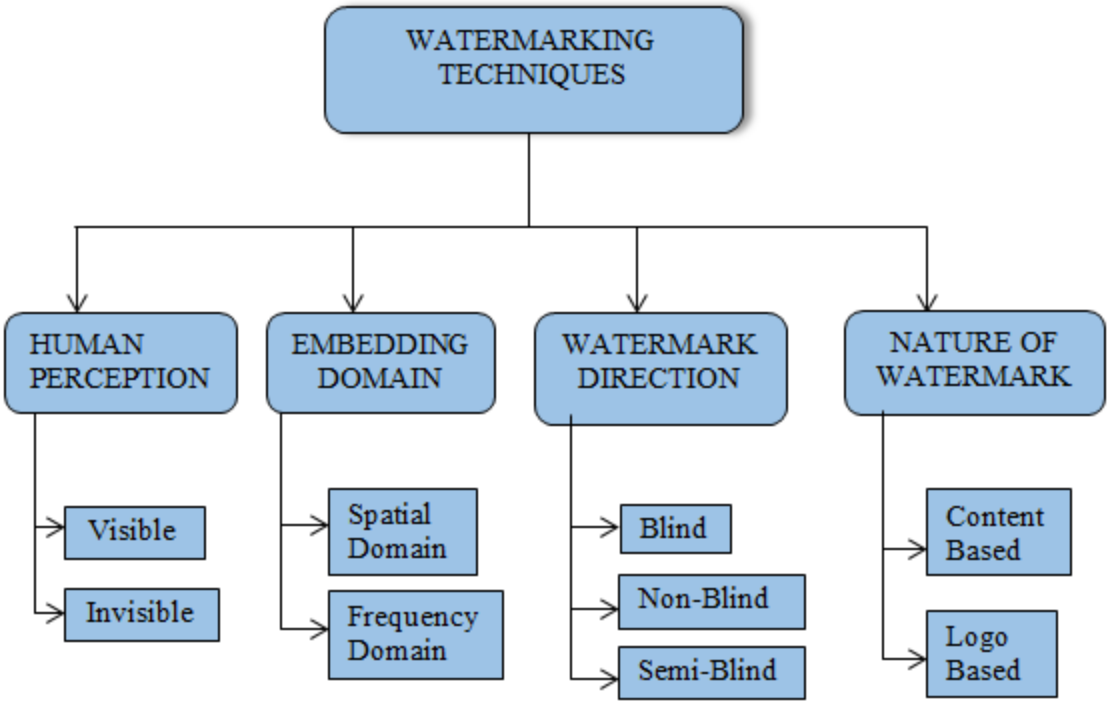


Figure 1.4Classification of watermarking techniques

Since image, authentication and content integrity are the important applications of the digital watermarking and have been analyzed in the aspect of robustness, fragility and semi-fragility.

According to human perception:

- Visible watermark: The watermark that is detectable in the input comparable to television channels e.g. HBO, printing a watermark on paper whose logo is detect super imposable on the ends of the Television impression.
- Invisible watermarking: The mechanism present is accessible that may introduce information within a picture that do not detect, yet can examine including the correct software [11]. The privacy of the picture had not prohibited this course, yet it can substantiate that this is the stolen picture.

According to embedding domain:

- Spatial domain: This concentrates on customizing the picture element of one or more uncertain preferred groups of pictures. It strictly bundles the fresh input as

input to the picture element. Many of its methods are SSM LSM Intonation situated method [9].

- Frequency domain: The concern is likewise term as transmute discipline. Standard regarding assured constancies had corrected in distinction to their main. It consists of many accepted worn mutate demesne manners, such as DWT, Discrete cosine mutation as well as diverse density mutation.

According to watermark detection:

- Non blind watermarking: The concern requires a base information in the modified plan as well as secure heftiness, yet utilization is narrow [6].
- Semi blind watermarking: This needs no more a primitive data considering apprehension.
- Blind watermarking: The concern no more require primitive input, that includes deep utilization range, yet needs some greater tidemark mechanism.

According to watermark type:

- Turbulence form: This type includes Gaussian random, bogus as well as anarchic arrangement.
- Image form: This incorporates dual image, logo, imprint as well as trademark.

According to host signal

- Image watermarking: The indicated is worn to shield the important knowledge into the image and to afterwards track down and abstract that unique knowledge for the writer‘s claim.
- Video watermarking: The mentioned casts tidemark in the video branch to sway telegenic operation. It is the expansion of image tide marking. This mechanism craves actual duration drawing and heftiness for acquiesce [8].
- Audio watermarking: This function field is one of the maximum attractive and torrid issues due to net, MP3 etc.

- Text watermarking: This casts tidemark to the DOC, PDF and extra data set to limit the adjustment formed to data. The tidemark is adding in the genesis architecture and the slots among caliber and straight zone.
- Graphic watermarking: It encloses the tidemark to either 3D or 2D processor developed visuals to demonstrate the ownership [10].

Watermarks are also classified according to the nature which includes robust, fragile and semi fragile techniques in robust watermarking the tidemark is chiefly use to clue absorbed knowledge of the digital entirety, the enclosed apogee can abide the typical processing, image processing and lossy acquiesce, and the tidemark is not divested subsequently some invasion and can pacifically identified to indulge confirmation. It abides different invasions, computative or non-computative beyond stirring enclosed tidemark [7] where as fragile watermarking technique is generally used for rectitude preservation which determines whether the data has been tampered is found and along with this, it is very sensitive to signal changes and Semi fragile approach is competent of enduring a little extent of the adjustment to a corrupted data, alike adding of quantized disturbance from loss confination [3]

1.7 Watermarking Applications

- Watermarks embedded into digital content attend a variety of purposes. The basic applications of digital watermarking are mentioned below:
- Ownership assertion– In order to prove the copyright ownership, the owner embeds any one of his/her identification in the host media [11].
- Copyright protection– Watermarking could be used to protect reallocation of copyrighted substantial over the entrusted network such as Internet or peer-to-peer links [11]. Since the content is stamped with a visible watermark which is very hard to eliminate and it can be publicly and easily circulated.
- Content archiving– Digital contents such as images, audio or video are stored by embedding their identifications such as digital object modifier or serial number as the watermark. It gives more information about the digital content. For example

an image is stored along with the information such as time and place. This information could be used for categorizing and organizing digital subjects [9].

- Broadcast monitoring– Watermarking could also be used for broadcast monitoring. In the advertisement applications, the advertising agencies can monitor whether their advertisements are essentially broadcasted at the true period and right interval. This can be achieved by embedding the watermark that is to be broadcasted together with the host media [12].
- Tamper detection – Watermarks find their advantage in tamper detection also. If the watermark is impaired or corrupted, it specifies the occurrence of tampering and hence, the digital content cannot be trusted. Tamper recognition is very significant for certain applications that include extremely delicate data like medical images [13].
- Digital fingerprinting– It is a system used to distinguish the possessor of the digital content. Fingerprints are distinctive to the vendor of the digital content. The owner inserts the fingerprint into each copy of the media [8]. Hence, a particular digital thing could have diverse fingerprints because they are appropriate to dissimilar users. The main challenge faced by fingerprinting is the collusion attack, in which numerous legal replicas of the identical media are attained.
- Copy prevention – In order to prevent illegal copying and limit the number of copies created, the owner embeds a never-copy watermark in the host media. The detector which is installed in the recording device restricts further recording.
- Authentication – The authenticity of the conventional media is verified by checking the existence of the watermark. If the watermarked media is employed, the embedded watermark becomes undetectable. Hence, the recipient would recognize that the media is inconsistent [15].
- Content integrity verification – The content is not allowed to be modified in such a way that the content meaning is altered. Embedding a watermark within the original media permits the relevant parties to confirm the integrity of the content [13].

1.8 OBJECTIVE OF THE THESIS

The objectives of this research are:

- To design, implement and improve digital watermarking system with the help of semi-fragile watermarking technique by using different methods for embedding and extracting the watermark for copy right protection, security and authentication. Further to enhance and improve the PSNR of watermarked image using unsharp masking.
- To analyze the performance of the proposed method stated in objective 1in terms of watermark imperceptibility of watermarked image and watermark robustness of the extracted watermark
- To check the vulnerability of proposed method to various attacks such as compression, tampering, noise addition, contrast adjustment and cropping.

1.9 ORGANIZATION OF THE THESIS

The thesis has been organized in six chapters as follows:

- **Chapter 1** includes basic introduction about digital watermarking and types of digital watermarking. The general model and introduction to image processing and semi fragile watermarking have also been discussed in this chapter.
- **Chapter 2** briefly summarizes reported literature in the area of semi fragile watermarking. This chapter throws a light on existing work done in the area of watermarking techniques.
- **Chapter 3** present detail discussions of semi fragile watermarking using Local binary method (LBP). The parameters used for evaluating the performance of same namely PSNR, MSE and SSIM have also been discussed here.
- **Chapter 4** provides analysis of results obtained for performance evaluation of proposed using Local binary method (LBP). Further these have been compared with conventional LBP method on the basis of PSNR, MSE and SSIM.
- **Chapter 5** presents the comparative analysis of the proposed semi fragile method with the conventional LBP method.
- **Chapter 6** concludes the work with some suggestions for further research.

CHAPTER-2

LITERATURE SURVEY

2.1 INTRODUCTION

Nowadays, almost the entire multimedia invention and distribution derived in the form of digital data. However, the sharing, replication and alteration of digital images are unsophisticated owing to the rapid escalation of digital means as both stationary images as well as video can be deployed [16]. Because of this purpose, copyright enforcement approaches for the security of copyright ownership had appeared as critical fundamentals and also being able to detect all the malicious changes that affect the quality of watermarked image. The literature survey is mainly focused on Ownership security, authentication and contented integrity verification of rational property in digital form [9]. These issues can be determined by the solution obtained by the digital watermarking. A review on served watermarking methods is performed through reported literature survey. A great deal of study on digital watermarking techniques has been done and this sub-section provides an outline of the efforts of various researchers, over last few years in this area.

Chamlawi R.*et al.* [1] addressed a protected semi-fragile watermarking for image verification and recovery centered on integer wavelet transform with constraints. The scheme is based on embedding two watermarks namely a binary signature and a picture digest. The binary signature is embedded in the LL3 sub-band and a compressed style of original image is produced as the image digest and is embedded in the HL2 &LH2 sub-bands. This technique is more complex and computationally expensive. However, it offers high degree of robustness against JPEG compression up to 70%.

A fragile watermarking scheme with a hierarchical contrivance in which pixel consequent and block derivative watermark is entrenched in the Least Significant Bits of all pixels is proposed by **Zhang Xing** *et al.* [2]. During the extraction of watermark, the blocks containing manipulated content are identified first. Then the hidden watermark

information in the remaining chunks is checked to precisely locate the altered pixels. Disadvantage of this scheme is that if the number of manipulated chunks is high then the algorithm is only able to indicate that the image is tampered but cannot locate the tampered pixels. However, the proposed arrangement is capable of recovering the novel watermarked style without any fault.

a semi-fragile watermarking arrangement is scheduled which implants a watermark in the quantized DCT province. It is sympathetic to JPEG compression to a pre-firmed lowest eminence factor, but is delicate to all additional malicious attacks, either in spatial or transform domains said by **Chi Kin Ho** *et al.* [3]. Feature codes are removed based on the qualified sign and amounts of coefficients, and these are consistent due to a significant property of JPEG firmness. The engagement of a neighborhood contrivance guarantees that nondeterministic block-wise requirement is attained.

A semi fragile scheme is presented in which the watermark has to embed in the spatial domain. The process is devised so that the LSB of the pixels are modified with the bits of watermark and is tolerant to Laplacian sharpening. The algorithm scheduled by **Xiaomei Zhuang** *et al.* [4] does not show robustness against incidental operations such as JPEG firmness and filtering operations. A large possibility of false alarm would emerge in the arrangement because acceptable incidental image processing operations may effect in an alteration in the LSB and supplementary bits.

Latha Parameswaran *et al.* [5] discussed a semi fragile gratified centered watermarking arrangement for image verification employing Independent Component Analysis (ICA) and Discrete Cosine Transform. The watermark is attained since the original image, in relation of the Frobenius norm of the collaborating matrix attained during ICA. It is entrenched in the mid-frequency DCT constants. This confirmation technique is robust in contrast to some of the supplementary image processing maneuvers and also perceives malicious altering and suitably detects the tampered region.

A.K. Parthasarathy *et al*. [6] devised a novel pattern for digital watermarking that would be semi fragile to whichever form of satisfactory distortions. The framework proposed in [17] uses a coding approach to design a secure watermark-based multimedia authentication system. The embedding and verification procedures of the semi fragile arrangements are retrieved and executed using lattice codes to attain robustness and fragility. The usage of nested lattice codes and MSBLSB decomposition ensure the security of watermarking process.

A semi fragile scheme in which the image element is produced based on the associations of DCT coefficients in the low/middle frequency dominion is put forward. The image elements are entrenched in high frequency field and can be removed without the unusual image. The algorithm classifies malicious attacks and is vigorous merely to the JPEG compression processes. This technique enfold both spatial and transformed domains and both scalar and vector quantization and results as a group of watermarking algorithms that are robust in contrast to different lossy image compression, filtering, cropping and row/column elimination attacks for a realistic range of image qualities. In addition JPEG2000 standard is a likely tool for generating new watermarking arrangements said by **C. Lin** *et al.* [7]

Zhu Xi'an *et al.* [8] proposed an integer wavelet transform based semi fragile watermarking arrangement for image verification with parameters. In order to achieve security, this method includes parameters and integer wavelet transform based on lifting scheme. It is able to locate tampered areas under malicious operations and resists JPEG compression to a large extent. However, the method is sensitive to the change of parameter and includes complex procedure for setting values of parameters.

Semi-fragile watermarking technique in which Wavelet domain is worn to build the content reliant watermark and is entrenched in the mid-frequency coefficients of the wavelet province is proposed by **MA Jmaa** *et al.* [9].The projected approach accomplishes a multi-resolution disintegration of the logo (watermark) image. The logo inset is started from the lowest frequency sub band of the disintegrated image and each

decomposed logo sub band is injected into its complementary sub band of the spoiled image. This arrangement is adept to endure attacks such as copy attack, crop attack and cryptographic attacks.

Chao-Yong *et al.* [10] projected the semi fragile watermarking scheme that examines the robustness of the scheme to incidental operations, especially on resisting compression with inferior bit rates. The watermark is embedded in the DCT coefficients so as to approximate the true Laplacian distribution. This method is centered on restoration of transformed domain data so that casual modifications can be removed through restoration.

Rafi Ullah *et al.* [11] reported that the watermark entrenched in the LL sub-band is extra strong in contrast to one assembly of attacks (JPEG firmness, distorting, adding Gaussian noise), besides watermark inserted in the HH band is further robust against alternative set of attacks (rescaling, histogram equalization, strength adjustment, gamma alteration). Instead of showing sensitiveness against malicious attacks, that method resists such kind of attacks.

Aamaurotic watermarking scheme is reported by **Amir Hazem** *et al.* [12] in which direction geo-dimensional statistics is protect in distinction to illicit service giving advantage of preventing from data format change data editing and random noise. As a result this method is highly robust against firmness, distorting and improving operations.

Xiaojun Qi *et al.* [13] conferred a semi-fragile tide marking technique that is stationed on block based SVD that can extract the tidemark without original data. The watermark is permuted and is implanted by altering the factors of the HH and LL sub-bands contingent on the tide mark bits.

A semi fragile watermarking procedure is presented by **Mohamed. U Celik** *et al.* [14] that admits JPEG lossy firmness on the watermarked image to a pre-resolute quality aspect and discards malicious attacks by the Secret Block Mapping function that controls

watermark generation and implanting processes and ensures security of the system. But the acceptable manipulations such as filtering operations, geometric transformations are not addressed.

Nasrin M. Makbol *et al.* [15] presented a semi fragile watermarking procedure that builds a tide mark from the basic image and introduces this tide mark posterior into the image and it eludes supplementary signature records. The arrangement is lenient of lossy firmness like JPEG, but malevolent fluctuations of picture would outcome in the destruction of the tide mark recognition.

A watermarking method in which wavelet transforms is done on digital image which is a skilled multi-resolution frequency domain approach that provides high security by using chaotic map technique has been discussed by **Abhilasha Singh** *et al.* [16].The effect of JPEG quantization on watermarked constants and on watermark is measured. The standard for coefficients collection is imitative, providing toughness for a random quantization mark. The altered arrangement of coefficients probability density function (PDF) points to the class of adapted optimal sensors.

Chin-Chen Chang *et al.* [17] conferred an amaurotic tide marking access in which direction geo-dimensional statistics is protect in distinction to illicit service giving advantage of preventing from data format change data editing and random noise. This program is resilient to most of the attacks particularly JPEG firmness, filtering operations, introduction of mild noises and rotation with cropping operations.

Sanjay Rawat *et al.* [18] scheduled an adaptive watermarking method. This proposal embeds watermark in terms of a binary image in DCT approach and the sable edge-analyzer method is used to access the leaning magnitude. This technique is strong against minor extent of noise and could contain other than one tide mark as different segments of m-sequences remain uncorrelated. The tide mark is easily detached or replaced by controlling the LSB. However, this method does not possess good localization properties.

A fragile watermarking topology is advised by **U. M. Gokhale** *et al.* [19] which is used to identify nasty improvements in case of malicious attacks. In this proposal, all tuples in an index relation are tightly divided into groups so that modifications can be reduced in worst case. This method can securely and successfully identify the malicious manipulations and recover the image in case of tampering.

Siddharth Singh *et al*. [20] proposal embeds tidemark in terms of a binary image in DCT approach the sable edge-analyzer method is used to access the leaning magnitude. This outcome is symmetrical to the quantity of watermarked chunk.

The Egger-Girod algorithm for semi-fragile watermarking that utilized a binary sequence as the watermark and is inserted into the 2nd through 8th coefficients in the zig-zag mandate of the 8x8 block DCT coefficients is presented by **Xiao J.** *et al.* [21]. The embedding scheme is controlled by two parameters namely the quantization step size and scaling factor. The algorithm is reliable for additive white Gaussian noise attack for a given variance and JPEG compression down to the quality factor of 30. However, it is very delicate to histogram equalization and leveling.

S. K. Maeno *et al.* [22] coined frequency domain tide mark scheme as they adopt a method named spread-spectrum to introduce watermark, that if the tide mark is entrenched in the low frequency mechanisms, it is vigorous in contrast to low pass filtering and geometric alterations. Oppositely, if the tide mark is inserted in high frequency constituents, it is vigorous against contrast and brightness modification, gamma improvement, histogram equalization and cropping.

An algorithm has been developed that embeds the watermark information without much distortion into the host image. The DWT is applied on the image and the LH and HL sub-band frequencies are selected for embedding reported by **Radu. O. Preda** *et al.* [23]. This scheme is highly robust against Gaussian noise and salt and pepper noise. The extraction is made without using original image.

Ruisong Ye *et al*. [24] conferred blind watermarking arrangement grounded on Singular Value Decomposition, Dither quantization and accretion for digital watermarking by means of Genetic. The imperceptibility of the watermarked image and the toughness of the watermark are improved. The projected process is more protected and resists a wide variety of attacks.

Archana Tiwari *et al.* [25] anticipated a scheme to ascent a digital image which disorders the pixel locations using orbit of the alteration. Due to chaotic things image can be improved after some iterations. This procedure helped to recover the toughness of watermark image from several intimidating attacks.

A robust watermarking technique is presented by **Hanan Elazhary** *et al*. [26] which have been based on image fusion. It utilized a gray scale and binary watermarks and was controlled by means of the Toral Automorphism. The embedding process is carried out additively. This method uses the secret image for watermark extraction instead of host image.

S. Shefali *et al*. [27] conferred a 3-level wavelet transmute on the image and the fingerprint of each sub-block of the image is attained by manipulating the hash value of the chunk, its adjacent blocks and its abrasive estimation in low-pass sub-image. The fingerprint is then encrypted by a cryptosystem and is embedded in the LSB of the block. The verification process needs only the public key of the user to verify whether the newly intended fingerprint is reliable with the decryption result of the LSB. This approach identifies spatial or wavelet auxiliary attacks competently.

The algorithm for watermarking verification system using dynamic parameters of the watermark has been discussed. A novel fast image watermarking and data hiding technique depending on the opinion proposed by **Said E. El-Khamy** *et al.* [28] in which chunk-wise addicted information in watermark had been conducted for crimping VQ encounter without negotiating on localization potential of the scheme.

A neural network technique namely the Back Propagation Network has been conferred by **V. Senthil** *et al*. [29] which uses exclusive-OR procedure to exemplary the relations between some arbitrarily selected pixels with their localities. Instead of embedding watermark, the procedure abstracts features from original image and is transferred as a separate image, so that the pictorial quality of the image is not degraded. The algorithm demonstrates excellent resistant enactments to JPEG compression and median filtering.

I. Amerini *et al.* [30] proposed a new methodology based on Scale Invariant Features Transform (SIFT) which is also able to detect the geometric transformations of the cloned part like rotation and scaling. The proposed method was tested on two datasets having forged images incorporating rotation, scaling or both in the cloned region. The presented technique was found effective for the detection of copy move image forgery as well as splicing. The method also dealt with multiple cloning successfully. The use of clustering algorithm improved the detection accuracy as well as True Positive Rate (TPR) as compared to the existing copy move detection algorithms.

A novel method is proposed by **T. A Kohale** *et al.* [31] which combine a block and a key-point based method to study the effect of different types of tampering on the digital images. The method proposed was based on DCT (a block based method) and SIFT (a key-point based method) to detect and locate copy-move forgery in digital images under various types of attacks. Thus authors proposed a single method that was able to detect combination of number of post-processed operations in the cloned region. The proposed method increased the detection rate and efficiency from the existing forgery detection methods.

Yueqiang Liu *et al* [32] designed a self-orientation image grounded robust watermarking arrangement. In order to overwhelm the uncertain robustness difficulty in spatial sphere, their robust watermarking arrangement improved the original image in the transmute domain and insert the watermark in the dissimilar values among the original image and its mentioned image. Additionally, the utilization had been extra practical in real life

application for possession verification since the original images are not essential for watermark abstraction.

A wavelet based watermarking scheme is presented in which the semi fragile watermark is generated from small frequency band of DWT and is inserted in the high frequency band through the help of HVS. The toughness of the procedure is examined for minor alterations like JPEG firmness and channel additive white Gaussian noise said by **X. A. Zhu** *et al.* [33]. This technique also evaluates the fragility against malicious attacks.

C. Y Lin *et al.* [34] allocate with the difficulties of error recognition and retrieval of still images. The content-based watermark bits, which embrace the authentication bits and retrieved bits are generated from some selected blocks of the host image and are embedded in the other remaining blocks of the image. They projected a Pre quantization procedure to amend the DCT quantities owned for implanting in progress and constructed on a necessary toughness compared to compression also the DCT coefficients were quantized once more to achieve entrenching. This practice can distinguish influences and recuperate an estimated original picture from the degraded area. This arrangement struggle firmness to a convinced part, but the trade-off among reliability and robustness repeatedly limits the attainable enactment.

A classified watermarking outline for semi-regular meshes has been presented by **S.W. Wang** *et al.* [35]. In this technique three watermarks are inserted in different appropriate resolution levels achieved by wavelet disintegration of the lattice. The strong watermark is injected by altering the standards of the wavelet factor vectors related with the lowermost determination plane, the fragile watermark is inserted in the great resolution level acquired impartial after one wavelet decomposition by amending the bearings and standards of the wavelet factor vectors and the great capability watermark is interleaved in one or numerous transitional levels by allowing groups of wavelet coefficient vector standards as watermarking indigene. The advantage of this practice is that robust watermark injected in it is capable to struggle all collective symmetrical attacks equal

with moderately durable amplitude, the fragile watermark is vigorous to gratify the conserving maneuvers, while actuality profound to former geometric attacks.

S.S. Sujatha *et al.* [36] scheduled the advantages of block-based permutation of neighboring constant and suggested a prime eminence as well as strong watermarking procedure. So as to cover additional data into great frequency blocks while not inflicting simple alteration to the watermarked image, the planned methodology used the link among the coefficients of neighboring blocks. Additionally the robustness to the middle frequency filter attacks had been enhanced by an altered extraction methodology.

A robust video watermarking method has been suggested by **Mohamed Sathik** *et al.* [37]. In this scheme, data is entrenched to the precise bands in the wavelet domain by means of motion estimation methodology. HL and LH bands of DWT were used to enhance the watermark whereas the indication in these ensembles would not upset the superiority of extracted watermark if the cinematographic is endangered to diverse categories of malicious attacks. Watermark is entrenched in a preservative manner using arbitrary Gaussian scattering in video sequences. This watermarking manner has durable robustness in contradiction of some attacks like as frame dropping, frame filtering and lossy compression.

Kwang-wook Lee *et al.* [38] have proposed an inventive watermarking scheme. According to this technique, the low frequency sub group of wavelet province and the rescaled style of basic picture are utilized in the watermark construction process. A scrambled version of watermark is acquired with the support of Arnold Transform. The procedure of entrenching and abstraction of watermark is completed in high frequency field of DWT subsequently minor alterations in this sphere would not apparent by human senses. This arrangement accord with the abstraction of watermark evidences without any compulsion of raw image.

Feature point detection and image regularization grounded watermarking arrangement is presented by **Wei Qi** *et al*. [39].This scheme recognizes some constant feature points

from the inventive image by means of the anticipated multi-resolution feature point detection filter. At that time, image standardization had been accomplished on the disks concentrated at these feature points. For each disk, the watermarks have been entrenched disjointedly in the sub band coefficients of DFT dominion.

Xinpeng Zhang *et al.* [40] presented an integer wavelet transform based semi-fragile watermarking arrangement for image verification. This method includes parameters and integer wavelet transform based on lifting scheme and is able to locate tampered areas under malicious operations and resists JPEG compression to a large extent in order to achieve security However, the method is sensitive to the change of parameter and includes complex procedure for setting values of parameters.

CHAPTER 3

SEMI FRAGILE WATERMARKING

3.1 INTODUCTION

The rapid development taking place in the field of image processing has revolutionized the entire world today. The visual quality of images, the requirement of high storage, the need for speedy processing and transmission posed great challenges to the scientific community. Digital Image Processing is the branch of Digital Signal Processing in which, various Image Processing algorithms are applied on digital images [3]. It grants the use of much more complicated algorithms and henceforth, can endeavor both refined performance at straight tasks and the implementation of approach which could be impractical by analog means. Processing an image is equivalent to processing a signal for which image act as an input and the turn out of this operation is an altered image or a list of criterion put successively as a model in many situations and determines the image in two ranges and utilizes assured image refining modes [5]. The acquisition of images that is generating the input image in the prime place is termed as imaging. It is an exercise of any algorithm, which takes input as an image and at the same time returns output as an image. Therefore, security and protection of everyone's production has become a difficult task. So holding the preservation of digital watermarked expression i.e. text, audio image and video has accepted appreciable attention [1].The watermarking has been scheduled as a relevant solution for copyright protection approach for digital data which embed a water mark with some extra information about the digital media without visibly altering them [6]. The security of intellectual materials has become a foremost problem in the digital age. The comfort of copying digital information without much loss of quality interrupts the conservation of mass materials of traditional media, which inhibited extensive global distribution in the past. Digital information is susceptible to be copied at the same quality as the original. A watermark is a design of bits introduced into a digital image that classifies the patent information. Digital tide marking approach consists of two parts; recovery and embedding algorithms. In the embedding algorithm, the tide mark is embedded in digital media with a unique algorithm. And this watermark is reclaimed from the tide marked image by extracting algorithm. Generally, there are two

common domains that tide mark is embed in them; the spatial domain or the transform domain. In the frequency demesne, tidemarks are infused like using the 'Discrete Cosine mutation', 'Discrete Fourier Transform' and 'Wavelet Transform' [9]. The tide mark is inserted directly in the pixels of the primary picture in the spatial domain approach. The most vital and simple approach of tidemark embedding is to drop the tidemark into the LSB of the prime image.

3.2 WATERMARKING PROCESS

Three different steps, embedding, attack and detection are usually worn to perform watermarking. Watermarking system performs these steps. In embedding, the watermark signal is produce by procedure that accepts host and data to be impose. Then this signal is capture or transmitted to other user [13].

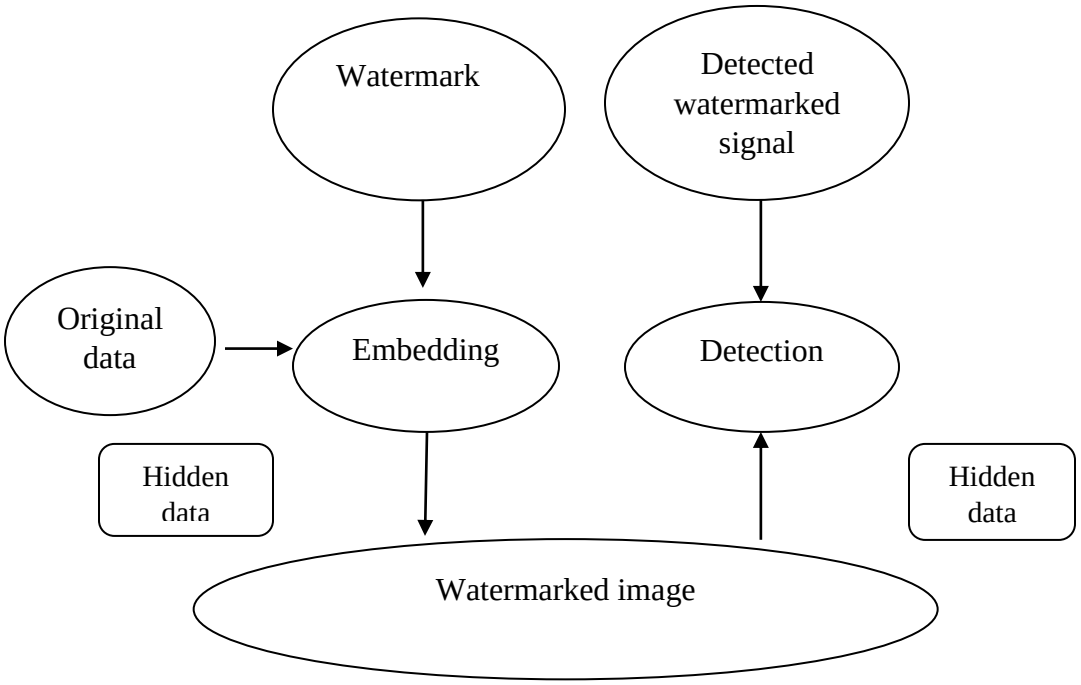


Figure 3.1 Block representation of Watermarking Process [13]

If another user performs any alteration on watermarked signal then it is coin as attack. There may be various available attacks on an image. To excerpt the watermark from image the algorithm has been applied to the bombarded signal. This is termed as detection. During transmission, if there is no modification then the watermark is still commenced and it can be derived. Figure 3.1 represents the basic section representation

of watermarking process. The original data or picture and the required tidemark are embedded using presently available. To extract the watermark decoder is used along with hidden information in reverse process opposite to embedding [14].

3.3 TYPES OF WATERMARKING TECHNIQUES

The digital image watermarking algorithms can be classified based on criteria as given below and are shown in figure 3.1.

- Robust watermarking
- Fragile watermarking
- Semi fragile watermarking

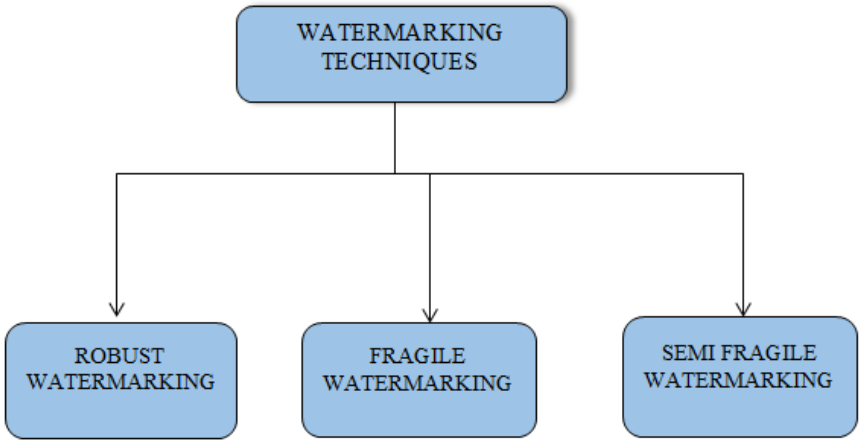


Figure 3.2 Types of watermarking techniques

Since the image, authentication and content integrity are the important applications of the digital watermarking and have been analyzed in the aspect of robustness, fragility and semi-fragility.

3.3.1 ROBUST TECHNIQUE

Robust watermarks are intended to withstand the attempts which are made to eliminate or destroy the watermark. They are primarily used in copyright protection and content tracking applications [16]. In this technique, the watermark should not be detached or

destroyed after any geometric or signal processing attack [20]. The attacks applied on the watermarked image may be malicious or non-malicious. An intruder may intentionally attack the watermarked image to remove the watermark completely or to change its position (synchronization attack) or to destroy it. A robust watermarking technique should also be able to detect collage attack, collusion or forgery attack.

3.3.2 FRAGILE TECHNIQUE

In converse to robust watermarking, fragile watermarks are sensitive to all types of incidental and intentional modifications. Fragile watermarks are designed so that they are easily damaged if the watermarked image is altered in the slightest manner. Because of this quality, fragile watermarks are mainly used for exact authentication application [17]. In this technique, watermark is embedded in such a way that any change ended to the watermarked image modifies the watermark itself. Thus a fragile watermarking system should be sensitive to even the slightest alteration made to the watermarked image. The fragile watermarking techniques are used for image authentication in medical science, military and defense to verify whether the received image is similar to image that was actually transmitted or some alterations are made to it during transmission over the channel [20].

3.3.3 SEMI FRAGILE TECHNIQUE

A semi-fragile watermark combines the properties of fragile and robust watermarks. Like a robust watermark, a semi fragile watermark is experienced of tolerating certain degree of modification to the watermarked image, like the addition of quantization noise from lossy compression. It is also proficient of localizing areas of the image that had been tampered and distinguishing them from regions that are still authentic. Thus, a semi-fragile watermark can differentiate among localized tampering and information-preserving, lossy transformations [19]. Since the chief applications of semi-fragile watermarks comprise tamper detection and duplicate authentication, the complete desires of a semi-fragile watermarking arrangement look like those of fragile watermarking schemes. The capability to identify areas of alleged alterations and discriminate those sections from additional regions wherever there is large sureness that the watermarked

data have not been spoiled is important. Similarly most substantiation systems, the watermark detector must not need that the novel, undamaged image is available (i.e. blind detection.) and as in the overall situation of invisible watermarking, the shield delivered by the watermark will not destroy the rate of the image [23].

3.4 FREQUENCY DOMAIN TECHNIQUES

In order to overcome the drawbacks of spatial domain methods, some sophisticated methods were proposed, which utilize frequency domain for embedding the watermark. The frequency domain technique converts a picture into a fixed set of frequency sphere constants where most distinguished information is hidden. The aim for altering an image from single depiction to a different are stated below:

- The conversion may segregate significant constituents of the image configuration so that they will be straight available for investigation.
- The transformation may abide the image data in an extra condensed practice so that they could be kept as well as communicated proficiently.

To move a picture to its frequency illustration, the flexible transforms like Discrete Cosine Transmute (DCT), Discrete Fourier Transmute (DFT) and Discrete Wavelet Transmute (DWT) are employed [15]. All the proposed algorithms aim at improving the invisibility or transparency of the embedded watermark regardless of the operation domain. The algorithms accomplish increased robustness against different types of attack.

3.4.1 Discrete Cosine Transform (DCT)

DCT remains a method aimed at altering a signal from basic frequency components and is extensively used in image compression and digital watermarking. It signifies an image as a summation of sinusoids of changeable scales and frequencies. A DCT contains of a fixed set of basis vectors that were sampled cosine functions [17]. Since a digital data, maximum of the visually significant information about the picture is densely placed in equitable rare coefficients of this transform. Discrete Cosine Transform divides the picture into altered frequency bands specifically small frequency sub-band, middle frequency sub-band and large frequency sub-band. After DCT, almost all values become equal to zero [18]. The non-zero values are thickly located at the upper left corner, known

as DC value; determine the average brightness in the block. All other values, referred as AC values, describe the variation around this DC value [3].

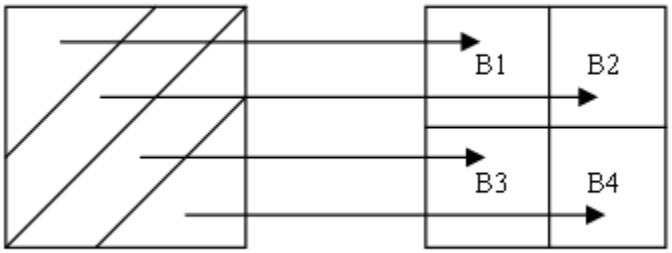


Figure 3.3 Mapping of DCT coefficients into 4 blocks [3]

DCT based watermarking depends upon two facts:

- Low frequency sub-band comprises the greatest significant visual portions of the picture.
- Large frequency constituents of the picture are typically eliminated by firmness and noise outbreaks [23].

The watermark is consequently inserted by altering the elements of the essential frequency sub-band subsequently that the distinguishability of the picture will not be distressed and the watermark would not be removed by compression. Let x be the input image. The DCT coefficients [10] are calculated according to equation (3.1), which gives the transformed output image y.

$$y(u,v) = \sqrt{\frac{2}{M}}\sqrt{\frac{2}{N}}\alpha_U\alpha_V \sum_{U=0}^{M-1}\sum_{U=0}^{M-1} x(m,n) \qquad (3.1)$$

where

$$\alpha_u = \begin{cases} 1/\sqrt{2} & u = 0 \\ 1 & u = 1,2,..N-1 \end{cases}$$

$$\alpha_v = \begin{cases} 1/\sqrt{2} & v = 0 \\ 1 & v = 1,2,..N-1 \end{cases}$$

The basic picture has M x N picture elements, and $x(m,n)$ signifies the strength of the

picture elements in n[th]column and m[th]row of the picture, also $y(u,v)$ is the DCT constants in u[th] row and v[th] column of this matrix.

3.4.2 Discrete Wavelet Transform (DWT)

This is a dominant measured method used to abstract localized time-frequency (spatial-frequency) data of an image. This transmutes use wavelet filters like Haar wavelet filter, Daubechies Orthogonal filter and Daubechies Bi-orthogonal filter to alter the image [29]. Everyfilter divides the picture into numerous frequencies. The DWT has a lot of special advantages that the usual transforms, such as DCT and DFT, cannot attain and so it is becoming the fundamental image transform in JPEG2000 standard.

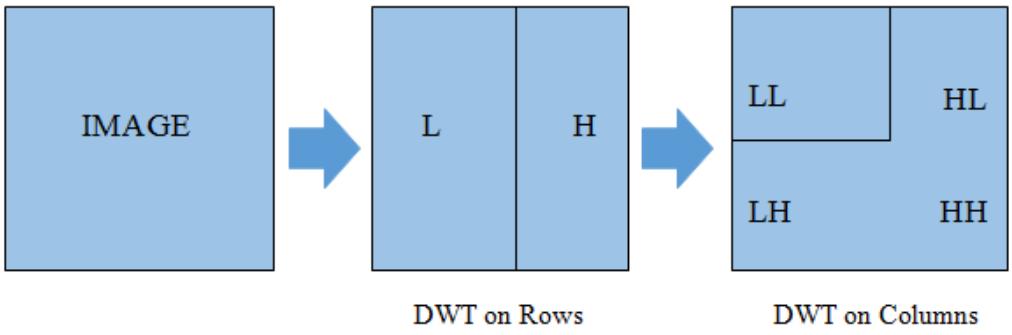


Figure 3.4 DWT decomposition of an image [8]

This Transmute divides the cover image with in four sub-parts specifically LL, LH, HL and HH where the leading letter match up to employ either one a low-pass frequency procedure or high-pass frequency action to the rows whereas another letter mentions to the filter enforced to the columns [8], that is exposed in figure 1.4.

The DWT signifies an image as an amount of wavelet utilities recognized as wavelets through diverse situation and position. It signifies the data into a set of high pass (detail) and low pass (estimated) constants. The basic data is distributed through fixed part of low pass and high pass filters. The lowermost resolution side LL contains the lower resolution estimate portion of the basic image [9]. For a single plane breakdown, the distinct two-dimensional wavelet transmutes [21] of the picture function f(x, y) could be written as:

$$LL = \left[\left(f(x,y) * \varphi(-x)\varphi(-y) \right)(2n, 2m) \right]_{(n,m)\in z^2} \quad (3.2)$$

$$LH = \left[\left(f(x,y) * \varphi(-x)\psi(-y) \right)(2n, 2m) \right]_{(n,m)\in z^2} \quad (3.3)$$

$$LH = \left[\left(f(x,y) * \varphi(-x)\psi(-y) \right)(2n, 2m) \right]_{(n,m)\in z^2} \quad (3.4)$$

$$HL = \left[\left(f(x,y) * \psi(-x)\varphi(-y) \right)(2n, 2m) \right]_{(n,m)\in z^2} \quad (3.5)$$

The steps involved in DWT domain watermarking are as monitors:

- Employ DWT on owner image with any one of the wavelet filters.
- Every of these filters disintegrate the picture in LL, LH, HL and HH sub-bands.
- Embed the watermark in the selected sub-band(s).
- Apply Reverse Discrete Wavelet Transmute (IDWT) to acquire the watermarked image [28].

The wavelet transmute splits the picture into three indications namely horizontal, vertical and diagonal. Therefore, wavelets replicate the assets of HVS extra accurately. It is computationally effectual and could be executed by using modest filter convolution. Magnitude of DWT coefficients is superior in the bottommost bands (LL) at every level of disintegration and is lesser for former bands (LH, HL and HH). Watermark recognition at minor resolutions is estimated impressive as at every succeeding resolution level only rare frequency bands are engaged [29].

3.5 PROPOSED ALGORITHM

Image authentication and content integrity are the relevant applications of digital water marking and have been consider in the aspect of robustness, fragility and semi-fragility. A semi-fragile tide mark couples the attribute of fragile and robust tide marks. Similar to robust tide mark, a semi fragile tide mark is able to tolerate a few amount of alteration to the tide marked image, just as the inclusion of quantization noise from compression that is lossy in nature. It is also able of localizing sections of the picture that are interfered and differentiating these from sections those are still credible [12].

The most basic and simple approach of tide mark insertion is to deposit the tide mark into the minimum significant bit of the prime picture. This technique is an example for spatial domain technique, which precisely modifies the intensities of a few chosen pixels. The LSB was modified with the help of techniques such as checksum and adding identification string. These approaches embed the watermark in the LSB plane for affective transparency and are dependent on the replacement of LSB level of the actual image with the specified watermark. If the watermark is smaller than the host object, it can be embedded multiple times so as to achieve the correct size [30]. Ultimately, the condition posed here is that the dimension of the moderator image is divisible by the dimension of watermark. Hence forth, the idea behind LSB replacement is the following:

- If the image include size $M \times N$ (where M and N represent image dimension), picture element value in the position (i, j) is a binary value.
- This binary number can be then partitioned into bits, so that it contains a Most Significant Bit (MSB) and LSB. The MSB contains quite a lot of information and LSB contains little information [12].

The LBP operator has been purposed to calculate the local disparity with in structure investigation. It is prosperously enforced to image review and picture recovery. It is specified in a round limited neighborhood. The threshold is to be assumed as a centermost pixel, the neighbor T rounded symmetric in a assured radii R is independently labeled as 1 when the term is greater than the center, or specified as 0 when the term is lower than the middlemost. In this T is defined as T= (2R+1)2−1.

The constants R and T, which restraint the quantization of the spatial resolution and oblique space respectively, the local binary pattern number, construed by LBP p, indicating the regional divergence in the neighborhood, is described as [2]

$$LBP_t = \sum_{r=0}^{r-1} \mathrm{S}(\mathrm{g}_r - \mathrm{g}_c) \times 2^t \qquad (3.6)$$

Where g_c signifies the gray level of the innermost pixel c in the T neighborhood, g_r signifies the gray level of the nearby pixels t, and S(x) stands for the sign function described as

$S(x) = 1; if\ x \geq 0$

$0; otherwise$ (3.7)

The inception terms which are 0 and 1 are multiplied by density accustomed to the analogous picture element, and adding up the output as an outcome the code for the center pixel is formed [16].

Watermark embedding algorithm

To insert tidemarks, the Boolean functions $f(s_a)$ to be applied on the binary sign vector part s_a is defined as

$f \oplus (s_a) = s_o \oplus s_1 \oplus ..... \oplus s_{a-1}$ (3.8)

$f(s_a) = Bool(1(s_a) - 0(s_a) > N)$ (3.9)

Where $s_a = \{s_i \mid s_i = sign(g_i - g_c),\ i = 0,1....A-1\}$ (3.10)

The Exclusive or (XOR) operator is used in Eq. (6). As $f \oplus s_a$ and XOR fulfill the commutative and associative laws, so any rounded bit shuffled on s_a counterclockwise or clockwise does not alter the value of function [34]. If either one bit change from 1 to 0 or from 0 to 1 in s_p the function value gets reversed. $\#1(s_a)$ indicated total count of picture element as "1" term in (s_a), $\#0\ (s_a)$ is the count of "0" in (s_a), N is an integer, and $N \leq R-1$. If $\#1\ (s_a) - \#0\ (s_a) > N$, then $f_{\#}(s_a)$ gives 1; else it gives 0 showing resistance against bit rotation and shifting [18].

The embedding method has been epitomize in the subsequent steps:

- The basic picture is splitted into non-overlapping bounded region blocks. This pattern is worn to calculate s_a. Let w be any of bits in the tide marks and β be the tide marking intensity factor.
- If $f \oplus s_a = 1$ equals to the value of w, nothing to do with the pixels in the adjacent. Else way, modification of one of picture element is done by generating the value of $f \oplus s_a = 1$ persistent with the corresponding w [39].

Watermark extraction procedure

The watermark extraction method in the scheduled algorithm is straight. The value of the $f \oplus s_a = 1$ in the tide marked picture to eradicate the watermark w is judged. That is

$w = 1$ When $f \oplus s_a = 1$, else $w = 0$

3.6 UNSHARP MASKING

To restore the quality of image lost by dividing image into blocks is incorporated by linear unsharp masking [13]. It is a method for augmenting the perceptual quality of an image by highlighting its high-frequency components. It is an application concentrating on enhancing end contrast to boost nature of the picture. This has been implemented by subsequent steps.

- Generation of an unsharp mask M by high passing filtering the original picture I i.e.

$M = I \otimes H$ (3.11)

The convolution operator and a high pass filtering are specified by $\otimes$ and H respectively.

- Addition of the proportioned unsharp mask M to the original picture I to produce a smooth picture.

$I' = I + YM$ (3.12)

In this Y signify the scaling coefficient which is to be remarked as sharpening power. It can also be achieved through Gaussian filtering [21], as

$M = I - I \otimes G_\sigma$ (3.13)

Where G_σ specifies a Gaussian filter and can be owed to manage the area of sharpening.

Above said algorithm has been summarized in the following figure 3.3:

Semi fragile watermarking by using LBP method has been implemented to enhance the security of the image. First the cover image of size 512*512 is divided in the 64 blocks each of size 8*8 and watermark image is immerged into all the 64 blocks through semi fragile watermarking then recombination of these 8*8 blocks is done to form the original image of 512*512.The quality of image is somehow degraded due to recombination so modified technique is used to enhance the quality of the image. Unsharp masking is

process that focus on enhancing end contrast to improve quality of picture. Image enhancement concluded by applying unsharp sharpening is different to that achieved by smoothing of the image.

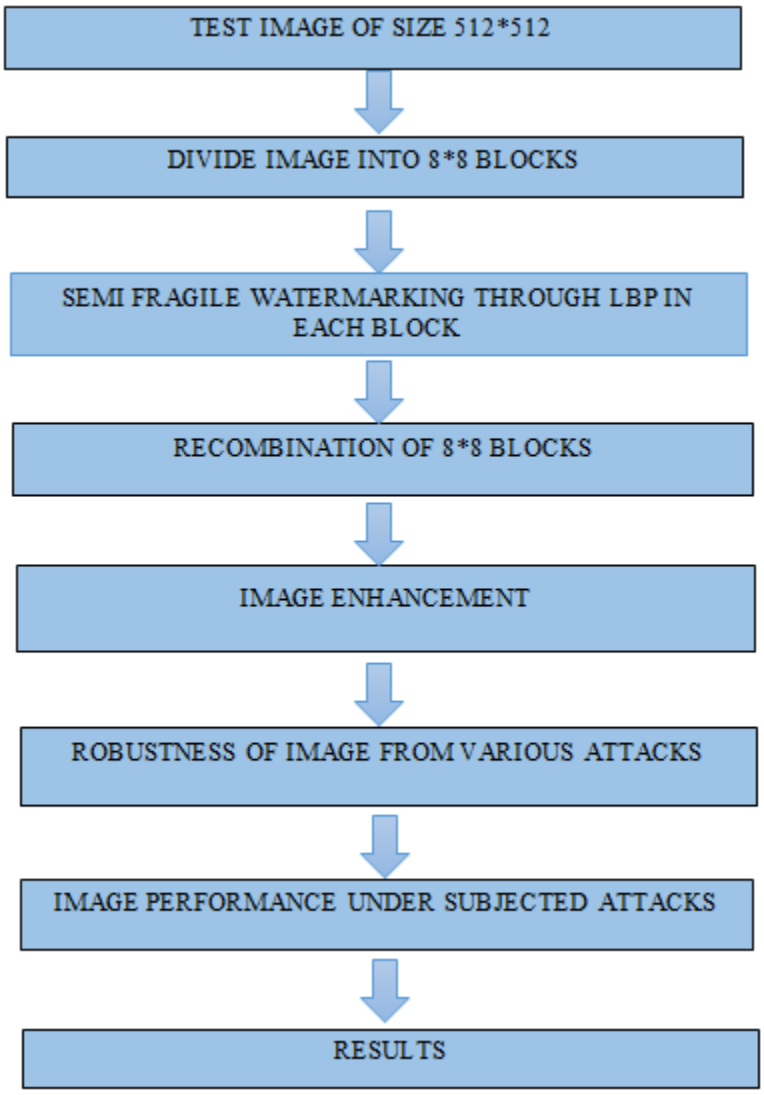


Figure 3.5 Schematic of the proposed System

Watermarked digital image is transmitted or stored, where it can suffer from distinct attacks because multimedia data have to process digitally so recombined image is subjected to different attacks [22]. The attacks may be malicious or non-malicious. There are many promising modifications, such as cropping an image, lossy compression of the information or adding noises. So protections against such attacks are being incorporated in this. So authenticity of the image is restored by unsharp masking.

3.7 PERFORMANCE ANALYSIS

Performance interpretation is foremost part in the any analytical design in tide marking. The fundamental task of this is to appraise the quality pattern of algorithm. Some of the attribute patterns an image tide marking method or algorithm [24] is:

3.7.1 Mean square error (MSE)

Among owner image and the tide marked image this parameter that is squared mean error (MSE) is used to measures or evaluates the squares of the "errors" and takes the average of that [25].

$$MSE = 1 \div KL \sum \sum ((Kij - Lij^2)) \tag{3.14}$$

where K, L is pixel values in owner picture

Kij = Pixel value in tide marked picture

Lij= Pixel value in owner picture

3.7.2 Peak signal to noise ratio (PSNR)

PSNR (Peak Signal to Noise Ratio) has been worn to measure embedding distortion and the visual quality of the watermarked images. Competence of tide marking is determined with regard to the turbulence. The noise will deteriorate the essence of picture [26]. It is given by

$$PSNR = 10 * log(P^2 / MSE) \tag{3.15}$$

Where P= superlative value in owner picture.

This factor persuaded the imperceptibility of picture. More the PSNR shows that tide marked picture is perceptible or bare eyes do not diagnose tidemark.

3.7.3 Structural similarity index (SSIM)

This is an approach for anticipating the perceived aspect of digital pictures, as well as of digital videos. SSIM is worn to calculate the similarity among two images. The SSIM index predict or anticipate the nature of picture depend on initial image as reference [27]. The divergence with regard to another methods coined previously is that those methods estimate absolute inaccuracy, whereas, SSIM is an impression based technique that acknowledge picture degradation as anticipated alteration in structural knowledge.

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (3.16)$$

where, μ_x is defined as the average value of *x*,

μ_y is defined as the average value of *y*,

σ_x^2 is defined as the variance of *x*,

σ_y^2 is defined as the variance of *y*,

σ_{xy} is defined as the covariance of *x* and *y*,

$c_1 = (k_1 L)^2$ and $c_2 = (k_2 L)^2$ are defined to secure the division ,

L is defined as the range of the pixels.

3.8 POSSIBLE ATTACKS

In digital tide marking system, infiltrator tries to apply some malicious attacks to change the ownership of the digital media. Attacks applied on watermarked information can also be non-malicious like compression, smoothing/blurring etc. [30]. Non-malicious attacks are not performed intentionally; rather they attack the watermarked information during transmission over network or storage. Watermark attacks can be geometric like Rotation, Scaling and Translation (RST) attacks, flipping, cropping and affine transformation or can be signal-processing attacks like compression, Gaussian noise accumulation and filtering. Watermark attacks are grouped into four categories based on their purpose [31].

a) Simple attack
b) Detection-disabling attack
c) Ambiguity attack
d) Removal attack

a) Simple attacks

Simple attacks otherwise referred to as wave form attacks or noise attacks which are easy attacks that decide to damage the embedded watermark by handling the full watermarked knowledge (host knowledge and watermark) deprived of an effort to recognize and segregate the tide mark [39]. Embrace filtering, compression, accumulation of noise,

adding of an offset, cropping, geometrical operations etc. are the examples of this attack. Therefore, this attack is compressing of interactive media data in a lossy mode and destroying watermark. In case of image multimedia, a turning or scaling can vary pixel standards and damage tide mark, while preserving the visual content of the image. Signal dispensation operations like re-sampling, color decrement, swapping some pixels and so on can damage the watermark data [36].

b) Detection-disabling attacks

It is also called synchronization attack. These are the attacks that endeavor to halt the association and to mark the reclamation of the tide mark difficult or inaccessible for a watermark sensor, include the operations that make the detection of tidemark impossible by changing the position of the watermark [37]. Attacks that disable the detection of watermark are zooming, scaling, translation, shift in direction, revolution, cropping, element permutations, sub selection, elimination or inclusion of elements or pixel groups, or the further geometric conversion of the information.

c) Ambiguity attack

Ambiguity attacks is also called deadlock attack, invertibility attack, forgery attack and fake-original attacks that is applied by inserting some fake watermark to change the ownership of the watermarked contents or to allow multiple claims of ownership on the watermarked contents. These are attacks that effort to complicate by generating false original figures or forged watermarked records. Inversion attack that makes an attempt to disrepute the right of the watermark by entrenching one or many further tide marks corresponding to that it was uncertain that was primary, authoritative watermark is an example of this attack [39].

d) Removal attacks

Removal attacks are applied not to destroy the watermark, rather they include the operations that remove the watermark from the watermarked contents that is they are arranged to examine the tide marked information, approximate the watermark as well as the moderator information, distinct the watermarked information into owner information and reject solely the watermark [40]. Collusion attacks, denoising, assured filter actions

and firmness attacks employing artificial modeling of the image are the examples of this attack.

Generally, there are two common domains to embed watermark that is spatial domain and the frequency domain. In the frequency domain, watermarks are infused into the coefficients of a transformed picture, for example using the ‘Discrete Cosine mutation’, ‘Discrete Fourier Transform’ and ‘Wavelet Transform’ [9]. The watermark is inserted directly in the pixels of the primary picture in the spatial domain approach. The most vital and simple approach of watermark embedding is to drop the watermark into the LSB of the prime image that is employing LBP watermarking. As the need for secure information over network is of high security when the information is shared over network or retrieved from network. There are many promising modifications, such as cropping an image, lossy compression of the information or adding noises. Watermark attacks are grouped into four categories based on their purpose as Simple attack, Detection-disabling attack, Ambiguity attack and Removal attack. So protection against various attacks must be employed.

CHAPTER 4
EXPERIMENTAL RESULTS

4.1 INTRODUCTION

In this dissertation work, semi fragile watermarking has been studied and implemented by using modified approach of LBP (Local binary pattern). Moreover the quality of the original image is maintained without any degradation in the information. Watermarked digital image is transmitted or stored, where it can suffer from distinct attacks because multimedia data have to process digitally so recombined image is subjected to different attacks. The attacks may be malicious or non-malicious. There are many promising modifications, such as cropping an image, lossy compression of the information or adding noises. So protections against such attacks are being incorporated in this. The simulation results obtained by implementing the proposed semi-fragile watermarking algorithms are discussed in this chapter. Research has been supported out with 'Lena' image to evaluate the effectiveness of the proposed methods using PSNR (Peak Signal to Noise Ratio, Mean square error (MSE) and Structural similarity index (SSIM) as performance parameters.

4.2 RESULTS AND DISCUSSION

For testing, the image taken in this research is 'lena.png' (figure 4.1(a)) of size 512 × 512 and the watermarked picture is 'ALICE logo (figure 4.1(b)). The input host images have equal number of rows and columns; subsequently the implanted watermark is a square matrix. According to the algorithm the cover picture is distributed into 64 blocks each of size 8 × 8 and the watermark image is inserted in every block. After embedding all the 64 blocks are recombined to form the cover image of same size that is of 512 × 512 and PSNR value is being calculated between the basic raw image and the watermarked picture. Moreover the quality of the picture is maintained through this algorithm after being subjected to various attacks.

(a)Original Picture

(b) Watermark logo

Figure 4.1 Original cover Picture and watermark image

The quality of picture is somehow degraded due to recombination so modified technique is used to enhance the quality of the image. In the extraction part, watermark logo from every of the block has been obtained. Superiority of the withdrawn watermark is checked visually and by calculating PSNR, MSE and SSIM among the original logo and extracted watermark logo from every block.

4.2.1 Visible watermarking

In this section simple visible watermarking has been employed on the image. Text named "alice" is inserted in the image as shown below.

Fig 4.2(a) Basic Lena image

Fig 4.2(b) text inserted image

Figure 4.2 Original cover Picture and text inserted image

In Fig 6.2(a) basic Lena image is taken and in Fig 6.2(b) name is inserted in the original picture showing visible watermarking.

4.2.2 Division of 512*512 image into 8×8 blocks with text inserted

In this segment the basic image of size 512×512 is segmented into 64 blocks each block is of size 8*8 and text is inserted in each every block as shown below. The objective of division is to abridge or alter the demonstration of a picture into somewhat that is further significant and simple to examine. This is done so that to cooperatively bind the whole picture or a fixed part of contours removed from the picture.

Fig 4.3(a) Original Lena image

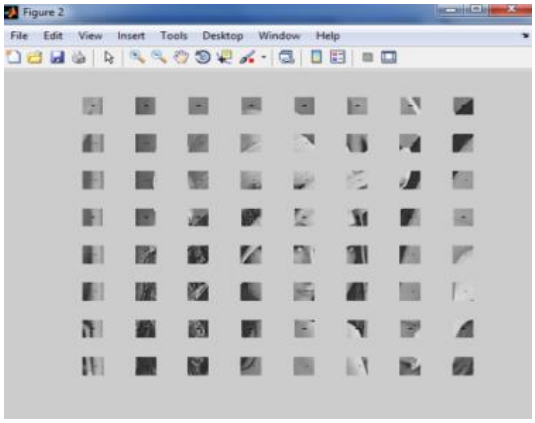


Fig 4.3(b) blocks of 8*8 with text inserted

Figure 4.3 Original cover Picture and divided image

In Fig 4.3(a) original Lena image is taken and in Fig 4.3(b) that image is splitted into 8×8 blocks which are total of 64 blocks and after that semi fragile watermarking is done in each block that is name is inserted in all 64 blocks.

4.2.3 Recombination of 8*8 blocks

The current section provides a technique for image recombination and image identification and an arrangement for image acquiring and identification. Features with regard to the blocks are recombined and enhanced so as to form a recombined watermarked image. After that, the recombined watermarked picture has been managed to accentuate the features of the recombined picture so that the recombined image is skilled of being recognized effortlessly. Furthermore, the current provides a scheme to accomplish the foregoing method, whereby reducing anonymous issues caused as a result of poor quality image of the observation system.

Figure 4.4 (a) recombined image

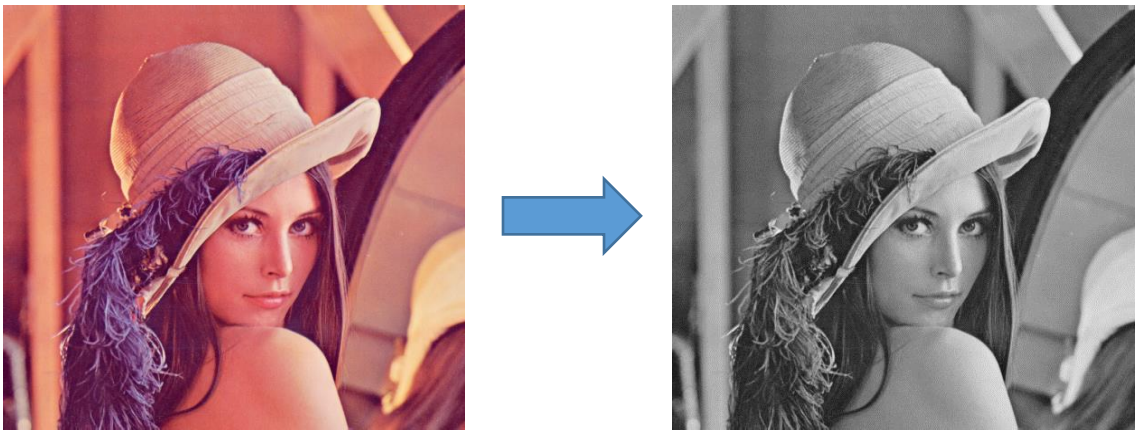
Figure 4.4 (b) Text watermarked through LBP

In Fig 4.4.1 original Lena image which was divide into 8×8 blocks that is total of 64 blocks is recombined showing "name" in all 64 blocks and in Fig 4.4.2 the text which was earlier visible is made invisible through LBP algorithm.

A. PSNR Improvement

There is a significant improvement in the value of PSNR of an image. When conventional semi-fragile spatial watermarking method based on LBP operators by using

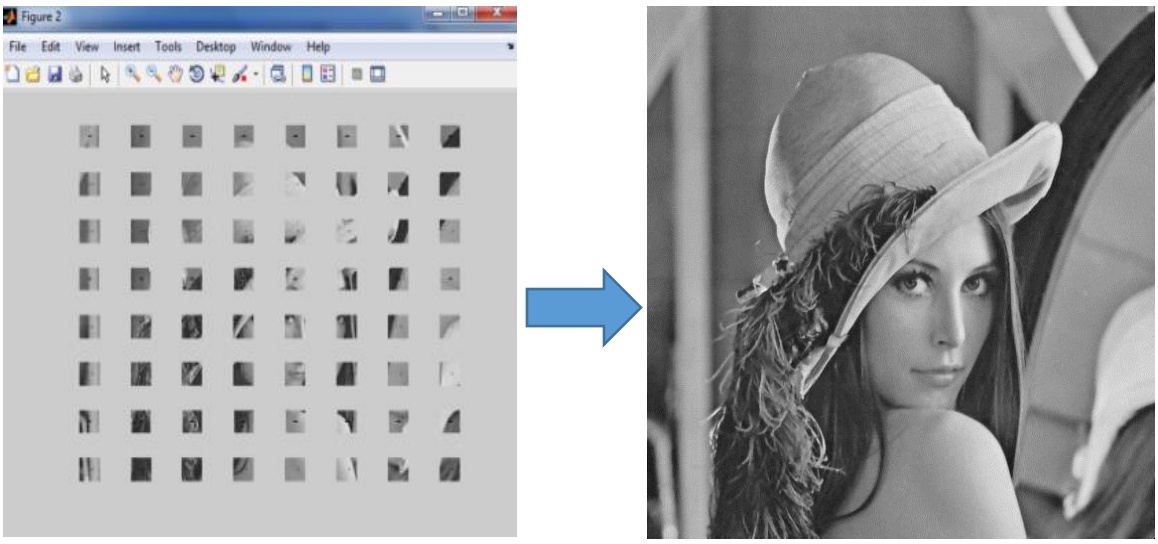
the local pixel is used it will yield a PSNR value of 45.039



(a) Original image b) Watermarked image (randomly)

Figure 4.4 (c) Original cover Picture and watermark image

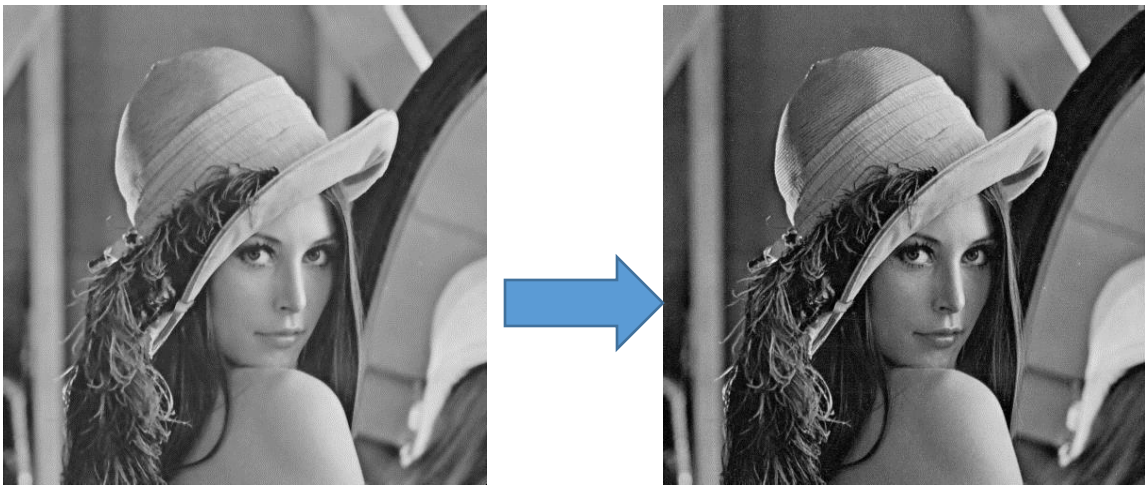
But when the image is divided in the 64 blocks each of size 8*8 and watermark logo is immerged into all the 64 blocks through semi fragile watermarking then recombination of these 8*8 blocks is done to form the original image of 512*512. The quality of image is somehow degraded due to recombination and PSNR value is degraded.



(a) LBP Watermarking in each block (b) recombined image after segmentation

Figure 4.4 (d) Segmented and recombined image

To improve the quality of image this is degraded due to segmentation operation modified image enhancement technique is employed is used to enhance the quality of the image.



(a)LBP Watermarking (b) Unsharp masked image

Figure 4.4 (e) Watermarked and Unsharped masked image

According to the proposed algorithm the value of PSNR is calculated as 61.2204 which show a major improvement in the value of PSNR through this algorithm. Copyright protection of image is also incorporated in this algorithm because of insertion of watermark at the block level.

B. Resilience through Attacks

This system has been verified against many attacks which include cropping, noise, compression and contrast attack. The watermarked logo with various attacks being applied and equivalent extracted tide mark logo and the value of PSNR, SSIM and MSE is being calculated under the respective attacks.

4.3 Calculation of MSE, SSIM and PSNR under respective attacks

Standard Lena image of 512×512 size is used as the host images in this experiment. In this section robustness of digital image watermarking using proposed LBP algorithm at block level is employed. For evaluating the robustness of the anticipated watermarking algorithm, the tide marked picture is subjected to various attacks. Then watermark is extricated from the attacked picture using identical proposed extraction algorithm.

4.3.1 NOISE ATTACK

In this section semi fragile watermarking is employed on Lena image at block level. To ensure the security of image, noise attack is being performed on the Lena image. Salt and

pepper noise characterizes itself as an arbitrarily happening white and black picture element. Salt and pepper noise with intensity level 0.5 is added with the watermarked image and is shown in fig below. PSNR (peak to signal noise ratio), MSE (mean square error) and SSIM (Structural similarity index) is being calculated after this attack.

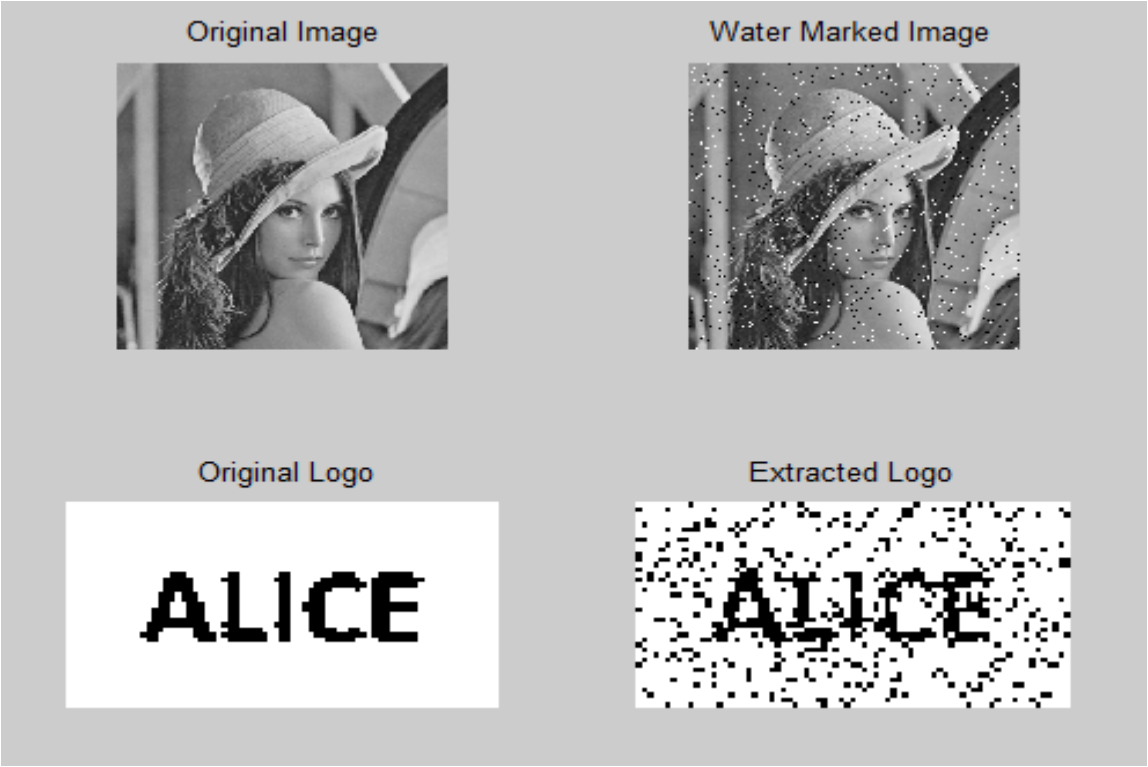


Fig 4.5 Watermarked image and extracted logo after noise attack

In the proposed watermarking embedded algorithm, logo is inserted in the image and is subjected to noise attack. It is a procedure that supplements a noise signal to a picture in order to intentionally corrupt the image, hence risking its pictorial quality. Value of PSNR, MSE and SSIM is being calculated under subjected attack. The method executes good under noise attack giving PSNR, MSE and SSIM of 45.0631, 0.3245 and 0.9896 respectively.

4.3.2 CONTRAST ATTACK

In this section semi fragile watermarking is employed on Lena image and to ensure the security of image and contrast attack is being performed on the Lena image. The value of PSNR, MSE and SSIM are calculated after this attack.

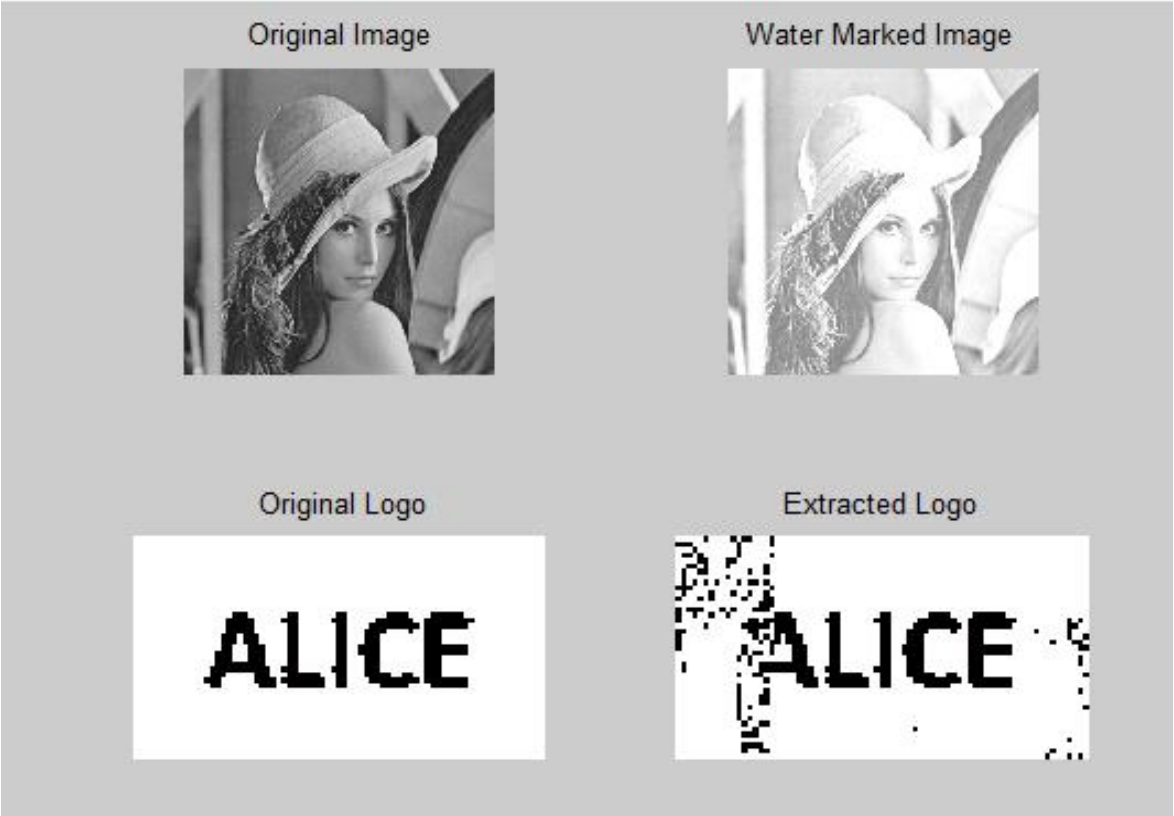


Fig 4.6 Watermarked image and extracted logo after contrast attack

In this figure cover image, tide marked image, original logo and removed logo after contrast attack is shown. Values of PSNR (peak to signal noise ratio), MSE (mean square error) and SSIM (Structural similarity index) is being calculated between the basic image and modified picture by applying contrast attack. The value of PSNR calculated is 45.0631, MSE is 0.3245 and SSIM is 0.9896.From the high PSNR values obtained it is clear that the attacks insertion method does not destroy the quality even in the presence of attacks.

4.3.3 COMPRESSION ATTACK

Compression is one of the most used formats in internet and digital camera. The watermarked image is compressed using quality factor ranging from 0 to 100 and then watermark is extracted. Original and watermarked image along with original and extracted logo after compression attack has been shown in the given figure.

Fig 4.7 Watermarked image and extracted logo after compression attack

Figure shows the watermarked figure and the removed logo later the compression attack is applied to the same image. The proposed method is robust to thisattack providing PSNR of 56.6190, MSE of 0.0560 and SSIM of 0.9935 which shows significantly improvement in these values.

4.3.4 CROP ATTACK

For cropping attack, a part of the watermarked picture had been cropped and each cropped pixel is replaced with another pixel so as the size of the cropped image remains same that is 512 × 512. The removed watermark from the cropped watermarked picture is shown below.

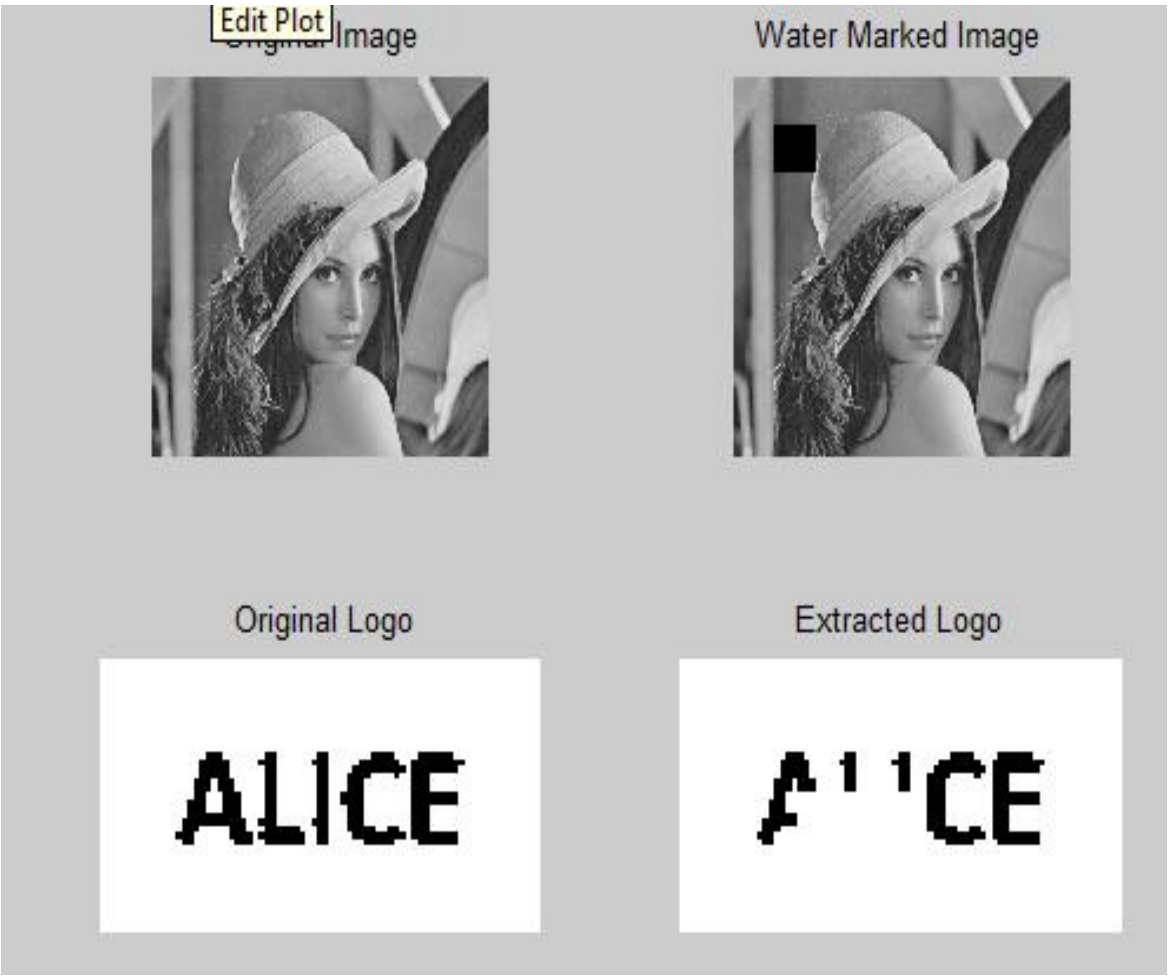


Fig 4.8 Watermarked image and extracted logo after crop attack

The value of mean square error is found to be 0.0978 and the value of peak signal to noise ratio is found to be 48.6339 and SSIM is 0.9895 when crop attack is being employed. From the high PSNR values obtained it is clear that the attacks inserting progression will not affect the quality even in the presence of crop attack.

4.3.5 TAMPERING ATTACK

In this section tampering attack is being performed on the Lena image. The parity section of the watermark is used for tamper recognition and the restoration part of the watermark is used for the image recovery [57].The value of PSNR, MSE and SSIM is calculated after this attack is calculated below.

Fig 4.9 Watermarked image and extracted logo after tampered attack

In the above figure original basic image, tide marked image, original logo and extracted logo after tampered attack is shown. Under tampering the authentic picture is not able be reclaim due to the perpetual loss of sectional content but the proposed method provides high value of PSNR under this attack also. The value of mean square error is found to be 0.5674 also the value of peak signal to noise ratio is found to be 43.0486 and SSIM is 0.9878 when the image is subjected to this attack.

Evaluation results of the algorithms with respect to robustness are discussed in this part. The robustness nature of the projected algorithm is determined using basic three parameters PSNR, MSE and SSIM values by analyzing the original watermarked logo and the extracted watermarked logo with and without the selected attacks. The PSNR, MSE and SSIM results are tabularized in Table 4.1

Table 4.1 Value of PSNR, MSE and SSIM under respective attacks

ATTACKS	PROPOSED METHOD		
	PSNR	**MSE**	**SSIM**
NOISE ATTACK	51.0631	0.2245	0.9896
CONTRAST ATTACK	50.0969	0.3336	0.9887
COMPRESSION ATTACK	59.6190	0.0560	0.9935
TAMPERING ATTACK	41.0486	0.7674	0.9718
CROP ATTACK	43.6339	0.6781	0.9795

From Table 4.3 it can be seen that in all cases, the proposed algorithm has shown improved performance in terms of PSNR when compared to its traditional model. Also the proposed method is robust to numerous typical image processing attacks including compression providing PSNR of 59.6190, MSE of 0.0560 and SSIM of 0.9935 and contrast attack providing PSNR of 50.0969, MSE of 0.3336 and SSIM of 0.9887. The method executes good under noise attack giving PSNR, MSE and SSIM of 51.0631, 0.2245 and 0.9896 respectively. From the high PSNR values obtained it is clear that the attacks inserting progression will not destroy the quality even in the presence of attacks. Under cropping and tampering the authentic picture is not able be reclaim due to the perpetual loss of sectional content, so these are generally considered as a serious attack in the tide marking system but this scheme provides better results for these two attack also. The value of PSNR, MSE and SSIM calculated are 43.6339, 0.6781 and 0.9795

respectively under crop attack and for tampered attack the values calculated 43.6339for PSNR, 0.6781for MSE 0.9795for SSIM under proposed algorithm.

The best result was obtained once no attack had performed on the picture giving the PSNR of 66.2204. The proposed LBP algorithm is robust against all attacks while considering watermarking application. With regard to copyright and authentication applications, even though the performance was better when compared with the traditional LBP algorithm, the PSNR values are still good under all the attack. The results indicate that the suggested algorithm gives best result when compression attack is applied achieving the highest PSNR value of 59.6190 which shows the logo is extracted in an efficient manner under subjected attack with minimum degradation to cover image quality.

CHAPTER-5
COMPARITIVE ANALYSIS

5.1 INTRODUCTION

In this chapter comparative analysis has been carried out between the conventional LBP method and proposed semi fragile algorithm. The focus of the present research is to compare the embedding and extraction watermark with the basic method. Moreover comparison of PSNR values of content based watermarking under subjective attacks is also employed in this part and the quality of the original image is maintained without any degradation in the information. There are many promising modifications, such as cropping an image, lossy compression of the information or adding noises so protections against such attacks are being incorporated in this with better results. The simulation results obtained by implementing the proposed semi-fragile watermarking algorithms are compared with the conventional LBP method in this chapter. Experiments have been carried out with 'Lena' image to evaluate the efficiency of the proposed methods using PSNR (Peak Signal to Noise Ratio, Mean square error (MSE) and Structural similarity index (SSIM) as performance parameters.

5.2 CONVENTIONAL LBP METHOD

The cover image used in this experiment is 'lena.jpg' of size 512 × 512 and the watermark image is 'ALICE logo. The performance of the semi fragile algorithms is also evaluated under incidental and intentional attacks. The performance of the semi fragile algorithms is also evaluated under incidental and intentional attacks. The performance of the semi fragile watermarking methods under consideration is investigated by measuring their imperceptible and semi fragile capabilities. Also the proposed method is robust to numerous typical image processing attacks including compression, additive noise, luminance change, and contrast adjustment. At the equivalent time, they preserve good fragility to certain window operations, such as filtering and blurring, and have improved sensitivity to image tampering.

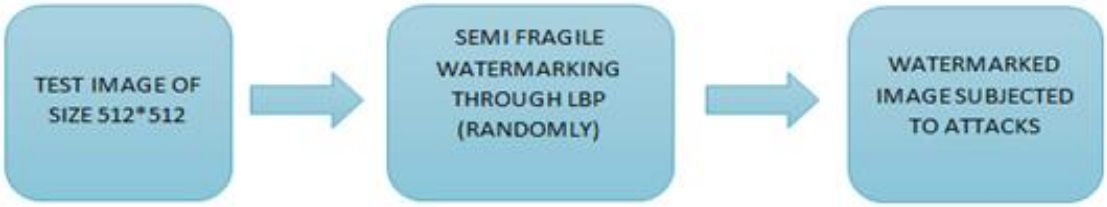


Figure 5.1(a) Conventional method

Table 5.3 showing the values calculated for PSNR, MSE and SSIM for subjected attacks under the conventional method.

Table 5.1 Value of PSNR, MSE and SSIM for conventional method

ATTACKS	**LBP**		
	PSNR	MSE	SSIM
NOISE ATTACK	41.5952	0.7019	0.9752
CONTRAST ATTACK	40.4393	0.8110	0.9711
COMPRESSION ATTACK	50.2471	0.4216	0.9845
TAMPERING ATTACK	31.0413	0.9748	0.9613
CROP ATTACK	32.8168	0.9365	0.9675

The PSNR value calculated between the cover image and the watermarked image using LBP alone is 45.0398 using semi-fragile spatial watermarking technique grounded on LBP operators. Also this method is subjected to numerous typical image processing attacks including compression providing PSNR of 50.2471, MSE of 0.4216and SSIM of 0.9845and contrast attack providing PSNR of 40.4393, MSE of 0.8110and SSIM of 0.9711. Under noise attack PSNR, MSE and SSIM are calculated as 41.5952, 0.7019 and 0.9752respectively.Cropping and tampering are considered as a serious attack in the

watermarking system. The value of PSNR, MSE and SSIM is 46.8168, 0.3765 and 0.9815 under crop attack. Similarly for the tampered attack the values calculated are 39.0413 for PSNR, 0.8348 for MSE and 0.9697 for SSIM.

5.3 PROPOSED METHOD

Same cover image and logo is used in this. According to the algorithm the cover picture is distributed into64 blocks each of size 8 × 8 and the tide mark image is inserted in every block. After embedding all the 64 blocks are recombined to form the cover image of same size that is of 512 × 512.The quality of picture is somehow degraded due to recombination so modified technique is used to enhance the quality of the image. In the extraction part, watermark logo from every of the block has been obtained. Superiority of the withdrawn watermark is checked visually and by calculating PSNR, MSE and SSIM among the original logo and extracted watermark logo from every block.

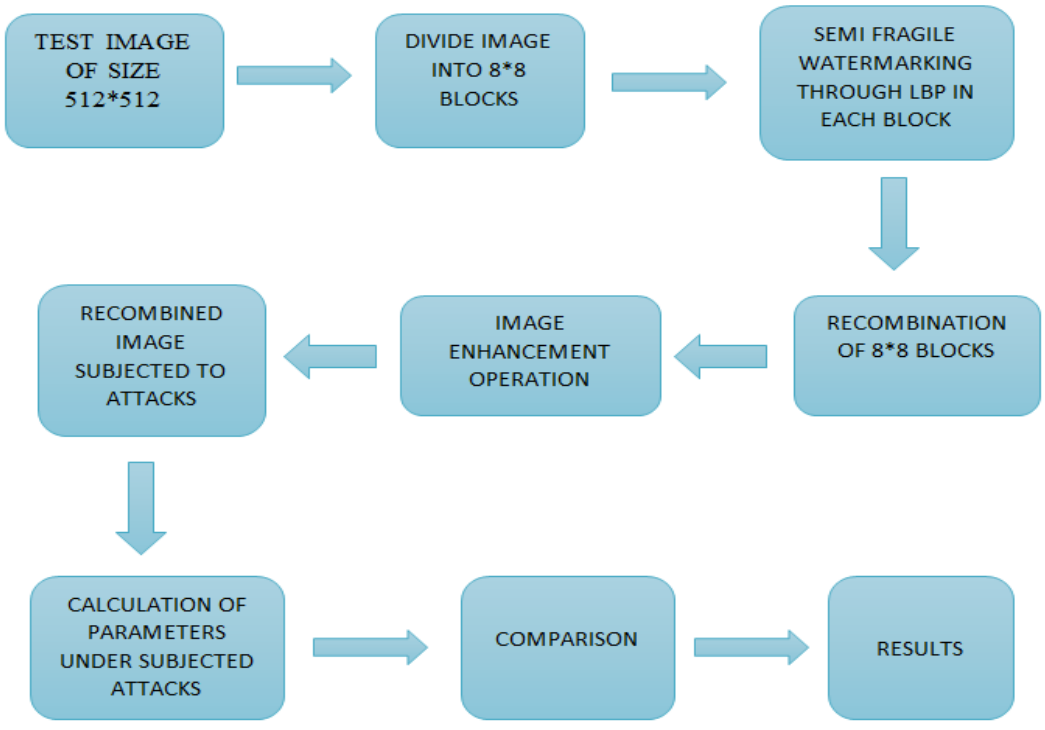


Figure 5.1(a) Proposed method

Table 5.3 showing the values calculated for PSNR, MSE and SSIM for subjected attacks under the proposed algorithm.

Table 5.2 Values of PSNR, MSE and SSIM for proposed method

ATTACKS	PROPOSED METHOD		
	PSNR	MSE	SSIM
NOISE ATTACK	51.0631	0.2245	0.9896
CONTRAST ATTACK	50.0969	0.3336	0.9887
COMPRESSION ATTACK	59.6190	0.0560	0.9935
TAMPERING ATTACK	41.0486	0.7674	0.9718
CROP ATTACK	51.0631	0.2245	0.9896

In the proposed algorithm semi fragile watermarking at block level is employed. Overall the image quality is enhanced as the PSNR value calculated among the cover picture and the water marked image using proposed algorithm the value has improved to 66.2204. Also the proposed method is robust to numerous typical image processing attacks including compression providing PSNR of 59.6190, MSE of 0.0560 and SSIM of 0.9935 and contrast attack providing PSNR of 50.0631, MSE of 0.3336 and SSIM of 0.9887. The method executes good under noise attack giving PSNR, MSE and SSIM of 51.0631, 0.2245 and 0.9896 respectively. Under cropping and tampering the authentic picture is not able be reclaim due to the perpetual loss of sectional content, so these are generally considered as a serious attack in the tide marking system but this scheme provides better results for these two attack also. The value of PSNR, MSE and SSIM is 32.8168, 0.9365 and 0.9675 under LBP alone which is significantly improved to 43.6339, 0.6781 and 0.9795 respectively under crop attack. Similarly for the tampered attack also the values calculated are being improved from 32.0413 to 43.6339 for PSNR, 0.9365 to 0.6871 for MSE and 0.9697 to 0.9795 for SSIM under proposed algorithm.

5.4 COMPARISON

Compared with the LBP-based method, novelty has been introduced in the proposed method as a semi-fragile spatial watermarking scheme at block level with image enhancement approach is implemented. Table5.3 showing the values calculated or PSNR, MSE and SSIM for subjected attacks between two methods.

Table 5.3 Comparison of Proposed method with conventional method

ATTACKS	LBP			PROPOSED METHOD			% IMPROVE-MENT
	PSNR	MSE	SSIM	PSNR	MSE	SSIM	PSNR
NOISE ATTACK	41.5952	0.7019	0.9752	51.0631	0.2245	0.9896	22.7620%
CONTRAST ATTACK	40.4393	0.8110	0.9711	50.0969	0.3336	0.9887	23.8817%
COMPRESSION ATTACK	50.2471	0.4216	0.9845	59.6190	0.0560	0.9935	18.6510%
TAMPERING ATTACK	31.0413	0.9748	0.9613	41.0486	0.7674	0.9718	32.2230%
CROP ATTACK	32.8168	0.9365	0.9675	43.6339	0.6781	0.9795	32.9692%

As the authentication data is entrenched into the LSB of the pixel of every image block, quality of watermarked image remains acceptable. The proposed method provides PSNR value of 61.2204 against previous method and is also robust against additive noise with improved PSNR of 22.7620%, contrast adjustment with 23.8817% improvement in PSNR, compression with 18.6510% improvement in PSNR. This technique provides good results against cropping and tampering attacks also with improvement in PSNR 32.2230% and 32.9692% respectively.

CHAPTER-6

CONCLUSION AND FUTURE SCOPE

5.1 CONCLUSIONS

In the digital era, image watermarking has become a challenging issue. There exist several types of algorithms for watermarking however the main focus of the current research in this field is to make the watermarking algorithm more secure and resilient to geometric transformations. In this research, a framework for enhancement of watermarked image quality using LBP (Local Binary Pattern) watermarking and image enhancement is proposed. The performance of the same has been tested and proved that it is an effective method for embedding and detection of image even in the presence of image processing attacks [49].

Watermarked image is obtained by embedding the watermark in 64 blocks of original 'LENA' image by using semi fragile watermarking. Compared with the LBP-based method, novelty has been introduced in the proposed method as a semi-fragile spatial watermarking scheme at block level with image enhancement approach is implemented. A quantity index, PSNR is employed to evaluate the perceptual change between the original and the watermarked image. The proposed method provides PSNR value of 61.2204.The performance of the semi fragile algorithms is also evaluated under incidental and intentional attacks. Also the proposed method is robust to numerous typical image processing attacks including compression providing PSNR of 56.6190, MSE of 0.0560 and SSIM of 0.9935 and for contrast attack providing PSNR of 45.0631, MSE of 0.3245 and SSIM of 0.9896. The method executes good under noise attack giving PSNR, MSE and SSIM of 45.0631, 0.3245 and 0.9896 respectively. Under cropping and tampering the authentic picture is not able be reclaim due to the perpetual loss of sectional content, so these are generally considered as a serious attack in the water marking system but this scheme provides better results for these two attack also. The value of PSNR, MSE and SSIM is 48.6339, 0.0978 and 0.9895 respectively under crop attack. Similarly for the tampered attack also the values calculated are 43.0486 for PSNR, 0.5674 for MSE and 0.9878 for SSIM under proposed algorithm. The quality of the

proposed techniques is compared with existing LBP technique. The proposed algorithm provides better robustness along some usually used image processing processes such as additive noise with improved PSNR of 22.7620%, contrast adjustment with 23.8817% improvement in PSNR, compression with 18.651% improvement in PSNR. This technique provides good results against cropping and tampering attacks also with improvement in PSNR 32.223% and 32.9692% respectively.

5.2 FUTURE SCOPE

Data transmission does not include only images, but also audio, video and text files. Hence the algorithms can also be applied on those media and security of watermark is carried out with the help of complex procedure can be enhanced by introducing watermarking keys. Future work can be extended in these fields as incidental attacks like sharpening, rotation and Gamma correction have not been considered, the robustness of the algorithms can be verified under these attacks. Almost all algorithms do well on detecting and substitution and have low rate of susceptible to attacks and they offer satisfactory detection and localization of image operation while restoration performances would still need to be improved. More improvement in the value of PSNR using watermarking techniques should be done and also there is need to explore coding tools to increase the efficiency and explore the possibility of a blind or semi blind watermark scheme that remains invisible.

REFERENCES

[1] R. Chamlawi, A. Idris, and Z. Munir, "Secure Semi- Fragile Watermarking Scheme for Authentication and Recovery of Images based on Wavelet Transform," *World Academy of Science, Engineering and Technology*, vol. 23, no. 2, pp. 49-53, 2012.

[2] Zhang Xing and Frank Y. Shih, "Semi-fragile spatial watermarking based on local binary pattern operators," *Optics Communication*, vol. 284, pp. 3904 - 3912, 2012.

[3] Chi Kin Ho and Ling Du, "Semi-fragile watermarking for image tamper localization and self-recovery," *International Conference on Security, Pattern Analysis and Cybernetics*, pp. 328 - 333, 2014.

[4] Xiaomei Zhuang, Chunxing Wang and Fei Han, "Robust Digital Watermarking Scheme of Anaglyphic 3D for RGB Color Images," *International Journal of Image Processing*, vol. 3, no.4, pp. 156 - 165, 2015.

[5] Latha Parameswaran and Anbumani K., "A semi-fragile image watermarking using wavelet inter-coefficient relations," *International Journal of Information Security & Privacy*, vol. 1, pp. 61-75, 2007.

[6] A.K. Parthasarathy and K. Subhash, "An Improved Method of Content Based Image Watermarking," *IEEE Transactions on Broadcasting*, vol.53, no.2, pp.468-479, 2007.

[7] C. Lin, S. Shie and J. Guo, "Improving the Robustness of DCT-Based Image Watermarking against JPEG Compression," *Computer Standards & Interfaces*, vol.32, no. 3, pp.54-60, 2010.

[8] Zhu Xi'an, "A Semi-Fragile Digital Watermarking Algorithm in Wavelet Transform Domain Based on Arnold Transform," *Journal of Systems and Software*, vol. 84, no. 9, pp. 1462-1470, 2011.

[9] MA Jmaa, "Based on the Fourier Transform and the Wavelet Transformation of the Digital Image Processing," *International Conference on Computer Science and Information Processing,* pp. 1232-1234, 2012.

[10] Chao-Yong and Qing Zhu, "A DCT-based dual watermarking algorithm for three-dimensional mesh models," *International Conference on Consumer Electronics, Communications and Networks,* pp. 1509 - 1513, 2012.

[11] Rafi Ullah, Asifullah Khan and Aamir Saeed Malik, "Dual-purpose semi-fragile watermark Authentication and recovery of digital images," *Computers & Electrical Engineering,* vol. 39, no. 7, pp. 2019-2030, 2013.

[12] Amir Hazem and Munawer Al-Otum, "Semi-fragile watermarking for grayscale image authentication and tamper detection based on an adjusted expanded-bit multiscale quantization-based technique," *Journal of Visual Communication and Image Representation*, vol. 25, no. 5, pp. 1064-1081, 2014.

[13] Xiaojun Qi and Xing Xin, "A quantization-based semi-fragile watermarking scheme for image content authentication," *Journal of Visual Communication and Image Representation,* vol. 22, no. 4, pp. 187-200, 2011.

[14] Mohamed.U Celik & A.M. Tekalp, "Hierarchical Watermarking for Secure Image Authentication with Localization," *IEEE Transactions on Image Processing*, vol.11, pp. 585-595, 2010.

[15] Nasrin M. Makbol and Bee Ee Khoo, "Robust blind image watermarking scheme based on Redundant Discrete Wavelet Transform and Singular Value Decomposition," *International Journal of Electronics and Communications*, vol. 67, no.2, pp. 102-112, 2013.

[16] Abhilasha Singh, Osamah M. Al-Qershi, Bee Ee Khoo, "ROI–based Tamper Detection and Recovery for Medical Images Using Reversible Watermarking Technique," *IEEE International Conference on Information Theory and Information Security,* pp. 151-155, 2010.

[17] Chin-Chen Chang, Kuo-Nan Chen and Li-Jen Liu, "secure fragile watermarking scheme based on chaos-and-hamming code," *Journal of Systems and Software,* vol. 84, no. 9, pp. 1462-1470, 2011.

[18] Sanjay Rawat and Balasubramanian Raman, "A chaotic system based fragile watermarking scheme for image tamper detection," *International Journal of Electronics and Communications,* vol. 65, no. 10, pp. 840-847, 2011.

[19] U. M. Gokhale , Y.V.Joshi, "A Semi Fragile Watermarking Algorithm Based on SVD-IWT for Image Authentication," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 1, no. 4, pp. 217-222, 2012.

[20] Siddharth Singh, Rajiv Singh and H.K Singh, "OCT-domain robust data hiding using chaotic sequence," *International Conference on Multimedia, Signal Processing and Communication Technologies,* pp. 300-303, 2011.

[21] J.Xiao, Li Sukang and Mei Jiansheng, "A Digital Watermarking Algorithm Based On OCT and DWT," *International journal on Web Information Systems and Applications,* vol. 3, no.2, pp. 104-107, 2009.

[22] S.K. Maeno, Qibin Sun, Shih-Fu Chang and M. Suto, "New semi-fragile image authentication watermarking techniques using random bias and non-uniform quantization," *IEEE Transactions on Multimedia,* vol. 8, pp. 32 - 45, 2006.

[23] Radu. O. Preda, "Semi-fragile watermarking for image authentication with sensitive tamper localization in the wavelet domain," *Journal of Visual Communication and Image Representation*, vol. 46, no.1, pp. 367-373, 2013.

[24] Ruisong Ye, "Fast Modified Signed Discrete Cosine Transform For Image Compression," *Pacific-Asia Conference on Circuits, Communications and System*, pp. 485-488, 2009.

[25] Archana Tiwari and Manisha Sharma, "Comparative Evaluation of Semi-fragile Watermarking Algorithms for Image Authentication*," Journal of Information Security*, pp. 189-195, 2012.

[26] Hanan Elazhary, "A Fast, Blind, Transparent, and Robust Image Watermarking Algorithm with Extended Torus Automorphism Permutation", *International Journal of Computer Applications*, vol. 32, no.4, pp. 34-41, 2011.

[27] S. Shefali and S.M. Deshpande, "Information Security through Semi-fragile Watermarking," *International Journal of Electronics and Communications*, vol. 3, pp. 235-239, 2007.

[28] Said E. El-Khamy and Mohamed Shokry, "Enhanced Performance of Blind and Non-Blind Adaptive Arrays using Wavelet Beamforming," *International Conference on High Performance Computing and Simulation,* vol. 2, pp. 347-351, 2013.

[29] V. Senthil, R. Bhaskaran, "Robustness Analysis of Blind and Non-Blind Multiple Watermarking using Edge Detection and Wavelet Transforms," *Journal of Visual Communication and Image Representation*, vol. 3, no. 2, pp. 106-111, 2008.

[30] I.Amerini, L. Ballan and Serr G., "A SIFT-based Forensic Method for Copy-Move Attack Detection and Transformation Recovery," *IEEE Transactions on Information Forensics and Security*, vol. 13, pp. 1099-1110, 2011.

[31] T. A Kohale, P. R. Lakhe and S. D.Chede, "Detection of Post-operated Copy-Move Image Forgery by Integrating Block based and Feature based Method," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 9, no. 4, pp. 788-790, 2014.

[32] Yueqiang Liu, Guiduo Duan, and Xi Zhao, "An improved watermarking algorithm using adaptive threshold," *World Academy of Science, Engineering and Technology*, vol. 23, no. 2, pp. 49-53, 2012.

[33] X. A. Zhu, "A Semi-Fragile Digital Watermarking Algorithm in Wavelet Transform Domain Based on Arnold Transform," *IEEE Transaction on Signal Processing*, vol. 6, pp. 2217-2220, 2010.

[34] C. Y Lin and S. Chang, "A robust image authentication method distinguish JPEG compression from malicious manipulation," *IEEE Transactions on Image Processing*, vol. 2, pp. l53-168, 2001.

[35] S.W. Wang and K.C. Fan, "A Wavelet based Public Key Image Authentication Watermarking," *IEEE Transaction on image processing*, vol. 13, pp.321-324, 2009.

[36] S.S. Sujatha and Mohamed Sathik, "Feature Based Watermarking Algorithm by Adopting Arnold Transform," *Proceedings of the Springer International Conference on Information and Communication Technologies*, vol. 10, pp.78-82, 2010.

[37] Mohamed Sathik and Sujatha S.S., "A Secure Blind Semi-Fragile Watermarking Technique for Digital Image Authentication," *International Journal of Advanced Research in Computer Science*, vol. 3, pp.18-22, 2012.

[38] Kwang-wook Lee, You-sun Kim and Sung-jea Ko, "Effective color distortion and noise reduction for unsharp masking in LCD," *IEEE Transactions on Consumer Electronics*, vol. 54, no.3, pp. 1473 - 1477, 2008.

[39] Wei Qi, Xing-Jun Chen and Dong Xu, "A Novel Semi-Fragile Audio Watermarking Technique Based on Support Vector Regression," *Ninth International Conference on Frontier of Computer Science and Technology*, pp. 81-86, 2015.

[40] Xinpeng Zhang and Shuozhong Wang, "Fragile Watermarking Scheme using a Hierarchical Mechanism," *Signal Processing*, vol. 89, no. 4, pp.675-679, 2009.

[41] R. C. Gonzalez, R. E. Woods, and S. I. Eddins, *Digital Image Processing*, 3rd ed. Knoxville: Gatesmark Publishing, 2009.

[42] Xunzhan Zhu, Anthony T.S. Ho, Pina Marziliano, "A new semi-fragile image watermarking with robust tampering restoration using irregular sampling," *Signal Processing*, vol. 22, no. 5, pp. 515-528, 2007.

[43] Chamidu Atupelage, Koichi Harada Atupelage & K. Harada, "PKI based Semi-Fragile Watermark for Visual Content Authentication," *Proceedings of the World Congress on Engineering and Computer Science*, vol. 3, pp. 1-6, 2008.

[44] Mohamed Sathik and S. Sujatha "Application of Toeplitz matrix in Watermarking for Image Authentication", *Optics Communication*, vol. 284, pp. 3904-3912, 2012.

[45] Megha Kansal, Sukhjeet K. Ranade and Amandeep Kaur, "Fragile Watermarking For Image Authentication Using a Hierarchical Mechanism", *International Journal of Engineering Research and Applications*, vol. 2, no.4, pp. 1759-1763, 2012.

[46] Al-Mualla M.E., "Content Adaptive Semi-fragile Watermarking for Image Authentication," *Journal of Computer Science*, vol.3, no.9, pp.740-746, 2007.

[47] Sha Wang, Dong Zheng and Filippo Speranza, "Adaptive Watermarking and Tree Structure Based Image Quality Estimation," *IEEE Transactions on Multimedia*, vol 16, pp. 311-325, 2014.

[48] Guiduo Duan, Yueqiang Liu and Xi Zhao, "An improved watermarking algorithm using adaptive threshold," *International Conference on Progress in Informatics and Computing (PIC),* pp. 385 - 389, 2014.

[49] Mei Yu, Jing Wang and Ting Luo, "New fragile watermarking method for stereo image authentication with localization and recovery," *AEU - International Journal of Electronics and Communications*, vol. 69, no.1, pp. 361-370, 2015.

[50] Kusam, Abrol and P. Devanand, "Digital Tampering Detection Techniques: A Review," *International Journal of Information Technology*, vol. 16, no. 3, pp. 125-132, 2009.

[51] Zhicheng Ni, Yun Q. Shi, Qibin Sun and Xiao Lin, "Robust Lossless Image Data Hiding Designed for Semi-Fragile Image Authentication," *IEEE Transactions on circuits and systems for video technology*, vol. 18, pp. 497 - 509, 2008.

[52] Chuhong Fei, D. Kundur and R. H. Kwong, "Analysis and design of secure watermark-based authentication systems," *IEEE Transactions on Information Forensics and Security*, vol. 1, pp. 43 - 55, 2006.

[53] Ali Al-Haj, "Combined DWT-DCT Digital Image Watermarking," *Journal of Computer Science*, vol. 3, no. 9, pp. 740-746, 2007.

[54] M. Sathik and S. Sujatha, "Authentication of Digital Images by Using a Semi-Fragile Watermarking Technique," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, no. 11, pp. 39-44, 2012.

[55] Angela Piper and Reihaneh Safavi-Naini, "Scalable fragile watermarking for image authentication," *IET Information Security*, vol. 7, pp. 300-311, 2013.

LIST OF PUBLICATIONS

- Alice Ghai, Ankush Kansal, "Enhancing image security by using semi fragile techniques" communicated in *Journal of engineering research.*
- Alice Ghai, Ankush Kansal, "Image security enhancement against various attacks by using semi fragile watermarking" communicated in *Computer Vision and Image Understanding - Journal - Elsevier.*

Alice_final_thesis.docx

ORIGINALITY REPORT

11%	4%	7%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Higher Education Commission Pakistan Student Paper	1%
2	Shunzhi Zhu. "An Improved Semi-fragile Digital Watermarking Scheme for Image Authentication", 2007 International Workshop on Anti-Counterfeiting Security and Identification (ASID), 04/2007 Publication	1%
3	www.ijert.org Internet Source	1%
4	Wenyin, Z.. "Semi-fragile spatial watermarking based on local binary pattern operators", Optics Communications, 20110801 Publication	1%
5	Zhang, Wenyin. "Watermarking Based on Local Binary Pattern Operators", Multimedia Security Watermarking Steganography and Forensics,	1%