DEVELOPMENT OF IMPROVED ATTACK RESISTANT IMAGE WATERMARKING TECHNIQUE

By

Simmal Pasha

A thesis submitted to the faculty of Information Security Department,
Military College of Signals, National University of Sciences and Technology,
Islamabad, Pakistan, in fulfillment of the requirements for the degree of MS in
Information Security

July 2020

DECLARATION

I hereby declare that no portion of the work presented in this thesis has been submitted either at this institution or elsewhere in support of another award or qualification.

DEDICATION

This work is a dedication to

MY PARENTS AND MY SIBLINGS

for their love and support

ACKNOWLEDGEMENTS

All praises be for the ALMIGHTY ALLAH; al-Hadi, al-Fattah, and al-Muizz

The achievement of this thesis is accomplished with the participation and cooperation of all guidance committee. With affection and deep appreciation I acknowledge our indebtedness to his honorable thesis supervisor Brig Dr. Abdul Ghafoor and thesis co-supervisor Dr. Mohsin Riaz , who not only supported me with every possible guidance but also encouraged my spirits at critical junctures that lead to the completion of work submitted as thesis.

I express my thanks to Brig Dr. Abdul Ghafoor, from whom I sought valuable advice and encouragement to achieve this task. I'm thankful to my committee members; Asst Prof Dr. Naima Iltaf and Dr. Adil Masood for their guidance.

I would also take this opportunity to appreciate my parents who continually pushed me to be the best version of myself.

SUPERVISOR CERTIFICATE

This is to certify that **Simmal Pasha** student of **MSIS-15** Course Reg.No: **00000104955** has completed her MS Thesis title "**Development of improved attack resistant image watermarking technique**" under my direction. I have gone through her work and am content with it.

Thesis Supervisor
(Dr. Abdul Ghafoor)

Dated: 24/8/2020

THESIS ACCEPTANCE CERTIFICATE

Certified that final version of MS thesis written by **Simmal Pasha**, Registration No. **00000104955** of Military College of Signals has been examined by undersigned, found to be complete in all respects in compliance with NUST Statues /Regulations, free of p lagiarism, errors and approved as partial fulfillment for MS degree award. It is further confir med that required modifications have also been introduced into the said thesis as pointed out by the student's GEC representatives.

Signature: ______________________

Name of Supervisor: Dr. Abdul Ghafoor

Date: 24/8/2020

Signature (HoD):______________________

Date: ______________________

Signature (Dean):______________________

Date: ______________________

ABSTRACT

Digital watermarking is a method that prevents unauthorized distribution of copyrighted material by providing means of proving ownership of the material. This thesis introduces a watermarking technique based on lifting wavelet transform (LWT), schur and singular value decomposition (SVD). Generalized arnold transform (GAT) scrambling is applied on a grayscale watermark logo which works for improving the security of the watermark. The colored image is decomposed into high level and low level sub-bands using LWT, first schur decomposition is applied on watermark as well as the selected High-High (HH) sub-band to get the upper triangular matrices and then watermark is embedded in the image using SVD. "Peak-Signal-to-Noise-Ratio" (PSNR) and "Normalized Correlation" (NC) are the two metrics through which we can measure the perceptual quality and similarity of the extracted watermarks. The proposed scheme is compared under various attacks including noising attacks (salt & pepper, multiplicative etc.), geometric attacks (crop, translation, projection etc.), image processing attacks (histogram equalization, gaussian smoothing, contrast enhancement etc) were also applied on the watermarked images to check the performance of the scheme under attacks. The results show that the proposed scheme performs better in terms of quality and robustness in various attacks than the existing scheme.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

CT Contourlet Transform

DWT Discrete Wavelet Transform

DFT Discrete Fourier Transform

DCT Discrete Cosine Transform

FCT Fast Curvelet Tansform

GAT Generalized Arnold Transform

HVS Human Visual System

LWT Lifting Wavelet Transform

MSE Mean Square Error

NC Normalized Correlation

PSNR Peak-Signal-to-Noise-Ratio

RPCA Robust Principal Component Analysis

RGB Red, Green and Blue color model

SVD Singular Value Decomposition

SDE Self-Adaptive Differential Evolution

SIFT Scale Invariant Feature Transform

SVM Support Vector Machine

Chapter 1

INTRODUCTION

For years, digital watermarking was introduced to avoid unauthorized data copying. An effective watermarking system has two important characteristics, robustness against attacks and perceptual imperceptibility which helps to measure the watermark quality. This thesis introduces a watermarking technique which is based on a new “LWT-SCHUR-SVD” combination. “Arnold transform” is applied for security purposes to render the data on the watermark meaningless. The scheme is verified by running attacks such as “image processing” and “geometric attacks”. The algorithm and contrast of its results with the techniques proposed by Ramsha et al. [1] Gupta and Raval [2] and J. Liu et al. [3] are given in the subsequent chapters.

Chapter 1 discusses the different watermarking techniques, the motivation for watermarking, the general scheme of watermarking, its classification and the real life applications. Also included in this chapter are the multiple types of attacks that watermarked image may be a subject to, the methods to measure watermarking performance and the structure of the proposed thesis for the evaluation.

1.1 Introduction

Now-a-days the digital data is not only being produced at a very rapid pace but is also made available and easily deliverable with lesser and lesser costs. As the communication and collaboration increases using digital world, the need for maintaining data and its integrity will only increase. Therefore, securing digital data and multimedia content is a vital issue that needs to be worked on. For the protection and authentication of the content owners researchers have found solutions in encryption and watermarking [4, 5].

Watermarking not only provides authenticity but also acts as a deterrent control for activities such as data exfiltration, by ensuring that the data remains protected from unauthorized usage. In case of a document leak, watermarking provides a means to identify the content owner. Performing encryption for protection of information is also a very strong control which render the information completely meaningless for the users who do not have any means to decrypt it but converting information into unintelligent and random data using some algorithm. However, the limitation with encryption is that one as long as the data remains encrypted it remains protected, considering a strong algorithm was used to decode it, but once decoded the data can be misused if gotten into the hands of unintended person. Secondly that data might not always require to be encrypted, sometimes the nature of the data is such that it may only require to prove the ownership of the content. Watermarking therefore, offers an alternate solution which addresses the limitation of encryption and protects the ownership of data even if it is in intelligent form.

The technology to incorporate the watermark into data should be such that operations such as filtering, rotation, smoothing, etc. can hardly be altered or removed during transition. The scheme chosen for watermarking depends on the goal one is trying to achieve with watermarking. One concern is what needs to be added in the host signal, if the goal is integrity then a hash [6] or random bit sequence, which usually is derived from the host signal, may be added in the image so that after extraction process the same hash or sequence may be generated to prove integrity. If the goal is prove uniqueness [7] or ownership then the watermark may not have any relation with the host image. Secondly, if the watermark should be visible or not in the image. Embedding of the host signal in the visible water-marking technique can be seen directly by human eyes. The invisible watermarking technique implies that the use of operations on the image and the integration of watermark information is invisible.

In this study, an invisible image watermarking scheme is discussed which embeds the watermark of size 256x256 into the host image of 512x512 so that it achieves imperceptibility and robustness.

1.1.1 General Properties of Watermarking

A watermarking scheme may be viewed as a box [8], taking certain inputs and returning an output that should have few important and basic properties[9, 10]. The design of the watermarking system define the outputs and hence its properties which vary from design to design. As discussed before the use case of the watermark defines the need for one particular property [11] These properties include invisibility, robustness, high data embedding capacity and security [12]. It is the designer's decision on what must be traded-off for the gains in other properties as usually some properties may conflict with one another. Discussed below are few of the properties of a watermarking system:

1.1.1.1 Invisibility

The watermark inserted should be done using techniques so that it does not cause any visible amount of alteration in the image causing degradation of its visual quality, 'Human Visual System' (HVS) characteristics serve as an indicator for this purpose [13, 14]. This property in the case of image watermarking is known as invisibility whereas in other signals it is referred to as un-detectability. Most of those measures used to quantify the invisibility of the watermark are detailed in [15]. Listed below are the most common ones used.

Bit Error Rate (BER) is the bits ratio different from the host image's total bits.

Peak Signal to Noise Ratio (PSNR) the measurement of image quality after operations in a primary image and most commonly used metric in the research to determine the watermarking visibility.

Normalized Correlation (NC) which quantifies how similar the built-in watermark is to the extracted watermark.

Mean Square Error (MSE) which assesses the excellence of a predictor generally and especially used in machine learning algorithm models [8] but can also give an estimate of the "error" caused by introduction of the watermark in the host signal. Higher values of MSE denote that the signal is more distorted.

1.1.1.2 Robustness

Digital images during transmission can be a subject to multiple types of image attacks. The level of difficulty required to remove the watermark from the original signal is defined by the robustness property, whether the attempt is carried out by a malicious attacker or is by natural degradation during transmission. A robust scheme of watermarking is calculated by its capacity to resist the image and geometric attacks and in keeping the watermark secure. There are three levels of robustness [16] each with its own applications.

Fragile Watermarking

For this type of watermarking the inserted signal can easily be extracted or modified as it is fragile towards intentional and unintentional attacks [17]. Any changes made in the host signal would result in destroying the watermark. The applications of this kind of watermarking is that it can be used for authentication applications for content [18, 19] where the goal is to ensure that integrity of the host signal, proving that it has not been tampered with.

Semi-Fragile Watermarking

Related to 'fragile watermarking', this type of watermarking ensures that significant modifications have not been made in the image, and that the watermark is fragile to only certain alterations. This scheme, like fragile watermarking can be used for integrity check [19] as it shows good results against certain attacks such as noise attacks.

Robust Watermarking

In this scheme, the signal is added in the image in a way that it is hard to extract the watermark from the image. Even if it subject to attacks [20] etc., usually high robustness can be achieved by using techniques such as embedding in the lower bits of image, embedding watermark multiple time. It can also be used for integrity but main use of this type of watermarking is content authentication [16].

1.1.1.3 Capacity

This property measures for the material that can be inserted in the image, usually defined by bits per signal unit. The more amount of information embedded results in distortion of the image whereas a watermarking system must be able to embed reasonable amount information so it is practical for use.

1.1.1.4 Blindness

This explains how the watermark is removed from the host signal depending on its usage. This property is divided into three categories [10].

Blind Watermarking:

In this host image or watermark are not required for extraction and only the watermarked signal and the key are required for removal [21]. This scheme uses techniques such as statistical analysis and correlation techniques or location map [15] etc. for extraction of watermark.

Non-Blind Watermarking:

In this the image and the original watermark both are required for extraction [22]. Availability of the original host signal or image may help in restoration after attacks hence giving a chance for more robustness than blind watermarking.

Semi-Blind Watermarking:

This type may not be require the image, but the inserted watermark and secret key (if applicable) may be required for extraction [23, 24]. This scheme gives more robustness as the original contents are present, which may help in improvement against attacks and distortions.

1.1.1.5 Time Complexity

This property of the watermarking scheme can be calculated by adding the period required to insert the watermark in the image and the period necessary to retrieve a watermark from the image. Time complexity gives a measure of the delay that might be faced during the watermarking process.

1.1.2 Applications of Digital Watermarking

The wide techniques that are introduced for watermarking have many applications [25]such as owner identification, tampering authentication, content authentication, copy control, steganography, access control etc. These applications map against the four pillars of information security confidentiality, integrity, authentication and availability.

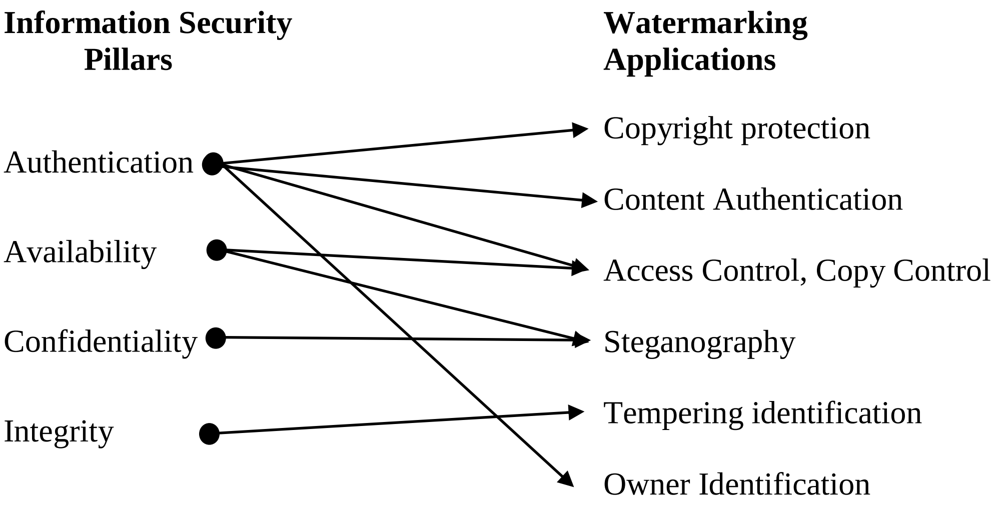


Figure 1.1 Applications of watermarking mapped to the information security pillars

1.2 A General Framework of Image Watermarking

The common structure of image watermarking is summarized in Figure 1.2 that defines the major phases of the watermarking scheme.

1.2.1 Context Setting

This involves making the best decision of two things, the carrier signal selection. For example in case of video watermarking it could either be audio or video channel that may carry watermark. Also the embedding data selection is considered which is determines if it is going to be an image, a signal an audio etc. Keeping in mind the application the scheme is being developed for it may also be decided that if encryption can be used an added security element in the scheme, such as work presented in scheme [1] uses arnold transform for watermark scrambling.

1.2.2 Embedding

Embedding stage consists mostly of making a decision about the intensity of the logo, which is to be integrated in the image and the position of the watermark and the algorithm to be adopted by the scheme.

1.2.3 Signal Transmission

This stage involves the transmission of the embedded host signal over network or using file transfer and represents the malicious and non-malicious attempts that may degrade the watermark.

1.2.4 Extraction

Watermark is extracted from the host signal in this stage depending on the inputs provided, such as the original host signal and watermark may or may not be available depending on the blindness property of watermark described earlier. It also verifies the extracted watermark and measures the accuracy and the robustness with which the watermark is extracted.

1.2.5 Utilization

This stage covers the applications of the watermark which after extraction it can be utilized for, for example it can prove tamper detection [26] or can prove ownership [27] of the host signal.

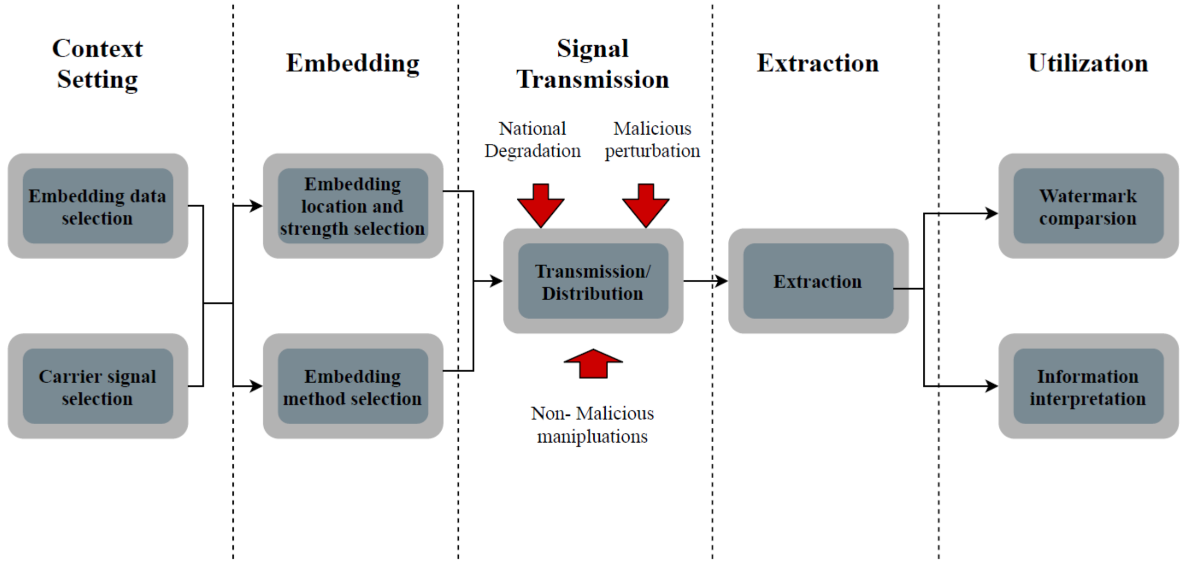


Figure 1.2 General framework of image watermarking

1.3 Domain based Watermarking System Classification

The schemes are classified according to algorithm steps followed for watermarking if the watermark is inserted directly in the host image or if the image is transformed.

1.3.1 Spatial Domain based Watermarking

To add the watermark the bits of the image are modified in spatial domain. The steps in spatial domain is are easy to implement and understand.

1.3.2 Frequency Domain based Watermarking

Frequency domain watermarking techniques can provide better performance against certain attacks [1]. It works by modifying the bits of image after applying some type of transform so that it causes minimum change in the image.

1.4 Problem Statement and Objectives

Despite a lot of work in the field of watermarking, the existing watermarking techniques exist with trade-off between accuracy and speed and only perform well for a small set of images. To resolve this “a robust attack resistant image watermarking scheme” is introduced. The objectives of the proposed research are:

- To improve accuracy by exploring new techniques for embedding and detection of watermark
- To increase speed of the watermarking process
- To increase robustness in different attack scenarios such as rotation, translation, X-shearing, Y-shearing and affine attacks.

1.5 Contribution in this Thesis

In this paper, a “lifting wavelet transform” (LWT), “schur decomposition” (SD) and “singular value decomposition” (SVD) based watermarking is introduced.

A gray-scale watermark image is picked and for security purposes and robustness is scrambled using GAT. The image is transformed to YCbCr color model, and LWT is applied on one channel to get the sub-bands. Schur decomposition is applied on one band and again SVD is applied on the upper triangular matrix obtained using schur. The processed watermark is then added using SVD. Simulation results on a set of over 25 images show the imperceptibility and robustness against various attacks.

1.6 Structure of the Thesis

This thesis is broken down in five chapters:

- Chapter 1: Introduction, outline the different types of watermarking and the attacks that can be used on it.
- Chapter 2: Literature review summarizes the work already carried out on the proposed topic. Quantitative metrics used for measuring the results are also discussed in this section.
- Chapter 3: Proposed attack resistant image watermarking scheme is discussed in detail.
- Chapter 4: Experimental results and quantitative analysis of the suggested scheme and contrast of results with [1] are discussed in detail.
- Chapter 5: Conclusion, represents a summary of all work and covers the possibility of expanding the suggested work for resolution of more problems.

For reader facilitation, a bibliography is given after the conclusion of the thesis.

Chapter 2

LITERATURE REVIEW

Watermarking is usually accomplished in spatial and frequency domains. To incorporate the watermark in spatial domain, the bits of the original image are modified in spatial domain. The advantage of these methods is that they are easy to implement, are less complex than frequency domain methods and can be mathematically analyzed easily. In frequency domain, complete image or chunks of the image are often transformed to add the watermark bits into the image, however, it is possible to embed watermark directly in this domain. The benefit of frequency domain is that changes are less visible which improves robustness of the image.

Few of the existing watermarking techniques are described below categorized in spatial and frequency domains [10].

2.1 Spatial Domain

These methods are sensitive to different image attacks, to counter that problem often the information is embedded multiple times in the image.

2.1.1 Least Significant Bit (LSB) Method

One such system in spatial domain is the LSB method. The method involves changing of the least significant bits of the cover image, to embed the watermark [28]. First, the watermark is converted into bits and then those bits are added to the original image. Another implementation presented by *Venugopala et al*.[29], selects blocks from the original image, in which blocks are selected from one of host image channels and watermark is inserted by representing the selected blocks in 8 bit form. *Somwanshi et al*.and *Wang et al*. [30, 31] embeds watermark using XOR operation in addition to LSB where first the image is split into various blocks followed by generation of data for authentication by XORing binary representation of singular value from one of the blocks and watermark bits. Each block is translated into the LSB plane and then watermark is added into each plane. *Zhang et al*. [32] and *Shehab et al*. [33] proposes a fragile watermarking scheme by embedding data in the image after applying Singular Value Decomposition (SVD) on the image and incorporating watermark in the least significant bit of the pixel data. The advantage of LSB method is that it provides good imperceptibility, ease in implementation and low value of image quality but disadvantages are that since the least significant bits are easily manipulated by rotation, noise attacks and cropping it offers less robustness and watermark can easily be distorted.

2.1.2 Correlation Based Method

Miyazaki [34] uses a correlation based approach, in which correlation measure in the pseudo random code and the image helps in identification of the watermark. *Gajriya et al.* [35] further implemented this using a pseudo-random sequence and the host image to produce a random sound that is then inserted in the image to acquire the watermark embedded signal. The resultant image is then compared to the host image and is identified using the corresponding watermark. This method depends on the fact that the characteristics of host images must be sufficiently rich for distinguishing and the image quality may decrease if the watermarking strength too high.

2.1.3 Linear Mask Embedding

One of the techniques which aims at improving watermark's effectiveness includes defining a mask identifying parts of the image which are less sensitive and then adapting the strength of the watermark when embedding in the image pixel. This mask may be same for all the frames as shown by *Nikolaidis* [36] or may be calculated as described by *Yamuna* [37]. *Yamada* [38] proposes such a solution in which a mask is first created and then embedded in one frame of the image using the following equation:

$$Yi' = Yi + \alpha i\, Wi \tag{2.1}$$

where *Yi* is the original pixel value i, αi represents watermark intensity mask in pixel *i* belonging to frame *f*, and *Wi* represents the watermark bit *i*. Calculation of average of all frames is done for the extraction.

2.2 Frequency Domain

Watermarking methods applied in the frequency domain, tend to provide better results against image attacks such as processing, compression, filtering and cropping. The reason for this is that firstly unlike spatial domain where watermark bits directly manipulate the image bits, in frequency domain watermark is inserted using transforms to modify the image, enabling the watermark values to be distribute evenly throughout the image, making watermark stable against many attacks. Further, the obtained image coefficients are small when the transform is applied, hence the modifications made in the image are less visible, the image quality is better as a result.

2.1.1 Watermarking Techniques using Fourier Transforms

2.2.1.1 Discrete Cosine Transform (DCT) Techniques

Discrete Cosine Transform (DCT) has been used alone as well as with a combination of other transforms. DCT can either be used as described by *Garg et al.*[39] on whole image or as *Lin et al.*[40] applied on a 8x8 non-over lapping image blocks followed by insertion of the watermark to the modified coefficients. After applying DCT on 8x8 blocks the coefficients are divided into two parts, one is the Direct Current (DC) coefficient whose value is often the largest of the 63 additional coefficients are known as coefficients for alternating current (AC). Coefficients are zigzagged and picked from the DC, positioned at the upper left corner, to the 64th component.

Because the watermark is incorporated into high and low frequency coefficients, different techniques have been suggested which explore both options. The watermark is found integrated within high frequency coefficients, as done by Chen *et al.*[41], where image quality is improved but the watermark is prone to filtering attacks as filtering operation may aid in erasing the watermark from the image. For trying out an alternate possibility if the coefficients with lower frequency, as done by *Nakano* [42], maybe chosen for embedding the watermark it might be more resistant towards attacks such as filtering, noise and compression.

A DCT watermarking method is introduced for video watermarking [10] where the watermark is added in the nth lowest coefficients depending on the relation of a block to another one of video's frame. *Roy* [43] embeds watermark information in the DCT transformed coefficients of image by applying a mathematical remainder theorem to enhance the image quality. Abdi *et al.* [44] proposes to insert the watermark by selecting the last two coefficients in decreasing order of frequency coefficients by applying the quantization in order to reduce sync error and improve quality of the host image. *Ma et al.* [45] proposes a technique that integrates more than one watermark copies into an image by applying DCT on the blue and green image components and using the repletion code for medium AC coefficients.

For embedding in high frequency coefficients *Poljicak et al.* [46] proposes a method to add the watermark in non-zero high-frequency AC image coefficients so that the watermark's robustness is maintained. In another alternate approach *Pun* [47] proposes to insert watermark in the AC values of the macro-blocks after selection.

Advantage of DCT is that we can get high robustness against processing attacks, but the disadvantage is that it is vulnerable to "cropping and scaling". Also the amount of changes that are performed on the DCT transformed coefficients have a grave effect on the transparency of the watermark and as a result image quality may be effected.

2.2.1.2 Discrete Fourier Transform (DFT) Techniques

Discrete Fourier Transform (DFT) is one another example of the 2D transforms. DFT translates the image matrix into range of high, medium and low factors. DFT is phase dependent and embeds watermark based phase characteristics hence, it is also resilient against rotation, noise, translation and scaling attacks. As proved by *Jimson* [48] it can give better robustness for watermark against above listed attacks. DFT comes with a cost of heavy calculations but a variant of DFT, Discrete Fractional Fourier Transform (DFRFT) can embed a watermark of larger sizes that other transforms like DCT and DFT both as it can compute additional two degrees.

Pun [47] uses DFT to embed watermark by choosing high frequency values for improved image quality and the similarity measure between resultant watermarked image and the host image, is used to detect the watermark. Another technique involves applying DFT [48] to 8x8 size image blocks and inserting a binary watermark based on relationship of the selected coefficients from each of the DFT transformed blocks. *Kaur et al.*[49] incorporates watermark in the image, by applying DFT. Even though the resultant watermarked image quality is good, this approach fails to perform against certain rotation, scaling and translation attacks. Another technique proposed which inserts the watermark in the image by manipulating the magnitude coefficients in the modified DFT image. The technique performs well against attacks such as rotation and cropping and is computationally efficient but does not perform well against blurring attacks.

2.2.1.3 Discrete Curvelet Transform Techniques

Even though wavelet domain based watermarking systems were used for quite some time, recent research shows that the traditional methods carried out for multi resolution representation of images is inaccurate, as it gives good results when used for one dimensional signals but when used for high dimensional forms the wavelet transform fails to provide an accurate representation of the image. To overcome this Curvelet based transforms were introduced, as they are able to represent the curves and edges of an image with accuracy. “Curvelet transforms” are implemented either by wrapping specially selected Fourier transforms known as FDCT-Wrapping, which is also computationally efficient than the second implementation known as “unequally spaced fast fourier transform” (USFFT).

Xu et al. [50] uses fast curvelet transform in his watermarking system, which applies FDCT on the original image to get transformed coefficients, Arnold scrambling is applied to the binary watermark for enhancing the watermark security and the resultant is incorporated into curvelet’s medium frequency values.

Gnanapriya [51] proposes chaotic watermarking to embed the watermark in the coarse image values, obtained through curvelet transform. The scheme also proposes using a genetic algorithm as an optimization technique to calculate the watermark strength for inserting in the image which improves the outcome of the watermarking scheme. The suggested technique does well against noise and rotation attacks but does not offer good results for attacks such as blurring.

Thanki et al. [52] uses DCT with Fast Discrete Curvelet Transform (FDCT) in his research where image is first transformed using FDCT, then the chosen sub-band is fragmented into various blocks and DCT is applied on all of them. A White Gaussian Noise random sequence is employed as a watermark which is first generated and then added to the original image. The scheme performs well under noise attacks such as sharpening and compression attacks but has poor values of watermarks against certain rotation, median filtering and blurring attacks. *Hien* *et al.* [53] incorporates a watermark comprising of a pseudo random sequence and applies curvelet transform on the original image. The generated watermark is added in the image based on threshold value. The technique shows good results against attacks such as compression but does not perform well against such as cropping.

A hybrid scheme is proposed by *Ramsha et al.* [1] which first applies applying “principal component analysis” on the image to obtain the sparse and low rank components and applies FDCT transform on the low rank component and uses SVD to create a watermarked image. Even though the scheme produces good quality images, it is computationally heavy and does not perform well against attacks such as blurring, median filtering and in many cases shearing attacks as well.

2.2.1.4 Walsh Hadamard Transform (WHT) Techniques

WHT is another example of two dimensional transform and produces a transformation matrix knows as hadamard ordered. Hadamard ordered matrix has pixels transformed and permutated in the growing order of frequency.

Meenakshi et al.[54], initially uses WHT on the original image to get 4 quadrants and then uses SVD on the highest frequency coefficients selected from all quadrants, to incorporate the watermark. This scheme though proves resilient for cropping and median filtering attacks but the results in case of noise attacks (e.g. Salt & Pepper) provide poor NC values. *Kalarikkal et al.* [55] uses “Code Division Multiple Access” method with WHT, converts the image into YUV format and then splits the image into block of 8x8 and applies WHT on all the blocks, the scheme is computationally efficient but the performance of scheme has not been studied against attacks such as “rotation and translation”. *Ishikawa et al.* [56] uses a combination of FWHT and DCT is applied to get accuracy in results. *Parvathavarthini* [57] incorporates the watermark by applying WHT and discusses the effect, the varying scaling factor has on the watermark embedded images but this technique has not been tested under attacks.

2.2.2 Watermarking Techniques using Wavelet Transforms

Wavelet transforms use convolution or lifting based methods for computation. Both of these method involve image decomposition into “low-pass” and “high-pass” sub band, with a half-sample of original image in each sub-band. The DWT works by transmitting the image through an analysis filter bank and sampling. After passing through a filter bank, the image gets divided into two sub-bands, one containing frame details and the second, coarse image data. The low-pass filter is able to extract the coarse information by performing averaging operation and high-pass filter enables extraction of image details by performing the difference operation. DWT is a lossless transform [12] and is tolerant to high localization scheme in both domains but is generally vulnerable to attacks such as noise and scaling and is computationally complex compared to DCT.

An example of DWT is presented by *Ali* [58] who applies Self-adaptive Differential Evolution (SDE) to adjust the input parameters of the watermark to be embedded. It applies DWT on the image and uses SVD to embed the embed the watermark along with the calculated inputs, but the proposed scheme is not only computationally expensive but also shows poor values of NC for noise attacks. *Al-Afandy et al.* [59], host image has DWT applied on to get the sub-bands and then embedding is done using the SVD algorithm. The drawback of this scheme is that the watermark size is dependent on the total number of pixels in an image based on capacity property. Also the scheme shows less robustness values against “geometric and transformation attacks”. *Makbol et al.* [60] uses DWT for dividing image into sub-bands and applies SVD for insertion of the watermark but the scheme shows poor quality of the extracted watermarks under filtering, rotation, noise and shearing attacks.

An alternate approach to increase robustness, involves insertion of the watermark by multiple applications of the transforms on the image as performed by *Tabassum and Barni et al.* [61, 62]. They apply a 3 level DWT on an image and select high frequency sub-band for adding the watermark. *Barni et al.* [62] introduce a method to embed a large capacity watermark but have relatively poor value of NC except in case of frame dropping attack because of the incorporation of the watermark in each frame. *Yadav et al.* [63] proposes application of 3 level DWT on an image and applies SVD to embed watermark in all the sub-bands in the resultant image. The recovered watermark from each sub-band is an average of the 4 sub-bands. This technique shows promising results for median filtering blurring and noise attacks, but does not carry our performance evaluation against rotation attacks.

Ghebleh et al. [64] employs chaotic maps with DWT and two copies of a binary watermark, in 2 selected sub-bands of the image, adopting two different methods, is embedded in the image. This is done in order to improve overall robustness of the embedded watermark. *Liu et* *al.* [65] uses watermark scrambling technique using logistics maps for security purposes and then incorporates into host image but this methodology again gives poor results for geometric attacks including shearing, translation and rotation. Even small rotations in host image can have a major impact on the PSNR and NC values both as they show poor values. *Keshavarzian* [66] the extracted watermarks have poor NC values and show poor quality.

2.2.2.1 Lifting wavelet transform (LWT)

DWT even though was used successfully for quite some time the scheme based on DWT are computationally heavy in terms of memory and hence a faster and more computationally efficient. *Verma* [67] and *Daubechies* [68] have proposed implementation of the original wavelet known as "lifting wavelet transform" ,which has been recently used in watermarking schemes. LWT like DWT provides image sub-bands with a low-low sub-band containing the approximation co-efficient matrix of the host signal and remaining bands (HL,LH & HH) containing detailed co-efficient matrix of the image.

Liu et al. [69] uses LWT, where a "PN-sequence generator" is used for generating random bits for watermark and inserts in two image sub-bands (LH & HL). But the scheme shows poor results under geometric attacks (scaling, cropping and rotation).

Loukhaoukha et al. [70] have proposed using an ant colony algorithm to calculate the optimized value of the strength with which the watermark is to be embedded, but the scheme does not use one scaling factor for whole image, instead based on varying intensities in the image, the scheme calculates multiple scaling factors of one image for the watermark. A binary watermark is generated and inserted into the LWT transformed image, the scheme shows performance evaluation against many attacks such as the noise attacks and compression, but uses a binary watermark of very small size, in addition the extracted watermark is not clear after attacks including median filtering and blurring and the scheme performs poorly against rotation and shearing attacks.

Kabra [71] applies 3 level LWT on image and divides the watermark image into distinct blocks of four. Every block is embedded in one of every high-low, high-high, low-low and low-high sub-bands of the LWT transformed image, by the application of SVD. This method proves effective for noise and cropping attacks but does not perform well against attacks such as blurring and median filtering.

2.2.2.2 Stationary Wavelet Transform (SWT)

SWT is used because it is less complex than the other transformation techniques, but has redundancy and hence unlike DWT the number of samples produced are same as the input signal, however it is efficient in noise removal and hence serves as a good option for better robustness as shown by *Nagarjuna et al.* [72].

Pandey et al. [73] presents converting the image in YCbCr color space and applies SWT to get the sub-bands for the resultant image. SVD is employed to incorporate the watermark. The paper also compares the results of varying values of PSNR and NC when the watermark strength factor is changed and shows good results against noise and compression attacks, but shows poor NC values even against the smallest rotation angles and doesn't study any geometric attacks. *Nagarjuna et al.* [72] proposes a similar technique where SWT and spread spectrum algorithm is employed for embedding the watermark in low-low sub-band. Proposed technique again uses very low grade values for the attacks, in most cases performs poorly against considered attacks and does not evaluate performance for geometric attacks (translation and scaling).

2.2.3 Watermarking Techniques using Contourlet Transforms

Contourlet transform can take into account the edges of smooth objects in the images, lately many variants have been proposed which try to overcome the inherent issues in the original contourlet transform such as the "sharp frequency localized contourlet transform" (SFLCT) as shown by *Lu* [74].

A technique [75] using Contourlet Transform (CT) and Principal Component Analysis (PCA) is proposed where contourlet transform is implemented on an image. Watermark strength is calculated using Noise Visibility Function (NVF) and is embedded into contourlet transformed coefficients obtained from the image. This technique proves efficient against image processing attacks but security wise, the scheme is weak as it uses no encryption for confidentiality of the watermark.

Najafi [76] employs a watermarking strategy using Sharp Frequency Localized Contourlet Transform (SFLCT) where the watermark and the image are of the same size, and SFLCT is implemented on the watermark and the image. Proposed scheme proves effective towards many attacks including the geometric and image processing attacks.

Ranjbar et al. [77] applies an alternate method of embedding using the CT transform is proposed in which a two-stage dual watermarking approach is taken, in the first stage CT is used to transform the image and watermark is applied to the selected low frequency coefficients in the image. Next, the watermark is applied to the high frequency values again. The scheme performs well against many attacks but does not perform well against attacks such as median filtering.

2.2.4 Watermarking Techniques using Deep Learning Algorithms

Recently machine learning and deep learning algorithms have been introduced to add and extract the watermark. Mostly these methods proceed by converting the image into small blocks and learning the relationship of one pixel with its neighboring pixels. The techniques are usually effective against attacks but the main issue with them is that they take computation power and time to train the classifier on the test images. Classifiers such as *Support-Vector Machine* (SVM), *least square* as shown by *Wang et al.* [78], *Random Forests* and most recently extreme learning machines. Another application of machine learning algorithms is that they are used for enhancing watermark's strength by determining optimal values for achieving balance between its transparency and effectiveness [12].

Islam et al. [79] applies 3 level *Lifting Wavelet Transform* (LWT) on the image for embedding a binary watermark in the image. Watermark bits are added depending on the relation of largest coefficients in the LWT transformed image. The scheme integrates the watermark into nine different image sub-bands and extracts using Support Vector Machines (SVM). This technique compares embedding results in all the sub-bands of image with individual sub-bands and concludes that the high low sub-band of 3 level LWT produces best results in almost all attacks. In using an extreme learning machine for watermarking, a scheme has been introduced by *Dabas* [80], where *Integer Wavelet Transform* (IWT) is applied to the image, which provides a high low sub-band in return. Further, 4x4 blocks of the selected sub-band are created, and SVD is applied and using cox's formula watermark is added in the image. The scheme compares results on two extreme learning machines *Kernel based Extreme Learning Machine* (KELM) and *Reduced Kernel Extreme Learning Machine* (RKELM). Results of quality analysis of both are compared against various attacks, but the scheme performs well under only a small degree of rotations and does not consider attacks such as scaling.

Mehta et al. [81] uses *Lifting Wavelet Transform* (LWT), selects the low-low sub-band and adds watermark using the *QR factorization*. Watermark is also jumbled using the arnold transform for the purpose of the security. The scheme uses *Lagrangian Support Vector Machine* (L-SVM) for extraction of watermark. The scheme performs well against many attacks but does not perform well against attacks such as shearing, and considers attacks against very low degree of rotations.

2.2.5 Watermarking using Hybrid Techniques

A lot of studies have also been carried out by combining previously described techniques to achieve better values of robustness and lower error rates these combined scheme are called as hybrid domain watermarking schemes. The main issue with these schemes is that they are computational heavy and they include increased complexity.

Thind et al. [82] first uses DWT, transforms the image, followed by application of SVD for adding the watermark in the chosen HH sub-band. *Ganic et al.* [83] uses a hybrid scheme in which watermark is inserted in all sub-bands for attaining higher efficiency.

Agarwal et al. [84] use IWT with a combination of DCT to add the watermark, where original image goes under the application of a 3 level IWT. From there on, frequency coefficients are obtained for the selected 3 level HH sub-band by the application of DCT. Watermark is transformed into a binary sequence and then added by changing values of the frequency coefficients matrix based on the watermark bits. The scheme shows good PSNR and NC values but does not study the performance of the scheme under attacks.

Garg et al. [39] employs both *Discrete Stationary Wavelet Transform* (DSWT) and *Discrete Cosine Transform* (DCT) for incorporating a colored watermark into the original image. First the image and the watermark both are broken down into the RGB components and then arnold scrambling is applied on image's color components for security. DSWT is applied on all three channels of the watermark. Next, the watermark and the image undergo the application of DCT on the LL sub-band. Finally information is embedded into the image using SVD. This technique shows good results against various attacks but against very low values such as noise attacks.

Hamidi et al. [85] employs *Arnold Scrambling* and a hybrid of DCT and DFT for watermark security. This method delivers good results for image processing attacks (e.g. median filtering) and for small values of noise attacks (salt & pepper), whereas does not consider rotation, shearing (geometric) attacks.

2.2.6 Geometric correction based Techniques

Recently there has been some work done on techniques which aim to correct the image based on some learning algorithm and before extraction of the watermark geometric correction is done so that high robustness results can be achieved.

Hernandez et al. [86] proposes DFT to insert the watermark and for performing geometric correction, *Speeded up Robust Features* (SURF) technique is employed which learns the image features, and uses them for further calculations. Once an attacked image is received these feature points are gain calculated using SURF and are compared to correct the distortions in the image. However, the discussed technique shows poor results against many attacks such as blurring and Gaussian noise attacks.

Yang et al. [87], employs FSVM for geometric corrections and *Discrete Wavelet Transform* (UDWT) to create image sub-band. This method performs well but is computationally complex.

2.3 Threat Models for Watermarking Schemes

During its lifecycle, a watermarked signal will potentially be prone to various malicious threats/attacks including Geometric attacks, Gaussian noise, filtering etc., non-malicious attacks or natural degradations such as packet loss which may affect the watermark in different ways. Attacks on digital watermarks [12] are classified as:

2.3.1 Legitimate Threats

Natural degradations can be categorized into two types, based on nature first is physical causes and second is transmission over the network.

2.3.1.1 Physical causes

Natural degradations occur when a signal is subject to external effects that may cause watermark to be hard to detect such as additive white Gaussian noise which is due to the noise present during transmission and cause modifications in the watermark.

2.3.1.2 Network causes

When a signal is transmitted over the network it might be subject to one of the following:

Packet Loss

Due to issues such as buffer full at the receiver's end, packet losses may occur and are usually handled by network protocols by means of retransmission of packet, but if the watermarking scheme is reliant on time for embedding, this could translate into means for an attacker intentionally trying to keep from watermark extraction or destroy it.

Compression

Over network compression is a very useful property and usually signals are compressed to achieve speed, but if the compression is lossy it may lose the bits which have watermark embedded and affect the quality of the watermark.

2.3.2 Malicious Threats

Malicious threats are carried out by an attacker with an intention of removing the watermark from the host signal and can be categorized as one of the following:

2.3.2.1 Oracle attack

In this attack the attacker relies on an oracle [88] which can distinguish between a watermarked signal and a plain signal. The attacker starts by making small modifications in the signal until finally the oracle is unable to distinguish the watermarked signal. These attacks are mostly combined with machine learning algorithms [89] to improve efficiency by improving sensitivity.

2.3.2.2 Removal attacks

Removal attacks are the most common types of attacks that are carried out on watermarks. Such attacks abolish the embedded watermark in the signal such that it is impossible to retrieve. They often work in phases where a watermark might be estimated [89, 90] first and then removed.

2.3.2.3 Distortion attack

Distortion attacks include linear filter, noise and geometric attacks which may cause damage to the watermark so it cannot be extracted from the host signal

2.3.2.4 Cryptographic attacks

The secret information that has been embedded in the host signal may be compromised by such attacks [91]. They work by gathering information on the algorithm of the watermark scheme. Since this is such a powerful attack it gives the attacker power to embed a new watermark or delete the embedded watermark. Luckily these require high computational power and are expensive hence are not that common.

2.3.2.5 Geometric Attacks

Geometric attacks which aim for breaking the synch between the original and watermarked data. An example could be a rotation attack, where even a few degrees of rotation are enough to break the sync between the host signal and the resultant image rendering the receiver unable to detect the watermark.

2.4 Performance Evaluation and Quantitative Measures

The system of watermarks should ideally not only be imperceptible [92, 93] and should not aim to calculate the quality, but also be robust, measuring the similarity of the watermarks, against various attacks of signal processing such as compression, shearing, rotation, translation etc. PSNR and NC are the quantitative methods employed to calculate and compare to an established reliable watermarking [1] technique with the suggested watermarking technique.

2.4.1 Peak-Signal-to-Noise-Ratio (PSNR)

In decibel (db), the PSNR measured is the metric for calculating the strength of the host signal against the watermarked signal. Higher "PSNR" values are an indication of better image quality and therefore a good watermarking technology. Firstly a "mean square error (MSE)" is computed to calculate PSNR [1], a square error calculation between the host image and the resultant image. The lesser value of which shows a lower error and therefore better PSNR value. The "PSNR" and the "MSE" are inversely related to each other. MSE is calculated using the equation given below, in which I, WI, P and R represents the host image, the resultant image with watermark, total rows in the images and the total columns in the image respectively:

$$MSE = \frac{1}{PR}\sum_{p=0}^{P}\sum_{r=0}^{R}\left(I(p,r) - WI(p,r)\right)^2$$

$$PSNR = 10\log_{10}\frac{M^2}{MSE}$$

Where, M is a representation of possible values in an image, which is 255 when a 8-bit unsigned representation is used and 1 in case of floating point representation. PSNR for colored images is calculated by getting the color spaces of the original image and using the luminance channel for calculation of PSNR for example in the suggested technique YCbCr color space is used, hence PSNR is calculated on the “luma channel” Y.

2.4.2 Normalized Correlation (NC)

This property measures how identical is the removed watermark to the watermark that was added initially in the image [1]. This ranges between [-1 1] and values closer to one are considered more accurate. Usually NC values of 0.7 are considered good. NC is found using the equation given below, where W_1 and W_2 are the “original” and the “removed watermark” respectively:

$$NC = \frac{\sum_{p=1}^{P}\sum_{r=1}^{R}\left(W(p,r) \times \breve{W}(p,r)\right)}{\sum_{p=1}^{P}\sum_{r=1}^{R}\left(W(p,r)\right)^2}$$

Details of contrast of results of the suggested technique with the current technique [1] are presented in chapter 4 in the thesis.

Chapter 3

PROPOSED METHODOLOGY OF ATTACK RESISTANT WATERMARKING IN LIFTING WAVELET DOMAIN

3.1 Proposed Watermarking Technique

The suggested method is of using three techniques “lifting wavelet transform (LWT)”, “schur decomposition (SD)” and “singular value decomposition (SVD)”. The image to be used as watermark is rendered meaningless using “arnold transformation” which serves the purpose of improving the security and robustness. The scheme takes a colored image Io as input, and for the watermark a grey-scale image is used. The image is translated into “YCbCr color space”, lifting wavelet transform gives the sub-bands of the image, schur decomposition is applied on the certain sub-band and finally SVD is used to add the watermark in the image.

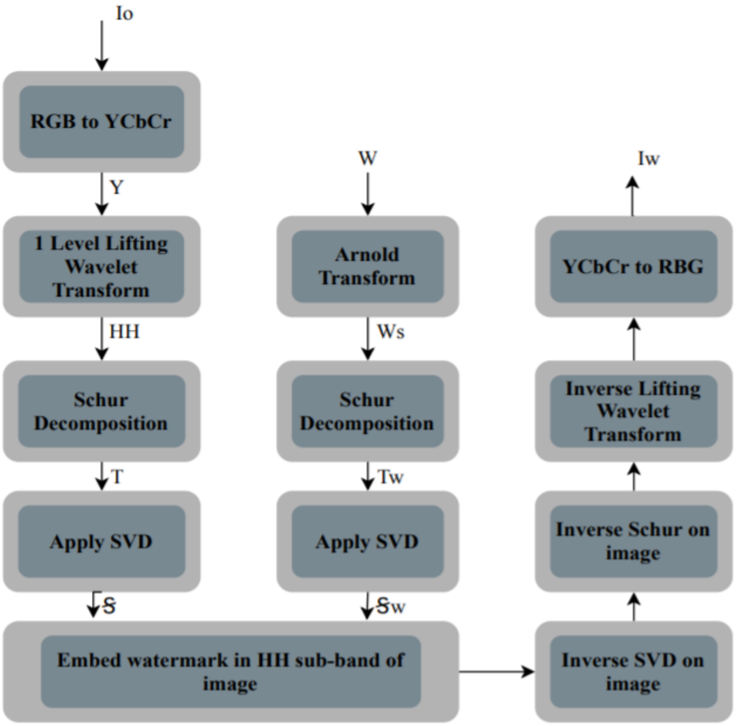


Figure 3.1 Steps for inserting the watermark

The framework of the suggested “attack resistant image watermarking technique” is given above, figure 3.1 shows embedding process followed for the watermark and figure 3.2 shows the process followed for removal.

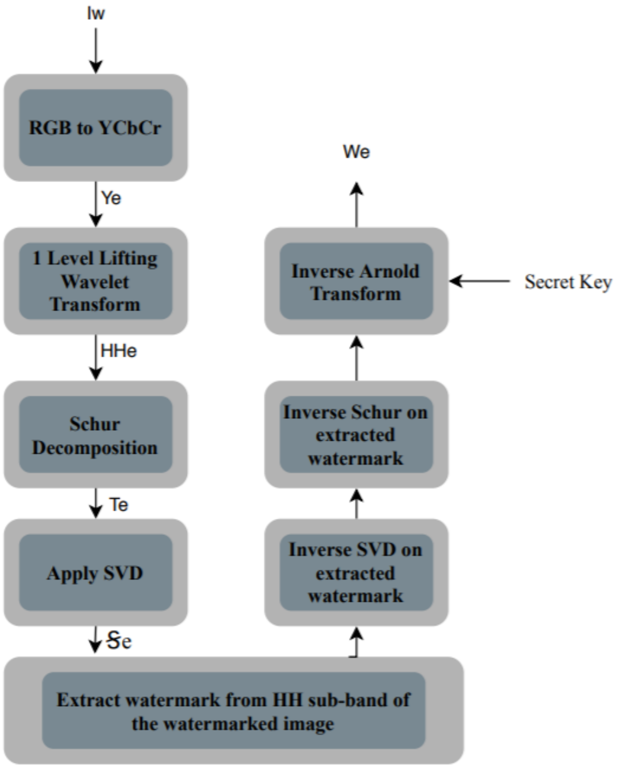

Iw
RGB to YCbCr
Ye
1 Level Lifting Wavelet Transform
HHe
Schur Decomposition
Te
Apply SVD
Se
Extract watermark from HH sub-band of the watermarked image
Inverse SVD on extracted watermark
Inverse Schur on extracted watermark
Inverse Arnold Transform
Secret Key
We

Figure 3.2 Steps for removal of watermark

Moreover, the experimental results are evaluated both graphically and quantitatively to show that the proposed technique under various attacks including noising attacks (salt & pepper, multiplicative etc.), geometric attacks (crop, translation, projection etc.), image processing attacks (histogram equalization, Gaussian smoothing, contrast enhancement etc) shows good imperceptibility and robustness and thus, verify that the suggested technique is better in comparison to the existing technique based on FCT [1].

3.1.1 Watermark Embedding

For the below process, let I and W be the colored host and “gray-scale” watermark image. The image with dimensions R×C×B is used, where r (r=1, 2 … R) represents the rows of image, c (c=1, 2 … C) represents the total columns of the image and b represents the bands of the original host image, with values ranging from 1 to 3 respectively. The watermark of size MxN is used where m are the rows and n are the columns of the image used as watermark respectively. In the first step the host image I is converted into a different color space so that watermark information may be embedded in the "luma" component i.e,

$$(Y_I, Cb_I, Cr_I) \xleftarrow{RGB\ to\ YCbCr} I \tag{4.1}$$

where Y_I is the "luma component". 1 level LWT is applied on Y_I to transform the image into low-low (LL), low-high (LH), high-low (HL) and high-high (HH) sub-bands.

$$Y_I = LL_i+LH_i+HL_i+HH_i \tag{4.2}$$

the LL_i is the approximation coefficients matrix whereas LH_i, HL_i and HH_i are the details coefficients matrix of the image [68]. The watermark W is jumbled using the "arnold transform".

$$\begin{matrix} m' \\ n' \end{matrix} = \begin{bmatrix} 1 & 1 \\ S & S+1 \end{bmatrix}^i \begin{matrix} m \\ n \end{matrix} \quad (\text{Mod } M) \tag{4.3}$$

where S illustrates the secret key, total number of repetitions is denoted by i , m' and n' are coordinates of the resultant watermark and dimensions of the watermark is represented by M. Schur decomposition is used on the sub-band HH_i of the image to decompose it into two matrices.

$$HH_i= U_i T_i \tag{4.4}$$

where U_i represents the unitary matrix and T_i is the upper triangular matrix [94]. SVD is applied on T_i again so that watermark can be added in the singular value matrix.

$$T_{i=} \theta_i \mathcal{S}_i \psi_i \tag{4.5}$$

where $\mathcal{S}_i$ is the singular values "diagonal matrix". For the next step schur and then SVD decomposition are used respectively on the jumbled watermark W' as well.

$$W'= U_w T_w \tag{4.6}$$

where U_w is the unitary matrix and T_w is the upper triangular matrix. SVD is applied on T_w

$$T_{w=} \theta_w \mathcal{S}_w \psi_w \tag{4.7}$$

where $\mathcal{S}_w$ is the diagonal matrix. The resultant matrix can be obtained by adding the singular vector matrices $\mathcal{S}_w$ and $\mathcal{S}_i$ of the image where α is the strength of the watermark which has a range of 0 to 1. The values closer to 1 provide better robustness and closer to zero provide better imperceptibility.

$$\mathcal{S} = \mathcal{S}_i + \alpha \mathcal{S}_w \qquad (4.8)$$

The modified *Ti'* is found by applying inverse

$$T_i' = \theta_i \mathcal{S} \psi_i \qquad (4.9)$$

inverse schur is used to get the modified high-high sub-band, and inverse lifting wavelet transform is used to get the image which is watermarked. Figure 3.3 shows the intermediate steps and image representation after each operation, as discussed in the above steps till we get the “watermarked image”. The results discussed in chapter 4 show comparison between the input and output watermark image for simplicity purposes.

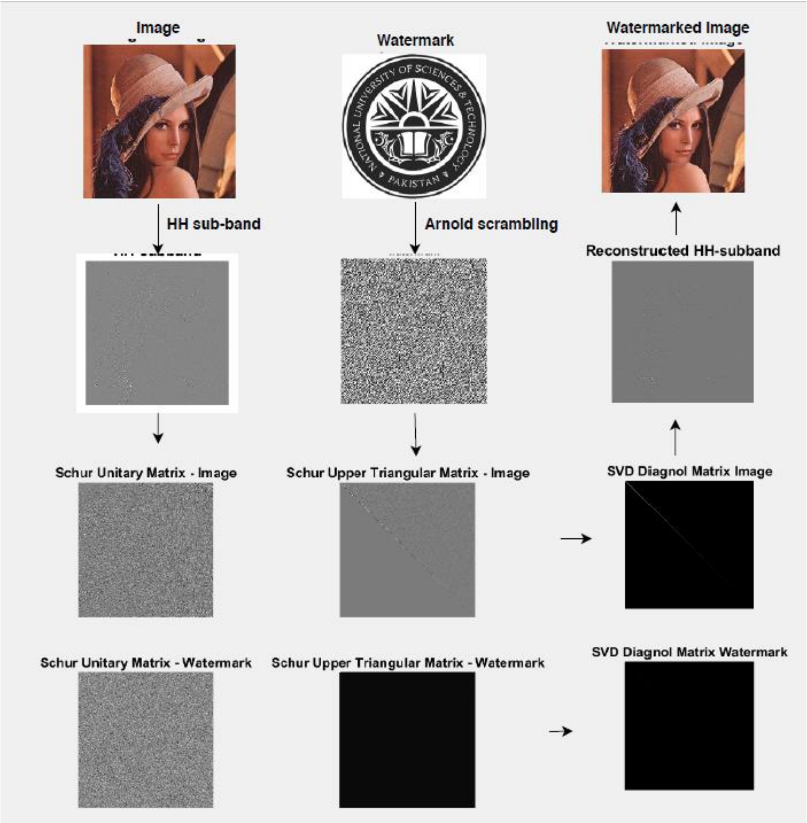


Image
Watermark
Watermarked Image
NATIONAL UNIVERSITY OF SCIENCES & TECHNOLOGY
PAKISTAN
HH sub-band
Arnold scrambling
Reconstructed HH-subband
Schur Unitary Matrix - Image
Schur Upper Triangular Matrix - Image
SVD Diagnol Matrix Image
Schur Unitary Matrix - Watermark
Schur Upper Triangular Matrix - Watermark
SVD Diagnol Matrix Watermark

Figure 3.3 Intermediate steps for watermark embedding

3.1.2 Watermark Extraction

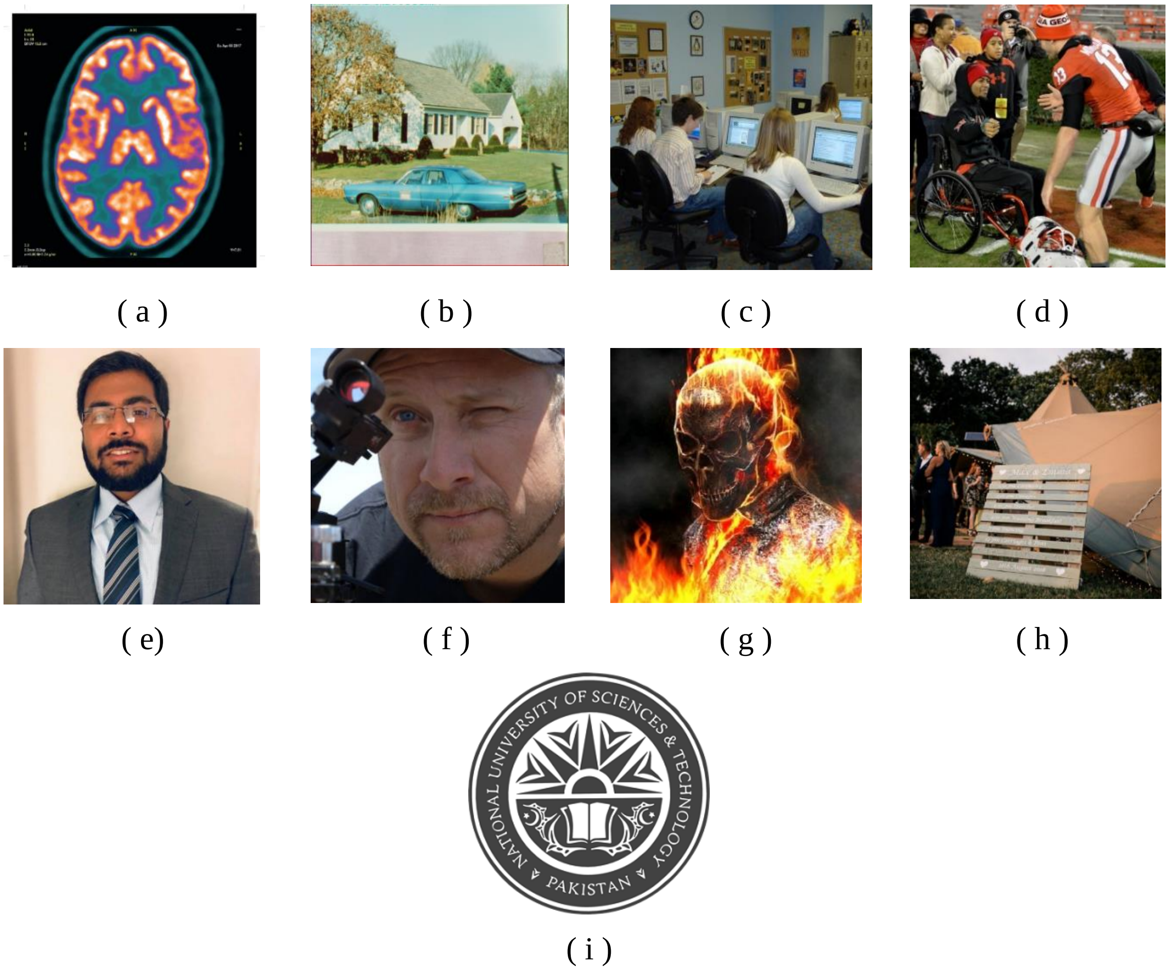
The removal of the watermark can be done by reversing the steps mentioned above in section 3.1.1. However for successful retrieval at the receiver’s end, the original image, watermark and the key should be known.

Chapter 4

RESULTS

4.1 Experimental Results

Cover images of dimensions 512x512 and a watermark logo with dimensions 256x256 are used for checking the execution of the suggested scheme for watermarking. Few colored images from the manual data set and grey-scale watermark used are as shown in figure. 4.1.



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

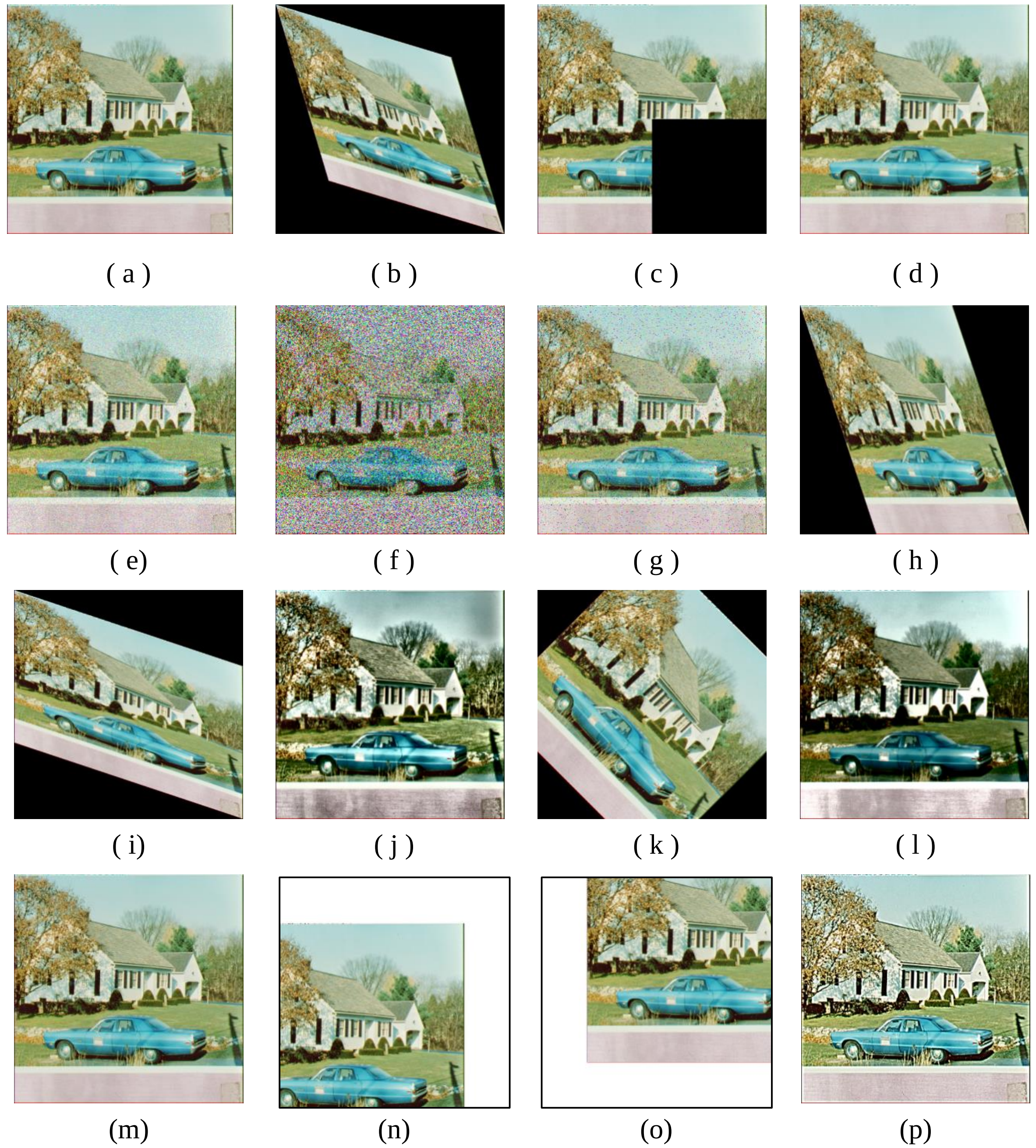
(e) (f) (g) (h)

(i)

Figure 4.1Test color images (512 x 512) and watermark (256 x 256) used, (a) brain (b) house (c) computers (d) wheelchair (e) man (f) sniper (g) man on fire (h) tent (i) watermark (logo).

Watermark strength (α) with a factor of 0.05 was selected for insertion of the watermark as it was observed by the visual quality of the resultant watermark and the image that the value of 0.05 works best under different attacks than any value less than 0.1.

The proposed technique is compared with existing "FCT-RPCA-SVD" based technique proposed by Ramsha et al. [1], the "DWT –SVD" based technique by Gupta and Raval [2] and the "DWT-HD-SVD" technique proposed by J. Liu et al. [3] under various attacks including noising attacks (salt & pepper, multiplicative etc.), geometric attacks (crop, translation, projection etc.), image processing attacks (histogram equalization, gaussian smoothing, contrast enhancement etc) so that the performance of the suggested scheme can be evaluated. Figure 4.2 illustrates the image "House" under different attacks, figure (a) shows image under no attack, figure (b) shows image under affine attack, figure (c) shows image under cropping attack, figure (d) shows image under gaussian smoothing attack, figure (e) shows image under gaussian noise attack, figure (f) shows image under speckle noise attack, figure (g) shows image under salt and pepper attack, figure (h) shows image under X-shearing attack, figure (i) shows image under Y-shearing attack, figure (j) shows image under contrast enhancement attack, figure (k) shows image under rotation attack, figure (l) shows image under histogram equalization attack, figure (m) shows image under jpeg compression attack, figure (n) shows image under translation attack [-100,100], figure (o) shows image under translation attack [100, -100] and figure (p) shows image under sharpening attack.



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

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

(i) (j) (k) (l)

(m) (n) (o) (p)

Figure 4.2 The image "House" under different image attacks

4.1.1.1 Qualitative Comparison of Suggested Watermarking Technique with Other Techniques under Attacks

Figure 4.3, 4.4, 4.5 and 4.6 show the watermarks extracted from image “House” under different categories of attacks. Figure.(a) illustrates the watermarks obtained under different attacks using the scheme proposed by Ramsha et al. [1] figure.(b) illustrates the watermarks obtained under different attacks using the scheme proposed by Gupta and Raval and figure.(c) illustrates the watermarks obtained under different attacks using the scheme proposed by J. Liu et al. [3]. The qualitative analysis show that the proposed scheme out performs the results of the previous schemes under various attacks as illustrated by the visual quality of the extracted watermarks.

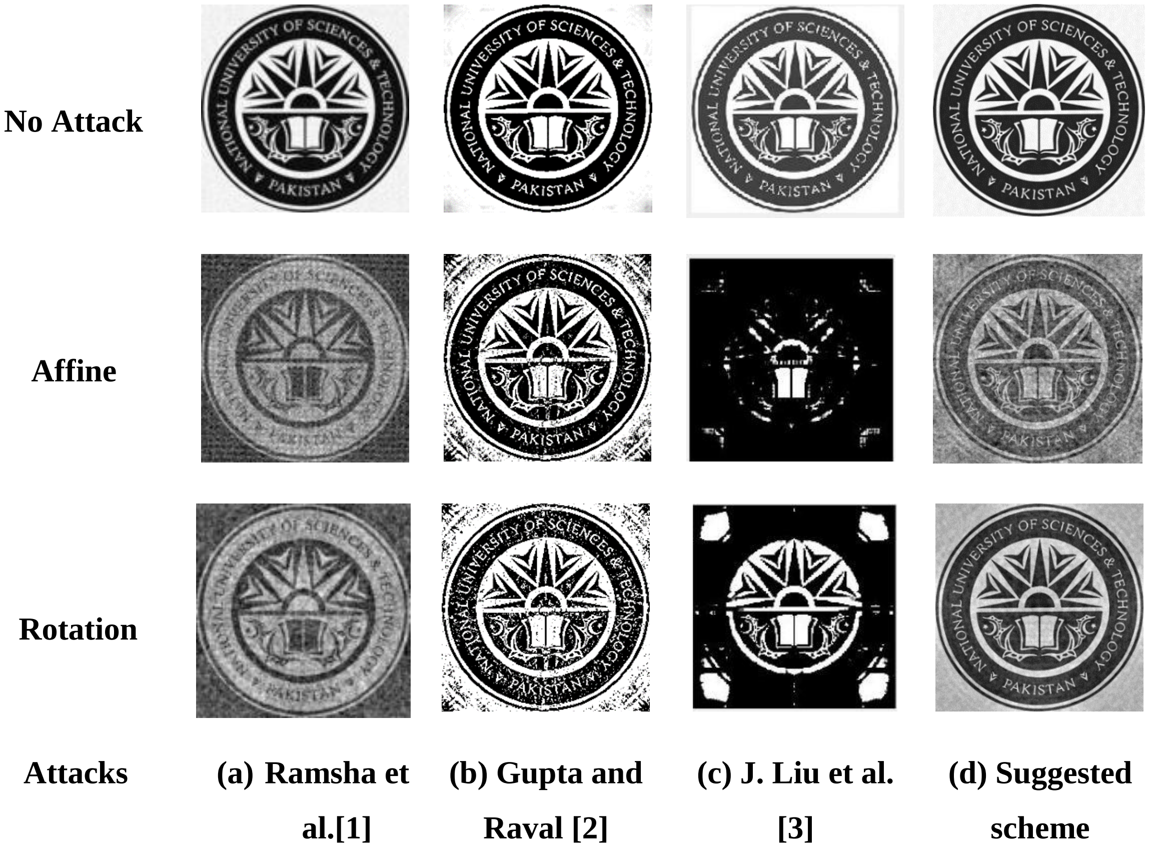


Figure 4.3 Watermark comparison of the proposed technique with Ramsha et al. [1], Gupata and Raval [2] and J. Liu et al. [3] under affine, rotation and no attack.

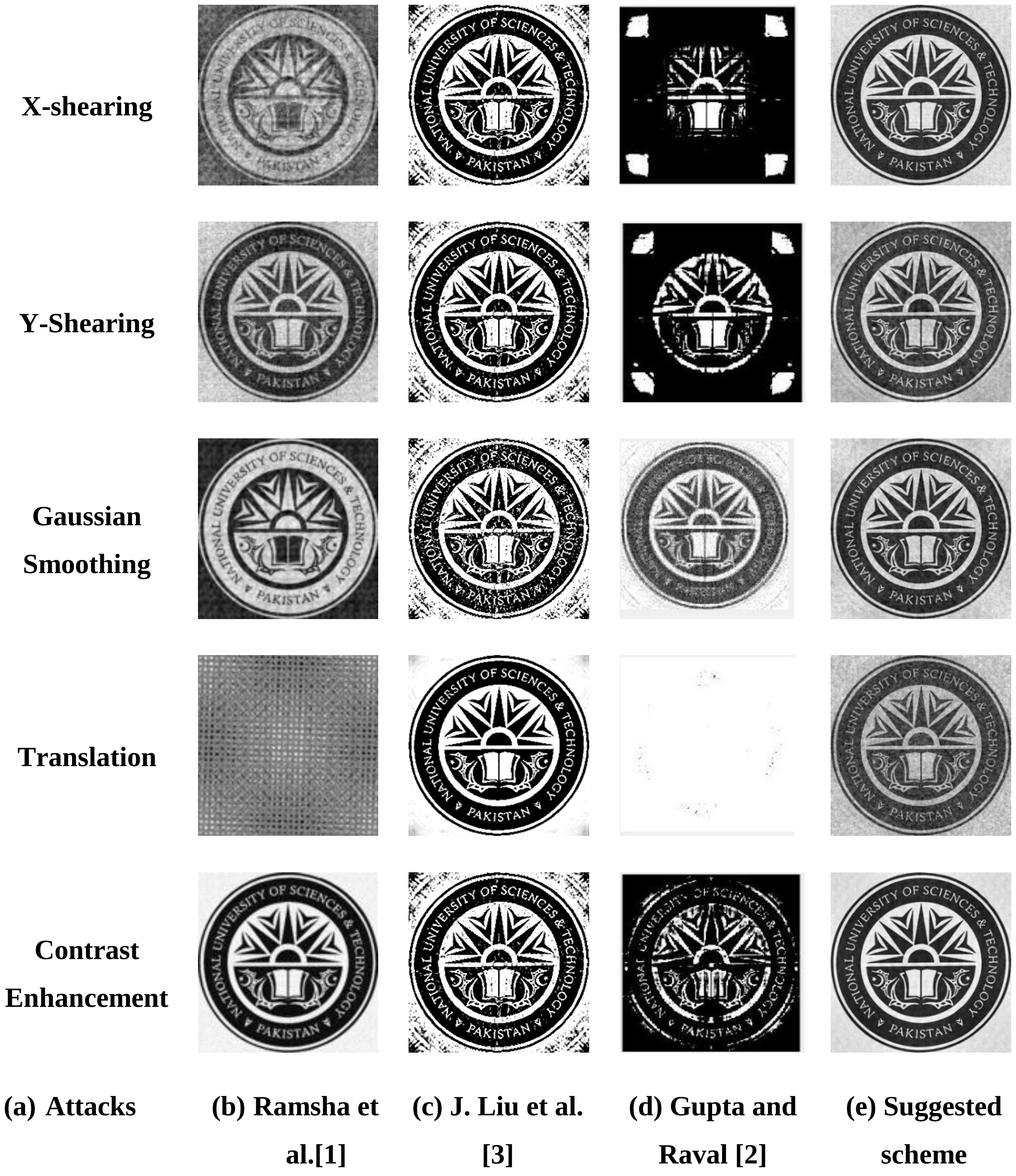
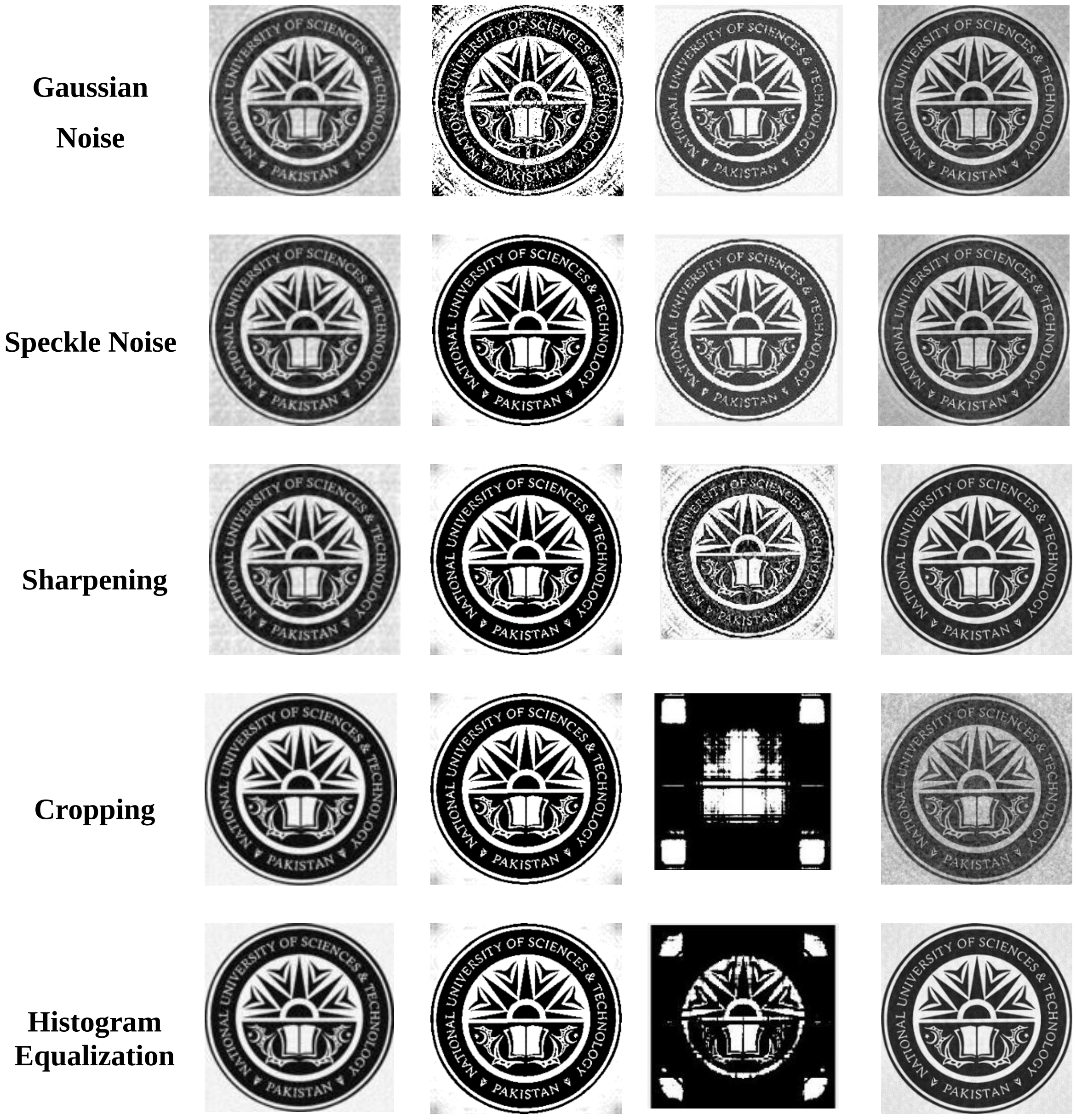


Figure 4.4 Watermark comparison of the proposed technique with Ramsha et al. [1], Gupata and Raval [2] and J. Liu et al. [3] under x-shear, y-shear, gaussian smoothing, translation, contrast enhancement attacks.



(a) Attacks **(b) Ramsha et al.[1]** **(c) J. Liu et al. [3]** **(d) Gupta and Raval [2]** **(e) Suggested scheme**

Figure 4.5 Watermark comparison of the proposed technique with Ramsha et al. [1], Gupata and Raval [2] and J. Liu et al. [3] under gaussian noise, speckle noise, sharpening, copping and histogram equalization attacks.

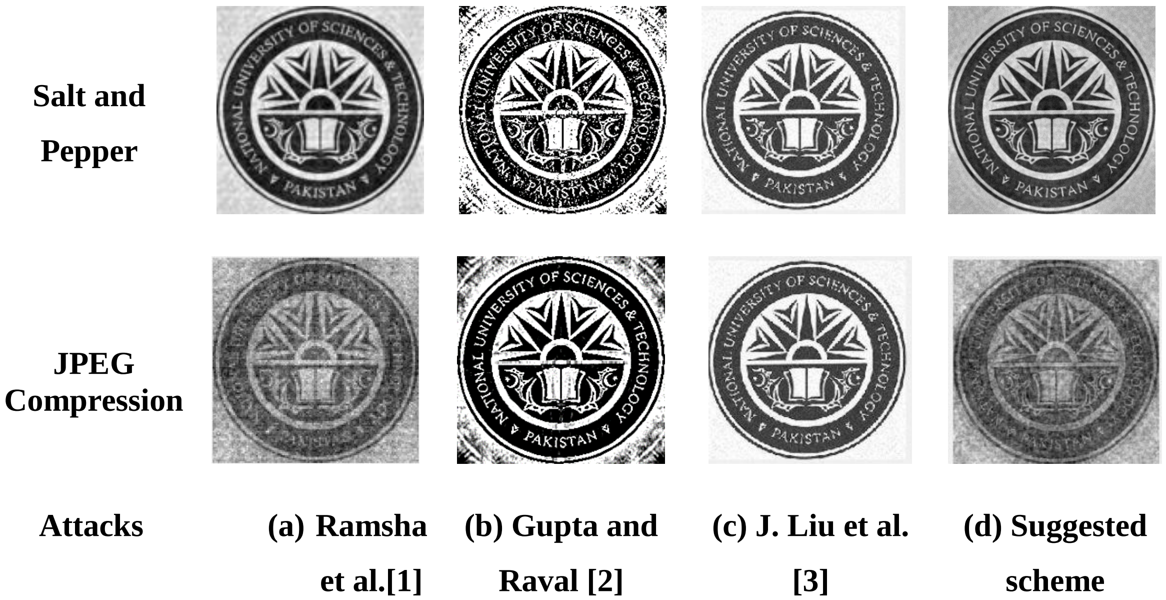


Figure 4.6 Watermark comparison of the proposed technique with Ramsha et al. [1], Gupata and Raval [2] and J. Liu et al. [3] under salt and pepper and jpeg compression attack.

4.1.1.2 Qualitative Comparison of Suggested Watermarking Technique with FCT Based Technique under Attacks

In carrying out the analysis the results were inserted in all sub-bands (low-low, low-high, high-low, high-high) of the image and based on the comparison HL band was chosen as it had the best NC values against all attacks. It was also observed that in attacks like blurring and affine transformation attack, the LL band produced good NC values, whereas in attacks like rotation, translation and shearing HH band had better NC values. Table 4.1 and 4.2 show the NC values of all sub-bands obtained for the watermarked images (brain, house, computers, wheelchair, man, sniper, man on fire, tent) against all attacks.

Table 4.1Average NC value comparison of all watermark images against translation, affine, rotation, X-shear, Y-shear and gaussian smoothing attacks in all sub-bands.

Attacks	**Sub-band**			
	LL	**LH**	**HL**	**HH**
Translation Attack	0.813663	-0.88721	-0.93715	0.895963
Affine Attack	0.3811	0.514342	0.212718	0.884104
Rotation Attack	0.655404	0.859796	0.831314	0.978991
X-shearing Attack	0.378386	0.861399	0.870404	0.954785
Y-shearing Attack	0.363805	0.63431	0.619033	0.959876
Gaussian Smoothing Attack	0.800884	0.958335	0.919639	0.930948

Table 4.1 displays the average values of NC for 8 images shown in Figure 4.2, against a few attacks showing why HH band was chosen for embedding the watermark. It was observed over a set of over 25 images that NC value of HH band is more “robust” than any other band against most geometric attacks including affine attack, also the image imperceptibility was best when watermark was embedded in HH band instead of the HL band, hence the HH sub-band was chosen for embedding the watermark.

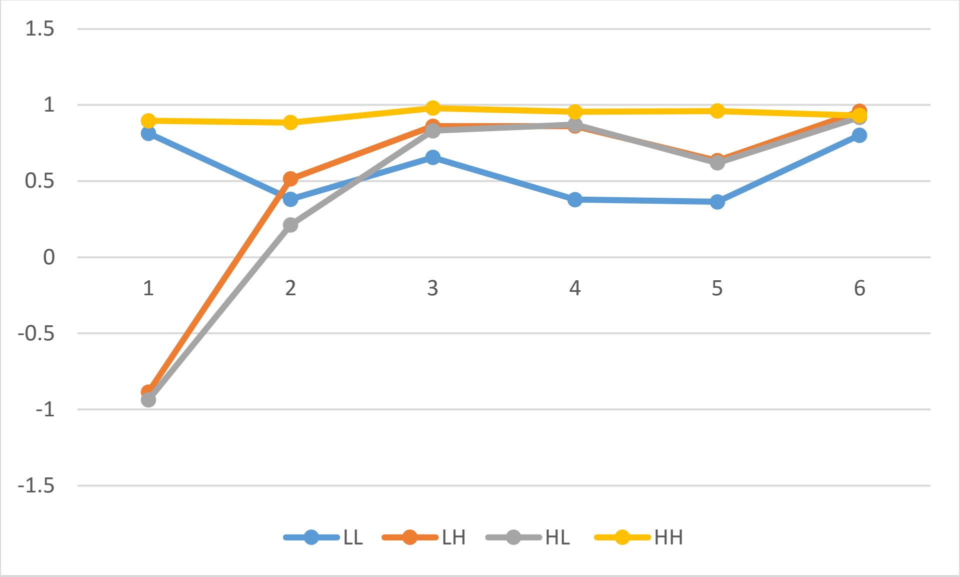


Figure 4.7 illustrates the graph of average calculated values of NC for 8 images against 6 attacks where 1 is translation, 2 is affine 3 is rotation, 4 is X shearing 5 is Y shearing and 6 is gaussian smoothing attack. The graph also clearly illustrates how HH band gives values close to 1 in all cases.

Table 4.2, 4.3 and 4.4 give the quantitative comparison of suggested technique with the Ramsha et al. [1], Gupata and Raval [2] and J. Liu et al. [3] when the watermarked test images have gone under various geometric, noise and cropping attacks to compare the imperceptibility via PSNR values. The values obtained in each case clearly show that the suggested technique provides good PSNR values.

Table 4.2 Quantitative comparison of all watermark images against no attack, translation, salt and pepper, gaussian noise and speckle noise attacks (PSNR values)

Test Image	**Scheme**	**No Attack**	**Translation Attack**	**Salt and Pepper**	**Gaussian Noise**	**Speckle Noise**
Brain	J. Liu et al. [3]	49.9431	4.176	33.2733	31.2322	37.3544
	Gupta and Raval [2]	20.0199	7.3308	14.9028	14.836	12.891
	R. Ahmed et al. [1]	11.27	7.6764	14.407	12.219	13.318
	Proposed	**69.84**	**57.348**	**62.821**	**61.926**	**64.403**
House	J. Liu et al. [3]	47.8705	10.2017	35.263	29.0832	33.0222
	Gupta and Raval [2]	22.2229	16.295	14.954	14.823	13.765
	R. Ahmed et al. [1]	28.49	7.6717	18.927	16.697	18.828
	Proposed	**81.3**	**60.306**	**63.885**	**63.865**	**64.967**
Computers	J. Liu et al. [3]	47.5948	6.8744	35.2378	30.0889	37.2321
	Gupta and Raval [2]	21.8928	21.37	14.9301	14.633	13.8472
	R. Ahmed et al. [1]	23.99	7.6775	17.948	14.125	17.993
	Proposed	**76.17**	**61.593**	**64.804**	**64.751**	**66.099**
Wheelchair	J. Liu et al. [3]	47.3664	6.1437	34.544	30.278	36.8281
	Gupta and Raval [2]	21.9559	13.354	13.0173	13.786	12.4145
	R. Ahmed et al. [1]	23.22	7.6796	19.752	16.258	19.322
	Proposed	**83.35**	**58.328**	**64.099**	**63.867**	**65.757**

Table 4.3 Quantitative comparison of all watermark images against affine, sharpening, rotation, x-shearing and y-shearing attacks (PSNR values)

Test Image	**Scheme**	**Affine Attack**	**Sharpening Attack**	**Rotation**	**X-shear**	**Y-shear**
Brain	J. Liu et al. [3]	6.4333	34.6445	6.3122	7.2323	8.2231
	Gupta and Raval [2]	14.9028	9.2837	12.4073	14.0971	14.5738
	R. Ahmed et al. [1]	8.1459	10.579	8.0181	7.5043	7.7085
	Proposed	**57.497**	**63.81**	**60.161**	**58.469**	**59.105**
House	J. Liu et al. [3]	5.542	31.2332	8.23232	11.123	6.2212
	Gupta and Raval [2]	13.205	9.1233	14.7966	15.1221	14.5738
	R. Ahmed et al. [1]	4.705	21.479	4.5806	4.6185	14.983
	Proposed	**58.822**	**70.952**	**63.936**	**68.271**	**63.293**
Computers	J. Liu et al. [3]	10.2323	33.231	10.2322	11.223	11.2281
	Gupta and Raval [2]	14.335	10.343	13.0293	14.011	14.6712
	R. Ahmed et al. [1]	7.3244	14.231	4.5438	8.1655	9.7171
	Proposed	**64.668**	**72.542**	**66.154**	**66.764**	**63.993**
Wheelchair	J. Liu et al. [3]	8.542	31.5171	8.6222	9.5223	8.9018
	Gupta and Raval [2]	13.3915	9.0191	12.0293	14.2124	14.0817
	R. Ahmed et al. [1]	7.6995	18.775	2.5292	11.477	13.082
	Proposed	**59.558**	**71.426**	**64.059**	**59.769**	**64.633**

Table 4.4 Quantitative comparison of all watermark images against, gaussian smoothing cropping, histogram equalization and contrast enhancement attacks (PSNR values)

Test Image	**Scheme**	**Gsmooth Attack**	**Cropping Attack**	**Histogram Eq. Attack**	**Contrast Ench Attack**
Brain	J. Liu et al. [3]	37.323	12.1221	13.928	21.3233
	Gupta and Raval [2]	14.112	19.887	13.5653	17.7237
	R. Ahmed et al. [1]	5.6437	11.302	11.279	11.279
	Proposed	**57.231**	**65.036**	**66.648**	**60.939**
House	J. Liu et al. [3]	38.2121	9.3122	14.6783	16.333
	Gupta and Raval [2]	14.2212	14.2857	14.6599	14.6987
	R. Ahmed et al. [1]	2.9327	28.647	28.498	28.498
	Proposed	**66.192**	**62.509**	**73.323**	**71.044**
Computers	J. Liu et al. [3]	39.2321	12.2123	15.2722	15.3433
	Gupta and Raval [2]	14.001	14.2928	14.5653	14.696
	R. Ahmed et al. [1]	4.8825	24.063	23.994	23.994
	Proposed	**68.148**	**61.901**	**74.264**	**70.579**
Wheelchair	J. Liu et al. [3]	38.4345	10.231	16.3846	14.3433
	Gupta and Raval [2]	14.112	19.786	13.5661	17.5541
	R. Ahmed et al. [1]	4.0611	24.025	23.22	23.22
	Proposed	**62.155**	**66.711**	**74.876**	**72.636**

Table 4.5 Quantitative comparison of all watermark images against no attack, translation, salt and pepper, gaussian noise and speckle noise attacks (NC values)

Test Image	**Scheme**	**No Attack**	**Translation Attack**	**Salt and Pepper**	**Gaussian Noise**	**Speckle Noise**
Brain	J. Liu et al. [3]	0.9975	0.9835	0.9792	0.9777	0.977
	Gupta and Raval [2]	0.9567	0.9421	0.692	0.6972	0.7419
	R. Ahmed et al. [1]	0.93	0.21642	0.96964	0.92009	0.98457
	Proposed	**0.99**	**0.62042**	**0.97126**	**0.96089**	**0.95111**
House	J. Liu et al. [3]	0.998	0.9835	0.9792	0.9777	0.977
	Gupta and Raval [2]	0.9567	0.9236	0.692	0.6972	0.7122
	R. Ahmed et al. [1]	0.99	0.21412	0.99255	0.98764	0.99291
	Proposed	**0.99**	**0.92704**	**0.97996**	**0.97978**	**0.98495**
Computers	J. Liu et al. [3]	0.9975	0.9835	0.9792	0.9777	0.977
	Gupta and Raval [2]	0.9567	0.987	0.6903	0.667	0.7319
	R. Ahmed et al. [1]	0.99	0.21695	0.99082	0.97082	0.99086
	Proposed	**0.99**	**0.95626**	**0.98452**	**0.98465**	**0.98976**
Wheelchair	J. Liu et al. [3]	0.9871	0.8835	0.8792	0.8777	0.877
	Gupta and Raval [2]	0.9567	0.8843	0.6875	0.6995	0.7035
	R. Ahmed et al. [1]	0.99	0.21799	0.99489	0.98394	0.99396
	Proposed	**0.9975**	**0.9835**	**0.9792**	**0.9777**	**0.977**

Table 4.6 Quantitative comparison of all watermark images against affine, sharpening, rotation, x-shearing and y-shearing attacks (NC values)

Test Image	Scheme	Sharpening Attack	Affine Attack	Rotation	X-shear	Y-shear
Brain	J. Liu et al. [3]	0.9761	0.9835	0.9792	0.9777	0.977
	Gupta and Raval [2]	0.9663	0.7282	0.7845	0.7708	0.7439
	R. Ahmed et al. [1]	0.8244	0.39346	0.34866	0.15392	0.23565
	Proposed	**0.9772**	**0.69887**	**0.9225**	**0.79152**	**0.84561**
House	J. Liu et al. [3]	0.9761	0.9711	0.9761	0.976	0.9712
	Gupta and Raval [2]	0.9609	0.7112	0.7204	0.78277	0.7634
	R. Ahmed et al. [1]	0.99611	-0.89487	-0.89318	-0.88288	0.97439
	Proposed	**0.99731**	**0.81734**	**0.97958**	**0.99422**	**0.97415**
Computers	J. Liu et al. [3]	0.9761	0.9835	0.9792	0.9777	0.977
	Gupta and Raval [2]	0.9521	0.7701	0.7095	0.7667	0.7339
	R. Ahmed et al. [1]	0.9682	0.12364	-0.88213	0.4041	0.77085
	Proposed	**0.99819**	**0.98084**	**0.98958**	**0.99154**	**0.98629**
Wheelchair	J. Liu et al. [3]	0.8761	0.8835	0.8792	0.8777	0.877
	Gupta and Raval [2]	0.9221	0.8209	0.7211	0.7232	0.7221
	R. Ahmed et al. [1]	0.9934	0.24291	-0.99341	0.88764	0.94095
	Proposed	**0.99764**	**0.87666**	**0.98002**	**0.88101**	**0.98349**

Table 4.7 Quantitative comparison of all watermark images against gaussian smoothing, cropping, histogram equalization and contrast enhancement attacks (NC values)

Test Image	**Scheme**	**Gsmooth Attack**	**Cropping Attack**	**Histogram Eq. Attack**	**Contrast Ench Attack**
Brain	J. Liu et al. [3]	0.9761	0.9835	0.9792	0.9777
	Gupta and Raval [2]	0.9678	0.992	0.9447	0.8672
	R. Ahmed et al. [1]	-0.55365	0.93047	0.93062	0.93062
	Proposed	**0.6484**	**0.98817**	**0.99094**	**0.942**
House	J. Liu et al. [3]	0.9182	0.9835	0.9792	0.9777
	Gupta and Raval [2]	0.9548	0.8113	0.8317	0.8162
	R. Ahmed et al. [1]	-0.98861	0.99943	0.99934	0.99934
	Proposed	**0.98997**	**0.96875**	**0.99856**	**0.99746**
Computers	J. Liu et al. [3]	0.9761	0.9835	0.9792	0.9777
	Gupta and Raval [2]	0.9898	0.8115	0.8447	0.8672
	R. Ahmed et al. [1]	-0.82988	0.99841	0.99802	0.99802
	Proposed	**0.99506**	**0.97177**	**0.99888**	**0.99684**
Wheelchair	J. Liu et al. [3]	0.8761	0.8835	0.8792	0.8777
	Gupta and Raval [2]	0.9771	0.9911	0.9232	0.8552
	R. Ahmed et al. [1]	-0.93058	0.99826	0.99778	0.99778
	Proposed	**0.96241**	**0.99106**	**0.9991**	**0.99829**

Table 4.6, 4.7 and 4.8 give the quantitative comparison of both the current and suggested techniques when the watermarked test images have gone under various geometric, noise and cropping attacks to compare the robustness via NC values. The values obtained in each case clearly show that the suggested technique provides good NC values, which proves that the technique is more robust and watermark is extracted with better NC values.

Figure 4.8, 4.9, 4.10 and 4.11 are graphical illustration of how the proposed scheme performs against state of the art watermarking techniques including Ramsha et al. [1], Gupata and Raval [2] and J. Liu et al. [3] against all image attacks. The values obtained in each case clearly show that the suggested technique provides better PSNR values.

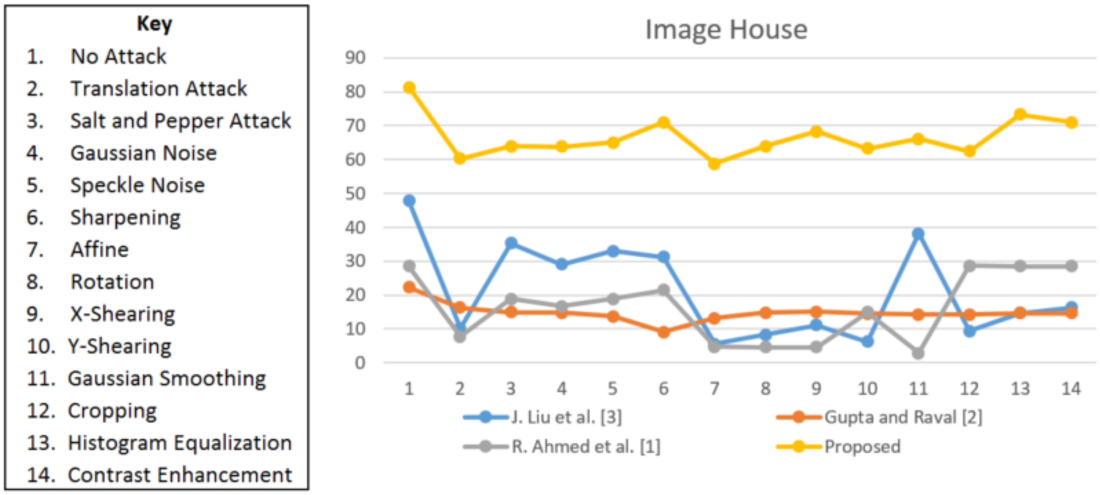


Figure 4.8 PSNR value comparison of the suggested technique with Ramsha et al. [1], Gupata and Raval [2] and J. Liu et al. [3] against all attacks using image “House”

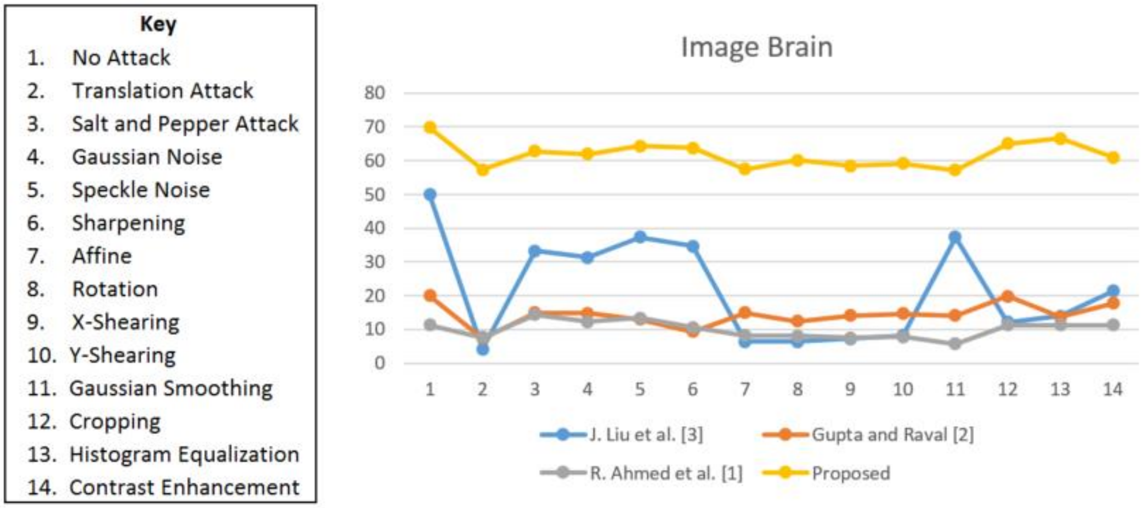


Figure 4.9 PSNR value comparison of the suggested technique with Ramsha et al. [1], Gupata and Raval [2] and J. Liu et al. [3] against all attacks using image "Brain"

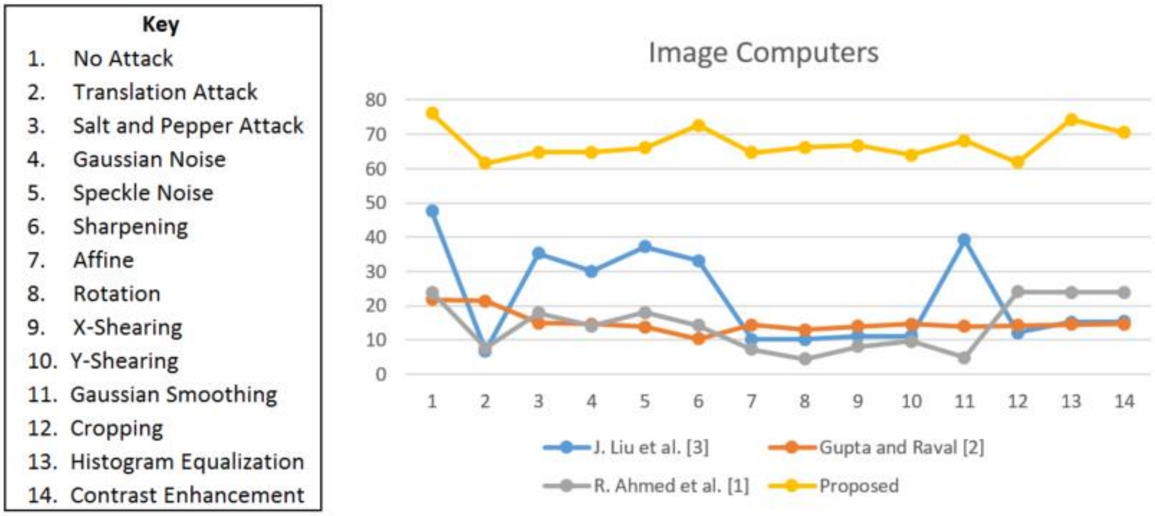


Figure 4.10 PSNR value comparison of the suggested technique with Ramsha et al. [1], Gupata and Raval [2] and J. Liu et al. [3] against all attacks using image "Computers"

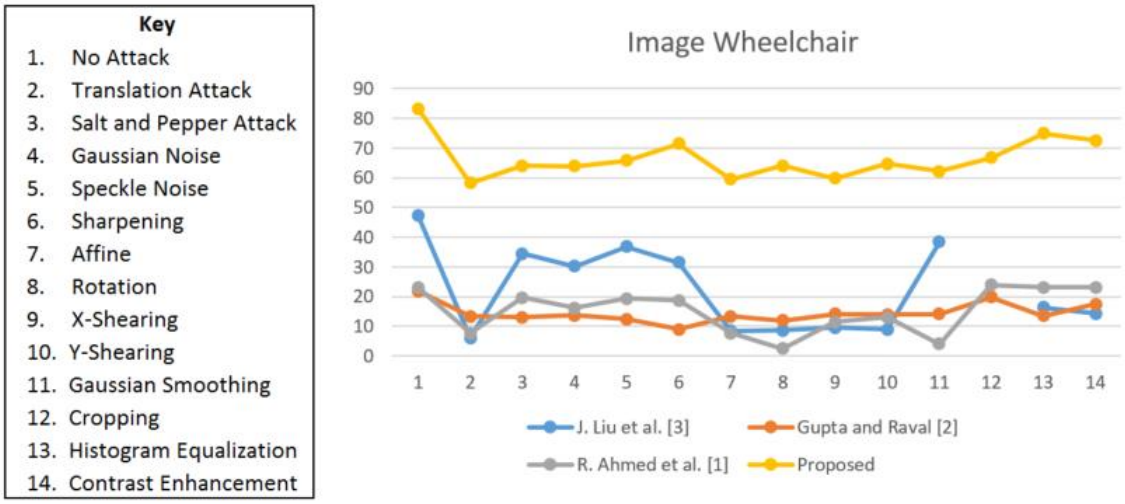


Figure 4.11 PSNR value comparison of the suggested technique with Ramsha et al. [1], Gupata and Raval [2] and J. Liu et al. [3] against all attacks using image "Wheelchair".

Figure 4.12, 4.13, 4.14 and 4.15 are graphical illustration of how the proposed scheme performs against state of the art watermarking techniques including Ramsha et al. [1], Gupata and Raval [2] and J. Liu et al. [3] against all image attacks. The values obtained in each case clearly show that the suggested technique provides good NC values.

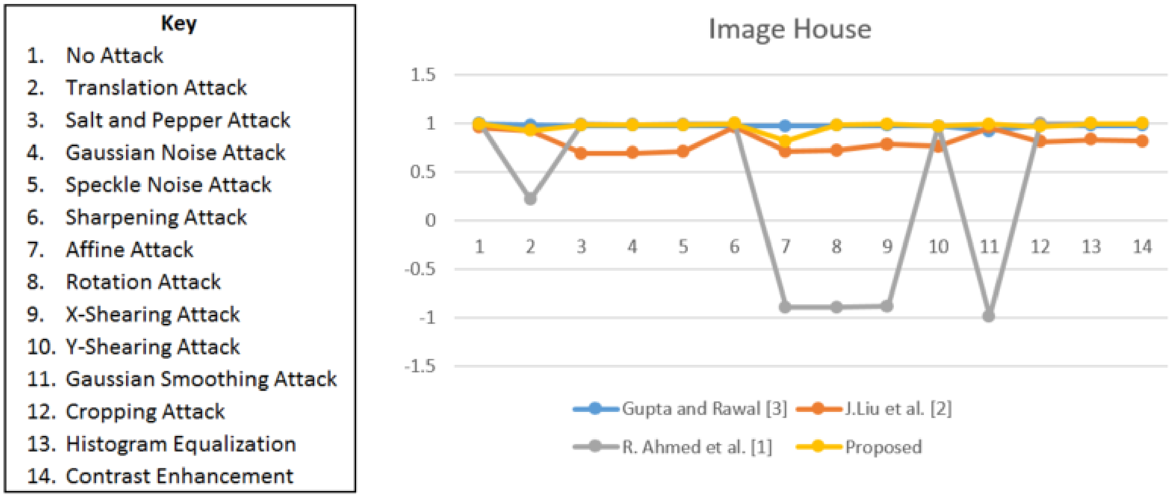


Figure 4.12 NC value comparison of the suggested technique with Ramsha et al. [1], Gupata and Raval [2] and J. Liu et al. [3] against all attacks using image "House".

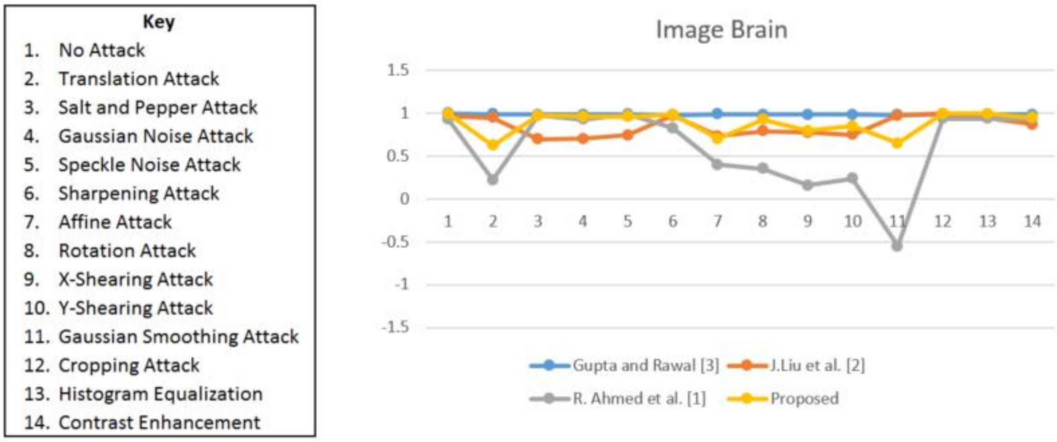


Figure 4.13NC value comparison of the suggested technique with Ramsha et al. [1], Gupata and Raval [2] and J. Liu et al. [3] against all attacks using image “Brain”.

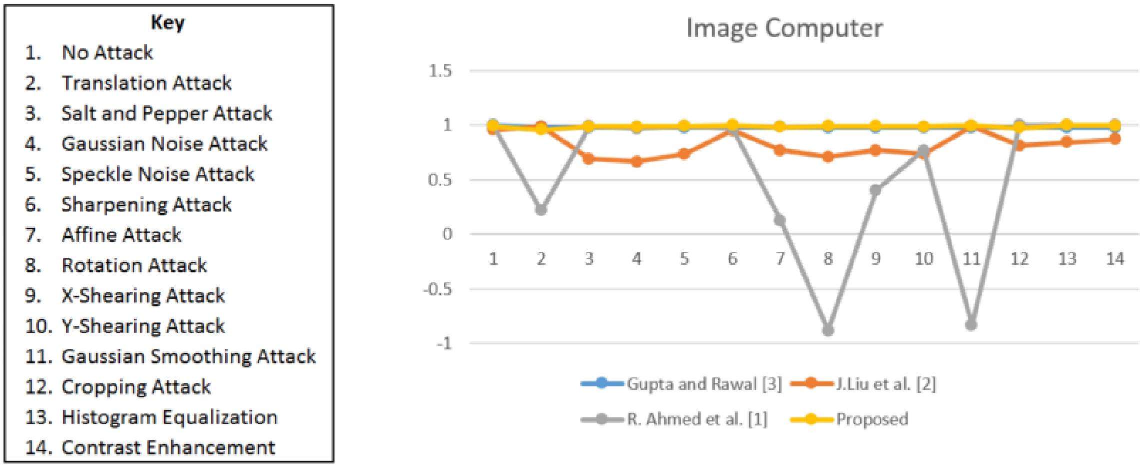


Figure 4.14 NC value comparison of the suggested technique with Ramsha et al. [1], Gupata and Raval [2] and J. Liu et al. [3] against all attacks using image “Computers”.

Key

1. No Attack
2. Translation Attack
3. Salt and Pepper Attack
4. Gaussian Noise Attack
5. Speckle Noise Attack
6. Sharpening Attack
7. Affine Attack
8. Rotation Attack
9. X-Shearing Attack
10. Y-Shearing Attack
11. Gaussian Smoothing Attack
12. Cropping Attack
13. Histogram Equalization
14. Contrast Enhancement

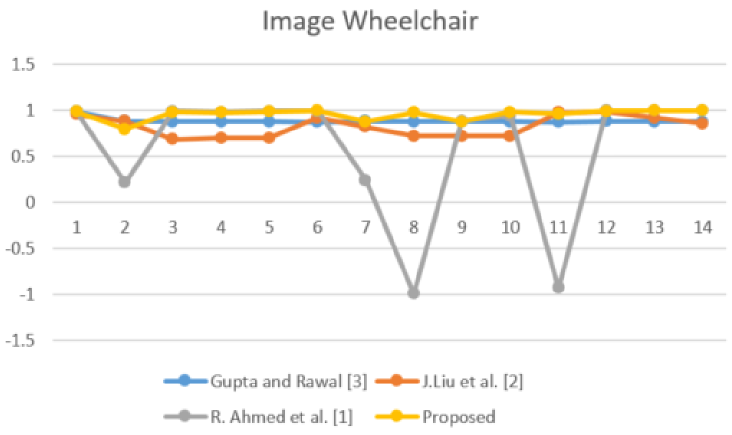
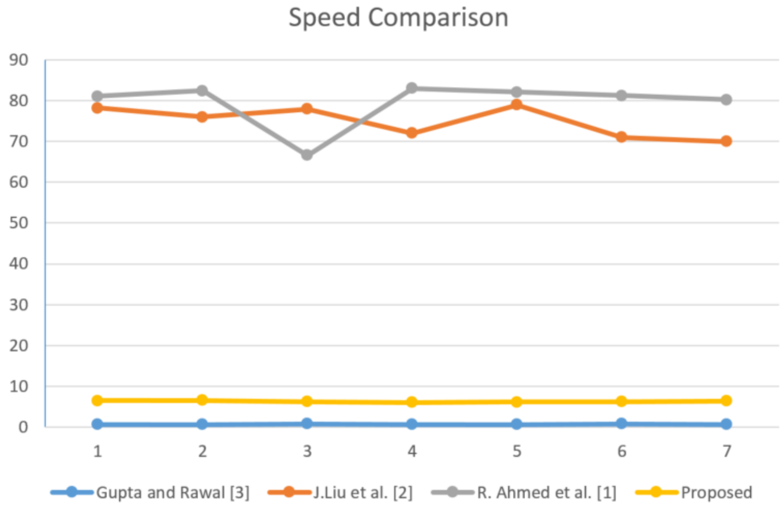


Figure 4.15 NC value comparison of the suggested technique with Ramsha et al. [1], Gupata and Raval [2] and J. Liu et al. [3] against all attacks using image “Wheelchair”.

Table 4.8 Comparison of speed of the suggested technique and current techniques under no attack. The tests were carried out on 16GB RAM system and is an average speed of 7 images.

Ramsha et al. [1]	Gupta and Raval [2]	J. Liu et al. [3]	Suggested scheme
78.55 secs	76.113 secs	0.612 secs	6.22 secs



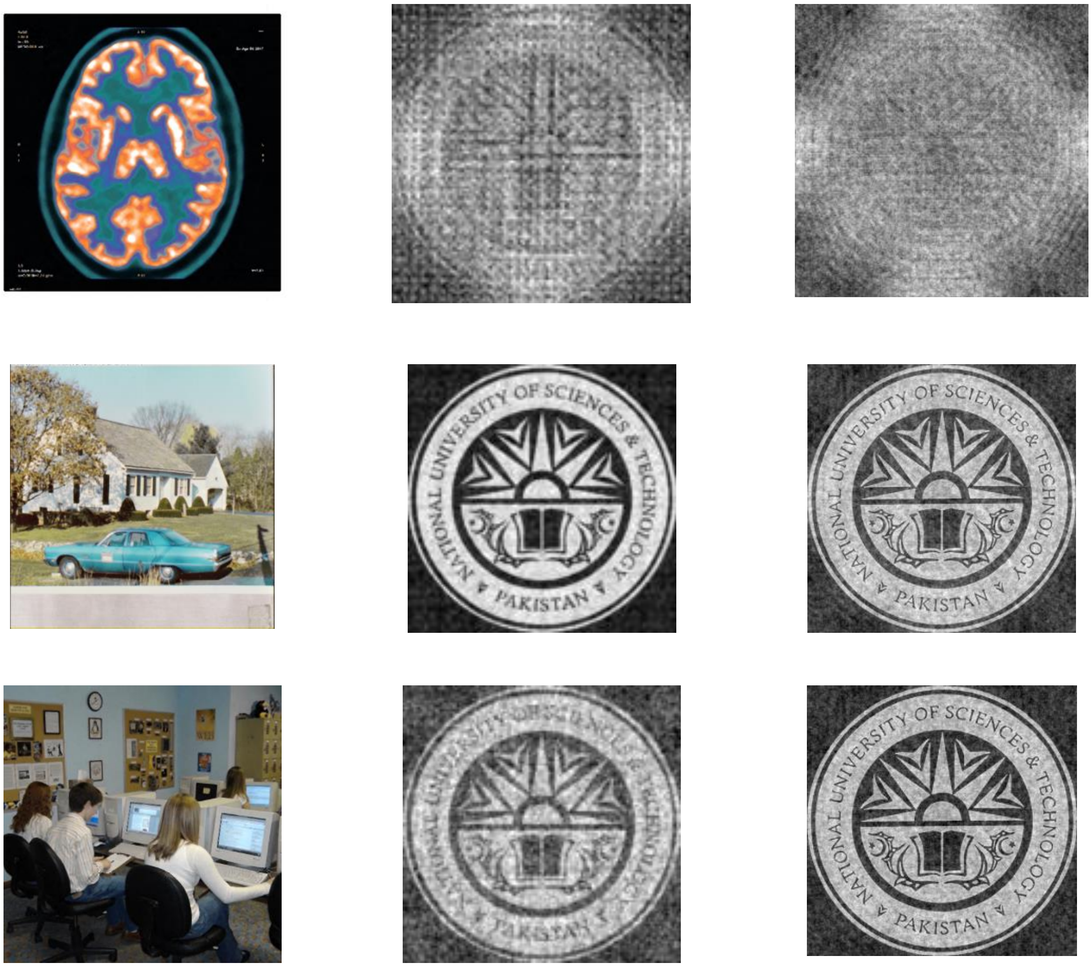
Key

1. Image Brain
2. Image House
3. Image Computers
4. Image Wheelchair
5. Image Man
6. Image Sniper
7. Image Baseball

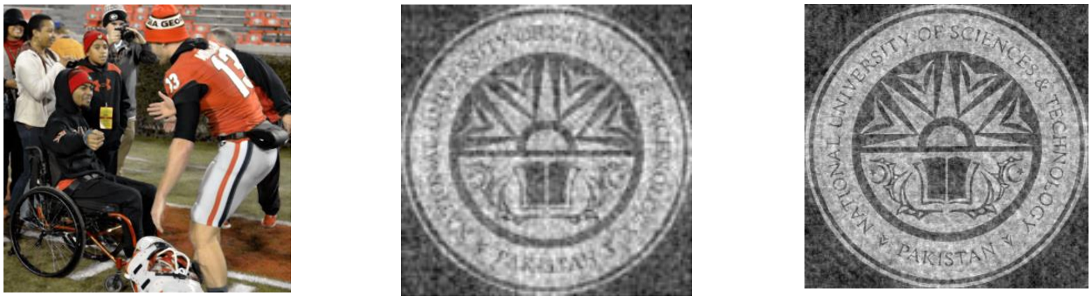
Figure 4.16 Speed comparison graph of proposed scheme with Ramsha et al. [1], Gupata and Raval [2] and J. Liu et al. [3].

It is worth noting that J. Liu et al. is performing better in terms of speed than the proposed scheme which is due to the fact the for the purpose of security Arnold scrambling has been used, since flipping the matrix required more computation hence as trade off with increased security the proposed scheme performs comparatively slower.

However in the case of median filtering attack and motion blurring attack the suggested technique does not perform well and gives negative values for NC (range of normalized correlation is defined as [-1 1]), which results in reduced quality of the watermark. Figure 4.17 represents the watermarks obtained from images (brain, house, computers, wheelchair, man, sniper, man on fire, tent) when the received watermarked images are under median filtering attack. Figure.(a) illustrates the host images, figure.(b) illustrates the watermark images extracted using the current technique [1], while figure.(c) illustrates the extracted watermark images using the suggested scheme.



(a) Watermark images (b) Ramsha et al.[1] (c) Suggested scheme



(c) Watermark images (d) Ramsha et al.[1] (c) Suggested scheme

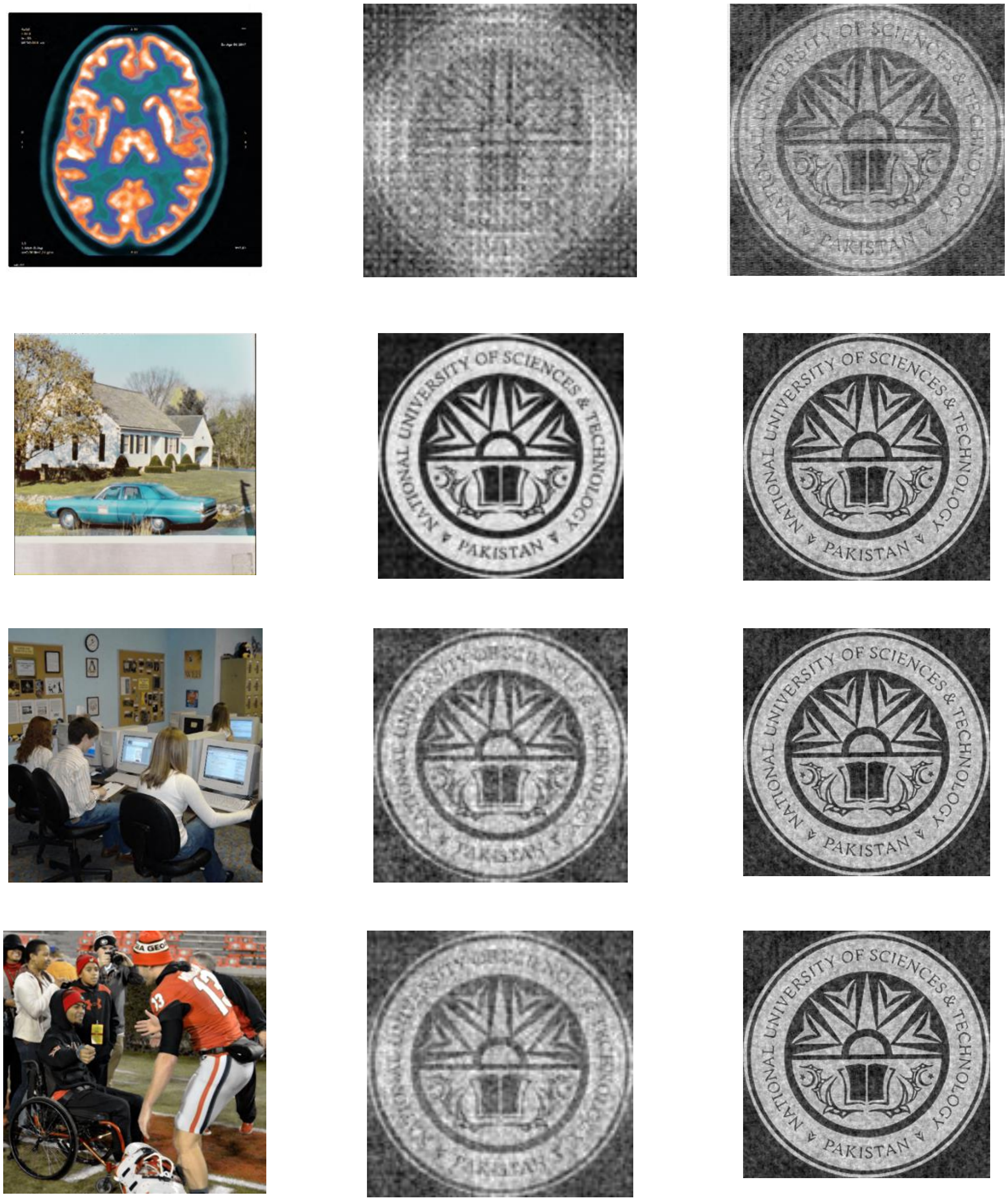
Figure 4.17 Resultant watermark images when images are under median filtering attack (current [1] and suggested technique)

Table 4.9 Quantitative comparison of all watermark images against median filtering attack

Test Image	**Scheme**	**Median Filtering Attack**	
		PSNR	**NC**
Brain	Current [1]	5.4782	-0.63392
	Suggested	54.715	-0.38662
House	Current [1]	2.6235	-0.99243
	Suggested	5.4782	-0.63392
Computers	Current [1]	4.1141	-0.92248
	Suggested	51.801	-0.97039
Wheelchair	Current [1]	4.398	-0.90662
	Suggested	52.699	-0.90917

Figure 4.18 represents the watermarks obtained from images (brain, house, computers, wheelchair) when the received watermarked images are under motion blurring attack. Figure.(a) illustrates the host images, figure.(b) illustrates the watermark images extracted

using the current technique [1], while figure.(c) illustrates the extracted watermark images using the suggested scheme.



(a) Watermark images (b) Ramsha et al.[1] (c) Suggested scheme

Figure 4.18 Resultant watermark images when images are under motion blurring attack (current [1] and suggested technique)

Table 4.10 Quantitative comparison of all watermark images against motion blurring attack

Test Image	**Scheme**	**Median Filtering Attack**	
		PSNR	**NC**
Brain	Current [1] **Suggested**	5.49 53.15	-0.6673 -0.7576
House	Current [1] **Suggested**	2.486 52.13	-0.994 -0.981
Computers	Current [1] **Suggested**	4.18 52.26	-0.93 -0.9896
Wheelchair	Current [1] **Suggested**	3.38 52.00	-0.975 -0.99

4.1.2 Conclusion

The proposed image watermarking technique was demonstrated on set of 25 images that were watermarked under different attacks including noising attacks (“salt & pepper, multiplicative noise, gaussian noise”), geometric attacks (“cropping, translation, rotation, X-shearing and Y-shearing, affine”) processing attacks on image (“histogram equalization, gaussian smoothing, sharpening and contrast enhancement”) to examine the imperceptibility of the suggested technique using peak-signal-to-noise ratio and noise correlation. Under certain attacks both the techniques had good NC but suggested technique has much higher PSNR value, and under attacks such as affine, translation, x-shearing, y-shearing and rotation the suggested technique yields better results, outperforming the current technique with better results under almost all the discussed attacks.

Chapter 5

CONCLUSION AND FUTURE WORK

The purpose of watermarking is to insert the data secretly into the host image to prevent illegal usage by providing authentication and establishing ownership. But images may be a subject to attacks which may be unintentional such as during transmission or intentional such as blurring or distortion. Hence an efficient image watermarking technique should provide imperceptibility and robustness against all possible attacks that may be carried out on the image. An attack resistant image watermarking technique is presented in this thesis based on grouping of “LWT, schur and SVD” transforms. The processed logo is embedded in the HH band of original cover image.

The suggested technique is demonstrated on a set of images where the images are watermarked and then are subjected to various attacks such as (“salt & pepper, multiplicative noise, gaussian noise, cropping, translation, rotation, X-shearing and Y shearing, affine, histogram equalization, gaussian smoothing, sharpening, contrast enhancement and median filtering”) to investigate the imperceptibility and robustness of the suggested technique using two metrics i.e. PSNR and NC. Thus, from the visual and quantitative analysis the suggested watermarking technique is verified to yield better imperceptibility and robustness outperforming the current technique with better results of both PSNR and NC in all the cases.

5.1 Future Work Directions

In the future;

1. Severe image degradations using geometric transformation attacks desynchronize the location of watermark embedding in the cover image. A geometric attack correction technique may be explored that estimates the geometrical distortion in the attacked image and then aims to restores the host image to its original form before applying the detection process, hence improving the results.

2. It has been observed that images with more details and higher resolutions perform better under higher strength of embedded watermark while maintaining the image imperceptibility and images with low resolution or less details perform well under embedding strength with lower values. Hence a possibility of optimally adjusting the embedding strength of the digital watermark may be explored.
3. To learn the image details a feature detection scheme may be explored, using machine learning algorithms that can insert the watermark with strength dependent on the feature relation of the images.
4. The suggested watermarking technique may be also be used for watermarking of audio and video files.

BIBLOGRAPHY

[1] R. Ahmed, M. M. Riaz, and A. Ghafoor, “Attack resistant watermarking technique based on fast curvelet transform and Robust Principal Component Analysis,” *Multimedia Tools and Applications,* vol. 77, no. 8, pp. 9443-9453, 2018.

[2] A. K. Gupta, and M. S. Raval, “A robust and secure watermarking scheme based on singular values replacement,” *Sadhana,* vol. 37, no. 4, pp. 425-440, 2012.

[3] J. Liu, J. Huang, Y. Luo, L. Cao, S. Yang, D. Wei, and R. Zhou, “An optimized image watermarking method based on HD and SVD in DWT domain,” *IEEE Access,* vol. 7, pp. 80849-80860, 2019.

[4] A. M. Eskicioglu, and E. J. Delp, “An overview of multimedia content protection in consumer electronics devices,” *Signal Processing: Image Communication,* vol. 16, no. 7, pp. 681-699, 2001.

[5] E. Lin, A. M. Eskicioglu, R. L. Lagendijk, and E. J. Delp, “Advances in digital video content protection,” *Proceedings of the IEEE,* vol. 93, no. 1, pp. 171-183, 2005.

[6] P. W. Wong, "A watermark for image integrity and ownership verification." pp. 374-379.

[7] K. Joshi, and R. Yadav, "A new LSB-S image steganography method blend with Cryptography for secret communication." pp. 86-90.

[8] M. Abdullatif, A. M. Zeki, J. Chebil, and T. S. Gunawan, "Properties of digital image watermarking." pp. 235-240.

[9] A. S. Panah, R. Van Schyndel, T. Sellis, and E. Bertino, “On the properties of non-media digital watermarking: a review of state of the art techniques,” *IEEE Access,* vol. 4, pp. 2670-2704, 2016.

[10] T. Dutta, and H. P. Gupta, “An efficient framework for compressed domain watermarking in p frames of high-efficiency video coding (HEVC)--encoded video,” *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM),* vol. 13, no. 1, pp. 1-24, 2017.

[11] P. W. Wong, and N. Memon, “Secret and public key image watermarking schemes for image authentication and ownership verification,” *IEEE transactions on image processing,* vol. 10, no. 10, pp. 1593-1601, 2001.

[12] R. Artru, A. Gouaillard, and T. Ebrahimi, “Digital Watermarking of video streams: Review of the State-Of-The-Art,” *arXiv preprint arXiv:1908.02039,* 2019.

[13] S. Daly, "Digital images and human vision," *The Visible Differences Predictor: An Algorithm for the Assessment of Image Fidelity,* pp. 179-206: MIT press, 1993.

[14] S. J. Daly, "Visible differences predictor: an algorithm for the assessment of image fidelity." pp. 2-15.

[15] K. Das, J. Jiang, and J. Rao, “Mean squared error of empirical predictor,” *The Annals of Statistics,* vol. 32, no. 2, pp. 818-840, 2004.

[16] S. Ramakrishnan, T. Gopalakrishnan, and K. Balasamy, “A wavelet based hybrid SVD algorithm for digital image Watermarking,” *Signal & Image Processing,* vol. 2, no. 3, pp. 157, 2011.

[17] V. Santhi, and A. Thangavelu, “DWT-SVD combined full band robust watermarking technique for color images in YUV color space,” *International Journal of Computer Theory and Engineering,* vol. 1, no. 4, pp. 424, 2009.

[18] C. Qin, P. Ji, X. Zhang, J. Dong, and J. Wang, “Fragile image watermarking with pixel-wise recovery based on overlapping embedding strategy,” *Signal processing,* vol. 138, pp. 280-293, 2017.

[19] M.-J. Tsai, and C.-C. Chien, "A wavelet-based semi-fragile watermarking with recovery mechanism." pp. 3033-3036.

[20] S. A. Parah, J. A. Sheikh, N. A. Loan, and G. M. Bhat, “Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing,” *Digital Signal Processing,* vol. 53, pp. 11-24, 2016.

[21] W. Yongqi, and Z. Hui, "A color image blind watermarking algorithm based on chaotic scrambling and integer wavelet." pp. 413-416.

[22] X. You, L. Du, Y.-m. Cheung, and Q. Chen, “A blind watermarking scheme using new nontensor product wavelet filter banks,” *IEEE Transactions on Image Processing,* vol. 19, no. 12, pp. 3271-3284, 2010.

[23] R. Ni, Q. Ruan, and H.-D. Cheng, “Secure semi-blind watermarking based on iteration mapping and image features,” *Pattern Recognition,* vol. 38, no. 3, pp. 357-368, 2005.

[24] W.-L. Chao, “Comparison of Video Copy Detection Techniques: The Robustness against Distortion and Attacking,” *Technical Paper, Graduate Institute of Communication Engineering, National Taiwan University*, 2009.

[25] D. Kirovski, *Multimedia watermarking techniques and applications*: CRC Press, 2006.

[26] R. Sreejith, and S. Senthil, "A novel tree based method for data hiding and integrity in medical images." pp. 1-4.

[27] M. D. Swanson, B. Zhu, and A. H. Tewfik, "Transparent robust image watermarking." pp. 211-214.

[28] N. Bansal, V. K. Deolia, A. Bansal, and P. Pathak, "Digital image watermarking using least significant bit technique in different bit positions." pp. 813-818.

[29] P. Venugopala, H. Sarojadevi, N. N. Chiplunkar, and V. Bhat, "Video watermarking by adjusting the pixel values and using scene change detection." pp. 259-264.

[30] D. Somwanshi, I. Chhipa, T. Singhal, and A. Yadav, "Modified Least Significant Bit Algorithm of Digital Watermarking for Information Security," *Soft Computing: Theories and Applications*, pp. 473-484: Springer, 2018.

[31] D.-s. WANG, J.-p. LI, D.-k. HU, and Y.-h. YAN, "A novel biometric image integrity authentication using fragile watermarking and Arnold transform," *Information Computing And Automation: (In 3 Volumes)*, pp. 799-802: World Scientific, 2008.

[32] H. Zhang, C. Wang, and X. Zhou, “Fragile watermarking for image authentication using the characteristic of SVD,” *Algorithms*, vol. 10, no. 1, pp. 27, 2017.

[33] A. Shehab, M. Elhoseny, K. Muhammad, A. K. Sangaiah, P. Yang, H. Huang, and G. Hou, “Secure and robust fragile watermarking scheme for medical images,” *IEEE Access*, vol. 6, pp. 10269-10278, 2018.

[34] A. Miyazaki, "An improved correlation-based watermarking method for images using a nonlinear programming algorithm." p. 5.

[35] L. Gajriya, M. Tiwari, and J. Singh, “Correlation based watermarking technique-threshold based extraction,” *Int J Emerg Technol*, vol. 2, no. 2, pp. 80-83, 2011.

[36] N. Nikolaidis, and I. Pitas, “Robust image watermarking in the spatial domain,” *Signal processing*, vol. 66, no. 3, pp. 385-403, 1998.

[37] G. Yamuna, and D. Sivakumar, “Novel reversible watermarking scheme for authentication of military images,” *International Journal of Signal and Imaging Systems Engineering*, vol. 2, no. 3, pp. 134-140, 2009.

[38] T. Yamada, M. Maeta, and F. Mizushima, “Video watermark application for embedding recipient ID in real-time-encoding VoD server,” *Journal of Real-Time Image Processing*, vol. 11, no. 1, pp. 211-222, 2016.

[39] P. Garg, L. Dodeja, and M. Dave, "Hybrid Color Image Watermarking Algorithm Based on DSWT-DCT-SVD and Arnold Transform," *Advances in Signal Processing and Communication*, pp. 327-336: Springer, 2019.

[40] S. D. Lin, S.-C. Shie, and J. Y. Guo, “Improving the robustness of DCT-based image watermarking against JPEG compression,” *Computer Standards & Interfaces*, vol. 32, no. 1-2, pp. 54-60, 2010.

[41] H.-C. Chen, Y.-W. Chang, and R.-C. Hwang, “A watermarking technique based on the frequency domain,” *journal of multimedia*, vol. 7, no. 1, pp. 82, 2012.

[42] M. Nakano-Miyatake, and H. Perez-Meana, “Video watermarking technique using visual sensibility and motion vector,” *Visual Serving, INTECH Open Access*, pp. 217-234, 2010.

[43] S. Roy, and A. K. Pal, “A blind DCT based color watermarking algorithm for embedding multiple watermarks,” *AEU-International Journal of Electronics and Communications*, vol. 72, pp. 149-161, 2017.

[44] L. Abdi, F. B. Abdallah, and A. Meddeb, “Real-time Watermarking Algorithm of H. 264/AVC Video Stream,” *International Arab Journal of Information Technology (IAJIT)*, vol. 14, no. 2, 2017.

[45] Z. Ma, J. Huang, M. Jiang, and X. Niu, “A video watermarking DRM method based on H. 264 compressed domain with low bit-rate increasement,” *Chinese Journal of Electronics*, vol. 25, no. 4, pp. 641-647, 2016.

[46] A. Poljicak, L. Mandic, and D. Agic, “Discrete Fourier transform-based watermarking method with an optimal implementation radius,” *Journal of Electronic Imaging,* vol. 20, no. 3, pp. 033008, 2011.

[47] C.-M. Pun, "A novel DFT-based digital watermarking system for images."

[48] N. Jimson, and K. Hemachandran, "DFT Based Coefficient Exchange Digital Image Watermarking." pp. 567-571.

[49] J. Kaur, E. V. Kaur, and N. Dhillon, “Improved Image Watermarking using Fast Fourier Transform and Arnold Transform based SVD Technique,” *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),* vol. 5, no. 1, 2016.

[50] J. Xu, H. Pang, and J. Zhao, “Digital Image Watermarking Algorithm Based on Fast Curvelet Transform,” *JSEA,* vol. 3, no. 10, pp. 939-943, 2010.

[51] M. Gnanapriya, and A. Sivasankar, “Discrete curvelet transform based digital image watermarking using genetic algorithm (DCUT-WAGA),” *International Journal of Computational Intelligence Research,* vol. 6, no. 3, pp. 443-449, 2010.

[52] R. Thanki, S. Borra, V. Dwivedi, and K. Borisagar, “An efficient medical image watermarking scheme based on FDCuT–DCT,” *Engineering science and technology, an international journal,* vol. 20, no. 4, pp. 1366-1379, 2017.

[53] T. D. Hien, K. Miyara, I. Kei, F. F. Ali, Y. W. Chen, and Z. Nakao, "Digital watermarking based on curvelet transform." pp. 1-4.

[54] K. Meenakshi, C. S. Rao, and K. S. Prasad, "A robust watermarking scheme based Walsh-Hadamard transform and SVD using ZIG ZAG scanning." pp. 167-172.

[55] S. Kalarikkal Pullayikodi, N. Tarhuni, A. Ahmed, and F. B. Shiginah, “Computationally efficient robust color image watermarking using fast walsh hadamard transform,” *Journal of Imaging,* vol. 3, no. 4, pp. 46, 2017.

[56] Y. Ishikawa, K. Uehira, and K. Yanaka, “Practical evaluation of illumination watermarking technique using orthogonal transforms,” *Journal of Display Technology,* vol. 6, no. 9, pp. 351-358, 2010.

[57] S. Parvathavarthini, and R. Shanthakumari, “An adaptive watermarking process in Hadamard transform,” *International Journal of Advanced Information Technology,* vol. 4, no. 2, pp. 1, 2014.

[58] M. Ali, and C. W. Ahn, “An optimized watermarking technique based on self-adaptive DE in DWT–SVD transform domain,” *Signal Processing,* vol. 94, pp. 545-556, 2014.

[59] K. A. Al-Afandy, O. S. Faragallah, E.-S. M. EL-Rabaie, F. E. Abd El-Samie, and A. ELmhalawy, "Efficient color image watermarking using homomorphic based SVD in DWT domain." pp. 43-47.

[60] N. M. Makbol, B. E. Khoo, and T. H. Rassem, “Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics,” *IET Image processing,* vol. 10, no. 1, pp. 34-52, 2016.

[61] T. Tabassum, and S. M. Islam, "A digital video watermarking technique based on identical frame extraction in 3-Level DWT." pp. 101-106.

[62] M. Barni, F. Bartolini, and A. Piva, “Improved wavelet-based watermarking through pixel-wise masking,” *IEEE transactions on image processing,* vol. 10, no. 5, pp. 783-791, 2001.

[63] B. Yadav, A. Kumar, and Y. Kumar, "A robust digital image watermarking algorithm using DWT and SVD," *Soft Computing: Theories and Applications*, pp. 25-36: Springer, 2018.

[64] M. Ghebleh, A. Kanso, and H. S. Own, “A blind chaos-based watermarking technique,” *Security and Communication Networks,* vol. 7, no. 4, pp. 800-811, 2014.

[65] N. Liu, H. Li, H. Dai, D. Guo, and D. Chen, “Robust blind image watermarking based on chaotic mixtures,” *Nonlinear Dynamics,* vol. 80, no. 3, pp. 1329-1355, 2015.

[66] R. Keshavarzian, and A. Aghagolzadeh, “ROI based robust and secure image watermarking using DWT and Arnold map,” *AEU-International Journal of Electronics and Communications,* vol. 70, no. 3, pp. 278-288, 2016.

[67] V. S. Verma, and R. K. Jha, “Improved watermarking technique based on significant difference of lifting wavelet coefficients,” *Signal, Image and Video Processing,* vol. 9, no. 6, pp. 1443-1450, 2015.

[68] I. Daubechies, and W. Sweldens, “Factoring wavelet transforms into lifting steps,” *Journal of Fourier analysis and applications,* vol. 4, no. 3, pp. 247-269, 1998.

[69] S. Liu, B. M. Hennelly, and J. T. Sheridan, “Digital image watermarking spread-space spread-spectrum technique based on double random phase encoding,” *Optics Communications,* vol. 300, pp. 162-177, 2013.

[70] K. Loukhaoukha, J.-Y. Chouinard, and M. H. Taieb, “Optimal image watermarking algorithm based on LWT-SVD via multi-objective ant colony optimization,” *Journal of Information Hiding and Multimedia Signal Processing,* vol. 2, no. 4, pp. 303-319, 2011.

[71] R. G. Kabra, and S. S. Agrawal, "Robust embedding of image watermark using LWT and SVD." pp. 1968-1972.

[72] P. Nagarjuna, D. Tyagi, and R. B. Ramachandra, "SWT and Spread Spectrum Coding Based Copyright Protection Technique for Digital Images." pp. 58-63.

[73] M. K. Pandey, G. Parmar, R. Gupta, and A. Sikander, “Non-blind Arnold scrambled hybrid image watermarking in YCbCr color space,” *Microsystem Technologies,* vol. 25, no. 8, pp. 3071-3081, 2019.

[74] Y. Lu, and M. N. Do, "A new contourlet transform with sharp frequency localization." pp. 1629-1632.

[75] L. Chen, and J. Zhao, "Adaptive contourlet-based image watermarking robust to geometric transformations and image compression." pp. 1-6.

[76] E. Najafi, and K. Loukhaoukha, “Hybrid secure and robust image watermarking scheme based on SVD and sharp frequency localized contourlet transform,” *Journal of information security and applications,* vol. 44, pp. 144-156, 2019.

[77] S. Ranjbar, F. Zargari, and M. Ghanbari, “A highly robust two-stage contourlet-based digital image watermarking method,” *Signal Processing: Image Communication,* vol. 28, no. 10, pp. 1526-1536, 2013.

[78] X.-y. Wang, C.-p. Wang, H.-y. Yang, and P.-p. Niu, “A robust blind color image watermarking in quaternion Fourier transform domain,” *Journal of Systems and Software,* vol. 86, no. 2, pp. 255-277, 2013.

[79] M. Islam, A. Roy, and R. H. Laskar, “SVM-based robust image watermarking technique in LWT domain using different sub-bands,” *Neural Computing and Applications,* vol. 32, no. 5, pp. 1379-1403, 2020.

[80] N. Dabas, and R. P. Singh, “ELM-Kernel and reduced kernel ELM based watermarking scheme,” *Journal of Information Security and Applications,* vol. 46, pp. 173-192, 2019.

[81] R. Mehta, N. Rajpal, and V. P. Vishwakarma, “LWT-QR decomposition based robust and efficient image watermarking scheme using Lagrangian SVR,” *Multimedia Tools and Applications,* vol. 75, no. 7, pp. 4129-4150, 2016.

[82] D. K. Thind, and S. Jindal, “A semi blind DWT-SVD video watermarking,” *Procedia Computer Science,* vol. 46, pp. 1661-1667, 2015.

[83] E. Ganic, and A. M. Eskicioglu, "Robust DWT-SVD domain image watermarking: embedding data in all frequencies." pp. 166-174.

[84] S. L. Agrwal, A. Yadav, U. Kumar, and S. K. Gupta, "Improved invisible watermarking technique using IWT-DCT." pp. 283-285.

[85] M. Hamidi, M. El Haziti, H. Cherifi, and M. El Hassouni, “Hybrid blind robust image watermarking technique based on DFT-DCT and Arnold transform,” *Multimedia Tools and Applications,* vol. 77, no. 20, pp. 27181-27214, 2018.

[86] M. Cedillo-Hernandez, F. Garcia-Ugalde, M. Nakano-Miyatake, and H. Perez-Meana, "Robust digital image watermarking using interest points and DFT domain." pp. 715-719.

[87] H.-Y. Yang, X.-Y. Wang, and C.-P. Wang, “A robust digital watermarking algorithm in undecimated discrete wavelet transform domain,” *Computers & Electrical Engineering,* vol. 39, no. 3, pp. 893-906, 2013.

[88] X. Zhang, and S. Wang, “Watermarking scheme capable of resisting sensitivity attack,” *IEEE Signal Processing Letters,* vol. 14, no. 2, pp. 125-128, 2007.

[89] E. Quiring, D. Arp, and K. Rieck, “Fraternal twins: Unifying attacks on machine learning and digital watermarking,” *arXiv preprint arXiv:1703.05561,* 2017.

[90] E. Quiring, D. Arp, and K. Rieck, "Forgotten siblings: Unifying attacks on machine learning and digital watermarking." pp. 488-502.

[91] P. Venugopala, S. Jain, H. Sarojadevi, and N. N. Chiplunkar, "Study of possible attacks on image and video watermark." pp. 3505-3510.

[92] C.-q. Yin, L. Li, A.-q. Lv, and L. Qu, "Color image watermarking algorithm based on DWT-SVD." pp. 2607-2611.

[93] R. Agarwal, M. Santhanam, and K. Venugopalan, "Multichannel digital watermarking of color images using SVD." pp. 1-6.

[94] R. Gunjan, P. Mitra, and M. S. Gaur, "Contourlet based image watermarking scheme using Schur factorization and SVD." pp. 337-340.