# Efficient Algorithms for Embedding Digital Watermark in Curvelet Domain

*A*

*Thesis*

*Submitted in fulfillment of the*

*Requirements for the award of the degree of*

## Doctor of Philosophy

*Submitted by*

**Ranjeeta**

**(Registration No. 950903047)**

*Under the supervision of*

**Dr. Sanjay Sharma**
**Professor**
**Department of Electronics and communication Engineering**

**Dr. L. R. Raheja**
**Professor (Retd.)**
**IIT, Kharagpur**

**Computer Science & Engineering Department**
**Thapar University**
**Patiala -147004, Punjab, India**

**2017**

# CERTIFICATE

I, **Ranjeeta** hereby certify that the work presented in this thesis entitled "**Efficient Algorithms for Embedding Digital Watermark in Curvelet Domain**", in fulfillment of requirements for the award of the degree of DOCTOR OF PHILOSOPHY being submitted in Computer Science and Engineering Department (CSED), Thapar University, Patiala, Punjab, is an authentic record of my own work carried out under the supervision of Dr. Sanjay Sharma (Professor, ECED, Thapar University, Patiala) and Dr. L.R. Raheja (Professor (Retd.), IIT, Kharagpur).

The matter presented in this thesis has not been submitted either in part or full to any other university or institute for award of any degree.

(Ranjeeta)
(Signature of Candidate)

Date: - 26.6.17

This is certified that the above statement made by the candidate is correct to the best of our knowledge.

26.6.2017

Dr. Sanjay Sharma
Professor
ECED, Thapar University, Patiala
Pin -147004 (INDIA)

L.R. Raheja

Dr. L.R. Raheja
Professor (Retd.)
IIT, Kharagpur
Pin-721302 (INDIA)

# ACKNOWLEDGEMENT

The real spirit of achieving a goal is the way of excellence and discipline. I would have been never succeeded in completing my task without the cooperation, encouragement, and help provided to me by a range of personalities.

I have indeed, been privileged to have worked under the guidance of Dr. Sanjay Sharma (Professor, ECED, Thapar University, Patiala) and Dr. L.R. Raheja (Professor (Retd.), IIT, Kharagpur). I do not find adequate words to express my deep sense of gratitude toward them. Their personal guidance, encouragement, Constructive criticism, invaluable feedback and stimulating discussion at all time have been a source of inspiration to me in my work. This work has been possible only because of their priceless and unvarying efforts. Besides, I shall be failing in my duty if I do not express thanks to all the faculty members of Computer Science and Engineering Department, Thapar University, Patiala for their ungrudging help and suggestions during the course of research work.

I wish to dedicate this thesis to my mother Smt. Savita and father late Sh. Ved Parkash, who has always been an endless source of inspiration and joy in my life. I would like special regards and thanks to Dr. Shankar Deep Chauhan, AEE, Electricity Board, Haryana, whose never ending support and wholehearted help was the real impetus that continuously motivated me to do my best. I find myself spellbound to thank my niece/nephew Yagya, Rishika and Maniratan for their encouragement and affection without which this work would never have been possible.

**(Ranjeeta)**

# TABLE OF CONTENTS

## CHAPTER 3



## CHAPTER 4

# LIST OF FIGURES

# LIST OF TABLES

# LIST OF ABBREVIATIONS

| | |
|---|---|
| BER : | Bit Error Rate |
| CT : | Curvelet Transform |
| CWT : | Continuous Wavelet Transform |
| DC-DM : | Digitally Controlled Delta Modulation |
| DC-PME : | Distortion Compensation Pdf-Matched Embedding |
| DCT : | Discrete Cosine Transform |
| DFT : | Discrete Fourier Transform |
| DWT : | Discrete Wavelet Transform |
| ECG : | Electrocardiogram |
| EEG : | Electroencephalogram |
| FFT : | Fast Fourier Transform |
| FT : | Fourier Transform |
| GT : | Global Threshold |
| HIPAA : | Health Insurance Portability and Accountability Act |
| HL : | High-Low |
| HVS : | Human Visual System |
| ICA : | Independent Component Analysis |
| ISS : | Improved Spread-Spectrum |
| JANIS : | Just Another N-Order Side-Informed Scheme |
| JND : | Just Noticeable Difference |
| JPEG : | Joint Photographic Expert Group |
| KL : | Kullback–Leibler Divergence (KL) |
| LH : | Low-High |
| LL : | Low-Low |
| LOT : | Lapped Orthogonal Transform |
| LSB : | Least Significant Bit |
| LT : | Level Dependent Threshold |
| MATLAB : | Matrix Lab |
| MRI : | Magnetic Resonance Imaging |
| MSB : | Most Significant Bit |
| MSE : | Mean Square Error |

| | |
|---|---|
| MSSIM : | Mean Structure Similarity Index Measure |
| NC : | Normalized Correlation |
| PME : | Pdf-Matched Embedding |
| PRD : | Percentage Residual Difference |
| PSNR : | Peak Signal to Noise Ratio |
| QMF : | Quadrature Mirror Filters |
| RAM : | Random Access Memory |
| RDM : | Rational Dither Modulation |
| RGB : | Red Green Blue |
| RT : | Ridgelet Transform |
| SCS : | Scalar Costa Scheme |
| SIM : | Subscriber Identity Module |
| SPIHT : | Set Partitioning In Hierarchical Trees |
| SSIM : | Structure Similarity Index Measure |
| ST-DM : | Spread Transform - Dither Modulation |
| STFT : | Short Term Fourier Transform |
| SVD : | Singular Value Decomposition |
| TME : | Texture Masking Energy |
| TRP : | Television Rating Point |
| WT : | Wavelet Transform |
| $YC_bC_r$ : | Luminance, Chroma blue and Chroma red |

# ABSTRACT

Due to the popularity of the internet and its increasingly easy access to digital multimedia, many powerful tools are available for editing digital media without the loss of quality. So, authentication and intellectual property rights of digital media are critical issues. The Intellectual Property Rights (IPR) of the author are required to be protected i.e. Copyright Protection. The number of solutions to this problem, from encryption to watermarking, is growing every year. Many authors are working in the field of watermarking to protect the author ownership. Among these watermarking algorithms, some algorithms are better than the others in terms of basic watermarking requirements like invisibility, robustness and computational cost, etc.

In this thesis, we propose six watermarking techniques based on curvelet transform, which can be applied to different problems. The main aim of these techniques is to use the properties of curvelet transform and show that these are more suitable for hiding the watermark in more robust and invisible manner.

The first technique proposed is a non-blind watermarking technique for embedding a watermark in different scales of curvelet transform domain. The quality of extracted watermark of curvelet domain embedding technique is compared with wavelet domain at different number of decomposition levels. This technique is an application to a grayscale image. The second technique is also a non- blind watermarking technique. This technique utilizes the property of HVS as the edge part of an image is less sensitive. Imperceptibility of the watermark is high if it is inserted into the texture part rather than smooth part. Accordingly, in this application, information is embedded into the texture blocks of the cover image by using curvelet transform. This technique can be applied to protect the author ownership for gray scale images.

The third technique proposed is a semi-blind watermarking technique of embedding the color watermark using curvelet coefficient in the RGB cover image. This algorithm uses the bit plane method and the blue color plane of the cover image for embedding the watermark. The most significant bit (MSB) plane of watermark image is embedded into the selected scale and orientation of the curvelet coefficients of the blue channel in the cover image. The fourth algorithm combines the technique of cryptography and watermarking for application to color images. This technique demonstrates a secure,

robust and semi-blind watermarking technique for a color image by using Bijection mapping function and curvelet domain.

The fifth and sixth techniques proposed here are blind digial image watermarking techniques. These techniques are more suitable for the application of copywrite protection, forgery detection and security. The fifth technique embeds a random sequence i.e., watermark, into the curvelet transform of the color image. To make this technique more secure and robust, the luminance of the cover image is used. The luminance part of the image is transformed into curvelet domain and clustering approach is used to embed the watermark into the selected scale and orientation of curvelet domain. This technique is used to detect tampering in an image. First the technique identifies whether an image is tampered or not by comparing the embedded watermark with extracted one. Second, if image is tampered it locates the tampered region of the image.

The sixth technique is applicable to a variety of medical images. Here, it embeds the patient's information used as watermark into curvelet domain of ECG signal. Nowadays, with the help of wearable medical devices, it is easy to monitor a patient even from remote locations. Patient's information is broadcast to the hospital servers over wireless or wired media without any security. An electrocardiogram (ECG) is simply a representation of the electrical activity of the heart muscle as it changes with time. ECG can provide useful information and remains a crucial element for the assessment of cardiac patients. Embedded watermark into an ECG signal is a challenging work, because any change in ECG signal will affect the diagnosability of ECG. In this technique, it is emphasized that embedding a watermark as image is more robust as compared to text or numbers. In this technique, the QRS complex attributes of ECG are preserved so that embedding patient information does not affect the diagnosability. This algorithm is also applicable to other medical images e.g. EEG, CT scan, MRI, X-Ray etc.

In addition, the thesis provides hypothetical analysis for the performance and practicability of all the above-said techniques. To evaluate the performance of proposed techniques, performance evaluation metrics such as PSNR, NC, SSIM, BER and MSSIM are used. For sixth technique, the embedding domain is 1D signal, so the performance of technique is evaluated by all above said metrics as well as by PRD and KL as additional metrics. Also, we present experimental results to authenticate the hypothetical explanation and comparison of results for all the algorithms with existing popular technique.

# CHAPTER 1

# INTRODUCTION

In the current scenario, from satellite to home, electronic media is playing a dominating role in all areas of human life. A digital media is a conventional way to store all types of information which enables ease of use both for the users and the people involved in the creation of this information. Digital media offers a conducive way to the content providers for creating and manipulating audio and video information. Another benefit of digital media is that it offers a relatively high quality than analog media. Also, with time, no decay is observed in the quality of the material stored in a digital media as can be seen in case of analog material storage. The internet and World Wide Web are important tools to distribute the digital media, which also reduces the overhead costs. It is observed that by the ubiquitous nature of digital network systems, digital documents can be transcribed and distributed easily to large numbers of people with very low cost [1]. People can upload, download and share audios, videos, and images, as well as they, can also modify, replace or delete the original contents [2]. Though, there are several advantages offered by digital media but the same may be misused. The digital information can be modified gradually with mischievous intentions. The illegal circulation of copyright material is facilitated by the ease of access to internet by the users. There are some other worries which arise as a result of easy manipulation of digital images or videos. With some powerful processing software's, such as Adobe Photoshop, one can remove/replace some features in a picture easily without any visible trace. These kinds of operations are known as tamper. The decision in a court of law may be influenced by altering images or videos which are presented as evidence in the court. The legitimacy of the image is most important in military, medical, and judiciary [3]. So authentication and the intellectual property copyright of digital media is an important issue. As used by Walton [4], there is a film which shows, how badly image authentication is needed. Digital media copyright issues are addressed by Digital Millennium Copyright Act (DMCA). DMCA acts as a catalyst for the further advancement in the current state of the art technology in this context. There are many methods available for protecting digital media.

The traditional approach includes cryptography technique, in which data is encrypted at the transmission end and decrypted at receiving end. Cryptography consists of techniques such as mixing of words microdots, and merging words, to change the content

of the information. In today's computer savvy world, cryptography is more often associated with converting plaintext into cipher text. To understand the content of information, decryption is required to convert a ciphertext into the original text. The well known algorithms for cryptography are given by Naor and Shamir [5]. It is observed that the cryptography technique is not sufficient for data protection. Modern cryptography concerns with secrecy, integrity, non-repudiation and authentication for text data only.

The alternative method to protect unauthorized distribution is steganography. It is a technique that hides the data into the images. Steganography is defined as the science of invisible communication. Steganography takes a step further from cryptography by hiding an encrypted message such that anyone will fail to detect the encrypted data. But the hidden information could not be extracted if marked signals are corrupted during transmission [6]. Another easy alternative is an electronic signature. An electronic signature is just similar to the signature on the document duly scanned and put in the footer of the document page. The digital signature is used to verify the identity of the person who has sent the message or document. Once the identity of the sender has been established, it is easy to confirm that the content of the original document is not altered. But, these signatures are not robust enough against the noise and image processing attacks. Besides, the specific portion of the document only contains the signature giving the attacker an opportunity to modify or cut the content of the original signal easily. Owing to these drawbacks it is not regarded as a reliable authentication technique. The best and cost effective solution to save the interest of the author is watermarking.

Generally, watermarking is defined as a method that embeds a message directly in a cover message. This message becomes an essential part of the cover, which travels with the cover data to its destination. The main aim of watermarking is hiding the owner information in such a manner that no degradation is reported in the quality of the original signal [7]. This embedded information (watermark) is robust in nature, in the sense that adding of noise, filtering, compression or any attacks will not destroy the watermark.

Andrew Tirkel and Charles Osborne invented the term “Digital Watermark” in 1992. But it was used for the first time in Italy during the $13^{th}$ century. Watermark is the word obtained from the German word wassermarke and its English meaning is watermark. Watermark reflects an effect of water on the paper. The term had its origin in paper industry where each paper sheet got branded (or watermarked) automatically when the paper pulp flowed on heated drum on which the watermark was machine-written/ engraved. At that time the meaning and purpose of watermarking were very limited.

Watermark got its popularity in Europe and America in the 18th century. America utilized the watermark to indicate the authenticity i.e. to mark the certificate or paper as a trademark. In 1779, John Mathison used it for counterfeit currency detection. After then, the watermark was employed for authorization and originality on bank currency, certificates, and other documents. By this time, the meaning of watermark was the imperceptible logo or company information or owner message about the object in which it was embedded. Developments in watermark technology became a tool for fraud and tamper detection. Numerous techniques had been developed for making the watermark more popular in the field of counterfeiting. In the 19th century, digital watermarking became a powerful technique for copyright protection.

## 1.1 FUNDAMENTALS OF WATERMARKING SYSTEM

The basic nature of the watermarking system is communication, in which the transmitter or producer wants to communicate with the receiver by hiding the information (in form of watermark) into the original signal. At receiving end the extracted watermark is treated as the authorization certificate. Therefore, it is expected that watermarking shell fit into the model of a communications system as shown in Figure 1.1 below, which shows a traditional model used for communication media to transfer the data from one end to another. But this is not secured as there is an inference of noise that may damage the data.

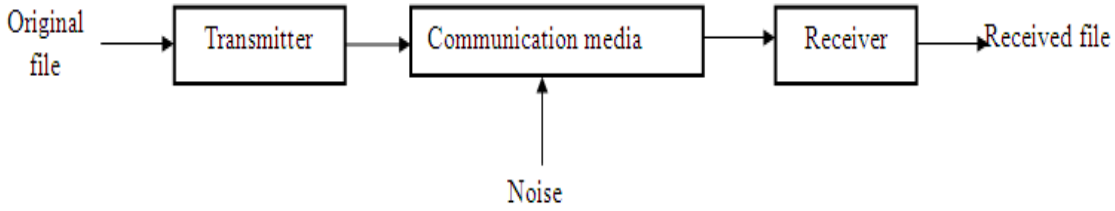


**Figure 1.1 Traditional communication system**

To make communication secured, encoders and decoders are used. Figure 1.2 below shows a secure and effective communication system. In this figure, an input message m is communicated by using encoder at transmitting end. The work of channel encoder is to encrypt the content of the original text by using a key. Here the encrypted message is shown by $x$ which is transmitted through a medium that contains some noise($n$). Consequently, the encrypted message becomes the combination of noise and information ($y$). At the receiving end, this message is decrypted into original text by using the decoder resulting in output message $m_n$.

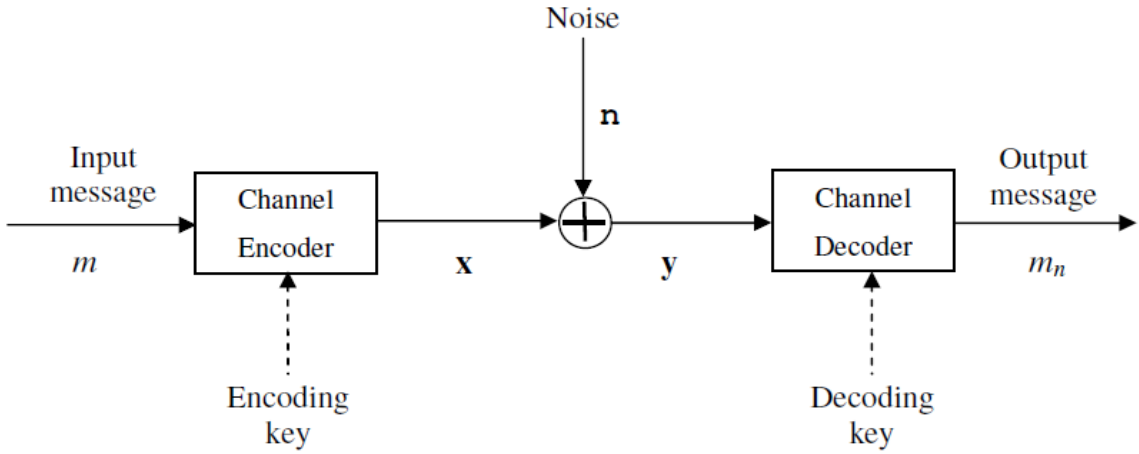


**Figure 1.2 Secure and effective communication system**

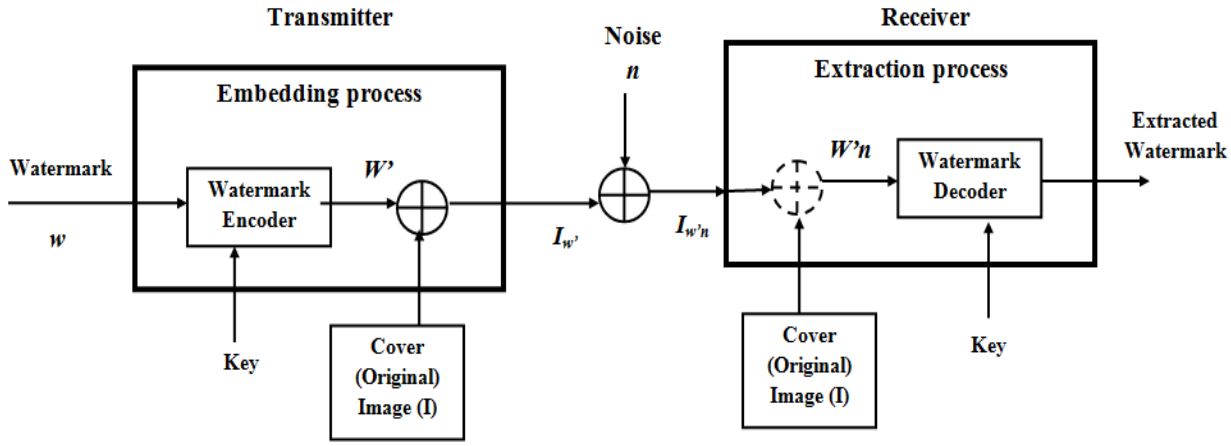


**Figure 1.3 Watermarking system with non-blind embedding and detection mapped into the communication model**

To enable secured communication, the watermarking system is seen as a combination of three processes, namely watermark embedding, watermark communication and watermark extraction. So to map the watermarking system into the communication system, there are two alternatives. The first alternative depicted in Figure 1.3. Here the cover image is treated as a noise. It is a matter of choice that this noise will be used as side information or not. The watermark (w) passes through watermark encoder (key) resulting in w'. The encrypted message w' embedded into cover image I. Resulting image is denoted by Iw' and transmitted through a communication media that contain noise n giving finally Iw'n at the receiving end. At the time of extraction the same cover image is used for extracting the watermark from the watermarked image (Iw'n). This extraction is called non-blind extraction.

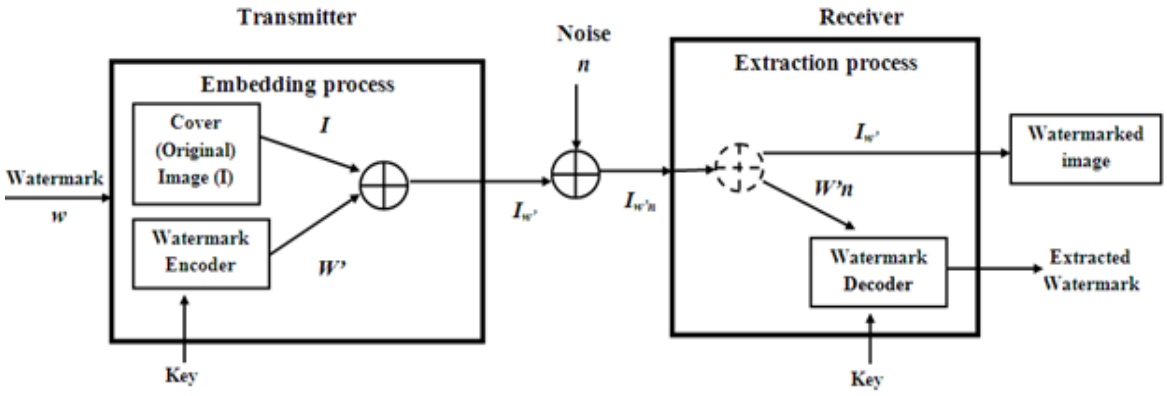


**Figure 1.4 Watermarking system with blind embedding and detection mapped into the communication model**

In other method, the cover image is transmitted with the watermark in the same signal. This method is like the time-division or frequency-division multiplexing, which transmit multiple signals on a single medium. So this model behaves like a traditional communication system. Figure 1.4 shows the watermarking system with blind detection (explained blow) mapped into the communication system. The receiver receives watermarked image i.e. similar to cover image in earlier system. The watermark detection process detects and extracts the watermark without requiring the cover image. In the figure 1.4 transmitter hides the encoded watermark message (w') into the cover image (I). The combined signal is transmitted over a communication medium to the recepient. At the receiving end, a blind extraction is used. Here, the cover image is not needed.

The main function of embedding is mapping of watermark *w* to a pattern using a key. This pattern is then embedded into the cover image in a more imperceptible manner. The embedding process aids in transmitting the watermarked image over a communication medium and thus noise is added into the cover image. Further, techniques such as filtering, decompression, compression, and digital-analog-digital conversion may be applied to the watermarked image. The watermark detector at the receiving end may be of one of the two configurations i.e. non-blind (Figure 1.3) or blind (Figure 1.4). The extraction process using non-blind extraction involves the subtraction of the cover image is usable at the extraction point for obtaining a noisy watermark pattern *W'n.* This obtained pattern is then decoded using the watermark key for extracting the original message *w*. In case of blind extraction, one uses the intelligent function used at the time of embedding for recovery of watermark without using the cover image. Since the information is communicated after hiding it into the actual image and the actual image is

subtracted from the received image: the addition of the actual image can be ignored and a blind embedding process may be followed. The system becomes analogous to the communication system as shown in Figure 1.1.

## 1.2 TYPES OF WATERMARKING

Watermarking techniques vary from application to application and types of cover images. Mohanty [8] classified the watermarking schemes as shown in Figure 1.5 below. In a spatial domain, the watermark can be directly hidden into the pixel intensity of the original image whereas in the frequency domain, the original image which is treated as a time domain signal, is converted into the frequency domain by applying some transforms. Then the frequencies of the cover image are modified as per a pre-decided pattern by the watermarking system to hide the watermark. But in feature or characteristic domain, the Human Visual System (HVS) features are used for embedding the watermark. This domain utilizes the region, boundary, contrast and other features of the object to embed the watermark.

Based on the perception of the human visual system, the digital watermarking can also be classified as visible, invisible-robust, invisible-fragile and dual. A transparent watermark is superimposed into the cover in visible watermarking, so that it is visible by human eye and careful examination. Examples of visible watermarks are watermark present in currency notes, certificates, digital documents and books for the authorization. But a watermark which is invisible as well as robust against image processing attacks is called invisible-robust watermark. The cover signal is used to embed the watermark in such a manner that the watermark is not perceived by the human eyes. Invisible-fragile watermark is destroyed if any attacker tries to modify the watermarked image in pursuit of recovery of the watermark. A combination of the visible and invisible watermark is called a dual watermarking. This watermarking scheme utilizes the benefits of both the watermarking aspects.

Basically, the applications of watermarking are authentication and fingerprinting. According to applications, watermarking schemes are classified as shown in Figure 1.5. Source-based watermarks are used for establishing identity of the owner. Here, a unique watermark is used to identify the owner. This type of watermark may also be used to determine any kind of tampering in a received image or other electronic data. A private watermark is extracted or detected by the authorized people only as because the key for extraction is private.

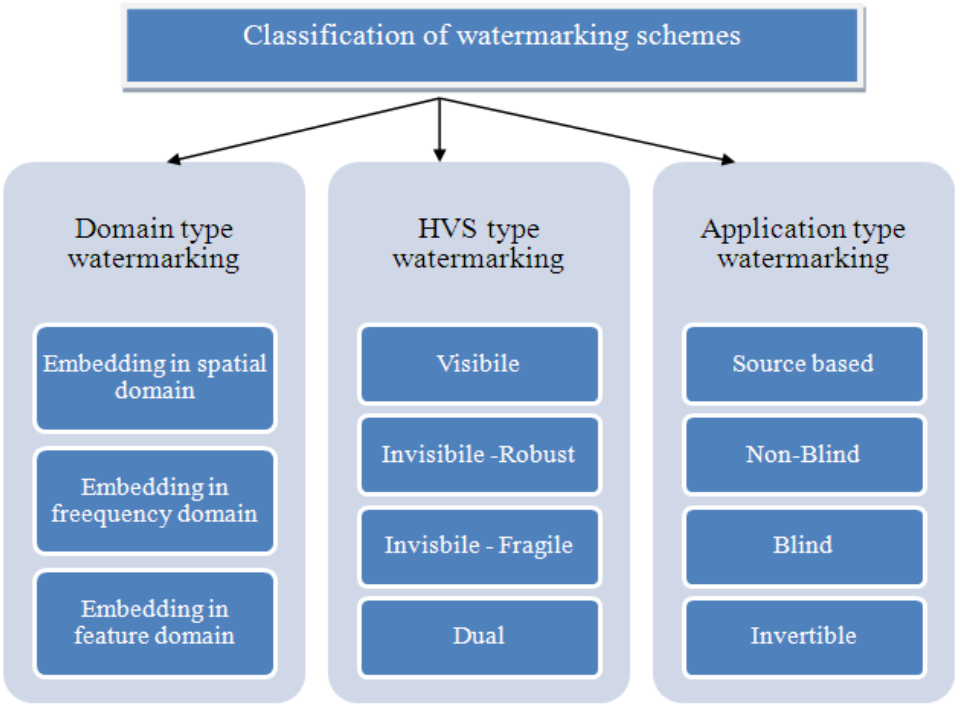


**Figure 1.5 Classification of watermarking scheme**

At the destination end, it is impossible to extract the watermark in the absence of the private key, so, unauthorized people could not extract it. In Blind Watermarking schemes, it is possible to extract the watermark from the watermarked signal without the use of the original signal. A watermarking algorithm is termed as non-blind if it requires original signal to extract the watermark from the watermarked signal. A watermarking technique is invertible if there exists an inverse mapping of embedding algorithm and the quality of the marked and non-marked document is similar [9].

## 1.3 REQUIREMENTS OF WATERMARK

A watermarking system has several requirements such as invisibility, efficiency, tamper resistance, robustness, low computation cost, high payload and low false positive rate [10] etc. But, designing a watermarking scheme that is equally effective for all is almost impossible. Obviously, different applications have different concerns. Therefore, there is no set of requirements which are same for all watermarking systems.

### 1.3.1 Invisibility

The invisibility of watermarking system means watermark should not be noticed by the human eyes. In other words, the cover medium which is being protected, should not be altered by the presence of the watermark. If invisibility is not ensured in a watermark embedding algorithm, the host signal (or image) will change its visual

appearance and its content. The embedding method that modifies the host signal will never be appreciated by the owner of the content. So, to protect the copyright material, the invisibility requirement is very important. The best way to evaluate invisibility is to conduct subject tests, where both original and watermarked signals are presented to human subjects [11]. Invisibility property is also termed as imperceptibility. The watermark is truly imperceptible if there is no visual quality difference between the marked signal and unmarked signal.

### 1.3.2 Watermark Payload

Watermark payload is the embedding capacity of the watermark. The payload is the maximum amount of data or information that can be embedded into the cover signal. It is usually expressed in bits per pixel (bpp). While referring to the payload capacity, the fidelity requirement is implicitly imposed. By modifying the characteristics of the cover image, we can be able to embed more information. But, this modification in the cover signal will deviate it from its originality that affects the fidelity. With reference to fidelity, properties of HVS are used to embed bulky size of data into the cover signal. Properties of the HVS provide knowledge about the domains that do not have a big effect on originality of the cover signal.

### 1.3.3 Effectiveness

Effectiveness in watermarking system refers to whether an extraction process is able to extract a watermark instantaneously by following the embedding process in reverse order [10]. It is often not possible to achieve a 100% of effectiveness if the watermarking system embeds the watermark using a random scheme. Bulk of the watermarking techniques are based on specific applications, so the effectiveness is replaced by robustness, invisibility, and security.

### 1.3.4 Robustness

Robustness property of watermarking system means that the embedded watermark should not get replaced, modified or distorted, if any image processing operation, manipulation or malicious attack is performed on the watermarked signal. In digital watermarking systems, one of the most widely tested properties is robustness. In most applications, preventing distortion in the watermarked signal before reaching the receiver end is unavoidable. It is a property as well as a requirement of watermarking that its applicability depends on the application area. To protect the copyright material, it is mandatory that embedded watermark should be extractable and/or detectable even after the signal is subjected to distortion, like compression, noise addition, filtering, and

distortion due to channel gains. Compromising robustness often increases the embedding capacity and thus is more tempting. Making a watermarking system robust against all signal processing operations is almost impossible.

### 1.3.5 Security

The main application of the watermarking system is to protect the illegal use and distribution of digital content. In other words, we can say watermarking is a security based method i.e. to secure the digital media from the unauthorized uses. However, the security of digital media becomes weak if the attackers can modify, replace or remove the watermark. Here security varies from application to application.

## 1.4 WATERMARKING APPLICATIONS

Over the past two decades, the research on watermarking is relatively increased. The reason for its development is its application that includes digital copyright management and protection [12-13], broadcast monitoring, tamper-proofing, content verification, copy control, and data integrity etc.

### 1.4.1 Owner Authentication

If a document or an image created by someone is being illegally used by any other person then, to protect the interest of the owner the only solution is watermarking. By using the watermarking process, it is easy to identify the changes made in the image or in the document, as it will not be possible to extract the original watermark from an unauthorized tampered copy.

### 1.4.2 Tamper Detection

A tampered image or documents can be used as presented as a proof of ownership in court of law or evidence to a forensic authority. So to identify whether an image is tampered or not, a suitable watermarking technique is best suited. If the image has been tampered, watermark extracted will not be the same as embedded one. Some of watermarking procedures are also intelligent to locate the tampered region.

### 1.4.3 Copy Control

The watermarks are used after owner's complaint that the original content of a file is modified or distributed illegally. Watermarks establish the ownership of the author and as regards control on copying the contents, there are some intelligent tools that can exercise control on copying and therefore can be used in association with watermarking for copy control. The cryptography technique is not able to prevent plagiarism of the original signals, after the receiver has used the legal key to decrypt [14]. Technologies

which permit to view the media but don't permit the media to be replaced or modified are need of the hour. There are some powerful copy protections tools developed by the researchers. Most of them have utilized the capability of the watermarking to control, open, download, copying, modified and print for the authorized users [15]. The unauthorized user cannot copy or modify even if they are able to open the document.

### 1.4.4 Fingerprinting (Transaction Tracking)

Digital watermarking can be utilized to discover the source of infringement of the patent or copyright agreement. The different digital watermarking algorithms use secret keys to embed watermark into the copies provided to diverse clients. A unique watermark gives an assurance about the possibility of tracing the customer who provided the copies of the product unlawfully to a third party. Fingerprinting is used as transactional watermark that allow a content distributor to recognize the source of an illegal copy by ensuring each legal copy has a unique watermark embedded. The owner can recognize the assailant, which misused the document or image by using this watermarking technology.

### 1.4.5 Broadcast Monitoring

Broadcast monitoring is both active and passive monitoring. Passive broadcast monitoring strives to identify directly the content being broadcast, whereas active monitoring relies on linked information that is broadcast along with the contents. Another possible application of broadcast monitoring is the detection of illegal (unauthorized) rebroadcasts of copyrighted material by pirate stations [16]. Digital watermarks can be used to automatically monitor broadcasting streams at satellite nodes all over the world and identify any illegal broadcast material. A unique watermark is embedded into each video or sound clip at transmission. Receiving station extracts the watermark to identify the exact location and time of each clip's broadcast. Verance's Confirmedia is the tool that used watermarking technique for broadcast monitoring and verification.

### 1.4.6 Device Control

Device control is basically intended to ensure protection of digital media from illegal distribution or copying [17]. This can be done by using watermarks to inform recording equipment i.e. what type of contents should not be documented. Patent license requires compliant players to check for watermarks in the content being played. Similarly, a digital watermark can be used to enable copy control devices. To use such techniques, manufacturers need to incorporate new encoders, which are guarded by patent law regulations in their devices to protect the global media market [18].

## 1.5 PERFORMANCE EVALUATION METRICS

The performance of digital image watermarking techniques is assessed by using parameters i.e. imperceptibility, data loss, robustness, and effectiveness. Imperceptibility and robustness can be measured by the Peak Signal to Noise Ratio (PSNR), Normalized Correlation (NC), Kullback–Leibler divergence (KL), and Percentage Residual Difference **(**PRD) [19-20]. Data loss and effectiveness can be evaluated by using Bit Error Rate (BER), Mean Square Error (MSE), and Structure Similarity Index Measure (SSIM) [21-22].

### 1.5.1 Mean Square Error (MSE)

MSE (Mean Square Error) is defined in equation.

$$MSE = \frac{1}{n*m}\sum_{i,j}(I_m(x,y) - I_w(x,y))^2 \quad (1.1)$$

Where $I_m(x,y)$ = original image pixel intensity at location $i,j$

$I_w(x,y)$= watermarked image pixel intensity at $i,j$ location.

$n * m$ = size of image $n$ no. of rows whereas m is no. of column of image.

### 1.5.2 Peak Signal to Noise Ratio (PSNR)

Embedding extra information in the original signal will cause degradation and perceptual distortion. The ratio between the maximum possible power of an original and the power of corrupting signal is called PSNR, which influences the fidelity of its representation. More PSNR means better similarity between two images or signals. The PSNR is generally represented in scale i.e. logarithmic decibel scale. Following equation shows the expression for PSNR:

$$PSNR = 20\log_{10}\left(\frac{Max_I}{\sqrt{MSE}}\right) \quad (1.2)$$

Where $Max_I$ represents the maximum possible intensity value of the cover image. The value of $Max_I$ is 255 for grayscale image. For color image expression of PSNR is the identical apart from the MSE value i.e the sum over all squared value divided by 3 and image size.

### 1.5.3 Normalized Correlation (NC)

Normalized Correlation between the extracted watermark and original watermark is used to evaluate the quality of the extracted watermark. Following equation shows the expression for NC coefficients:

$$NC = \frac{\sum_{i,j}((I_m(i,j) - I_w(i,j))}{\sum_{i,j}\sqrt{I_m(i,j)^2}} \quad (1.3)$$

### 1.5.4 Bit Error Rate (BER)

Bit Error Rate (BER) is the number of bit changed (error) during transmission. BER is the ratio of number of bit error and total number of bits transmitted for the duration of the time. The equation shows the expression for BER:

$$BER = \frac{\sum_{i,j} I_m(i,j) \oplus I_w(i,j)}{(m*n)} \tag{1.4}$$

In above equation $\oplus$ symbol is Ex-or operater.

### 1.5.5 Structure Similarity Index Measure (SSIM)

Although, PSNR and NC are appropriate to calculate and have an apparent physical meaning, but still, it does not associate strongly with the visual quality of the image for most applications [19]. The extent of perceptual quality is widened in the Structure Similarity Index Measure (SSIM) [20-21]. SSIM is the combination of three HVS properties namely luminance, contrast and structure. The HVS properties of two images are compared at every point. The values of SSIM are in [0, 1]. A value of 1 implies that the two images are highly identical and a value of 0 implies that there is no correlation between images. For calculating SSIM, compare the images by breaking them into a number of windows of B*B size. The two images being compared must be similar in size [22]. Considering $I_m$ and $I_w$ as two images, $m$ is the no. of B*B windows and $p$ is the number of pixels in each window, then SSIM may be defined by the equation:

$$\text{SSIM} = \frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)} \tag{1.5}$$

Where $\mu_x = \frac{1}{p}\sum_{i=1}^{n} I_m$ , $\mu_y = \frac{1}{m}\sum_{i=1}^{m} I_w$

$\sigma_x = \sqrt{\left(\frac{1}{p}\sum_{i}^{n}(I_m - \mu_x)^2\right)}$ , $\sigma_y = \sqrt{\left(\frac{1}{m}\sum_{i}^{m}(I_w - \mu_x)^2\right)}$,

$c_1 = (k_1 L)^2$,$c_2 = (k_2 L)^2$and $k_1$= 0.01, $k_2$=0.03,$L$= Intensity values in dynamic range (for grayscale image L =255)

### 1.5.6 MSSIM (Mean Structure Similarity Index Measure)

Mean SSIM is given as follows:

$$MSSIM = \frac{1}{m*n}\sum_{j=1}^{m*n} SSIM(I_m, I_w) \tag{1.6}$$

### 1.5.7 Percentage Residual Difference (PRD)

The percentage of relative squared difference between original and disturbed signals is called PRD. As the difference between the cover signal and the watermarked signal increases, there is a linear increase in PRD [23]. The equation shows the expression for PRD:

$$\mathrm{PRD} = \sqrt{\left(\frac{\sum_{i=1}^{N}(I_m - I_w)^2}{\sum_{i=1}^{N}(I_m)^2}\right)} * 100 \tag{1.7}$$

Where $I_m$, $I_w$, N represent original signal, watermarked signal.

### 1.5.8 Kullback–Leibler Divergence (KL)

Kullback–Leibler divergence (KL) is a metric that measure of distance between two original and distorted signals. KL divergence is a non-symmetric measure of the information lost [24]. KL divergence closely related to relative entropy, information divergence, and information for discrimination. Let $I_m$ is cover image and $I_w$ is watermarked image. KL divergence $D_{KL}$ is defined in equation:

$$D_{KL}\,(I_m I_w) = \int_{-\infty}^{\infty} I_m \log \frac{I_m}{I_w}\, dx \tag{1.8}$$

The benefit of using KL is that as it works in the frequency domain, [24] therefore, it can be used in conjunction with the other metrics.

## 1.6 TRANSFORMS

Normally, there are two domains for representing a signal or an image. First domain is called time-domain where signal is represented as a function of time and second is frequency domain, where signal is represented as a function of frequency. In time-domain the signal is plotted against one independent variable called time and other dependent variable called amplitude. But it is not very conducive for all types of applications, because this representation only gives the time and amplitude information which is in general irregular and contains more than one frequency. It does not provide any information related to frequency. As a result, the most important information that is in the form of frequency remains undetected (unseen) in this representation. Frequency domain representation gives various frequencies that exist and compose the signal. A transformation is needed to find the frequencies in the signal. There are several transforms such as Discrete Cosine Transform (DCT), Wavelet Transform (WT), Discrete Fourier Transform (DFT), Ridgelet Transform (RT), Curvelet transform (CT) and many more, which represent the signal in frequency domain. To understand curvelet transform,

it is mandatory to know about the basic transforms and their advantages and disadvantages. The brief introduction of these transforms is as follows

Fourier Transform (FT) is applied on raw signal to find the frequency amplitude spectrum of that signal. It shows amount of the presence of a frequency in the raw signal. The following equation shows the FT transform, that decomposes a time domain signal into complex exponential function of different frequencies.

$$Z(f) = \int_{-\infty}^{\infty} z(t) * e^{-2j\pi ft} \, dt \tag{1.9}$$

Where f = frequency, t = time, and $z$ = amplitude of the raw signal and j being the conventional representation for imaginary quantity i.e. $j = \sqrt{-1}$. If a transform can recover a time domain signal from its frequency domain signal than that transform is called reversible. The inverse FT is given below:

$$z(t) = \int_{-\infty}^{\infty} Z(f) * e^{2j\pi ft} \, df \tag{1.10}$$

Where $t, f$ and $z$ are same as in equation (1.9), here $Z$ represents the signal in frequency domain.

It is well understood that in FT there is no information of frequency at any instant of time when signal is in time domain, as well as if signal is in frequency domain it will not give any information related to time at any value of frequency. FT provided only frequency components of the signal, but does not tell which frequency component exist in which time. Accordingly, FT is appropriate transform for stationary signals, because in stationary signals frequency and time information are not required simultaneously. For non-stationary signals, FT provides the spectral content of the signal, but it does not provide any information as regards where in time those spectral components appear. Therefore, FT is not used for all type of applications.

To solve the above-mentioned problem of FT, some part of a non-stationary signal is assumed to be stationary. This revised version of FT is called Short Term Fourier Transform (STFT). STFT divides signal into small parts which are then treated as stationary signal. For implementing this, a window function *w* is used. The width of this window must be of the same size as the small part of divided signal. Firstly, we locate this window function at the starting of the signal, then multiply signal with window function. The result of this product resembles the FT of that signal. The window function would be shifted to a new successive location, and taking FT of the signal that is in the

window. This procedure continues until the window reaches the end of the signal by shifting step by step. The following equation summarizes the above said procedure.

$$STFT(t^{'},f) = \int_t \ [\, z(t) * v^{\circ}(t - t^{'})] * e^{-j2\pi ft} dt \tag{1.11}$$

In above equation $z(t)$, and $v \circ (t)$ are signal and window function respectively. A new STFT is computed for every $t^{'}$ and $f$. The equation also interprets that the STFT be simply a FT of the signal multiplied by a window function. FT of a real signal is always symmetric, therefore STFT is also symmetric in nature as STFT is nothing but a windowed version of FT [25]. It is concluded that, the STFT is true time-frequency representation of a signal. But, the STFT is not obeying the Heisenberg uncertainty principle, which states that it is not possible to represent the time and frequency of a signal together exactly. STFT can recognize the time intervals in which certain band of frequency exists and this problem is called resolution problem. The problem of resolution is basically the size of window. The problem of resolution is overcome by a new transform called wavelet transform.

Continuous Wavelet Transform (CWT) has a strong similarity with STFT. In CWT, signal is reproduced with window function and the transform is totaled separately for various segments of the time-domain. The width of the window is changed for every transform computed for signal spectral components. The CWT is defined in equation:

$$CWT\ (\tau, s) = \ \psi_x^{\varphi}(\tau, s) = \ \frac{1}{\sqrt{|s|}} \int x(t) \psi^{*} \left(\frac{t-\tau}{s}\right) \, dt \tag{1.12}$$

The transformed signal in the above equation is a function of two variables, $\tau$ and $s$, which are translation and scale parameters respectively. A mother wavelet $\psi(t)$ is the transforming function. Translation refers to the position of window as the window is shifted through the signal. Scale is defined as $\frac{1}{Frequency}$ and it either dilates or compresses a signal. Compressed signals are represented by small scales and stretched or dilated signals are represented by large scales. $\psi$, the mother wavelet is used for generating the other window functions. There are number of functions like Haar, Morlet, Mexican hat, Meyer, etc, which can be used as mother wavelet [26]. Here, wavelet means a small wave the smallness refers to the condition that this (window) function is of finite length (compactly supported). The wave refers to the condition that this function is oscillatory. The term mother signifies that the functions are derived from one main function.

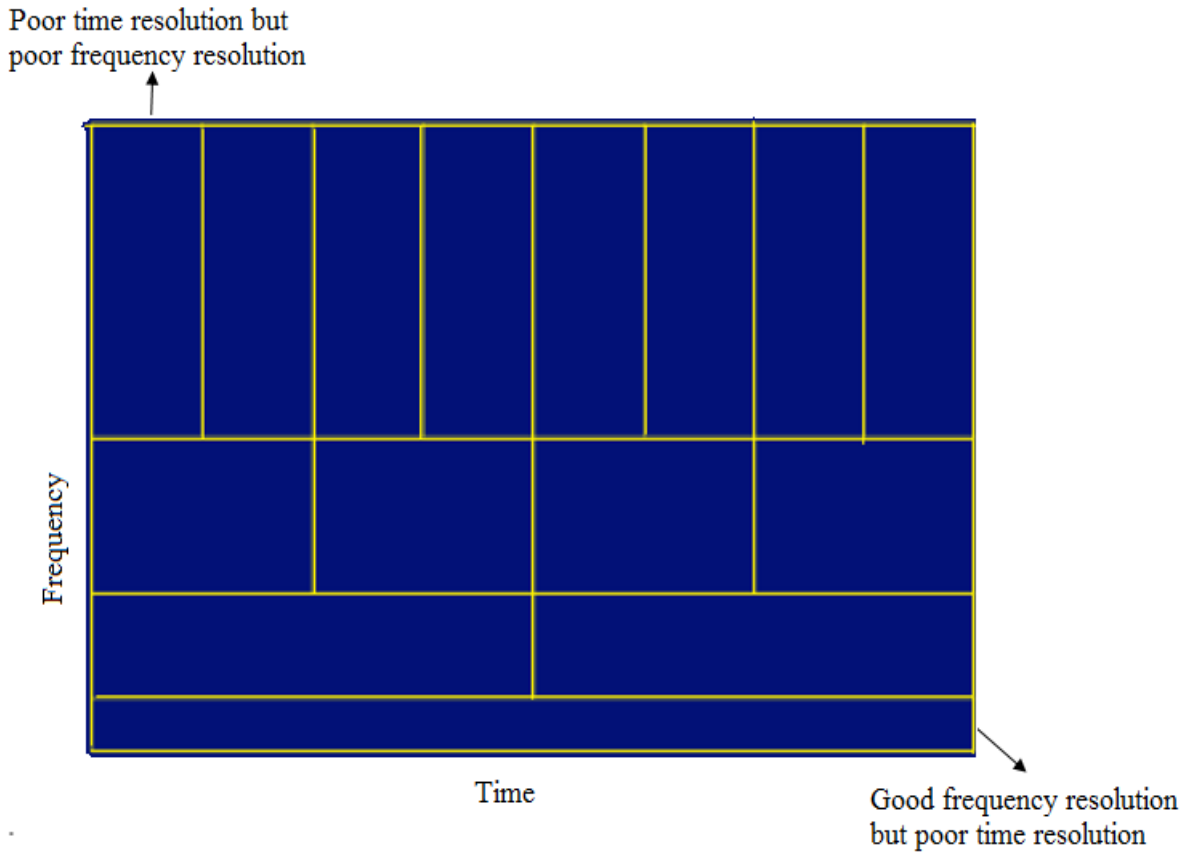


**Figure 1.6 Wavelet transform in the time-frequency plane**

Figure 1.6 is used to analyze the resolution properties of wavelet transform. This figure explains how we can understand time and frequency resolutions. Here, we observe that despite of the difference in heights and widths of the boxes, the area of each box is constant. Each box gives an equal portion of time-frequency plane, although representing different portion to time and frequency [27]. The shorter height of the box interprets better frequency resolution means less ambiguity regarding the information of the frequency. On the other hand, the longer width provides poor time resolution, which implies that there is more ambiguity regarding the information of the exact time.

Sufficient information is provided by the discrete wavelet transform (DWT), both for analysis and synthesis of the original signal in affordable computation time. The main aim of DWT is the same as CWT. Here, digital filtering techniques are used to find time-scale representation of digital signal. Signal at different scales is analyzed using filters of different cutoff frequencies. Low frequencies are investigated by passing the signal through a sequence of low-pass filters. As well as high frequencies are examined by passing the signal through a series of high-pass filters. The procedure starts with original signal $x[m]$ being passed through a half band high-pass filter $g[m]$ and low pass filter $h[m]$. As per Nyquist's principle half of the samples are rejected by using down

sampling. Now, highest frequency of the signal is half of its original frequency. This level of decomposition is shown by equations:

$$F_{high}[s] = \sum_n x[m] \cdot g[2s - m] \tag{1.13}$$

$$F_{low}[s] = \sum_n x[m] \cdot h[2s - m] \tag{1.14}$$

In the above equations $F_{high}[s]$ = high-pass filter and $F_{low}[s]$= low-pass filters. These filters $F_{high}[s]$ and $F_{low}[s]$ are the output after down sampling by 2. The connection between the impulse responses of the low-pass and high-pass filters is the most important property of DWT. The dependency of high-pass and low-pass filters on each other is shown in equation as:

$$g[L - 1 - n] = (-1)^n . h[m] \tag{1.15}$$

In above equation $h[n]$, represents low pass filter, $g[n]$ represents high pass filter and $L$ represents the filter length. Low-pass to high-pass conversion is provided by the $(-1)^n$ term. These filters are also termed as Quadrature Mirror Filters (QMF). Due to this property, they find a place in image and signal processing.

## 1.7 LIMITATION OF WAVELET TRANSFORM ON IMAGE REPRESENTATION

Now briefly conclude that wavelets perform extremely well for objects with point singularities, or with 1-D signal. We shall show that the same is not true with 2-D signals or objects with edge singularities. Let us calculate the number of wavelet coefficients for an object $f$on the square$[0,1]^2$. This object $f$ is smoothen away from a discontinuity along a $C^2$ curveΓ. A grid of squares of side $2^{-j}$ by $2^{-j}$ , $j = 1,2$ ..... has order $2^j$ squares intersecting Γ.In the 2D wavelet pyramid, at each level $j$, each wavelet (small waves) is limited to concentric square of size $2^{-j}$ by $2^{-j}$ . Therefore, around $O(2^j)$ wavelets are incoherence along Γ. Following equation is used to control such a wavelet coefficient:

$$\left|\langle f, \psi_{j,k_1,k_2}\rangle\right| \leq \|f\|_\infty \cdot \left\|\psi_{j,,k_1,k_2}\right\|_1 \leq C \cdot 2^{-j} \tag{1.16}$$

No better control is available, since the object $f$ is not smooth within the support of $\psi_{j,k_1,k_2}$ [28-29]. As a result, there are about $2^j$ coefficients of size about $2^{-j}$. We can also say that the $N^{th}$ largest wavelet coefficient is of size about 1/*N*. Wavelets representation is not sparse because, discontinuities across edges are spatially distributed. The summary of problems of image representation using wavelets is as follows:

i. Singularities along lines and along curves: It efficiently deals with point singularities, but it does not properly deal with singularities along lines and along curves, etc. Wavelets are not best for representing images that have discontinuities along curves [30].

ii. Fixed number of directional elements: Wavelets have two parameters one is translation and other is scale. There is no parameter for angle or orientation of edge. Wavelets have only a static number of directional elements which are not dependent upon scale of transform.

iii. Anisotropic Elements: Wavelets has limitation with scaling concepts. It does not have capability to represent anisotropic objects.

## 1.8 CURVELET TRANSFORM

Curvelet transform overcomes the limitations of wavelets. Wavelet transform is not able to represent objects having randomly oriented edges and curves as it could not representing line singularities. Curvelet transform is multi-scale and multidirectional transform. Candes and Donoho [30-31] developed the 1st generation curvelet transform in 1999. The need of a finer image analysis acted as a motivation for the development of curvelet transform. The performance of the first generation curvelet is slow. Second generation curvelet transform is introduced in 2006 which discarded the use of ridgelet transform. As compared to first generation curvelet the new curvelet transform is fast, simple and less redundant. Second generation curvelet can take highly anisotropic shapes obeying the parabolic scaling law: $width \propto length^2$.

### 1.8.1 1st Generation Curvelet Transform

The implementation of first generation curvelet transform is presented briefly. It comprises of following steps:

**Step 1: Sub-band decomposition**

The object, say f, is divided into several resolution layers which represent details of different frequencies using a band pass filter as defined in equation:

$$f \rightarrow (P_0 f, \Delta_1 f, \Delta_2 f, \Delta_3 f \ldots\ldots \Delta_s f) \tag{1.17}$$

Where $P_0$ and $\Delta_1, \Delta_2 \ldots\ldots \Delta_s$ are high and low pass filters respectively with s being a scale parameter. $P_0 f$ is the smooth low-pass layer and $\Delta_s f$(s>0) are high-pass layers. Figure 1.7 shows the sub-band decomposition of the image f.

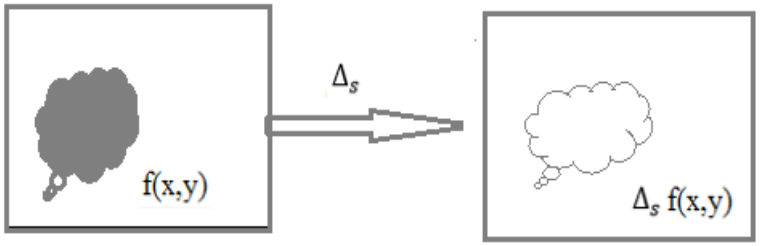


**Figure 1.7 Sub-band decomposition of image**

**Step 2: Smooth partitioning:**

A collection of smooth window $\omega_Q(x_1, x_2)$ localized around squares is defined in equation:

$$Q = \left[\frac{c_1}{2^s}, \frac{(c_1+1)}{2^s}\right] \times \left[\frac{c_2}{2^s}, \frac{(c_2+1)}{2^s}\right] \tag{1.18}$$

$\omega_Q$ = window function that produces a localized $Q$. For executing this for all $Q = Q(s, c_1, c_2)$, $Q$ = certain scale, with $c_1$ and $c_2$changing but $s$ remains fixed that produces a smooth partition of the function into squares. Figure 1.8 demonstrates the smooth partitioning of a high pass layer. Here the windowing dissection shown in equation below is applied to each of the sub-band isolated in the previous step.

$$\Delta_s f \mapsto \left(\omega_Q \Delta_s f\right)_{Q \in Q_s} \tag{1.19}$$

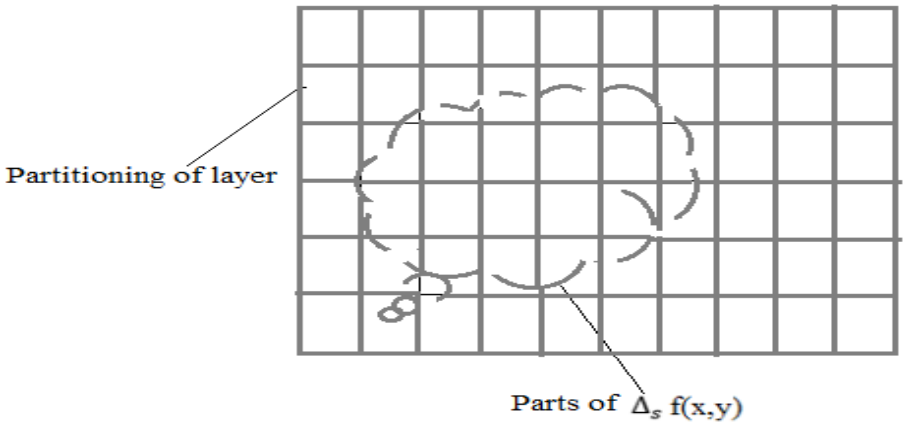


**Figure 1.8 Smooth partitioning of layer**

**Step 3: Renormalization**

A renormalized and transport operator $T_Q f(x_1, x_2)$ is applied to the object. The operator $T_Q f = 2^s f(2^s x_1 - c_1, 2^s x_2 - c_2)$. The main objective of applying this operator is to change the input sequence supported near $Q$ to output supported i.e. near $[0,1]^2$. Each square obtained from this is normalized into $[1,0] \times [0,1]$ (unit square). The squares

not containing any edge are dropped. Expression for renormalization is given in equation 1.20. Renormalization is shown in Figure 1.9.

$$g_q = \left(T_Q\right)^{-1}\left(\omega_Q \, \Delta_s \, f\right)_{Q \in Q_s} \tag{1.20}$$

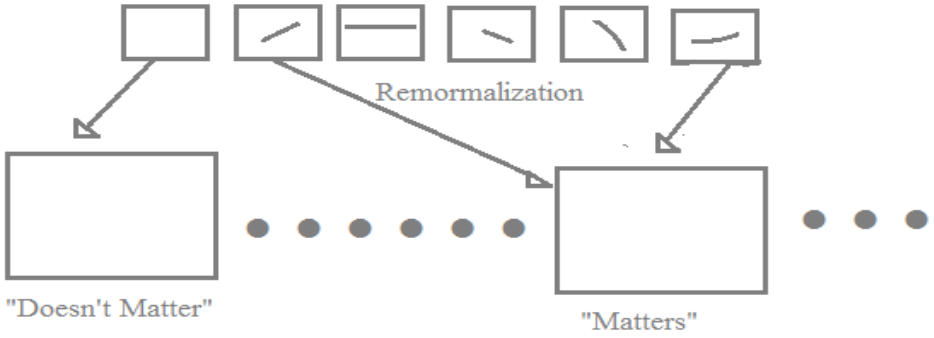


**Figure 1.9 Renormalization of each unit**

**Step 4: Radon Transform**

Decomposition of object and normalized square will represent data in the frequency domain. Then each square is now divided into coronae or wedges by plotting concentric square and redial lines as shown in Figure 1.10. Each coronae is Cartesian array of frequencies is converted into time domain by applying inverse FFT on it. The whole procedure is termed as Radon transform.

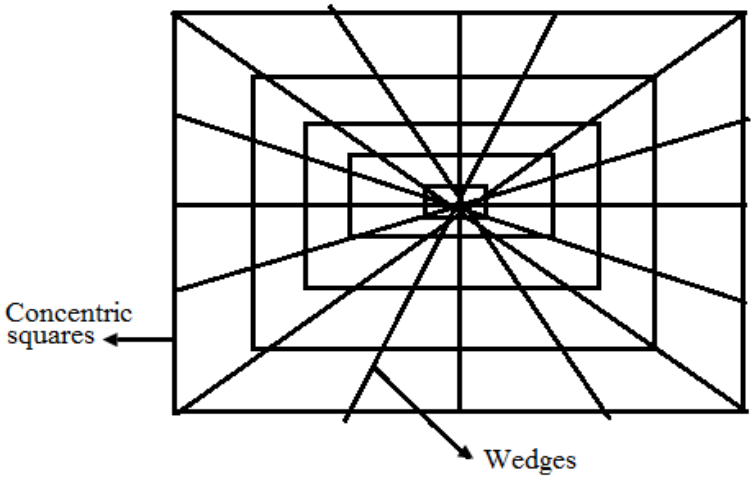


**Figure 1.10 Frequency domain concentric squares and wedges**

**Step 5: Ridgelet Transform**

Time domain values of radon transform are processed further by applying a 1D wavelet transform to each coronae at different scales and translation (DWT parameters). This way we get three parameters, namely scale, translation and orientation (angle). This

analysis is called ridgelet transform. The complete procedure as described above is called curvelet transform and the coefficients of ridgelet transform are called curvelet transform coefficients. The procedure described above is depicted in the Figure 1.11 for better understanding.

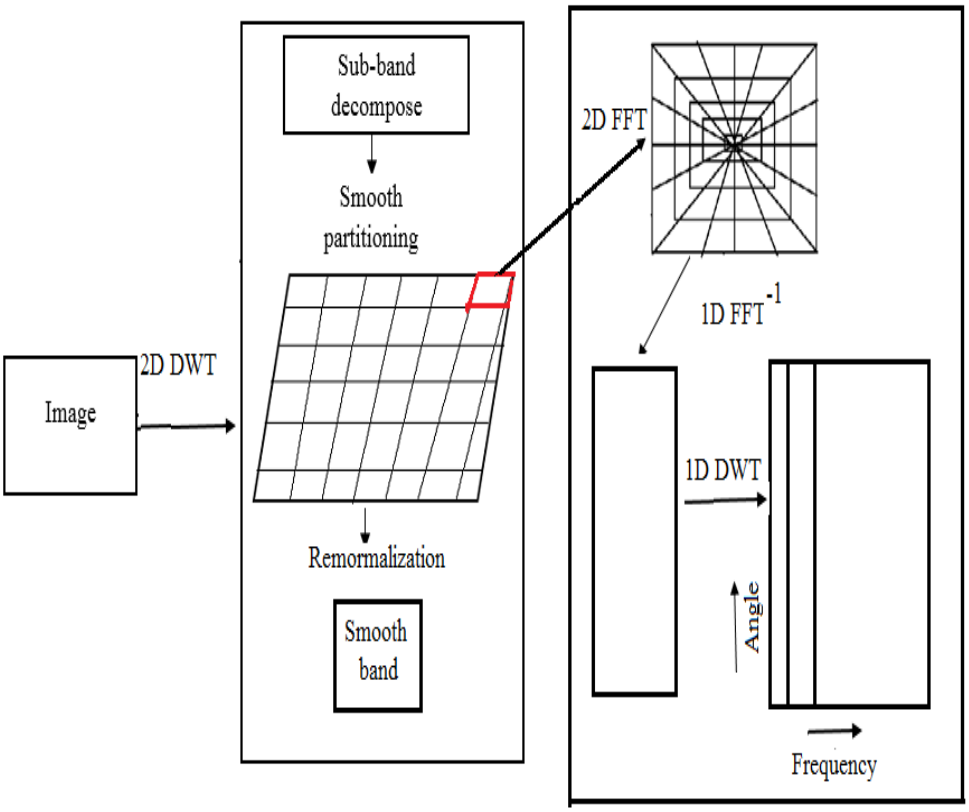


**Figure 1.11 First generation curvelet transform**

To comprehend the procedure let assume an $f$ image which exhibits $n$ numbers of edges. According to sub-band filter operator, thickness out to a width $2^{-2s}$ of each subsequent scale $\Delta_s f$ which map number of edges in object. Now the sub-band seems to be a collection of smooth ridges. After that each sub-band is smoothly divided into squares. It is noted that the unit square does not intersect a ridge (edge) fragment. It is observed that the object ridge fragments are straight in the square because edge is approximately straight at fine scales.

### 1.8.2 2nd Generation Curvelet Transform

This curvelet transform adds a new parameter namely orientation in the wavelet transform to represent the image in more efficient way. For analysis of images and signals 1D wavelet is converted into curvelet. For this purpose a function $\mu_{x,y}$ that is generated

by one other mother wavelet where $\left\{\mu_{x,y} \coloneqq 2^{\frac{x}{2}}\mu(2^x - k): x, y \in \mathbb{Z}\right\}$ and $\mu \in L^2(\mathbb{R})$. Each signal can be exclusively epitomized in a wavelet expansion equation given below:

$$f = \sum_{x,y} m_{x,y}(f)\mu_{x,y} \tag{1.21}$$

In above equation $m_{x,y}(f) \coloneqq \langle f, \mu_{x,y} \rangle$ are wavelet coefficients. To divide the frequency axis into octaves, wavelets are elementary property. If wavelet coefficients are smooth and localized then it is guaranteed that in spatial domain wavelet transform also provide localized property [32-33].

To overwhelmed the drawback of wavelet transform and for image analysis, curvelet transform combine definite orientation invariance. To construct a frame structure mainly orientation, dilations and translation parameters are used. These frames are obtained from basic curvelets. The elements of the curvelet family now divided into frequency band of the 2D frequency space. In Figure 1.12 demonstrate the wedges on circular ring. At each scale the number of wedges is $N_4 = 4 \cdot 2^{\lceil j/2 \rceil}$ [34-35].

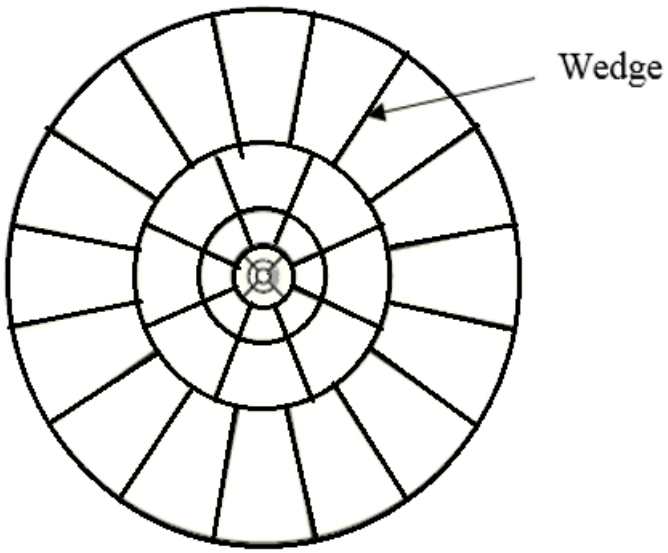


**Figure 1.12 Dividing of the frequency domain into wedges for curvelet construction**

Let's a function $\zeta = (\zeta_1, \zeta_2)^T$, and polar coordinates $r = \sqrt{{\zeta_1}^2 + {\zeta_2}^2}$ and $\omega = arctan\frac{\zeta_1}{\zeta_2}$ in frequency domain. Following equation represents the mathematical assumption is used for the widened elementary curvelets in polar coordinates:

$$\hat{\phi}_{x,0,0}(r, \omega) \coloneqq 2^{-\frac{3x}{4}} D(2^{-x}r)\, Q_{N,x}(\omega), \quad r \geq 0, \omega \in [0, 2\pi), j \in \mathbb{N}_0 \tag{1.22}$$

Here, a perfect window function $D$ and $Q_{N,x}$, and a rotation $\hat{\phi}_{x,0,0}$ are used. $N_j$ specifies the number of wedges in the circular ring at scale $2^{-x}$ as shown in Figure 1.12. To create

a basic curvelet, $D$ and $Q_{N,x}$, two window functions are used which give compact support to basic wedge. Here, we have $r \in [0, \infty)$, therefore, Meyer wavelet cannot be used to determine D, on the other hand only a portion that is supported in $\left[\frac{1}{2}, 2\right]$. So, D is redefined using the below-mentioned equation.

$$\sum_{x=-\infty}^{\infty} |D(2^{-x}r)|^2 = 1 \tag{1.23}$$

Further, N is a random progressive integer representing the tilling of a spherical ring into N wedges. Then here we required a $2\pi$- periodic positive window $Q_{N,x}$ with inside support, $\left[\frac{-2\pi}{N}, \frac{2\pi}{N}\right]$ as defined in equation 1.16 is satisfied.

$$\sum_{l=0}^{N-1} Q_{N,x}\left(\omega - \frac{2\pi l}{N}\right) = 1 \ \ for\ all\ \omega \in [0,2\pi) \tag{1.24}$$

The mathematical derivation of $D$ and $Q_{N,x}$ is giving [36]

So, we obtain the objective to acquire a set of curvelet functions in frequency domain on edges using this approach. In this, the circular ring, which parallels to the scale $2^{-j}$ . As depending upon the values $D(2^{-x}r)$, the summation of the squared curvelet function is given in below equation:

$$\sum_{l=0}^{N_x-1} \left|2^{\frac{3}{4}}\hat{\phi}_{x,0,0}\left(r, \omega - \frac{2\pi l}{N}\right)\right|^2 = |D(2^{-x}r)|^2 \sum_{l=0}^{N_x-1} Q_{N,x}\left(\omega - \frac{2\pi l}{N}\right) = |D(2^{-x}r)|^2 \tag{1.25}$$

Equations 1.24 and equation 1.25 show that the rotation of the basic curvelets, $\phi_{x,0,0}$, guarantee an admissibility condition. Since the orientation of the dilated curvelets depends only on the scales $2^{-x}$for j= 0,1,2 ... ... . It is also noted that the "hole" is around zero in the frequency plane. Taking all translated and orientated curvelets together with $N_j = 4 \cdot 2^{\lceil x/2 \rceil}$, The coefficients for each the scales $2^{-j}$, $j = 0,1,2$ ... ..... are obtained using below equation:

$$\sum_{x=0}^{\infty} \sum_{l=0}^{N_x-1} \left|2^{3j/4}\hat{\phi}_{x,0,0}\left(r, \omega - \frac{2\pi l}{N}\right)\right|^2 = \sum_{j=0}^{\infty} |D(2^{-x}r)|^2 \tag{1.26}$$

and this sum is $r \geq 1$. As a result, we are required to describe a low-pass element to cover the frequency plane. This represents in equations given below:

$$\hat{\phi}_{-1}(\zeta) = D_0(|\zeta|) \tag{1.27}$$

$$D_0^2(r)^2 = 1 - \sum_{x=0}^{\infty} D(2^{-x}r)^2 \tag{1.28}$$

Here, we need to determine the number of wedges that must be occupied in a single circular ring. Admissibility condition for a tight frame is the most crucial factor for

choosing the number of wedges in each scale. Curvelet transform is different from other transforms due to the important points discussed in [37-38].

i. By taking the number of wedges, that are counted using certain secure method, a steerable wavelet is obtained, and these are independent of the scale.

ii. A tight frame of ridgelet transform is attained if the number of wedges increases like $\frac{1}{2^{-x}}$.

iii. Curvelet is obtained, if the number of wedges increases like $2^{-x/2}$. $\sqrt{\frac{1}{scale}}$ thus is the important property and it's also called scaling law.

### 1.8.3 Digital Curvelet Transform

Digital curvelet transform is diverse from continuous because digital curvelet takes cartesian array as an alternative of polar tilling. This gives virtual concentric squares instead of circle as shown in Figure 1.13.

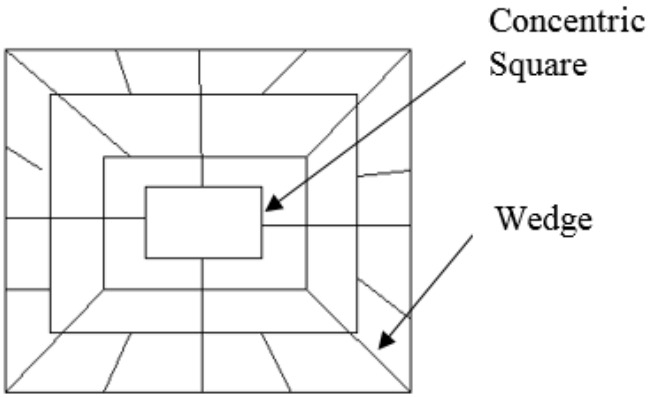


**Figure 1.13 Cartesian array on input**

Shearing replaces basic curvelet according to new tiling rotation as shown in equation:

$$\widetilde{\emptyset_{x,0,0}}(\zeta) = 2^{-3x/4} D\left(2^{-j}\zeta_1\right) Q\left(\frac{2^{-\frac{x}{2}}\zeta_2}{\zeta_1}\right) \tag{1.29}$$

The adopted basic curvelet $\emptyset_{x,o,o}$ determine the frequencies in the trapezoid as equation:

$$\left\{(\zeta 1, \zeta 2): 2^{x-1} \leq \zeta 1 \leq 2^{x+1}, -2^{\left\lfloor \frac{x}{2} \right\rfloor}.\frac{2}{3} \leq \frac{\zeta 1}{\zeta 2} \leq 2^{-\frac{x}{2}}.\frac{2}{3}\right\} \tag{1.30}$$

For replacing spin of curvelet elements by trimming in the different grid, it required to cogitate the cones of each side separately instead of equi-spaced angles. We define equi-spaced slopes for all cones $tan\theta_{x,l} = l2^{-\lfloor x/2 \rfloor}$ where $l = -2^{\lfloor x/2 \rfloor} + 1 \ldots\ldots\ldots 2^{\lfloor x/2 \rfloor} - 1$. Now the curvelet like function be given in equation:

$$\varphi_{x,y,l}(g) = \varphi_{x,0,0}(S^{t}_{q,x,l}(g - b^{x,l}_{y})) \tag{1.31}$$

with shear matrix $S_{q=}\begin{bmatrix} 1 & 0 \\ \tan\theta & 1 \end{bmatrix}$ and $b^{x,l}_{y}$ is defined as following equation:

$$b^{x,l}_{y} = S^{-t}_{q,x,l}(c_1 2^{-x}, c_2 2^{-x/2} \tag{1.32}$$

The digital curvelet transform is shown in below in equation:

$$\varphi_{x,y,l}(\zeta) = e^{-i(}b^{j,l}_{k}, \zeta)\, \varphi_{j,0,0}(S^{-t}_{q,j,l}, \zeta) = e^{-i(}b^{j,l}_{k}, \zeta)\, 2^{-3j/4} W(2^{-j}\zeta_1) Q(\frac{2^{-\frac{x}{2}}\zeta_2}{\zeta_1}) \tag{1.33}$$

We discovery the cartesian equivalent of the coefficients in equation:

$$\tilde{v}_{x,k,l}(f) = \int_{\mathbb{R}^2} \hat{f}(\zeta)\, \hat{\phi}_{x,0,0}(s^{-1}_{\theta,x,l}\zeta) e^{i(b_k^{-x,l},\zeta)} d\zeta, \quad c_j = \left(c_1 2^{-x}, c_2 2^{-\frac{x}{2}}\right) \tag{1.34}$$

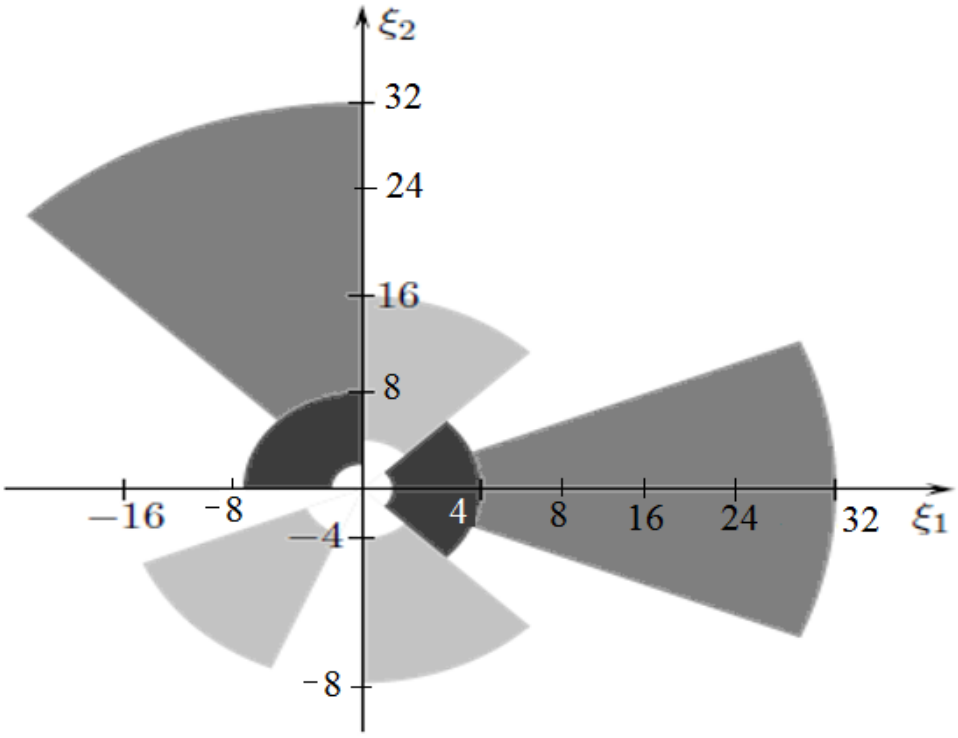


**Figure 1.14 Demonstration of $\hat{\phi}_{x,c,0}$. The grey part is support of $\hat{\phi}_{4,c,0}$, $\hat{\phi}_{4,c,11}$ where as light grey color shows the $\hat{\phi}_{3,c,3}$, $\hat{\phi}_{3,c,6}$, $\hat{\phi}_{3,c,9}$ and dark grey is $\hat{\phi}_{2,c,0}$ and $\hat{\phi}_{2,c,11}$**

### 1.8.4 Curvelet Properties

Now let's talk about the properties of curvelet elements. Rotation and translations are consider for basic element $\phi_{j,0,0}$ , to obtain the complete curvelet family [39-40]. For this choose rotation and position from following points

i. An equidistant sequence of rotation and $\theta_{x,l}$, $\theta_{x,l} = \frac{\pi l 2^{-\lceil x/2 \rceil}}{2}$ with $l - 0,1,2 \ldots\ldots N_j - 1$

ii. The position $P_c^{x,l} = P_{c_1,c_2}^{x,l} = R_{\theta_{x,l}}^{-1}\left(\frac{c_1}{2^x}, \frac{c_2}{2^{x/2}}\right)^T$ with $c_1, c_2 \in \mathbb{Z}$ and $R_\theta$ (rotation matrix) with different $\theta$ angles. Then the family function is derived by using equation below:

$$\phi_{x,c,l}(g) = \phi_{x,0,0}(R_{\theta,x,l}(g - P_c^{x,l})) \tag{1.35}$$

Where x$\in \mathbb{N}_0$ and $c = (c_1, c_2)$ and $l$ is as defined above.

It is noted that for each different orientation angle, the locations, $P_c^{x,l}$ are on diverse consistent grids. These grids have diverse arrangement which are reliable with the parabolic scaling las. A ratio of angles and scales is formula for parabolic scaling. This will result in a curvelet organization that forms a close-fitting frame. Curvelet transform will be invertible because all functions will be representable by a curvelet series. For understand it let us take an example for x= 0 , angles $\theta_{x,l} = \frac{\pi l}{2}$ here values of $l = 0,1,2,3$ and the locations$\{P_c^{x,l}\}k \in \mathbb{Z}^2$. For $x = 4$, the orientation angles $\theta_{o,l} = \frac{\pi l}{8}, l = 0 \ldots\ldots 15$ take place, and value of $l = 0, \ldots, 7$ is totally dependent on orientation angle $\theta_{4,l}$,.

The fundamental knowledge for the selection of the translation grids is described in this section. Let take a function , and this $\boldsymbol{f}$ is band limited. One another $\boldsymbol{h'}$ function witch is supported by wedge as shown in above Figure 1.14. To map wedge into the center of the frequency plane, now defined an orientation angle and a translation parameter. Then discovery $\mathbf{2^x \times 2^{x/2}}$ size of rectangle that cover the wedge. After all for covering the wedge, Shannon sampling is applied that gives the required sampling rate. Sampling rate given by Shannon is used to find the required locations. The different properties and support benefits are given below.

i. **Support in transformed domain:** $\hat{\phi}_{j,c,l}$ curvelet function is maintained in the polar wedge with different angles $\frac{2^{-\lceil x/2 \rceil}\pi\,(-1-l)}{2} < \omega < \frac{2^{-\lceil x/2 \rceil}\pi\,(1-l)}{2}$ and

radius $2^{x-1} \leq r \leq 2^{x+1}$. The location of $P_c^{x,l}$ is not affect the support of $\hat{\phi}_{x,c,l}$ .

ii. **Support in spatial domain:** The curvelet function $\phi_{x,c,l}$ cannot have compact support in spatial domain where as $\hat{\phi}_{x,c,l}$ has compact support in frequency domain. The smoothness of $\hat{\phi}_{x,c,l}$ in transformed domain is depend upon the decrement of $\phi_{j,k,l}(g)$. Smoothness of $\phi_{j,k,l}(x)$ is decrease botanically in spatial domain.

iii. **Oscillatory property:** As shown in Figure 1.4, $\zeta_1 = 0$ the horizontal axis $\zeta_2 = 0$ vertical axis, $\hat{\phi}_{x,c,l}(\zeta)$ is supported. Therefore, function $\phi_{x,0,0}(g)$ is precise oscillatory in $x_2$-direction and less oscillatory in another direction

iv. **Tight frame property:** every function $f \in L^2(\mathbb{R}^2)$ can be epitomized as a curvelet coefficients as shown in equation:

$$f = \sum_{x,c,l} \langle f, \phi_{x,c,l} \rangle \, \phi_{x,c,l}, \tag{1.36}$$

and the Parseval identity is given in equation:

$$\sum_{x,c,l} \left| f, \phi_{x,c,l} \right|^2 = \|f\|^2_{L^2(\mathbb{R}^2)}, \tag{1.37}$$

Terms $c_{x,c,l}(f) = \langle f, \phi_{x,c,l} \rangle$are called curvelet coefficients. We obtain curvelet coefficients using equation below:

$$C_{x,c,l}(f) = \int_{\mathbb{R}^2} \hat{f}(\zeta) \hat{\phi}_{x,0,0} \left(R_{\theta_{x,l}}, \zeta\right) e^{i(P_c^{x,l}, \zeta)} d\zeta \tag{1.38}$$

## 1.9 MOTIVATION AND PROBLEM DESCRIPTION

Now a days, the world has developed in digital era due to advancement in information and communication technology. In every fraction of a second, gigabytes of digital information is generated, transmitted and copied with the help of internet or electronic gadget like mobile phones and computer. Also, the uprising in medical and health field is brought by development in internet and communication technology. E-health technology and related principles demand sturdy protection and authentication of medical information worldwide. An obvious serious issue that has surfaced is the reliability of digital content. Digital image data security is achieved by diverse ways. Digital image watermarking technique is an effective and active branch of information hiding. It is used for protecting the privileges of the proprietors in number of ways including copyright identification, automated monitoring, authenticity determination, copyright protection, user identification and fingerprinting,. This research work is

motivated by several applications which required robust security by embedding information into cover data. Image data security is an essential requirement in many application areas because of advancement in communication technology and extensive usage of electronic gadget and internet. Thus, need of the hour is to produce highly secure, strongly robust data with high data hiding capacity and blind watermarking methods for greyscale, medical and RGB images. The inspiration leads to the problem declaration of the research is as follows:

"The primary objective of this work is to build blind, semi-blind, non-blind, secured, robust and perceptually transparent digital image watermarking system in curvelet transform domain by embedding high capacity payload in an image".

### 1.9.1 Gap Analysis

In past image is represented with point singularities in one-dimensional space but recently representation image with line singularities in two-dimensional space and also try to represent of signal with curve singularities on higher dimensions. Wavelet transform cannot represent line singularity because it has only two directional elements namely scale and orientation. Wavelet also fails to represent anisotropic elements such as edges and curves. The Human Visual System (HVS) concepts and advantages are utilized to illustrate the use of embedded information as a masking phenomenon with limits of non-visibility. Much research has been done on increasing the robustness and the data hiding capacity of watermarking techniques based on perceptual properties of the HVS. In this work, we consider the texture, luminance, corner and edge information of an image for creating a mask that will make the watermark addition to the image less perceptible to the human eyes. The embedding and extraction are done in frequency domain by using curvelet transform. The development and improvement of accurate human vision models helps in the design and growth of perceptual masks that can be used to better hide the watermark information thereby increasing its security. Analysis of algorithms is based on image quality only but recently analysis of algorithms is based on image quality, extracted watermark quality, watermark payload and robustness. The following are current challenges:

- To maintain balance b/w imperceptibility, robustness, and capacity. Because by increasing one, it will affects the other.
- To reduce false positive rate

- To use of digital watermarking techniques in different applications as it provides tool to establish authenticity.

### 1.9.2 Research Objectives

The following are the objectives for the proposed research work.

1. To compare and analyze existing digital watermarking techniques
2. To propose a new digital watermarking technique to satisfy the requirements such as invisibility, robustness, quality of the image and the quality of extracted watermark.
3. To develop an efficient digital watermarking algorithm based on the proposed technique.
4. To compare the robustness of the proposed algorithm with existing ones.

## 1.10 THESIS CONTRIBUTIONS AND ORGANIZATION

Watermarking techniques for embedding watermark in the curvelet transform is the underlying idea of this thesis. The main aim of these techniques is to utilize the properties of curvelet transform and show that these are more suitable for hiding the watermark in more robust and invisible manner. To achieve this aim, many robustness tests are carried out and the performance of each algorithm is verified by evaluation of performance metrics. With emphasis on the techniques, the results of the proposed techniques are compared with several existing techniques and analyzed.

This thesis contains in total six chapters. The basic aim of each chapter is to explore the application of watermark in different types of problems in order to improve the results. Each chapter deals with different applications. First chapter as usual is introduction. This chapter gives brief description of watermarking, a review of transforms and explaining curvelet transform in detail. The second chapter is titled as Survey of the Literature. The chapters 3 to 5 give the non-blinds, semi-blind and blind watermarking techniques for applications of curvelet transform to different problems with along experimental results. The chapter 6 gives conclusion and future work. The brief description of each chapter is given below:

**1. Introduction**

In this chapter, the basic concepts of watermarking are introduced. Its uses and applications are explained in detail. This chapter also introduces curvelet transform going through the stages of DCT and wavelet transform. Description of curvelet transform

along with necessary mathematical details is presented. Benefits of curvelet transform for better representation of images are highlighted.

**2. Survey of Literature**

This chapter includes an extensive literature review related to the thesis research area. The literature survey is classified in two domains, namely spatial and frequency domain.

**3. Non-blind Watermarking technique**

This chapter contains two non-blind watermarking techniques. The first one is an application to gray scale image, where the results are compared with wavelet transform and the effect of variation of scale is also investigated. The second technique uses texture blocks of image to hide watermark in curvelet domain. The hiding of data by this technique has more advantages over conventional methods.

**4. Semi-blind watermarking techniques**

This chapter describes two semi-blind watermarking techniques for color images. The first technique utilized the concept of HVS and bit plane for embedding the watermark into the curvelet coefficients. The results obtained are compared with the other transforms. The second technique combines the technique of cryptography and watermarking for application to a color image. It has been shown that this procedure results in more robust watermark.

**5. Novel Blind watermarking techniques**

Two watermarking techniques one for a forgery detection technique and another for securing patient information into ECG signals are proposed in this chapter. The First technique not only detects the forgery but also locate the modified or tampered region. The second blind watermarking technique is proposed for application of curvelet transform to medical images e.g. ECG, MRI, X-Ray and etc. Here an ECG has been used as an example and the patient information is used as watermark. The results are compared with other transforms and discussed.

**6. Conclusions and Future Scope**

# CHAPTER -2

# LITERATURE REVIEW

In this chapter, an exhaustive and systematic review of the literature in the area of watermarking is presented. This includes different techniques, some standards, books, research papers, technical notes and some other resources from the internet. The literature of watermarking is classified into two domains of embedding:

i. Embedding keen to the spatial domain
ii. Embedding keen to the frequency domain.

## 2.1 WATERMARKING IN SPATIAL DOMAIN

Spatial domain specified the image in time domain, where the pixel intensities are a true representation of the image. The randomly selected pixel intensities of an image are utilized to hide the watermark into the image. There is a minor change in the intensities of the image. But it will not affect the visual quality of the image. The main advantage of spatial domain embedding is its easiness to implement. The disadvantage of the spatial technique is that it does not provide good robustness beside image processing attacks [41]. There are various methods used to modify image intensities, such as embedding in LSB, spread spectrum, correlation based, etc. The following section gives a brief introduction towards the approaches of spatial domain.

### 2.1.1 Embedding in Least Significant Bit (LSB)

The easiest technique in the spatial domain is Least Significant Bit modification method. As the Most Significant Bit (MSB) represents the color and all other bits represent the shades of that color, the LSB does not contain so many values. So, LSB of image is used to embed the watermark. Macq and Quisquater proposed a technique to embed the watermark into the LSB of pixel intensities located in the surroundings of the

image edges [42]. But as the LSB bit is modified by the watermark, so it is not robust against image processing attacks. Rhoads and G. B. introduced a technique that embeds the watermark by addition and subtraction of a random number sequence from the pixels intensities [43]. By comparing the binary mask, the random sequence is added or subtracted from the pixel intensities. If the binary mask is equal to the LSB, after that the random sequence is added, if not, it is subtracted. This technique provides high imperceptibility to watermark and some robustness. But this does not overcome the collusion attacks problem.

### 2.1.2 Correlation Based Watermarking Schemes

One more method in the spatial domain is to use the correlation properties of random noise. A random noise sequence (SN) is embedded into the host image I. A gain factor g gives the strength to the watermark and resulting image is named as watermarked image $I_w$. Embedding of watermark using correlation is given below:

$$I_w(x,y) = I(x,y) + g * SN(x,y), \quad x,y = 1,2 \ldots \ldots \ldots \quad (2.1)$$

The gain factor gives the strength to the watermark to resist the image processing attack. The invisibility of watermark is proportional to the gain factor and robustness. The embedded noise sequence is random. A generator is used with same key to make a correlation between watermark image and noise sequence [44]. At the receiving end the correlation value is compared with certain threshold value. If this value is less than the correlation value, then a single bit of watermark is detected. This approach can also be used to embed multiple watermarks by decomposing the image into blocks.

### 2.1.3 Patchwork Based Watermarking Schemes

Another technique in the spatial domain is based on patchwork. Bender et al. [45] introduced this patchwork technique in which a pair of points is randomly selected from the image. The brightness of one point is increased by one unit, whereas decreasing the pixel intensity of other point. Another embedding procedure is described as "texture block coding" in which, by using autocorrelation, a random texture pattern is selected. This texture pattern is copied into the image area. The main problem with this technique is that it is not applied for smooth images. There are some more algorithms [46-47] that are based on this patchwork.

### 2.1.4 Spread –Spectrum Watermarking Schemes

In spread spectrum, the watermark is embedded in each bit randomly all over the cover image. The watermark is in the form of a vector and by using the independent seed a PN sequence is generated. The seed is used as a key of embedding. At the time of

extraction, this seed is used to generate the PN sequence and after that, this sequence correlates with the cover image [44-45]. The watermark is present in the cover if the correlation is high, otherwise, there is no watermark. Yeung and Mintzer's is a pioneer of side information technique [48]. Here, the watermark is hide by modifying the pixel values which luminates, as a result, and becomes a function of extraction. Because of the luminance of the modified image, the embedded watermark will become the detection function. For extraction, the detection function is selected from a secret lookup table. The main problem of this technique is the randomly generated watermark that embeds in the spatial domain, which is not robust against the compression and filtering image operations. The solution of this problem is provided by Su and Girod by using perceptual masking [49]. They also demonstrated that to make watermark resistant against filtering, the spectral uniqueness of the cover image is matched with the watermark. Spread spectrum provides a robustness of the watermark as well as increases the embedding capacity without losing the visual quality, but its computation cost is very high.

### 2.1.5 Some Other Spatial Techniques

Voyatzis and Pitas [50] introduced a chaotic spread watermarking technique. In this technique, each pixel of the watermark image is mapped with the cover image. To embed the watermark, an appropriate function and neighbor pixel intensities are used. The time of extraction for the same function determine the watermark value. The other method is proposed by Pitas [51], using the cover image divided into two parts. In one part, the watermark is added by a constant strength parameter, k. For the extraction of watermark, difference of the mean values is calculated. If the difference is equal to k, then watermark value is detected as one, otherwise, the watermark value is zero. But this method does not provide robustness against image processing attacks. So, to increase the robustness in the above method, grouping of pixels is introduced in [52]. In this approach, an optimization algorithm is used to calculate the embedding value for each pixel to unitize the low frequencies and make sure the invisibility of the watermark. Probabilities approach to detect false negative and false positive is introduced by Kalker et al. [53]. The ratio of the watermark and the cover image power is represented as the probabilities of the technique. Several spatialdomain watermarking techniques for images are proposed in [54-56].

## 2.2 WATERMARKING IN TRANSFORM DOMAIN

As compared to the spatial domain, transform domain provides robust watermarking techniques. In transform domain, instead of modifying the pixel intensity, the frequencies of the cover image are modified to hide the watermark. Adding watermark in the frequencies of cover image gives more invisibility and robustness against the image processing attacks. The transformations involved in watermarking are common, which include Discrete Cosine Transform (DCT), Fourier transform (FT), Ridgelet Transform (RT), Digital Wavelet Transform (DCT) and much more.

### 2.2.1 DFT Based Watermarking Schemes

The first transformation is DFT. Here, we start the literature of watermarking using DFT. To embed watermark, some authors modified the DFT coefficients and phase coefficients. Ruanaidh et al. [57] introduced a robust watermarking method, in which watermark is inserted into the phase coefficients of DFT. Afterward, Ruanaidh and Pun [58] examined the novel watermarking method by using Fourier-Mellin transform. Fourier-Mellin transform is correlated to apply DFT to the log-polar coordinate system of the host image. This technique is robust against noise and filtering operations.

De Rosa et al. [59] projected a robust image watermarking method in which the authors utilized middle-frequency components of DFT to hide the watermark. The watermark resists to the compression like Set Partitioning in Hierarchical Trees (SPIHT) and Joint Photographic Expert Group (JPEG). Ramkumar et al. [60] hided the watermark in the magnitude of DFT coefficients. Their experimental results proved survival of watermark under compression operation. By utilizing the magnitude of DFT components, the watermark is robust against the image processing attacks. Lin et al. [61] embedded the watermark by re-sampling the log-polar mapping of DFT coefficients. In this technique, the watermark is not robust against compression and cropping operations. Solachidis and Pitas [62] presented a robust watermarking method that uses a circular watermark and embeds it into the DFT coefficients. In this method, the watermark shape is circular and it is hided into the middle coefficients of DFT domain. By use of this approach, the watermark is recovered from the rotated image. A semi-blind digital watermarking method is proposed by Ganic and Eskicioglu in which copy of watermarks are embedded into the DFT domain [63]. The original watermark is embedded by inserting the watermark to the lower frequency of DFT and copies of the watermark are hided into the higher coefficients of DFT domain. To reduce the time and space complexity of the watermarking technique, Pereira et al. uses a Fast Fourier Transform (FFT) that provides resistance to compression and filtering attacks [64].

### 2.2.2 DCT Based Watermarking Schemes

Cox et al. investigated that watermark should resist against the image processing operation [65]. It must be situated in perceptually significant areas of the cover image. Cox generated a watermark which was a combination of thousand random distributions. This watermark was hided into the largest coefficients of DCT of the cover image. To generate the watermarking image, inverse DCT is required. For the extraction of watermark, the DFT coefficients of cover image are subtracted from watermarked image. Afterward, Huang et al. declared that the DC coefficients have the larger perceptual capacity than any AC coefficients, so they investigated a method of embedding in DC components [66]. But this technique is not suitable for the large-sized watermark. DC coefficients of DCT transform are utilized as the embedding domain because they give more imperceptibility to watermark. A coding technique is used to hide the watermark into the DCT coefficients of the host image [67]. Chen and Wang combine the properties of digital signature and watermarking for authorization of image [68]. To increase the imperceptibility of the watermark, Das et al. introduces a method, this method utilized the Just Noticeable Difference (JND) and DCT coefficients [69]. In this method, the watermark is hide by analyzing the Just Noticeable Difference (JND) of the neighboring coefficients of DCT domain. Koch et al. introduce a method of pulse position modulation and multiplemodulations [70]. In this method, the author applied DCT on 8*8 blocks and randomly selected the DCT blocks for embedding the watermark. From these blocks, three coefficients of mid frequencies are selected by using the key. From these selected frequencies, author embedded the watermark. Lin and Delp proposed a method in which thewatermark is generated by using Gaussian method with zero average and unit variance [71]. The generated watermark is localized in each 8*8 blocks. As a result, the watermark is embedded in each 8*8 blocks, but the sharing of the watermark in all DCT blocks is same. This property makes watermark more imperceptible as well as robust against compression operation. Fridrich [72] proposed a technique in which the cover image was decomposed into 16×16 blocks [72]. It is mentioned in the paper that there are total N 16*16 blocks in the cover image. A watermark of K*N size is generated by using a secret key in which entries are equally distributed in the interval [0, 1]. Zhang et al. presented a watermarking technique that hides a watermark sequence in the low frequency (DC coefficients) and high frequency (AC coefficiencies) in the DCT domain [73]. Licks et al. proposed a different circular symmetric watermarking technique that requires an exhaustive search at the time of extraction [74]. Stankovic et al. embedded multiple

watermarking by means of a 2D radon –Wigner distribution [75]. Choi et al. and Luo et al. use inter-block correlation to insert the watermark into the chosen DCT coefficients [76-77]. The cover image is JPG image and the DCT coefficients of cover image are modified by subtracting or adding the mean value of the nearest coefficients.

### 2.2.3 Wavelet Transform Based Watermarking Schemes

The wavelet transform is a multi-resolution transform that describes the image in a more convenient way. In wavelet transform, an image can be represented at distinct level of resolution. The image can also be processed from low to high resolution. Like DCT, wavelet transform does not split the image into blocks to get the DCT coefficients. As a result, the visual artifacts represented by wavelets transform are less evident. Any change in the DFT or DCT transform components will affect the whole image apart from block-based DCT. On the other hand, changes in Discrete Wavelets Transform coefficients will only affect the image locally. This property of DWT is called spatial frequency locality. As a result, DWT offers both spatial and frequency description of an image. Other than these qualities, DWT has many features that understand and implement Human Visual System (HVS) more strongly than the DCT. As per these above-said advantages, many authors utilized the wavelet transform in digital image watermarking.

Wang et al. demonstrated a blind watermarking method based on wavelet casting [78], in which, firstly determine significant wavelet transform sub-bands and then use perceptual watermark casting method to select perceptual important wavelet coefficients from the generated sub-bands. For watermark energy, the author also used weighting factor that effortlessly adjusted the reliability of the watermark sequence. Perceptually significant coefficients give invisibility to watermark as well as a higher tolerance for the attacks. Kundur and Hatzinakos introduced a secure watermarking method for tamper proofing and authorization of digital image [79]. A 64-bit secure credentials key is used to select the scaling function of the wavelet transform. The DWT decomposing is applied on the cover image as per the key. Again, the same key is used to select the decomposition levels with the location of the coefficients that are used to hide the watermark. To embed the watermark quantization is used in which 1s are hide by even quantization of the chosen coefficients, whereas the 0s are hide by odd quantization. A semi-fragile watermarking for color image certification is presented by Kostopoulos et al. [80]. This technique takes benefit of $YC_bC_r$ color plane instead of RGB color plane. Firstly, the 24-bit RGB color plane cover image is transformed into $YC_bC_r$ color plane. The luminance components allow the restoration of tampered regions, so author utilized it

to embed the watermark. To improve the space complexity, the brightness of the image is encrypted into 8-bit pixel intensity and it rejected the two LSB bits. Paquet and Ward also proposed digital image authentication method based on the DWT [81]. Barni et al. presented a novel wavelet based watermarking method using pixel–wise masking [82]. The authors masked the watermark bits according to the uniqueness of the HVS. This technique inserts the watermark bits by modifying the wavelet coefficients of the cover image.

Hien et al. [83] presented a robust logo watermarking method. In this method, watermark is embedded into the frequencies of Discrete Wavelet Transform (DWT) of the cover image. By utilizing the properties of Independent Component Analysis (ICA), blind extraction method is also proposed. This algorithm can detect and extract the watermark from the noised, compressed or filtered watermarked image. Pla et al. introduced image independent watermarking technique that embeds a watermark into the most significant coefficients of DWT domain [84]. The authors also used the visual adaptive technique to embed the watermark. To provide robustness against the compression, median filtering, and sharpening operations a noise sequence is inserted into the watermark. To determine the watermark coefficients, a hierarchical tree structure is used. Lu et al. presented a technique, which uses multilevel vector quantization for embedding multipurpose watermark in the image [85].This algorithm proposed a novel, semi-fragile and robust watermarking technique that embeds a watermark using multistage vector quantization. The emphasis of the technique is not only to provide a robust and invisible watermark, but also to provide versatility to copyright material. The authors planned to include one more constraint for watermark bits dissimulation. This embeds the watermark bit in the location that initiates the smallest possible further distortion. Three novel, as well as a blind watermarking schemes for a digital image, were proposed in [86].

John N. Ellinas investigated that distortions are less perceptible on edges [87]. So, to embed the watermark, an edge detection method and wavelet transform are used. The wavelet coefficients are selected around edges and watermark is inserted into the chosen coefficients with dissimilar scale factor and watermark strength parameter. The wavelet coefficients are selected by using the morphological dilation operation. Watermark strength parameter provides resistance to attacks and this technique provides good invisibility and robustness to watermark. Jumma et al. combined the DWT and DCT transforms for protecting the digital image from tampering [88]. Holliman et al.

introduced a collage; it is an attack against image authentication [89]. By using this collage, a fraudster can unite independently genuine blocks to produce counterfeit content. Preda overcame the drawbacks of the block based scheme using DWT based approach and random variation [90]. Guo and Prasetyo presented a watermarking method used redundant discrete wavelet transform and Singular Value Decomposition (SVD) [91]. Here, a redundant discrete wavelet transform is implemented on host. The SVD values of the transformed image are modified by adding the intensity value of grayscale watermark. This technique provides more invisibility to watermark as it uses redundant discrete wavelet transform. It also provides robustness to watermark by exploiting the SVD stability property.

### 2.2.4 Curvelet Transform Based Watermarking Schemes

In literature, many authors embedded the watermark in the wavelet domain. Although wavelet transform has been explained broadly in image processing, but due to the problem of representing line singularity, it fails to represent edges and curves. The wavelet transform is not suitable for describing anisotropic elements. It includes only two directional elements. It means transform is independent of scale. The disadvantage is overcome by the ridgelet transform. This transform gives idea to plot a line singularity in the 2-D domain using a point by means of a RT. There are also some watermarking techniques which are based on the ridgelet transform. But ridgelet transform cannot well represent curve edges. So, curvelet transform is developed. Curvelet transform [31] provides bare representation of needle-shaped elements and it is anisotropic properties. Thai Hien et al. proposed a method of embedding the watermark in the curvelet transform, containing maximum edge information [92]. This proposed technique gives good imperceptibility but the watermark does not survive under image processing operations. To increase the robustness, Thai Hien et al. proposed one more watermarking technique which utilized the threshold parameter for embedding the watermark in curvelet coefficients [93]. This technique gives invisibility and robustness to watermark. Shi et al. proposed a semi-fragile watermarking algorithm by embedding the watermark in the supreme model of curvelet coefficient [94]. This algorithm provides good robustness against a compression operation. Zhang et al. proposed a watermarking technique using a genetic algorithm and curvelet transform [95]. In this, the watermark is inserted into the coarse coefficients having a higher value than the optimum value of the threshold. This optimization of the threshold is selected by using the genetic algorithm and a strength parameter used to provide good robustness. One more approach by using

curvelet transform is proposed in Zhang et al. [96]. In this, the author utilized the HVS and curvelet to embedding watermark. The work is extended by Leung et al. [97] that uses Hamming code and contrast sensitivity function of HVS to estimate the Just Noticeable Difference (JND) threshold. Xiao et al. also proposed a robust watermarking method by considering frequency and orientation sensitivity [98]. The proposed method is blind because it only needed a key for generating the template. A strong watermarking technique by using selective curvelet coefficients is demonstrated by Leung et al. [99]. In this technique, a proper location to embed the watermark is selected by analyzing the payload and variation of the curvelet coefficients.

**2.2.5 Some Other Transform Domains**

Falkowski and Lim investigated a digital image watermarking technique by using the multi-resolution Hadamard transform and complex Hadamard transform [100]. In the first step, to decompose the cover image into frequencies such as HH (High-High), LL (Low-Low) and LH (Low-High). On the cover image Hadamard transform is applied. The second step, the LL frequency is decomposed into blocks of size 8x8 and then implemented a 2D complex Hadamard transform on blocks. Watermark is inserted in 2D complex Hadamard transform the phase component of the image. Because phase components are robust against image processing operations. One more image watermarking technique by using multi-resolution Hadamard transform is proposed by Gilani and Skodras [101]. In this approach, the high-frequency Hadamard coefficients are selected as the embedding domain instead of lowest frequency. It uses DWT and Hadamard transform to get multi-resolution Hadamard Frequency domain. A cover image goes through wavelet transform and after that Hadamard transform is used. In the Hadamard transforms most of the energy is packed on upper left corner of the image that the reason the upper left corner of a cover image is selected as embedding domain. From experimental results, the author emphasizes that HH frequency of Hadamard transform provide good resistance to watermark against noise. But for JPEG compression attacks robustness is poor.

Liu et al. presented a block-based, robust and invisible digital image watermarking technique using the Lapped Orthogonal Transform (LOT) [102]. To embed large-sized watermark without exploiting the imperceptibility, a spread spectrum watermarking approach and an HVS model are used. In this method, each block is classified into four are as named as texture, fine-texture, edge and plain areas. The energy of the embedded watermark is adjusted by following the Texture Masking Energy (TME)

approach of HVS. A pdf-matched embedding (PME) method is introduced by N. Liu et al. [103]. In this method, firstly pdf-matched quantizer is generated and this generated pdf-matched quantizer provides resistance to watermark from attacks as well as increases the embedding capacity. Secondly, by using vector flipping and DC-PME, the distortion due to embedding is reduced. The proposed technique provides better robustness against signal processing attacks as compared to uniform quantization schemes. Seo et al. [104] demonstrated a content-based watermarking method by utilizing the feature points of a cover image. The watermark is embedded into all the feature points by using affine normalization i.e. according to the characteristic of scale. For identifying feature points, a local search technique is used by the algorithm. The proposed algorithm gave a blind watermark extraction method. The author emphasizes on the survival of watermark if a watermarked image is processed by cropping, compression filtering, and affine normalization operations. It also supports flexibility against different non-geometric and geometric attacks in watermark detection.

## 2.3 HOST INDEPENDENT WATERMARKING

Except for some techniques that used perceptual masking for embedding, all other above discussed techniques are host dependent watermarking techniques. In these techniques, the watermark is embedded by considering the imperceptible parameters of the cover image. But at the time of extraction, the cover image is completely neglected which affects the quality of extracted watermark. Therefore, some of the researchers believed that the cover image is unambiguously considered in the complexity of the watermark. Chen and Wornell introduced the Spread Transform - Dither Modulation (ST-DM) [105]. In this technique, to produce a secret codebook or set of center points, a key is used. One more side-information idea introduced by Furon et al. that named as Just Another N-Order Side-Informed Scheme (JANIS) [106]. In this technique, a number for embedding watermark in a hidden way is demonstrated and the direction in each scale is different. Here, the direction of embedding is selected consequently so as to match the incline of a key dependent extraction function estimated in the cover. Malvar et al. generated the watermark using the spread-spectrum scheme [107]. They developed an Improved Spread-Spectrum (ISS) and a Scalar Costa Scheme (SCS) technique. In these techniques, the authors developed scalar embedding and reception functions [108]. Miller et al. proposed a technique that embeds multiple watermarks by using a lattice [109]. In this technique, all messages are firstly mapped into a set of paths on a lattice and then

associated number to every transition becomes key-dependent spreading vector. At the time of extraction, the highest correlation is considered to set the path on the lattice. Rational Dither Modulation (RDM) approach used lattice quantization [110]. Here, the quantization step modify as a function of the watermarked information. This method can produce satisfactory results if this positive function is key dependent. An alternate method, codebook randomization for DC-DM methods, is presented by Moulin et al. [111]. In this method investiogated a key-dependent rotation lattice for embedding watermark. A lattice-based codebook method which is randomized by means of a key-dependent dither signal is proposed by Fei et al. [112]. In this method, a key hash function is used to embed the watermark.

## 2.4 MEDICAL IMAGES WATERMARKING

In this context, patient's information is hidden as a secret message in Magnetic Resonance Imaging (MRI), Electroencephalogram (EEG), and electrocardiogram (ECG) signals [113]. Protection of ECG signals using watermarking is an emerging field. Hiding the watermark in ECG signals is an intricate task because the diagnosability of disease is based on the medically important QRS complex attribute points of ECG. So, in ECG watermarking, it is important to diminish the worsening at these QRS complex points. The amount of worsening is a common performance computation of watermarking. ECG watermarking is achieved by frequency and spatial domain. In the spatial domain, the secret message is inserted in the time domain of original signal. Yang et al. presented a lossy and reversible ECG watermarking method by using alignment of coefficients [114]. However, in the transform domain, firstly, ECG signal is converted into the frequency domain by applying the transformation. The information is hided into the coefficients at transmitting end after that the watermark is extracted at receiving side. In ECG Watermarking, Discrete Wavelet Transform (DWT) is mainly used. Zhang et al. pioneered reversible ECG Watermarking technique by utilizing the DWT [115]. Jero et al. projected an ECG Watermarking technique of embedding secret information into the wavelet coefficients by using the Singular Value Decomposition (SVD) [116]. The author also investigated that embedding in HH (High High) band provides the best imperceptibility. The ECG signals are combinations of peak values and curved lines. But Wavelet transform fails to represent 2D and higher dimensional singularity due to limited number of directional elements. So, curvelet has been developed specially to exhibit the objects having a higher dimensional singularity. In the year 2000, Candes et al. [31]

projected a novel transform that overcomes the disadvantage of wavelet and provides an optimal sparse representation of edges. The curved edges are represented in a better way using curvelet  Some of the authors take the benefit of curvelet transform coefficients to hide the watermark in ECG signals. Hien et al. uses the threshold method to insert the information in the curvelet transform of the cover [117]. The coefficients having lesser value than the selected threshold, are used as the embedding domain. Jero et al. also demonstrated a novel technique of ECG watermarking by utilizing the n*n sequence in curvelet transform [118]. Use of n*n sequence avoids the overlapping and is an adaptive approach to select the location of the watermark to insert the message. Jeroet et al. also introduced a new quantization approach to secure the patient information [119]. In this approach, theauthor used the curvelet coefficients whose values are around zero as the embedding domain. These proposed methods show that curvelet transforms efficiently hides and extract the information from the ECG.

## 2.5 CONCLUSION

From the literature review, it is apparent that the research in digital watermarking is powerfully aggravated by a growing necessitate from the copyright proprietors to consistently guard their privileges. Since of the huge financial stakes, digital watermarking is assured to a bright prospect. New applications are probable to appear and may come together existing techniques. Spatial domain methods are fast and simple, but watermark is not survive if image processed by image processing operations. In comparison, frequency domain watermarking procedures are robust.

Several techniques have been developed in transform domain. In any watermarking algorithm, the domain of embedding the watermark is very important and must be chosen carefully. Embedding in DCT coefficients offer good robustness against JPEG compression, filtering and enhancement operations. There is a capability of restoration of images. But this domain is more sensitive to geometrical transformation. DWT embedding techniques provide robustness to all image processing attacks, even watermark also withstands MPEG compression. The major disadvantage is that it has no restoration capability. Some authors also used texture blocks for embedding watermark that gives invisibility and robustness against JPEG compression, filtering, and enhancement operations because it includes HVS property. The texture blocks are sensitive to lossy compression, sometime undesirable for color images and it has no restoration capabilities.

# CHAPTER 3

# NON-BLIND WATERMARKING TECHNIQUES

In this chapter, the author proposed two non-blind watermarking techniques by using curvelet coefficients. The first technique demonstrates embedding of a watermark in different scales of curvelet domain for the grayscale image. The experimental results are compared with wavelet transform and the effect of variation of scale is also investigated. The second technique utilizes texture blocks of color image to protect the interest of the authors. Since, human visual system is less sensitive to texture area rather than the smooth part therefore in this technique texture blocks are used to hide the watermark of the cover image. Masking property of HVS is used to extract the texture blocks from the original image. Curvelet transform is applied on the texture blocks, then the curvelet coefficients of are exploited to embed the watermark. For improving the robustness of watermark a strength parameter (α) has been also used. It has been shown that techniques give robustness to watermark.

## 3.1 DIGITAL WATERMARKING TECHNIQUE BASED ON MULTI-RESOLUTION CURVELET TRANSFORM

This Technique proposes a robust and non-blind watermarking technique based on multi-resolution curvelet transform. Curvelet transform is more efficient in representing isometric objects as compared to wavelet transform and other traditional transforms. The proposed technique implements the embedding and extraction of the watermark in different scales of curvelet domain. The results are compared using various evaluation metrics such as NC, PSNR, and SSIM. The visual quality of watermarked image, the efficiency of data hiding and the quality of extracted watermark of curvelet domain embedding techniques, with wavelet domain at a different number of decomposition levels, are also compared.

### 3.1.1 Embedding algorithm

The following steps are carried out in order to insert the watermark in a grayscale image:

i. An image (I) of M*N size and image (W) of m*n size are taken as the host (original) image and watermark image respectively.

ii. The watermark image W is converted into a binary image (B).

iii. Now, curvelet transform is applied to decompose the cover image (I) into frequency domain (C). In this domain, the cover image is separated into two levels: Coarse (lowest level) and Detail (highest level).

iv. Select the scale s and orientation j. The selection of scale s and orientation j affect the invisibility and robustness of watermark. It is desirable to hide the watermark in the Coarse level since most of the energy resides in it. Let the selected domain of curvelet is denoted by $C_{sel}\{s\}\{j\}$.

v. If $(sizeof(C_{sel}\{s\}\{j\}) \leq sizeof(W))$then add zeros as padding or pad the duplicate matrix elements in watermark image W to make both the images equal.

vi. For each coefficient $k$ of selected domain $C_{sel}\{s\}\{j\}$ embed the watermark B by using equation given below:

$$\hat{C}(s,j,k) = C_{sel}(s,l.k) + (\alpha * B[k]) \quad (3.1)$$

Where $\alpha$ is a strength parameter defined in the equation below and it is treated as the key of embedding.

$$\alpha = \alpha_{in} * k * I_{avg} * \log(|C_{avg} - 128| + 10 \quad (3.2)$$

Where $I_{avg}$ = Average intensity value of the cover image I, $\alpha_{in} = \frac{0.01 * X_{avg}}{127}$, $k \ll$ 0.01, $C_{avg}$ is the average of the coarse coefficients of image i.e. $C_{sel}\{s\}\{j\}$

vii. To convert frequency domain back into time domain, apply an inverse curvelet transform on modified curvelet coefficients $\hat{C}(s, j, k)$ with appropriate scaling that we used in forward curvelet transform. The resulting image is in time domain called watermarked image and it is represented as $I_w$

### 3.1.2 Extraction Algorithm

The following algorithm gives the non-blind extraction. Here, the selected scale and orientation are used in embedding algorithm and $\alpha$ is the strength parameter, is used as a key for extraction of watermark. In order to extract the watermark, the following steps are follows.

i. Resulting image from 3.1.1 $I_w$ represents watermarked image. Time-domain images ( $I_w$ , I) are converted into frequency domain by applying the curvelet transform. The resulting frequency domain of I and $I_w$ is represented as $C$ and $\hat{C}$ respectively.

ii. Use the first key, i.e., the scale and orientation that we selected in embedding procedure 3.2.1 for obtaining the curvelet coefficients of original and watermarked image represented by $\hat{C}(s, j, k)$

iii. Now determine the $\alpha$ strength parameter which is defined in equation (3.2).

iv. Obtain the watermark by using equation below:

$$B = \frac{\hat{C}(s,j,k) - C(s,l.k)}{\alpha} \tag{3.3}$$

v. The watermark image in time domain is obtained by applying inverse curvelet transform on B.

### 3.1.3 Experimental Results

To emphasize and to assess the performance of the above discussed technique, seven distinct images are used as a cover image. These images have different formats and sizes as shown in Figure 3.1 to Figure 3.7. Figure 3.8 shows the watermark image. The watermark image is embedded into each image by selecting 4 orientation and 2nd scale of curvelet transform. The invisibility of the embedded information is evaluated by using evaluation metric. The result of invisibility is discussed in invisibility test below:

**Figure 3.1 Woman.tif**

**Figure 3.2 Leaf.tif**

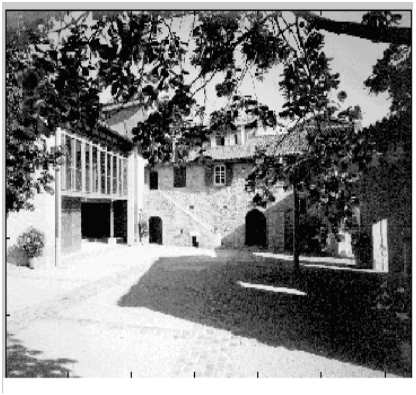

**Figure 3.3 House.png**

**Figure 3.4 Fingerprint.tif**

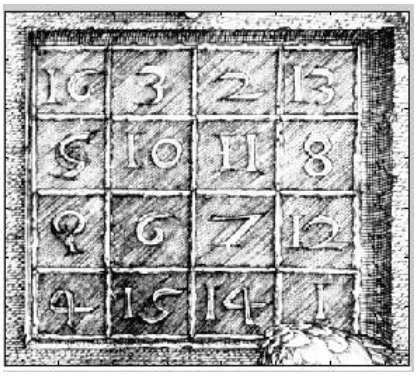


**Figure 3.5 Magic.png**

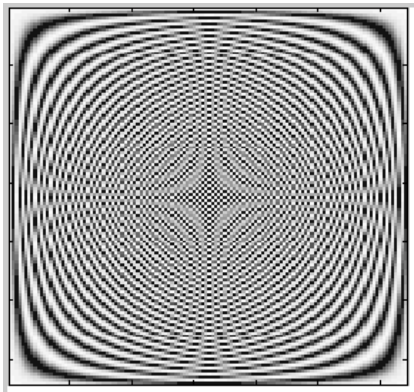

**Figure 3.6 Vortices.tif**

**Figure 3.7 Cameraman**

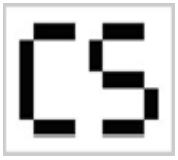

**Figure 3.8 Copyright image (Watermark)**

### 3.1.3.1 Invisibility Test

For invisibility, the visual appearance of watermarked image and cover image is compared with the help of quality assessment metrics. Figure 3.8 is embedded into all the above shown cover images. The resulting watermarked images are shown form Figure 3.9 to Figure 3.15. The visual quality of watermarked images and cover images are very similar. The invisibility of watermark is certified by analyze the visual quality of cover and watermarked images. The performance of invisibility is analyze by the evaluation matrices such as PSNR, NC, SSIM and MSSIM.

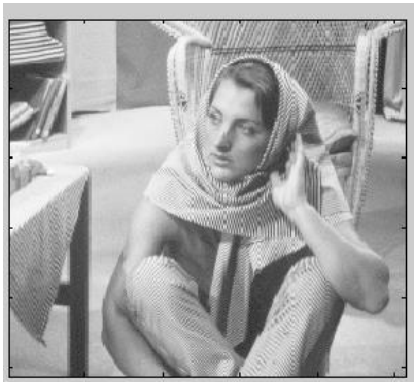

**Figure 3.9 Watermarked women**

**Figure 3.10 Watermarked Leaf**

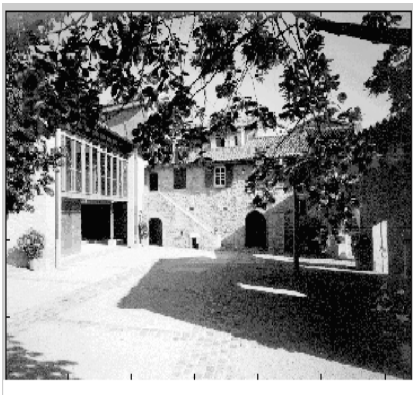

**Figure 3.11 Watermarked House**

**Figure 3.12 Watermarked Fingerprint**

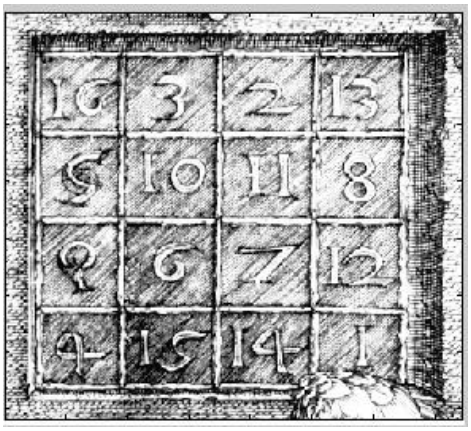

**Figure 3. 13 Watermarked Magic**

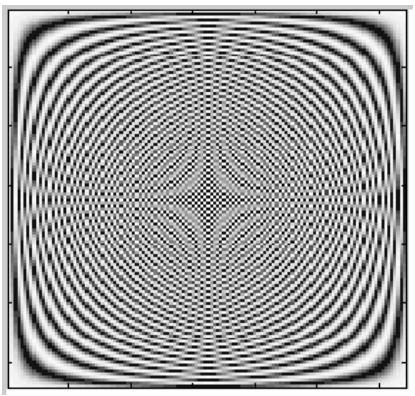

**Figure 3.14 Watermarked Vortices**

**Figure 3.15 Watermarked Cameraman**

**Figure 3.16 Extracted watermark**

The results corresponding to each image are analyzed by using MSE, PSNR, NC, SSIM and MSSIM. It may be observed that the MSE is approximately 0 confirming a high imperceptibility of the digital watermark. For all the images, PSNR value is more than 76 which is also good. Besides, the NC, SSIM, and MSSIM are 1 for all images confirming almost exact similarity between both the images. This clearly shows that the watermark is perfectly invisible.

### 3.1.3.2 Effectiveness test

For testing the effectiveness of the technique, watermark is extracted from the watermarked image as shown in Figure 3.15. The resulted extracted watermark is compared with the original watermark. The PSNR values of extracted watermark from all watermarked images are equal to 53 and values of NC and MSSIM are 90% that confirm the visual appearance of the extracted watermark is very much similar with the embedded one.

### 3.1.3.3 Robustness Test

In order to test the robustness of the technique, one requires adding some sort of noise into the watermarked image and then extracting the watermark. Besides, robustness is also tested by applying various operations such as compression, rotation, cropping, and filtering on the watermarked images before extracting the watermark. Thereafter, the extracted watermark is evaluated by using the evaluation metrics. Two types of noise namely salt & pepper and Gaussian are applied on watermarked image. The watermarked is extracted from the noised images and then compared with original watermark. Figure 3.17 and Figure 3.18 show the extracted watermark from salt & pepper and Gaussian noised watermarked image. The similarity measure MSSIM and SSIM confirm the presence of watermark to the extent of more than 50 % similarity. This shows that the technique is robust enough against noise addition.

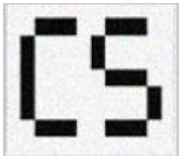

**Figure 3.17 Extracted watermark from salt & pepper noised image**

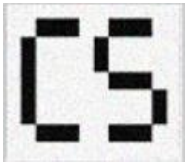

**Figure 3.18 Extracted watermark from Gaussian noised image**

Compression is a very important image processing operation and is used in reducing the size of digital media frequently. To test the robustness against the compression operation, two types of compression techniques, namely Global Threshold (GT) with two threshold values ($T_r$) and Level dependent Threshold (LT) are applied. Table 3.1 demonstrations the performance of extracted watermark under diverse type of compression. It is clear from the table that the extracted watermark is highly similar (more than 50 % in general) to the original watermark as the metric SSIM and MSSIM have reasonably good value.

**Table 3.1 Evaluation of extracted watermark after compression**

| Image | Compression type | Threshold ($T_r$) | Retained energy (Compression) | PSNR | SSIM | MSSSIM |
|---|---|---|---|---|---|---|
| Woman | GT | $T_r$- 20 | 99.9176 | 23.858 | 0.7496 | 0.6120 |
| | | $T_r$- 100 | 99.3559 | 23.551 | 0.7914 | 0.6984 |
| | LT | | 99.8933 | 23.854 | 0.7495 | 0.6115 |
| House | GT | $T_r$- 20 | 99.8974 | 36.907 | 0.6632 | 0.5578 |
| | | $T_r$- 100 | 98.2837 | 25.877 | 0.6729 | 0.4221 |
| | LT | | 99.8582 | 21.824 | 0.6041 | 0.4378 |
| Leaf | GT | $T_r$- 20 | 99.7725 | 39.406 | 0.8791 | 0.7100 |
| | | $T_r$- 100 | 96.7267 | 29.580 | 0.7685 | 0.5133 |
| | LT | | 99.7000 | 25.495 | 0.7268 | 0.5071 |
| Fingerprint | GT | Tr- 20 | 99.9340 | 38.045 | 0.7738 | 0.6084 |
| | | Tr-100 | 97.8177 | 22.734 | 0.5461 | 0.3913 |
| | LT | | 99.9144 | 17.415 | 0.5314 | 0.374 |
| Magic | GT | Tr- 20 | 99.9179 | 36.878 | 0.7631 | 0.5472 |
| | | Tr-100 | 97.6871 | 23.606 | 0.558 | 0.394 |
| | LT | | 99.8967 | 22.967 | 0.5144 | 0.397 |
| Vortices | GT | Tr- 20 | 99.8721 | 38.129 | 0.8615 | 0.6096 |
| | | Tr-100 | 98.8426 | 33.706 | 0.8283 | 0.5037 |
| | LT | | 99.8178 | 26.041 | 0.8177 | 0.4608 |
| Cameraman | GT | Tr- 20 | 99.9100 | 40.031 | 0.8823 | 0.7299 |
| | | Tr-100 | 99.3170 | 33.107 | 0.8393 | 0.6079 |
| | LT | | 99.8880 | 40.357 | 0.8835 | 0.7369 |

For evaluating the technique corresponding to robustness against filtering operation. The watermark is extracted from the filtered image and compared with the original watermark. Table 3.2 shows the values of assessment metrics. It is observed that similarity metric SSIM, MSSIM are not very high (less than 50%), which shows that the technique is not so robust against filtering operation. However, the values confirm the presence of the watermark.For testing the robustness against rotation operation, the watermarked image is rotated by 90 degrees and the watermark is extracted. This extracted watermark is compared with original watermark duly rotated by 90 degrees. Table 3.2 shows the values of quality assessment metrics. It may be observed that both

similarity measures, SSIM and MSSIM, are reasonably good confirming the similarity of watermarks. Therefore, we can conclude that the technique is robust against rotation operation.

**Table 3.2 Evaluation of extracted watermark after filtering operation**

| | Filtering operation | | | 90-degree rotation | | |
|---|---|---|---|---|---|---|
| **Image** | **PSNR** | **SSIM** | **MSSSIM** | **PSNR** | **SSIM** | **MSSSIM** |
| Woman | 16.1639 | 0.438 | 0.493 | 25.6391 | 0.7493 | 0.7195 |
| House | 12.2395 | 0.4142 | 0.372 | 22.8770 | 0.7968 | 0.7567 |
| Leaf | 17.1890 | 0.4099 | 0.3712 | 26.4257 | 0.7676 | 0.7053 |
| Fingerprint | 8.3993 | 0.432 | 0.3912 | 18.5641 | 0.7365 | 0.7152 |
| Magic | 9.8325 | 0.5377 | 0.5142 | 20.4737 | 0.7533 | 0.7288 |
| Vortices | 18.0163 | 0.4443 | 0.359 | 26.7995 | 0.7622 | 0.7347 |
| Cameraman | 21.6064 | 0.4732 | 0.3945 | 28.9615 | 0.7883 | 0.7473 |

### 3.1.4 Analysis of scales and comparison with wavelets

The PSNR, NC and the embedding capacity of the watermarked image at different scales in curvelet domain are also analyzed. The Figure 3.19shows that embedding in lower scale gives better invisibility without significantly affecting the PSNR values. Values of NC =1 confirm that the visual quality of watermarked image is similar to cover image in every selected scale. Further, all scales have the same embedding efficiency with respect to data hiding capacity. As we increase the embedding efficiency of the watermark, the visual quality or invisibility of watermark is affected.

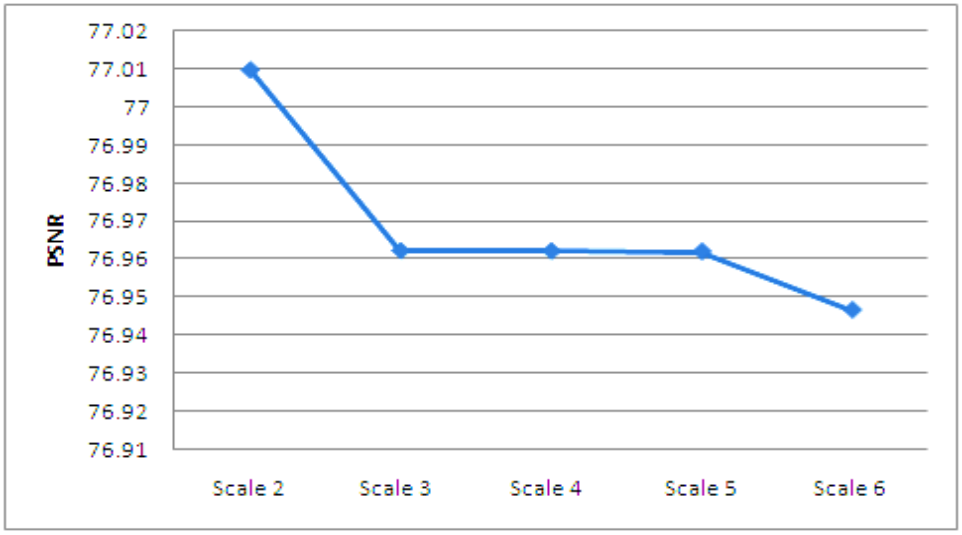

**Figure 3.19 Variation of PSNR of watermarked image by proposed algorithm embedding in different scales**

In order to analyze different embedding techniques, we compared our proposed scheme with wavelet transform technique at various levels. We have embedded the same watermark in the Low-Low (LL), the High-Low (HL) and the Low-High (LH) frequencies of the wavelet transform. Table 3.3 shows the performance of watermarking technique that embed the watermark into the wavelet domain with different frequencies. From the table, it is evident that the embedding in LL frequencies give better invisibility of watermarked image but the efficiency of data hiding reduces. It may be observed that the PSNR in curvelet is relatively higher compare to DWT even at the best LL level.

**Table 3.3 PSNR values of watermarked image, extracted watermark & embedding efficiency of different decomposing level in wavelet transform domain**

| | | | PSNR | | |
|---|---|---|---|---|---|
| Technique | Domain | Level DWT | Watermarked image | Extracted watermark | Embedding Efficiency |
| Wavelet transform | HL & LH freq. | 1 DWT | 57.0287 | 56.1278 | (128*128) |
| | | 2 DWT | 63.0363 | 56.8453 | (64*64) |
| | | 3 DWT | 69.0148 | 57.7729 | (128*128 |
| | LL freq. | 1 DWT | 60.0390 | 53.0184 | 128*128 |
| | | 2 DWT | 66.0466 | 53.0054 | 64*64 |
| | | 3 DWT | 72.0251 | 53.9633 | 64*64 |

## 3.2 AN IMAGE OWNERSHIP PROTECTION METHOD: HIDING DATA INTO THE TEXTURE BLOCKS ON CURVELET DOMAIN

In this technique, a non-blind watermarking technique using texture blocks, for an image ownership protection is proposed. This technique comprises of three algorithms. The first algorithm identifies texture blocks in the cover image, the second algorithm embeds the watermark into the curvelet domain of texture blocks and the third algorithm extracts the embedded watermark from the watermarked image.

### 3.2.1 Identification of Texture Blocks

The texture is a key component of human visual perception. HVS states that the

human eye sensitivity decreases both in the direction of the low and high brightness and in high-resolution bands. So, the perceptibility of embedded information is very less in a texture blocks of an image. To get the benefits of higher invisibility, the texture part of the image is used to hide the watermark. To extract the texture from the cover image, an edge detection method is used. The image edge can be detecting by identifying the gray scale variation of first and second order directional derivative of the adjacent edge. The following steps are followed to detect the edge surface in the image.

i. The noise of the image ($I$ )is removed by convoluting on the image ($I$ ) using the Gaussian filters.

ii. Find the zero crossing points and calculate the Gradient (G) and the direction (D) using the following equation:

$$G(i,j) = \sqrt{P^2 I(i,j) + \phi^2 I(i,j)} \tag{3.4}$$

$$D(i,j) = \arctan\left[\frac{\phi(i,j)}{P(i,j)}\right] \tag{3.5}$$

Where, $P = \frac{1}{2} * \begin{bmatrix} -1 & 1 \\ -1 & 1 \end{bmatrix}$ (3.6)

i.e. 2*2 first order approximation of partial differential coefficient in the x and y-direction.

$$\phi = \frac{1}{2} * \begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix} \tag{3.7}$$

iii. By following the above steps, the edge surface of the cover image $I$ is detected. The resultant image is called as edge surface or texture image (B). Here, B is denoted $B = \{b(i,j) | 1 \le i \le M, 1 \le j \le N,\ b(i,j) \in \{0,1\}\}$.

### 3.2.2 Watermark Embedding

A gray scale image and an author's logo image also in gray color are taken as cover and watermark images respectively. Let $I = \{x(i,j), 1 \le i \le M, 1 \le j \le N\}$, and $W = \{w(i,j) | 1 \le i \le m, 1 \le j \le n,\ w(i,j) \in \{0,1\}\}$ denote the cover image and the binary logo watermark image respectively. The procedure of watermarking is as follows.

i. Get a texture image (B) from the original image (I) by applying the algorithm as discussed in section 3.2.1. Now divide both the images into 8*8 size non-overlapped blocks. Let $B_k$ and $I_k$ are corresponding blocks of edge surface image B and original image I respectively, where k is number of block i.e. $k = 1,2, \ldots \ldots \left(\frac{M*N}{8*8}\right)$.

ii. Set a threshold number $T_h$ for edge points, to be used as the first key of embedding procedure. Calculate the edge points in each block $B_k$ of image B, Blocks having number of edge points more than $T_h$ are identified as texture blocks. Let V represents the total number of texture blocks in B image.

iii. Extract the corresponding blocks ($I_k$ ) of original image that are selected as texture blocks in edge surface image (B) and then combine these $(I_k)$ blocks resulting in the image called texture image $T = \{t(i,j)|\ 1 \le i \le p, 1 \le j \le p,\ t(i,j) \in I\}$, where p*p is the size of texture image where $p * p \le V$.

iv. The texture image T is converted into frequency domain by using curvelet transform to obtain the number of scales $p_{scale} = log_2 p - 2$, where p*p is the size of the texture image. After decomposition, the T image is separated into Detail and Coarse levels. Here, we select the coarse level (C) for embedding the watermark because most image energy is packed into the Coarse.

v. Determine the strength factor α as given in equation (3.8). This is treated as the key of embedding.

$$\alpha = \alpha_{in} * k * I_{avg} * \log(|C_{avg} - 128| + 10 \quad (3.8)$$

Where $I_{avg}$ is the pixel average of the original image I, $\alpha_{in} = \frac{0.01 * X_{avg}}{127}$, $k \ll 0.01$, $C_{avg}$ is the average of the coarse coefficients of texture image i.e. C.

vi. Transform the watermark image W into vector $\widehat{w}$ of size (m*n).Embed the watermark into the curvelet domain by using equation:

$$\hat{C}(i,j) = C(i,j) * (1 + \alpha * \widehat{w})\ , i,j = 1,2 \ldots\ldots\ldots \quad (3.9)$$

Where $\hat{C}(i,j)$ are the modified curvelet coefficient of selected scale of the texture image T, $C(i,j)$ is the curvelet coefficient of selected scale of the texture image T, $\alpha$ is the strength factor as defined above, and $\widehat{w}$ is the watermark intensity in vector form.

vii. Convert this frequency domain texture image, i.e. $\hat{C}(i,j)$, into time domain by applying the inverse curvelet transform. Watermarked image $(\hat{I})$ is obtained by reallocating the modified texture blocks into their correct positions in original image.

### 3.2.3 Watermark Extraction

The process of watermark extraction from the watermarked image is reverse of embedding procedure. In this case, the steps are as follows:

i. Obtain texture image T and $\hat{T}$ from the cover image $I$ and the watermarked image $\hat{I}$ respectively as discussed in section 3.2.1. Here the first key, $T_h$, is required to identify the texture blocks as discussed in steps in section 3.2.1.

ii. The texture image T and $\hat{T}$ are transform into frequency domain by applying curvelet transform. Then, we select embedding level, i.e., the coarse level (C) for T and the coarse level ($\hat{C}$) for the $\hat{T}$ image.

iii. The second key that we require at the time of extraction is the strength parameter (α) by using equation (3.8).

iv. Extract the components of the watermark image as defined in equation:

$$w(i,j) = \frac{C_i'(i,j)/(C_i(i,j)-1)}{\alpha} \quad (3.10)$$

If $w(i,j) = 1$ then the information exists, otherwise, if $w(i,j) = 0$ then information is not there. The watermark bits are arranged in the form of m*n image.

### 3.2.4 Experimental Results and Discussion

The above discussed technique has been extensively tested on various standard images. 32*32 size of binary logo is embedded into the cover images. In order to test the invisibility and to compare the performance with existing techniques, grayscale images of 256*256 size named as 'Lena', 'Cameraman', 'Men', boat', and 'Peppers' images from the SIPI image database [120] are used as the cover images (host image) as shown in Figure 3.20(a) to Figure 3.20(e) respectively .

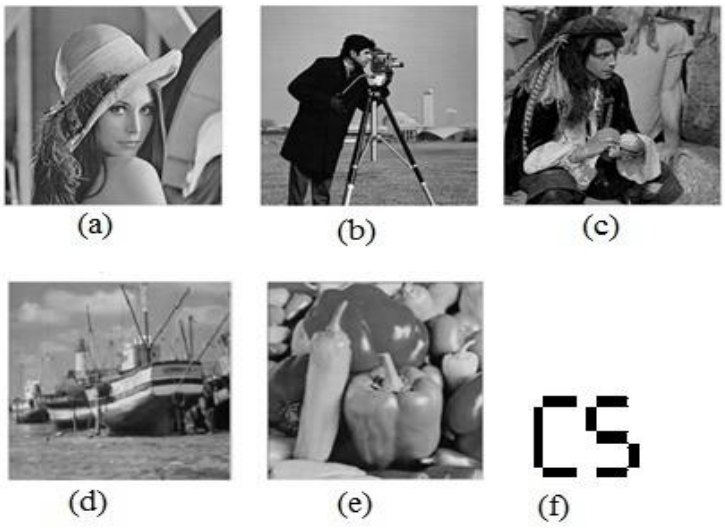


**Figure 3.20 The Original images (a) Lena (b) Cameraman (c) Men (d) Boat (e) Pepper and (f) Original watermark**

A binary logo of 32*32 size watermark image is shown in Figure 3.20(f). Figure 3.21(a) to Figure 3.21(e) below show the corresponding watermarked images. The visual quality and similarity between the watermarked images and cover images are very high; human eyes cannot distinguish between the cover and watermarked images.

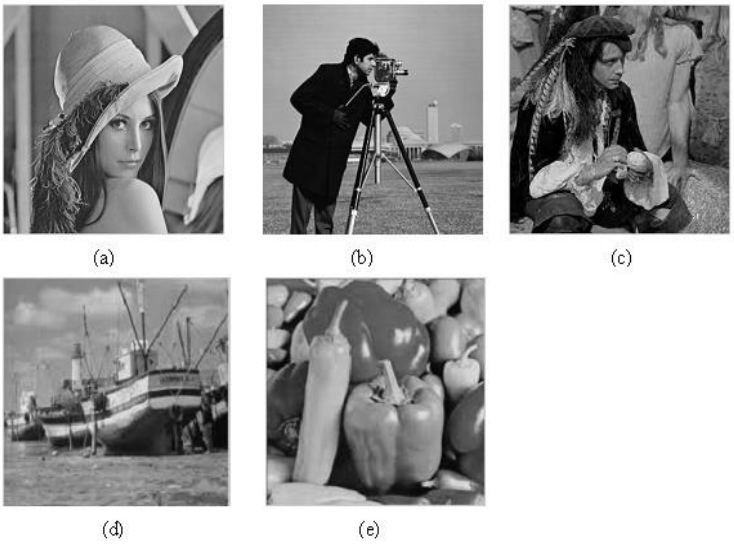


**Figure 3.21 The watermarked image (a) Lena (b) Cameraman (c) Men, (d) Boat and (e) Pepper**

Figure 3.22(a) to Figure 3.22(e) show the extracted watermark from the corresponding watermarked images. The visual quality of the extracted watermark is also very good. The similarity of the extracted watermark with the original one is verified by the high value of NC. The value of SSIM is very close to 1, it means thereby that there is no loss of luminance and is a contrast of the extracted watermark. This means extracted watermark is extremely identical with the original watermark.

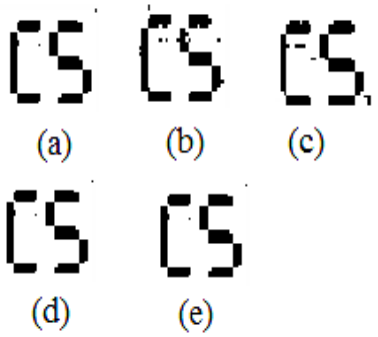


**Figure 3.22 Corresponding extracted watermark from Figure 3.21 (a) to Figure 3.21 (e), (a) SSIM=0.9992, NC=1.000, (b) SSIM =0.9995, NC=1.000, (c) SSIM=0.9995, NC=1.000, (d) SSIM =0.9994, NC=1.000 and (e) SSIM = 0.9992, NC=1.000**

To evaluate the robustness of the proposed technique, Gaussian noise addition, rotation, cropping, sharpening, sparsity and histogram equalization image processing operations were applied on the watermarked images. The performance of extracted watermark is shown in Figure 3.23 when a Gaussian noise with the different variance is added to the watermarked images. From the Figure (BER vs. variance of the noise), it is observed that the robustness of the watermark is high even at very high noise density, the extraction algorithm is still able to detect the watermark.

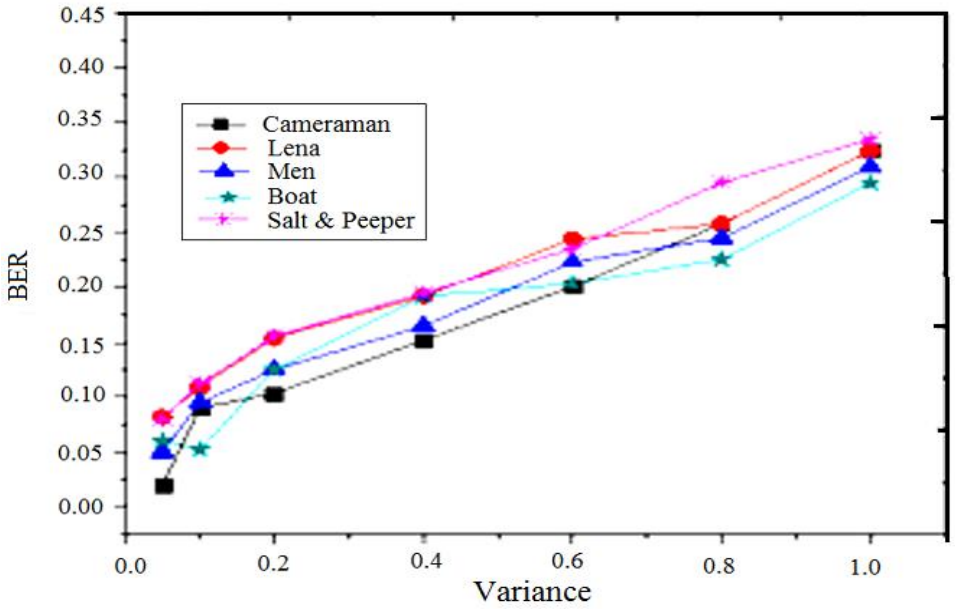


**Figure 3.23 BER of extracted watermark under Gaussian noise**

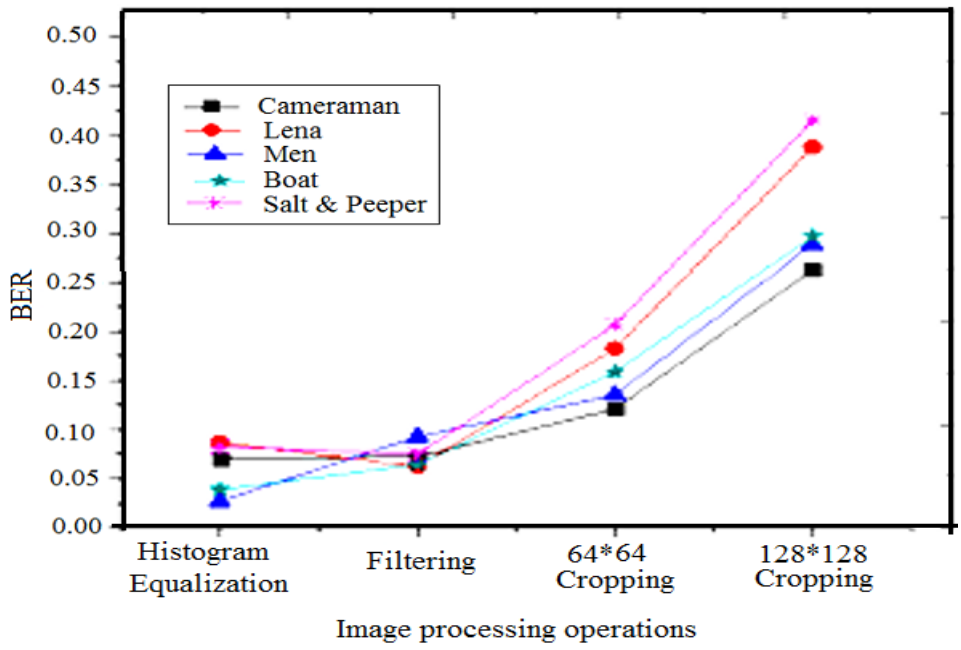


**Figure 3.24 BER of extracted watermark under Histogram equalization, filtering and cropping operation**

Figure 3.24 shows the BER of extracted watermark from the histogram equalization images, [3*3] filtered images, and cropped images. Watermark is robust against histogram equalization and filtering operation. The visual appearance of extracted watermark is good. The Figure 3.25 shows the results of watermark extraction from 20 degrees to 120 degrees rotated watermarked images.

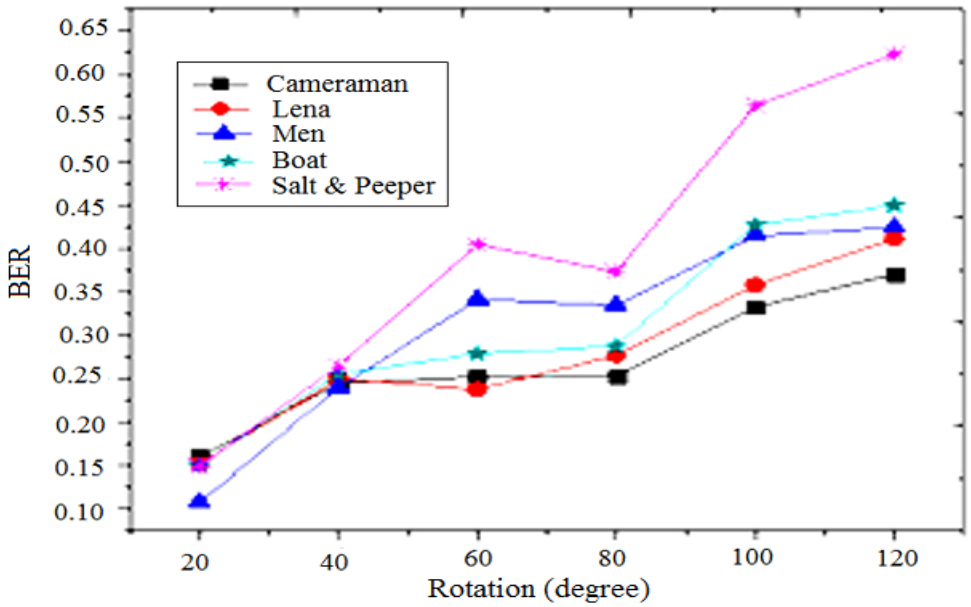


**Figure 3.25 BER of extracted watermark under rotation**

Further, the results of above technique are compared with some standard techniques. Table 3.4 compares the PSNR values of proposed technique with existing algorithms. It is can be verified from the table that (i) The PSNR of the six watermarked images≈54, which shows the similarity between the watermarked images and the original images. (ii) The PSNR values of the watermarked images from the proposed technique are better as compare to other techniques used by different authors, which shows the imperceptibility of the proposed algorithm is good.

**Table 3.4 Invisibility of proposed method v/s existing techniques**

| Image Name | Proposed technique | MSF algorithm [121] | LWT-SVD [122] |
|---|---|---|---|
| Lena | 53.293 | 55.729 | 47.718 |
| Cameraman | 53.6927 | 53.6549 | 48.902 |
| Men | 53.7119 | 51.1733 | 50.181 |
| Boat | 53.8293 | 51.4943 | 53.81 |
| Pepper | 53.7898 | 52.1592 | 48.097 |

The experiments are performed in MATLAB 7.2 environment, and on a 2.27 GHZ computer with 2G RAM. The complexity of the proposed algorithm is compared with DC component based technique [123] which do not use curvelet transform in Table 3.5. From the table, it is analyzed that the time complexity of the technique is less than the DC component based technique [123]. This shows that the curvelet transform takes less time as compared to the genetic algorithm and also DWT.

**Table 3.5 Comparison of time complexity**

| Time | Proposed Method | DC component based [123] |
|---|---|---|
| Embedding time complexity | 0.40716 | 0.5244 |
| Extraction time complexity | 0.2076 | 0.3701 |
| Total complexity | 0.6123 | 0.8945 |

## 3.3 CONCLUSION

This chapter considered two techniques for watermark embedding in the curvelet coefficients. The first technique is to embed a gray scale image in the different scales of curvelet transform of cover image by using a strength parameter. Second technique proposed is a non-blind watermarking technique by using curvelet transforms and texture blocks. This technique emphasized that the watermark embedded into texture blocks gives better imperceptibility rather than into the smooth part of the image. In this watermark is a logo type binary image. To test the robustness, intensive image processing operations with different variation are applied on watermarked image and thereafter the watermark is extracted. The performance of extracted watermark is analyzed by using NC, PSNR, SSIM and MSSIM and also compared with existing techniques.

# CHAPTER 4

# SEMI- BLIND WATERMARKING TECHNIQUES

In this chapter, two semi-blind digital image watermarking techniques based on the curvelet coefficients are presented. The first technique inserts the watermark in RGB image by utilizing the HVS property. It is evident that the eyes are not much sensitive to blue color. The processed watermark has been embedded into the blue color plane of frequency domain of the cover image. Selected scale and orientation of the curvelet coefficients of the blue channel have been used for embedding the MSB plane of the watermark. The second technique utilizes the characteristics of cryptography and watermarking technique to propose a secure and semi-blind watermarking technique for a color image. It has been shown that this technique gives robustness to watermark. The following sections describe these techniques one by one.

## 4.1 SEMI-BLIND WATERMARKING SCHEME FOR RGB IMAGE USING CURVELET TRANSFORM

This technique proposes a semi-blind watermarking technique of embedding a color watermark using curvelet coefficient in RGB image. This technique utilizes the property of HVS and bit plane. Most Significant Bit (MSB) plane of watermark image is used as embedding information. The experimental results show that the proposed technique gives better invisibility of watermark, superior quality of extracted watermark and better robustness against different attacks.

### 4.1.1 Embedding Algorithm

A frequency spectrum is independent of the transmission media. Absorption spectrum gives the idea about the spectral sensitivity of rods and cones of human eye. It shows that the eyes are not much sensitive to blue color. The blue color plane of frequency domain of the original image is used to embed watermark. Selected scale and orientation of the curvelet coefficients of the blue channel have been used for embedding the MSB plane of

the watermark. All other 0-7 bit planes are used as a key which is used at the time of extraction. The semi-blind technique of embedding watermark in curvelet domain is describe below.

i. Read the original cover image I and decomposed it into RGB color planes. Let $I_r$, $I_g$ and $I_b$ represent the red, green and blue color plane of the original cover image respectively.

ii. Perform a curvelet transform on the blue color plane ($I_b$) with a j number of decomposition level, l number of scales and k is orientation. The resultant curvelet coefficients being stored in a multidimensional array.

iii. The watermark image is also colored so, firstly separate their color planes $B_r$, $B_g$ and $B_b$ red plane, green plane and the blue plane of the image respectively. Now obtain bit planes of each color plane. Let $\{B_{r1}, B_{r2}\ldots B_{r8}\}$, $\{B_{g1}, B_{g2}\ldots B_{g8}\}$ and $\{B_{b1}, B_{b2}\ldots B_{b8}\}$ be the set of bit planes of red, green and blue color respectively.$B_{r8}$, $B_{g8}$, and $B_{b8}$ are most significant bit plane of red, green and blue color used as the watermark (to be embedded) and remaining $\{B_{r1}, B_{r2}\ldots B_{r7}\}$, $\{B_{g1}, B_{g2}\ldots B_{g7}\}$ and $\{B_{b1}, B_{b2}\ldots B_{b7}\}$ are used as a key at the time of extraction.

iv. Select the orientation and scale for embedding the watermark. Let selected scale be j and orientation be $k_1$, $k_2$ and $k_3$ for embedding the bit planes $B_{r8}$, $B_{g8}$ and $B_{b8}$ respectively. Let the selected domain of coefficients $C_s$.

v. Determine the strength factor α given below. This is treated as the key for embedding.

$$\alpha = \alpha_{in} * k * I_{avg} * \log(|C_{avg} - 128| + 10 \quad (4.1)$$

Where, $I_{avg}$ is the pixel average of the original image I, $\alpha_{in} = \frac{0.01 * X_{avg}}{127}$, $k \ll 0.01$,$C_{avg}$ is the average of selected domain of coefficients i.e. $C_s$

vi. Modify each coefficient of selected orientation and scale as follows:

$$If\left(\left(\frac{\lfloor (C_s(j,k_1)/\alpha)\rfloor + B_{r8}}{2}\right) == 1\right) \text{then}(C_s(j,k_1) = (C_s(j,k_1) - 0.5) * \alpha$$

$$\text{Else } (C_s(j,k_1) = (C_s(j,k_1) + 0.5) \quad (4.2)$$

$$if\left(\left(\frac{\lfloor (C_s(j,k_2)/\alpha)\rfloor + B_{g8}}{2}\right) == 1\right) \text{then } (C_s(j,k_2) = (C_s(j,k_2) - 0.5) * \alpha$$

$$\text{Else } (C_s(j,k_2) = (C_s(j,k_2) + 0.5) * \alpha \quad (4.3)$$

$$if\left(\left(\frac{\lfloor (C_s(j,k_3)/\alpha)\rfloor + B_{b8}}{2}\right) == 1\right) \text{then } (C_s(j,k_3) = (C_s(j,k_3) - 0.5) * \alpha$$

$$\text{Else } (C_s(j,k_3) = (C_s(j,k_3) - 0.5) * \alpha \quad (4.4)$$

vii. Apply inverse curvelet transform with the same scale on to the modified coefficients to change the resulting image from the frequency domain to time domain. Add this modified blue color plane to red and green plane. Resulting image is an RGB watermarked image ($I'$)

### 4.1.2 Extraction Algorithm

In this section a semi-blind method of extraction watermark is presented. In semi-blind extraction, original image is not required to extract the watermark. Here it is semi-blind because the keys required to be used are namely 0-7 bit planes of the original watermark. To extract the watermark follow the following steps:

i. Read watermarked image $I'$and decompose it into color planes. Let $I'_{red}$, $I'_{green,}$, $I'_{blue}$ represent the red, green and blue color plane of watermarked image $I'$ respectively.

ii. Perform a curvelet transform on blue color plane $I'_{blue}$ with a $j$ number of decomposition level and l number of scales.

iii. Then select the scale and orientation that is used in procedure 4.1.1. This is treated as the key in extraction. The selected coefficients are denoted as $C'_{sel}$.

iv. Extract each bit plane ($EW_r, EW_g$ and $EW_b$) of the watermark as follows:

$$if \left(\frac{(C'_{sel}(j,k_1)/\alpha)}{2} \equiv 1\right) then \;\; EW_r = 1; \;\; else \; EW_r = 0; \quad (4.5)$$

$$if \left(\frac{(C'_{sel}(j,k_2)/\alpha)}{2} \equiv 1\right) then \;\; EW_g = 1; \;\; else \; EW_g = 0; \quad (4.6)$$

$$if \left(\frac{(C'_{sel}(j,k_3)/\alpha)}{2} \equiv 1\right) then \;\; EW_b = 1; \;\; else \; EW_b = 0; \quad (4.7)$$

v. From the above step the most significant bit planes of the watermark are obtained and now we use stored watermark bit plane to extract the color watermark. For each color plane and for each bit,

$$R = EW_r * 2^7 + B_{r7} * 2^6 \ldots\ldots\ldots\ldots\ldots + B_{r1} * 2^0 \quad (4.8)$$

$$G = EW_g * 2^7 + B_{g7} * 2^6 \ldots\ldots\ldots\ldots\ldots + B_{g1} * 2^0 \quad (4.9)$$

$$B = EW_b * 2^7 + B_{b7} * 2^6 \ldots\ldots\ldots\ldots\ldots + B_{b1} * 2^0 \quad (4.10)$$

vi. *R, G* and B are the color planes of red, green and blue color plane of extracted watermark image. Combining these color planes and we get the RGB extracted watermark.

### 4.1.3 Experimental Results and Discussion

To test the algorithm colored “lena.jpg” image is used as cover image and a colored “thapar.jpg” image is used as watermark image. Figure 4.1 and Figure 4.2 show the “lena.jpg” and “thapar.jpg” image respectively. Figure 4.3 and Figure 4.4 show the resulting watermarked image and extracted watermark respectively. The algorithm has been tested against all the required parameters such as invisibility, effectiveness, and robustness. Here, we compared the quality of watermarked image and extracted watermark with respect to the quality assessment metrics PSNR, NC, and SSIM. To show that the algorithm gives good robustness, the different image processing operations are applied to the watermarked image. The quality of extracted watermark from the distorted image has been analyzed by the quality assessment metrics.

**Figure 4.1 lena.jpg (cover image)**

**Figure 4.2 Thapar.jpg (watermark)**

**Figure 4.3 Watermarked Image**

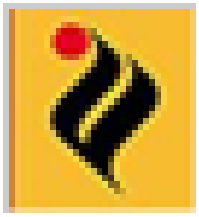

**Figure 4.4 Extracted watermark**

#### 4.1.3.1 Invisibility Test

Embedding extra information in the original signal will cause degradation and perceptual distortion. To test the invisibility aspect of the algorithm, the performance of cover image and watermarked image are compared with the help of quality assessment metrics. The quality of watermarked image has been analyzed by PSNR, NC and MSSIM

metrics on each plane. Table 4.1 shows the visual quality of watermarked image and Red_NC, Gr_NC, Bl_NC, Red_SSIM, Gr_SSIM, and Bl_SSIM represent the Normalized Correlation (NC) and SSIM of the red, green and blue color respectively. It may be observed that the PSNR is 54.94 confirming a high invisibility of the watermark. Besides, the NC and MSSIM are 0.99 for image confirming similarity between the watermarked and cover image. This clearly verify that the watermark is perfectly invisible. All the invisibility indices value are more than 99% confirming good invisibility of watermark.

**Table 4.1 Invisibility test**

| Image Name | PSNR | Red_NC | Gr_NC | Bl_NC | Red_SSIM | Gr_SSIM | Bl_SSIM |
|---|---|---|---|---|---|---|---|
| Watermarked | 54.94 | 0.9996 | 0.997 | 0.999 | 0.9941 | 0.9950 | 0.9943 |

#### 4.1.3.2 Effectiveness Test

To test the effectiveness of the algorithm, the same scheme, but in reverse order, is used to extract the watermark. There is no need of cover image while extracting the watermark because the above-discussed algorithm gives semi-blind extraction. Figure 4.4 shows the extracted watermark image, then its visual quality is compared with the embedded (original watermark) watermark. Table 4.2 analyzes the visual quality of extracted watermark using performance evaluation metrics such as PSNR, NC and SSIM. The PSNR of extracted watermark is 38.562, NC is one in all planes and SSIM is also more than 97%. Table 4.2 confirms that the visual quality of extracted watermark is very good as it matches highly with the original one.

**Table 4.2 Effectiveness test**

| Extracted watermark Image | PSNR | Red_NC | Gr_NC | Bl_NC | Red_SSIM | Gr_SSIM | Bl_SSIM |
|---|---|---|---|---|---|---|---|
| Figure 4.4 | 38.562 | 1 | 1 | 1 | 0.9761 | 0.9981 | 0.9953 |

#### 4.1.3.3 Robustness Test

The ability to detect the watermark even after image processing attacks such as channel noise, format conversion, filtering, compression, and cropping is called robustness. In order to test the robustness of the technique, one requires adding some sort of noise into the watermarked image and then extracting the watermark. Besides, robustness is also evaluated by applying various attacks such as filtering, rotation, cropping, adding sparsity and shearing on the watermarked image. Then watermark is extracted from the disturbed image. Thereafter, the extracted watermark is compared with

the embedded one by applying quality assessment metrics. Figure 4.5 to Figure 4.11 below show the quality of extracted watermarks from the distorted images.

The robustness is also being tested against noise addition operation. For this purpose two types of noise operations namely salt & pepper noise with noise density 0.01 and Gaussian noise with 0.1 variance, are applied on watermarked image. Then, the watermark is extracted from that noisy watermarked image. Figure 4.5 and Figure 4.6 show the visual quality of extracted watermark from Gaussian noised watermarked image and pepper salt noised watermarked image respectively. The values of PSNR, NC, and SSIM of each color planes are presented in Table 4.5. The similarity measure SSIM and NC confirm the presence of watermark to the extent of more than 70 % similarity on red and green color planes. The red color planes are more sensitive to human eyes. The NC and SSIM of red color planes of extracted watermark are 0.9. This shows that the technique is robust enough against noise addition.

**Figure 4.5 Extracted watermark from Gaussian noise watermarked image**

**Figure 4.6 Extracted watermark from Pepper salt noised watermarked image**

Rotation is very important in image processing operation. To test the robustness against rotation operation, the watermarked image is rotated by 90 degrees and then the watermark is extracted from rotated image. Figure 4.7 shows the visual quality of the extracted watermark from 90 degrees rotated watermarked image. The extracted watermark is compared withoriginal watermark image using different quality assessment metrics on each color planes.

**Figure 4.7 Extracted watermark from $90^0$ rotated watermarked image**

To check the robustness against filtering operation, the un-sharp filter was applied on watermarked image and thereafter the watermark was extracted from the filtered watermarked image. Figure 4.8 shows the visual quality of extracted watermark from un-

sharp filtered watermarked image.

**Figure 4.8 Extracted watermark from un-sharp filtered watermarked image**

Cropping of an image means to cut a part of the image. Accordingly, it is now required to identify whether the watermark is present in the cropped part of the watermarked image. Here, cropped parts of size 128*128 of the watermarked image are taken and then the watermark is extracted from the cropped part of watermarked image. Figure 4.9 shows the visual quality of extracted watermark.

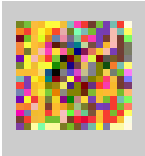

**Figure 4.9 Extracted watermark from 128*128 cropped part of watermarked image**

To show the performance regarding robustness of the above discussed technique two more attacks are performed on watermarked image, one is projective shearing and the other is adding some sparsity. Sparsity means adding some number of zeros in the image. Here, a vertical 128*256 sparsity is added into watermarked image. Figure 4.10 and Figure 4.11 show the visual quality of extracted watermark after the projective shearing operation and after adding 128*256 sparsity on watermarked image respectively.

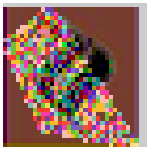

**Figure 4.10 Extracted watermark after projective shearing operation on watermarked image**

**Figure 4.11 Extracted watermark after sparsity (128*256) on watermarked image**

The performance of robustness against filtering, cropping, shearing and sparsity is evaluated by the quality assessment metric shown in Table 4.3. For filtering operation, the values of NC and SSIM are good in all the color planes that show the resemblance of extracted watermark with the embedded watermark even after the image is disturbed from

filtering operation. It is observed that NC and SSIM values of extracted watermark from cropped image are slightly lesser than 0.6 in general. This is obviously due to the relatively smaller size of the cropped part. However, the values confirm the presence of the watermark in the cropped part of the image. In the case of sparsity and shearing, the values of SSIM and NC in each color planes are nearly 0.7 in general, which is reasonably good for confirming the similarity of watermarks. Therefore, it may be concluded that the technique provides robustness to watermark against numbers of image processing attacks.

**Table 4.3 Robustness test against image processing operations**

| Attacks | PSNR | Red_NC | Gr_NC | Bl_NC | Red_SSIM | Gr_SSIM | Bl_SSIM |
|---|---|---|---|---|---|---|---|
| Gaussian Noise | 19.631 | 0.9596 | 0.8979 | 0.7136 | 0.8998 | 0.7916 | 0.6555 |
| Pepper Salt Noise | 18.953 | 0.9496 | 0.8579 | 0.7086 | 0.8783 | 0.7716 | 0.5955 |
| 90 Degree Rotation | 14.649 | 0.9293 | 0.7614 | 0.6682 | 0.8629 | 0.7311 | 0.6216 |
| Un-sharp Filtering | 11.232 | 0.8787 | 0.7583 | 0.7025 | 0.8073 | 0.6889 | 0.6665 |
| Cropping 128*128 | 13.089 | 0.7843 | 0.6339 | 0.5994 | 0.7723 | 0.6047 | 0.5418 |
| Projective Shearing | 8.5845 | 0.8555 | 0.7001 | 0.6879 | 0.7858 | 0.6530 | 0.6338 |
| Sparsity (128*256) | 11.649 | 0.8379 | 0.7487 | 0.8122 | 0.7912 | 0.6939 | 0.7979 |

## 4.2 A SECURE AND SEMI-BLIND TECHNIQUE OF EMBEDDING COLOR WATERMARK IN RGB IMAGE USING CURVELET DOMAIN

In this section a secure and semi-blind watermarking scheme is presented. The bit plane and HVS concepts are used for embedding the watermark into the images. To make the algorithm more secure, a cryptographic technique has been combined with it. As the proposed technique is semi-blind, a cover image is not required at the time of extraction.

### 4.2.1 Cover Image Preprocessing

The algorithm uses 24-bit true color image as cover image $I = \{x(i,j), 1 \leq i \leq M, 1 \leq j \leq N\}$ and watermark image as watermark $W = \{w(i,j) | 1 \leq i \leq m, 1 \leq j \leq$

$n$.To make the algorithm secure, a cryptographic approach is used. First, the cover image is preprocessed step by step as describe below:

i. Read the cover image ($I$) and decompose its RGB color planes. Let $I_{red}$, $I_{green,}, I_{blue}$ represent the red, green and blue color plane of the original cover image respectively.

ii. Divide each color plane. $I_{red}$, $I_{green,}, I_{blue}$ into blocks ($B_{k,}$) of 8* 8 size which are not overlapped to any other blocks. Where $k = 1,2, \ldots \ldots \left(\frac{(M*N)}{8*8}\right)$.

iii. For each color plane $I_{red}$, $I_{green,}, I_{blue}$, compute a new sequence $N_k$

iv. Let $L$ is the largest serial number, and $l$is the mid of series

If (mod ($B_{k,}$2) == 0) then $N_{k,}$= $L$; $L$= $L$-1

Else $N_{k,} = l$; and $l = l - 1$;

v. Combine the blocks with new sequences ($N_k$). The resulting image is called as processed image denoted by $I_{processed}$.

### 4.2.2 Embedding Algorithm

i. Obtain the processed image ($I_{processed}$) from the cover image I by applying the algorithm as discussed above.

ii. Decompose the processed image $I_{processed}$ into color planes. Let $IP_{red}$, $IP_{green,}, IP_{blue}$ represent the red, green and blue color plane of processed image $I_{processed}$ respectively.

iii. Perform a curvelet transform on each color plane with l number of scales and j decomposition levels.

iv. The watermark image is also colored image. Separate their color planes, $B_r$, $B_g$ and $B_b$, a red plane, green plane and the blue plane of the watermarked image respectively. Now obtain bit planes of each color plane. {$B_{r1}$, $B_{r2}$….$B_{r8}$}, {$B_{g1}$, $B_{g2}$…$B_{g8}$} and {$B_{b1,}$ $B_{b2}$…$B_{b8}$} are the set of bit planes of red, green and the blue color planes respectively.$B_{r8}$, $B_{g8}$ and $B_{b8}$ are most significant bit plane of red, green and blue color used as the watermark (to be embedded) and remaining other {$B_{r1}$, $B_{r2}$….$B_{r7}$}, {$B_{g1}$, $B_{g2}$…$B_{g7}$} and {$B_{b1,}$ $B_{b2}$…$B_{b7}$} are used as a key at the time of extraction.

v. Select the orientation and scale for embedding the watermark. Let the selected scale is j and orientation being k1, k2 and k3 for embedding the bit planes $B_{r8}$, $B_{g8}$, and $B_{b8}$ respectively. Let this be the selected domain of coefficients $Cs$.

vi. Each coefficient of the selected domain is compared with its 8 neighbor coefficients. Let $N_r$, $N_g$, and $N_b$ represent the total number of neighbors having values less than the coefficients of red, green and blue planes respectively.

vii. For each color plane, compute new matrix $U_r, U_g$ and $U_b$ by using following equations:

$$if\big((N_r \geq 4)\&\&B_{r8} == 1\big) than\ \mathrm{U_r} = 1\ ;\ Else\ \mathrm{U_r} = -1 \tag{4.11}$$

$$if\ \Big(\big(N_g \geq 4\big)\&\&B_{g8} == 1\Big)\ than\ \mathrm{U_g} = 1\ ;\ \ Else\ \mathrm{U_g} = -1 \tag{4.12}$$

$$if\big((N_b \geq 4)\&\&B_{b8} == 1\big) than\ \mathrm{U_b} = 1\ ;\ Else\ \mathrm{U_b} = -1 \tag{4.13}$$

viii. Modify the coefficients of selected domain as follows:

$$C'_s(j,k_1)) = Cs(j,k_1) + \alpha * \mathrm{U_r} \tag{4.14}$$

$$C'_s(j,k_2)) = Cs(j,k_2) + \alpha * \mathrm{U_g} \tag{4.15}$$

$$C'_s(j,k_3) = Cs(j,k_3)) + \alpha * \mathrm{U_b} \tag{4.16}$$

Where $\alpha$ is strength parameter as defined in equation 4.1.

ix. Convert this frequency domain $C'_s$ into time domain by applying the inverse curvelet transform.

x. Combine the entire three color plane and make it RGB image. Obtain watermarked image on the time domain signal and resulting watermarked image is represented by $I'$.

### 4.2.3 Extraction Algorithm

In a semi-blind method of extraction, we require a small part of information regarding watermark but do not require the cover image. The following procedure is performed to extract the watermark:

i. Read watermarked image $I'$and apply algorithm cover image processing on watermarked image as discussed in 4.2.1. The resulting image is called the watermarked processed image $I'_{processed}$ .

ii. Decompose the processed image $I'_{processed}$ into color planes. Let $IP'_{red}$, $IP'_{green,}$, $IP'_{blue}$ represent the red, green and blue color plane of watermarked processed image $I'_{processed}$ respectively.

iii. Perform a curvelet transform on each color plane $IP'_{red}$, $IP'_{green,}$, $IP'_{blue}$ with $j$ number of decomposition levels and l number of scales.

iv. Then select the scale and orientation used in procedure 4.2.2. This is treated as the key for extraction. The selected coefficients are denoted as $Z'$.

v. For each selected scale and orientation, do the following:

Each coefficient of the selected domain is compared with its 8 neighbor coefficients. Let $E_r$, $E_g$, and $E_b$ represent the total number of neighbors having value a less than the coefficient of red, green and blue planes respectively.

vi. Extract the watermark bit by using following equations:

$$(if(E_r \geq 4 \;\&\&\; U_r \equiv 1) than\; B'_{r8} = 1;\; Else\; B'_{r8} = 0 \tag{4.17}$$

$$(if\big(E_g \geq 4 \;\&\&\; U_g \equiv 1\big) than\; B'_{g8} = 1;\; Else\; B'_{g8} = 0 \tag{4.18}$$

$$(if(E_b \geq 4 \;\&\&\; U_b \equiv 1) than\; B'_{b8} = 1;\; Else\; B'_{b8} = 0 \tag{4.19}$$

vii. Combine the color planes to obtain R, G and B colors.

$$R = \sum_{i=1}^{8} B'_{ri} * 2^{i-1} \tag{4.20}$$

$$G = \sum_{i=1}^{8} B'_{gi} * 2^{i-1} \tag{4.21}$$

$$B = \sum_{i=1}^{8} B'_{bi} * 2^{i-1} \tag{4.22}$$

viii. Combine the R, G and B colors information as computed above to get the image of the colored extracted watermark.

### 4.2.4 Experimental Results

To test the algorithm, colored image "lena.jpg" is used a cover image and a colored image "thapar.jpg" is used a watermark image. Figure 4.1 and Figure 4.2 show the "lena.jpg" and "thapar.jpg" image respectively. In the algorithm, firstly, the cover image is processed using procedure of 4.2.1.

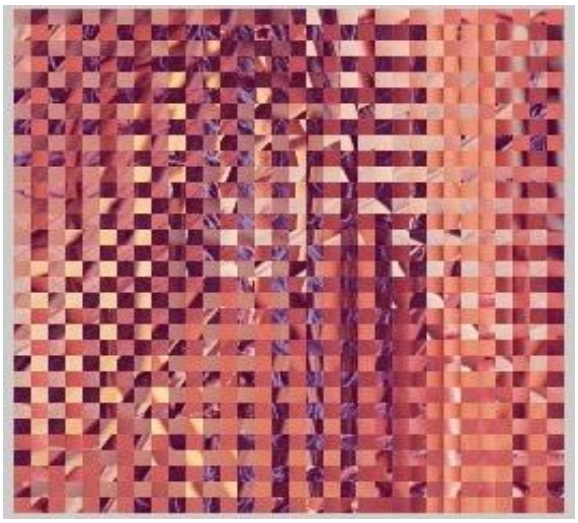

**Figure 4.12 Processed cover image**

Figure 4.12 shows the processed cover image. Figure 4.13 shows the resulting watermarked image. The technique has been tested against image operations such as invisibility, effectiveness, and robustness. The extracted watermark is shown by Figure 4.14.

**Figure 4.13 Watermarked image**

**Figure 4.14 Extracted watermark**

**Table 4.4 Performance evaluation**

| Test | PSNR | R_NC | G_NC | B_NC | R_SSIM | G_SSIM | B_SSIM |
|---|---|---|---|---|---|---|---|
| Invisibility | 44.94 | 0.9996 | 0.9996 | 0.9991 | 0.9941 | 0.995 | 0.9943 |
| Extraction | 38.562 | 1 | 1 | 1 | 0.9761 | 0.9981 | 0.9953 |

Next, we compare the quality of watermarked image and extracted watermark with respect to the above defined quality assessment metrics such as PSNR, NC, and SSIM. Table 4.4 shows the visual quality of watermarked image and R_NC, G_NC, B_NC, R_SSIM, G_SSIM, and B_SSIM represent the Normalized Correlation (NC) and SSIM of the red(R), green (G) and blue (G) color respectively. Table 4.4 shows the values of quality assessment metrics. The table shows the similarity index of each color plane with the original one. The values of PSNR, NC, and SSIM demonstrate that the quality of watermarked image is same as that of the original image. The value of NC is 1 for each color plane which demonstrates that the quality of extracted watermark is similar to the original embedded watermark.

To show that the algorithm gives good robustness, different image processing operations are applied to the watermarked image. The quality of the extracted watermark from the distorted watermarked image has been analyzed with respect to the quality assessment metrics. Table 4.5 shows the values of quality assessment metrics after extracting the watermark from the Gaussian noised, Salt & Pepper noised and rotation application. Table exhibits that the embedded watermark is robust against the addition of noise and rotation.

**Table 4.5 Performance of extracting the watermark under image processing attacks**

| Attacks | PSNR | R_NC | G_NC | B_NC | R_SSIM | G_SSIM | B_SSIM |
|---|---|---|---|---|---|---|---|
| Gaussian Noise | 19.631 | 0.9596 | 0.8979 | 0.7136 | 0.8998 | 0.7916 | 0.6555 |
| Pepper Salt Noise | 18.953 | 0.9496 | 0.8579 | 0.7086 | 0.8783 | 0.7716 | 0.5955 |
| 90 Degree Rotation | 14.649 | 0.9293 | 0.7614 | 0.6682 | 0.8629 | 0.7311 | 0.6216 |
| Un-sharp Filtering | 11.232 | 0.8787 | 0.7583 | 0.7025 | 0.8073 | 0.6889 | 0.6665 |
| Cropping 128*128 | 13.089 | 0.7843 | 0.6339 | 0.5994 | 0.7723 | 0.6047 | 0.5418 |
| Projective shearing | 8.5845 | 0.8555 | 0.7001 | 0.6879 | 0.7858 | 0.653 | 0.6338 |
| Sparsity (128*256) | 11.649 | 0.8379 | 0.7487 | 0.8122 | 0.7912 | 0.6939 | 0.7979 |

Table 4.5 also shows the performance of proposed technique with respect to filtered, projected and sparse image processing operations. Values of NC in every test are above 0.8 which show that the extracted watermark is very similar to original watermark. Values of SSIM are also above 0.65 in each test confirming that contrast, luminance and the structure of watermarked image are very similar to original one. Values of NC and SSIM confirm the similarity of extracted watermark with the original watermark as well as the quality of extracted and watermarked image is reasonably high. Table 4.4 and Table 4.5 confirm that technique gives good invisibility, effectiveness, and robustness.

Further, the performance of the proposed technique is evaluated against different image processing attacks with various density and variance. Figure 4.15 shows the NC and MSSIM values of watermark extracted from the watermarked image which carries Gaussian noise with a different variance.

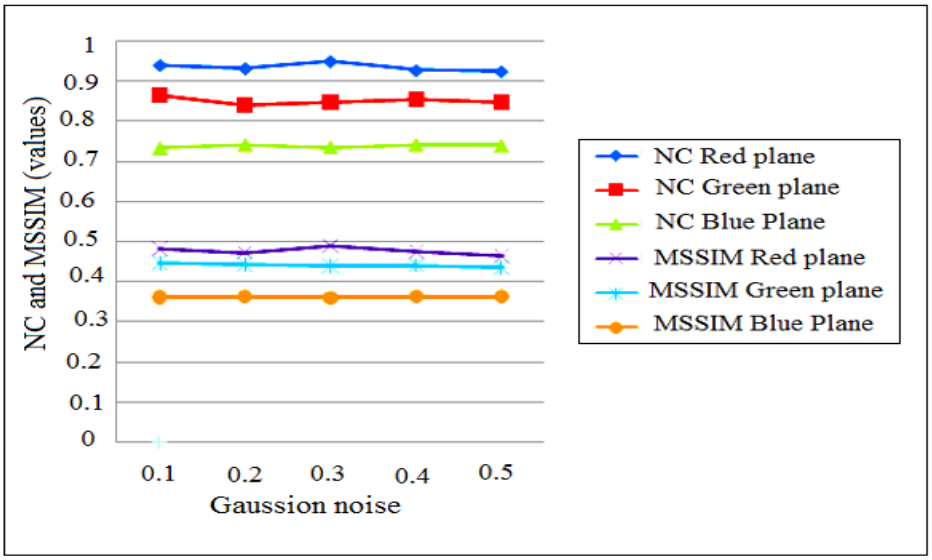


**Figure 4.15 NC and MSSIM of extracted watermark with different Gaussian noise variance**

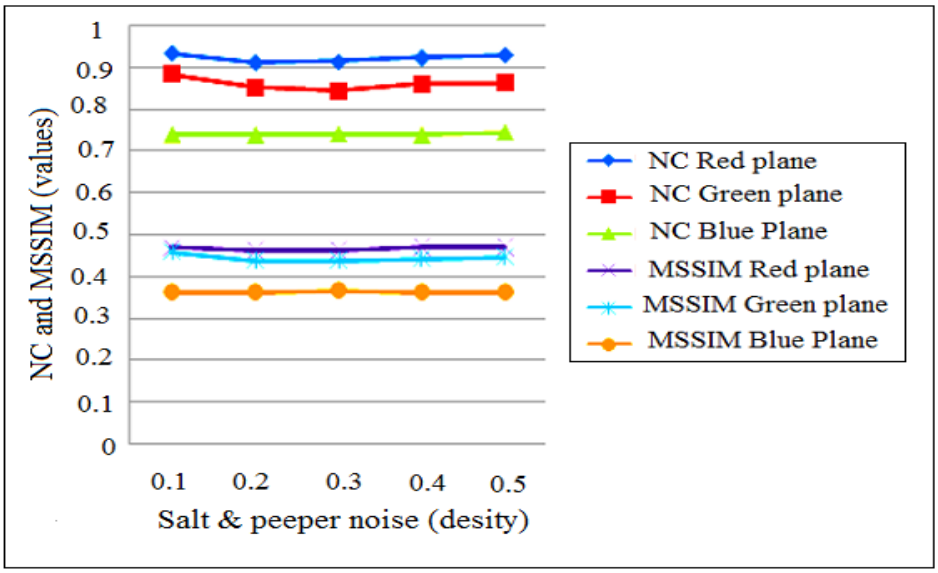


**Figure 4.16 NC and MSSIM of extracted watermark from pepper & salt noised image with different density**

Figure 4.16 shows the performance of each color planes with watermark extracted from pepper & salt noised watermarked image with different density. From both the Figures, it is concluded that the most affected area is the blue plane but as the human eyes are less sensitive to the blue plane, it may be concluded that the proposed technique gives enough robustness against noise addition.

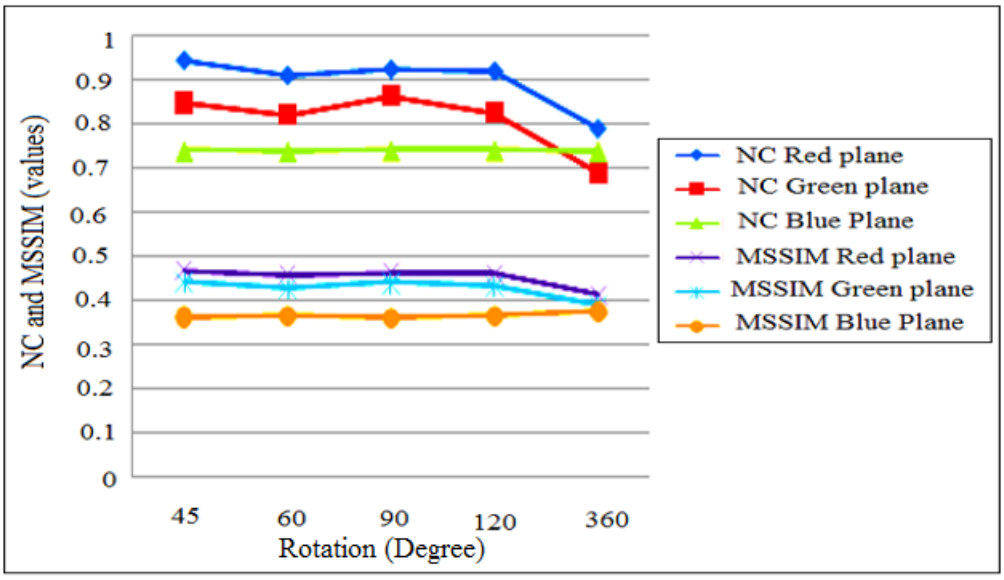


**Figure 4.17 NC and MSSIM of extracted watermark with rotated image**

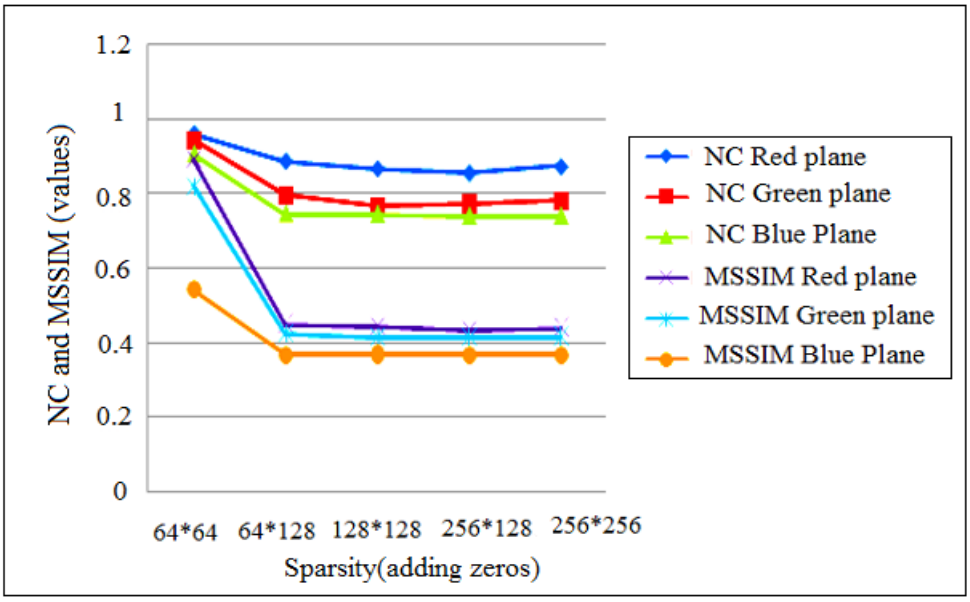


**Figure 4.18 NC and MSSIM of extracted watermark with sparse image with different number of zeros**

Figure 4.17 and Figure 4.18 show the performance of proposed algorithm against rotation and sparse operations. It is also observed from the figures that the values of MSSIM on all plane are very good. The visual quality of extracted watermark is visibly good, so it is concluded that the proposed algorithm provides a technique that is relatively more robust against the image processing attacks.

## 4.3 CONCLUSION

This chapter considered two semi-blind techniques for watermark embedding in the curvelet transform coefficients. The first technique is introduced for embedding a logo image watermark into the curvelet coefficients of blue color plane by using bit plane

method. The second technique combines the properties of cryptography and watermarking. Both algorithms are the application on the color image and provide watermark robustness against attacks (image processing operation). In the presented technique, the effectiveness of using different scaling factors was examined in relation to robustness and invisibility. The performance assessment metrics such as PSNR, NC and SSIM are used for evaluating the performance of the technique.

# CHAPTER 5

# NOVEL BLIND WATERMARKING TECHNIQUES

In this chapter, two novel blind watermarking techniques are proposed. First watermarking technique is used curvelet transform and luminance of color image to detect tamper. The first technique embedded the watermark in curvelet domain by using clustering. The similarity of extracted watermark and original watermark are used to identify whether an image is tampered or not. Filters and morphological operators are used to locate the exact region of tamper. An ECG watermarking technique is the second technique for securing patient information. In this technique, the patient's information is inserted into the curvelet transform of ECG signals. The QRS complex attributes of ECG are preserved so that the embedding of patient information does not affect the diagnosability.

## 5.1 IMAGE FORGERY DETECTION USING CURVELET TRANSFORM

In this section a color image forgery detection method using watermarking and curvelet transform is proposed. The RGB cover image is converted into $YC_bC_r$ color plane to obtain the luminance. That will provide security and robustness to the watermark. Then, the luminance part of the image is converted into curvelet domain and clustering approach is used to embed the watermark into the selected scale and orientation of curvelet domain. For extracting the watermark, a blind approach is used. Hence, there is no need of original cover image at the time of extraction. At last, the results from the technique are analyzed with performance evaluation metric and are also compared with existing techniques. The following sections describe the algorithms and results.

### 5.1.1 Watermark Embedding

The algorithm has used 24-bit true color image as host image (I), a binary random sequence is the watermark that is generated using a secret key. As $YC_bC_r$ color planes are best suited for digital image processing as well as luminance$(Y)$, they can be stored separately in high resolution and chromatic $C_b$ and $C_r$ components treated separately to enrich the storage performance. The procedure of watermark embedding is described in following steps:

i. To utilize the benefits of $YC_bC_r$ color space, firstly, the RGB color space host image I is converted into the $YC_bC_r$ color space. Equation given below are used to convert the color space [80].

$$\left.\begin{matrix} Y = (0.257 * R) + (0.584 * G) + (0.098 * B) + 16 \\ C_b = (-0.148 * R) + (0.291 * G) + (0.439 * B) + 128 \\ C_r = (0.439 * R) + (0.368 * G) + (0.071 * B) + 128 \end{matrix}\right\} \quad (5.1)$$

ii. Here R, G and B are the red, green and blue color planes of the cover image (I) and $Y$,$C_b$ and $C_r$ are luminance, chroma blue and chroma red respectively. The grayscale cover image is quite similar to the luminance of that image. Therefore, it is used as the embedding domain. $C_b$ is strong wherever parts of the image contain blue color. For red color $C_r$ is strong.

iii. Luminance $Y$ is converted into frequency domain by applying curvelet transform. We can obtain the number of scales $p_{scale} = log_2 p - 2$, where p*p is the size of the image.

iv. Select the scale s and orientation j in curvelet transform. The selection of curvelet transform and its coefficients affect the invisibility and robustness of watermark. Since the most of the energy is packed into the lower bands of curvelet coefficient, therefore, it is desirable to hide the watermark in the lowest level. Let selected domain of curvelet be denoted by $Z$.

v. Classification of coefficients: Let the selected domain ($Z$) contain $n$ number of curvelet coefficients. Let $L$ be the greatest coefficient and $s$ be the smallest coefficient $Z$. Set initial cluster centers and divide the $Z$ into $N$ equal intervals. Then find out cluster's centers $c_i = \frac{i}{N}L$ , $c_0 = 0$, $c = \frac{i}{N}s$, Where $1 \leq i \leq N-1$. For each cluster center $C_j$, calculate the Euclidean distance where Euclidean distance$(D_{i,j})$is shown in equation:

$$D_{i,j} = |Z_i - C_i| \quad (5.2)$$

vi. The above step divides the $Z$ coefficients into clusters ($d$). Number of clusters control the embedding capacity of the algorithm. In every group of cluster $d$ a watermark bit is embedded. The watermark is generated using the secret key k on a binary random sequence $w$. The number of clusters of curvelet coefficients is same as the length the watermark sequence.

vii. The above step divides the $Z$ coefficients into clusters ($d$). Number of clusters control the embedding capacity of the algorithm. A watermark bit will be embedded in every group of clusters $d$. The watermark is generated using the secret key k on a binary random sequence $w$. The length of this watermark is the same as the number of clusters of curvelet coefficients.

viii. For give more robustness against attacks, the weighted mean $M_i$ of every cluster of curvelet coefficients is computed using below equation:

$$M_i = \sum_{j=1}^{d} (-1)^j * Z_j\,(c_i) \tag{5.3}$$

Where, $Z_j(c_i)$ denotes the j[th] coefficient of group i.

ix. Initialize the quantization size $Q$. The sensitivity of tampering detection depends upon $Q$. If $Q$ is large, tampering sensitivity increases, but with larger size of quantization the visual quality of watermarked image decreases. For each cluster $i$ compute a new weighted mean matrix $M_{i(new)}$ by using equation:

$$M_{i(new)} = \begin{cases} M_i & if(M_i\%2 == w_i) \\ M_i + Q & otherwise \end{cases} \tag{5.4}$$

x. Due to the random operation, every cluster must contain one coefficient that have an absolute value. Therefore, the next step is to modify the value of the highest coefficient of each cluster $i$ using the equation:

$$Z_{imax}(j) = Z_{imax}(j) + (-1)^j * (M_{i(new)} - M_i) \tag{5.5}$$

xi. Apply an inverse curvelet transform on modified coefficients to convert frequency domain into time domain and get the modified values of luminance, chroma blue and chroma red denoted by $Y'C_b'C_r'$ respectively.

xii. Then use the equation given below on $Y'C_b'C_r'$ to convert the $YC_bC_r$ color image into the RGB color image [80].

$$I_w = \left\{ \begin{matrix} R = 1.164(Y' - 16) + 1.596(C_r' - 128) \\ G = 1.164(Y' - 16) - 0.391(C_b' - 128) - 0.813(C_r' - 128) \\ B = 1.164(Y' - 16) - 2.018(C_b' - 128) \end{matrix} \right\} \tag{5.6}$$

The resulting image $I_w$ is called watermarked image.

### 5.1.2 Watermark Extraction

This algorithm proposes blind watermarking extraction so that cover image is not needed to extract the watermark. The watermarked image obtained from 5.1.1 algorithm

is treated as the input for extraction process. To extract the watermark follows the following steps:

i. The watermarked $I_w$ is first converted from RGB color space to $YC_bC_r$color space by using 5.1 equation. Here, the luminance of this watermarked image is denoted by $Y'$. Then, luminance $Y'$is decomposed into frequency domain using curvelet transform. By applying curvelet transform, the number of scales ($p_{scale} = log_2 p - 2$, where p*p is the size of the image) are obtained. Then we select the scale and orientation that are used in procedure 5.1.1. The corresponding coefficients are treated as a key for extraction process. The selected coefficients are denoted as $Z'$.

ii. The selected coefficients $Z'$ are divided into $d'$ number of clusters by using the procedure discussed above. Calculate the weighted mean $M_i^{'}$ of every cluster $i$ by using equation (5.3).

iii. Extract the watermark w' from the weighted mean $M_i^{'}$ of every cluster.

iv. If ($M_i^{'}\%\ Q == 0$ ) then $w_i^{'} = 0$ otherwise $w_i^{'} = 1$ . Combine the $w_i^{'}$ sequence. It is assumed to be same as the embedded sequence.

**5.1.3 Tampering Detection**

If the watermark sequence extracted by the procedure 5.1.2 i.e. $w^{'}$ is equal to embedded (original) watermark w, then the watermarked image is genuine i.e. no tampering has taken place. But if extracted and embedded sequences are not same then some tampering has been done with the image. To locate the tampering region in the watermarked image, follow the following steps:

i. Coefficients belonging to cluster $i$ are marked if extracted watermark bit $w_i^{'}$ is not equal to embedded watermark bit $w_i$.

ii. All the marked coefficients are now spread over the selected scale. The highest density of marked coefficients contains the actual tamper region. The other marked coefficients are like a random noise and they appear isolated in the cluster. These isolated coefficients are treated as false positive detection.

iii. A same size of binary authentic matrix (B) of the selected scales is used to find the tampered region by using equation below:

$$\left(B(x,y) = \begin{matrix} 1 & if Z'(x,y)\ is\ mapped \\ 0 & otherwise \end{matrix}\right) \quad (5.7)$$

iv. To remove the isolated ‘1’ bits in the matrix B, the filtering operation is applied. Filtering operation will remove the isolated ‘1’ and solve the false positive detection.

v. Further morphological operator erosion and dilation are successively applied on matrix B. Now ‘1’ bits appropriately locate the tampered region. The mapped positions in B are then converted into the time domain by using inverse curvelet transform, to indicate the actual tampered locations.

### 5.1.4 Results and Discussion

To test the technique an RGB image is practiced as a cover image as shown in Figure 5.1. To embed the watermark, the procedure as discussed in section 5.1.1 is applied on figure 5.1. The resulting image is shown in Figure 5.2, which is called as the watermarked image.

**Figure 5.1 Cover image**

The visual quality of the original image is very much similar to the watermarked image. Even upon careful examination of both the images, human eyes are not able to find any difference between them. The resemblance of the watermarked image and cover image demonstrates that invisibility of the watermark is very good.

**Figure 5.2 Resulted Watermarked image**

Table 5.1 shows the BER of extracted image with different scales of curvelet, quantization level (Q) and the cluster size (d). Values of BER are extremely less. This proves that the visual quality of watermarked image is very high as well as the proposed technique gives a higher level of invisibility.

**Table 5.1 BER of extracted watermark with different scales of curvelet, quantization level (Q) and the cluster size (d)**

| D | Q | n=2 | n=3 | n=4 |
|---|---|---|---|---|
| 8 | 4 | 0.3333 | 0.4543 | 0.523 |
| 8 | 8 | 0.0534 | 0.1576 | 0.0534 |
| 8 | 12 | 0.1767 | 0.0466 | 0.0532 |
| 8 | 16 | 0.3398 | 0.0875 | 0.0625 |
| 8 | 20 | 0.5977 | 0.0823 | 0.0705 |
| 8 | 24 | 0.5667 | 0.0853 | 0.0565 |
| 12 | 4 | 0.1498 | 0.1342 | 0.7843 |
| 12 | 8 | 0.3166 | 0.2222 | 0.1534 |
| 12 | 12 | 0.8958 | 0.0456 | 0.0343 |
| 12 | 16 | 0.946 | 0.0254 | 0.0223 |
| 12 | 20 | 0.8978 | 0.0346 | 0.0223 |
| 12 | 24 | 0.7867 | 0.0212 | 0.0112 |
| 16 | 4 | 0.1589 | 0.3546 | 0.9212 |
| 16 | 8 | 0.255 | 0.2134 | 0.123 |
| 16 | 12 | 0.556 | 0.0245 | 0.0165 |
| 16 | 16 | 0.9866 | 0.0232 | 0.0165 |
| 16 | 20 | 1.256 | 0.0512 | 0.0132 |
| 16 | 24 | 0.966 | 0.0234 | 0.0032 |

To obtain the robustness of the above discussed technique, image processing operation such as noise addition and rotation, have been applied on watermarked images. Table 5.2 shows the robustness in term of BER with different scales and quantization. In the table, the watermark is extracted from a watermarked image afflicted with Gaussian noise, salt & pepper noise, and rotation operation. It is observed from the table that the quality of extracted watermark is good with lower BER. The technique is robust against noise addition and rotation operation.

**Table 5.2 Robustness test in term of BER with different scales and quantization**

| | | **Bit Error Rate (BER)** | | | |
|---|---|---|---|---|---|
| **Attacks** | **Variance** | **N=3,d=8, Q=12** | **N=3,d=12, Q=12** | **N=4, d=8, Q=12** | **N=4, d=12, Q=12** |
| Pepper & salt noise | 0.1 | 0.04 | 0.0323 | 0.023 | 0.0200 |
| | 0.2 | 0.08 | 0.0543 | 0.0453 | 0.3451 |
| | 0.4 | 0.12 | 0.0978 | 0.7647 | 0.7342 |
| | 0.6 | 0.154 | 0.1356 | 0.1103 | 0.1000 |
| | 0.8 | 0.24 | 0.2297 | 0.2099 | 0.2010 |
| | 1 | 0.27 | 0.2546 | 0.2401 | 0.2376 |
| Gaussian noise | 0.1 | 0.03 | 0.0287 | 0.2133 | 0.1231 |
| | 0.2 | 0.09 | 0.0753 | 0.0643 | 0.0555 |
| | 0.4 | 0.14 | 0.1219 | 0.1032 | 0.9543 |
| | 0.6 | 0.186 | 0.1543 | 0.1456 | 0.1123 |
| | 0.8 | 0.256 | 0.2245 | 0.2057 | 0.2000 |
| | 1 | 0.31 | 0.2871 | 0.2753 | 0.2564 |
| Rotation | 5 | 0.08 | 0.0542 | 0.0487 | 0.3302 |
| | 10 | 0.1345 | 0.1201 | 1.110 | 0.9321 |
| | 20 | 0.1678 | 0.1487 | 1.2146 | 1.9922 |
| | 40 | 0.2456 | 0.2234 | 0.2017 | 0.1985 |
| | 60 | 0.357 | 0.3402 | 0.3298 | 0.3124 |

To locate the tampered portion of an image, two regions of the watermarked image shown in Figure 5.2 were tampered. First, face of the girl (second row rightmost)

has been replaced by some other girl face and second the envelope in the hand of the boy (left most 1st row) has been replaced by a bag.

**Figure 5.3 Tempered image**

Figure 5.3 shows the tampered image, where tampered regions are encircled. Firstly, we detect the watermark from the coefficients of the curvelet transform by selecting the scale = 2 using cluster number d=8, and quantization Q=16. Because n=2, the tamper detection resolution of the proposed algorithm is 4*4 pixels. We can easily see the noise and actual tamper region in the cluster. Cross shaped filter of size F=5 is applied to remove the isolated '1' bits from the authentic metric B. Further morphological operator erosion with disk of radius (R=1) and dilation of 3*3 size are successively applied on the authentic matrix. Now '1' bits correctly indicate the tampered region.

**Figure 5.4 Detection of tempered regions**

Figure 5.4 indicates the actual tampered locations. The white rectangles show the tampered region. As observed, in figure the tampered image is encircled. Figure 5.4 exactly whitens the encircled areas. From the figure, it is confirmed that the above discussed algorithm locates the tampered region correctly.

To emphasize the superiority of the technique, its performance is compared with two other image authentication techniques based on DWT. For the sake of easiness these two authentication techniques are named as tamper localization [90] and block based method [112]. Figure 5.5 shows the comparison of PSNR with different quantization.

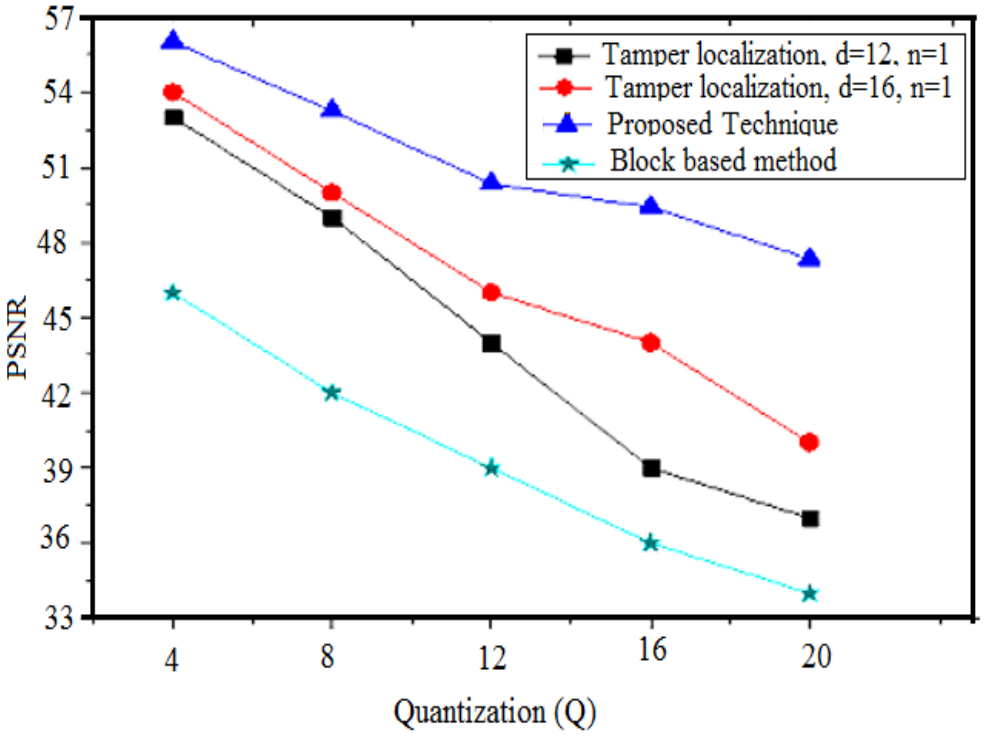


**Figure 5.5 Quality of watermarked image compared with traditional authentication methods**

As discussed above, the quantization affects the invisibility of watermark. As quantization increases, watermark payload capacity of the technique is also increased. But the payload capacity affect the visual quality of watermarked image therefore the PSNR value of the watermarked image goes down. It is observed from the figure that values of PSNR for every quantization level are higher in proposed algorithm as compared to tamper localization and block based methods. Hence, it is proved that the presented technique provides a superior visual quality of watermarked image.

## 5.2 ECG WATERMARKING TECHNIQUE USING CURVELET TRANSFORM

A variety of electronic equipment is used in medical field for quick and correct diagnosis of diseases. In E-health application, patients are monitored constantly using wearable medical devices which accumulate their physiological signals. These signals are then broadcast to the hospital servers over wireless or wired media. This enables the physicians to diagnose and treat the disease of even those patient, who are unable to visit the hospital regularly. In contrast, e-health system sends bio-medical and personal informationof the patient to the server without any data protection. This information can be accessed, intercepted, tampered, falsified and hacked, which compromises the privacy of the patient and affects the diagnosis of the disease [124]. In 1996 Health Insurance Portability and Accountability Act (HIPAA) came into effect. The act mandated the confidential and private information related to the patient be protected and communicated with the help of internet and stored in a secured manner [125].

### 5.2.1 ECG Signal Converted to 2D Image and Transformed into Curvelet Domain

The activity of the heart muscles changes with time, to measure or represent these changes medical term electrocardiogram (ECG) is used. In medical field ECG is a simple representation of heart pulse to diagnose the heart disease. It can provide useful information and remains a crucial element for the assessment of cardiac patients. So, a biomedical 1D ECG signal from MIT-BIH arrhythmia database [126] sampled at 128Hz is used as input. Figure 5.6 shows the 1D ECG signal.

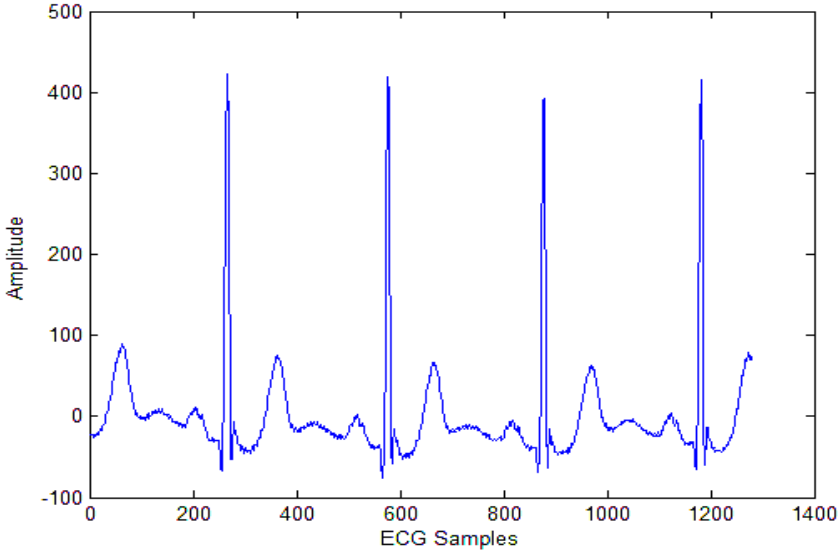


**Figure 5.6 Original 1D ECG signal**

ECG contains several waves. Out of these QRS waves, are the major element for diagnosing a cardiac disease. Normal QRS width is 70-100ms (milli second) for a healthy person. To determine the source of each QRS complex (heart wave), the width of QRS is utilized. QRS > 100 (broader width) diagnoses that heart complex travel to lower chamber of the heart i.e. ventricle in origin. For QRS<100 (narrow width) heart waves origin above the ventricle of the heart (Supraventricular complex). To detect these QRS complex attributes, Tompkins algorithm [127] is used.

In Tompkins algorithm, the 1D EGC signal is squared after filtration from a band pass filters. To remove the noise from the squared ECG signals, the signal is averaged with moving window. And to obtain the fiducial mask, QRS complex is localized to a particular instant of time. Then algorithm again searches for any missed QRS complex, next it abrogate multiple detection within defined period. At last, R-wave, P-wave and the QRS complex are identified in ECG signals. These characteristics of waves (R-wave, P-wave and the QRS complex) are main components to identify any disease. To convert a 1D ECG signal into a 2D image, 28Hz sampling rate is selected and take 64 points of fiducial mask from both sides of each trained ECG [116]. Now the 1D ECG signal is converted into 2D ECG image. The size of this 2D image depends upon the number of ECG trains. Fiducial mask are also employed to change the 2D ECG image into 1D ECG signal with negligible data loss,but this loss does not affect the diagnosability of the disease. Figure 5.7 shows the 2D ECG image produced from 1D ECG signal.

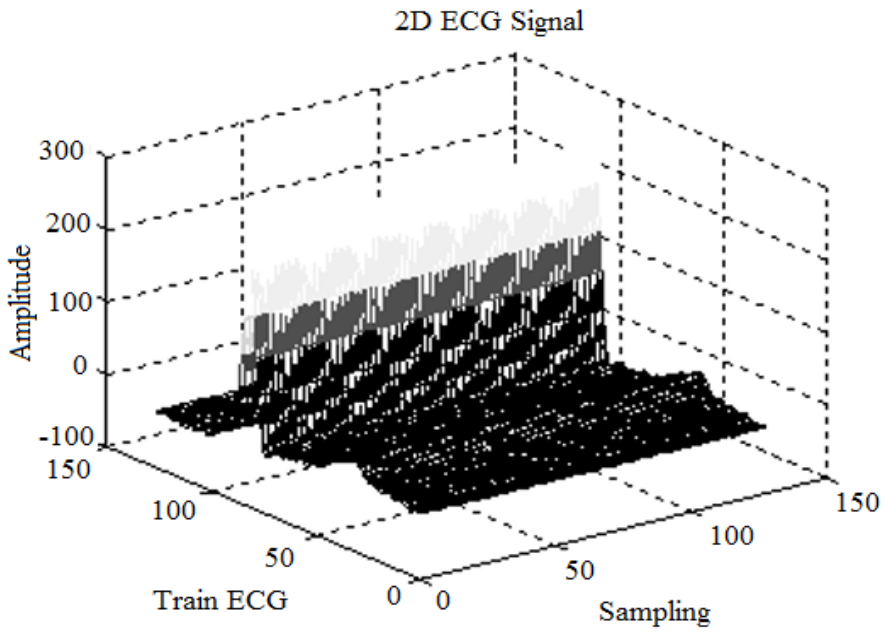


**Figure 5.7 2D ECG image**

### 5.2.2 Processing Patient Information

The main objective of this section is to gather patient information and process it in such a way that illegal one cannot access or tamper the confidential information of the patient. The personal information of the patient is saved in text and is then converted into an image. Embedding image in ECG is easy and provides a decent quality extracted watermark. Figure 5.8 shows an example of patient information that could be embedded into the curvelet transform of ECG signal.

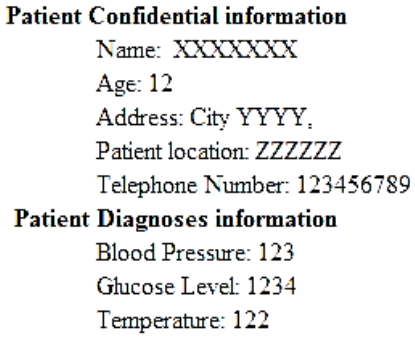


**Figure 5.8 Image of patient information**

### 5.2.3 Curvelet Transform Coefficients Clustering

The host 2D ECG image is disintegrated into the frequency domain applying Curvelet Transform (CT) on it. After decomposition, the 2D ECG image is divided into two levels: Coarse and Detail. Here, we selected the coarse level (C) as embedding domain because almost energy of the ECG image is packed down into the lower-band.

Let coarse level (Z) contains n number of curvelet coefficients. Euclidean distance b/w the coefficients can be chosen as a non-similarity measure. With the help of Euclidean distance $D_{i,j} = |Z_i - Z_j|$ where $i, j = 1,2 \ldots \ldots \ldots$ Domain Z is separated into c number of subsets called clusters based upon the Euclidean distance $D_{i,j}$. Next we find the cluster's center $c_i, i = 1,2 \ldots \ldots$ as the mid-point of the clusters. Divide the domain $Z$ into $N$ equal intervals by using the following equation.

$$c_i = \frac{i}{N} L \ , \quad c_0 = 0, \quad c = \frac{i}{N} s \tag{5.8}$$

Where $L$ is the greatest coefficient and $s$ is the smallest coefficient in the domain $Z$. If $s > 0$, we just take the greatest coefficient $L$ $and$ $1 \leq i \leq N - 1$.Then, classify the coefficients according to the minimum Euclidean distance and put the coefficient corresponding to the cluster centers. The total number of clusters is $2N - 1$. They are

$B_i, B_0, B_{-i}$ . Then update cluster's center by using a threshold $T_h = 0.1$, $A_j$ = average value of $B_i$, $T_i = A_i - A_j$. If $T_i > T_h$, update the cluster center. The algorithm divides coefficients into clusters ranging from $B_{(N-1)}$ to $B_{-(N-1)}$. Patient's information image is inserted into clusters between $B_{(N-1)} - B_0$, and $B_0 - B_{-(N-1)}$ .

**5.2.4 Embedding Procedure**

Select a cluster for hiding patients information. Let it be cluster $B_i$ to $B_j$. Rename the selected cluster $S_1$, $S_2 \ldots\ldots S_k$, where $k = 2(i-j) + 2$. For cluster $S_i$, find the radii of cluster by using following equations and use it as the key for embedding.

$$r_{i1} = c_i - \min(S_i) \tag{5.9}$$

$$r_{i2} = c_i - \max(S_i) \tag{5.10}$$

Where $r_{i1}$ and $r_{i2}$ are the radii of cluster $S_i$, and $c_i$= center of the $S_i$

For each selected cluster $k$ evaluate$R_0, R_1, M_0$ and $M_1$using the following equations:

$$R_0(k) = c_i - {}^{x}/_{X} * r_{i1} \tag{5.11}$$

$$R_1(k) = c_i - {}^{(x-1)}/_{X} * r_{i1} \tag{5.12}$$

$$M_0(k) = c_i + {}^{x}/_{X} * r_{i2} \tag{5.13}$$

$$M_1(k) = c_i + {}^{(x-1)}/_{X} * r_{i2} \tag{5.14}$$

Where $X = N$ be the integer number N that is used in clustering for a number of cluster classes and $x = 1,2, \ldots\ldots X$. Every coefficient must belong to any of $R_0$,$R_1$,$M_0$ and $M_1$ set For each curvelet coefficient, find the cluster number of the coefficient of Z. If cluster number is not equal to $S_i$ (selected cluster), find the cluster number of the next coefficient of curvelet Otherwise, patient information is added to Z by using following equation:

$$\begin{cases} Z' = Z - \frac{1}{X} * ri2 & \text{if } (R_0 \geq Z \geq M_1) \\ Z' = Z - \frac{1}{X} * ri1 & \text{if } (R_1 \geq Z \geq M_0) \\ Z' = Z & \text{Otherwise} \end{cases} \tag{5.15}$$

Now, apply inverse curvelet transform on Z' to convert frequency domain image into the time domain.

### 5.2.5 Extraction Procedure

The proposed technique investigates the blind extraction method, in which host 1D EGC signal is not required to detect or extract hidden information. The process of extracting patient's information from the watermarked ECG is as follows:

Read the watermarked 1D ECG and convert it into a 2D image, then transformed the image into transform domain by applying the curvelet transform. Select the scale to be used by the embedding procedure, where selected scale will be treated as the first key to extraction. Classify the curvelet coefficients by using clustering algorithm discussed above. Curvelet coefficients are clustered from $B_{(N-1)}$ to $B_{-(N-1)}$. Selected cluster $B_i \ldots \ldots B_j$ is another key for extraction. Apply another key $\mathrm{R_{i1}}$, $\mathrm{R_{i2}}$, $X$ and obtain the threshold $T_h$ and calculate $\mathrm{R_0, R_1, M_0, M_1}$ for each cluster as discussed earlier. For each coefficient of curvelet domain $Z'$, find the cluster number. If cluster number is not equal to $B_i$ (selected cluster), then the watermark (W) is not there. Otherwise extract the watermark using equation:

$$\begin{cases} \mathrm{W} = 1 & \text{if (And } ((\mathrm{M_0} \le \mathrm{Z} \le \mathrm{M_1}, \mathrm{X\%2} == 1)) \\ \mathrm{W} = 1 & \text{if(And } ((\mathrm{R_0} \le \mathrm{Z} \le \mathrm{R_1}, \mathrm{X\%2} == 1) \\ \mathrm{W} = 0 & \text{Otherwise} \end{cases} \tag{5.16}$$

### 5.2.6 Experimental Results

For experiment, MIT-BIH arrhythmia database [126] are source of the ECG signals that sampled at 128Hz. Figure 5.6 and Figure 5.7 show the 1D ECG signal and 2D ECG image respectively.

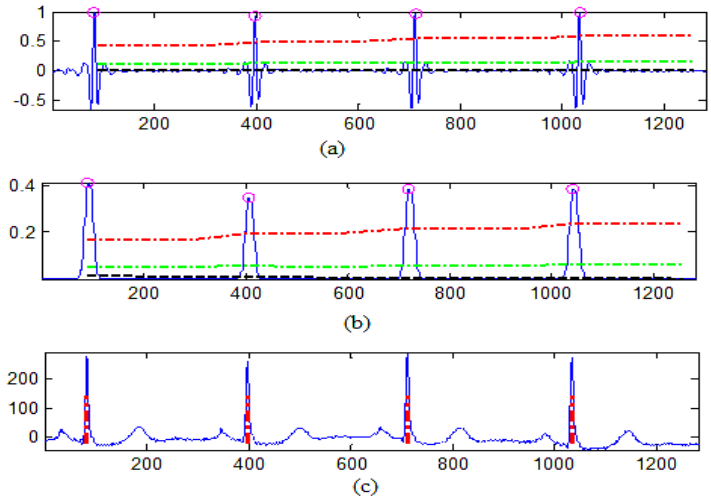


**Figure 5.9 QRS detection (a) QRS on filtered signal, (b) QRS complex and signal level(red), Adaptive Threshold(green) and Noise level (Black) (c) Pulse train of detected QRS on ECG signal**

Figure 5.8 shows the patient information in image format. QRS complex, R wave are the most important attributes of ECG signal. Figure 5.9 (above) shows detection of QRS complex attributes in original 1D ECG. The fiducial point's value is maximum on the peak of R wave or at slope of QRS. The watermarked ECG signal obtained from the proposed technique is shown in Figure 5.10. It is observed that the watermarked ECG signal has no difference with the original ECG signal and it has preserved the QRS complex attributes. Both the signals are indistinguishable.

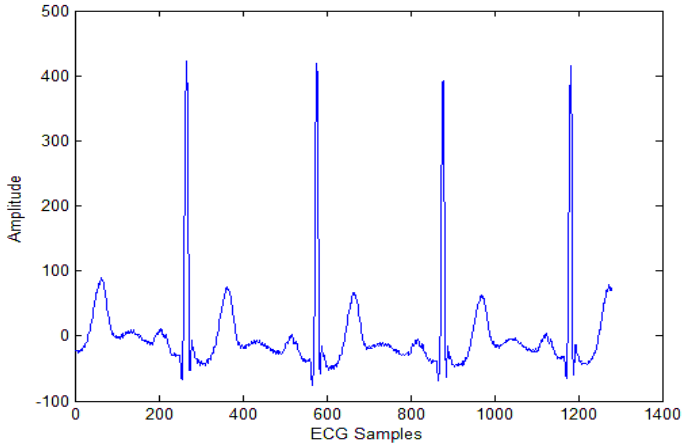


**Figure 5.10 Watermarked ECG**

The proposed method is tested against the different size of watermark and cluster size and the results are presented in below Table 5.3. It is observed that the size of the watermark does not affect the diagnosability of ECG. The similarity of original and watermarked ECG is verified by the values of PSNR, NC, MSE, BER and SSIM, which is one shown in Table 5.3.

**Table 5.3 Performance of proposed technique with different watermark sizes and clusters**

| Cluster | Watermark size | PSNR | NC | KL | MSE | PRD | BER | SSIM |
|---|---|---|---|---|---|---|---|---|
| 0-1 | 32*32 | 84.513 | 1.000 | 1.9989e-005 | 5.11674e-005 | 0.0421 | 0 | 1.000 |
| 0,1 | 64*64 | 79.748 | 1.000 | 2.1533e-005 | 5.7621e-005 | 0.0545 | 0 | 1.000 |
| 0,1,2 | 80*80 | 83.627 | 1.000 | 0.0001 | 0.0001 | 0.0494 | 0 | 1.000 |
| 0,1,2,3 | 100*100 | 74.285 | 1.000 | 0.0007 | 0.0005 | 0.0674 | 0.011 | 1.000 |
| 0-7 | 128*128 | 66.825 | 1.000 | 0.0012 | 0.0011 | 0.0967 | 0.214 | 1.000 |

As we know the size of patient's information will reduce the quality of a signal. But, in proposed technique, the large size of watermark also gives good imperceptibility and it is verified by the values of various metrics e.g. MSE, BER, NC, KL, and PRD. By analysis of performance metric values provided in the table, it is concluded that the proposed technique allows a safe transfer of patient's information transmission without compromising the diagnosability and imperceptibility.

The quality of extracted patient information is also compared with the original embedded information. In the proposed technique, the embedded information is in the form of an image, which gives the benefit that a minor change in data will not affect the whole image. Figure 5.11 shows the visual quality of extracted watermark and performance evaluation of the original and watermarked ECG.

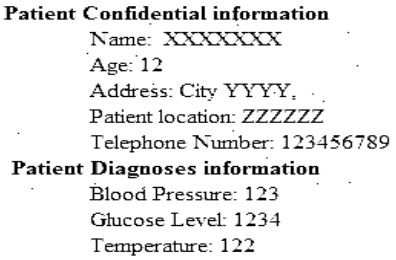


**Figure 5.11 Extracted patient information, PSNR =65.31, MSE= 1.8649e+004, NC=1, BER=0, SSIM=0.9911**

**Table 5.4 Robustness of proposed technique corresponding to different attacks**

| | Performance Metric | | | |
|---|---|---|---|---|
| **Operations** | **PSNR** | **BER** | **NC** | **SSIM** |
| Gaussian noise (0.01) | 43.6168 | 0.3210 | 0.9992 | 0.9832 |
| Salt & pepper (0.01) | 42.5698 | 0.3786 | 0.9853 | 0.9753 |

| | | | | |
|---|---|---|---|---|
| Median filter [3*3] | 40.2738 | 0.4001 | 0.9798 | 0.9522 |
| Rotation ($5^0$) | 41.4900 | 0.3986 | 0.9832 | 0.9589 |
| Compression (5%) | 38.2123 | 0.4543 | 0.9783 | 0.9283 |
| Cropping (5% ) | 32.1112 | 0.5743 | 0.9212 | 0.9033 |

The embedded patient information may get effected by the image processing attacks. The proposed method extracted the patient's information by applying different operations such as Gaussian noise, rotation, compression, filtering, and cropping. The visual characteristics of extracted information is not exactly match with the original one, but the distortion is negligible. The values of PSNR, NC, and BER verified that the extracted information is understandable and the proposed technique gives a robust watermark that can survive even when the signal is distorted by signal processing attacks. Table 5.4 shows the presentation of the above discussed technique under different image processing attacks. It is verified from the table, that the ECG watermarking by using curvelet transform technique is robust against signal processing attacks.

To emphasize and to evaluate the performance of proposed technique, three other ECG Watermarking techniques based on DWT and curvelet transform have been compared. Forsimplicity, these three ECG Watermarking techniques, are named as, HH scale DWT-SVD [116**]**, Adaptive threshold [118], and Quantization approach [119]. Table 5.5 compares the statistics of measured PSNR, MSE, BER, KL, and PRD of different existing ECG techniques and proposed technique. For the proposed technique, the PSNR of the watermarked ECG is 78.0702 dB when the size of embedded information is 67*67 (4489 bits). The PSNR is visual quality indicator as well as it also observed as a performance evaluation metric. The PSNR shows the resemblance of the original EGC signal and watermarked ECG. The PSNR attained by Quantization approach is 73.75 dB, which can serve as a baseline for performance evaluation. The PSNR values of Adaptive threshold and HH scale DWT-SVD techniques are simply 60.68 dB and 50.44 dB respectively.

**Table 5.5 Comparison of proposed technique with existing ECG techniques**

| **Performance Metrics** | **HH scale DWT-SVD [116]** | **Adaptive threshold [118]** | **Quantization approach [119]** | **Proposed technique** |
|---|---|---|---|---|
| **Watermark size** | 67*67 (4489 bits) | 251 bytes (2008 bits) | 251 bytes (2008 bits) | 67*67 (4489 bits) |
| **PSNR** | 50.44 | 60.68 | 73.75 | 78.0702 |

| | | | | |
|---|---|---|---|---|
| **KL** | 0.15 | 0.0027 | 2*10-6 | 4.5478e-004 |
| **MSE** | 0 | 0.05 | 0.002 | 3.3801e-004 |
| **BER** | 0 | 0 | 0.04 | 0 |
| **PRD%** | 0.59 | 0.0018 | 0.04 | 0.1051 |

By using the Quantization approach [119], the author exploited the coefficients having zero or equal to zero value. In this technique, the author cannot hide the data more than the number of coefficients having the value near to zeros. In Adaptive threshold method, a n*n sequence is used to locate the watermark. This method also restricts the capacity to embed the information. The presented technique, on the other hand, uses cluster approach which does not restrict the size of embedding information. The selection of coefficients depends on the size of embedding information. Ideally, the coefficients having minimum values are the best to hide the information as it provides the best imperceptibility.

All three techniques mentioned in Table 5.5 used text information and converted it to binary to embed the information into the transform. If the information in form of text or binary is embedded into the transform domain of ECG, the false positive detection will change the complete patient's information and extracted one will not be the same as the original. In proposed method, the text information is first converted into the image then embedded into curvelet transform. Patient's information in the form of an image has a benefit that a false positive in this case will create only a minor change in the pixel intensity and that will not change the entire image message. Since the false positive detection only deteriorates the quality of extracted information, so embedding data in image form will lead to more robustness against image processing attacks.

## 5.3 CONCLUSION

This chapter includes two blind watermarking techniques. First watermarking technique is for detecting a tampering in an image is proposed. This technique is based on the curvelet transform and clustering. Here a random sequence watermark is hidden into the curvelet transform of a cover image by using the clustering approach. The proposed technique first identifies that whether an image is manipulated (tampered) or not. If the answer is yes, further procedure identifies the manipulated area of that image. In the presented technique results of embedded watermark in different scales with different cluster size are also analyzed by using BER and PSNR. To establish the better performance of the presented technique, it is compared with standard well know

techniques e.g. tamper localization [84] and block based method. Second is an ECG watermarking technique by using clustering and curvelet transform is proposed. To show the application of watermarking in medical field, the patient's information (used a watermark) is used to embed into the ECG signal. In this technique it is emphasized that the embedding a watermark as image is more robust as compare to text or numbers. Embedded watermark into an ECG signal is challenging work, because any change in ECG signal will affect the diagnosability of ECG. To keep in mind the diagnosability, the QRS waves are identified and watermark is embedded into the ECG signal learning QRS undisturbed. The performance of second technique is analyzed by using NC, SSIM, BER, PRD and KL metrics. The proposed techniques performance is also compared with existing techniques.

# CHAPTER 6

# CONCLUSIONS AND FUTURE SCOPE

The research work paying attention on the development of novel watermarking techniques using curvelet transform. This is applied to both grayscale and color images. Six new techniques are developed and compared with existing techniques for various applications of watermarking to establish the usefulness of newly developed techniques. The major findings may be summarized as follows:

It was found that the use of curvelet transform offers improvements in robustness against image processing operations compared to the method of embedding watermark using wavelets and DCT. It was also found that the watermarking using DCT is not robust against rotation operation because a change in the DFT or DCT components affects the whole image instead of block-based DCT. It has also been proved that wavelet transform cannot represent line singularity because it has only two directional elements namely scale and orientation. Wavelet also fails to signify anisotropic elements like edges and curves. Images are combinations of edges and curves, so it is shown that curvelet transform represents an image in a better way. Further, it is a multi-scale pyramid with several directions. It positions at each fine scale and has needle-shaped elements. Curvelet transform also provides sparse representation of objects along a curve and it is anisotropic with strong direction attribute.

In this thesis, six algorithms were developed based on the curvelet transform. Due to the representation of edges and curves, the curvelet transform is used as an embedding

domain to embed the watermark. HVS concepts, textures, bit planes and cryptographic methods are also used to change the characteristics of the original image to improve the robustness while maintaining the perceptual invisibility. Particular attention is given to the proposed schemes to guarantee secure watermark embedding and easy extraction. The watermark is required to be faint to the human eye and easily recoverable. All the developed algorithms have undergone subjective judgment and objective measurements to check the image quality and faithful reconstruction of the extracted watermark. The watermarked images were assessed for fidelity by using PSNR, NC, BER, and SSIM.

The first algorithm simply demonstrates the benefits of embedding watermark in curvelet transform. Watermark is embedded into different scales of curvelet transform to emphasize its characteristics. The invisibility of watermark is verified by values of MSE i.e., approximate 0, and values of PSNR i.e. approximately 75, for every watermarked image. The proposed algorithm is non-blind watermarking that also offers a good quality of extracted watermark. To test the robustness, almost all possible image processing operations are applied on the watermarked images. The quality of extracted watermark from noised watermarked images is verified by the PSNR values which are above 25 except the fingerprint image. This technique offers resistance to watermark distortion even for compressed, rotated and filtered images. To emphasize the proposed technique, cropping operations are also applied on the watermarked image and watermark is extracted from the 64*64 and 128*128 cropped watermarked images. The values of PSNR and SSIM confirm that watermark is detectable even from the cropped parts of watermarked images. The performance of each scale is also analyzed. It is concluded that the embedding in scale 6 in curvelet transform gives better robustness in comparison with image processing attacks to lower scales.

Second algorithm used texture blocks of color image and curvelet transform coefficients to embed the watermark. The texture blocks are extracted from the original image by using masking property of HVS. The PSNR of six watermarked images is ≈54, which shows the similarity between the original images and the watermarked images. The visual quality of the extracted watermark is very good. The value of NC shows the similarity of the extracted watermark with the original watermark. The value of SSIM is ≈ 1 which examines that there is no loss of luminance. The complexity of the proposed algorithm is also very low as compared to other existing algorithms.

Third algorithm proposes a semi-blind watermarking technique of embedding the color watermark using curvelet coefficient in RGB image. This algorithm utilizes the

property of HVS and bit plane. Most Significant Bit (MSB) plane of watermark image is used as embedding information. PSNR is 54.97 confirming a high invisibility of the watermark. Besides, the NC and MSSIM are 0.99 for image confirming almost zero difference between the cover and watermarked image. The PSNR of extracted watermark is 38.5623, NC is one in all planes and SSIM is also quite good.

A secure and semi-blind watermarking system is proposed in fourth algorithm. This algorithm combines the properties of cryptography and watermarking and offers good invisibility of watermark which is confirmed by the value of NC=1. The embedded watermark can resist the image processing operations. Values of NC in robustness test are above 0.8 which show that the extracted watermark is very similar to original watermark. Values of MSSIM are also above 0.65 in each test confirming that contrast, luminance and the structure of watermarked images are very similar to original one.

A fifth technique proposed a blind watermarking technique for tampering detection in color image. This proposed algorithm first identifies whether an image is manipulated (tampered) or not. If the image is manipulated, this technique can identify the manipulated area of that image.

An ECG watermarking technique using curvelet transform is the sixth technique presented that is used for securing patient information into the image as watermark. In this technique, the patient's information is embedded into curvelet coefficients of ECG signals. The medically significant QRS complex attributes of ECG are preserved so that the embedding of patient information does not affect the diagnosability. In this technique, it is emphasized that the embedded watermark as an image is more robust as compared to text or numbers. For the proposed technique, the PSNR of the watermarked ECG is 78.0702 dB when the size of embedded information is 67*67 (4489 bits).

**Table 6.1 Comparison of all proposed algorithms**

| Algorithm | Type of watermarking | Host Type | Type of embedded signal | Invisibility (PSNR) | Embedding Efficiency | Robustness | Security | Application Area |
|---|---|---|---|---|---|---|---|---|
| Digital Watermarking Technique Based on Multi-Resolution Curvelet Transform | Non-blind | Gray Scale image | Gray Scale image | 57.86 | 128*128 | Not resist against cropping and sparse operations | Not secure | Information hiding and watermarking |
| An Image Ownership Protection Method: Hiding Data into the Texture Blocks on Curvelet Domain | | Gray Scale image | Gray Scale image | 53.293 | 256*256 | Not robust against sparsity | Secure | Image Ownership detection |
| Semi-Blind Watermarking Scheme for RGB Image using Curvelet Transform | Semi-blind | RGB Color image | RGB Color image | 54.94 | 128*128 | Robust | Secure | Color image watermarking |
| A Secure and Semi-Blind Technique of Embedding Color Watermark in RGB Image using Curvelet Domain | | RGB Color image | RGB Color image | 44.94 | 256*256 | Robust | Highly Secure | Secure watermarking |
| Image Forgery Detection using Curvelet Transform | Blind | RGB Color image | Random sequence | 57.23 | 16*16 | Robust | Highly Secure | Tampering detection |
| ECG Watermarking Technique using Curvelet Transform | | 1-D ECG signal | Text | 66.825 | 100*100 | Robust | highly Secure | Secure data transfer in medical image |

Comparison of all proposed techniques is given in above Table 7.1.The originality of the proposed schemes enable them to achieve significant robustness compared to conventional watermarking methods. Comparisons of the proposed algorithms with the established widely used algorithms confirm that they offer superior performance respecting the perceptual quality of the watermarked image and provide robustness against any attack. At the same time, it requires minimal overhead processing with both the embedding and extraction phases. The new algorithms offer an optimal trade-off between perceptual distortion caused by embedding and robustness against certain attacks. The new techniques could offer significant advantages to the digital watermark field and provide additional benefits to the copyright protection industry.

# LIST OF PUBLICATIONS

## Published Papers

i. **Ranjeeta, Sharma Sanjay and Raheja L. R. ,** "A Semi-Blind Watermarking Scheme for RGB Image using Curvelet Transform", in **International Journal in Foundation of Computer Science & Technology, Vol. 7, No. 1, Jan 2017**.

ii. **Ranjeeta, Sharma Sanjay and Raheja L. R. ,** "A Secure and Semi-Blind Technique of Embedding Color Watermark in RGB Image Using Curvelet Domain", in **International Journal of Information Technology and Computer Science, Vol. 9, No. 3, 2017.**

iii. **Ranjeeta, Sharma Sanjay and Raheja L. R. ,** "Digital Watermarking Technique Based on Multi-resolution Curvelet Transform" in **International Journal in Foundation of Computer Science & Technology, Vol. 7, No. 2, March 2017**.

## Communicated Papers

i. **Ranjeeta, Sharma Sanjay and Raheja L. R. ,** "Color Image Tempering, Detection using Digital Watermarking based on Curvelet Transform in The International **Arab Journal of Information Technology (IAJIT).**

ii. **Ranjeeta, Sharma Sanjay and Raheja L. R.,** "An Image Ownership Protection Method: Hiding Data into the Texture Blocks on Curvelet Domain" **in the IEEE Canadian Journal.**

iii. **Ranjeeta, Sharma Sanjay and Raheja L. R.,** "Improved ECG Steganography Technique using Curvelet transform" **Image and Vision Computing Journal - Elsevier**.

# REFERENCES


[1] Sewaif et al. "Walsh-coded signatures for robust digital image watermarking", in Proc. *IEEE Int. Conf.*, TENCON 2004.

[2] Ahmed et al. "Robust image watermarking using two dimensional Walsh coding", in Proc. *IET Int. Conf. Image Processing*, IET, 2012.

[3] Liu et al. "A texture-based tamper detection scheme by fragile watermark", in Proc. *IEEE Int. Conf. Circuits and Systems*, 2004.

[4] Walton, Steve. "Image authentication for a slippery new age." *Dr Dobb's Journal-Software Tools for the Professional Programmer*, 1995, vol. 20, pp. 18-27.

[5] Naor, Moni, and Adi Shamir. "Visual cryptography." *Advances in Cryptology—EUROCRYPT'94*. Springer Berlin/Heidelberg, 1995.

[6] Su, Po-Chyi, Ming-Tse Lu, and Ching-Yu Wu. "A practical design of high-volume steganography in digital video files." *Multimedia tools and applications*, 2013, vol. 66, pp. 247-266.

[7] Cox, Ingemar J. et al., "Digital Watermarking and Steganography", 2008.

[8] Mohanty, Saraju P. "Digital watermarking: A tutorial review." *URL: http://www. csee. usf. edu/~ smohanty/research/Reports/WMSurvey1999Mohanty. Pdf* (1999).

[9] Amon, Peter. "Signal-Processing Attacks on Watermarks", 1999.

[10] Cox, Ingemar, et al. *Digital watermarking and steganography*. Morgan Kaufmann, 2007.

[11] Swanson, Mitchell D., Mei Kobayashi, and Ahmed H. Tewfik. "Multimedia data-embedding and watermarking technologies." In *Pro. Int. Conf. IEEE Processing*, 1998, vol. 86, pp. 1064-1087.

[12] Wang et al, "Innovations in digital watermarking techniques". *Heidelberg: Springer,* 2009.

[13] Arnold et al. "Techniques and applications of digital watermarking and content protection". *Artech House*, 2002.

[14] Xie, Liehua, and Gonzalo R. Arce. "Joint wavelet compression and authentication watermarking" in Proc. Int. Conf. *IEEE Image Processing*, 1998, vol. 2.

[15] Podilchuk, Christine I., and Wenjun Zeng. "Image-adaptive watermarking using visual models" *IEEE Journal on selected areas in communications*, 1998, vol. 16 pp. 525-539.

[16] Kutter, Martin, Sviatoslav V. Voloshynovskiy, and Alexander Herrigel. "Watermark copy attack." *Electronic Imaging*. International Society for Optics and Photonics, 2000.

[17] Cox, Ingemar J., and Matthew L. Miller. "Electronic watermarking: the first 50 years." *Multimedia Signal Processing, 2001 IEEE Fourth Workshop on*. IEEE, 2001.

[18] Cox, Ingemar J. et al., "Watermarking applications and their properties." In Proc. *Int. Conf. IEEE Information Technology: Coding and Computing*, 2000.

[19] Marini, Enrico, et al. "Evaluation of standard watermarking techniques." *Electronic Imaging 2007*. International Society for Optics and Photonics, 2007.

[20] Kaur, Rupinder, "A medical image watermarking technique for embedding EPR and its quality assessment using no-reference metrics", *International Journal of Information Technology and Computer Science (IJITCS)*, 2013, vol. 5, pp.73-78.

[21] Wang, Zhou, and Alan C. Bovik, "Mean squared error: Love it or leave it", A new look at signal fidelity measures", *IEEE signal processing magazine*, 2009, vol. 26, pp. 98-117.

[22] Wang, Zhou, et al., "Image quality assessment: from error visibility to structural similarity", *IEEE transactions on image processing*, 2004, vol.13, pp. 600-612.

[23] Ibaida, Ayman, and Ibrahim Khalil "Wavelet-based ECG steganography for protecting patient confidential information in point-of-care systems", *IEEE Transactions on biomedical engineering*, 2013, vol. 60, pp. 3322-3330.

[24] Varol, Cihan, and CoskunBayrak, "Estimation of quality of service in spelling correction using Kullback–Leibler divergence", *Expert Systems with Applications*, 2011, vol. 38, pp. 6307-6312.

[25] Polikar, Robi. "The wavelet tutorial", 1996

[26] Meyer, Yves, and L. Ondelettes. "Algorithms and applications." *SIAM, philadelphia*, 1993.

[27] Daubechies, Ingrid. *Ten lectures on wavelets*. Society for industrial and applied mathematics, 1992.

[28] Meyer, Y. "Wavelets and Operators", 1992.

[29] Meyer, Yves. *Wavelets and operators*, Cambridge university press, 1995, vol. 1.

[30] Candès, Emmanuel J., and David L. Donoho. "Ridgelets: A key to higher-dimensional intermittency". *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 1999, vol. 357, pp. 2495-2509.

[31] Candes, Emmanuel J., and David L. Donoho. "Curvelets, A surprisingly effective nonadaptive representation for objects with edges". Stanford Univ Ca Dept of Statistics, 2000.

[32] Mallat, Stéphane. *A wavelet tour of signal processing*. Academic press, 1999.

[33] Mallat, Stéphane, and Gabriel Peyré. "A review of band-let methods for geometrical image representation." *Numerical Algorithms*, 2007, vol. 44, pp. 205-234.

[34] Candes, Emmanuel J., and David L. Donoho. "Continuous curvelet transform: I. Resolution of the wavefront set" *Applied and Computational Harmonic Analysis*, 2005, vol. 19, pp. 162-197.

[35] Donoho, David, and E. Candes "Continuous curvelet transform: II. Discretization and frames" *Applied and Computational Harmonic Analysis*, 2005, vol. 19, pp. 198-222.

[36] Ma, Jianwei, and Gerlind Plonka "A review of curvelets and recent applications" *IEEE Signal Processing Magazine*, 2010, vol. 27, pp. 118-133.

[37] Candès, Emmanuel J., and Laurent Demanet "The curvelet representation of wave propagators is optimally sparse" *Communications on Pure and Applied Mathematics"*, 2005, vol. 58, pp. 1472-1528.

[38] Candes, Emmanuel, et al. "Fast discrete curvelet transforms." *Multiscale Modeling & Simulation"*, 2006, vol. 5, pp. 861-899.

[39] Candes, Emmanuel J., Justin K. Romberg, and Terence Tao "Stable signal recovery from incomplete and inaccurate measurements" *Communications on pure and applied mathematics*, 2006, vol. 59, pp. 1207-1223

[40] Candes, Emmanuel J., and Terence Tao. "Decoding by linear programming" *IEEE transactions on information theory*, 2005, vol. 51, pp. 4203-4215.

[41] Bhatt, Santhoshi, et al, "Image steganography and visible watermarking using LSB extraction technique", in Proc. IEEE Int. Conf. *Intelligent Systems and Control (ISCO),* 2015.

[42] Macq, Benoit M., and J-J. Quisquater, "Cryptology for digital TV broadcasting" In Proc. IEEE Int. Conf. Image Processing, 1995, vol. 83, pp. 944-957.

[43] Rhoads and G. B. "Identification/authentication coding method and apparatus" in *World Intellectual Property Organization*, 1995.

[44] Langelaar, Gerhard C., IwanSetyawan, and Reginald L. Lagendijk. "Watermarking digital image and video data. A state-of-the-art overview." *IEEE Signal processing magazine*, 2000, vol. 17, pp. 20-46.

[45] Bender et al. "Techniques for data hiding", *IBM systems journal* , 1996, vol. 35, pp. 313-336.

[46] Weng, ShaoWei, Yao Zhao, and Jeng-Shyang Pan, "Reversible watermarking based on improved patchwork algorithm and symmetric modulo

operation", *Knowledge-Based Intelligent Information and Engineering Systems*. Springer Berlin/Heidelberg, 2005.

[47] Yeo et al."Generalized patchwork algorithm for image watermarking", *Multimedia systems*, 2003, vol. 9, pp.261-265.

[48] Yeung, Minerva M., and Fred Mintzer "An invisible watermarking technique for image verification" In Proc IEEE Conf. *Image Processing,* vol. 2. IEEE, 1997.

[49] Su, Jonathan K., and Bernd Girod "Power-spectrum condition for energy-efficient watermarking" *IEEE Transactions on Multimedia*, 2002, vol. 4, pp. 551-560.

[50] Voyatzis, George, and Ioannis Pitas, "Digital image watermarking using mixing systems" *Computers & Graphics*, 1998, vol. 22, pp. 405-416.

[51] Pitas, Ioannis "A method for watermark casting on digital image", *IEEE Transactions on Circuits and Systems for Video Technology*, 1998, vol. 8, pp. 775-780.

[52] Nikolaidis, Nikos, and Ioannis Pitas"Robust image watermarking in the spatial domain" *Signal processing*, 1998, vol. 66, pp. 385-403.

[53] Kalker, Ton, et al. "On the reliability of detecting electronic watermarks in digital images." *Signal Processing Conference (EUSIPCO 1998),* European. IEEE, 1998.

[54] M. Arnold et al., Techniquesand Application of Digital Watermarking and Content Protection", Eds. Northwood, Artech House, 2003.

[55] Rey, Christian, and Jean-Luc Dugelay "A survey of watermarking algorithms for image authentication" *EURASIP Journal on Advances in Signal Processing*, 2002, vol.6, pp. 21-32.

[56] Bender et al. "Techniques for data hiding." *IBM systems journal*, 1996, vol. 35, pp. 313-336.

[57] O'Ruanaidh et al., "Watermarking digita images for copyright protection", *IEEE Proceedings-Vision, Image and Signal Processing*, 1996, vol.143, pp. 250-256.

[58] O' Ruanaidh,"Rotation, scale and translation invariant spread spectrum digital image watermarking" *Signal processing*, 1998, vol. 66, pp. 303-317.

[59] De Rosa, Alessia, et al. "Optimum decoding of non-additive full frame DFT watermarks" in Int. Proc. Conf. *International Workshop on Information Hiding*. Springer Berlin Heidelberg, 1999.

[60] Ramkumar et al, "A robust data hiding scheme for images using DFT" in Proc. Int. IEEE Conf. *Image Processing,* 1999.

[61] Lin et al. "Rotation, scale, and translation resilient watermarking for images" *IEEE Transactions on image processing*, 2001, vol. 10, pp. 767-782.

[62] Solachidis, Vassilios, and Loannis Pitas, "Circularly symmetric watermark embedding in 2-D DFT domain", *IEEE transactions on image processing*, 2001, vol. 10, pp. 1741-1753.

[63] Ganic, Emir, and Ahmet M. Eskicioglu "Robust DWT-SVD domain image watermarking: embedding data in all frequencies", In *Workshop on Multimedia and Security*. ACM, 2004.

[64] Pereira et al. "Template based recovery of Fourier-based watermarks using log-polar and log-log maps", in Proc. IEEE Int. Conf. *Multimedia Computing and Systems*, 1999.

[65] Cox et al. "Secure spread spectrum watermarking for multimedia" *IEEE transactions on image processing*, 1997, vol. 6, pp. 1673-1687.

[66] Huang, Jiwu, Yun Q. Shi, and Yi Shi, "Embedding image watermarks in DC components", *IEEE transactions on circuits and systems for video technology*, 2000, vol. 10, pp. 974-979.

[67] Fu, Yonggang, "Robust oblivious image watermarking scheme based on coefficient relation", *Optik-International Journal for Light and Electron Optics*, 2013, vol. 124, pp. 517-521.

[68] Chen, Tao, Jingchun Wang, and Yonglei Zhou. "Combined digital signature and digital watermark scheme for image authentication", In Proc IEEE. Int. Conf. *Info-tech and Info-net*, Beijing.Vol. 5, 2001.

[69] Das, Chinmayee et al. "A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation", *AEU-International Journal of Electronics and Communications*, 2014, vol. 68, pp. 244-253.

[70] Zhao, Jian, Eckhard Koch, and Chenghui Luo. "In business today and tomorrow" *Communications of the ACM* , 1998, vol. 41,pp. 67-72.

[71] Lin, Eugene T. et al. "Detection of image alterations using semifragile watermarks" *Electronic Imaging*, International Society for Optics and Photonics, 2000.

[72] Fridrich, Jiri, Miroslav Goljan, and Arnold C. Baldoza. "New fragile authentication watermark for images." In Proc IEEE Int. Conf. *Image Processing*, 2000.

[73] Zhang, Yujin, Ting Chen, and Juan Li, "Embedding watermarks into both DC and AC components of DCT" *Photonics West 2001-Electronic Imaging*, International Society for Optics and Photonics, 2001.

[74] Licks, Vinicius, and Ramiro Jordan, "Geometric attacks on image watermarking systems", IEEE *multimedia*, 2005, vol. 12, pp. 68-78.

[75] Stankovic, Srdjan, Igor Djurovic, and Ioannis Pitas, "Watermarking in the space/spatial-frequency domain using two-dimensional Radon-Wigner distribution", *IEEE Transactions on Image Processing*, 2001, vol. 10, pp. 650-658.

[76] Choi, Yoonki, and KiyoharuAizawa, "Digital watermarking using inter-block correlation: extension to JPEG coded domain", in Proc. IEEE Int. Conf. *Information Technology: Coding and Computing*, 2000.

[77] Luo, Wenbin, Gregory L. Heileman, and Carlos E. Pizano. "Fast and robust watermarking of JPEG files", in Proc. IEEE Int. Conf. *Image Analysis and Interpretation*, 2002.

[78] Wang, Houng-Jyh Mike, Po-Chyi Su, and C-C. Jay Kuo, "Wavelet-based digital image watermarking", *Optics Express*, 1998, vol. 3, pp. 491-496.

[79] Kundur, Deepa, and DimitriosHatzinakos. "Digital watermarking for telltale tamper proofing and authentication." in Proc. IEEE Int. Conf., 1999, vol. 87, pp. 1167-1180.

[80] Kostopoulos et al. "Color image authentication based on a self-embedding technique", in Proc. IEEE Int. Conf. *Digital Signal Processing*, Vol. 2. IEEE, 2002.

[81] Paquet, Alexandre H., and Rabab K. Ward. "Wavelet-based digital watermarking for image authentication." *Electrical and Computer Engineering, 2002. IEEE CCECE 2002. Canadian Conference on*. Vol. 2. IEEE, 2002.

[82] Barni, Mauro, Franco Bartolini, and Alessandro Piva, "Improved wavelet-based watermarking through pixel-wise masking", *IEEE transactions on image processing*, 2001, vol. 10, pp. 783-791.

[83] Hien, Thai D., Zensho Nakao, and Yen-Wei Chen, "ICA-based robust logo image watermarking", *Electronic Imaging 2004*. International Society for Optics and Photonics, 2004.

[84] Pla, Oriol Guitart, Eugene T. Lin, and Edward J. Delp III, "A wavelet watermarking algorithm based on a tree structure", *Electronic Imaging*. International Society for Optics and Photonics, 2004.

[85] Lu, Zhe-Ming, Dian-Guo Xu, and Sheng-He Sun, "Multipurpose image watermarking algorithm based on multistage vector quantization" , *IEEE Transactions on Image Processing*, 2005, vol. 14, pp. 822-831.

[86] Wong, Peter HW, Oscar C. Au, and Yick Ming Yeung, "Novel blind multiple watermarking technique for images" *IEEE transactions on circuits and systems for video technology*, 2003, vol. 13, pp. 813-830.

[87] Ellinas, John N. "A robust wavelet-based watermarking algorithm using edge detection", *World Academy of Science, Engineering and Technology*, 2007, vol. 34, pp. 291-296.

[88] Jumaa, BassimAbdulbaki, and Arwa Aladdin, "Image Watermarking using DWT-DCT", *Engineering & Technology Journal*, 2010, vol. 28.

[89] Holliman, Matthew, and Nasir Memon, "Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes", *IEEE Transactions on image processing*, 2000, vol. 9, pp. 432-441.

[90] Preda, Radu O. "Semi-fragile watermarking for image authentication with sensitive tamper localization in the wavelet domain." *Measurement*, 2013, vol. 46, pp. 367-373.

[91] Guo, Jing-Ming, and Heri Prasetyo. "Security analyses of the watermarking scheme based on redundant discrete wavelet transform and singular value decomposition", *AEU-International Journal of Electronics and Communications*, 2014, vol. 68, pp. 816-834.

[92] Hien et al. "Digital watermarking based on curvelet transform." *Signal Processing and Its Applications, IEEE, 2007.*

[93] Hien Thai et al. "Curvelet-domain image watermarking based on edge-embedding", *Knowledge-Based Intelligent Information and Engineering Systems*. Springer Berlin/Heidelberg, 2007.

[94] Shi Jianping and ZhengjunZhai. "Curvelet transform for image authentication, "*Rough Sets and Knowledge Technology*, 2006, pp. 659-664.

[95] Zhang Changjiang, and Min Hu. "Curvelet image watermarking using genetic algorithms." *Image and Signal Processing*, 2008.

[96] Zhang Zhi-yu, et al. "Digital image watermark algorithm in the curvelet domain." " in Proc. IEEE Int. Conf. *Intelligent Information Hiding and Multimedia Signal Processing*, 2006

[97] Leung H. Y. et al. "Digital watermarking schemes using multi-resolution curvelet and HVS model." *International Workshop on Digital Watermarking*. Springer Berlin Heidelberg, 2009.

[98] Xiao, Yi, Lee-Ming Cheng, and L. L. Cheng. "A robust image watermarking scheme based on a novel HVS model in curvelet domain", in Proc. IEEE Int. Conf. *Intelligent Information Hiding and Multimedia Signal Processing*, 2008.

[99] Leung, Hon Yin, Lee-Ming Cheng, and Lee Lung Cheng,"A robust watermarking scheme using selective curvelet coefficients", *International Journal of Wavelets, Multiresolution and Information Processing*, 2009, vol. 7, pp. 163-181.

[100] Falkowski, B. J., and Lip-San Lim. "Image watermarking using Hadamard transforms." *Electronics Letters*, 2000, vol. 36, pp. 211-213.

[101] Gilani, A.M., Skodras, A.N., "Watermarking by Multi-resolution Hadamard Transform," in *Proc. Electronic Imaging & Visual Arts (EVA 2001)*, Florence, Italy, 2001, pp. 73-77.

[102] Y. Liu, B. Ni, X. Feng, E.J. Delp, "LOT Based Adaptive Image Watermarking", Security, Steganography, and Watermarking of Multimedia Contents, *VI SPIE*2004, vol. 53, pp. 513 – 523

[103] N. Liu, K.P. Subbalakshmi, "Vector Quantization Based Scheme for Data Embedding for Images", Security, Steganography, and Watermarking of Multimedia Contents, *VI SPIE*, 2004, vol. 53, pp. 548 – 559.

[104] J.S. Seo, C.D. Yoo, "Image Watermarking based on scale space representation", Security, Steganography, and Watermarking of Multimedia Contents, *VI SPIE*2004, vol. 53, pp. 560 – 570.

[105] Chen, Brian, and Gregory W. Wornell. "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding." *IEEE Transactions on Information Theory*, 2001, vol. 47, pp. 1423-1443.

[106] Furon, Teddy, et al. "JANIS: just another n-order side-informed watermarking scheme", in Proc. IEEE Int. Conf. *Image Processing. 2002.*

[107] Malvar and H.S., Florencio, “Improved spread spectrum: a new modulation technique for robust watermarking”, *IEEE Transactions on Signal Processing*, 2003, vol. 51, pp. 898–905

[108] Eggers et al. "Scalar costa scheme for information embedding." *IEEE Transactions on signal processing*, 2003, vol. 51, pp. 1003-1019.

[109] Miller et al. "Applying informed coding and embedding to design a robust high-capacity watermark," *IEEE Transactions on image processing*, 2004, vol. 13, pp. 792-807.

[110] Pérez-González et al. "Rational dither modulation: A high-rate data-hiding method invariant to gain attacks." *IEEE Transactions on Signal Processing*, 2005, vol. 53, pp. 3960-3975.

[111] Moulin, Pierre, and Anil Kumar Goteti, "Minmax strategies for QIM watermarking subject to attacks with memory", in Proc. IEEE Int. Conf. *Image* 2005.

[112] Fei, Chuhong, Deepa Kundur, and Raymond H. Kwong, "Analysis and design of secure watermark-based authentication systems," *IEEE transactions on information forensics and security*, 2006, vol. 1, pp. 43-55.

[113] Liu, Jing, Guangming Tang, and Yifeng Sun, "A secure steganography for privacy protection in healthcare system," *Journal of medical systems*, 2013, vol. 37, pp. 91-98.

[114] Liu, Jing, Guangming Tang and Yifeng Sun. “A secure steganography for privacy protection in healthcare system.” *Journal of medical systems, 2016, vol.* 40, pp. 66-73.

[115] Zheng, Kai-mei, and Xu Qian, "Reversible data hiding for electrocardiogram signal based on wavelet transforms", in Proc. IEEE Int. Conf. *Computational Intelligence and Security*, 2008.

[116] Jero, S. Edward, PalaniappanRamu, and S. Ramakrishnan, "Discrete wavelet transform and singular value decomposition based ECG steganography for secured patient information transmission", *Journal of medical systems*, 2014, vol. 38, pp. 132-141.

[117] Hien, et al. "Digital watermarking based on curvelet transform", in Proc. IEEE Int. Conf. *Signal Processing and Its Applications,* 2007.

[118] Jero, S. Edward, PalaniappanRamu, and S. Ramakrishnan, "ECG steganography using curvelet transform", *Biomedical Signal Processing and Control*, 2015, vol. 22, pp. 161-169.

[119] Jero, S. Edward, and P. Ramu, "Curvelets-based ECG steganography for data security", *Electronics Letter*, 2016, vol. 52, pp. 283-285.

[120] Signal, U.S.C, "Image Processing Institute", *USC–SIPI image database", aviliable on http://sipi. usc. Edu/database*.

[121] Mishra et al. "Optimized gray-scale image watermarking using DWT–SVD and Firefly Algorithm", *Expert Systems with Applications*, 2014, vol. 41, pp. 7858-7867.

[122] Loukhaoukha et al. "Optimal image watermarking algorithm based on LWT-SVD via multi-objective ant colony optimization", *Journal of Information Hiding and Multimedia Signal Processing*, 2011, vol. 2, pp. 303-319.

[123] Su and Qingtang, "A blind color image watermarking based on DC component in the spatial domain." *Optik International Journal for Light and Electron Optics*, 2013, vol. 124, pp. 6255-6260.

[124] Al Ameen, Moshaddique, Jingwei Liu, and KyungsupKwak, "Security and privacy issues in wireless sensor networks for healthcare applications", *Journal of medical systems*, 2012, vol. 36, pp. 93-101.

[125] Act, A. C. C. O. U. N. T. A. B. I. L. I. T. Y. "Health insurance portability and accountability act of 1996." *Public law*, 1996, vol. 104. pp. 191-201.

[126] Moody, George B., and Roger G. Mark. "The MIT-BIH arrhythmia database on CD-ROM and software for use with it", in Proc. IEEE Int. Conf. *Computers in Cardiology 1990, Proceedings*, 1990.

[127] Pan, Jiapu, and Willis J. Tompkins, "A real-time QRS detection algorithm", *IEEE transactions on biomedical engineering*, 1985, vol. 3, pp. 230-236.