Secure and Robust Watermarking Techniques for Medical Imaging

A project report submitted in fulfilment of the requirements
for the award of the degree of

Master of Technology

in the

Department of Computer Science and Engineering

under the Supervision of

Prof. Dr.S.P. Ghrera

(HOD CSE)

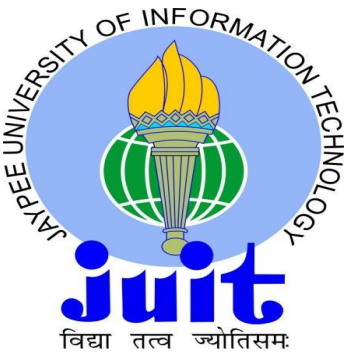
Mr.Amit Kumar Singh

(Co-supervisor)

By

Name: Abhilasha Sharma

Enrollment No: 132205



May 2015

Jaypee University of Information Technology
Waknaghat,Solan –173234, Himachal Pradesh

Certificate

This is to certify that project report entitled "Secure and Robust Watermarking Techniques for Medical Imaging.", submitted by "Abhilasha Sharma" in partial fulfillment for the award of degree of Master of Technology in Computer Science & Engineering to Jaypee University of Information Technology, Waknaghat, Solan has been carried out under my supervision. This work has not been submitted partially or fully to any other University or Institute for the award of this or any other degree or diploma.

Dated: Dr. S.P. Ghrera
HOD (CSE)

Dated: Mr. Amit Kumar Singh
(Assistant Professor)

Abstract

The current reliance of the Internet and multimedia technologies in medical domain has boosted the e-diagnosis applications such as telemedicine, tele-consultancy and tele-surgery.The sharing of medical information over network makes it important to protect medical information from unauthorized access and disclosure. The prime objective of this dissertation is to investigate how to protect the medical images and EPR data and recover the original image and data using the technique of Digital Watermarking. In order to facilitate sharing and remote handling of medical images, the techniques to solve the problem of copyright protection and content authentication are proposed using robust watermarking. This dissertation emphasis on the study of medical image watermarking methods for protecting and authenticating medical data. Additionally, it covers algorithm for application of watermarking technique on Non Region of Interest (NROI) of the medical image preserving Region of Interest (ROI).The watermarking algorithms proposed watermarking technique in the transform domain.

The watermarking techniques proposed in this dissertations is based on two popular transform domain techniques, discrete wavelet transforms (DWT) and discrete cosine transform (DCT), to ensure secure transfer of medical images and data. Using DWT transformation and substitution method, we embed the watermark into the cover image and the watermarked image is then encrypted by using the symmetric stream cipher techniques. The medical images are the most essential for the proper diagnosis. For the identity authentication purpose, multiple watermarks in the form of image and text are embedding into ROI and NROI part of the same cover media object respectively. The encrypted EPR data is embedded into the NROI region of medical images to enhance the security of the watermark. To enhance the security of EPR data and protecting the confidential patient reports from the unauthorized access and unwanted tamper, the hash values of watermarked images are generated using MD-5. The ERP data is encrypted public key cryptography such as RSA and encoded using error correction codes such as hamming codes to minimize the bit error rate. The performance

of the proposed methods are analyzed against known signal processing attacks such as compression, filtering, noise and histogram equalization and the desired outcome is obtained without significant degradation in extracted watermark and watermarked image quality.

Keywords: Watermarking, DICOM, DWT, DCT, Robustness, LSB, Medical images,IDWT, IDCT, Imperceptibility, Stream Cipher,ROI,NROI,MD-5, PSNR,NC, BER,imperceptibility, EPR, RSA

Acknowledgements

Compiling a year's work into this was an exhausting job, but writing this page of acknowledgement, I believe is a joyous task to cherish the memories of all those, who helped to enrich the newer experience of life.

At the very onset, I bow my head with reverence and dedicatedly accord my recondite and gratitude to "ALMIGHTY", the merciful and compassionate, whose grace, glory and blessings allowed me to complete this endeavour and without his encouragement and co-operation it would have never been possible for me to achieve this.

I owe my deep sense of respect and heart felt gratitude to my major supervisor ***Dr. S.P. Ghrera, Head of Department, Computer Science and Engineering, Jaypee University of Information Technology, Waknaghat*** for his meticulous and sagacious guidance, unstinted interest, sympathetic encouragement, precise and constructive criticism and ever willing help throughout the course of this investigation as well as in the preparation of this manuscript. I will always remain indebted to him for his unending guidance and untiring efforts in successful completion of this work. I consider myself fortunate to have worked under his able guidance.

I am highly obliged and grateful to co-supervisor, ***Mr. Amit Kumar Singh, Assistant Professor, Jaypee University of Information Technology, Waknaghat*** for his valuable suggestions and co-operation throughout my research work.I express my sincere and whole hearted thanks to him for rendering help and moral support.

I am thankful to office staff of the department for providing all the necessary and timely help. I am also thankful to respondents of my study for their co-operation which helped me to complete my study.

I wish to express my sincere thanks to all my friends for their support and guidance There is paucity of words to express my heartiest thanks to my friend ***Mr. Ajeet Singh*** who has helped me throughout my research work. I would also like to thank my friends ***Ms. Shailza Chaudhary, Ms. Kriti Pathak and***

Mr. Ravideep Singh for their timely help, best wishes and cheerful company remained a morale booster and made things smoother throughout the course of this study.

I owe my achievements to the unconditional love and support of my parents whose sacrifice I can never repay. This inspired me at every step of my life and encouraged me to never give up even in the face of overwhelming odds. I grope for words to express my deep feelings, love and affection to my elder brother.

Last but not least I would like to express my gratitude to all those who have helped, guided and supported me in one way or the other but have been inadvertently left out because all may not have been mentioned but none have been forgotten.

Needless to say, omissions are mine.

DATED: ABHILASHA SHARMA

15 May, 2015

Publication Outcome of this Work

1. Abhilasha Sharma, Mayank Dave, Amit Kumar Singh, and S P Ghrera **"Encryption Based Medical Image Watermarking against Signal Processing Attacks"** in Proc of *2015 International Conference on Future Computational Technologies (ICFCT'2015), Singapore,* March 29-30, 2015 pp. 78-84.

2. Abhilasha sharma, Amit Kumar Singh and S P Ghrera, **Encrypted EPR Data Hiding Technique using Medical Images"** communicated to *Second International Symposium on Computer Vision and the Internet (VisionNet'15),,Kerala, India* held on 10-13 August 2015.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

CT	**C**omputer **T**omography
MRI	**M**agnetic **R**esonance **I**maging
EPR	**E**lectronic **Pa**tient **R**ecord
DICOM	**D**igital **I**maging and **C**ommunications in **M**edicine
LSB	**L**east **S**ignificant **B**its
DFT	**D**iscrete **F**ourier **T**ransform
DCT	**D**iscrete **C**osine **T**ransform
DWT	**D**iscrete **W**avelet **T**ransform
PSNR	**P**eak **S**ignal to **No**ise **R**atio
MSE	**M**ean **S**quare **E**rror
NC	**N**ormalized **C**ross Correlation
BER	**B**it **E**rror **R**ate
ROI	**R**egion **o**f **I**nterest
NROI	**N**on-**R**egion **o**f **I**nterest
LL	**L**ow- **L**ow subband
LH	**L**ow-**H**igh subband
HL	**H**igh-**L**ow subband
HH	**H**igh-**H**igh subband
RSA	**R**ivest-**S**hamir-**A**dleman

IDCT	**D**iscrete **Co**sine **T**ransform
IDWT	**I**nverse **D**iscrete **Wa**velet **T**ransform
MD-5	**M**essage **D**igest-5

SYMBOLS

E	Encoding algorithm
D	Decoding Algorithm
I	Cover Image
S	Signature
S'	Decoded Signature
C_δ	Comarator
I_w	Watermarked Image
k	Gain Factor
N	Cover Image Size
$f(i,j)$	Intensity Value at $(i,j)^{th}$
$F(k,l)$	Transformation coefficient at $(k,l)^{th}$ location
N_{max}	Maximum possible pixel value
DB	number of bits which are incorrectly
NB	total number of bits of original watermark.
$LL2$	Second level Low-Low subband
$LH2$	Second level Low-High subband
$HL2$	Second level High-Low subband
$LL3$	Third level Low-Low subband
M	Mean Value in Gaussian Noise

V	Variance Value in Gaussian Noise
P, Q	Prime numbers in RSA

CHAPTER 1

INTRODUCTION

The widespread emergence of the computer network, communication field and electronic management of medical records, the sharing of medical information among medical institutions has become more prominent in the current era [1–3]. The growing technology offers substantial new opportunities to share and transmit valuable digital data such as images, audio and video over the Internet[4, 5]. The Internet and electronic media has boosted the enhanced medical facilities such as tele-medicine, tele-diagnosis, tele-consultancy etc[6] . With such advanced facilities, the medical information such as patient records, diagnostic images, consulting doctors' data etc. are commanded to be divvied up among several medical establishments [7, 8]. The digital resolution has boosted the dispense of medical images and confidential medical data among the health care professionals and health-care institutions [8–10].

In this new millennium, with the development in the Internet technology and networking, it is more convenient to share the information among hospital management systems. In the health care environment, this rapid evolution of technology offers different means to share and remotely access patient data[11, 12].The technological advancements have eased the duplication, manipulation and unauthorized distribution of the medical data , resulting in the prerequisite for protection from unauthorized access and maintaining the integrity of medical data[13, 14].

In the telemedicine, tele-diagnosis and tele-consultancy services, medical images play a prominent role for instant diagnosis, understanding of crucial diseases as well as avoiding the misdiagnosis.In the past few decades, use of advanced electronic and digital equipment in health care services has increased, replacing the traditional diagnostic system by e-diagnostic systems [14]. For efficient diagnosis of the patients, the physicians rely upon provided electronic and digital data such as Ultrasonic, Computed Tomography (CT), Magnetic Resonance Imaging (MRI), X-ray images and Electronic patient Records (EPR) data[15, 16].

With these evolutionary technologies, the security of the medical images and electronic medical records has attracted greater attention. The sharing of the digital medical information has led to the requirement of the safety issues concerned with the legal and ethical aspects specific to the medical domain[17, 18]. The duplication and distribution of digital data has raised the requirement of the effective content and copyright protection mechanisms. The digital handling of such information requires a systematic content validation, copyright management and content protection[18, 19]. For intellectual achievement and confidentiality, copyright protection and content authentication of medical data is critical, while exchanging the information over open network[19, 20].

Due to the recent advent of multimedia technology has boosted the potential power of tele-medicine applications, online storage and transmission of electronic patient records (EPR)[21–23]. Typically, ERP contains the physician's signature, the health history and physical examination reports etc. The transmission of medical information emphasis on safety issues against the demand of ethical and legal aspect of the medical domain[24–26].

The ease of transmitting and sharing the medical data increases the security issues in terms of[2, 20]:

- **Confidentiality:** Only the authorized user has access to the information.
- **Integrity:** The information has not been modified by unauthorized user.

- **Authentication:** A proof that the information belongs indeed to the correct person and is issued from the correct source.
- **Availability:** the ability of an information system to be used by the entitled user in the normal scheduled conditions of access and exercise.

To address these issues, various methods are used to hide the information. To protect the secret information from the intruders, it is necessary to convert information into unidentified form, making it impossible to the intruder to get the information.

1.1 Information Hiding Background

The medical information have a crucial role while communication between the healthcare centers. The electronic patient records (EPR) have crucial information regarding the clinical examination, diagnostic reports, prescriptions and history of patient etc. The digital handling of these reports requires a systematic content protection, which is aimed at the originality and reliability of the medical information [27].

Security of the medical information is mandatory to protect the intellectual rights and confidentiality of the patients[28, 29]. The protection of medical data is done by hiding the information within any appropriate medium . Information hiding is an art that involves communication of secret information in an appropriate carrier such as image, video, audio, audio etc[29]. To protect the information from the unauthorized access, the information hiding methods used are classified in figure 1.1[30]

Information-hiding techniques have recently become important in a number of application areas. In the medical domain, information hiding have prominent role to protect medical data and images against the unauthorized access, ensuring the integrity and confidentiality of information[29, 31]. The information can be hidden

in digital media such as audio, video and images[32].

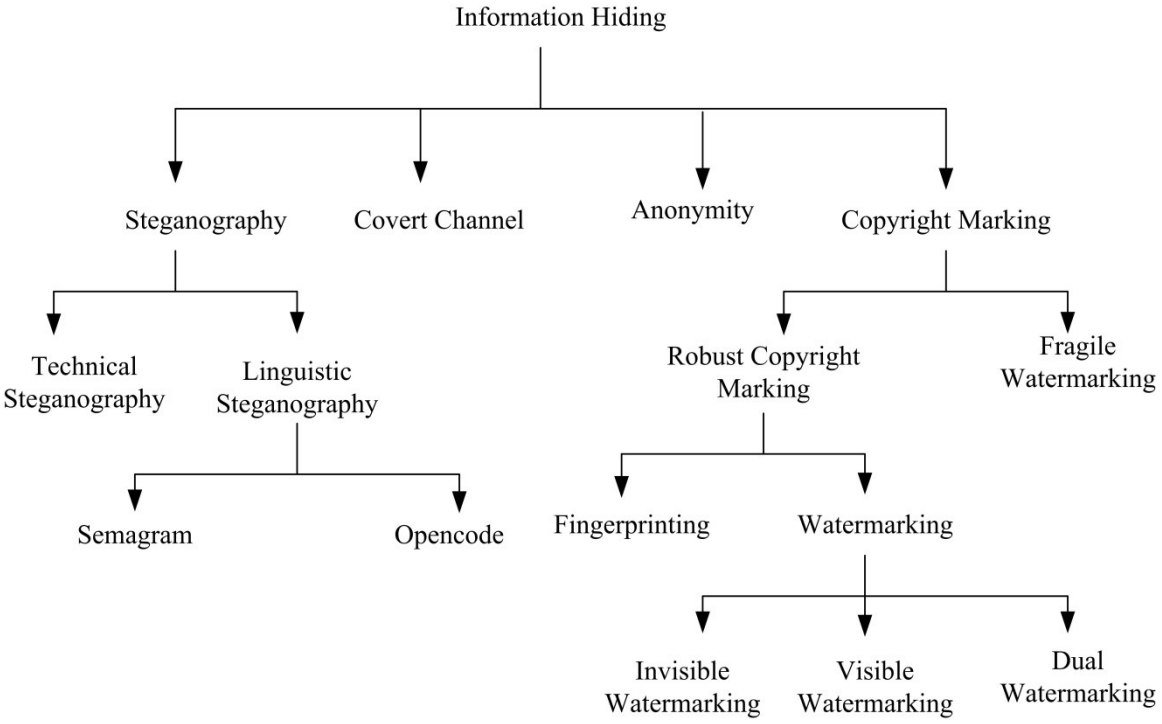


FIGURE 1.1: Information Hiding Techniques

1.1.1 Information Hiding Classification

Based on the mechanism used to hide the information in an open system, the information hiding can be classified as:

- Cryptography
- Steganography
- Watermarking

Cryptography means "Secret Writing"[5]. It is the method that allows information to be send and receive in a secure manner such that only receiver should

be able to recognize it. The main purpose of the cryptography to provide various security services like confidentiality, data integrity, authentication and non-repudiation[11]. The original message which we want to send is called as plain text. The process of converting plain text into cipher text is called as encryption[13]. The reverse of encryption process is called decryption process. The encryption process protects the content. The protection provided by the encryption process can be illusory. If the system where encryption is performed can be penetrated, then the intruder can get the access to the content[18].The cryptography system is shown in figure 1.2.

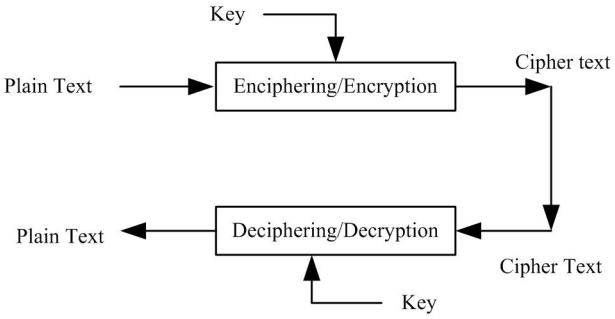
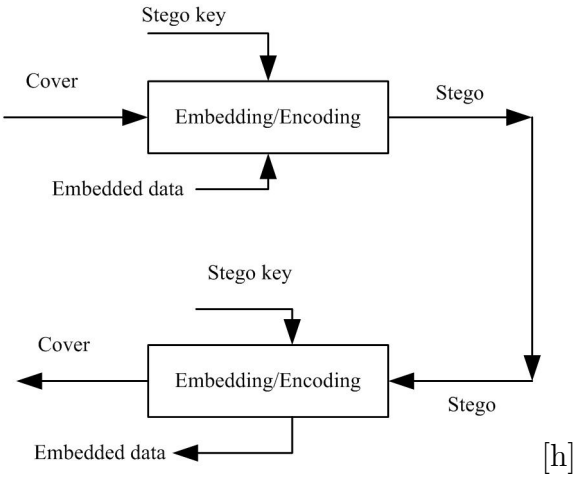


FIGURE 1.2: Cryptography

Steganography means "cover writing", derived from the Greek word "Stegno" [30]. It is the art of communicating in a way which hides a secret message behind any cover media such as image, audio or video. Steganography hides the message in the plain sight rather that encrypting it[33, 34].The main objective of steganography is to hide unrelated message behind cover. In steganography, Issues are concerned with the bandwidth used for the hidden message[34, 35]. The advantage of using steganography over cryptography is that it does not attract the attention of the intruder as the message is hidden [36].The steganography system is shown in figure 1.3.

Watermarking is the process of embedding data as watermark, tag or label into a digital media such image, audio, video etc[28, 30, 31]. A watermark can be perceived as an attribute of cover, embedding the related information with the cover [37]. It may contain information such as copyright license, authentication etc[38].



[h]

FIGURE 1.3: Steganography

The watermarking mainly concern with the robustness of the embedded data such that it can not be removed by the intruder[33, 39].The comparison between the information hiding techniques is given in table1.1 [2, 30].

1.2 Digital Image Watermarking

The digital watermarking, as an effective adjunct to the traditional encryption techniques, has become new and effective potent to protect digital information[40, 41]. The digital watermarking is used for the content protection, copyright management, content authentication and temper detection in medical image information[42].The digital watermarking is an emerging technology for digital image authentication and copyright protection and ensure the integrity of data[43].The digital watermarking is considered as the imperceptible, robust, secure communication of information by embedding it in and retrieving it from the other digital data[36, 44, 45].

Table 1.1: Comparison Between Information Hiding Techniques

	Cryptography	Steganography	Watermarking
Techniques	Transposition, Substitution,RSA	LSB,Spatial Domain	Compensated prediction, DCT
Capacity	Capacity is so high, but as message is long it chances to be decrypt	Differs as different Technology usually low hiding capacity	Capacity depends on the size of hidden data
Imperceptibility	High	High	High
Robust	Yes	Yes	Yes
Applicability	Universally	Universally	Universally
Strength	Hide message by altering the message by assigning key	Hide message without altering the message, it conceals information	Extend information and become an attribute of the cover image
Detection	Not easy to detect ,depend on technology used to generate	Not easy to detect because to find stenographic image is hard	Not easy to detect
Naked eye Identification	Yes, as message is convert in Other way, which sough something is hidden	No, as message is Hide within other carrier (cover image)	Yes, as actual message is hiding by some watermark
Usage	Content Protection	Covert communications	Authentication, copyright protection

1.2.1 The General Watermarking Framework

Watermarking is the process of embedding data called as watermark or a tag to the multimedia objects such as image, audio and video, for assertion of authenticity purpose[2, 43],.The watermark can be a signature, a logo, a serial numbers and medical reports etc[46, 47].
The watermarking algorithm can be generally consists of two parts[28, 30]:

- The encoder
- The decoder and comparator

1.2.1.1 The Encoder

The encoder is an embedding function, which takes an image and signature or watermark and generate the watermarked image[28]. Let I be the cover image, S be the signature and J be the watermarked image. E be the embedding algorithm, which can be shown mathematically as,

$$E(I, S) = J \tag{1.1}$$

The encoding processes is illustrated in figure 1.4:

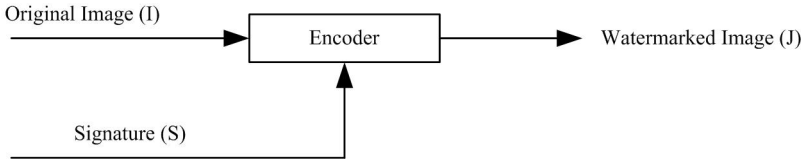


FIGURE 1.4: The Encoding Process

1.2.1.2 The Decoder

The decoder is an extraction function, which takes watermarked image and original image as input and recovers the embedded signature[28], which can be shown mathematically as,

$$D(I, J) = S' \tag{1.2}$$

The extracted signature S' is then compared with the original signatures using a comparator function C_δ and produced the binary output as,

$$C_\delta(S, S') = \begin{cases} 1 & \text{if } c \geq \delta \\ 0 & \text{otherwise} \end{cases} \tag{1.3}$$

The decoding processes is illustrated in figure 1.5:

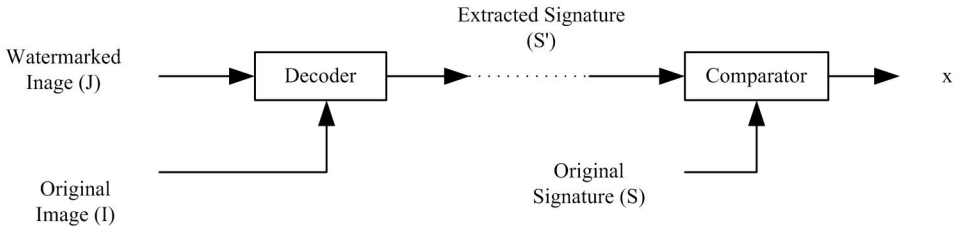


FIGURE 1.5: The Decoding Process

1.2.2 Requirements of Digital Watermarking System

The crucial requirement of digital watermarking are[48]:

- **Imperceptibility:** The watermarked image and the original image should be perceptually indistinguishable.
- **Robustness:** The robustness can be defined as "ability to detect the watermark after common operations". The watermark could be removed intentionally or unintentionally by simple image processing operations like cropping,

contrast or brightness enhancement etc. Hence the watermarks should be robust against variety of such attacks.

- **Security:** Watermark information owns the unique correct sign to identify, only the authorized users can legally detect, extract and even modify the watermark, and thus be able to achieve the purpose of copyright protection.
- **Capacity:** The capacity is defined as "the number of bits a watermark encodes within a unit of time". This property describes how much data should be embedded as a watermark to successfully detect during extraction. Watermarking should be able to carry enough information to represent the uniqueness of the image.
- **Visibility:** The watermark must be invisible to the human eye, that the document marked remains faithful to the original.
- **Complexity:**The watermarking operations must be possible in real time. This implies an additional constraint complexity of the operations used for the watermarking.
- **Computational Cost:** As with any technology intended for commercial use, the computational costs of inserting and detecting watermarks are important. This is particularly true when watermarks need to be inserted or detected in real-time video or audio.
- **Transparency:**The digital watermarking should not affect the quality of the original image after embedding watermark to it. Watermarking should not introduce visible distortions because if such distortions are introduced it reduces the quality of the image.

Depending on the medical application area such as health, administrative, teaching, research, there is trade-offs among robustness, imperceptibility and capacity varies[5]. A basic principle of watermarking is to exploit redundancy in images for embedding the watermark information. Given the fact that many of the existing image compression algorithms are not perfect, watermarking is made possible

by embedding extra information in the redundant parts. In addition, enhancing watermark robustness normally requires more image distortions and increased redundancy. This causes lower imperceptibility and more likely to be removed under malicious attacks [44].

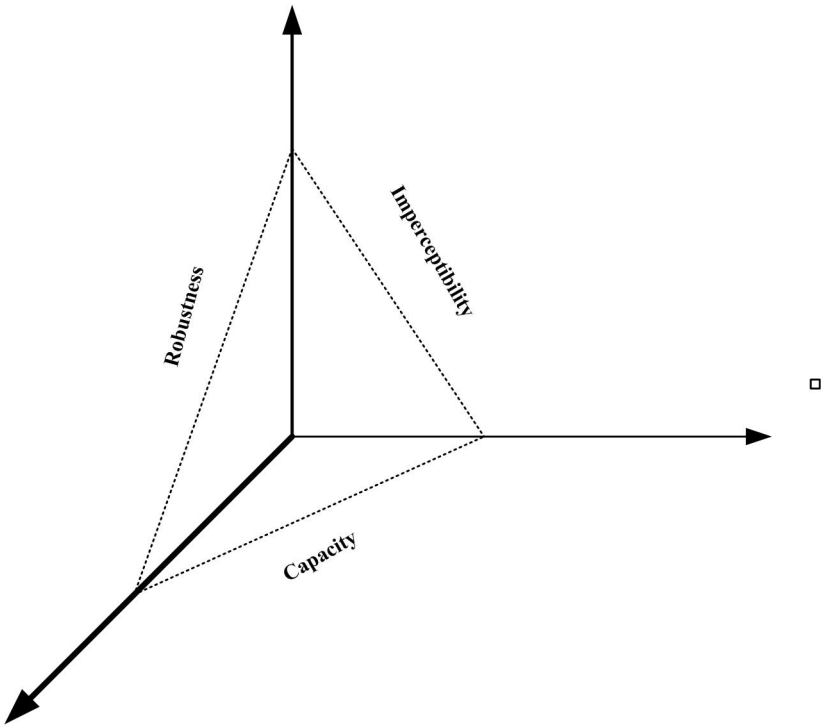


FIGURE 1.6: Relationship among the performance parameters of Watermarking

In e-health care system, medical image security is critical issue. Medical image security is provided by digital watermarking techniques, to protect patient medical information. The watermarking techniques are used to protect the EPR information from the unauthorized access, disclosure and non-repudiation.

1.2.3 Classification of Digital Watermarking

In the case of images, watermarking techniques are commonly distinguished based on two working domains: Spatial domain and Frequency domain[30, 49]. In spatial domain, the pixels of one or two randomly selected subsets of an image are modified

based on perceptual analysis of the original image. However, in the Frequency or transform domain, the values of certain frequencies are altered from their original image. Meanwhile, based on human perception, digital watermarks are divided into three categories as follows[28]:

- **Visible watermark,** where the secondary translucent overlaid into the primary content which would be seen visible by careful inspection.
- **Invisible-Robust watermark** is embedded in such a way that alterations made to the pixel value are perceptually unnoticed.
- **Invisible-Fragile watermark** is embedded in such a way that any manipulation of the content would alter or destroy the watermark.

From application point of view, digital watermarks could also be Source based where a unique watermark identifying the owner is introduced to all the copies of a particular content being distributed . Destination based is where each distributed copy gets a unique watermark identifying the ownership[42, 50].

1.2.4 Application of digital watermarking:

- **Copyright protection:**
  Watermarking can be used to protect redistribution of copyrighted material over the untrusted network like Internet or peer-to-peer (P2P) networks. Content aware networks (p2p) could incorporate watermarking technologies to report or filter out copyrighted material from such networks.
- **Content Authentication:**
  It detects all the types of modifications in the content and shows it as a sign of invalid authentication.
- **Temper detection:**
  Digital content can be detected for tampering by embedding fragile watermarks. If the fragile watermark is destroyed or degraded, it indicated the

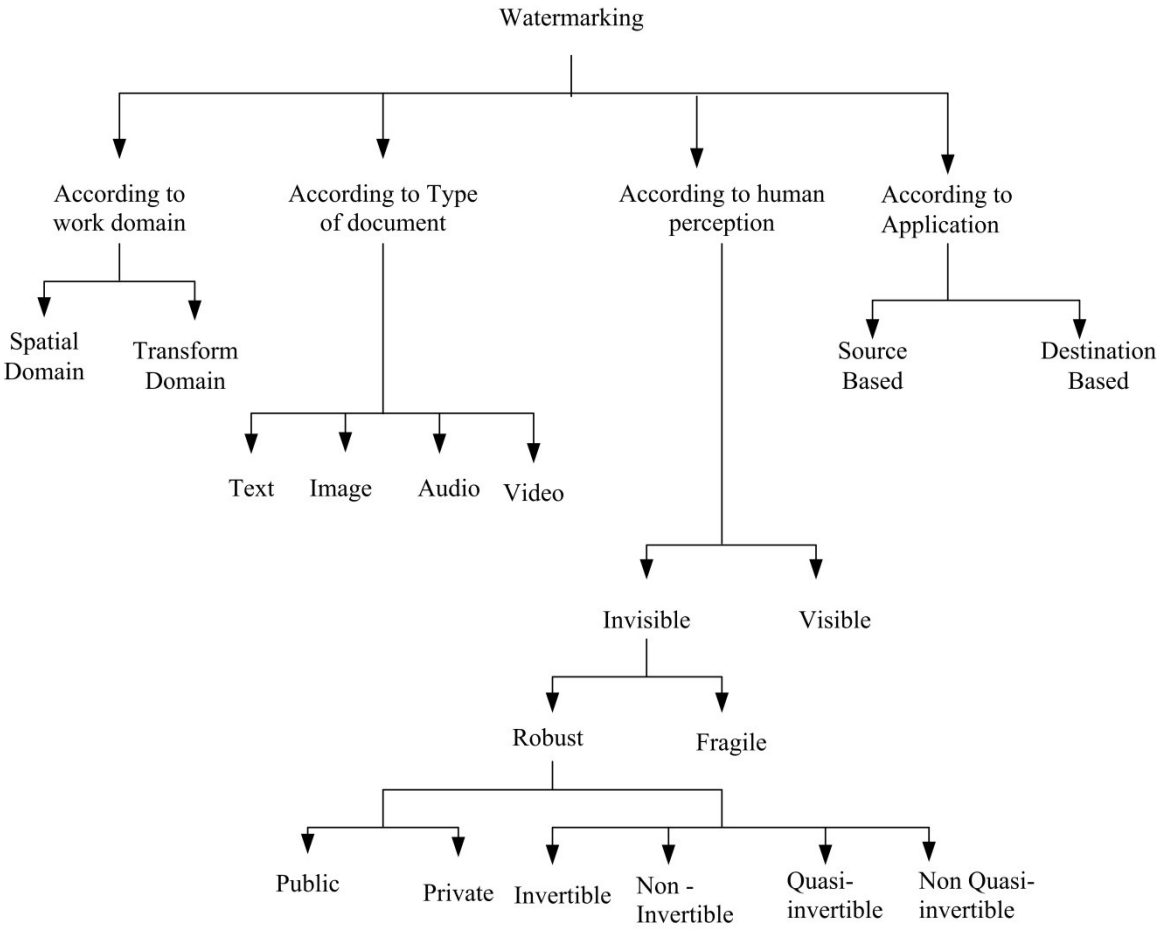


FIGURE 1.7: Types of Digital Watermarking

presence of tampering and hence the digital content cannot be trusted. Tamper detection is very important for some applications that involve highly sensitive data like satellite imagery or medical imagery. Tamper detection is also useful in court of law where digital images could be used as a forensic tool to prove whether the image is tampered or not.

- **Broadcast monitoring:**
  Broadcast Monitoring refers to the technique of cross-verifying whether the content that was supposed to be broadcasted (on TV or Radio) has really been broadcasted or not. Watermarking can also be used for broadcast monitoring. This has major application is commercial advertisement broadcasting

where the entity who is advertising wants to monitor whether their advertisement was actually broadcasted at the right time and for right duration.

- **Content Achieving:**
  Watermarking can be used to insert digital object identifier or serial number to help archive digital contents like images, audio or video. It can also be used for classifying and organizing digital contents. Normally digital contents are identified by their file names; however, this is a very fragile technique as file names can be easily changed. Hence embedding the object identifier within the object itself reduces the possibility of tampering and hence can be effectively used in archiving systems.

- **Meta-data Insertion:**
  Meta-data refers to the data that describes data. Images can be labeled with its content and can be used in search engines. Audio files can carry the lyrics or the name of the singer. Journalists could use photographs of an incident to insert the cover story of the respective news. Medical X-rays could store patient records.

- **Digital fingerprinting:**Digital Fingerprinting is a technique used to detect the owner of the digital content. Fingerprints are unique to the owner of the digital content. Hence a single digital object can have different fingerprints because they belong to different users.

- **Medical image security:** It is known as invertible watermarking and it is used to provide authentication and confidentiality in a reversible manner without effecting medical image in anyway. Names of the patients can be printed on the X-ray reports and MRI scans using techniques of visible watermarking. The medical reports play a very important role in the treatment offered to the patient. If there is a mix up in the reports of two patients this could lead to a disaster.

- **Medical Forensic:**Forensic watermark applications enhance a content owner's ability to detect and respond to misuse of its assets. Forensic watermarking

is used not only to gather evidence for criminal proceedings, but also to enforce contractual usage agreements between a content owner and the people or companies with which it shares its content.

- **Locating Content Online:**The volume of content being uploaded to the web continues to grow as we rely more and more on the Internet for information sharing, customer engagement, research and communication. It has also become a primary sales tool and selling environment, providing an opportunity to showcase our products or services and attract buyers from around the world.

1.3 Watermarking Techniques

Digital Watermarking describes methodologies that hide information in digital media, such as images, video or audio to ensure the security of confidential data. The embedding is done by manipulating the content of the digital media, keeping the valuable information of cover intact. The embedding process has to be performed in such a way that the modifications of the media have to be invisible in the images, ensuring the imperceptibility of the media.
Based on the embedding domain, watermarking schemes can be classified into two categories:

- Spatial Domain
- Transform Domain

1.3.1 Spatial Domain techniques

Spatial domain techniques directly deal with the image pixels[5, 46]. In this technique, the watermark is inserted in the cover image changing pixels or image characteristics. The embedding is done directly by modifying the pixels of the

cover image to hide the watermark[28]. The algorithm should carefully weight the number of changed bits in the pixels to ensure imperceptibility and robustness the watermark.
Spatial watermarking can also be applied using color separation. In this way, the watermark appears in only one of the color bands. This renders the watermark visibly subtle making it difficult to detect under regular vision[42]. The comparison between different spatial domain techniques is as shown in table 1.2.

1.3.2 Different Spatial Domain Techniques

The various spatial domain techniques used for the watermarking are[30, 34]:

- Least Significant Bits (LSB)
- SSM Modulation Based Technique
- Texture mapping Technique
- Patchwork Algorithm
- Correlation-Based Technique

1.3.2.1 Least Significant Bits (LSB):

This is the simplest approach, because the least significant bit carries the least relevant information and their modification does not cause perceptible changes[30]. It is the most common method of watermark embedding is to embed the watermark into the least significant- bits of the cover object. This method is easy to implement and does not distort to the cover image. However, it is not very much robust against the attacks.The schematic representation of LSB method is as shown in the figure 1.8.

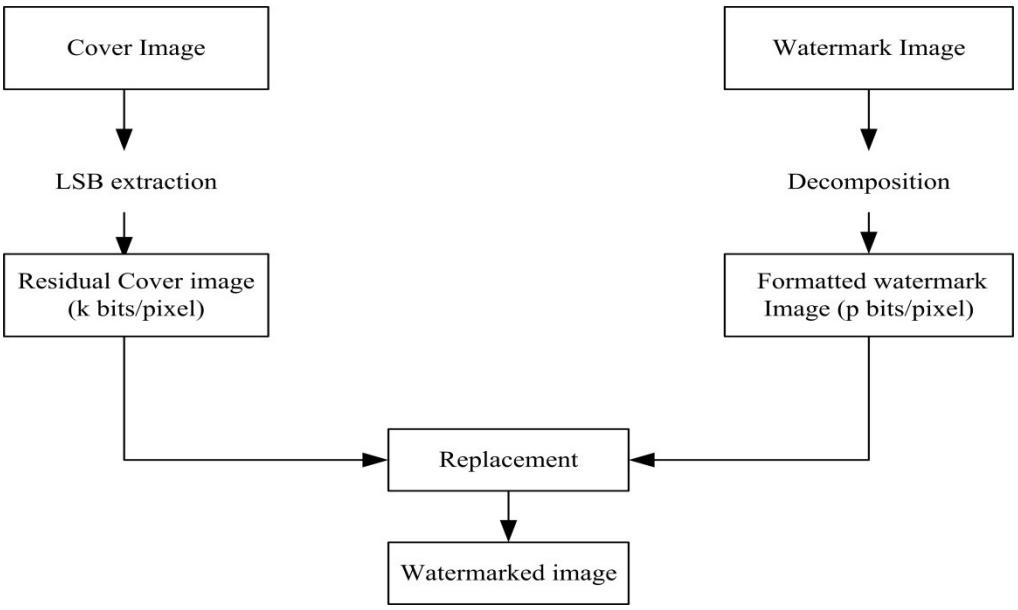


FIGURE 1.8: LSB Watermarking

1.3.2.2 SSM Modulation Based Techniques

Spread-spectrum techniques are methods in which energy generated at one or more discrete frequencies is deliberately distributed in time. When applied to the context of image watermarking, SSM based watermarking algorithms embed information as linear combination of the host image and a pseudo random signal which is being modulated by the embedded watermark. This is done for establishment of secure communications, increasing resistance to interference, to prevent jamming, and detection.

1.3.2.3 Texture mapping Technique

In this method, it is useful in only those images having some texture characteristics. This method hides the watermark in the texture portion of the image. In this method, a region of the random texture found in the image is embedded to an region of the image with similar texture.

1.3.2.4 Patchwork Algorithm

Patchwork randomly chooses pairs of image points and increases the brightness at one point by one unit while correspondingly decreases the brightness of another point. It is based on a pseudo-random statistical model. Patchwork imperceptibly inserts a watermark with a particular statistic using a Gaussian distribution.

1.3.2.5 Correlation-Based Technique

A well known technique for watermark embedding is to exploit the correlation properties of additive pseudo-random noise patterns as applied to an image .The watermark $W(x, y)$ is added to the cover image $I(x, y)$, according to the equation given below,

$$I_w(x, y) = I(x, y) + k * W(x, y) \tag{1.4}$$

In Equation (1.4), k denotes a gain factor and I_w the resulting watermarked image.The comparison between Spatial domain Techniques is given in table1.2.

1.3.2.6 The Characteristics of the Spatial Domain Watermarking Techniques

- The watermark is applied in the pixel domain.
- No transforms are applied to the host signal during watermark embedding.
- The combination with the host signal is done in the pixel domain.
- Detection of the watermark is done by correlating the expected pattern along with its received signal.

TABLE 1.2: Comparison between Spatial domain Techniques

S. No	Technique	Advantage	Disadvantage
1.	LSB	Easy to implement and understand.Low degradation of image quality.High perceptual transparency.	Lacks in Robustness.Vulnerable to noise.Vulnerable to scaling and cropping
2.	Texture mapping Technique	Hides data within the continuous random texture patterns of a picture.	Only suitable for those areas with large number of arbitrary texture images.
3.	Patchwork Algorithm	High level of robustness against most types of attacks.	It can hide only a very small amount of information.
4.	Correlation-Based Technique	Watermark image says$W(x, y)$ is added to cover image $I(x, y)$.Gain factor can be increased, increases robustness	Image quality gets decreased due to very high increase in gain factor.

1.3.3 Transform Domain Techniques

Transform domain watermarking is useful for taking advantage of perceptual criteria in the embedding process, to increase the robustness of the watermark[42]. The watermarking system modifies the frequency coefficients of cover image to hide the watermark. Firstly, the cover image is transformed to the transformation domain using the transformation techniques, embedding the watermark to transform coefficients and then the inverse transformation is done to restore the

watermarked image.There are a number of transformation methods which can be to digital images, but most commonly the following techniques are used in digital image watermarking[30, 33].

1.3.4 Different Transform Domain Techniques

The various transform domain Techniques are [46, 49]:

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

1.3.4.1 Discrete Fourier Transform (DFT)

Fourier Transform (FT) is an operation that transforms a continuous function into its frequency components. The equivalent transforms for discrete valued function requires the Discrete Fourier Transform (DFT), allowing analysis and processing of the images in transform domain, using analysis and modification these transformed coefficients [50].
In DFT based watermarking scheme, the watermark is embedded by modifying the DFT magnitude and phase coefficients. The non-periodic functions such as images can be expressed as the summation of sine and/or cosine multiplied by a weighing function, which determines the coefficients of the Fourier Transform of the image[51].
The DFT is the sampled Fourier Transform such that only a set of samples is efficient to completely describe the spatial domain image. The size of image in the spatial and Fourier transform domain are of the same, as the number of frequencies corresponds to the number of pixels in the spatial domain image[52].The schematic

representation of DFT is as shown in figure 1.9
For a square image of size N, the two dimensional DFT is given by

$$F(k,l) = \frac{1}{N} \sum_{i=0}^{N-1} \sum_{i=0}^{N-1} f(i,j) e^{-i2\pi(\frac{ki}{N} + \frac{lj}{N})} \tag{1.5}$$

Where $f(i,j)$ is the image in the spatial domain and the exponential term is the basis function corresponding to each point $F(k,l)$ in the Fourier space[51].

- The value of each point (k,l) is obtained by multiplying the spatial image with the corresponding base function and summing the result.
- The basis functions are sine and cosine waves with increasing frequencies, i.e having avg brightness as, $F(0,0)$, which is the DC-component of the image and $F(N-1, N-1)$ represents the highest frequency.

In a similar way, the Fourier image can be re-transformed to the spatial domain. The inverse Fourier transform is given by:

$$f(i,j) = \sum_{i=0}^{N-1} \sum_{i=0}^{N-1} F(k,l) e^{i2\pi(\frac{ki}{N} + \frac{lj}{N})} \tag{1.6}$$

1.3.4.2 Discrete Cosine Transform (DCT)

Discrete Cosine Transform is like as Discrete Fourier Transform which transforms an image from the spatial domain to the frequency domain [53]. The 2-dimensional DCT of giving matrix gives the frequency coefficients in the form of another matrix, having lower frequency components near the origin and the higher frequency components at the future away from origin. Watermarking with DCT techniques are robust as compared to spatial domain techniques [54].
The Discrete Cosine Transform (DCT) represents an image as a sum of sinusoids

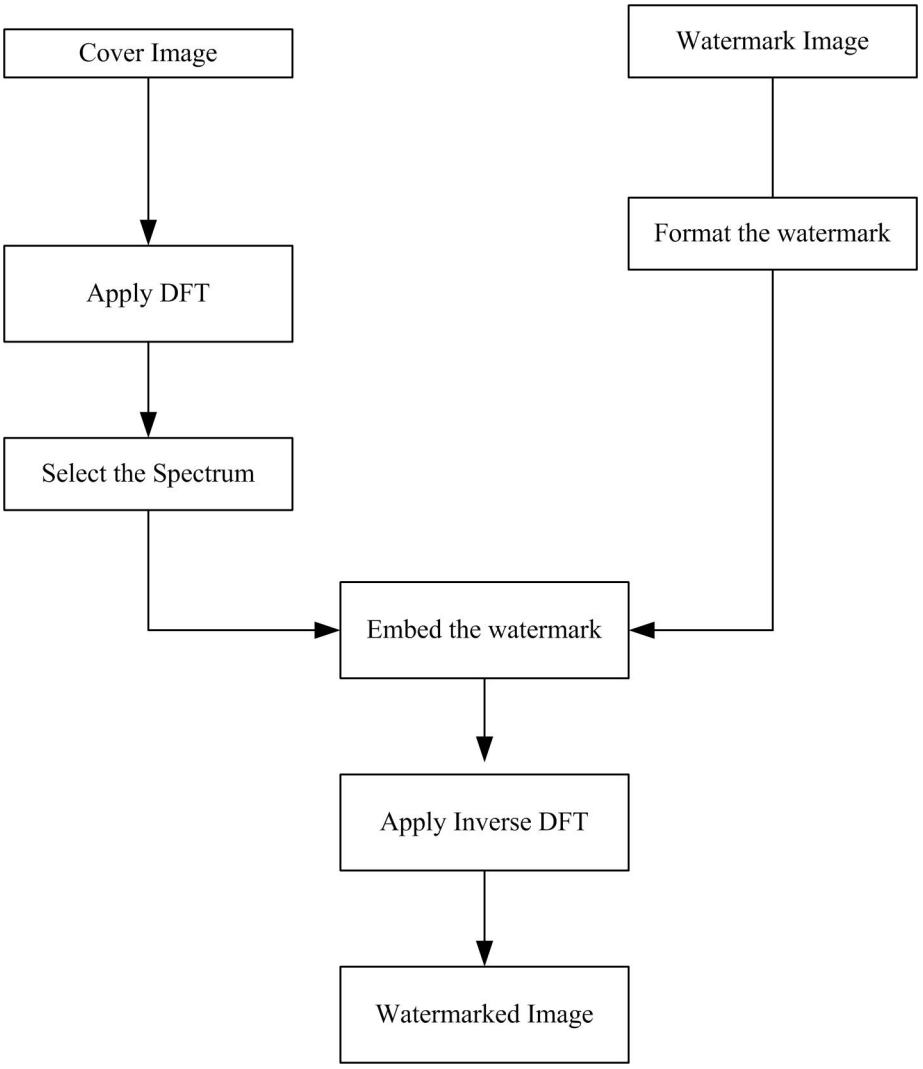


FIGURE 1.9: DFT Watermarking

of varying magnitudes and frequencies [55].For an image, the DCT concentrates the most significant information in few coefficients of varying energy.The Discrete Cosine Transform (DCT) expresses a finite sequence of sample points in terms of a sum of cosine functions oscillating at different frequencies[54, 55]. The discrete cosine transform (DCT) helps separate the image into spectral sub-bands of differing significance with respect to the image's visual quality[56].The schematic represntation of DCT watermarking is shown in figure 1.10.

The DCT of an image of size N is given by the following equation:

$$F(u,v) = \alpha(u)\alpha(v)\sum_{i=0}^{N-1}\sum_{i=0}^{N-1} f(x,y)\cos\frac{(2x+1)\pi u}{2N}]\cos\frac{(2y+1)\pi v}{2N}] \tag{1.7}$$

Where $f(x,y)$ is the image in the spatial domain and the normalization coefficients $\alpha(u)$,$\alpha(v)$ is given as,

$$\alpha(u) = \alpha(v) = \begin{cases} \sqrt{\frac{1}{N}} & \text{if } u = 0 \\ \sqrt{\frac{2}{N}} & u \neq 0 \end{cases} \tag{1.8}$$

The inverse transform is defined as:

$$f(x,y) = \sum_{i=0}^{N-1}\sum_{i=0}^{N-1} \alpha(u)\alpha(v)F(u,v)\cos\frac{(2x+1)\pi u}{2N}]\cos\frac{(2y+1)\pi v}{2N}] \tag{1.9}$$

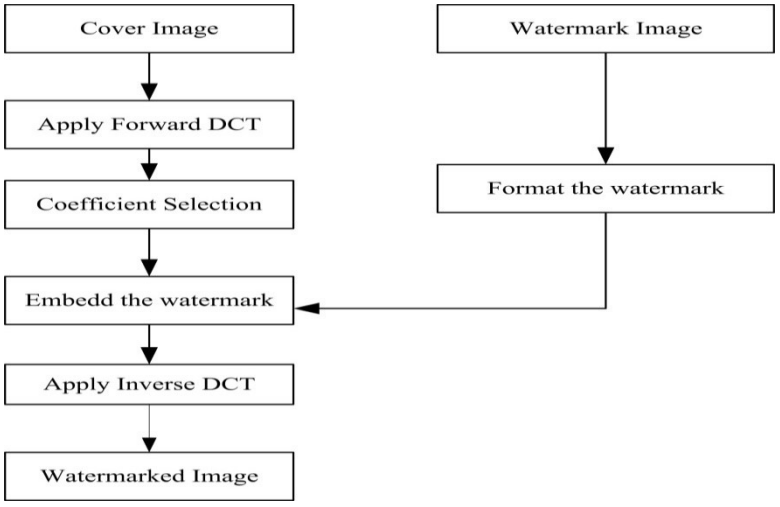


FIGURE 1.10: DCT watermarking

1.3.4.3 Discrete Wavelet Transform (DWT)

Wavelet Transform is a modern technique frequently used in digital image processing, compression, watermarking etc[57]. The transforms are based on segment

of waves, called wavelet, of varying frequency and finite duration[58]. A wavelet series is a representation of a square- integrable function by a certain orthonormal series generated by a wavelet function[59].The wavelet could decompose the original image into wavelet transform coefficients which contain the positional information. The original image can be completely reconstructed by performing Inverse Wavelet Transformation on transformed coefficients. Wavelet transforms provides both frequency and spatial description of an image.

The Discrete Wavelet Transform (DWT) is a linear transformation that operates on a data vector whose length is an integer power of two, segmenting it into numerically different vectors of the same length, having coefficients of different frequency components. The DWT segment the images into four sub-bands, namely LL, LH, HL, HH sub-band. The schematic representation of DWT transformation is given in the figure 1.11.

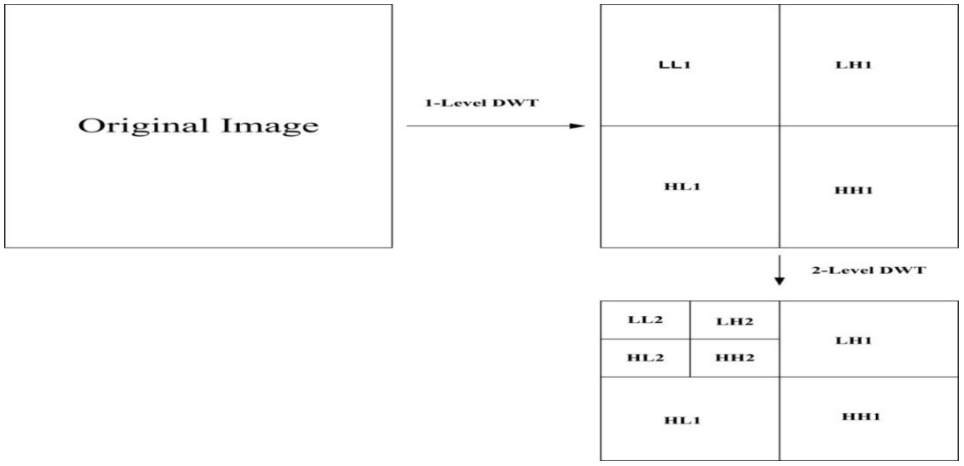


FIGURE 1.11: Second-level DWT

1.3.4.4 Comparison between Transform Domain Techniques

The differences between Transform Domain Techniques is as given in table 1.3

TABLE 1.3: Differences between transform domain techniques

S. No	Technique	Advantage	Disadvantage
1.	DFT	DFT is rotation,scaling and translation invariant.It can be used to recover from geometric distortions.	Complex Implementation.Cost of computing may be higher.
2.	DCT	The watermark is embedded into the coefficients of the middle frequency.The watermark will not be removed by any kind of attack.Block wise DCT destroys the invariance properties.	Certain higher frequency components tend to be suppressed during the quantization step.
3.	DWT	Allows good localization.Higher compression Ratio.	Cost of computing may be higher.Longer compression time.Noise near edges of image.

1.3.5 Comparison between Spatial and Transform Domain Techniques

The differences between Spatial and Transform Domain Techniques is as given in table 1.4

TABLE 1.4: Differences between Spatial and transform domain techniques

S. No	Factors	Spatial Domain	Transform Domain
1.	Computational complexity	Low	High
2.	Computation Time	Low	High
3.	Robustness	Fragile	More Robust
4.	Perceptual quality rate	High control	Low control
5.	Capacity	High	Low

1.4 Watermarking Performance Metrics

In medical image watermarking, after watermarking, it is mandatory to preserve the quality of the image along with the protection of confidential patient information. The performance of the watermarking algorithm is evaluated based on the quality of the watermarked image and to measure the correctness of the extracted watermark[41, 46].The quality of the image is determined by imperceptibility and the correctness of the extracted watermark is determined by robustness.

1.4.1 Imperceptibility Evaluation of Watermarked Image

Some distortion will occur in the images after embedding the watermark into a cover image.The imperceptibility of the watermarked image is determined by peak signal to noise ratio (PSNR). The large peak signal to noise ratio indicate that the watermark image resembles to the original cover image. The peak signal to noise ratio (PSNR) can be computed as,

$$PSNR = 10log\frac{(N_{max})^2}{MSE} \tag{1.10}$$

where N_{max} is the maximum possible pixel value of the original image. MSE is the mean square error.

The mean square error can be computed as,

$$MSE = \frac{1}{MN} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} (I(i,j) - I_w(i,j))^2 \tag{1.11}$$

where $I(i,j)$ represent the original image and I_w is the watermarked image of size $M \times N$.

1.4.2 Robustness Evaluation of Extracted Watermark

The following quantitative metrics is used to evaluate the reliability of the extracted watermark:

- **Normalized cross-correlation (NC)**, for image watermark.
- **Bit Error Rate (BER)**, for text watermark.

Normalized Cross-correlation (NC): The normalized cross-correlation (NC) is used to evaluated the compatibility between the original and extracted watermark and quantitatively can be measured as,

$$NC = \frac{\sum_{i=0}^{N-1} \sum_{j=0}^{N-1} W(i,j) W'(i,j)}{\sqrt[2]{\sum_{i=0}^{N-1} \sum_{j=0}^{N-1} W(i,j)^2 \times \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} W'(i,j)^2}} \tag{1.12}$$

where $W(i,j)$ represents the original watermark to be embedded and $W'(i,j)$ represents the extracted watermark.

Bit Error Rate(BER): This is used to evaluate the reliability of the text watermark.Bit Error Rate (BER) shows the probability of bits that are incorrectly decoded. Therefore, lower the BER, better is the performance of watermarking algorithm. The Bit Error Rate is computed as,

$$BER = \frac{DB}{NB} \tag{1.13}$$

where DB is the number of bits which are incorrectly decoded and NB is the total number of bits of original watermark.

1.5 Thesis Organization

Chapter 2 describes the image watermarking literature survey and problem statement.Chapter 3 describes the encryption based watermarking techniques for medical images and their performance evaluation. Chapter 4 describes the Encrypted EPR Data Hiding Technique in medical images and performance evaluation of such techniques.Chapter 5 describes the Encrypted EPR Data Hiding Technique in medical images using MD-5 and performance evaluation of such techniques.Chapter 6 discuss the conclusion and future scope of the project and at the end bibliography details are given.

CHAPTER 2

LITERATURE SURVEY

The advancement in the Internet technology provides the new ways to store, access and share the medical images and information, accelerating the services of telemedicine such as tele-consulting, tele-diagnosis etc. Security of medical information is important to protect patient confidentiality and prevents mismatching of diagnostic information.

While sharing the medical images, the confidentiality of medical records is protected using encryption. But during the data transfer, the data can be disclosed due to illegal copying and ill-intentions of legitimate authority. The measures against confidentiality violation is consists of access control and secure transfer protocols. In an open environment, access can be controlled by using firewalls [5]. The integrity of the medical information can be carried out by authenticating and identifying the user against identity usurpation. During transmission, the digital signatures are used for the data integrity[9]. The cryptographic methods alone are insufficient for all security aspects.In an open environment, several security problems are associated with the processing and transmission of images. Image security methods can detect whether medical images are tampered or modified but cannot protect them from being tempered.

Sahagun et. al[60] proposed the image encryption techniques, based on the permutation of the pixel values, were used to protect the image contents. Using this

encryption technique, unauthorized user cannot access the image content. But lacks in providing image authentication.

Rajput et. al [61] proposed the image encryption and authentication was provided by scrambling the pixel values and reducing the correlation among the pixel values. To improve the image security, the image encryption along with the image authentication confer the ideal alternative.

For high image security, the digital watermarking is an effective security and copyright mechanism. The watermarking scheme has been recognized to control the image reliability by emphasizing its integrity and authentication[3, 30].

Rui-mei et.al[62] proposed that the wavelet transformation was used, which divided the carrier image into sub blocks and watermark was embedded in each block. In this, the watermark embedding strength is unchangeable but not much robust.

Nassiri et. al [63] proposed the discrete wavelet transformation to find the coefficients and the watermark, to be embedded, was formatted by using either of error correcting codes, redundancy, key generation and pseudo random sequence. This improves the performance in terms of imperceptibility and maintains high resolution.

To secure the medical images and data, the cryptography is embedded with the digital watermarking to improve the security to a fair extent. Zaz et. al[64] determined that the data was embedded into the liberated zone, created by using the compression techniques and the watermark to be embedded was encrypted using the encryption techniques. In this, only the security, integrity and confidentiality is being respected, but no consideration for the robustness of the watermarked images.

Hui-fen[65], to improve robustness the data to be embedded to the image is hashed based on hashing techniques and embedded into the image. The encryption techniques are used to find the embodiment points in the image to provide the security also. During the transmission, compression of the images leads to the performance degradation.

Bouslimi et. al[4], the joint encryption/ watermarking method was introduced for the purpose of medical image protection. The content to be embedded was formed

as a stream using encryption techniques and embedded to the images. Using this, the image distortion is minimized and provides the high capacity rate, but the robustness is moderate. Joint encryption/watermarking is slower than simple encryption.

Kannammal et. al [66]proposed a method to enhance the robustness, the image was transformed and the data was embedded into the image using the non-tensor wavelet filter bank. The high security was provided by encrypting the watermarked image. This method have ability to grapple with different attacks.

In tele-medicine, tele-diagnosis and tele-consultancy services, the medical images plays a vital role. The medical images are segmented into two portions: Region of Interest (ROI) and Non-Region of Interest(NROI).The EPR data must be hidden in medical images without affecting the quality of Region of Interest (ROI) . There are numerous watermarking schemes based on discrete wavelet transform (DWT) has been proposed in the literature. The DWT based watermarking schemes enhances the robustness of the watermark.

Navas et. al [67]has proposed a method to hide the patient EPR data to medical image by extracting the ROI region. The 1-level integer wavelet transformations are used to obtain the wavelet coefficients and embed the encrypted EPR data to the high frequency subband namely LH and HL.

Nakhaie et. al [68] has been proposed a method based on spread spectrum and discrete wavelet transformations on the ROI and discrete cosine transform on NROI portion of the medical image. The watermark is formed by using the random number generator, selecting from the ROI region of the image and embedded to the DCT of NROI portion of image, resulting in the semi-fragile watermarking scheme.

Raul et. al[69] has been proposed a method to embed patient data in DICOM (Digital Imaging and Communications in Medicine) format to the medical diagnosis image. The method is based on compression of the medical data to generate the watermark, which is embedded in the selected image pixels based on the spiral scan and variance. This method is robust against the geometric attacks.

Memon et. al [70] has been proposed a method to authenticate the medical image. The watermark image is converted into the binary image and embedded to the NROI portion using the LSB substitution method. The encoded EPR data is added to the scrambled pixels of NROI portion, preserving the integrity of the ROI portion.

2.1 Summary of literature Survey

TABLE 2.1: Summary of Literature Survey

Author	Image Modality	Objective	Embedding Region	Embedding Technique	Fragility or Robustness
Ruimeit.al[62]	Natural Images	Authentication	Whole Image	DWT	Robust
Nassiri et. al[63]	Medical Images	Authentication	Whole Image	DWT	Robust
Zaz et. al[64]	Medical Images	Data Hiding	Whole Image	LSB	Less Robust
Hui-fen et. al[65]	Natural Images	Authentication	Whole Image	DWT,Hashing	Robustness
Bouslimi et. al[4]	Medical Images	Integrity, Authentication	Whole Image	LSB	Less Robust
Kannammal et. al [66]	Medical Images	Image Hiding	Whole Image	DWT	Robust
Navas et.[67] al	Medical Images	Data Hiding	NROI	DWT	Robust
Nakhaie et. al[68]	Medical Images	Authentication	NROI	Spread Spectrum	Fragile
Raul et. al[69]	Medical Images	Data Hiding	Whole Image	Spatial Domain	Less Robust
Memon et. al [70]	Medical Images	Authentication	NROI	Spatial Domain	Less Robust

2.2 Problem Statement

- To study and investigate detailed digital image watermarking techniques in spatial and transform domain. The most prospective technique among them will be retraced by analysis and simulation for medical images.
- To improve the robustness and security of the watermarking technique against signal processing attacks and cryptanalytic attacks respectively.
- To find the performance parameters to evaluate the quality of the watermarked image by Peak Signal Noise Ratio (PSNR) and the robustness of the extracted watermark by Normalized cross-correlation (NC).
- For the robustness analysis, performance of the considered algorithm against the well known signal processing attacks.

2.3 Objective

The objective of merging the cryptography and digital watermarking is:

- To improve the robustness and security of the watermark image without much degradation of the image quality.

CHAPTER 3

ENCRYPTION BASED MEDICAL IMAGE WATERMARKING

The protection of data is of at most importance in the medical field to boost the telemedicine applications. There is a need of robust and secure mechanism to transfer the medical images over the Internet. The algorithm proposed in this study is the watermarking technique in the transform domain to ensure secure transfer of medical data. Using DWT transformation and substitution method, we embed the watermark into the cover image and the watermarked image is then encrypted by using the symmetric stream cipher techniques. Performace of the proposed algorithm is analyzed against various signal processing attacks like compression, filtering, noise and histogram equalization and desired outcome is obtained without much degradation in extracted watermark and watermarked image quality.
In our proposed method, the watermark and cover images are transformed using Haar wavelets. The watermark image to be embedded is formatted to form the watermark key using modulus functions. To embed the watermark, a bit-plane is selected in the cover image and embedding is done on the selected bit-plane. To enhance the protection of the watermarked image, it is enciphered utilizing the

stream cipher symmetric key techniques.

3.1 Watermark Embedding

The proposed DWT based watermarking method is formulated as embedding and extraction process as given below:

i Convert the watermark and cover image to grayscale images.

ii Apply first-level DWT to watermark image 'W' to obtain the sub-bands LL, LH, HL and HH. Apply first-level DWT to cover image 'C' to obtain the sub-bands LL, LH, HL and HH.

iii Select the LL sub-band of the watermark image and format using the modulus function to obtain the watermark key.

iv Select the bit-plane to hide the image. Using the selected bit-plane, embed the watermark to the 'LL' sub-band on the cover image 'C'.

v Apply first level Inverse DWT.

vi The watermarked image is encrypted using the stream cipher (RC4) in the transform domain. The watermark embedding process is given in figure 3.1:

3.2 Watermark Extraction

i Select the encrypted watermarked image.

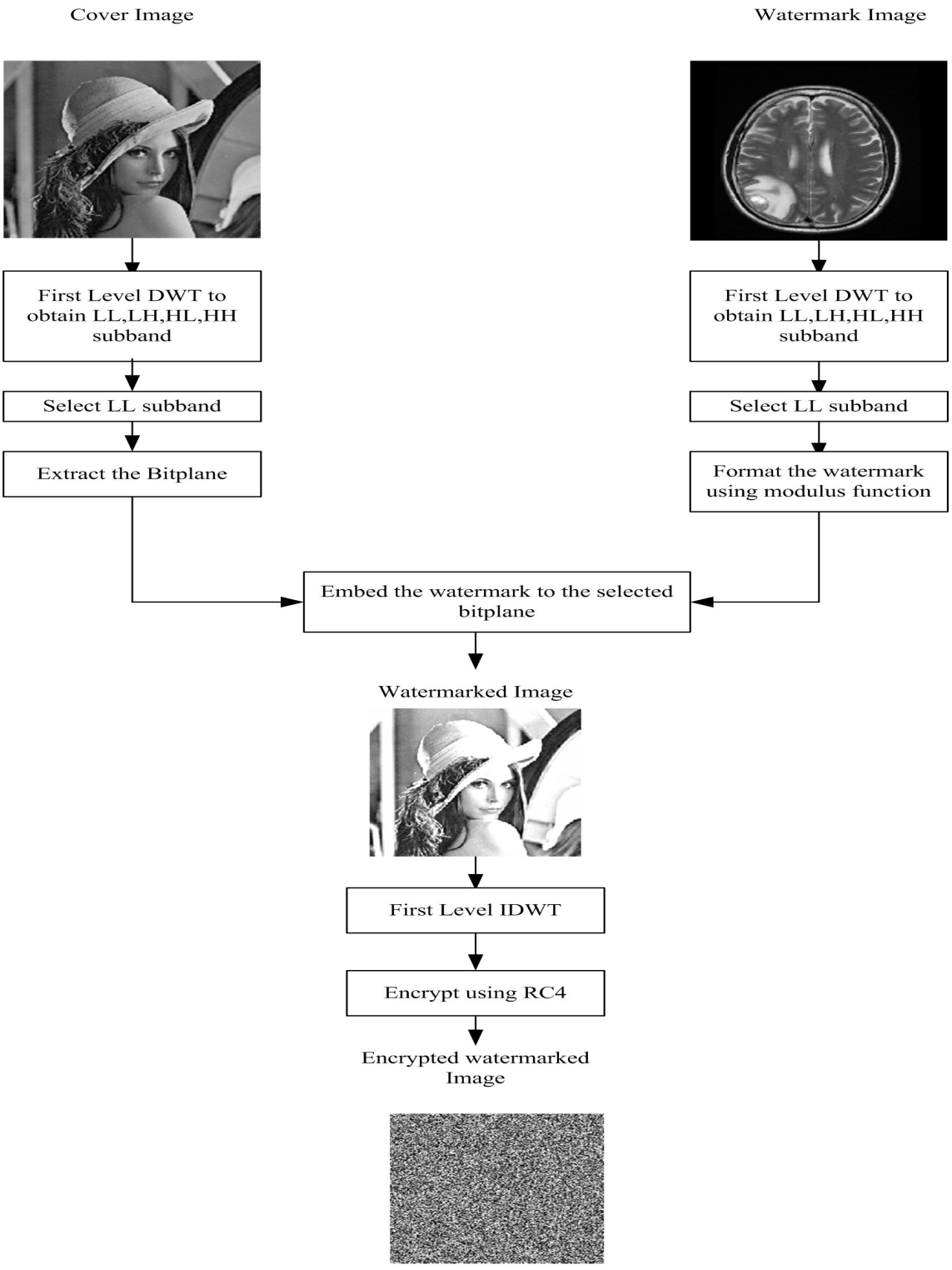


FIGURE 3.1: Watermark Embedding

ii Decrypt the image using the stream cipher, opposite to encryption. Apply first level DWT to obtain LL,LH,HL and HH subband.

iii Obtain the embedded watermark by extracting using the selected bit plane.

iv The watermark extraction process is given in figure3.2:

3.3 Experimental Results and Discussion

The watermarking embedding and extraction is done for the images of different sizes. The image size 512×512 is used as the cover image. First level DWT is applied to the images to obtain the sub-band.The embedding is done to the LL sub-band by using the LSB substitution methods. The watermarked images are encrypted by using the RC4 encryption techniques, which provides the additional security to the watermark images.The original and watermarked images are as shown in figure 3.3.

The proposed algorithm is simulated using MATLAB. Based on the experimental results, the Normalized cross correlation (NC) and peak signal to noise ratio (PSNR) values are illustrated in Table 3.1 to 3.3. The Table 3.1 describes the NC values at different gain factors ranging from 0.005 to 0.5. Without any noise attack, the PSNR values of different images are obtained for the various gain factors. Without any noise attack, PSNR values for all the images are above 66 dB, which indicates a high imperceptibility of the watermarked images. The Table 3.1 and 3.2 illustrate the NC and PSNR values for different images at different gain factors. The NC values obtained are above 0.819239, showing the robustness of the embedded watermark.The graphical representation of the NC and PSNR value at different gain factors is shown in figure 3.4 and figure3.5 respectively.

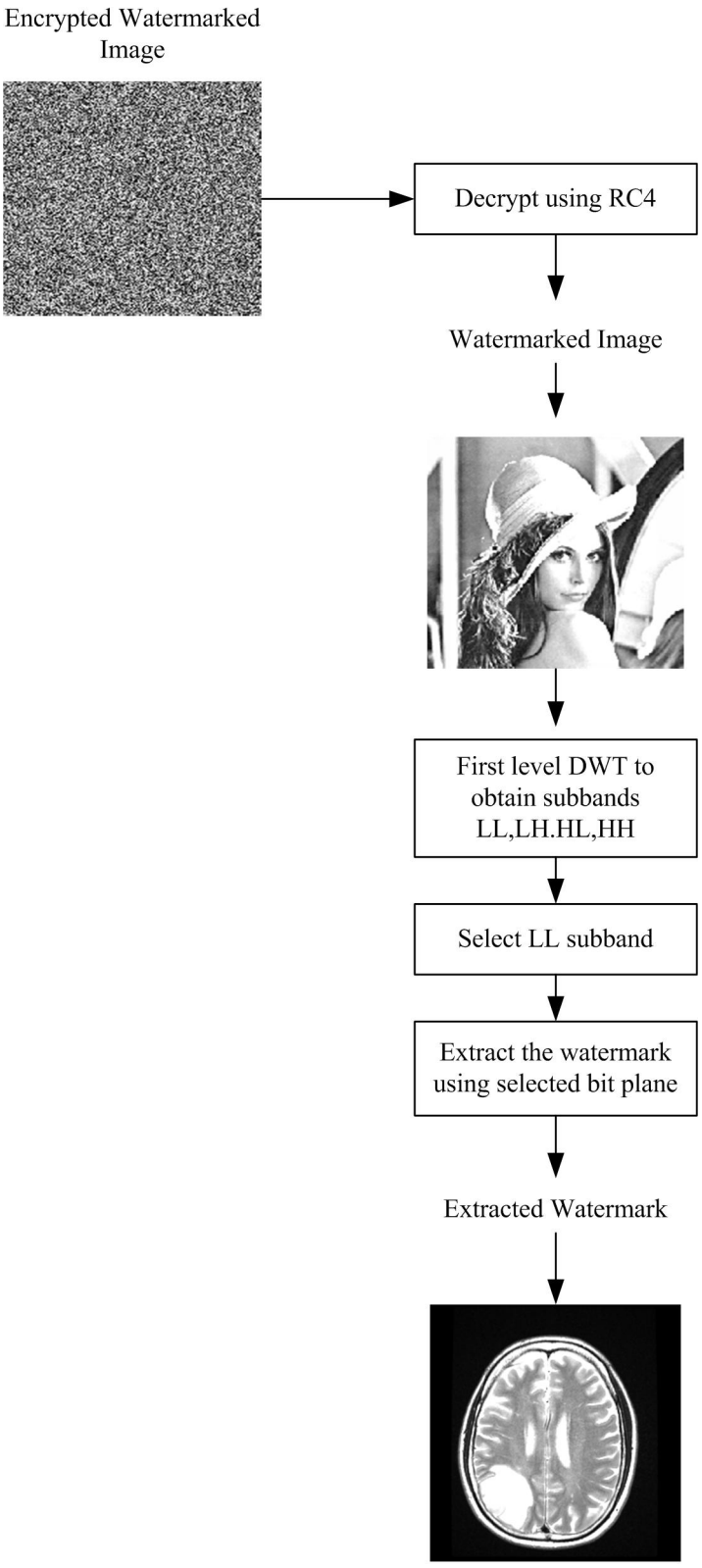
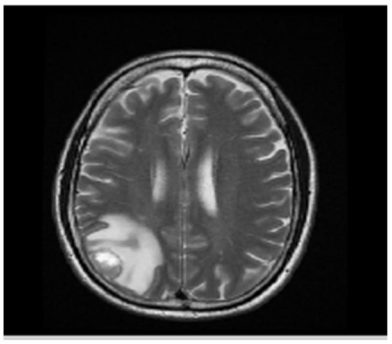


FIGURE 3.2: Watermark Extraction

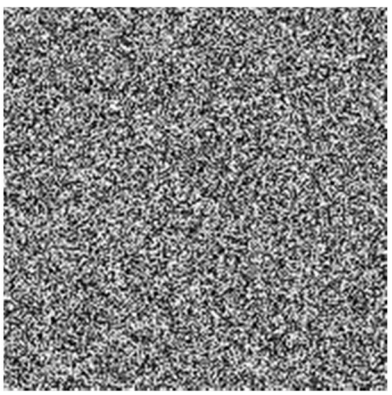
(a) Cover Image

(b) Watermark Image



(c) Watermarked Image

(d) Encrypted Watermarked Image



(e) Extracted Watermark Image

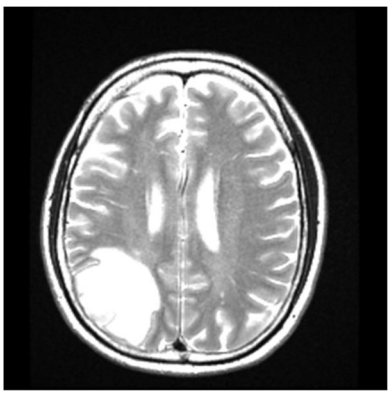


FIGURE 3.3: The Original and extracted watermark images

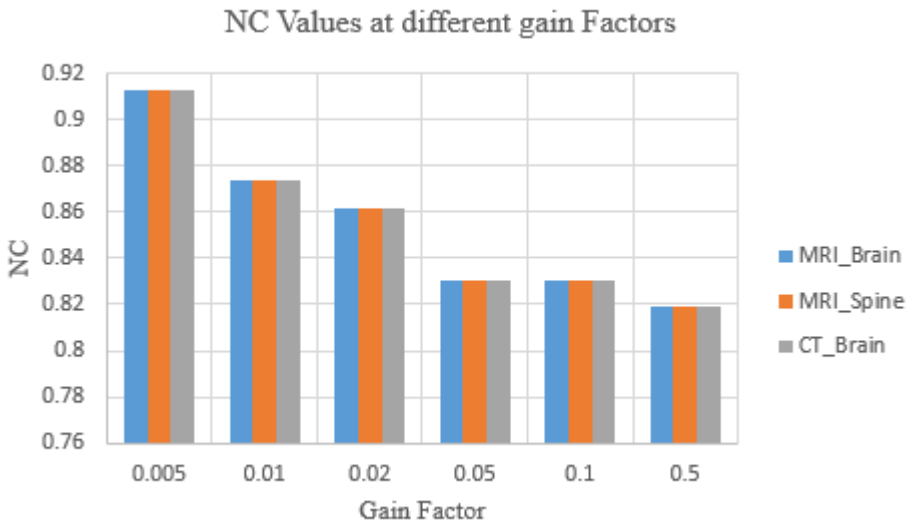


FIGURE 3.4: Variation of NC values with gain factor

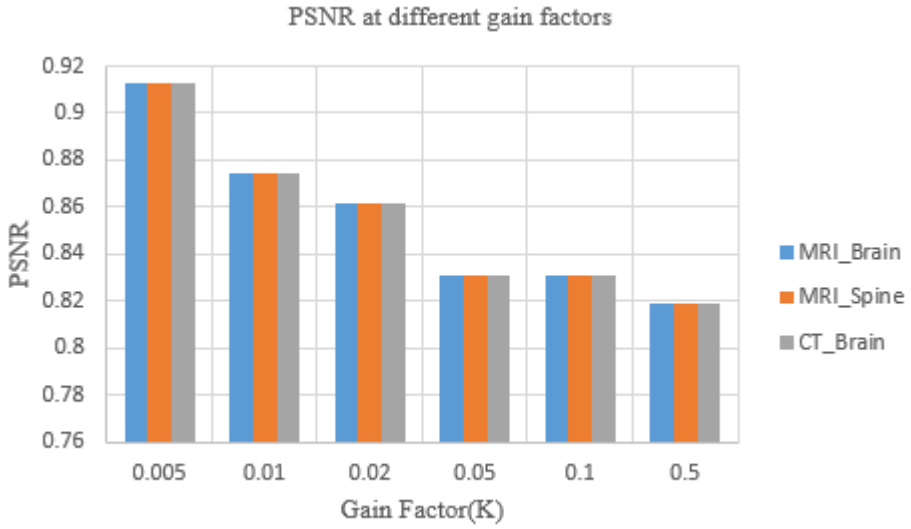


FIGURE 3.5: variation of PSNR with gain factor

TABLE 3.1: Performance of the proposed method at different gain factor

Gain Factor (K)	NC		
	Images		
	MRI		CT
	Brain	Spine	Brain
0.005	0.912624	0.912624	0.912624
0.01	0.874024	0.874024	0.874024
0.02	0.861216	0.861216	0.861216
0.05	0.830708	0.830708	0.830708
0.1	0.830708	0.830708	0.830708
0.5	0.819239	0.819239	0.819239

TABLE 3.2: PSNR at different gain factor

Gain Factor (K)	PSNR		
	Images		
	MRI		CT
	Brain	Spine	Brain
0.005	66.989667	68.540854	68.476300
0.01	67.780468	69.445400	69.313919
0.02	67.928538	69.627140	69.490127
0.05	68.288204	70.086778	69.865561
0.1	68.288204	70.086778	69.865561
0.5	68.405682	70.244338	69.994914

The watermarked image is attacked by the salt and pepper noise of different densities, shown in figure3.6.In Table 3.3 shows the evaluation of extracted watermark attacked by the noise at different noise density for salt and pepper noise at gain factors 0.1. The maximum NC values are obtained 0.912142 at noise density 0.001 with Lena image. However, the minimum NC values are obtained 0.685349 at noise density 0.02 with MRI image. The graphical representation of the variation of the NC value with different noise level is shown in figure 3.7.

In Table 3.4, the performance of the proposed method is evaluated against the different signal processing attacks. The highest NC value is obtained 0.8210 against JPEG attack with Lena image. However, minimum NC value 0.5780 against rotation attack with the same image. In this table, all NC values are acceptable except

(a) (b) (c)

FIGURE 3.6: The watermarked image attacked with salt and pepper noise of density (a)0.01(b)0.02(c)0.05

TABLE 3.3: NC values at different noise levels at k=0.1

Noise Level	NC		
	Images		
	MRI		CT
	Brain	Spine	Brain
0.001	0.912142	0.899075	0.873004
0.002	0.903781	0.890671	0.857468
0.005	0.883014	0.851669	0.817373
0.01	0.855245	0.814487	0.764562
0.02	0.804574	0.730041	0.685349

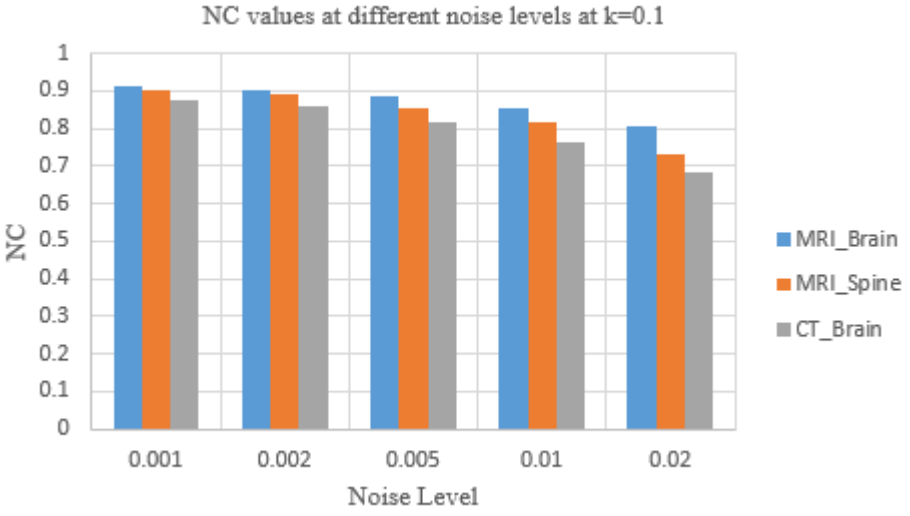


FIGURE 3.7: Variation of NC values with different noise levels

the rotation attack which is less than 0.7.The propose algorithm provides robust watermarking for medical data protection without degradation in the quality of the image.

TABLE 3.4: NC values at different signal processing attacks

Attacks	Lena	$MRI - brain - tumor$	$MRI - head$
Cropping	0.713410	0.666059	0.652286
Rotation	0.57801	0.547633	0.660975
Gaussian LPF	0.818905	0.750601	0.670656
JPEG Compression (Quality Factor = 65)	0.821044	0.802104	0.768578
Histogram Equalization	0.819204	0.762078	0.667692
Contrast Adjustment	0.819239	0.792079	0.668578

3.4 Conclusion

In the medical domain, after embedding the watermark, the quality of the image should remain high for the diagnostic purposes. Our proposed method provides a robust mechanism for watermarking with high invisibility. First level DWT is used for the transforming the cover and watermark images to frequency domain. The LL band is selected from watermark image and formatted using modulus functions. The formatted watermark is embedded in the LL band of the cover image. The watermarked image, then encrypted by using the stream cipher cryptographic techniques in order to achieved two level of security which may provide a potential solution to existing telemedicine security problem of patient identity theft.

CHAPTER 4

ENCRYPTED EPR DATA HIDING TECHNIQUE

The protection of data is of at prime urgency in the medical field to boost the telemedicine applications. There is a need of robust and secure mechanism to transfer the medical images over the Internet. The proposed watermarking method is based on two popular transform domain techniques, discrete wavelet transforms (DWT) and discrete cosine transform (DCT). In the embedding process, the cover medical image is divided into two separate parts, Region of Interest (ROI) and non region of interest (NROI). For the identity authentication purpose, multiple watermarks in the form of image and text are embedding into ROI and NROI part of the same cover media object respectively. In order to enhance the security of the text watermark, Rivest-Shamir-Adleman (RSA) encryption technique is applied to the text watermark before embedding and the encrypted EPR data is embedded into the NROI portion of the cover medical image. The performance of the proposed method is analyzed against known signal processing attacks such as compression, filtering, noise and histogram equalization and the desired outcome is obtained without significant degradation in extracted watermark and watermarked image quality.

4.1 Watermark Embedding

The proposed DWT-DCT based watermarking method is formulated as embedding and extraction process as given below:

1. Segment the cover image into ROI and NROI parts. Apply second-level DWT on ROI and NROI of the cover image to obtain the sub-bands as LL2, LH2, HL2 and HH2.
2. Apply third-level DWT on the watermark image and DCT transformation to LL3 sub-band of the DWT watermark image. Format the DCT transform of watermark image using modulus function to obtain watermark 'w1'.
3. Select the electronic patient record (EPR) data file as text watermark and encrypt the watermark using public key cryptography to obtain the watermark 'w2'.
4. Apply inverse discrete cosine transform (IDCT) and second-level inverse discrete wavelets transform (IDWT) to embed the image watermark in the ROI part of the cover image. Apply second-level inverse discrete wavelet transform (IDWT) to the embed text watermark in the NROI region.
5. Merge the embedded ROI and NROI parts of the medical cover image to form the final watermarked image.

The schematic representation of the embedding process is given in the figure 4.1.

4.2 Watermark Extraction

1. Segment the watermarked image into the ROI and NROI parts.

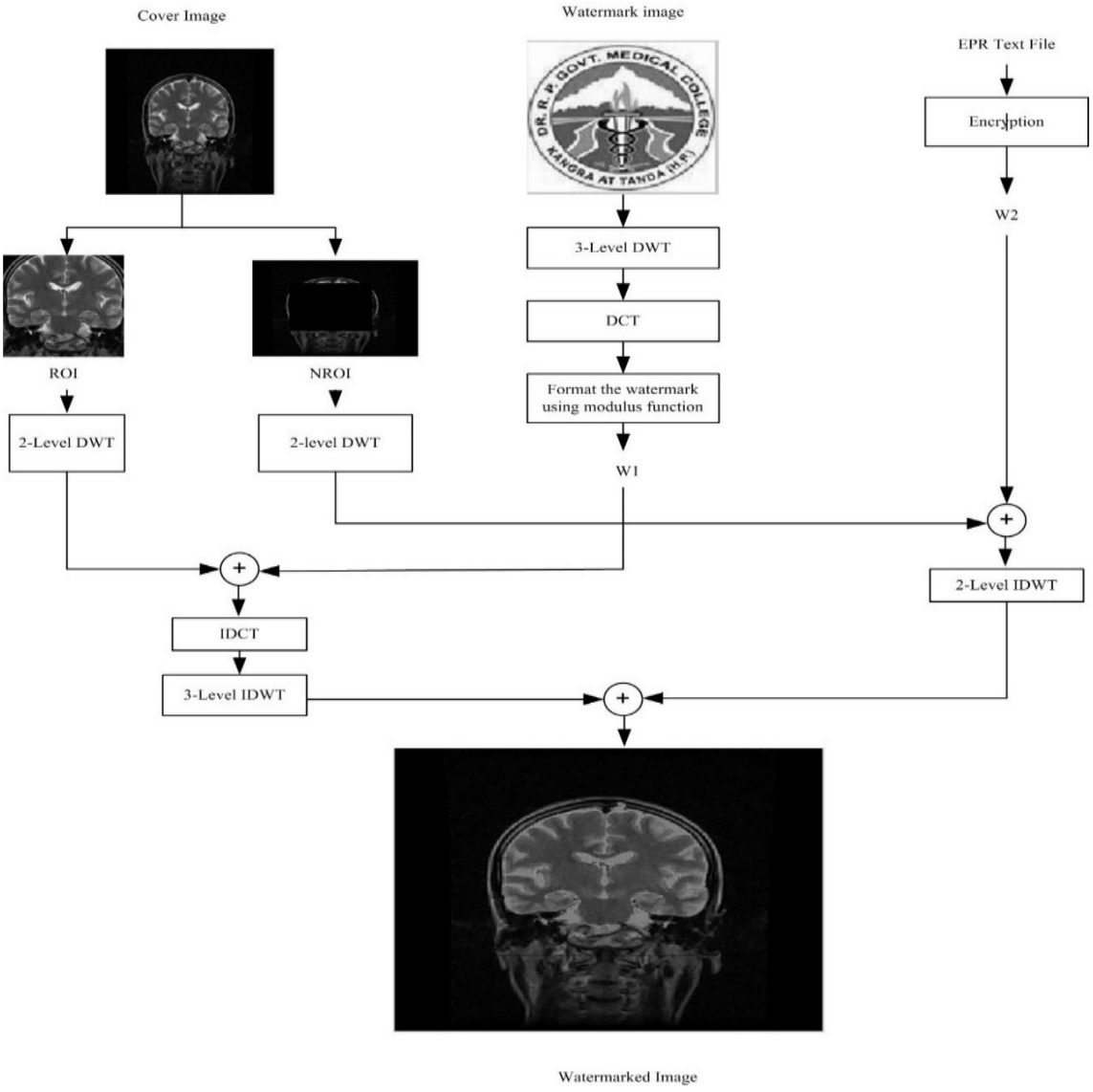


FIGURE 4.1: Watermark Embedding

2. Apply second-level DWT on NROI and third-level DWT on ROI of the cover medical image and DCT transform to the LL3 sub-band of ROI part of the cover.

3. Extract the watermark 'w1' from the ROI part and encrypted text watermark 'W2'from NROI of the cover image respectively.

4. Decrypt the watermark 'w2' using the public key cryptography to obtain EPR data. The schematic representation of the watermarking image is as shown in figure4.2.

4.3 Experimental Results and Analysis

The watermarking embedding and extraction is done for the MRI, CT and ultrasound images . The medical image size 512×512 is used as the cover image, which is divided into the ROI and NROI regions,shown in figure 4.3. The watermark image is embedded to the ROI region and the EPR data is embedded to the NROI region. The Extracted and the original watermark images and the EPR data are shown in the Figure 4.4.The watermarked image is subjected to the different signal processing attacks and analysis of the obtained peak signal to noise ratio (PSNR), normalize cross correlation(NC) and bit error rate (BER) is done for different MRI, CT-scan images. The quality of the watermarked image is evaluated by the parameter peak signal to noise ratio (PSNR) and the robustness of the extracted image and text watermark is evaluated by the parameter normalize cross correlation (NC) and bit error rate (BER) respectively . We simulated the proposed method using MATLAB. Based on the experimental results, the NC, BER and PSNR values are illustrated in Table 4.1 to 4.10. Table 4.1 describes the NC values for image watermark 'w1' at different gain factors ranging from 0.01 to 1.

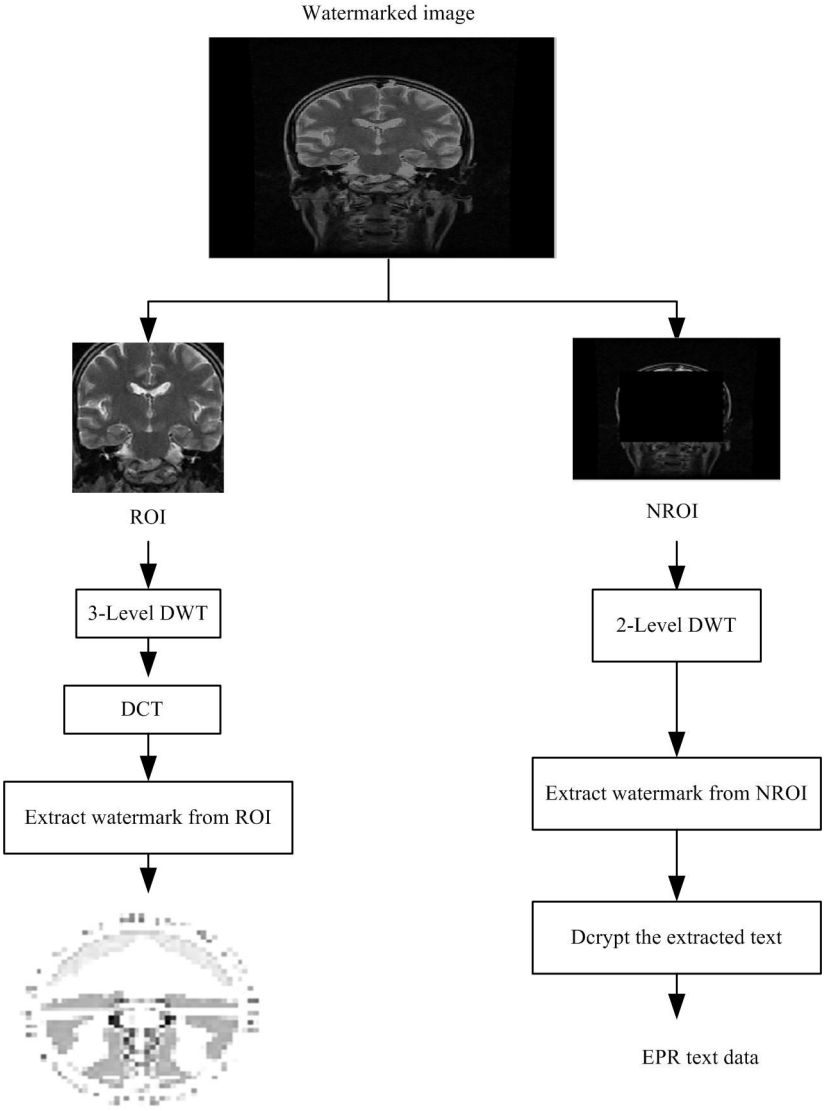


FIGURE 4.2: Watermark Extraction

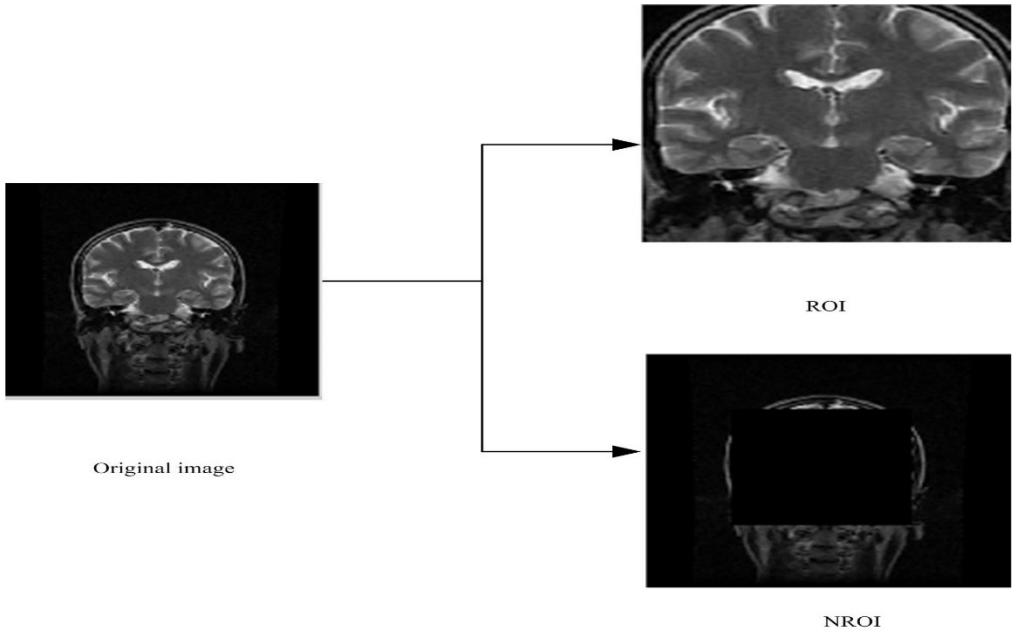


FIGURE 4.3: Segmentation into ROI and NROI of medical image

TABLE 4.1: Performance of the proposed method at different gain factor

Gain Factor (K)	NC		
	Images		
	MRI		CT
	Brain	Spine	Brain
0.01	0.8356	0.9350	0.9167
0.02	0.9314	0.9310	0.9214
0.05	0.9867	0.9854	0.9776
0.5	0.9999	0.9999	0.9999
0.6	0.9999	0.9999	0.9999
0.8	0.9999	0.9999	0.9999
1	1.0000	1.0000	1.0000

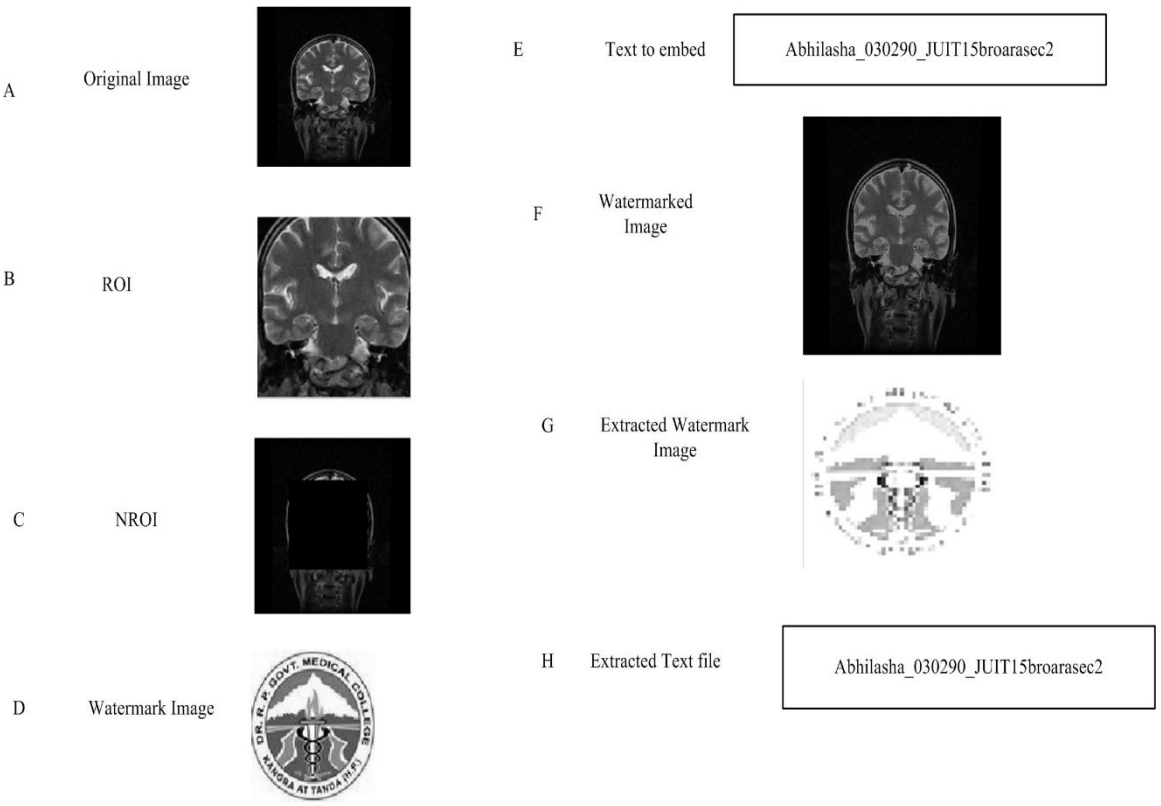


FIGURE 4.4: The Original and extracted watermark images and EPR data

It is observed that the robustness performance is increasing with increasing the gain factors. In this Table, the NC value evaluated at different gain factors and it is observed that the maximum value is obtained at gain factor = 1 for MRI images. For CT scan images, the NC values ranges from 0.9167 to 1 at gain factors 0.01 to 1 respectively.The graphical representation of variation of NC with gain factor is shown in figure 4.5.

Table 4.2 shows the PSNR performance obtained by the proposed method without the signal processing attacks.

From the experimental result it is observed that the PSNR value decreases with the increase in gain factor. For Brain MRI image, the PSNR ranges from 37.502050 to 49.150897 at gain factor 1 to 0.01. However, PSNR value ranges from 45.822401

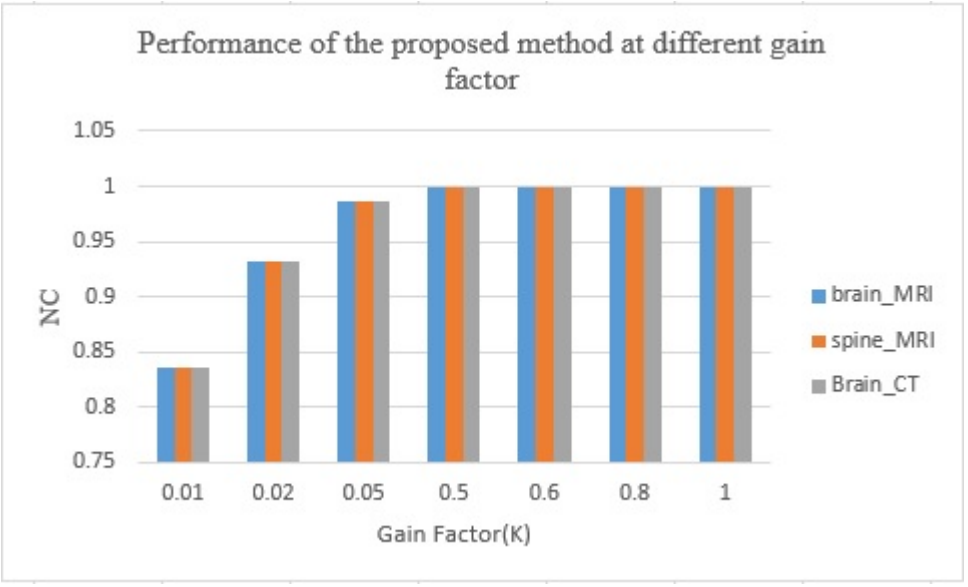


FIGURE 4.5: Variation of NC with gain factor

TABLE 4.2: PSNR evaluation at different gain Factors

Gain Factor (K)	PSNR		
	Images		
	MRI		CT
	Brain	Spine	Brain
0.01	49.150897	48.667850	45.822401
0.02	45.743550	44.762781	44.337568
0.05	43.916029	44.319781	42.671462
0.5	43.876238	42.094049	42.437707
0.6	41.357288	41.544884	41.858433
0.8	40.421644	40.659953	39.004608
1	38.906702	38.145452	37.502050

to 37.502050 at the same gain factors.The graphical representation of variation of PSNR is shown in figure 4.6.

The watermarked images are attacked by the noise at different noise density for salt and pepper noise with varying density, Gaussian noise at different mean (M) and variance(V) and speckle noise at different variance at different gain factors,shown in figure 4.7. With increase in the noise density NC value decreases but at a higher

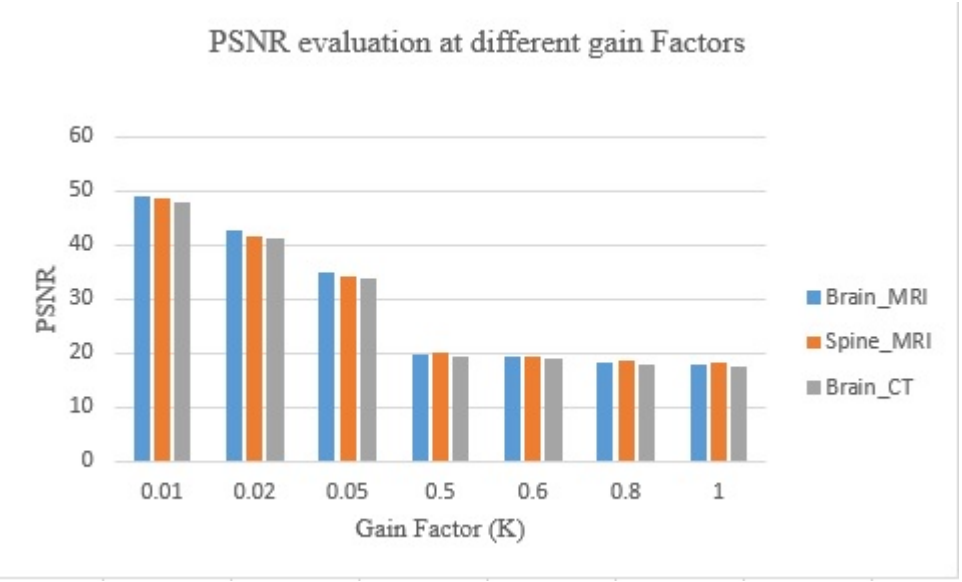


FIGURE 4.6: Variation of PSNR with gain factor(K)

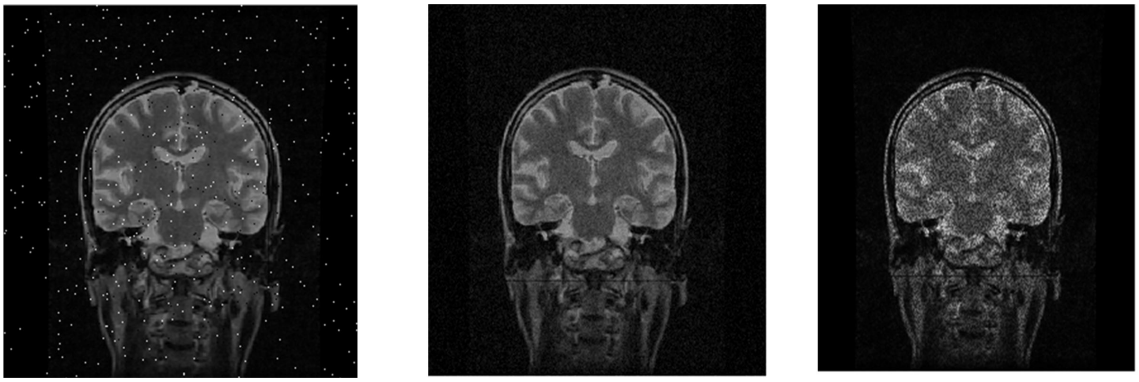


FIGURE 4.7: The attacked watermark images by (a)Salt and pepper at density 0.01 (b) Gaussian noise at mean 0.01 and variance 0.001 (c)Speckle noise at variance 0.1

gain factor NC is high for a particular noise value.
The PSNR value also decreased with increase in noise density but the value of PSNR is more at a smaller gain factor for a particular noise density.

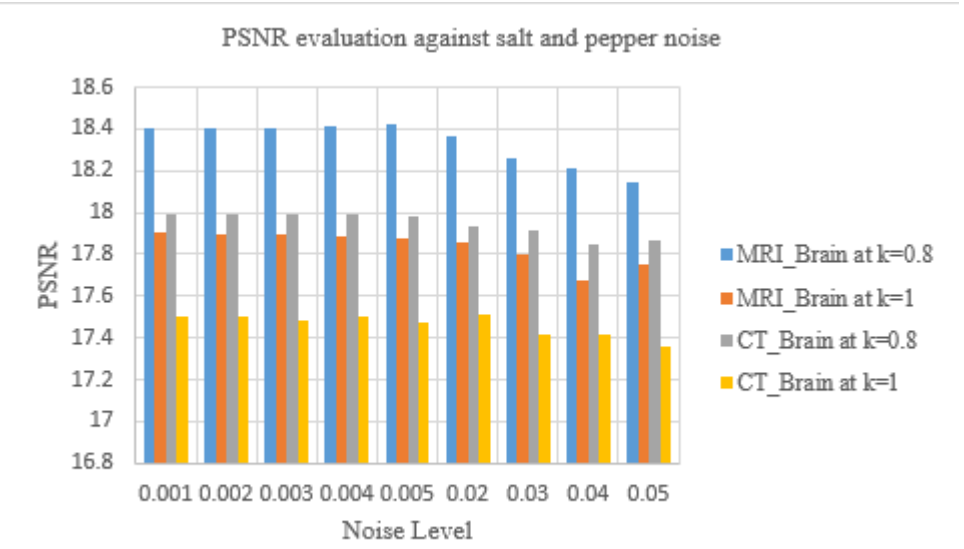


FIGURE 4.8: PSNR evaluation against salt and pepper noise

The graphical variation of PSNR at different noise levels for salt and pepper noise is shown in figure 4.8. The maximum values are obtained at gain factor k=1.Table 4.3 to 4.5 shows the NC values for image watermark 'w1' for different noise attacks at different levels.

Referring to this table it is observed that the proposed method is robust against the different noise attacks at various noise levels. The brain MRI and brain CT scan images are attacked by the different noise at different noise level.The graphical representation of the variation of NC at different noise levels of salt and pepper noise is shown in figure 4.9.

It is observed that for brain MRI images, the NC value is 0.9764 when watermarked image is attacked by salt and pepper noise at noise level 0.001,indicating the robustness of the image watermark. For Gaussian noise (mean (M) = 0 and variance (V) = 0.00001), the NC value is 0.9487 for brain MRI images and 0.9932

TABLE 4.3: Performance of the proposed method against salt and pepper attack

Noise Level	NC			
	MRI		CT	
	Brain		Brain	
	K=0.8	K=1.0	K=0.8	K=1.0
0.001	0.9764	0.9850	0.9595	0.9751
0.002	0.9064	0.9380	0.9607	0.9678
0.003	0.8842	0.9221	0.8959	0.9277
0.004	0.8642	0.9396	0.8672	0.9034
0.005	0.8673	0.9181	0.8376	0.8555
0.02	0.7921	0.7662	0.7200	0.7778
0.03	0.7645	0.7472	0.6953	0.7428
0.04	0.7063	0.7167	0.6882	0.7143
0.05	0.7245	0.7069	0.6862	0.6947

TABLE 4.4: Performance of the proposed method against speckle attack

Noise Level	NC			
	MRI		CT	
	Brain		Brain	
Variance(V)	K=0.8	K=1.0	K=0.8	K=1.0
0.00001	0.9830	0.9532	0.9972	0.9883
0.00002	0.9247	0.9526	0.9972	0.9963
0.00004	0.9109	0.9563	0.9943	0.9806
0.00005	0.92877	0.9273	0.9697	0.9895
0.0001	0.8770	0.8703	0.9572	0.9680
0.0002	0.8638	0.8449	0.9581	0.9668
0.0003	0.7775	0.8599	0.9266	0.9561

for brain CT images.The graphical variation of NC and PSNR at different levels of speckle noise is shown in figure 4.10 and 4.11 respectively.

Table 4.6 shows the performance of the proposed method has been evaluated for different signal processing attacks. It is observed from the NC value for MRI images is much better than CT scan images.

To evaluate the performance of the Text watermark, we calculate bit error rate (BER). The watermarked NROI image is attacked by the different noise levels of different density. The percentage bit error rate depends on the number of bits

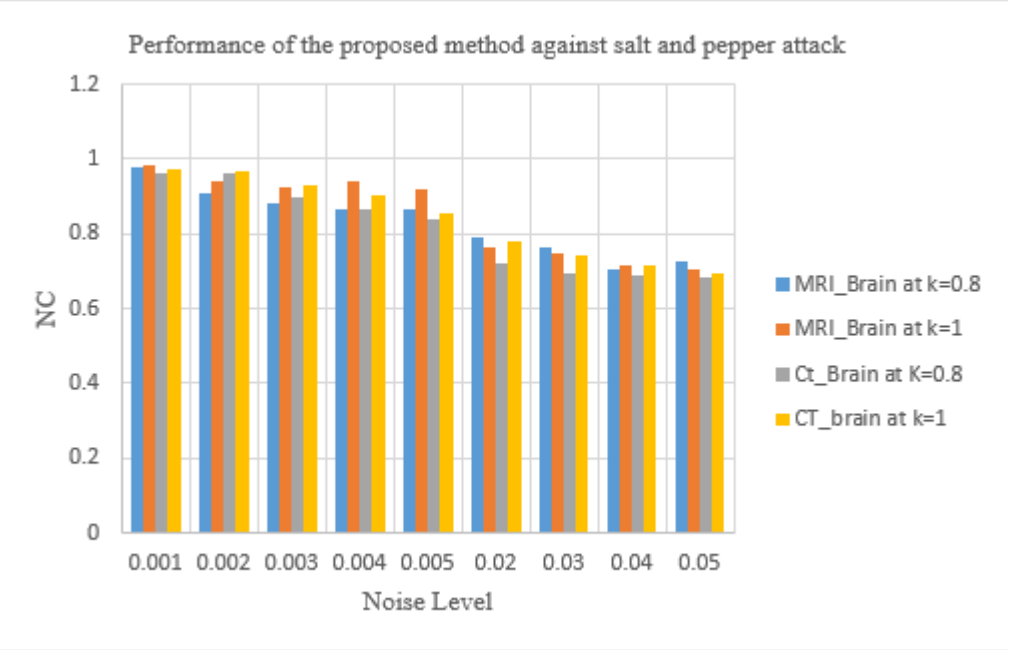


FIGURE 4.9: Variation of NC at different noise levels

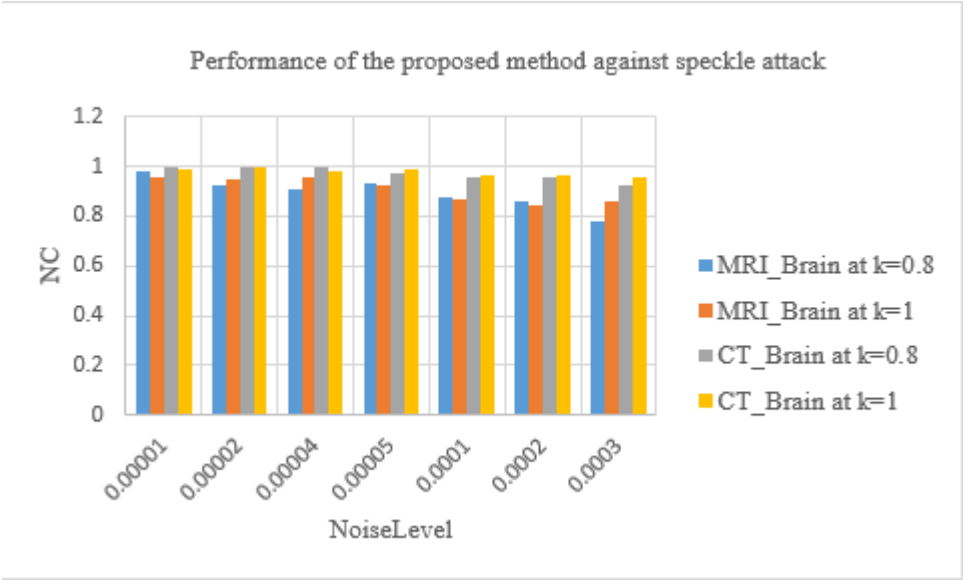


FIGURE 4.10: Performance of the proposed method against speckle attack

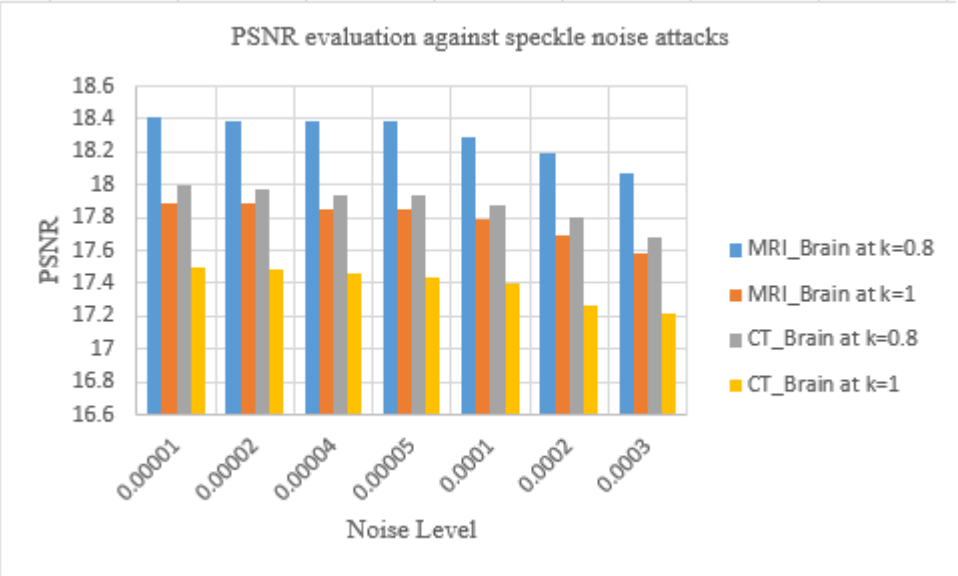


FIGURE 4.11: PSNR evaluation against speckle noise attacks

TABLE 4.5: Performance of the proposed method against Gaussian noise attack

Noise Level		NC			
		MRI		CT	
		Brain		Brain	
Mean(M)	Variance(V)	K=0.8	K=1.0	K=0.8	K=1.0
0	0.00001	0.9476	0.9487	0.9688	0.9932
0	0.00003	0.8577	0.9168	0.9725	0.9781
0	0.00005	0.8099	0.8679	0.9475	0.9605
0.0001	0.00002	0.9319	0.9027	0.9602	0.9853
0.0001	0.00003	0.8577	0.9072	0.9782	0.9728
0.001	0.00001	0.8762	0.9389	0.9843	0.9834
0.001	0.00002	0.8762	0.9110	0.9876	0.9734

changed by attacking the image.The table4.7 to 4.9 shows the BER (in %) for different noise attacks.The graphical representation of variation of BER (in %) at different noise levels of salt and pepper and speckle noise is shown in figure 4.12 and 4.13 respectively.Table4.10 shows the BER (in %) against different signal processing attacks.

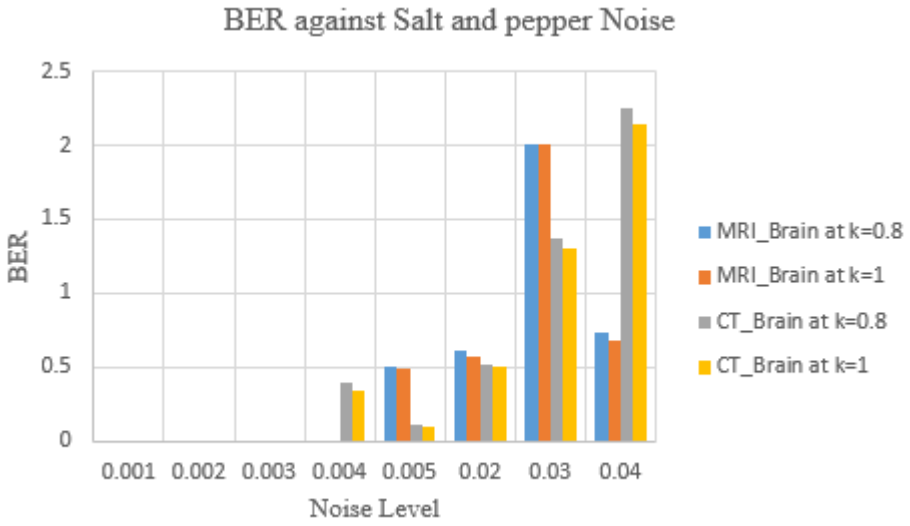


FIGURE 4.12: BER (in %) against salt and pepper noise attacks

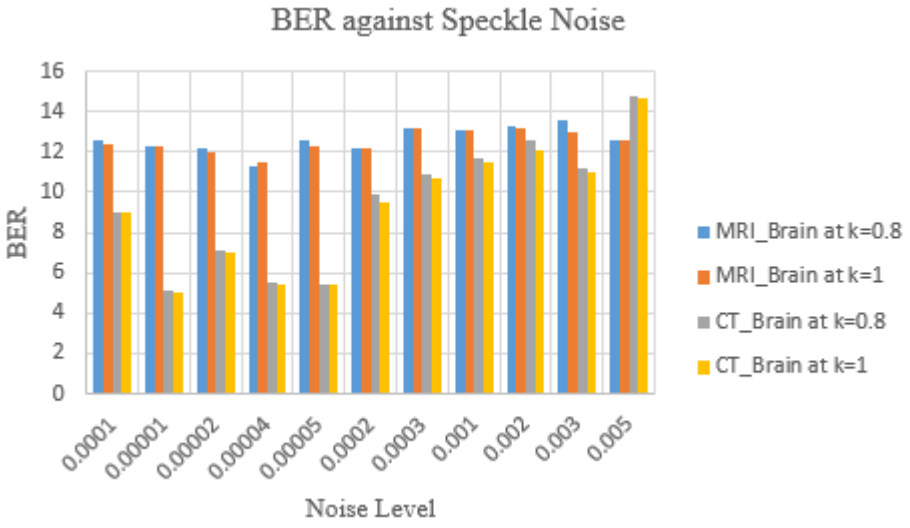


FIGURE 4.13: BER (in %) against Speckle Noise

TABLE 4.6: NC values against different signal processing attacks

Attacks	NC			
	MRI		CT	
	Brain		Brain	
	K=0.8	K=1.0	K=0.8	K=1.0
JPEG Compression (QF=65)	0.9999	1.0000	0.9999	1.0000
Contrast Adjustment	0.8185	0.8406	0.9999	1.0000
Histogram Equalization	0.7353	0.7498	0.7513	0.7751
Gaussian LPF	0.72017	0.7179	0.7459	0.7349
Rotation	0.6127	0.6327	0.6027	0.6127

TABLE 4.7: BER (in %) against salt and pepper noise attacks

Noise Level	BER(in %)			
	MRI		CT	
	Brain		Brain	
	K=0.8	K=1.0	K=0.8	K=1.0
0.001	0	0	0	0
0.002	0	0	0	0
0.003	0	0	0	0
0.004	0	0	0.3906	0.3446
0.005	0.5091	0.4859	0.1116	0.1026
0.02	0.6066	0.5766	0.5208	0.5108
0.03	2.0038	2.0008	1.3672	1.3072
0.04	0.7313	0.6813	2.2461	2.1417

To protect the confidential EPR data, it is encrypted using the public key cryptographic algorithms such as RSA. At different value of prime numbers P and Q, the encryption and decryption time for different EPR text files is evaluated. Table 5 shows the encryption and decryption time for different EPR text files is as at different P and Q values.The variation of encryption and decryption time for data files of different size is shown in figure 4.14.

The EPR data is encrypted by using the public key cryptographic method. Due to

Table 4.8: BER (in %) against Gaussian noise attacks

Noise Level		BER (in %)			
		MRI		CT	
		Brain		Brain	
Mean(M)	Variance(V)	K=0.8	K=1.0	K=0.8	K=1.0
0.001	0.00001	2.3333	1.5533	2.5868	1.9968
0.001	0.00002	2.9340	2.8740	2.1424	2.0014
0.0001	0.00002	5.6319	5.1678	5.7643	5.1910
0.0001	0.00003	8.0625	7.9999	9.0972	9.7823
0	0.00001	10.3299	9.9564	11.5000	10.6751
0	0.00005	12.6250	12.5067	13.3611	12.9936
0	0.0001	18.3267	18.6002	18.5307	17.3051

Table 4.9: BER (in %) against Speckle Noise

Noise Level	BER (in %)			
	MRI		CT	
	Brain		Brain	
Variance(V)	K=0.8	K=1.0	K=0.8	K=1.0
0.0001	12.5868	12.3489	9.0278	9.0018
0.00001	12.3264	12.3041	5.1215	5.0285
0.00002	12.1528	12.0078	7.1181	7.0034
0.00004	11.2847	11.4396	5.5556	5.4356
0.00005	12.5868	12.3107	5.4688	5.3987
0.0002	12.1528	12.1360	9.8958	9.4587
0.0003	13.1944	13.1811	10.9375	10.6575
0.001	13.1076	13.1004	11.7188	11.4571
0.002	13.2813	13.1334	12.5868	12.0573
0.003	13.5417	13.0143	11.1979	11.0017
0.005	12.5868	12.5840	14.7569	14.7035

the limited resource capacity of our experimental setup, we simulated the proposed algorithm on smaller prime numbers. But it can also perform well with large prime numbers. The encryption and decryption time depends on the size of the EPR data file.

TABLE 4.10: BER (in %) values at different signal processing attacks

Attacks	BER(in %)	
	MRI	CT
	Brain	Brain
JPEG Compression QF=65	2.8472	0
Contrast Adjustment	2.002	0
Histogram Equalization	7.6910	8.1563
Gaussian LPF	3.2813	7.9688
Rotation	7.6319	8.0507
Cropping	10.2857	10.8333

TABLE 4.11: Encryption and decryption time for different texts

P	Q	Encryption time(in sec)		Decryption time (in sec)	
		EPR 1(89 B)	EPR 2(110 B)	EPR 1(89 B)	EPR 2(110 B)
43	47	0.1563	0.1719	0.2500	0.265625
89	97	0.2701	0.2786	0.3700	0.3900
131	113	0.4856	0.4999	0.6066	0.6589

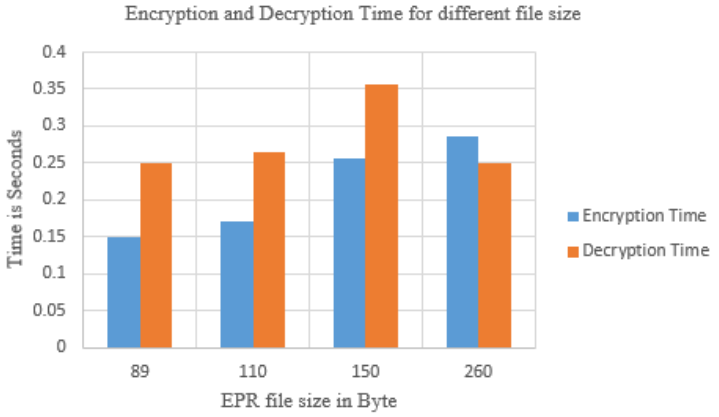


FIGURE 4.14: Encryption and Decryption time variation with different file size

4.4 Conclusion

In medical field, the security of EPR data is prime to protect the confidential patient reports from the unauthorized access and unwanted tamper. The medical images shared over the Internet must be protected from malicious attacks. In this paper, the proposed watermarking method based on DWT and DCT. For the identity authentication purpose, the method is used multiple watermarking in the form of text and image. The medical image is taken as cover image, diving it into ROI and NROI regions. The more robust and confidential data such as EPR data files are embedded into NROI region and less robust data such as logo is embedded to the ROI region.

The ROI and NROI portion is transformed using second-level DWT. By transforming the image using third-level DWT and then DCT is applied to LL3 sub-band of the watermark image to form the watermark 'W1'. The EPR data is encrypted using the public key cryptographic techniques such as RSA. From the simulated results, it can be concluded that the proposed algorithm is robust against the various signal processing attacks and also have good imperceptibility indicating the high quality of the watermarked image.

CHAPTER 5

ENCRYPTED EPR DATA HIDING TECHNIQUE USING MD-5

The protection of data is of at prime urgency in the medical field to boost the telemedicine applications. There is a need of robust and secure mechanism to transfer the medical images over the Internet. The proposed watermarking method is based on two popular transform domain techniques, discrete wavelet transforms (DWT) and discrete cosine transform (DCT). In the embedding process, the cover medical image is divided into two separate parts, Region of Interest (ROI) and non region of interest (NROI). For the identity authentication purpose, multiple watermarks in the form of image and text are embedding into ROI and NROI part of the same cover media object respectively.The image watermark is hashed using MD-5 to make it secure. In order to enhance the security of the text watermark, Rivest-Shamir-Adleman (RSA) encryption technique is applied to the text watermark before embedding and the encrypted EPR data is encoded using hamming codes and embedded into the NROI portion of the cover medical image. The performance of the proposed method is analyzed against known signal processing attacks such as compression, filtering, noise and histogram equalization and the

desired outcome is obtained without significant degradation in extracted watermark and watermarked image quality.

5.1 Watermark Embedding

The proposed $DWT - DCT$ and $MD - 5$ based watermarking method is formulated as embedding and extraction process as given below:

1. Segment the cover image into ROI and NROI parts. Apply second-level DWT on ROI and NROI of the cover image to obtain the sub-bands as LL2, LH2, HL2 and HH2.
2. Apply third-level DWT on the watermark image and DCT transformation to LL3 sub-band of the DWT watermark image. Format the DCT transform of watermark image using modulus function to obtain watermark.
3. Hash the formatted watermark using $MD - 5$ to generate watermark 'w1'.
4. Select the electronic patient record (EPR) data file as text watermark and encrypt the watermark using public key cryptography.
5. Encode the encrypted watermark using hamming codes to obtain the watermark 'w2'.
6. Apply inverse discrete cosine transform (IDCT) and second-level inverse discrete wavelets transform (IDWT) to embed the image watermark in the ROI part of the cover image. Apply second-level inverse discrete wavelet transform (IDWT) to the embed text watermark in the NROI region.
7. Merge the embedded ROI and NROI parts of the medical cover image to form the final watermarked image.

8. Encrypt the final watermarked image.

The schematic representation of the embedding process is given in the figure 5.1.

5.2 Watermark Extraction

1. Decrypt the watermarked image.
2. Segment the watermarked image into the ROI and NROI parts.
3. Apply second-level DWT on NROI and third-level DWT on ROI of the cover medical image and DCT transform to the LL3 sub-band of ROI part of the cover.
4. Rehash the image using $MD-5$ to extract the watermark 'w1' from the ROI part.
5. Extract the text watermark 'w2' from NROI of the cover image.
6. Decrypt the watermark 'w2' using the public key cryptography and then decode it using hamming codes to obtain EPR data. The schematic representation of the watermarking image is as shown in figure5.2.

5.3 Experimental Results and Analysis

The watermarking embedding and extraction is done for the MRI, CT-scan images . The medical image size 512×512 is used as the cover image, which is divided into the ROI and NROI regions,shown in figure 5.3. The watermark image is embedded to the ROI region and the EPR data is embedded to the NROI region. The original and extracted watermark images and EPR data are shown in the Figure 5.4.The watermarked image is subjected to the different signal processing

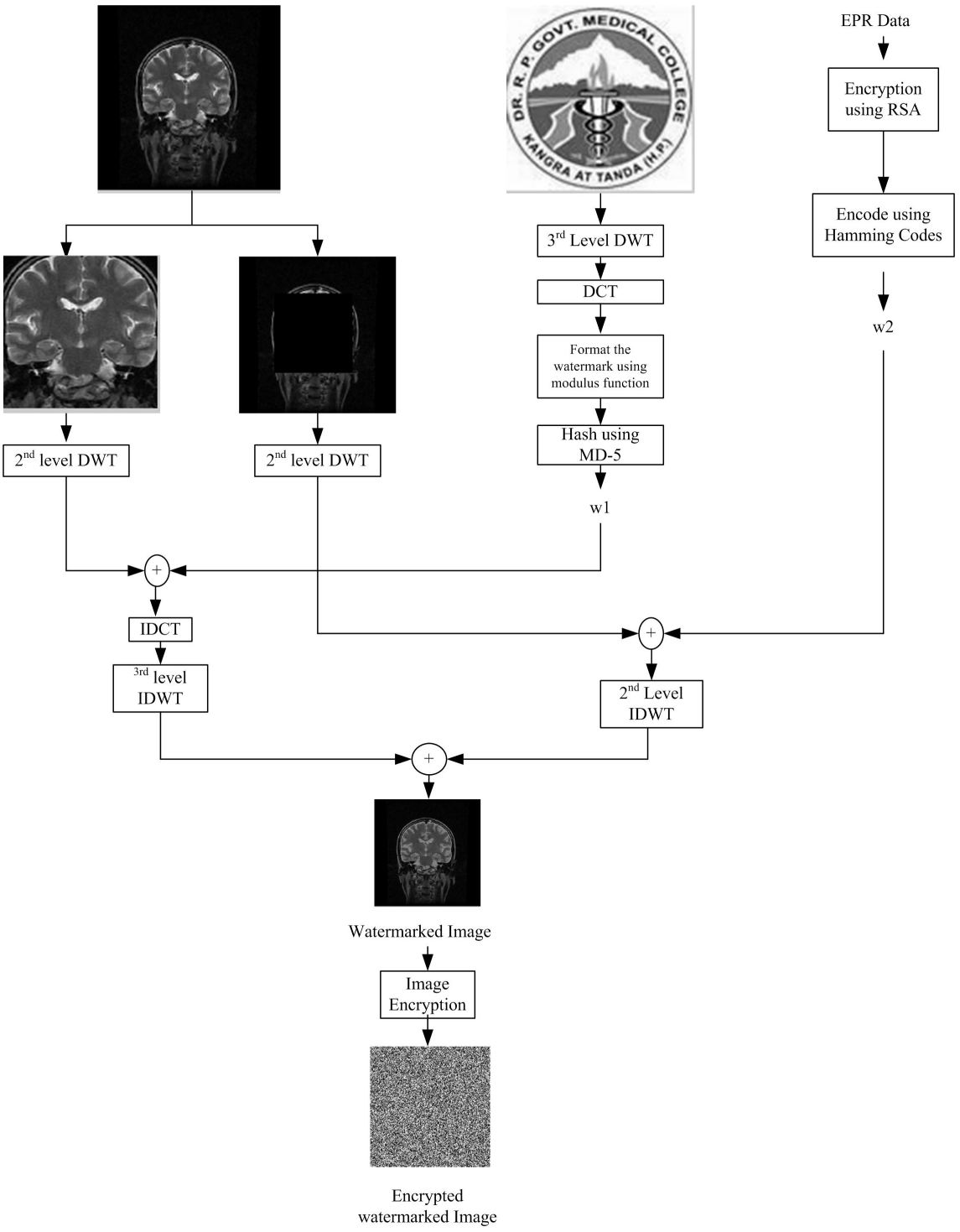


FIGURE 5.1: Watermark Embedding

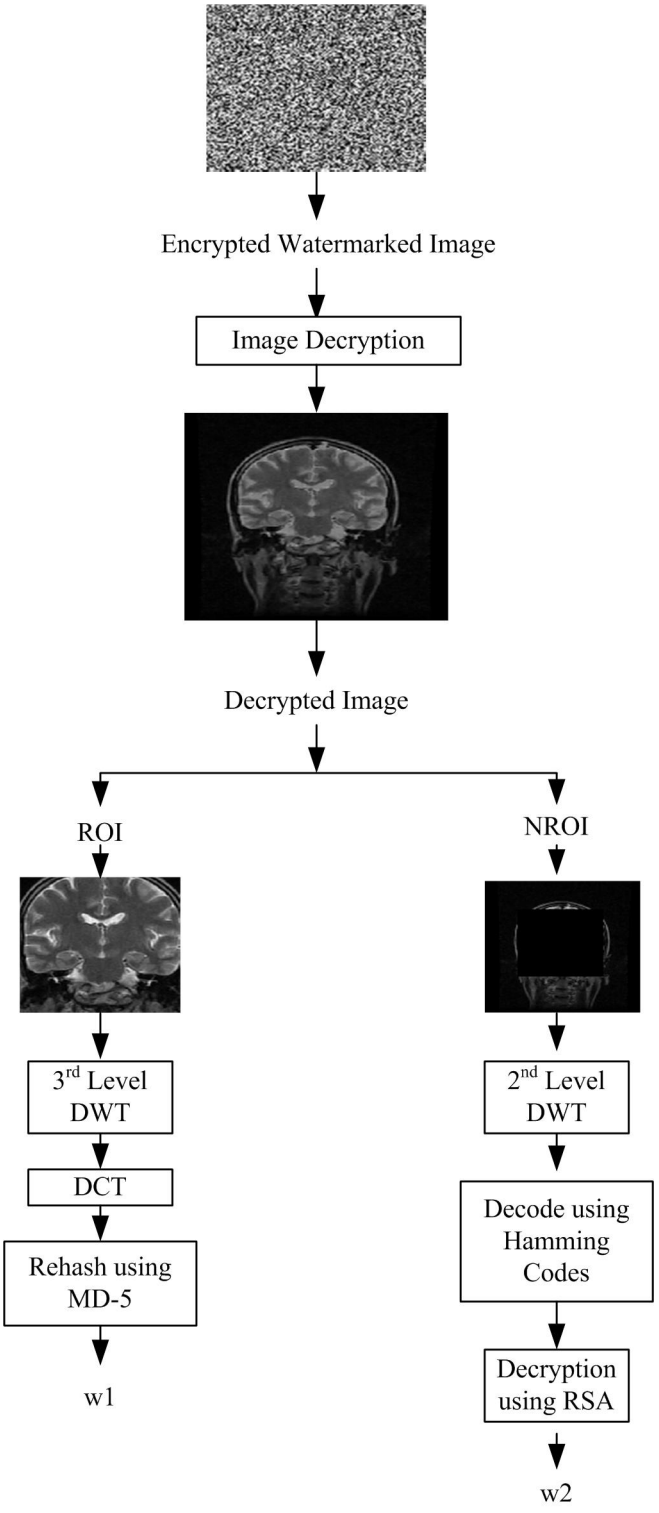


FIGURE 5.2: Watermark Extraction

attacks and analysis of the obtained peak signal to noise ratio (PSNR), normalize cross correlation(NC) and bit error rate (BER) is done for different MRI, CT-scan images.

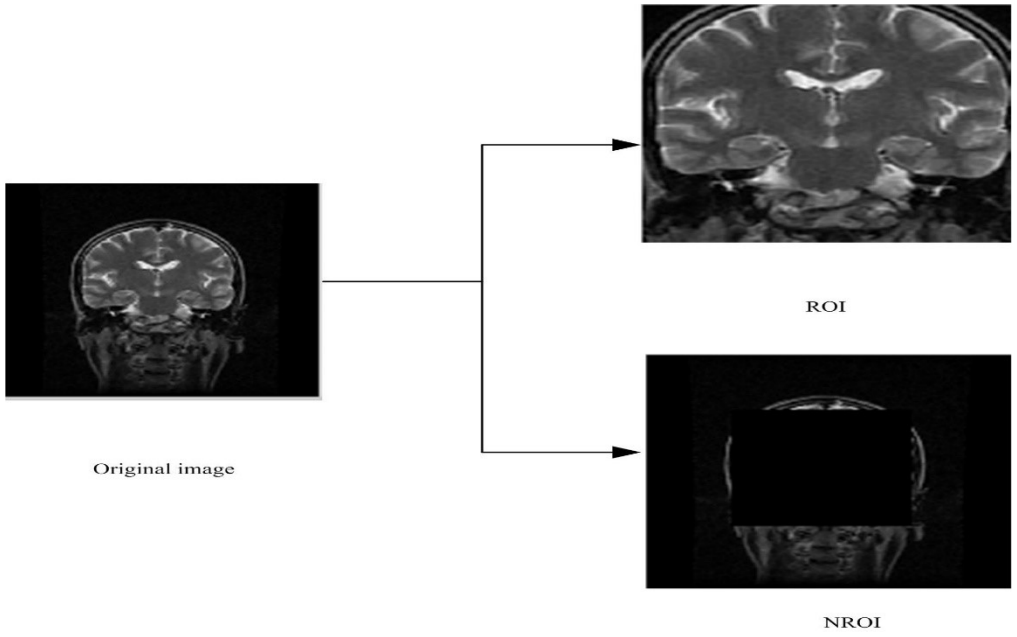


FIGURE 5.3: Segmentation into ROI and NROI of medical image

The quality of the watermarked image is evaluated by the parameter peak signal to noise ratio (PSNR) and the robustness of the extracted image and text watermark is evaluated by the parameter normalize cross correlation (NC) and bit error rate (BER) respectively . We simulated the proposed method using MATLAB. Based on the experimental results, the NC, BER and PSNR values are illustrated in Table 5.1 to 5.11. Table 5.1 describes the NC values for image watermark 'w1' at different gain factors ranging from 0.01 to 1.

It is observed that the robustness performance is increasing with increasing the gain factors. In this Table, the NC value evaluated at different gain factors and it is observed that the maximum value is obtained at gain factor one for MRI images.

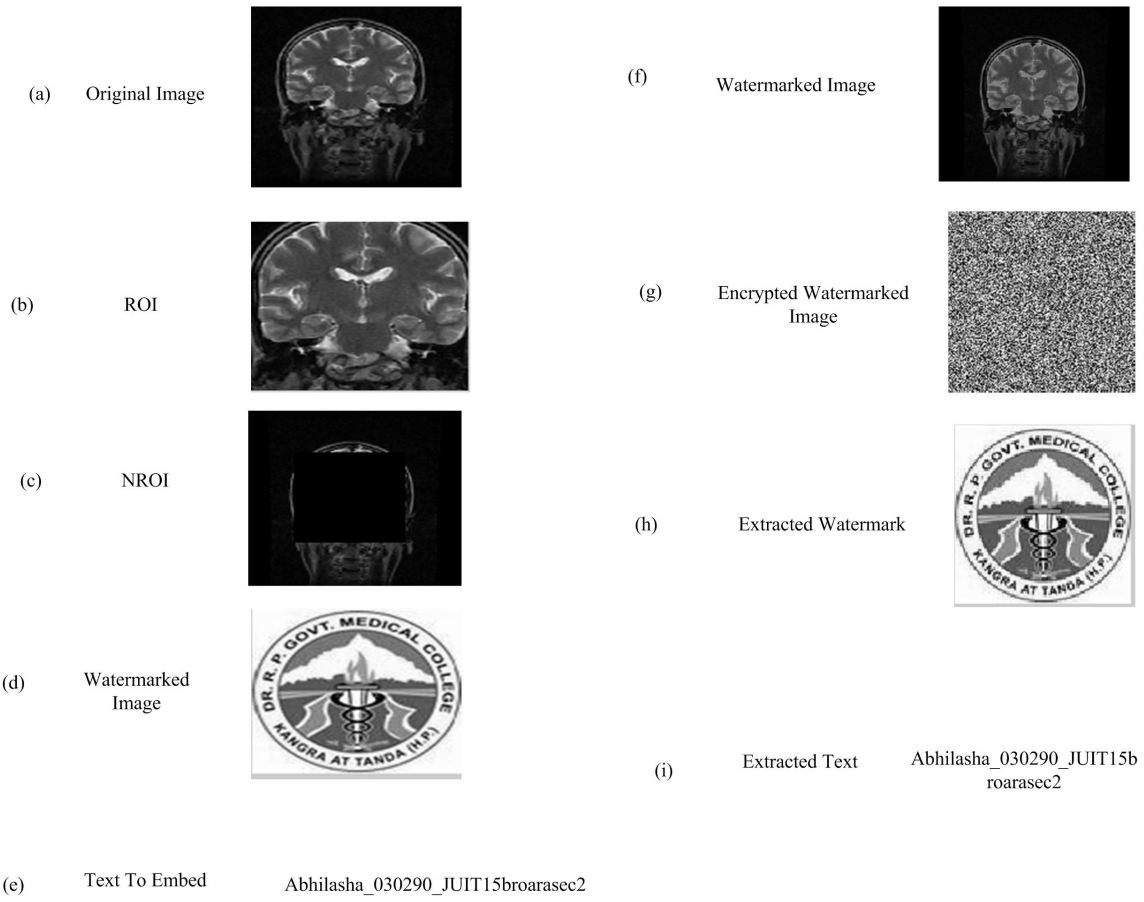


FIGURE 5.4: The Original and extracted watermark images and EPR data

TABLE 5.1: Performance of the proposed method at different gain factor

Gain Factor (K)	NC		
	Images		
	MRI		CT
	Brain	Spine	Brain
0.01	1.000000	1.000000	1.000000
0.02	1.000000	1.000000	1.000000
0.05	1.000000	1.000000	1.000000
0.5	1.000000	1.000000	1.000000
0.6	1.000000	1.000000	1.000000
0.8	1.000000	1.000000	1.000000
1	1.000000	1.000000	1.000000

For CT scan images, the NC values is 1 at gain factors 0.01 to 1.The graphical representation of variation of NC with gain factor is shown in figure 5.5.

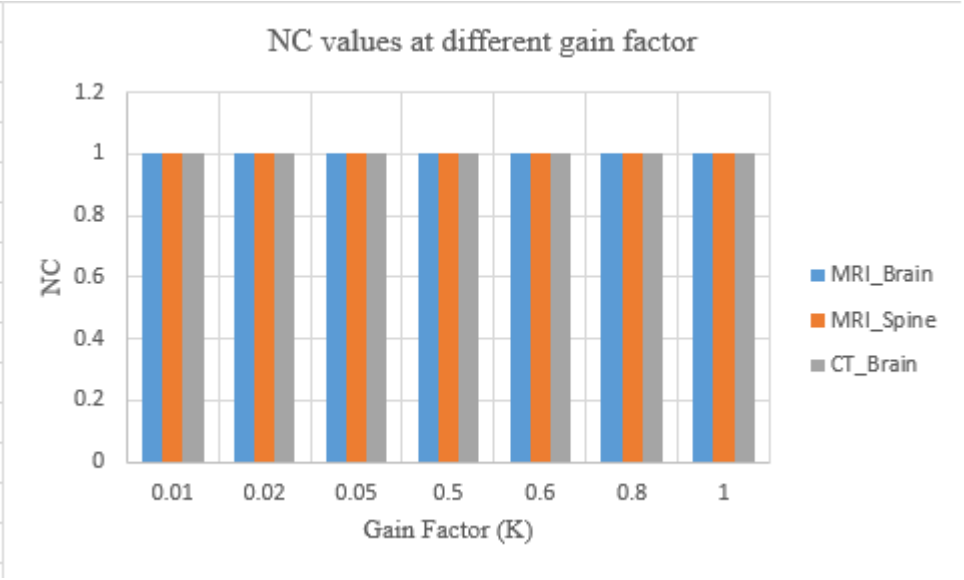


FIGURE 5.5: Variation of NC with gain factor

Table 5.2 shows the PSNR performance obtained by the proposed method without the signal processing attacks.

TABLE 5.2: PSNR evaluation at different gain Factors

Gain Factor (K)	PSNR		
	Images		
	MRI		CT
	Brain	Spine	Brain
0.01	51.833272	51.175099	52.161197
0.02	47.347614	47.475986	48.391136
0.05	38.856662	39.475693	40.040889
0.5	36.420885	37.042364	37.042364
0.6	36.420885	37.042364	37.042364
0.8	36.420885	37.042364	37.042364
1	36.420885	37.042364	37.042364

From the experimental result it is observed that the PSNR value decreases with the increase in gain factor. For Brain MRI image, the PSNR ranges from 36.420885 to 51.833272 at gain factor 1 to 0.01. However, for barin CT-scan images, PSNR value ranges from 37.042364 to 52.161197 at the same gain factors.The graphical representation of variation of PSNR is shown in figure 5.6.

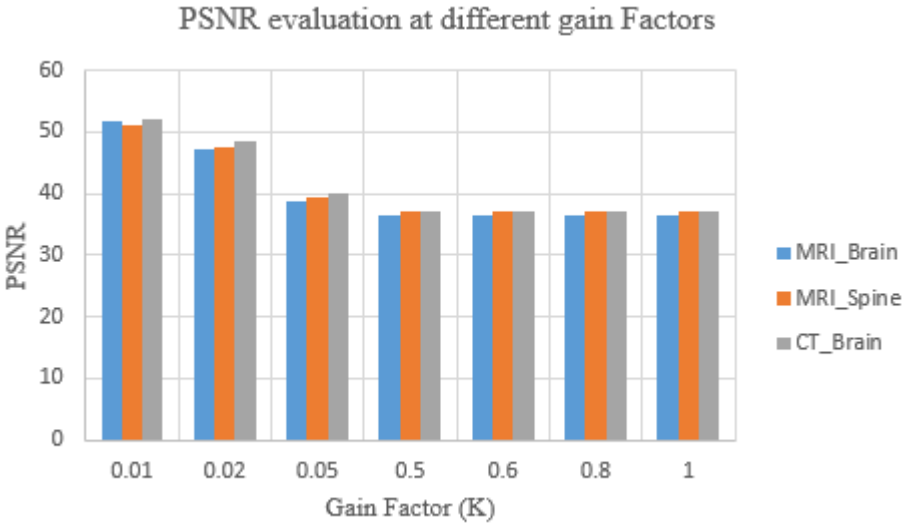
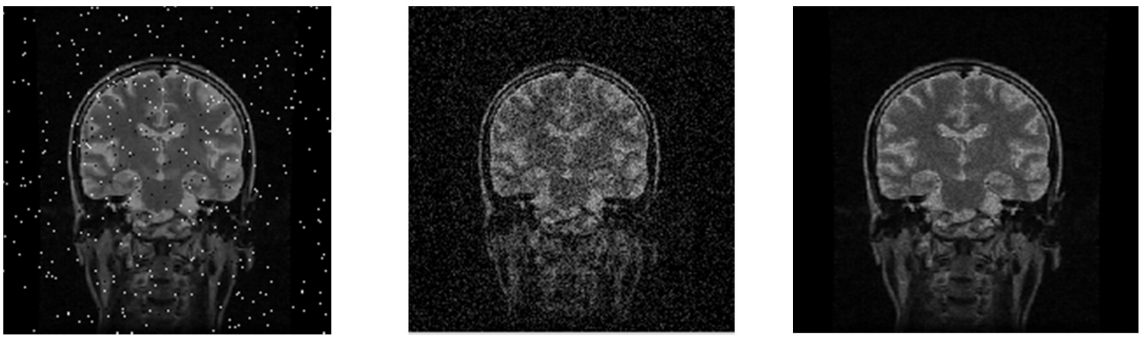


FIGURE 5.6: Variation of PSNR with gain factor(K)

The watermarked images are attacked by the noise at different noise density for salt and pepper noise with varying density, Gaussian noise at different mean (M) and variance(V) and speckle noise at different variance at different gain factors,shown in figure 5.7.

With increase in the noise density NC value decreases but at a higher gain factor NC is high for a particular noise value.The maximum values are obtained at gain factor k=1.Table 5.3 to 5.5 shows the NC values for image watermark 'w1' for different noise attacks at different levels.

Referring to this table it is observed that the proposed method is robust against the different noise attacks at various noise levels. The brain MRI and brain CT scan images are attacked by the different noise at different noise level.The graphical



(a) (b) (c)

FIGURE 5.7: The attacked watermark images by (a)Salt and pepper at density 0.002 (b) Gaussian noise at mean 0.0 and variance 0.01 (c)Speckle noise at variance 0.01

TABLE 5.3: Performance of the proposed method against salt and pepper attack

Noise Level	NC			
	MRI		CT	
	Brain		Brain	
	K=0.8	K=1.0	K=0.8	K=1.0
0.001	0.944050	0.943979	0.949754	0.949720
0.002	0.943998	0.944052	0.949894	0.949848
0.003	0.943979	0.944002	0.949901	0.949768
0.004	0.944012	0.944002	0.949917	0.944062
0.02	0.844708	0.844512	0.850455	0.849575
0.03	0.804794	0.846963	0.850282	0.850856
0.04	0.785314	0.847206	0.850384	0.850884

representation of the variation of NC at different noise levels of salt and pepper noise is shown in figure 5.8.

It is observed that for brain MRI images, the NC value is 0.943979 when watermarked image is attacked by salt and pepper noise at noise level 0.001,indicating the robustness of the image watermark. For Gaussian noise (mean (M) = 0 and variance (V) = 0.00001), the NC value is 0.944097 for brain MRI images and 0.949792 for brain CT images.The graphical variation of NC at different levels of speckle noise is shown in figure 5.9.

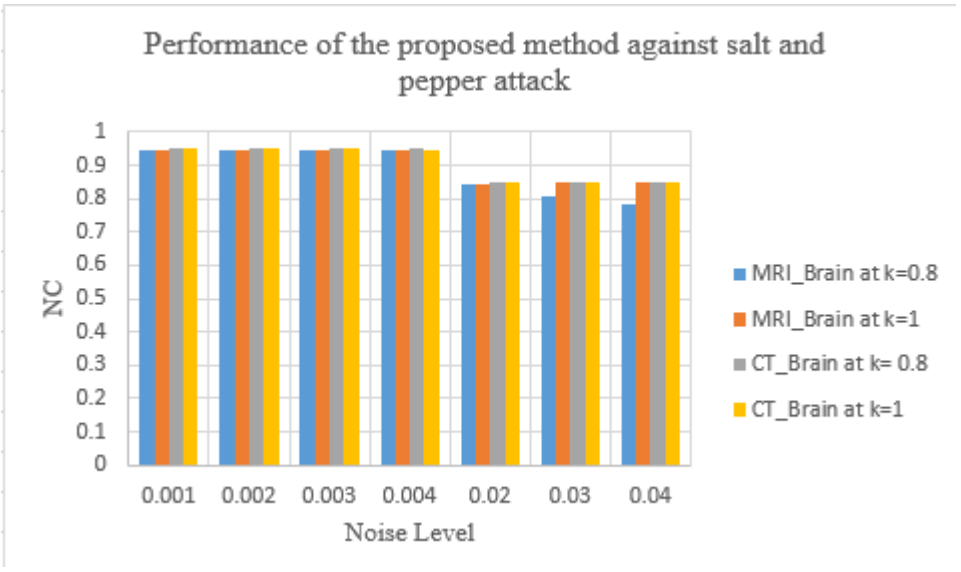


FIGURE 5.8: Variation of NC against different levels of salt and pepper noise

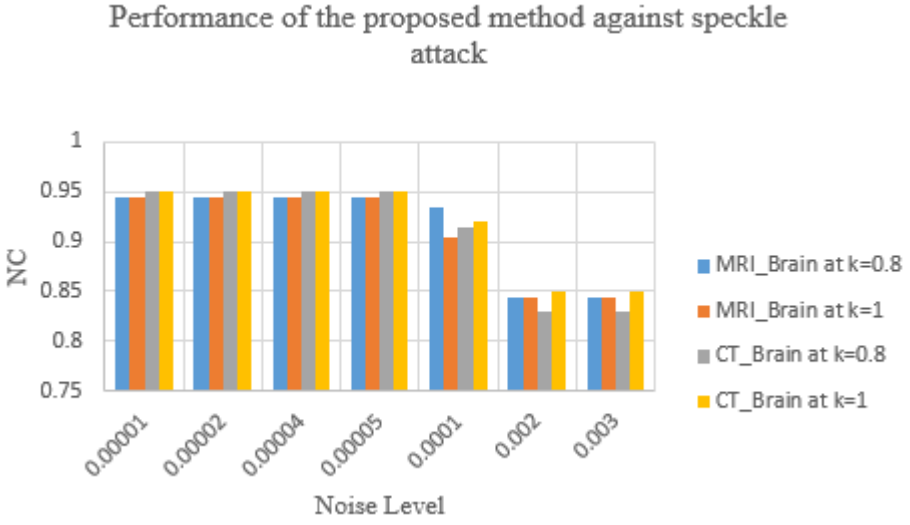


FIGURE 5.9: Variation of NC against different levels of speckle noise

TABLE 5.4: Performance of the proposed method against speckle attack

Noise Level	NC			
	MRI		CT	
	Brain		Brain	
Variance(V)	K=0.8	K=1.0	K=0.8	K=1.0
0.00001	0.943955	0.943955	0.949742	0.949742
0.00002	0.943951	0.943955	0.949742	0.949742
0.00004	0.943945	0.943955	0.949742	0.949742
0.00005	0.943875	0.943955	0.949742	0.949742
0.0001	0.933952	0.903955	0.914215	0.921102
0.002	0.843989	0.843993	0.829739	0.849746
0.003	0.843956	0.843920	0.828963	0.849744

Table 5.6 shows the performance of the proposed method has been evaluated for different signal processing attacks. It is observed from the NC value for MRI images is much better than CT scan images.

TABLE 5.5: Performance of the proposed method against Gaussian noise attack

Noise Level		NC			
		MRI		CT	
		Brain		Brain	
Mean(M)	Variance(V)	K=0.8	K=1.0	K=0.8	K=1.0
0	0.00001	0.944054	0.944097	0.950014	0.949792
0	0.00003	0.944001	0.843944	0.940069	0.949754
0	0.00005	0.943885	0.944097	0.930258	0.920054
0.0001	0.00002	0.844434	0.843744	0.849903	0.849804
0.0001	0.00003	0.844001	0.843909	0.849416	0.849565
0.001	0.00001	0.844109	0.843934	0.849002	0.841361
0.001	0.00002	0.843928	0.844093	0.830312	0.840093

To evaluate the performance of the Text watermark, we calculate bit error rate (BER).The percentage BER at the different gain factors is shown in table 5.7.The graphical representation is shown in figure 5.10 The watermarked NROI image is attacked by the different noise levels of different density. The percentage bit error rate depends on the number of bits changed by attacking the image.The table5.8 to

TABLE 5.6: NC values against different signal processing attacks

Attacks	NC			
	MRI		CT	
	Brain		Brain	
	K=0.8	K=1.0	K=0.8	K=1.0
JPEG Compression (QF=65)	0.949301	0.949301	0.949301	0.949301
Contrast Adjustment	1.000000	1.000000	1.000000	1.000000
Histogram Equalization	1.000000	1.000000	1.000000	1.000000
Gaussian LPF	0.965043	0.965043	0.965043	0.965043
Rotation	0.899266	0.899266	0.899266	0.899266
Cropping	1.000000	1.000000	1.000000	1.000000

5.10 shows the BER(in %) for different noise attacks.The graphical representation of variation of BER (in %) at different noise levels of salt and pepper and speckle noise is shown in figure 5.11 and 5.12 respectively.Table5.11 shows the BER (in %) against different signal processing attacks.

TABLE 5.7: BER (in %)at different gain factor

Gain Factor (K)	BER(in %)		
	Images		
	MRI		CT
	Brain	Spine	Brain
0.01	0.1429	0.1429	0.1429
0.02	0.1507	0.1507	0.1507
0.05	0.1455	0.1455	0.1455
0.5	0.1181	0.1181	0.1181
0.6	0.1293	0.1293	0.1293
0.8	0.1233	0.1233	0.1233
1	0.1563	0.1563	0.1563

To protect the confidential EPR data, it is encrypted using the public key cryptographic algorithms such as RSA. At different value of prime numbers P and Q,

Table 5.8: BER (in %)against salt and pepper noise attacks

Noise Level	BER(in %)			
	MRI		CT	
	Brain		Brain	
	K=0.8	K=1.0	K=0.8	K=1.0
0.001	0.1233	0.1563	0.1259	0.1563
0.002	0.1233	0.1563	0.1233	0.1563
0.003	0.1285	0.1426	0.1233	0.1563
0.004	0.1233	0.1563	0.1233	0.1563
0.02	0.1337	0.1465	0.1398	0.1293
0.03	0.1285	0.1426	0.1354	0.1415
0.04	0.1458	0.1455	0.1233	0.1396

Table 5.9: BER(in %) against Gaussian noise attacks

Noise Level		BER (in %)			
		MRI		CT	
		Brain		Brain	
Mean(M)	Variance(V)	K=0.8	K=1.0	K=0.8	K=1.0
0	0.00001	0.1545	0.1510	0.2630	0.2656
0	0.00003	0.1884	0.1736	0.3264	0.3160
0	0.00005	0.1875	0.2066	0.3264	0.3160
0.0001	0.00002	0.1910	0.1675	0.3481	0.3359
0.0001	0.00003	0.1806	0.1849	0.3160	0.3134
0.001	0.00001	0.1667	0.1675	0.2708	0.2847
0.001	0.00002	0.1823	0.1884	0.3021	0.3342

Table 5.10: BER (in%) against Speckle Noise

Noise Level	BER (in%)			
	MRI		CT	
	Brain		Brain	
Variance(V)	K=0.8	K=1.0	K=0.8	K=1.0
0.00001	0.1276	0.1207	0.1250	0.1357
0.00002	0.1285	0.1302	0.1328	0.1224
0.00004	0.1233	0.1276	0.1285	0.1181
0.00005	0.1293	0.1380	0.1372	0.1285
0.0001	0.1389	0.1267	0.1389	0.1215
0.002	0.1484	0.1311	0.2075	0.1953
0.003	0.1406	0.1293	0.1875	0.2075

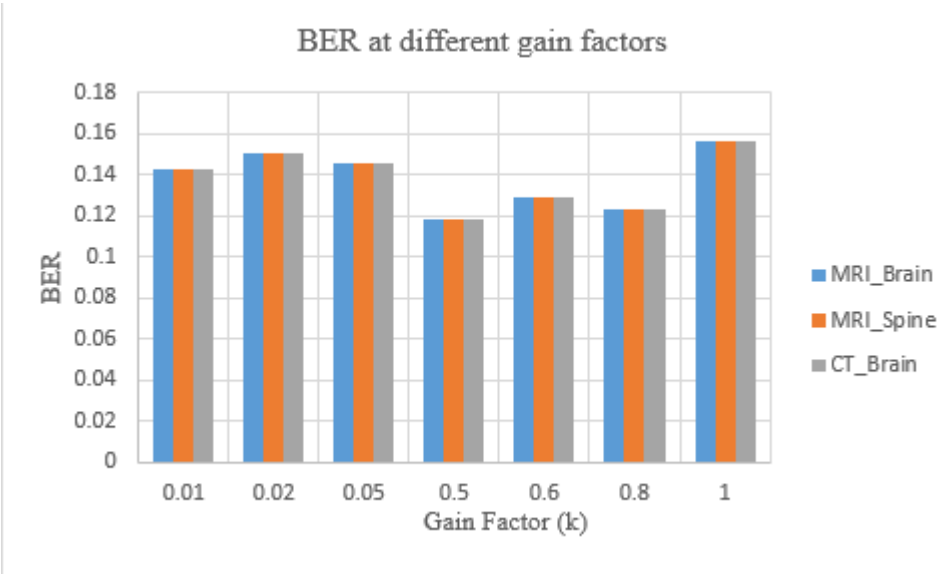


FIGURE 5.10: BER (in %)at different gain factors

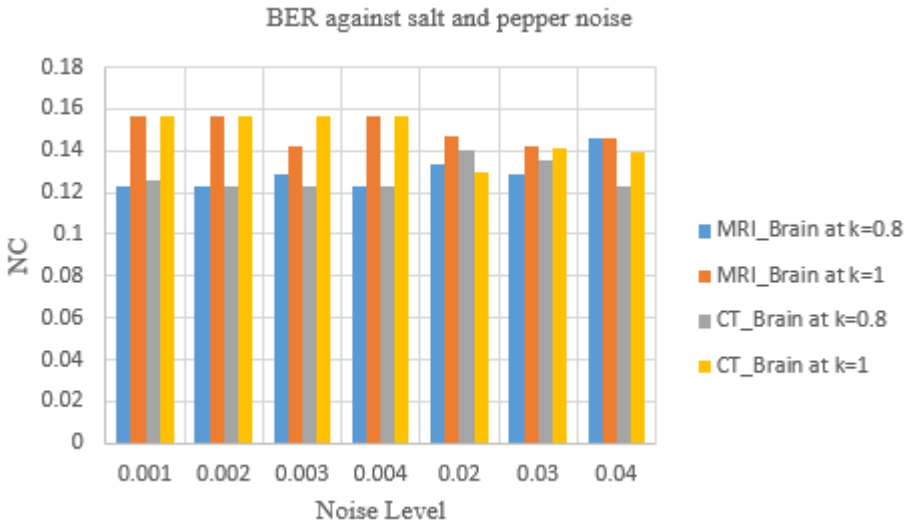


FIGURE 5.11: BER (in %) against salt and pepper noise attacks

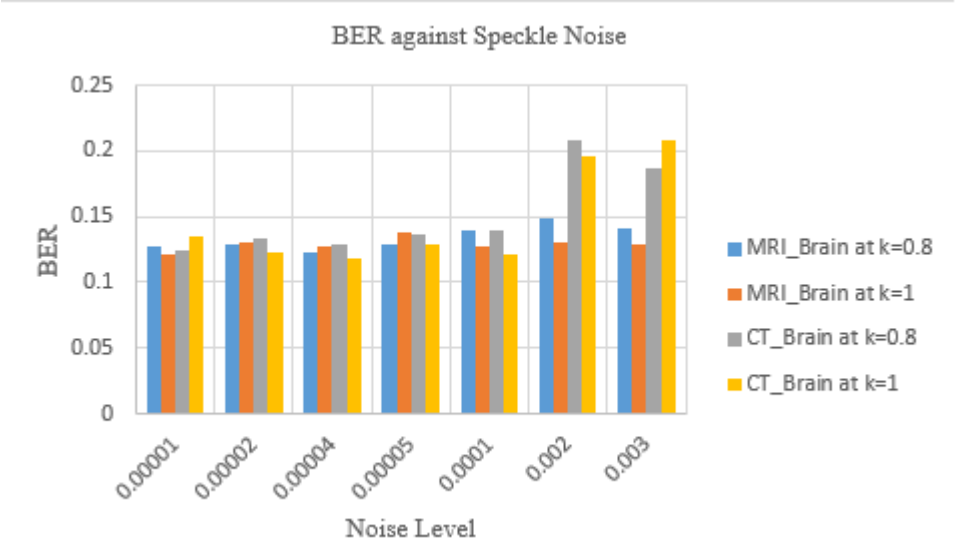


FIGURE 5.12: BER (in%) against Speckle Noise

TABLE 5.11: BER (in%) against different signal processing attacks

Attacks	BER(in %)			
	MRI		CT	
	Brain		Brain	
	K=0.8	K=1.0	K=0.8	K=1.0
JPEG Compression (QF=65)	0.1233	0.1563	0.1233	0.1563
Contrast Adjustment	0.1233	0.1563	0.1233	0.1563
Histogram Equalization	0.1233	0.1563	0.1233	0.1563
Gaussian LPF	0.1233	0.1563	0.1233	0.1563
Rotation	0.1233	0.1563	0.1233	0.1563
Cropping	0.1233	0.1563	0.1233	0.1563

the encryption and decryption time for different EPR text files is evaluated. Table 5.12 shows the encryption and decryption time for different EPR text files is as at different P and Q values.The variation of encryption and decryption time for data files of different size is shown in figure 5.13.

TABLE 5.12: Encryption and decryption time for different texts

P	Q	Encryption time(in sec)		Decryption time (in sec)	
		EPR 1(89 B)	EPR 2(110 B)	EPR 1(89 B)	EPR 2(110 B)
43	47	0.1563	0.1719	0.2500	0.265625
89	97	0.2701	0.2786	0.3700	0.3900
131	113	0.4856	0.4999	0.6066	0.6589

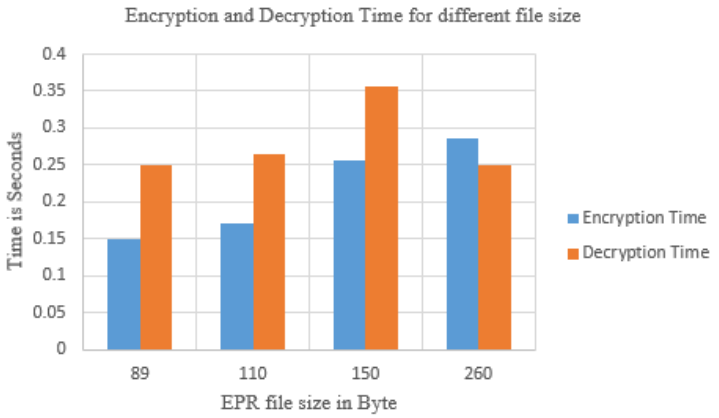


FIGURE 5.13: Encryption and Decryption time variation with different file size

The EPR data is encrypted by using the public key cryptographic method. Due to the limited resource capacity of our experimental setup, we simulated the proposed algorithm on smaller prime numbers. But it can also perform well with large prime numbers. The encryption and decryption time depends on the size of the EPR data file.

5.4 Conclusion

In medical field, the security of EPR data is prime to protect the confidential patient reports from the unauthorized access and unwanted tamper. The medical images shared over the Internet must be protected from malicious attacks. In this paper, the proposed watermarking method based on DWT and DCT. For the identity authentication purpose, the method is used multiple watermarking in the form of text and image. The medical image is taken as cover image, divided into ROI and NROI regions. The more robust and confidential data such as EPR data files are embedded into NROI region and less robust data such as logo is embedded to the ROI region.

The ROI and NROI portion is transformed using second-level DWT. By transforming the watermark image using third-level DWT and then DCT is applied to LL3 sub-band of it.The watermark 'w1' is formed by hashing the image using MD-5.The EPR data is encrypted using the public key cryptographic techniques such as RSA and encoded using the hamming codes.The final watermarked image is encrypted using the bitwise XOR operations to enhance the security of the medical image and data. From the simulated results, it can be concluded that the proposed algorithm is robust against the various signal processing attacks and also have good imperceptibility indicating the high quality of the watermarked image.

CHAPTER 6

CONCLUSION AND FUTURE SCOPE

6.1 Conclusion

The current reliance of the Internet and multimedia technologies merged the medical domain. The sharing of medical information over network makes it important to protect medical information from unauthorized access and disclosure. In medical domain, the security of EPR data is essential to protect confidential patient reports from the unauthorized access and unwanted tamper. The medical images shared over the Internet must be protected from malicious attacks.

In this dissertation, we have proposed an easy to use authentication systems for the content authentication and copyright protection of medical images. The proposed systems namely, ***Encryption Based Medical Image Watermarking, Encrypted EPR Data Hiding Technique And Encrypted EPR Data Hiding Technique Using MD-5***, are proven to be robust according to intensive experiments with various properties.

In ***Encryption Based Medical Image Watermarking***, the watermarking algorithm based on the least significant bit substitution method is used in the

transform domain. The method proposed provides a robust mechanism for watermarking with high invisibility. First -level DWT is used for the transforming the cover and watermark images to transform domain. The LL band is selected from watermark image and formatted using modulus functions. The formatted watermark is embedded in the LL band of the cover image. The watermarked image, then encrypted by using the stream cipher cryptographic techniques. The watermarked images are attacked by different signal processing attacks and the acceptable value of the performance parameters are obtained. The NC values obtained are above 0.819239, showing the robustness of the embedded watermark with PSNR above 66dB, indicating the high imperceptibility.

In ***Encrypted EPR Data Hiding Technique***, the watermarking method based on DWT and DCT. For the identity authentication purpose, the multiple watermarking in the form of text and image. The medical image is taken as cover image, divided into ROI and NROI regions. The ROI and NROI portion is transformed using second-level DWT. By transforming the image using third-level DWT and then DCT is applied to LL3 sub-band of the watermark image to form the watermark 'w1'. The EPR data is encrypted using the public key cryptographic techniques such as RSA. The proposed algorithm is robust against the various signal processing attacks and also have good imperceptibility indicating the high quality of the watermarked image. NC values for image watermark at different gain factors ranging from 0.01 to 1 are values from 0.9314 to 1 and BER for text watermark is 0%, indicate the exact recovery of the embedded text. For Brain MRI image, the PSNR ranges from 40.906702 to 52.743550 at gain factor 1 to 0.02, indicating the high quality of watermarked image.

In ***Encrypted EPR Data Hiding Technique Using MD-5***, the medical images are segmented into ROI and NROI portion. The ROI and NROI is transformed using second-level DWT. By transforming the watermark image using third-level DWT and then DCT is applied to LL3 sub-band of it. The watermark 'w1' is formed by hashing the image using MD-5.The EPR data is encrypted using the public key cryptographic techniques such as RSA and encoded using the hamming codes. The final watermarked image is encrypted using the bitwise

XOR operations to enhance the security of the medical image and data. The proposed algorithm is robust against the various signal processing attacks and also have good imperceptibility indicating the high quality of the watermarked image. NC values for image watermark at different gain factors ranging from 0.01 to 1 is 1, indicating the robustness of the extracted watermark with PSNR value ranges from 37.042364 to 52.161197 at the same gain factors, indicating the imperceptibility of watermarked image. From the experimental results, it can be concluded that the watermarking techniques proposed are robust against the various signal processing attacks such as noise, filtering, cropping, rotation and also have good imperceptibility indicating the high quality of the watermarked image.

6.2 Future Scope

In the emerging fields of computer technologies and reliance of medical field experts on the digital media has boosted the scope of medical image watermarking for secure communication between medical institutions. The work in this dissertation can be extended to the colored and 3-dimentional medical images, using the digital signatures, fingerprinting and Iris patterns of patients as well as experts to authentication purpose.

BIBLIOGRAPHY

[1] H. Munch, U. Englemann, A. Schroter, and H. Meinzer, "The integration of medical images with the patient record and their web based distribution," *Journal of Academic Radiology*, vol. 11, no. 6, pp. 661–668, June 2004.

[2] J. Zain and M. Clarke, "Security in telemedicine: Issues in watermarking medical images," *in Proc 3rd International Conference: Science of Electronic, Technologies of Information and Telecommunications,Tunisia*, 27-31, March 2005.

[3] G. Coatrieux, L. Lecornu, C. Roux, and B. Sankur, "The integration of medical images with the patient record and their web based distribution," *In Proc of 28th Annual International Conference Engineering in Medicine and Biology Society,EMBS '06, New York*, pp. 4691–4694, 30,August-3,September 2006.

[4] D.Bouslimi, G.Coatrieux, M. Cozic, and C. Roux, "A joint encryption/watermarking system for verifying the reliability of medical images:application to echographic images," *Journal of Computer Methods and Programs in Biomedicine*, vol. 106, no. 1, pp. 47–54, April 2012.

[5] G. Coatrieux, H. Maitre, Y. R. B. Sankur, and R. Collorec, "Relevance of watermarking in medical imaging," *in Proc. IEEE conference on Information Technology Applications in Biomedicine Arlington USA*, pp. 250–255, 9-10 November 2006.

[6] W. Pan, G. Coatrieux, N. Cuppens-Boulahia, F. Cuppens, and C.Roux, "Medical image integrity control combining digital signature and lossless watermarking," in *In Data privacy management and autonomous spontaneous security*, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2010, vol. 5939, p. 153–162, ed. Joaquin Garcia-Alfaro,Guillermo Navarro-Arribas,Nora Cuppens-Boulahia and Yves Roudier.

[7] A. Giokoumaki, S.pavlopoulos, and D. Koutsouris, ""secure and efficient health data management through multiple watermarking on medical images",," *Journal of Medical and Biological Engineering and Computing*, vol. 44, no. 8, pp. 619–631, August 2006.

[8] R. Acharya, P. S. Bhat, S. Kumar, and L. C. min, "Transmission and storage of medical images with patient information," *Computers in Biology and Medicine*, vol. 33, no. 4, pp. 303–310, July 2003.

[9] H.-M. Chao, C.-M. Hsu, and S.-G. Miaou, "A data-hiding technique with authentication, integration, and confidentiality for electronic patient records," *IEEE Transactions on Information Technology in Biomedicine*, vol. 6, no. 1, pp. 46–53, March 2002.

[10] L. Kuang, Y. Zhang, and X. Han, "A medical image authentication system based on reversible digital watermarking," *In Proc of 1st International Conference in Information Science and Engineering (ICISE), Nanjing*, pp. 1047 – 1050, 26-28 December 2009.

[11] C. Moumen and malek Benslama, "Cryptography of medical images," *In Proc. of Progress In Electromagnetics Research Symposium, PIERS,Kuala Lumpur*, pp. 42–48, 27-30,March 2012.

[12] A. Lavanya and V. Natarajan, "Watermarking patient data in encrypted medical images," *Sadhana*, vol. 37, no. 6, pp. 723–729, December 2012.

[13] U. Annamalai and Thanushkodik, "Medical image authentication with enhanced watermarking techhnique through visual cryptography," *Journal of*

Theoretical and Applied Information Technology, vol. 57, no. 3, pp. 484–494, November 2013.

[14] A. S. Brar and M. Kaur, "A survey of reversible watermarking techniques for data hiding with roi-tamper detection in medical images," in *In Mobile Communication and Power Engineering*, ser. Communications in Computer and Information Science. Springer Berlin Heidelberg, 2013, vol. 296, pp. 516–522, eds. Amrinder Singh Brar,Mandeep Kaur.

[15] J.M.Zain, A. Fauzi, and A. Aziz, "Clinical evaluation of watermarked medical images," *" In Proc of 28th Annual International Conference of the IEEE Engineering,New York, USA*, p. 5459–5462, 31 August-3 September 2006.

[16] A. Giakoumaki, S. .Pavlopoulos, and D. Koutsouris, "Multiple image watermarking applied to health information management," *IEEE Transactions on Information Technology in Biomedicine*, vol. 10, no. 4, pp. 722 – 732, October 2006.

[17] R.Acharya, D. Anand, S.Bhat, and U.C.Niranjan, "Compact storage of medical images with patient information," *IEEE Transactions on Information Technology and Biomedicine*, vol. 5, no. 4, pp. 320–323, December 2001.

[18] P. Viswanathan and P. Krishna, "Fusion of cryptographic watermarking medical image system with reversible property," in *in Computer Networks and Intelligent Computing*, ser. Communications in Computer and Information Science. Springer Berlin Heidelberg, 2011, vol. 157, pp. 533–540, eds. K. R. Venugopal, L. M. Patnaik.

[19] A. Wakatani, "Digital watermarking for roi medical images by using compressed signature image," *In Proc of the 35th Annual Hawaii International Conference on of System Sciences,HICSS,Hawaii*, pp. 2043–2048, 7-10 January 2002.

[20] G. Coatrieux, C. Quantin, J.Montagner, M.Fassa, F. Allaert, and C. Roux, "Watermarking medical images with anonymous patient identification to verify authenticity," *Studies in Health Technology and Informatics*, vol. 136, pp. 667–672, 2008.

[21] K.A.Navas and M.Sasikumar, "Survey of medical image watermarking algorithms," *In Proc. 4th International Conference on Science: Electronic, Technologies of Information and Telecommunication, Tunisia*, 25-29 March 2007.

[22] X. Guo and TG.Zhuang, "A region-based lossless watermarking scheme for enhancing security of medical data," *Journal of Digital Imaging*, vol. 22, no. 1, pp. 53–64, March 2009.

[23] R. Rodriguez, C. Feregrino, and J.Martinez, "A data-hiding technique with authentication, integration, and confidentiality for electronic patient records," *IEICE TRANSACTIONS on Information and Systems*, vol. 91, no. 3, pp. 862–864, March 2008.

[24] M.Osamah, O.Al-Qershi, and B.E.Khoo, "Authentication and data hiding using a reversible roi-based watermarking scheme for dicom images," *Journal of Digital Imaging*, vol. 24, no. 1, pp. 114–125, February 2011.

[25] J.M.Zain and A. Fauzi, "Medical image watermarking with tamper detection and recovery," *In Proc of 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBS),New York, USA*, pp. 3270–3273, 29-30 August 2006.

[26] A.Giakoumaki, S.Pavlopoulos, and D.Koutouris, "A medical image watermarking scheme based on wavelet transform," *In Proc of the 25th Annual International Conference of the IEEE in Engineering in Medicine and Biology Society,Cancun, Mexico*, vol. 1, pp. 856–859, 17-21 September 2003.

[27] H. Sheikh and A. Bovik, "Image information and visual quality," *IEEE Transactions on Image Processing*, vol. 15, no. 2, pp. 430–444, January 2006.

[28] N. Nikolaidis and I.Pitas, "Digital image watermarking: an overview," *In Proc of IEEE international conference on multimedia computing and systems,Florence*, vol. 6, no. 1, pp. 1–6, 07 June -11 June 1999.

[29] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding – a survey," 1999.

[30] S. P. Mohanty, "Digital watermarking :a tutorial review," *Report:Indian Institute of Science, India*, 1999. [Online]. Available: http://www.csee.usf.edu/~smohanty/research/Reports/WMSurvey1999Mohanty.pdf

[31] L. R. Matheson, S. G. Mitchell, T. G. Shamoon, R. E.Tarjan, and F. Zane, "Robustness and security of digital watermarks," in *In Financial Cryptography*, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 1998, vol. 1465, pp. 227–240, ed. Rafael Hirchfeld.

[32] J. Lacy, S. Quackenbush, A.Reibman, and J. Snyder, "Intellectual property protection systems and digital watermarking," in *in Information Hiding*, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 1998, vol. 1525, pp. 158–168, ed. Jack Lacy, R. Schuyler, Amy Reibman,James H. Snyder.

[33] C. Rey and J. L. Dugelay, "A survey of watermarking algorithm for image authentication," *Journal on Applied Signal Processing*, vol. 6, no. 1, pp. 613–621, January 2002.

[34] A. Cheddad, J. Condell, K. Curran, and P. M. Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, vol. 90, no. 3, pp. 727–752, March 2010.

[35] C. C. Lee, H. C.Wu, C. S. Tsai, and Y. P. Chu, "Adaptive lossless steganographic scheme with centralized difference expansion," *Pattern Recognization*, vol. 41, no. 6, pp. 2097–2106, June 2008.

[36] H. J. Kim, S. Sachnev, Y. Q. Shi, J. Nam, and H.-G. Choo, "A novel difference expansion transform for reversible data embedding," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, pp. 456–465, June 2008.

[37] N. Kaewkamnerd and K. Rao, "Wavelet based image adaptive watermarking scheme," *in IEEE Electronics Letters*, vol. 36, no. 4, pp. 312–313, 17 February 2000.

[38] G.Voyatzis and I.Pitas, "Digital image watermarking using mixing systems," *Computer Graphics*, vol. 22, no. 4, pp. 405–416, August 1998.

[39] S. Mohanty and K. Ramakrishnan, "A dual watermarking technique for images," *In Proc of the 7th ACM International Multimedia Conference,Orlando, FL, USA*, pp. 49–51, October 30 - November 5 1999.

[40] C.W.Tang and H. Hang, "A feature-based robust digital image watermarking scheme," *IEEE TRANSACTIONS ON SIGNAL PROCESSING*, vol. 51, no. 4, pp. 950–959, April 2003.

[41] S. M. Mousavi, A. Naghsh, and S. A. R. Abu-Bakar, "Watermarking techniques used in medical images: a survey," *Journal of Digital Imaging*, vol. 27, no. 6, pp. 714–729, December 2014.

[42] G. Langelaar, I. Setyawan, and R. Lagendijk, "Watermarking digital image and video data:a state-of-the-art overview," *IEEE Signal Processing Magazine*, vol. 17, no. 5, pp. 20–46, September 2000.

[43] C.-T. Hsu and J.-L. Wu, "Hidden digital watermarks in images," *IEEE Transactions on Image Processing*, vol. 8, no. 1, pp. 58–68, August 2002.

[44] T. Le, K. Nguyen, and H. Le, "Literature survey on image watermarking tools, watermark attacks, and benchmarking tools," *In Proc The Second International Conferences on Advances in Multimedia, Athens/Glyfada,Greece,*, pp. 67 – 73, 13-19 June 2010.

[45] J. J. K. O. Ruanaidh and T. Pun, "Rotation, scale and translation invariant spread spectrum digital image watermarking," *Signal Processing*, vol. 66, no. 3, pp. 303–317, May 1998.

[46] A. K. Singh, B. Kumar, M. Dave, and A. Mohan, "Robust and imperceptible dual watermarking for telemedicine applications," *Wireless Personal Communications*, vol. 80, no. 4, pp. 1415–1433, February 2015.

[47] C.Y.Lin, W. M. Bloom, J. U.Cox, M. Miller, and Y. Lui, "Rotation, scale and translation resilient watermarking for images," *IEEE Transactions on Image Processing*, vol. 10, no. 5, pp. 767–782, May 2001.

[48] J. Cox, M. L. Miller, and J. A. Bloom, "Watermarking applications and their properties," *In Proc of International Conference onInformation Technology: Coding and Computing, Las Vegas, NV*, pp. 6–10, 27 March-29 March 2000.

[49] R. Caldelli, F. Filippini, and R. Becarelli, "Reversible watermarking techniques: an overview and a classification," *Journal on Information Security*, vol. 1, no. 2, pp. 1–19, October 2010.

[50] F. Mintzer, G. Braudaway, and M. Yeung, "Effective and ineffective digital watermarks," *In Proc of International Conference on Image Processing, Santa Barbara, CA*, vol. 17, no. 5, p. 9–12, September 1997.

[51] V. Solachidis and L. Pitas, "Circularly symmetric watermark embedding in 2-d dft domain," *IEEE Transactions on Image Processing*, vol. 10, no. 11, pp. 1741–1753, August 2002.

[52] M. Cedillo-Hernandez, F. Garcia-Ugalde, M. Nakano-Miyatake, and H. Perez-Meana, "Robust watermarking method in dft domain for effective management of medical imaging," *Signal, Image and Video Processing*, vol. 9, no. 43, p. 1–16, October 2013.

[53] S. Das and M. K. Kundu, "Hybrid contourlet-dct based robust image watermarking technique applied to medical data management," in *in Pattern*

Recognition and Machine Intelligence, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 1998, vol. 6744, pp. 286–292, ed. Sergei O. Kuznetsov,Deba P. Mandal,Malay K. Kundu,Sankar K. Pal.

[54] J.R.Hernandez, M.Amado, and F.Perez-Gonzalez, "Dct-domain watermarking techniques for still images: detector performance analysis and a new structure," *IEEE Transactions on Image Processing*, vol. 9, no. 1, pp. 55–68, August 2000.

[55] M. Suhail and M. Obaidat, "Digital waternarking based dct and jpeg model," *IEEE Transactions on Instrumentation and Measuremnent*, vol. 52, no. 5, pp. 1640–1647, October 2003.

[56] B.Yang, M.Schmucker, N. XiaMu, C. Busch, and S. Sun, "Reversible image watermarking by histogram modification for integer dct coefficients," *6th IEEE Workshop on Multimedia Signal Processing,Siena, Italy*, vol. 52, no. 5, pp. 143–1467, 29 September-1 October 2004.

[57] M. Long, L. Changjun, and S.Shuni, "Digital watermarking of spectral images using dwt-svd," *In Proc International Conference on Communications, Circuits and Systems,Guilin*, vol. 1, p. 15–18, 25-28,June 2006.

[58] G.S.Kalra, R. Talwar, and H.Sadawarti, "Robust blind digital image watermarking using dwt and dual encryption technique," *In Proc of Third International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN),Bali*, p. 225–230, 26-28 July 2011.

[59] M.R.Keyvanpour and F.Merrikh-Bayat, "Robust blind digital image watermarking using dwt and dual encryption technique," *World Conference on Information Technology*, vol. 3, p. 238–242, 2011.

[60] M.T.Rodriguez-Sahagun and J. Mercado-Sanchez, "Image encryption using jacobi function," *In Proc of International Conference on Mechatronics, Electronics and Automotive Engineering (ICMEAE),Morelos*, pp. 109 – 114, 19-22 November 2013.

[61] A. S. Rajput, N. Mishra, and S. Sharma, "Towards the growth of image encryption and authentication schemes," *In Proc of International Conference on Advances in Computing, Communication and Informatics,Mysore*, pp. 454 – 459, 22-25 August 2013.

[62] Z. Rui-mei, W. Mei, and H. B.-N. Hua, "Digital watermarking algorithm based on wavelet transform," *In Proc of 3rd International Symposium on Intelligent Information Technoology Application,*, pp. 454 – 459, 21-22, December 2008.

[63] B. Nassiri, R.Latif, and A. Toumanari, "Secure transmission of medical images by watermarking technique," *In Proc of International Conference on Complex Systems (ICCS),Agadir*, pp. 1 – 5, 5-6 November 2012.

[64] Y. Zaz and L. E. Fadil, "Enhanced epr data protection using cryptography and digital watermarking," *In Proc of International Conference on Multimedia Computing and Systems (ICMCS),Ouarzazate*, pp. 1 – 5, 7-9 April 2011.

[65] H. Hui-fen, "Dwt digital watermarking algorithm based on one way hashing function," *Advances in Information Sciences and Services*, pp. 1 – 5, 7-9 April 2011.

[66] A. kannammal and S. S. Rani, "Two level security for medical images using watermarking/encryption algorithms," *International Journal of Imaging Systems and Technology*, vol. 24, no. 1, pp. 111–120, March 2014.

[67] K. A. Navas, S. A. Thampy, and M. Sasikumar, "Epr hiding in medical images for telemedicine," *In Proc. of the World Academy of Science, Engineering and Technology, Rome*, vol. 2, pp. 292–295, 20 February 2008.

[68] A. Nakhaie and S. Shokouhi, "No reference medical image quality measurement based on spread spectrum and discrete wavelet transform using roi processing," *In Proc 24th Canadian Conference on Electrical and Computer Engineering (CCECE), Niagara Falls*, pp. 121–125, 8-11 May 2011.

[69] R. Raul, F. Claudia, and G. Trinidad, "Data hiding scheme for medical images," *In Proc 17th International Conference on Electronics, Communications and Computers, CONIELECOMP '07,Cholula, Puebla*, pp. 32–37, 26-28 Febuarary 2007.

[70] N. Memon and S. Gilani, "Data hiding scheme for medical images," *In Proc IEEE International Multitopic Conference,INMIC 2008,Karachi*, pp. 106 – 110, 23-24 December 2008.