DEVELOPMENT OF EFFICIENT WATERMARKING TECHNIQUES IN MEDICAL IMAGES

Thesis submitted
for the award of the degree of

Doctor of Philosophy

submitted by

Roopam Bamal
(Registration No. 901411008)

Under the Supervision of

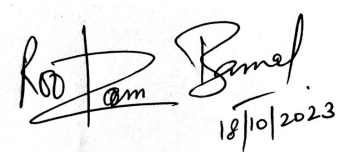
Dr. Singara Singh Kasana
Professor
Central University of Haryana

Computer Science and Engineering Department
Thapar Institute of Engineering and Technology
Patiala - 147004, India
July, 2023

Certificate

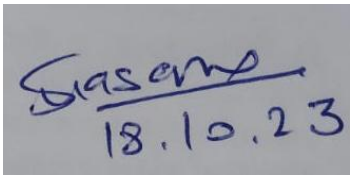
I hereby declare that the work presented in the thesis entitled **"Development of Efficient Watermarking Techniques in Medical Images"** in partial fulfillment of the requirements for the award of the Degree of **Doctor of Philosophy** and submitted in the Computer Science and Engineering Department of the Thapar Institute Of Engineering and Technology Patiala is an authentic record of my own work carried out during a period from 2016 to 2023 under the supervision of **Prof. Singara Singh Kasana**, Computer Science and Information Technology Department of the Central University of Haryana, Mahendergarh, Haryana.

The matter presented in this thesis has not been submitted by me for the award of any other degree of this or any other Institute/University.



(Roopam Bamal)
(Registration No. 901411008)

This is to certify that the above statement made by the candidate is true to the best of our knowledge and belief.



(Dr. Singara Singh Kasana)
Professor,
Department of Computer Science and Information Technology,
Central University of Haryana, Mahendergarh

Place: Patiala

Date: 18.10.2023

Dedicated to Mr. Anil Kumar Bamal and Sujata Devi

Acknowledgements

It is a great pleasure for me to express my respect and deep sense of gratitude to my Ph.D. supervisor Dr. Singara Singh Kasana, Professor, Computer Science and Information Technology Department of Central University of Haryana, Mahendergarh, for his wisdom, vision, expertise, guidance, enthusiastic involvement, and persistent encouragement during the planning and development of this research work. I also gratefully acknowledge his painstaking efforts in thoroughly going through and improving the manuscripts, without which this work could not have been completed.

I am highly obliged to Dr. Shalini Batra, Head of the Department, Computer Science and Engineering Department, Thapar Institute of Engineering and Technology, Patiala, for providing all the facilities, help, and encouragement for carrying out the research work. I am very thankful to Dr. Maninder Singh, Dr. Jitender Khatkar, Dr. Prashant Rana, Dr. Jhilik Bhattacharya and Dr. M. D. Singh for their valuable suggestions, life lessons and recommendations. I also would like to express my deep and sincere thanks to the staff members of Computer Science and Engineering dapartment, Thapar Institute of Engineering and Technology, for helping me either directly or indirectly in all even and odd times.

I am deeply obliged to my finest parents Mr. Anil Kumar Bamal and Mrs. Sujata Devi for their moral support, love, sacrifices, encouragement, and blessings throughout my life. I am especially thankful to my extra-ordinary dear husband Dr. Sunny Singhroha, my loving brother Daniel Bamal and my blissful son Hans Bamal Singhroha for their patience, care, love and encouragement during this journey.

I wish to express my appreciation to the my framily Dr. Sahil Sheokand, Dr. Harpriya Rana, Monika Barak, Subhpreet Shekhon and Dr. Manjeet Singh Shekhon for their help and motivation throughout my research work.

I would also like to extend my special thanks to my larger than life grandfather Late Ch. Sube Singh Numberdar for his dream and vision of sowing the seed in me of being a scientist, since my childhood.

My regards to all the staff members of CSE Department for their timely help and cooperation, extended throughout the course of an investigation. Finally, I am indebted and grateful to the almighty RAM for helping me in this endeavor.

(Roopam Bamal)

Abstract

Watermarking techniques are widely used for copyright protection, confidentiality and integrity issues in medical field. There are various watermarking techniques for hiding crucial patient's data while digital medical image transmission but most lack resistance against many unwanted attacks. There is a greater need for prevention of unauthorized access and tampering of medical may lead to misdiagnosis & wrongful treatment and can also influence the life of a human being. Reversibility, robustness, embedding capacity and invisibility are the essential requirements of a watermarking technique. This research proposes four different robust and reversible watermarking techniques for medical image watermarking.

Cogitating the need of security for medical images, this first technique, proposes a reversible high embedding capacity, high image fidelity, a hybrid robust lossless data hiding technique by using both transform and spatial domains. Proposed technique alters the mean of the selected non-overlapping slantlet transformed blocks of the host image whereas RS vector considers flipping factor for data embedding. The optimum thresholds to select the blocks are calculated through Particle Swarm Optimization (PSO) technique and watermark is generated by using patient details, biometric Identification (ID) and Region Of Interest (ROI) blocks of host image. This watermark is further compressed by applying Lempel-Ziv-Welch (LZW) technique and encrypted by Advanced Encryption Standard (AES) as well as Message Digest Algorithm 5 (MD5). The watermark bits are embedded in all three Red Green Blue (RGB) channels of a cover image, to increase the embedding capacity up to 3.3675 Bit Per Pixel (bpp).

The second proposed technique is a hybrid robust lossless data hiding algorithm that uses the Singular Value Decomposition (SVD) with Fast Walsh Transform (FWT) and Slantlet Transform (SLT) for image authentication. These transforms have good energy compaction with distinct filtering, which leads to higher embedding capacity from 1.8 bit per pixel (bpp) up to 7.5bpp. In this technique, Artificial Neural Network (ANN) is applied for *ROI* detection, and two different watermarks are created. Embedding is done after applying *FWH* by changing the SVD coefficients and by changing the highest coefficients of *SLT* subbands. In dual hybrid embedding, the first watermark is the *ROI*, and the other watermark consists of three parts: patients' personal details, unique biometric *ID*, and the key for encryption.

The third proposed technique focuses on robustness, reversible data hiding with tamper localization, and recovery for medical images. In this technique, Artificial Neural Network (ANN) is used to create a watermark creation by feature extraction, and the medical image is divided into *ROI* and Region of Non-Interest (RONI). Then, hybrid watermarking uses *SLT* and *RS* Vector. Secure Hash Algorithm 3 (SHA-3), *AES*, and *LZW* are used for reliability and confidentiality. Pre-processing is done to reduce the disordered pixels for minimal visual distortion and contrast enhancement. The tampered data recovery of the *ROI* from the watermarked image at the receiver's end is located by the difference matrix between the *ROI* bits after applying ANN and the bits extracted from the background.

The fourth proposed technique is called the Austere Viable Watermarking (AVW) technique. Low energy coefficients of Ridgelet Transform (RT) are used for hiding the watermark bits. AVW unravels three divergent watermarking algorithms for three different usage. Initially, a Unique Identity Document-AVW (UID-AVW) is used for mapping unique patient's information and biometric identification as a watermark with the *ROI*. Then, ROI-AVW is used for embedding in the *RONI* by

modifying the RT coefficient's mean values. Finally, fusion is done with the ratio of mean and variance with respect to threshold through particle swarm optimization for Tamper Detection/Recovery-AVW (TDR-AVW).

The credibility of the proposed techniques in comparison with other medical watermarking techniques is evidenced through experimental results. Experiments are simulated on the proposed techniques by casting numerous attacks for testing the visibility, robustness, security, authenticity, integrity and reversibility. The resultant outcome proves that the watermarked image has an improved imperceptibility with a high level of payload, low time complexity and high Peak Signal to Noise Ratio (PSNR) against the existing approaches. Experimental results demonstrate that in comparison with more than 30 existing articles, the third proposed technique achieves high robustness against more than 20 attacks along with tamper detection and recovery of ROI, preserving the visual quality of the cover image. Fourth proposed technique relinquishes much improved outcome in comparison to more than 30 published techniques in terms of attacks withholding resistance, Normal correlation, Standard deviation error, capacity, $PSNR$, BPP, Structural Similarity Index (SSIM) and execution time.

Contents

List of Publications

Papers Published in SCI Journals

[1] **Roopam Bamal** and Singara Singh Kasana, "Slantlet based hybrid watermarking technique for medical images," ***Multimedia Tools and Applications, Springer*** , Vol. 77,pp. 12493–12518, 2017, Impact Factor=2.577.

[2] **Roopam Bamal** and Singara Singh Kasana, "Dual Hybrid Medical Watermarking using Walsh-Slantlet Transform," ***Multimedia Tools and Applications, Springer*** , Vol. 78,pp. 17899–17927, 2019, Impact Factor=2.577.

[3] **Roopam Bamal** and Singara Singh Kasana, "Reversible Medical Image Watermarking for Tamper Detection using ANN and SLT," ***Multimedia Tools and Applications, Springer*** , Accepted, 2023, Impact Factor=2.577.

[1] **Roopam Bamal** and Singara Singh Kasana, "Reversible Robust Austere Viable Watermarking Medical Images using Ridgelet Transform," ***IEEE transactions on medical imaging*** , Communicated, 2023, Impact Factor=10.6.

List of Figures

List of Tables

List of Acronyms/Abbreviations

2D	Two Dimensional
3D	Three Dimensional
ABC	Artificial Bee Colony
AES	Advanced Encryption Standards
AGN	Additive Gaussian Noise
ANN	Artificial neural networks
AVW	Austere Viable Watermarking
AWGN	Additive white Gaussian Noises
BER	Bit Error Rate
BPP	Bit Per Pixel
C	Capacity
CAD	Computer aided diagnosis
CGR	Chaos Game Representation
CS	compressive sensing
CT	Computed Tomography
CTC	Cascading Trellis Coding
DBWT	Discrete Bi-orthogonal Wavelet Transform
DCT	Discrete cosine transform
DE	Differential Evolution
DES	Data encryption standard
DFT	Discrete Fourier transform
DICOM	Digital Imaging and Communications in Medicine
DOM	distortion oriented minimized
DS	Digital signature
DWT	Discrete Wavelet Transform
EEG	Electroencephalogram

FF	Flipping function
FFT	Fast Fourier Transform
FNN	Forward Neural Network
FPGA	Field Programmable Gate Array
FRAT	Finite Radon Transform
FRIT	Finite Ridgelet Transform
FWT	Fast Walsh Transform
GA	Genetic Algorithm
GP	Genetic Programming (GP)
HCDH	High-Capacity Data-Hiding
HIE	Health Information Exchange
HIPAA	Health Insurance Portability and Accountability Act
HIS	Hospital Information System
ICA	Independent Component Analysis
IER	Image Error Rate
ISLT	Inverse Slantlet Transform
ISO	International Organization for Standardization
ISVD	Inverse Singular Value Decomposition
ITI	Integer-to-Integer
ITI	Information Theoretic Index
IWHT	Inverse Walsh-Hadamard Transform
IWT	Integer Wavelet Transform
JPEG	Joint Photographic Experts Group
LSB	Least significant bit
LZW	Lempel–Ziv–Welch
MAP	Maximum a Posterior
MD5	Message-digest algorithm
MIS	Medical Information System
MLP	Multilayer perceptrons
MNRMSE	Maximum Normalized Root Mean Square Error
MRI	Magnetic Resonance Imaging
MSE	Mean Squared Error
MSSIM	Mean structural similarity

NC	Normalized correlation
NCA	Normal Correlation Average
NCC	Normalized cross correlation coefficient
NRMSE	Normalized root mean square error
PACS	Picture Archiving and Communication Systems
PCG	Phonocardiogram
PE	Prediction errors
PSNR	Peak Signal-to-Noise Ratio
PSA	Particle Swarm algorithm
PSO	Particle Swarm Optimization
RDH	Reversible data hiding
RDM	recursive dither modulation
RG	Regular group
RGB	Red Green Blue
ROI	Region of Interest
RONI	Region of Non-Interest
RT	Ridgelet Transform
SAW	Strict Authentication Watermarking
SD Error	Standard deviation error
SG	Singular group
SHA	Secure Hash Algorithm
SIM	Similarity Index Metric
SLT	Slantlet Transform
SNR	Signal-to-Noise Ratio
SOM	Self-organizing map
SSIM	The structural similarity
SVD	Singular Value Decomposition
TDR	Tamper Detection and Recovery
THM	Tent-Henon-Map

UG	Unused group
UID	Unique Identity Document
US	Ultrasonic
VLSI	Very Large Scale Integration
WHT	Walsh-Hadamard Transform

List of Symbols

μ_p	The average of p
μ_q	The average of q
σ_p^2	The variance of p
σ_q^2	The variance of q
σ_{pq}	The covariance of p and q
L	The dynamic range of the pixel values
V_i^k	The velocity of agent i at iteration k
w	Weighting function
c_j	Weighting factor
$rand$	Uniformly distributed random number between 0 and 1
s_i^k	Current position of agent i at iteration k
$pbest_i$	pbest of agent i
T	Threshold
μ^{LH}	The mean values of the slantlet transformation coefficients in LH subband
μ^{HL}	The mean values of the slantlet transformation coefficients in HL subband
w_j	Watermark bit
Th	Threshold calculated with PSO
x_i	The value of the pixel
Iw	The watermarked image before pixel adjustment
$Iw\ (i,\ j)$	The modified pixel value
w_j^*	The extracted bit
μ_{new}^{HL}	Watermarked mean values of the slantlet transformation coefficients in HL subband
μ_{new}^{LH}	Watermarked mean values of the slantlet transformation coefficients in LH subband.
H	Hadamard matrix
H^T	Transpose of Hadamard matrix
$H*$	Conjugate Hadamard matrix
H^{-1}	The inverse Hadamard matrix
Y	Spectrum vector
y	Signal vector

$WHT(y)$	The forward of WHT_h
$IWHT(Y)$	The inverse of WHT_h
H_w	The Walsh ordered matrix
N_i	The i-th bit in the binary representation of N
net_j	The level of internal activity of a neuron
x_i	The input signal
y_j	The output signal
$\varphi()$	The activation function
nb_i	The block number
T_i	The position of the onlooker bee
t	The iteration number
q_k	The randomly chosen employed bee
p	A series of random variable in the range
j	The dimension of a block
r	A random number between 0 and 1
A	The highest coefficient of a block before applying SLT
$A^{'}$	The highest coefficient of a block after applying SLT
A_1	The mean of a block
A_2	The standard deviation of a block
A_w	The modified highest coefficient of each block
OU_w	The watermarked image before pixel adjustment
$OU_w^{'}$	The modified pixel value after pixel adjustment
$A^{'''}$	The $ISLT$ coefficient of A
$W_2^{''}$	The recovered watermark
Vel_i^k	The velocity of an agent i at iteration k
$pbests_i$	$pbest$ of agent i represents the best position found by agent i up to the current iteration
we	Weighting function
d_j	Weighting factor
r_i^k	The current position of agent i at iteration k
$randm$	Uniformly distributed random number that can take any value between 0 and 1 with equal probability

$gbests$	The global best position found by any particle in the swarm
ϕ	The ratio between each block's mean and standard deviation
w_j^*	The extracted bit
$\rho^{HL}new$	The pixel values of the slantlet transformation coefficients in the sub-band HL
$\rho^{LH}new$	The pixel values of the slantlet transformation coefficients in the sub-band LH
$\phi^{'}$	Difference between the ϕ value of the original image and watermarked image
$W(k,l)$	Pixel value of the watermarked image at position (k,l)
$C(k,l)$	Pixel value of the corresponding position in the cover image
h	The height of an image
w	The width of an image
r_i^k	The current position of agent i at iteration k
Px_{xy}	The set of indices of all the lines that go through a point (x,y)
ϑ	The highest coefficients of each block before applying the ridgelet transform
$\vartheta^{'}$	The highest coefficients of each block after applying the ridgelet transform
ϑ_W	The modified highest coefficient of each block
η	The pseudo-random number sequence used to implant watermark bits
$W_{tech2}^{''}$	The recovered watermark
Weg	The weighted value of R
$\vartheta^{'''}$	The inverse ridgelet coefficient
$H_{\triangle}$	The hash value of a watermark

Chapter 1

Introduction

1.1 Watermarking

Information superhighway, commonly referred as Internet, shares data among millions of users. With the rapid growth in Internet technology, computational power, medical imaging applications and multimedia; security and integrity of the data has become an important concern. Every person connected to the Internet today, is hugely dependent on the use of multimedia. Multimedia is used in every aspect ranging from health, communication, business, education, information, *etc.* As multimedia data can be accessed easily over the Internet, it poses a danger of being modified or tampered easily using image processing tools. Thus making it vulnerable to attacks like tampering, compression, geometric, encryption attacks. So, protection of intellectual property rights, private information, authentication and content have become an important issue. Protecting sensitive data and its confidentiality is a top priority, which is achieved through three primary techniques: Cryptography, Steganography, and Watermarking. These techniques serve different purposes in protecting digital data.

1. **Cryptography** deals with the security of the digital content. It encrypts and decrypts the data by using a key. There are a lot of cryptographic algorithms for three basic types of cryptography, called secret key, public key and hash function. It is very commonly used because of its efficient algorithms and trust models.

2. **Steganography** is a technique with a long history, dating back to the use of invisible ink by spies during revolutionary wars. It is highly practiced today as well, by the government for military purposes. Steganography involves hiding a secret message within a cover image or file. Hackers are also using this technique to smuggle malicious payloads and trick web users to pass the firewalls and security scanners.

3. **Watermarking** is an effective method utilized to guarantee the genuineness, privacy, and consistency of digital information. It entails the insertion of a concealed mark or signature within a resilient signal, such as images, audios, or video data. Digital watermarking presents numerous benefits, including the identification of copyrighted material ownership, source tracking, tracking of broadcasted content (e.g., watermarked videos by international news agencies), and clandestine communication (Thodi and Rodríguez (2007)).

1.2 Digital Watermarking

Digital watermarking is a method employed to incorporate a unique and frequently indiscernible mark or pattern onto digital or physical media content. It is a technology that is commonly used to protect digital media such as audio images, and videos Thabit and Khoo (2014). It is categorized

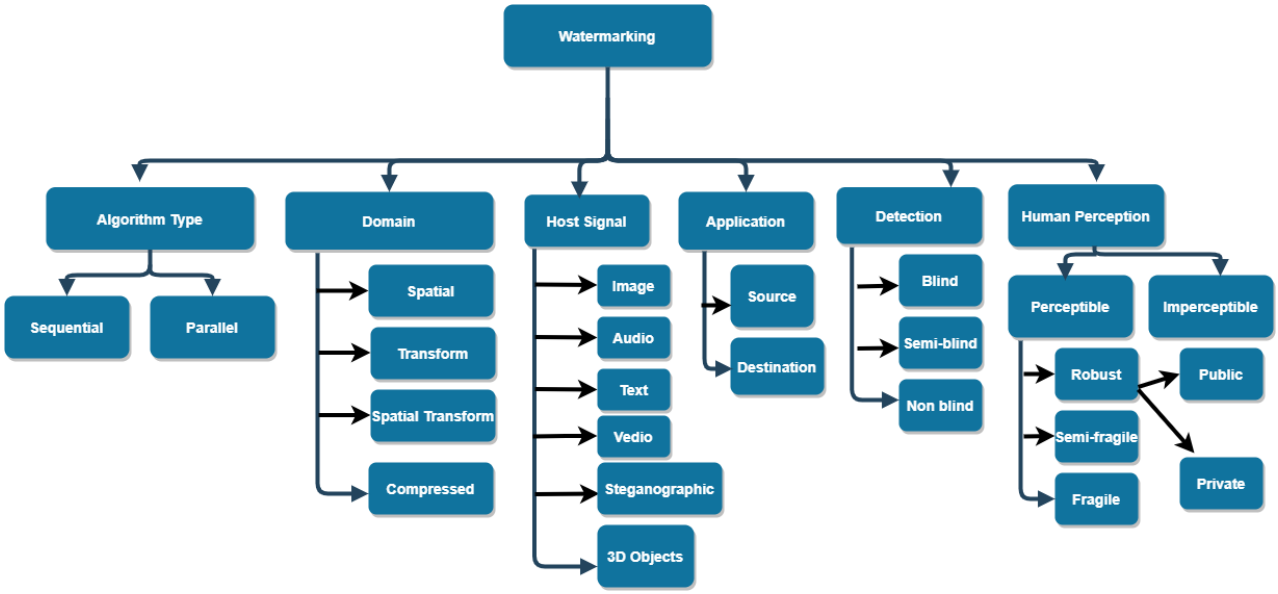


Figure 1.1: Classification of watermarking.

into various types, as depicted in Figure 1.1. The watermarking process involves two main types of algorithms:

1. **Sequential Algorithms**: Serial algorithms are executed in a sequential manner, from beginning to end, without any other processing executing simultaneously. This is in contrast to concurrent or parallel algorithms, with most traditional computer algorithms being sequential by default. The term "sequential algorithm" is not typically used to describe standard algorithms, as it is an implicit assumption.

2. **Parallel Algorithms**: Parallel algorithms are specifically developed to carry out multiple tasks concurrently. They provide benefits like instantaneous problem-solving, cost-effectiveness, and scalability. The overall execution time of a parallel algorithm, when multiplied by the number of processors, approaches the runtime of the most efficient known sequential algorithm. Nonetheless, parallel algorithms do have certain constraints. These include the necessity for an infinite number of processors, each equipped with unrestricted local memory, possessing a unique Identification (ID), and capable of accessing shared memory in constant time. Additionally, parallel algorithms require unlimited shared memory for processing.

Domains in which watermark is embedded effects the whole embedding algorithm. It means that the watermarking algorithm is applied on which level of the following:

1. **Spatial domain based watermarking**: Spatial domain watermarking techniques directly add watermark bits to the pixels of the cover image, making them easy to mathematically model and analyze (Zain and Fauzi (2006)). However, these methods are vulnerable to various signal processing attacks, including filtering, cropping, and histogram equalization, which can destroy or remove the embedded watermark. Additionally, the use of human visual systems in spatial domain techniques makes them sensitive to image scale and requires repeated embedding of the same information at different locations in the host image. One example of a spatial domain technique is the least significant bit (LSB) method, which embeds the watermark in the least significant bits of the cover image.

2. **Watermarking in the Transform Domain**: In transform domain-based watermarking, the watermark bits are inserted into a cover image after it has undergone a specific transformation, such as discrete wavelets, discrete cosines, hardmard, ridgelets, etc. These transformations divide the cover image into different frequency bands, allowing the selection of a particular low-energy or high-energy band for the embedding process (Wu et al. (2008)). Performing watermarking in the frequency domain can enhance the resilience and imperceptibility of watermarked images by distributing the watermark coefficients throughout the entire image. This approach offers improved resistance against compression and filtering attacks. In the frequency domain, the watermark is embedded by modifying the image coefficients using image transforms. Masking techniques based on the transform domain are more robust compared to the *LSB* method, particularly in terms of resistance to cropping, compression, and image processing. The key advantage of masking techniques is their ability to embed watermark coefficients in large areas of the host image. Many of these transform coefficients are small, so even if they are discarded during compression, the impact is negligible. A comprehensive review of wavelet-based image watermarking techniques by Singh et al. (2014) examines their robustness, imperceptibility, capacity, and security. The study analyzes embedding and extraction methods, discussing their advantages and disadvantages while addressing research challenges and requirements to enhance the efficiency of watermarking systems. The findings underscore the importance of implementing effective watermarking methods for researchers in the field of information security.

3. **Hybrid Domain-Based Watermarking**: Hybrid domain-based watermarking refers to the utilization of both spatial domain and transform domain techniques simultaneously. Spatial domain techniques are characterized by lower complexity and high payload capacity (Bamal and Kasana (2018)). However, they are vulnerable to low-pass filtering and common image attacks. In contrast, transform domain techniques involve modifying the transform coefficients instead of pixel values. The watermark detection process involves performing an inverse transform. By combining these two domains, hybrid watermarking approaches aim to achieve a balance between robustness and payload capacity.

4. **Compressed based watermarking**: Compressed-based watermarking is a technique used to embed watermarks directly into the compressed version of media content, such as images or videos. It addresses the need for efficient and effective watermarking in scenarios where the media content is compressed, such as in streaming services, online platforms, and storage with limited capacity.

   One example of compressed-based watermarking is Joint Photographic Experts Group (JPEG)-based watermarking. *JPEG* is a widely used image compression standard, and embedding watermarks directly into the compressed *JPEG* data stream offers advantages in terms of efficiency and compatibility. Watermarks can be inserted by modifying the quantized Discrete Cosine Transform (DCT) coefficients or by exploiting the unused bits in the compressed *JPEG* file. This allows for the seamless integration of watermarks without the need for full decompression and recompression. Watermark signal into the obtained *DCT* values. This watermark bits embedded after compression of the original cover image by using various compression techniques like speech waveform. This compression can be performed in the frequency domain or in the spatial doamin, depending on the techniques and algorithm type (Shih and Wu (2005)).

1.2.1 Human Perception for Watermarking

1. **Perceptible**: Perceptible watermarks are a type of watermark that involve overlaying a secondary, translucent image on top of the primary image (Arsalan et al. (2017)). This technique is similar to the traditional method of stamping bond paper with an identifying pattern to alter the paper's opacity. Perceptible watermarks are commonly used for logos and are only applicable to images. They are typically inlaid into the image and have a transparent appearance. Unlike other types of watermarks, perceptible watermarks cannot be easily removed by cropping the center part of the image, and they are designed to be resistant to statistical analysis attacks.

   (a) **Robust**: A medical watermarking scheme is commonly used to embed copyright information in digital works, providing robustness against common editing processes and various attacks.

      i. **Public**: In watermarking, it is possible to extend the encoder by using secret or public keys and other parameters. The effectiveness of a watermarking technique can be measured by its ability to withstand severe distortions and attacks without being destroyed. If the watermark can survive even under such conditions, it is considered to be robust.

      ii. **Private**: Robust medical watermarking using secret key on the host signal. It is most reliable and secure technique.

      iii. **Invertible**: An invertible medical watermarking scheme is a type of invisible robust watermarking scheme that can be attacked by creating a counterfeit original.

   (b) **Fragile**: Fragile watermarking is a type of watermarking technique that is primarily used for ensuring the integrity of digital content Zain and Fauzi (2006). It is highly sensitive to any changes in the signal, and can easily detect any tampering that may have occurred. For instance, invisible watermarking can be used to ensure the trustworthiness of digital cameras. In this case, images are captured using a digital camera and later used in news articles. Additionally, invisible watermarking can be used to detect alterations in images stored in digital libraries Chiang et al. (2008). For instance, images such as human fingerprints can be scanned and stored in digital libraries, and the content owner may desire the ability to detect any changes made to the images without having to compare them to the scanned materials.

   (c) **Semi Fragile**: Semi-fragile watermarking is a technique that allows for some level of modification to a watermarked image, such as the introduction of quantization noise or compression attacks, while still being able to detect more significant changes Wu et al. (2008).

2. **Imperceptible**: Imperceptible watermarks are used to hide information in a document without the end user being aware of it. When the imperceptible watermark itself contains data, it is referred to as data hiding. If the imperceptible watermark is unknown to the end user, it is considered steganographic. These watermarks are commonly utilized to track the origin of images, documents, or videos and their rightful owners.

Classification of watermarks based on host signals are as image, audio, text, video, steganographic and 3 Dimensional (D) objects. An image watermark can be a logo, graphic, or pattern that is

overlaid on top of an image. For instance, an artist may embed their signature or a small logo in the corner of their artwork. Audio watermarks can be imperceptible sounds or signals embedded within an audio file. These watermarks are designed to be undetectable by human ears but can be extracted using specialized algorithms. Audio watermarking is commonly used for copyright protection in the music industry. A text watermark can be a copyright notice or the creator's name overlaid on an image. It may appear as semi-transparent text at the bottom or corner of the image. Video watermarks can be overlaid on top of video frames as visible watermarks or embedded as invisible watermarks within the video content. A common example is a television channel logo displayed in a corner of the screen during a broadcast. Steganographic watermarking hides information within the media content itself. For example, a text watermark can be embedded by slightly modifying the *LSB*s of the pixel values in an image or video frame.

1.2.2 Components of Digital Watermarking

Digital watermarking is a technology utilized for safeguarding digital media, including video, audio, and images Alattar (2004), by embedding a watermark, which is secret information, into the digital media using specific algorithms. The watermarked media is then processed, and the watermark can be extracted using the particular algorithm. The purpose of digital watermarking is to authenticate data and protect copyright Arsalan et al. (2017). The process of digital watermarking comprises two phases, namely, embedding the watermark and detecting and extracting the watermark.

Figure 1.2 shows the working of a digital watermarking system, here

1. Cover image: The carrier image in which watermark is embedded.
2. Watermark: It is the signature or identification mark, which needs to be embedded for the ownership purposes.
3. Watermark key: It is the key used to embed the watermark into the cover image with a watermarking algorithm. Unique key makes the watermark more secure.
4. Watermarked image: It is the output image after embedding the watermark into the cover image.
5. Noise/Attacks: These are the unwanted signals which will corrupt the watermarked image. It is then, very difficult to retrieve the watermark, as it can be tempered.
6. Noisy watermarked image: It is the image watermarked image along with the noise and attacks.
7. Watermark detector: It is the receiver's side watermark extraction application. It takes the noisy watermarked image and watermarked key as input and provides with the watermark as output.

1.3 Medical Image Watermarking

In today's corporate world, the transmission of digital data through the Internet has become crucial, involving various forms such as audio, images, files, documents, and videos. However, during this transmission process, digital data can encounter obstacles like data corruption, integrity issues, loss of confidentiality, and unauthorized access. It is imperative to protect and control sensitive

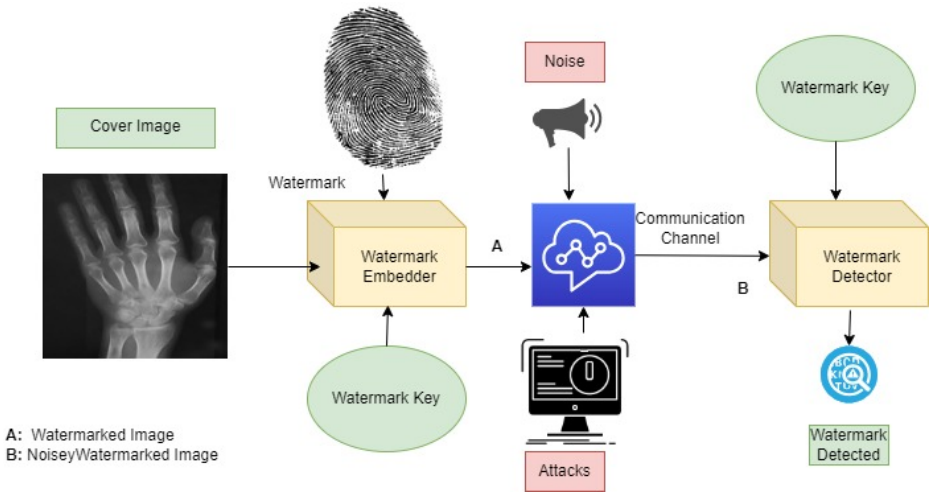


Figure 1.2: Digital Watermarking System.

data to ensure its confidentiality and prevent tampering. This issue is particularly prevalent in medical images, which serve as vital visual representations for clinical purposes. Any corruption or alteration of information stored in medical images can significantly impact a person's life. To address this concern, there is a growing need for highly secure, robust, and reliable techniques that can effectively prevent falsification and corruption of clinically relevant data. Electronic Medical Information Systems (MIS) and Hospital Information Systems (HIS) are widely used to manage healthcare organizations, while medical images are often exchanged through computer networks or the Internet. Medical images play a crucial role in diagnostic procedures, allowing physicians to evaluate patient conditions, monitor treatment effects, and conduct disease research. Consequently, safeguarding medical images from unauthorized access is an essential requirement in this field.

A comprehensive exploration of bioelectronics and its potential in healthcare is presented in the study by Srivastava and Khari (2021). The research discusses various technologies utilized in bioelectronics, highlighting their applications in healthcare, such as diagnostic tools, therapeutic devices, implantable sensors, and neural interfaces. The paper also addresses the challenges faced in the field and offers insights into future prospects, underscoring the positive impact of bioelectronics on enhancing healthcare outcomes.

Several techniques play a significant role in ensuring the security of digital data, including steganography and watermarking. Steganography involves concealing secret data within other data, while watermarking is a technique used to hide information within carrier data for purposes such as confidentiality, security, copyright protection, and ownership verification. The embedded digital information is typically imperceptible to humans but can be detected by computers, web networks, and various digital devices like printers and scanners. Therefore, it is essential to have a highly reliable watermarking technique that can withstand such attacks. In the case of medical images, a watermark can consist of patient information, such as their *ID* or even their unique biometric identity, combined with the image's hash value. This watermark can be embedded within the medical image without corrupting it, and the original image, along with the watermark, can be retrieved at the receiver's side. The relevance of watermarking in medical images is discussed by Coatrieux et al. (2000), who present different scenarios focusing on authentication, integrity, and traceability of the images while maintaining control of patient records. Their approach enables the reconstruction of the original image while preserving its authenticity. In the realm of telemedicine

security, Zain and Clarke (2005) propose a method that enhances security by examining attacks against security within the context of a computer system functioning as an information portal. They address concerns related to watermarked medical images, including reversible watermarking versus permanent/irreversible watermarking, content authentication versus complete authentication, and the practical issue of compression.

There are generally two regions in which medical images are divided. The part which is considered important is the Region of Interest (ROI) part. The other part is called Region of Non-interest (RONI) as shown in figure 1.3. Data hiding techniques are generally used for watermarking *ROI* part of the image. To avoid misdiagnosis while recovering original image, tamper detection in *ROI* is executed. Recovery data for *ROI* is generally embedded in *RONI*. This is done, if tamper is detected inside *ROI*, then it is replaced with recovery data from *RONI*. Tamper localization, tamper detection and recovering tamper region capable watermarking techniques have been proposed. In tamper localization techniques, tamper is detected on modified pixel values in the image. From the watermark area inside the image, the original pixel values can be stored for the detected tampered area. This technique is useful in deriving the need of tamper whether it is real or not. Based on Jasni's scheme Zain and Fauzi (2006), tamper localization, watermarking and recovery is done in *ROI*. The article by Wakatani (2002) suggests a technique for preserving signature information in the non-*ROI* region of an image in order to prevent any alteration of the image data within the *ROI*. A lossless algorithm is utilized to compress the *ROI* without losing any information, while the signature information is produced using a progressive coding algorithm. The results show that the signature image can be detected even from the clipped image, which contains *ROI* area or only a part of it. Lin and Otoya (2022) presents a novel approach for pose-invariant face recognition, addressing challenges related to face pose, illumination, and facial expression. The proposed method incorporates a large pose detector and feature descriptors, achieving impressive results on the *CMU-PIE* database. The combination of large pose detection and feature-based recognition models significantly enhances accuracy for faces with pose angles ranging from -90° to $+90^\circ$. This approach holds promise for applications requiring robust face recognition in varying conditions.

Tamper detection and recovery in medical image watermarking focuses on enhancing the security and integrity of medical images by embedding robust watermarks that can detect and localize any tampering attempts. Through advanced watermarking techniques, such as robust feature-based or transform-based methods, the embedded watermarks can be utilized to detect unauthorized modifications or tampering in the medical images. In case of tampering, the recovery mechanism enables the restoration of the original content, ensuring the accuracy and reliability of the medical image data for critical healthcare applications.Lin et al. (2006) presents a novel image watermarking scheme that incorporates tamper detection and recovery capabilities. The proposed method accurately detects and recovers tampered regions while being robust against *JPEG* compression and cropping attacks. It offers the advantage of both tamper detection/recovery and robust watermarking, providing an efficient solution for verifying ownership and restoring tampered regions in images. Experimental results validate the effectiveness of the proposed technique.

1.3.1 Need of Medical Image Watermarking

Images can be accessed electronically with the advancement in technology. Corruption of medical images may lead to wrong diagnosis & treatment and can affect the life of a person. Thus, security of medical images is essentially important for patients' privacy and life. Security of medical images

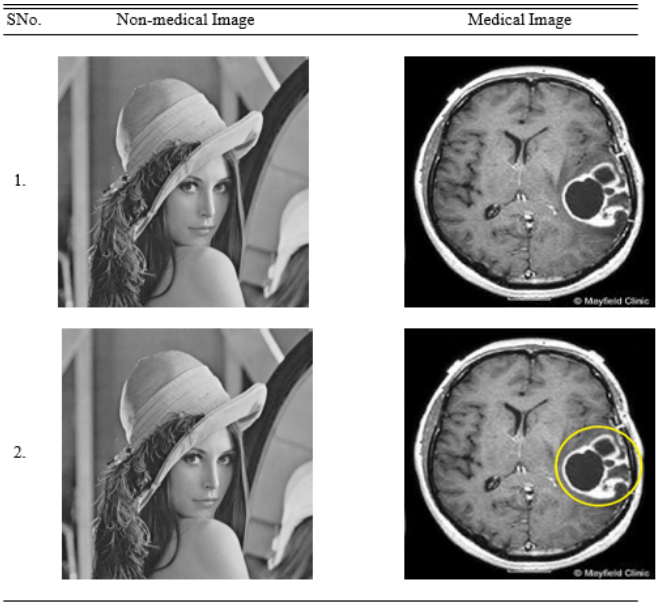


Figure 1.3: 1. is the original Lena image and medical image (MRI). 2. is the watermarked Lena image and watermarked medical image(MRI).

requires three compulsory characteristics:

- Confidentiality - Image can be accessed by entitled person only.
- Reliability - includes integrity where, only authorized person can modify the image. Secondly, authentication, which is the validation of image being true to source and destination and is of correct patient.
- Availability - Image can be accessed and modified by entitled person anytime in normal environment.

Medical image watermarking serves several important purposes and addresses specific needs in the healthcare domain. Here are some key reasons why medical image watermarking is necessary:

1. **Authentication and Integrity Verification:** Medical image watermarking provides a means to authenticate the origin and integrity of medical images. By embedding unique and tamper-resistant watermarks into the images, it becomes possible to verify their authenticity and detect any unauthorized modifications or tampering attempts. This is crucial for ensuring the trustworthiness and reliability of medical images used for diagnosis, treatment, and research.
2. **Copyright Protection:** Medical image watermarking helps protect the copyrights of medical professionals, researchers, and institutions. Watermarks can be used to identify and attribute ownership to medical images, preventing unauthorized use, distribution, and plagiarism. This encourages ethical practices, respects intellectual property rights, and safeguards the interests of content creators in the medical field.
3. **Patient Privacy and Confidentiality:** Watermarking can play a role in preserving patient privacy and maintaining the confidentiality of sensitive medical information. By embedding watermarks containing anonymized patient identifiers or other privacy-related metadata, it becomes possible to trace the source of leaked or misused medical images and ensure accountability in case of data breaches or unauthorized disclosures.

4. **Forensic Analysis and Investigation:** Watermarked medical images can assist in forensic analysis and investigation by providing traceability and evidence of authenticity. In situations where medical images are used as legal evidence or in research studies, watermarks can help establish the chain of custody, verify the integrity of the images, and ensure their admissibility and reliability in legal proceedings or scientific publications.

5. **Quality Control and Image Management:** Watermarking can facilitate quality control and image management in medical imaging systems. Watermarks can contain metadata related to acquisition parameters, patient demographics, imaging protocols, or quality indicators. This information aids in data organization, retrieval, and quality assessment, ensuring proper archiving, retrieval, and analysis of medical images.

6. **Deterrence and Discouragement of Unauthorized Use:** Visible watermarks act as a deterrent against unauthorized use and unauthorized redistribution of medical images. The presence of visible watermarks discourages individuals from misusing or misrepresenting medical images, as the watermark serves as a visible indicator of ownership and authorized usage.

7. **Collaborative Research and Data Sharing:** Watermarking can support collaborative research and secure data sharing in the medical field. By embedding watermarks that contain secure access control information, researchers can selectively grant access to watermarked images, ensuring that only authorized individuals or organizations can view or analyze the data. This helps protect patient privacy while enabling controlled sharing of medical images for research and innovation.

1.3.2 Characterstics of medical watermarking

Medical image watermarking encompasses several properties that are desirable in the context of healthcare and medical imaging. The relationship between these properties is shown in Figure 1.4. Here are some key properties of medical image watermarking:

a. **Robustness:** Medical image watermarks should be robust to withstand various image processing operations and medical image manipulations that can occur during image acquisition, transmission, storage, or analysis. Robustness ensures that the watermark remains detectable even in the presence of common image modifications, such as compression, noise addition, cropping, or geometric transformations. Al-Zewairi et al. (2020) discusses the utilization of machine learning and artificial intelligence in security, specifically intrusion detection. It highlights the challenge of detecting unknown security attacks and the need for a standardized definition. The researchers propose a categorization of unknown attacks and evaluate the performance of intrusion detection systems, emphasizing the requirement for new approaches to address this problem.

b. **Imperceptibility:** Watermarks embedded in medical images should be imperceptible or minimally perceptible to the human visual system. It is crucial to preserve the diagnostic quality and integrity of medical images, ensuring that the embedded watermark does not interfere with the interpretation or analysis of the image by medical professionals. It also depends on the communication networks. Ahlawat and Dave (2021) addresses the issue of node capture attacks in wireless sensor networks (WSNs) and proposes a secure hybrid key predistribution scheme (HKP-HD) to enhance network resistance against such attacks. The scheme combines

the robustness of the q-composite scheme with the threshold-resistant polynomial scheme. By considering the adversary's intelligent behavior and vulnerabilities in the network, the scheme constructs an attack matrix and calculates attack coefficients for each node. A hash chain and multiple key pools are utilized to reduce the probability of key compromise and communication overhead. Simulation results demonstrate the effectiveness of the proposed scheme in reducing key compromise probability, communication overhead, and storage overhead compared to other schemes.

c. **Security:** Medical image watermarking should provide a level of security to prevent unauthorized removal, alteration, or tampering of the watermark or the medical image itself. Security measures can include encryption, digital signatures, and authentication mechanisms to ensure the integrity and authenticity of the watermarked medical images. Hamdan et al. (2023) proposes an edge computing architecture for Internet of Things (IoT)-based cyber-physical systems, addressing the challenges of integrating machine learning. It employs distributed multi-task learning over edge networks, optimizing the learning process without relying on transmitting extensive data to the cloud. Simulation experiments confirm high accuracy and efficient resource utilization compared to traditional approaches. Rahouti et al. (2021) addresses the vulnerabilities and risks associated with IoT devices and the need for efficient security solutions. It discusses the evolution of real-time machine learning (RTML) approaches and proposes a cyber risk detection framework utilizing Boosting- and Bagging-based ensemble learning methods. The framework aims to enhance security in IoT applications by detecting and mitigating cyber threats effectively.

d. **Localization:** Localization refers to the ability to precisely locate and extract the watermark from a medical image. This property is particularly important in scenarios where specific regions of interest or annotations are watermarked, and it is necessary to accurately identify and extract the embedded information.

e. **Capacity:** The capacity of a medical image watermarking technique refers to the amount of auxiliary information or data that can be embedded within the image while maintaining the desired level of robustness and imperceptibility. Sufficient capacity is required to embed relevant patient information, annotations, or other metadata without significantly degrading the image quality or increasing the risk of detection.

f. **Compliance with Standards:** Medical image watermarking techniques should adhere to relevant standards and guidelines in the healthcare domain, such as those defined by Digital Imaging and Communications in Medicine (DICOM). Compliance ensures interoperability, compatibility, and the seamless integration of watermarking methods within existing medical imaging systems and workflows.

g. **Reversibility:** In some cases, it may be desirable to have reversible watermarking in medical images, where the original, unmarked image can be perfectly restored after extracting the watermark. Reversible watermarking allows for the complete recovery of the original medical data without any loss or degradation. It is an optional component of watermarking.

h. **Resistance to Collusion:** Watermark remains detectable even when multiple copies of the content are combined or manipulated.

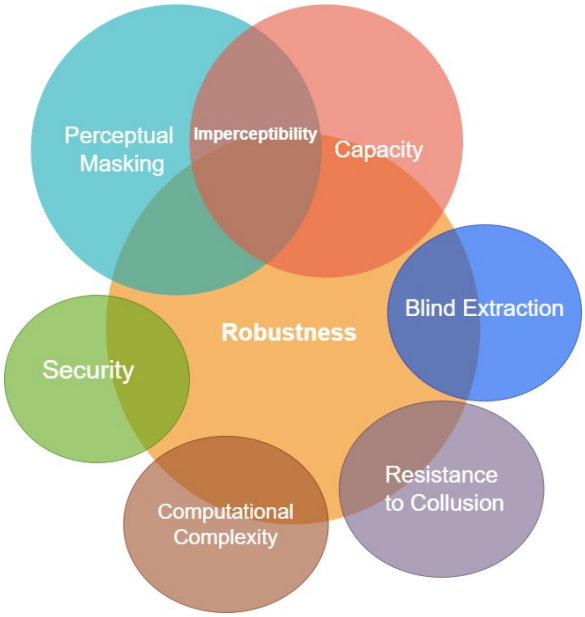


Figure 1.4: Dependencies between various characterstics of medical watermarking.

i. **Data Payload:** Watermark can carry different types of data, such as text, images, or binary patterns.

j. **Blind Extraction:** Watermark can be extracted without the need for the original, unmarked content.

k. **Computational Complexity:** Watermarking algorithms should be computationally efficient.

l. **Perceptual Masking:** Watermark can be embedded in regions where it is less likely to be perceived.

Figure 1.4 shows the dependencies between the characterstics of watermarking. There is a trade-off between imperceptibility and robustness. Embedding a watermark in a highly imperceptible manner can make it more vulnerable to attacks or modifications, reducing its robustness. Conversely, enhancing robustness may require more visible or perceptible watermarks, potentially compromising imperceptibility. Security measures can enhance the robustness of a watermark i.e. incorporating security measures like encryption or authentication, can enhance the robustness of a watermark. By incorporating security techniques, the watermark can be more resistant to unauthorized removal or alteration attempts, thus increasing its robustness. Increasing the capacity of a watermark, allowing it to carry more data, can impact imperceptibility. Higher-capacity watermarks may require more significant modifications to the content, making them more perceptible. Striking a balance between capacity and imperceptibility is crucial for optimal performance.

Blind extraction techniques may introduce additional challenges to achieve robustness. Techniques that allow blind extraction, where the original content is not required during watermark extraction, may introduce additional challenges to achieve robustness. Blind extraction often relies on statistical or structural characteristics of the watermarked content, which can be more vulnerable to attacks. Higher levels of robustness may require more complex algorithms, resulting in increased computational complexity. Balancing the computational demands with the desired level of robustness is necessary to ensure practical implementation and processing efficiency. Leveraging perceptual

masking techniques can enhance imperceptibility. Placing watermarks in less perceptible regions can enhance imperceptibility, but requires careful consideration of the limitations of human perception.

These properties ensure that medical image watermarking techniques are effective in safeguarding patient information, maintaining data integrity, and supporting accurate diagnosis and analysis in healthcare settings. The choice of specific properties depends on the specific application, regulatory requirements, and the balance between security and the diagnostic quality of the medical images.

1.4 Approaches of Medical Watermarking techniques

Medical image watermarking is the image processing technology for integrity and security issues. In order to embed and convert information into digital data in the form of image, the original data is imperceptibly modified with watermarking. The hidden information can later be extracted as and when required. The techniques of medical image watermarking are classified in different methods.

- On the basies of domain, the medical image watermarking can be classified as either spatial domain or frequency domain techniques. The medium which is used for the data hiding plays a vital role in the classification. In frequency domain watermarking techniques, the data is embedded into a transformed host image Wu et al. (2008); Chiang et al. (2008); Al-Qershi and Khoo (2009). On the other hand, the host image embeds the data directly in the spatial domain techniques Zain and Fauzi (2006).

- Watermarking techniques are classified into two categories based on data compression: reversible techniques and irreversible techniques. Reversible watermarking is generally preferred over the latter, as it does not make any loss when the watermarked image retrieves the original imageChiang et al. (2008); Al-Qershi and Khoo (2009). On the other hand, there is some loss while retrieval of the original image in the irreversible watermarking techniques Wu et al. (2008).

- Watermarking technique is classified into three categories based on application: robust, fragile, and hybrid.

    1. Images that require protection of copyright information use robust watermarking techniques, as this technique can sustain intentional or unintentional attacks on images.
    2. Images requiring tampers detection during transmission and authorization of source image use fragile watermarking techniques Zain and Fauzi (2006).
    3. Images requiring privacy and integrity control use hybrid watermarking techniques Giakoumaki et al. (2006a), Al-Qershi and Khoo (2011).

1.4.1 Visible Medical watermarking

Visible medical watermarking refers to the application of visible watermarking techniques specifically in the context of medical images. It involves adding visible marks or overlays to medical images, such as X-rays, Magnetic Resonance Imaging (MRI) scans, Computed Tomography (CT) scans, or Ultrasound (US) images, to indicate relevant information about the image or its usage.

The visible watermarks in medical imaging can include logos, text, symbols, or graphical elements that convey important details. These watermarks are typically overlaid on the medical image without

significantly obstructing the diagnostic information. They may contain information such as patient identification, study date, institution name, copyright notices, or usage restrictions.

Visible medical watermarking serves multiple purposes in the medical field. It helps in the identification and tracking of medical images, ensuring proper attribution and ownership. It assists in maintaining the integrity and authenticity of medical images, preventing unauthorized alterations or tampering. Additionally, visible watermarks can aid in legal and ethical compliance, such as patient privacy protection and adherence to regulatory requirements.

By incorporating visible watermarks, medical professionals, healthcare institutions, and medical imaging vendors can enhance the traceability, accountability, and security of medical images, contributing to accurate diagnosis, research, and proper usage of healthcare data. Visible watermarking techniques from figure 1.5 are as follows:

1. **Logo Watermarking:** A logo watermark involves overlaying a company or brand logo on top of the media content. It is commonly used for branding and copyright protection purposes.

2. **Text Watermarking:** Text watermarking involves overlaying text, such as copyright information, the creator's name, or a message, onto the media content. The text is typically semi-transparent and placed in a corner or along the bottom of the image or video.

3. **Graphic Watermarking:** Graphic watermarking involves overlaying a graphic or pattern onto the media content. It can be a design, pattern, or any graphical element that identifies the owner or adds a visual mark of ownership.

4. **Date and Time Watermarking:** Date and time watermarking involves adding a visible timestamp on the media content, indicating when it was created or modified. This type of watermarking is commonly used for proof of authenticity and documentation purposes.

5. **Visible Watermarking for Advertisement:** In the context of advertisements, visible watermarking can include product logos, promotional messages, or overlays that identify the source or purpose of the advertisement.

6. **Forensic Watermarking:** Forensic watermarking involves embedding visible marks or information that can be used for forensic analysis or tracking. These watermarks are often used in legal contexts to deter unauthorized use or distribution of media content.

1.4.2 Invisible Medical watermarking

Invisible medical watermarking refers to the application of watermarking techniques specifically in the context of medical images, where the watermarks are not directly visible to the naked eye. It involves embedding imperceptible marks or data within the medical images to provide additional information, authentication, or copyright protection.

Unlike visible watermarks, which can be seen as visible overlays or marks on the image, invisible watermarks are designed to be hidden within the image data itself. They are embedded in a way that does not significantly alter the visual appearance or diagnostic quality of the medical image. These watermarks are typically embedded using techniques that modify specific image features or characteristics, such as pixel values or frequency components.

The purpose of invisible medical watermarking is to enable the identification, authentication, and traceability of medical images without interfering with their clinical use. The embedded watermarks can contain metadata, digital signatures, unique identifiers, or other information that can be

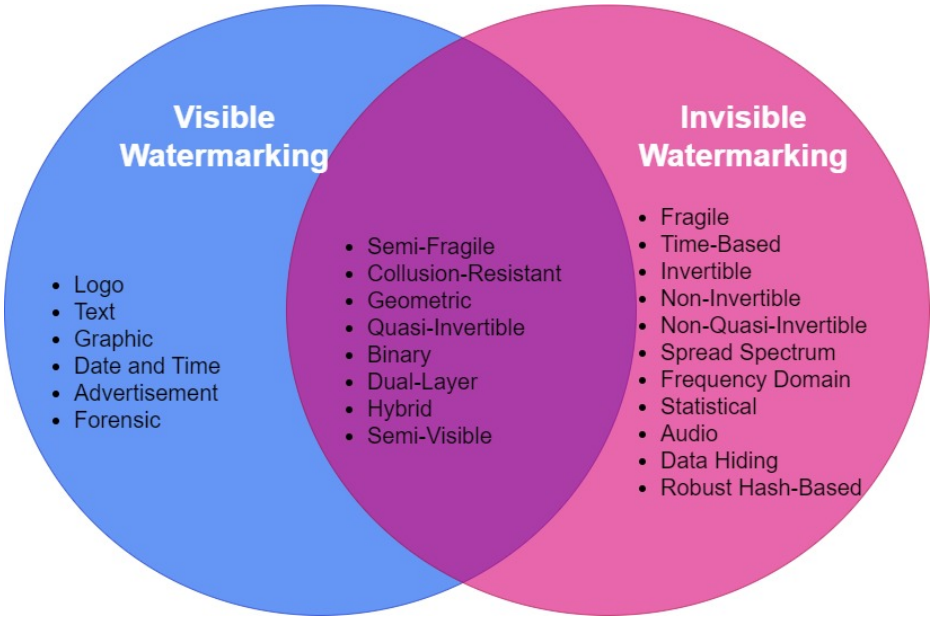


Figure 1.5: Different types of medical watermarking.

extracted using specialized algorithms or tools. These watermarks help in establishing the origin, ownership, and integrity of medical images, enabling verification of their authenticity and preventing unauthorized modification or misuse.

Invisible medical watermarking plays a crucial role in medical data security, copyright protection, and forensic analysis. It supports various applications such as data tracking, image verification, content integrity, patient privacy protection, and legal compliance in the healthcare industry. By employing invisible watermarks, medical professionals, researchers, and healthcare organizations can enhance the security, trustworthiness, and accountability of medical image data while preserving its clinical value. Following are some invisible watermarking techniques from figure 1.5:

1. **Fragile watermarking techniques:** are designed to detect any modifications or tampering attempts made to the watermarked content. Even slight alterations to the content will result in a noticeable change or complete loss of the watermark. Fragile watermarking is commonly used for integrity verification and authentication purposes. Fragile watermarking is typically implemented as an invisible watermark, as the focus is on detecting any modifications or tampering attempts made to the watermarked content.

2. **Time-based watermarking** involves embedding the watermark in the temporal domain of media content, such as video or audio. These watermarks are designed to be robust against temporal modifications like frame reordering or time scaling. Time-based watermarking is often used for copyright protection and authentication in multimedia streaming and broadcasting scenarios. Time-based watermarking is typically implemented as an invisible watermark, embedded in the temporal domain of media content. The focus is on withstanding temporal modifications while ensuring copyright protection and authentication.

3. **Invertible medical watermarking** refers to a technique where the original, unmarked medical image can be perfectly restored after extracting the embedded watermark. This means that the watermark can be added and subsequently removed without any loss of the original image data. Invertible watermarking techniques ensure that the clinical information contained

in the medical image remains intact and unaffected by the watermarking process. This property is desirable in medical applications where the watermark needs to be added and removed without altering the underlying diagnostic information. Invertible watermarking is typically implemented as an invisible watermark, allowing the original content to be perfectly restored after extracting the watermark.

4. **Non-invertible medical watermarking**, also known as irreversible watermarking, is a technique where the original, unmarked medical image cannot be perfectly restored after extracting the watermark. The watermarking process introduces some irreversible modifications to the image data, making it impossible to recover the exact original image. Non-invertible watermarking techniques are often used in scenarios where the primary focus is on copyright protection, content integrity, and deterrence rather than the ability to restore the original image. Non-invertible watermarking is typically implemented as an invisible watermark, introducing irreversible modifications to the data, making it impossible to recover the exact original content.

5. **Non-quasi-invertible medical watermarking** techniques do not provide any means for even approximate restoration of the original medical image after watermark extraction. These techniques introduce significant irreversible modifications to the image data, making it impossible to recover the original image or achieve any form of restoration. Non-quasi-invertible watermarking is often used in medical applications where the primary objective is robustness, tamper detection, or authentication, and the ability to restore the exact original image is not a requirement. Non-quasi-invertible watermarking is typically implemented as an invisible watermark, introducing significant irreversible modifications to the data, making it impossible to recover the original content.

6. **Frequency Domain Watermarking:** Frequency domain watermarking techniques utilize transformations like Fourier or wavelet transforms to embed the watermark in the frequency domain of the media content. The watermark is embedded by modifying the amplitudes or phases of certain frequency components, making it invisible to the human eye.

7. **Statistical Watermarking:** Statistical watermarking techniques exploit statistical properties of the media content to embed the watermark. These methods often modify the statistical distribution of pixel values or coefficients in a way that is difficult to perceive visually but can be detected through statistical analysis.

8. **Robust Hash-Based Watermarking:** Robust hash-based watermarking techniques utilize cryptographic hash functions to embed the watermark. The hash value is computed from the media content and serves as a digital fingerprint that is imperceptible but can be used to verify the authenticity or integrity of the content.

1.4.3 Hybrid Medical watermarking

There are watermarking techniques that combine both visible and invisible aspects, offering a hybrid approach. These techniques allow for the presence of a visible watermark while also embedding an invisible watermark for additional security or authentication. Here are a few examples:

- **Dual-Layer Medical Watermarking:** In dual-layer medical watermarking, two watermarks are embedded in the medical image—one visible and the other invisible. The visible watermark

serves as a deterrent or notice of ownership, branding, or information about the medical institution. Simultaneously, the invisible watermark provides additional security, authentication, or tamper detection features, ensuring the integrity and traceability of the medical image.

- **Hybrid Medical Watermarking:** Hybrid medical watermarking techniques combine both visible and invisible watermarking methods to strike a balance between the visibility of the watermark and the robustness of the protection. The visible watermark can contain copyright information, patient identifiers, or annotations visible to the human eye, while the invisible watermark provides additional security against tampering, unauthorized use, or counterfeit.

- **Semi-Visible Medical Watermarking:** Semi-visible medical watermarking involves embedding a watermark that is partially visible to the human eye. The watermark appears as a faint or translucent overlay on the medical image, allowing it to be noticed but not obtrusive. Alongside the semi-visible watermark, an invisible watermark can be embedded to provide additional security, authentication, or traceability features.

These techniques in medical image watermarking aim to combine the benefits of visible elements for branding, ownership, and deterrence, with the advantages of invisible components for robust security, authentication, integrity verification, and tamper detection. The specific implementation and selection of visible and invisible watermarking components depend on the requirements, compliance, and objectives of the medical imaging application. A few examples from figure 1.5 of hybrid watermarking are are follows

1. **Semi-fragile watermarking** lies between robust and fragile watermarking techniques. These watermarks can withstand certain benign modifications like compression or noise addition. They are highly sensitive to malicious tampering or unauthorized modifications. Semi-fragile watermarking is often used for content authentication and integrity verification. Semi-fragile watermarking can be implemented as either visible or invisible, depending on the specific implementation and requirements. It can withstand certain benign modifications while being sensitive to malicious tampering.

2. **Collusion-resistant watermarking** techniques are specifically designed to withstand collusion attacks. Collusion occurs when multiple watermarked copies of the same content are combined to remove the watermark. Collusion-resistant watermarks remain detectable even when multiple copies are available, and colluders try to eliminate or reduce the watermark signal. Collusion-resistant watermarking can be implemented as either visible or invisible, depending on the specific requirements. The focus is on designing watermarks that remain detectable even when multiple copies are available and colluders attempt to eliminate or reduce the watermark signal.

3. **Geometric watermarking** techniques modify the geometric features or spatial arrangement of the media content to embed watermarks. They are primarily used for copyright protection and authentication of images, illustrations, or graphical designs. Geometric watermarking involves techniques like geometric transformations, warping, or feature-based embedding. Geometric watermarking can be implemented as either visible or invisible, depending on the specific implementation and requirements. It involves modifying the geometric features or spatial arrangement of the media content for copyright protection and authentication.

4. **Binary watermarking** techniques involve embedding a binary pattern or sequence into the media content by modifying specific features or characteristics. They are commonly used for copyright protection, authentication, or data hiding applications. Binary watermarking can be implemented as a visible watermark by overlaying a logo, text, or other graphical elements on top of the media content. Non-visible: Binary watermarking can also be implemented as a non-visible watermark, where the watermark is imperceptible to the human eye but can still be detected or extracted using specialized algorithms.

5. **Quasi-invertible medical watermarking** lies between invertible and non-invertible watermarking techniques. It allows for an approximate restoration of the original medical image after removing the watermark, but it does not guarantee perfect restoration. Quasi-invertible techniques aim to strike a balance between the ability to extract the watermark and preserving the visual quality or diagnostic accuracy of the medical image to a certain extent. These techniques may introduce some degradation or loss of information during watermark extraction, but the impact on the clinical interpretation is minimized. Quasi-invertible watermarking can be implemented as either visible or invisible, allowing for an approximate restoration of the original content after removing the watermark.

Table 1.1: DIfferent types of medical watermarking with associated properties and the need.

S.No.	Types of Watermarking	Need	Properties
1	Fragile watermarking	Authentication and Integrity Verification	Robustness, Tamper detection
2	Visible watermarking, Invisible watermarking	Copyright Protection	Ownership identification
3	Invisible watermarking	Patient Privacy and Confidentiality	Anonymization, Privacy metadata
4	Visible watermarking, Invisible watermarking	Forensic Analysis and Investigation	Traceability, Authenticity evidence
5	Visible watermarking, Invisible watermarking	Quality Control and Image Management	Metadata embedding, Quality indicators
6	Visible watermarking	Deterrence and Discouragement	Visible indication of ownership
7	Invisible watermarking	Collaborative Research and Data Sharing	Secure access control

A watermarking algorithm is typically evaluated based on its ability to achieve high robustness, high capacity for data hiding, and high degree of imperceptibility without compromising any of these properties. Table 1.1 shows the usage of techniques, according to the required properties. Nonetheless, the robustness of digital watermarking is generally less in the spatial domain when compared to the frequency domain. There are multiple transformation techniques available in order to convert an image to the frequency domain from the spatial domain, Namely: Fast Fourier Transform (FFT), Wavelet, *DCT*, Laplace or Walsh/Hadamard, Discrete Wavelet Transform (DWT). These transformation techniques have the potential to generate better robustness and more embedded information against common attacks, although the spatial domain generally has a lower computational cost.

.

1.4.4 Medical Watermarking Quality Evaluation Parameters

1. **Computational Cost**: The computational cost of watermarking depends on the method used. If the method is more complex, requiring complex algorithms and more software and hardware, then the computational cost will increase. Conversely, if the method is less complex, the computational cost will decrease.

2. **Peak Signal to Noise Ratio (PSNR)**: The degree of invisibility, or how much distortion is introduced by the watermarking process in the original image, can be evaluated by calculating the *PSNR* value between the original and watermarked images. *PSNR* is calculated using the Eq. 1.1:

$$PSNR = 10 \times log_{10} \frac{(2^b - 1)^2}{MSE} \tag{1.1}$$

where b is the bit depth of the image and Mean Square Error (MSE) is defined as,

$$MSE = \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{\delta(i,j)^2}{H \times W} \tag{1.2}$$

where $\delta(i,j)$ is defined as

$$\delta(i,j) = S(i,j) - C(i,j) \tag{1.3}$$

where $S(i,j)$ is the pixel of watermarked image and $C(i,j)$ is the pixel of cover image, H and W is the height and width of image respectively.

3. **Capacity**: is measured by the size of the image and size of hidden bits *i.e.*

$$Capacity(C) = (H \times W)/Y \tag{1.4}$$

For an image I_m with size $H \times W$ with total number of hidden bits Y.

4. **Reveresibility**: The reversibility of a watermarking scheme depends on the Image Error Rate (IER), which is calculated as the ratio of the number of recovered images with errors to the total number of test images. Another important factor is the number of bits of information stored per pixel, as a higher number of bits allows for more colors to be represented but also requires more memory to store or display the image.

5. **Structural Similarity Index (SSIM)**: is a commonly used metric for measuring the perceived quality of digital images. Unlike other image quality metrics, *SSIM* is designed to take into account perceptual phenomena such as luminance masking and contrast masking, as well as the perceived change in structural information caused by image degradation. To compute *SSIM*, an image is typically divided into multiple windows, and the index is calculated for each window separately. The measure between two windows p and q of common size $N \times N$ is:

$$\text{SSIM}(p,q) = \frac{(2\mu_p\mu_q + d_1)(2\sigma_{pq} + d_2)}{(\mu_p^2 + \mu_q^2 + d_1)(\sigma_p^2 + \sigma_q^2 + d_2)} \tag{1.5}$$

The *SSIM* index is calculated based on the average of p denoted as μ_p, the average of q denoted as μ_q, the variance of p denoted as σ_p^2, the variance of q denoted as σ_q^2, and the covariance of p and q denoted as σ_{pq}. Two variables, $d1 = (b1L)^2$ and $d2 = (b2L)^2$, are used to stabilize the division with a weak denominator, where L represents the dynamic range of the pixel values and $b1 = 0.01$ and $b2 = 0.03$ by default. The *SSIM* index satisfies the symmetry condition such that $SSIM(p;q) = SSIM(q;p)$. The concept of structural information is based on the idea that pixels have strong inter-dependencies, especially when they are spatially close. The *SSIM* index can be used to predict the perceived quality of digital images, and a plot of the mean opinion score (MOS) as a function of mean *SSIM* (MSSIM) can provide a simple arithmetic average of each of the local scores. *MSSIM* can deliver better consistency with perceptual evaluations.

6. **Normalized Correlation (NC)**: The technique of *NC* has found widespread application in fragment-based recognition, under the assumption of fixed viewing conditions or availability of examples from all viewing conditions. It is considered acceptable if a patch is not matched to a version of itself that has been rotated by 90°.

7. **Signal-to-Noise Ratio (SNR)**: is a widely used metric in digital imaging to measure the sensitivity of a digital image. It is calculated as the ratio of the average signal value to the standard deviation of the background noise.

8. **Bit Per Pixel (BPP)**: is calculated by :

$$\text{BPP} = \frac{\text{number of watermark bits}}{\text{total number of pixels in original image}} \tag{1.6}$$

9. **Time Complexity**: shows the efficiency of the watermarking algorithm. The algorithm should have least processing time with high payload.

1.4.5 Attacks on Medical watermarked images

Medical watermarked images can be susceptible to various attacks that aim to compromise the integrity, security, or authenticity of the watermarked content. Here are some common types of attacks on medical watermarked images:

a. **Removal Attacks:** Removal attacks involve attempts to completely remove or partially remove the embedded watermark from the medical image. Attackers may employ image editing techniques, such as cropping, filtering, or inpainting, to eliminate or tamper with the watermark, thereby making it undetectable or altering its information.

b. **Tampering Attacks:** Tampering attacks aim to modify specific regions or features of the watermarked medical image while trying to maintain the visual quality and appearance of the image. These attacks can include content manipulations, such as altering the pixel values, introducing localized modifications, or changing the metadata associated with the image.

c. **Collusion Attacks:** Collusion attacks occur when multiple watermarked medical images are combined to collectively remove or reduce the visibility of the watermark. Attackers may utilize statistical analysis, averaging techniques, or other collusion methods to cancel out the watermark signal by exploiting multiple watermarked copies of the same image.

d. **Compression Attacks:** Compression attacks involve compressing the watermarked medical image using lossy compression algorithms or techniques. Lossy compression methods, such as *JPEG* compression, can introduce quantization errors and perceptual distortions that may affect the visibility and detectability of the watermark.

e. **Geometric Attacks:** Geometric attacks target the spatial arrangement or geometric features of the watermarked medical image. Attackers may perform geometric transformations, such as rotation, scaling, or affine transformations, to manipulate the image and potentially render the watermark ineffective or less visible.

f. **Encryption Attacks:** Encryption attacks aim to encrypt or obfuscate the watermarked medical image, making it challenging to extract or detect the embedded watermark. Attackers may employ encryption algorithms or cryptographic techniques to protect the content and prevent watermark extraction without authorized decryption.

g. **Print-and-Scan Attacks:** Print-and-scan attacks involve printing the watermarked medical image and subsequently scanning the printed copy. This process can introduce various distortions and artifacts that may impact the watermark visibility and quality, making it harder to extract or detect the watermark accurately.

h. **Statistical Attacks:** Statistical attacks exploit statistical properties or vulnerabilities of the watermarking algorithm or the watermarked medical image. Attackers may analyze statistical characteristics, such as noise distribution, frequency domain properties, or spatial correlations, to identify weaknesses in the watermarking method or reveal hidden information.

i. **Stirmark Attacks:** Stirmark attacks refer to attacks that specifically target the watermarking algorithms or systems by utilizing the Stirmark benchmarking suite. Stirmark provides a standardized framework for evaluating the robustness and security of watermarking techniques, allowing attackers to identify vulnerabilities and weaknesses in the watermarking system.

These attacks highlight the need for robust and secure watermarking techniques in the context of medical imaging to ensure the protection of patient data, maintain the integrity of medical images, and prevent unauthorized manipulation or tampering. Watermarking algorithms and systems should be designed to withstand these attacks and provide effective countermeasures to ensure the reliability and security of watermarked medical images.

1.5 Contribution of the research work

This research aims to address several challenges and limitations in the field of medical watermarking, thereby making significant contributions. The motivation behind this work stems from the recognized need to overcome existing obstacles and enhance the effectiveness of watermarking techniques specifically tailored for medical applications using data compression, image feature extraction, security, and tamper detection. By leveraging the potential of the Slantlet Transform (SLT), Fast Walsh Transform (FWT), and Ridgelet Transform (RT), *RS* vector embedding, and advanced techniques such as Artificial Neural Network (ANN) and cryptographic algorithms, this research aims to overcome these challenges and provide innovative solutions with improved performance and enhanced capabilities. The overarching goal of this research is to enhance the capacity, security, robustness,

and visual quality of watermarked medical images while addressing the challenges and limitations present in existing techniques.

One of the primary motivations for using *SLT* in data embedding is its ability to increase the energy percentage of the image or signal after compression. This enhancement in energy retention not only improves the embedding capacity but also contributes to a more robust and reliable embedding process. In comparison to other transformations like *DWT* and *DCT*, *SLT* exhibits superior noise removal capabilities and achieves better performance in signal compression. This improvement in performance, particularly in terms of Bit Error Rate (BER), drives the motivation to utilize *SLT* as a transformative technique for data embedding.

Moreover, *SLT* proves to be highly effective in feature extraction for image classification purposes. By utilizing *SLT* to extract image features, this research enables more accurate region classification and facilitates tasks such as tamper detection and localization. This motivation is grounded in the potential for *SLT* to capture relevant image characteristics and provide valuable insights for image analysis and classification.

Another transformation technique employed in this research is the *FWT*. *FWT* is known for its effectiveness in transforming data into the frequency domain and its applications in image compression and watermarking. By incorporating the *FWT* into the proposed technique, the research aims to enhance the capacity, security, and imperceptibility of watermarked images. This transformation technique contributes to improving the overall quality and visual perception of watermarked images, ensuring that the embedded watermark remains robust against attacks and provides reliable authentication.

Furthermore, the *RT* is another important component of this research. *RT* is renowned for its geometrically accurate representation, eliminating wrap-around artifacts. It provides a powerful tool for detecting lines and other geometric features in images. By integrating the *RT* into the proposed technique, this research aims to improve the robustness, security, and imperceptibility of watermarked images. *RT* enhances the capacity for watermark embedding and contributes to the overall quality and visual perception of watermarked images.

The inclusion of the *RS* vector for embedding further amplifies the motivation behind this work. The hybrid embedding approach, combining *SLT* and *RS* vector embedding, enhances both the capacity and security of the watermarking process. By leveraging the benefits of both techniques, this research aims to optimize the embedding process and achieve robust and secure watermarking.

Additionally, the motivation for employing advanced cryptographic techniques such as Message Digest Method 5 (MD5), Advanced Encryption Standard (AES), Secure Hash Algorithm-3 (SHA-3) and biometric thumbprints of the patients is driven by the need to address security concerns associated with data embedding and medical imaging. Security issues, especially in the context of medical imaging, demand robust protection measures to safeguard patient information and prevent unauthorized access or tampering. The proposed techniques provide a multi-layered security framework, ensuring the confidentiality, integrity, and authenticity of the embedded data.

The motivation to address the limitations of existing techniques in terms of execution time, visual quality, and imperceptibility is a significant driving factor in this research. The proposed technique demonstrates significantly lower execution time, making it more efficient for real-time applications. The improved visual quality of watermarked images, including enhanced smoothness and contrast, enhances the overall user experience and ensures the imperceptibility of the embedded data.

Experimental results play a crucial role in motivating this work. The comparison of performance metrics such as correlation, Similarity Index (SIM), *SNR*, *PSNR*, *BPP*, and time complexity with

existing techniques showcases the superiority of the proposed approach. The obtained results validate the effectiveness and efficiency of the proposed techniques, thereby driving the motivation to further explore and refine the developed methodologies.

Finally, the importance of medical imaging security, particularly in critical situations like the Coronavirus disease 2019 (COVID-19) pandemic, serves as a broader motivation for this work. Recent literature emphasizes the significance of secure and reliable medical imaging techniques. By addressing the limitations of existing methods and providing improved robustness, contrast enhancement, tamper detection, and recovery capabilities, this research aims to contribute to the overall advancement and security of medical imaging practices.

In conclusion, the motivation behind the work conducted in this research is driven by the desire to overcome challenges in data embedding, signal compression, image feature extraction, security, and tamper detection. The utilization of *SLT*, *RT*, *FWH*, *RS* vector embedding, *ANN*, and advanced cryptographic techniques aims to enhance performance, security, and efficiency. Through experimental validation and the broader goal of advancing medical imaging security, this research endeavors to provide innovative solutions that contribute to the field and benefit various applications in image and data processing.

1.6 Organization of the Thesis

The research work presented in the thesis is organized and structured in the form of seven chapters, which are briefly described as follows:

Chapter 1 introduces the basic concepts, need of the research, motivation and quality parameters to access the proposed work.

Chapter 2 provides a comprehensive review of the literature in medical watermarking

Chapter 3 presents a *SLT* based hybrid watermarking technique for medical images. This chapter describes requirements of the proposed technique, review of *SLT*, watermark creation algorithm, watermark embedding algorithm, watermark extraction algorithm, experimental results and the conclusion of the proposed technique.

Chapter 4 deals with the second proposed technique which is a dual hybrid medical watermarking technique using walsh-slantlet transform. This chapter gives a brief introduction of Walsh-Hadamard transform and *ANN*. It also highlights the scope of this research along with proposed watermarking technique for feature extraction, watermark embedding and extraction algorithms. Assessment of this proposed technique is done on various parameters proving its credibility and robustness.

Chapter 5 presents a reversible medical image watermarking technique for tamper detection using *ANN* and *SLT*. Introduction of this chapter points out the crucial issues solved in proposed research. Proposed reversible medical watermarking technique is then described along with the ahead-preparations of the lossless data recovery, feature extraction algorithm and data recovery from extracted features. Different embedding and extraction algorithms are given for *ROI* and *RONI*. Invisibility evaluation, authenticity and integrity evaluation, reversibility evaluation, robustness evaluation, security of the watermark evaluation, improvement over state-of-the-art techniques is done. At-last the chapter is concluded precisely.

Chapter 6 describes a reversible Robust Austere Viable watermarking medical images using *RT*. Objectives and scope of proposing this fourth medical watermarking technique is mentioned, along with the detailed overview of *RT*. Unique Identity Document-Austere Viable Watermark- ing (UID-AVW), Region Of Interest-AVW (ROI-AVW) and Tamper Detection/Recovery- AVW (TDR-AVW), Watermark Extraction Algorithm for *UID-AVW*, Watermark Extraction Algorithm for *ROI-AVW* and *TDR-AVW* algorithms are proposed. Results and discussion include the evaluations of this technique against more than 25 existing techniques. The chapter is finally, concluded with highlights and remarks.

Chapter 7 concludes the thesis with overall discoveries of the present research work. The scope for future work is also mentioned.

Chapter 2

Literature Review

Extensive literature survey has been conducted in the field of medical image watermarking, leading to the classification of watermarking techniques into distinct categories. Specifically, these categories include spatial domain watermarking, transform/frequency domain watermarking, compressed domain watermarking, and hybrid domain watermarking. Each category represents a different approach to embedding watermarks in medical images and offers unique advantages and considerations.

2.1 Spatial Domain Watermarking

Spatial domain watermarking is a widely used technique in the field of medical image watermarking, aiming to embed and extract watermarks directly in the pixel values of a medical image. It operates in the original spatial representation of the image, making it a straightforward and effective approach for watermarking medical images.

One common technique in spatial domain watermarking is the *LSB* method. In this technique, the least significant bit of selected pixel values in the medical image is replaced with the watermark bits. Since the modification in the *LSB* is typically imperceptible, it allows for a high payload of watermark data to be embedded. However, it is important to note that *LSB* watermarking is vulnerable to simple image processing operations and can be easily removed or altered. Another approach in spatial domain watermarking is the Spread Spectrum technique, which applies a pseudo-random sequence to modify the pixel values of the medical image. The watermark is embedded by adding or subtracting a small value from each pixel based on the sequence. This technique offers robustness against common attacks and ensures the watermark remains intact even after various image processing operations. However, if the modification is significant, it may introduce visible noise to the medical image. Spatial domain watermarking techniques can also utilize the specific content of the medical image. For example, watermarks can be embedded by slightly altering the luminance or color components of specific *ROI*s within the medical image. This approach is particularly useful in medical imaging applications where watermarks can indicate important information such as patient data, medical annotations, or copyright information. Additionally, spatial domain watermarking can involve techniques like visual cryptography. In this method, the original medical image is divided into shares, where each share individually reveals no information about the watermark. The watermark can only be revealed when the shares are combined or superimposed using specific decoding algorithms, ensuring the security and privacy of the embedded information.

A technique proposed by Anand and Niranjan (1998) introduced an efficient watermarking approach in the spatial domain of medical images. This technique involved concealing the watermark by swapping its bits with the grey-level pixels of the watermark. The method ensured the privacy of patients by encrypting the watermarked information. Importantly, the diagnostic value of the medical images remained unaffected after watermarking. Additionally, this methodology could be extended to other types of patient data, such as Electroencephalogram (EEG) and Phonocardiogram (PCG), without requiring any modifications to the system configuration or software. Maximum Normalized

Root Mean Square Error (MNRMSE) is used as evaluating parameter which valued as 0.0042% for *CT* scan and 0.0052% for ultrasound image. The watermark is embedded directly into the spatial representation of the medical images by swapping bits with the grey level pixels.

Acharya et al. (2003) proposed an interleaving process with two types of error control coding techniques for digitally watermarking patients' information in a medical images for better security and reduction in transmission overheads with less storage. The algorithm result proves that hamming code provides superior results by using error correction codes while transmitting a data through the channel thus reducing noise errors generated through Gaussian noise. Li et al. (2005) proposed a fingerprint model for tracing illegal distribution of medical images from an authorized person in a group communication environment. The broadcast copy of a digitally watermarked medical image can become usable only after decoded by authorized watermark key holder. *PSNR* of 54.62 dB is achieved against 34.32 dB in abdomen image of 512×512.

In a study by Coatrieux et al. (2008), a watermarking technique was developed to enhance the protection and authenticity of medical images. This technique involved combining different identifiers, such as the *DICOM* standard, unique patient identifier, or the Anonymous European Patient Identifier, to improve the maintainability and authenticity of the images. The watermark was designed to incorporate these identifiers into the spatial representation of the medical images, providing an added layer of protection and ensuring their maintainability and authenticity. An advanced method for additive interpolation error expansion algorithm was introduced by Naheed et al. (2014). This study has enhanced the algorithm by integrating it with two optimization techniques: Particle Swarm Optimization (PSO) and Genetic Algorithm (GA). By leveraging the correlation of image pixel values, both *PSO* and *GA* were utilized to achieve improved estimation of neighboring pixel values. This integration led to an optimal balance between information storage capacity and imperceptibility, enhancing the overall performance of the algorithm.

In their work, Dragoi and Coltuc (2015) presented a method to lower the mathematical complexity caused by local prediction in difference expansion reversible watermarking. Instead of computing predictors for individual pixels, they computed distinct predictors for groups of pixels and then recovered them at detection. They provided predictions on a rhombus that is defined by four horizontal and vertical neighbors. By using their approach, the computational cost is halved without any impact on performance. Although in groups of three or four pixels, there may be a small loss in performance, the benefits of reducing the mathematical complexity by a third or a fourth are significant. Balasamy et al. (2016) proposed a multiple watermarking technique that involved fusing multiple images using the arithmetic blend extension method. The technique focused on manipulating pixel values and blending the watermark images within the host image, aligning with spatial domain watermarking methods. However, it is important to note that this method is not resilient against various types of attacks, particularly geometric attacks.

2.1.1 ROI/RONI based Watermarking in Spatial Domain

ROI/RONI based watermarking in the spatial domain of medical images involves selectively embedding watermarks within regions of interest or non-interest. It enables the protection and authentication of critical medical information within specific regions while preserving image quality and functionality. This technique enhances the security and integrity of medical data and aids in ownership verification and copyright protection. Shih and Wu (2005) proposed a *GA* for embedding digital watermark in important information area, *ROI*, in medical image. *ROI* part is compressed

using lossless compression and lossy compression is used to compress *RONI*.

Tian et al. (2011) presented an integrated watermarking technique based on visual saliency for copyright protection and synchronous image authentication. Moreover, the technique also utilizes a proto-object-based saliency attention model to extract the *ROI* automatically. The copyright information is then embedded using an enhanced quantization method that is designed to withstand signal-processing attacks. Gao et al. (2017) proposed a *RDH* algorithm. Contrast enhancement is achieved for *ROI* without distortion and tamper. Umamageswari and Suresh (2015) introduced a mechanism for medical images based on open network security. The contents of altered medical image can be recovered with this technique based on lossless watermarking with help of Digital Signature (DS). Additive hash functions are used so that if *DS* is lost through the network than the watermarked image is used for extracting *DS* in another format. Hence the *ROI* region for all types of medical images like *US*, Angiographic images, *MRI*, Endoscopic, and *CT* are covered.

Priya and Sadasivam (2015) introduced a lossless reversible watermarking scheme that employed a reversible embedding scheme to embed the watermark. The scheme incorporated a combination of hashing, compression, and digital signature techniques to create a content-dependent watermark, utilizing the compressed *ROI* for the recovery of the *ROI*. Although compression techniques were incorporated, the scheme primarily operated within the spatial domain, classifying it as a spatial domain watermarking technique.

2.1.2 Tamper Detection Watermarking in Spatial Domain

Tamper detection watermarking in the spatial domain for medical images is a technique that focuses on embedding watermarks that are specifically designed to detect any tampering or modifications to the image. These watermarks are strategically placed within the image to enable the detection of any unauthorized alterations, such as image tampering, region cropping, or content modification. Tamper detection watermarking provides an added layer of security and integrity verification for medical images, ensuring that any tampering attempts can be detected and flagged, allowing for reliable authentication and protection of the medical data.

In their study, Milanova et al. (2003) proposed three distinct watermarking techniques for image protection. The first technique, known as Strict Authentication Watermarking (SAW), involved embedding the digital signature of the image into the *ROI*, allowing the image to be restored to its original value. The second technique, called Strict Authentication Watermarking with *JPEG* (SAW-JPEG), utilized the same principle as *SAW* but was also capable of surviving some level of *JPEG* compression. The third technique, Authentication Watermarking with Tamper Detection and Recovery (AW-TDR), not only enabled tamper localization but also facilitated the reconstruction of the original image. In this technique, the watermark was directly embedded into the spatial representation of the *ROI* within the image.

Furthermore, Zain and Fauzi (2006) described a fragile watermarking technique for image recovery and tamper detection. The technique involved the utilization of a public chaotic mixing algorithm along with a secret key. The experiments were conducted using ultrasound grayscale images of dimensions $800 \times 600 \times 8$ bits. The results showed 100% recovery for tampered blocks up to 50%.

Zain and Fauzi (2007) provided an improvement to their existing technique Zain and Fauzi (2006) on cover image recovery from watermarked image and tamper detection. The recovery rate is enhanced, the watermark is better distributed to minimize distortion, and the image quality is improved. Kulkarni and Patil (2012) gave a reversible watermarking technique for tamper detection

and recovery, which uses an ultrasound grayscale image of size $800 \times 600 \times 8$ bits that are divided into *ROI* and *RONI*. The technique employs *LSB* for reversible watermarking, where the removed information is restored in another part.

A unique watermarking method for tamper detection for *ROI* with the complete recovery of *ROI* was given by Eswaraiah and Reddy (2014). This is a fragile block based medical image watermarking technique. This technique is used to avoid embedding distortion inside *ROI*, the tampered blocks inside *ROI* are accurately detected with integrity verification and lossless original *ROI* pixels. *ROI* pixels, border pixels and *RONI* pixels are the three sets of pixels in which medical image are segmented. Border pixels are then, embedded with authentication data, information of *ROI* and *RONI*. The watermarking technique operates at the block level within the spatial representation of the medical image, specifically focusing on the *ROI* and border pixels for tamper detection and recovery purposes.

2.1.3 Block-based Watermarking in Spatial Domain

Block-based watermarking in the spatial domain for medical images is a technique that involves dividing the medical image into smaller blocks and independently processing each block for watermark embedding or extraction. This approach allows for localized embedding and extraction of watermarks in medical images, enabling the protection, authentication, or identification of specific *ROI*s or medical data within the image. Block-based spatial domain watermarking in medical images aims to ensure the integrity and security of sensitive medical information while preserving the diagnostic quality of the image. Wu et al. (2008) proposes two block-based methods for recovery and to detect temper. In the first method, the recovery information and an authentication message of other blocks are added to a block. In contrast, information is added to the *ROI* in the second method. Tampering can be detected if the other blocks produce an approximate image.

2.1.4 Transform based Watermarking in Spatial Domain

In the spatial domain, the transform processes the image data directly in its spatial representation. It analyzes the image by decomposing it into different levels of details and approximations, allowing for localized analysis of image features. Manasrah and Al-Haj (2008) proposed a wavelet-based image multi-watermarking technique to implement issues like image source authentication, image annotation and image retrieval. The wavelet transform is used as the basis for embedding multiple watermarks and addressing issues related to image source authentication, annotation, and retrieval. Garcia-Hernandez et al. (2016) gives a technique of digital watermarking in medical images with high payloads using two methods, High-Capacity Data-Hiding (HCDH) algorithm and the Spread Spectrum based on the *DCT*. *HCDH* algorithm is better suited for high payload medical images in computer aided diagnosis (CAD). The *HCDH* algorithm and the use of the *DCT* in the Spread Spectrum method both operate in the spatial domain, embedding the watermark directly into the spatial representation of the medical images.

2.1.5 Reversible Watermarking in Spatial Domain

Reversible watermarking in the spatial domain is a technique used to embed watermarks in digital images while ensuring the original image can be perfectly restored without any loss of information. It allows for the recovery of the original image from the watermarked version, making it suitable

for applications where both the watermark and the original image need to be preserved. Reversible watermarking in the spatial domain achieves this by exploiting the redundancy present in the image data and carefully modifying pixel values to accommodate the embedded watermark information. The watermark can be extracted without any distortion, enabling reversible authentication, integrity verification, and content recovery in applications such as medical imaging. A lossless watermarking scheme to recover the original image from the watermark is proposed by Zain and Clarke (2007). The technique has a low distortion level, even having a large payload. Comparison is made between the *SHA-256* of the recovered image to that of the extracted watermark to show that 100% recovery is possible. Lee et al. (2007) propose a reversible watermarking technique based on the Integer-to-Integer *ITI* wavelet transform. The method partitions the input image into non-overlapping blocks and embeds the watermark into the high-frequency wavelet coefficients of each block. Guo and Zhuang (2009) proposed a lossless watermarking technique that does not introduce any distortion in *ROI* during the embedding process. A polygon is chosen as the embedding region for reconstruction, where the polygon's vertex information is carried to the decoder. Integrity and authenticity are achieved by digital signature and identifier of the image.

Sachnev et al. (2009) proposed a reversible watermarking method. Prediction errors (*PE*) are recorded using sorting technique which are then used to embed data. Rhombus prediction scheme along with histogram shift method and sorting is used to produce increased embedding capacity with less distortion and better results. Coltuc (2011) proposed a reversible watermarking method for reducing the embedding distortion of *PE* expansion. The expanded difference is split between the current pixel and its prediction context. Embedding is done at a lower distortion into the current pixel. Luo et al. (2010) proposed a reversible watermarking algorithm that is used to embed large amounts of watermark information into the host image. It uses an interpolation technique for the process. Interpolation error, along with the difference between the interpolation value and the corresponding pixel value, is calculated. Additive expansion is applied to the interpolation errors. High image quality is achieved with greater payload capacity and higher image fidelity.

Naseem et al. (2013) proposes a reversible and fragile watermarking method that employs the residue number system and a chaotic key. Specifically, the technique involves reducing the *ROI* and embedding the hash of the entire image in the *RONI* using the chaotic key and residue of the *ROI*. The watermarking technique is designed to detect tampering based on changes in the hash value. Siddiqa and Khan (2015) described a reversible watermarking method based on prediction error expansion. Embedded information depends on the scale of variation in neighbouring pixel values. A minimum amount of auxiliary information is required thus have high embedding performance, high capacity and less distortion.

The input image is segmented into *RONI* and *ROI* in automatic optimal thresholding method given by Wu et al. (2015a). The authors then applied an improved preprocessing technique to the *ROI* histogram, which expanded peak pairs and allowed for data embedding in the *ROI* and contrast enhancement. A difference matrix is utilized to locate tampered regions, and the experiments demonstrate performance improvement with respect to the contrast enhancement of the *ROI*. In Li et al. (2015), authors propose a data hiding technique that is reversible and efficient. Moreover, The data-hiding technique uses multiple histograms and is based on prediction error expansion. A prediction error histogram is generated through the collectively computed complexity of each pixel based on its context. Multiple histogram modification is then used to embed data with minimum distortion. Wu et al. (2015a) described a reversible data hiding (RDH) algorithm for improving the contrast of the host image. Data is embedded by selecting the highest two bins in the histogram.

Contrast-enhanced images are better preserved using this algorithm. Also, it provides lossless recovery of the original image.

In conclusion, spatial domain watermarking techniques play a crucial role in protecting and authenticating medical images. These techniques enable the direct manipulation of pixel values to embed watermarks, providing simplicity and effectiveness in ensuring the integrity, authenticity, and privacy of medical image data.

2.2 Frequency Domain Watermarking

Digital watermarking has been found to exhibit greater robustness when applied in the frequency domain, as compared to the spatial domain (Cox et al. (1997)). Various transformation techniques can be employed to convert an image from its spatial domain representation to the frequency domain. These techniques include *DCT, DWT, FFT,* Wavelet transform, Laplace transform, Walsh transform, Hadamard transform, among others. These transformations enable the analysis and manipulation of image data in the frequency domain, making them well-suited for effective watermarking applications. Transformation techniques yield, an increase embedding capacity and robustness against many common attacks. However, in comparison to spatial domain embedding, cost of computation is bit more. Naheed et al. (2014) described a reversible watermarking algorithm for improving the watermarking capacity and imperceptibility, which are based on Luo et al. (2010) additive interpolation error expansion algorithm. *GA* and *PSO* are used as techniques to manipulate the correlation of values of image pixels to achieve a better estimation of neighbouring pixel values.

2.2.1 Wavelet Transform based Watermarking in Frequency Domain

In the frequency domain, the wavelet transform provides a representation of the image in terms of frequency components. It decomposes the image into different frequency bands, similar to other frequency-based transforms such as the Fourier transform. This frequency representation captures both low-frequency and high-frequency information in the image. Xuan et al. (2004a) propose a lossless data hiding technique that utilizes the Integer Wavelet Transform (IWT) domain for embedding the data. Xuan et al. (2005) also consider the issue of overflow and underflow in the embedding process and propose a histogram modification technique to address this problem. Kumsawat et al. (2005) proposed watermarking scheme based on spread spectrum using discrete multi-wavelet transform. Genetic Algorithm (GA) optimization is done to improve performance of the algorithm. Embedding strength and threshold values are explored. The proposed method is robust and imperceptible.

In their work, Cruz et al. (2011) explained, the manner in which *ANN* can be modeled using optimization tools, with the ability to learn from a training set, making it useful in pattern recognition applications. Wavelet transforms are used to optimize the *ANN* for image processing, and other mathematical transforms are employed to develop soft computing tools.

Kishore et al. (2015) proposed an efficient watermarking technique in medical images. The medical images for this algorithm are used in the similar manner as an envelope image in the watermarking procedure, which remains visible to everyone on the network with patient images in wavelet domain. *BAT* algorithm is used optimally to perform the embedding process which results high *PSNR* and normalized cross correlation coefficient (NCC) values. *IWT* and Singular Value Decomposition (SVD) are utilized by Luo et al. (2021) for a method to secure multi-scale image

watermarking. The authors claim 0.92 average *NC* values for the Lena image, which is strong robustness, and 45 *d*B of *PSNR* values, which is a very high imperceptibility for multiple watermark sizes.

2.2.2 Discrete Cosine Transform based Watermarking in Frequency Domain

DCT based watermarking in the frequency domain for medical images is a technique that utilizes the frequency components obtained through the *DCT* to embed watermarks. The *DCT* is applied to decompose the image into its frequency coefficients, and the watermark is embedded in the selected *DCT* coefficients. By operating in the frequency domain, the watermark can be embedded and extracted efficiently while taking advantage of the frequency characteristics of the medical image. This approach offers robustness against various attacks and provides effective protection for the integrity and authenticity of medical images. Fakhari et al. (2011) proposed a method to protect patient's information using Wavelet transformation through *GA* and *PSO*. The visual quality of watermarked image and robustness are improved against various attacks in comparison to *DCT* based methods.

2.2.3 Walsh Hadamard Transform based Watermarking in Frequency Domain

The Walsh-Hadamard Transform (WHT) and *FWT* are widely used in the field of medical image watermarking. These transforms offer valuable tools for embedding watermarks into medical images and ensuring their integrity and authenticity. In medical image watermarking, the spatial domain approach is commonly employed, where the watermark is directly embedded into the pixel values of the image. The *WHT* and *FWT* play a crucial role in this process by providing a means to efficiently modify the image's pixel values while preserving the image's diagnostic information. By applying the *WHT* to a medical image, it is transformed into a set of Walsh-Hadamard coefficients, which represent the image's frequency domain characteristics. These coefficients capture different spatial frequency components, ranging from low-frequency to high-frequency information. This transformation allows for the identification and manipulation of specific frequency components, which can be utilized for watermark embedding.

The *FWT* is an algorithmic enhancement of the *WHT*, enabling faster computation and making it suitable for real-time medical image watermarking applications. With its reduced computational complexity, the *FWT* enables efficient embedding of watermarks into medical images without significant computational overhead. In medical image watermarking, the *WHT* and *FWT* can be used to modify selected Walsh-Hadamard coefficients according to the watermark data. By strategically manipulating these coefficients, the watermark can be embedded in a manner that ensures its imperceptibility while maintaining the diagnostic integrity of the medical image. The choice of specific coefficients and the watermarking algorithm employed are critical factors in achieving robust and imperceptible watermarking in medical images. Careful selection of coefficients and proper incorporation of the watermark ensure that the embedded information remains intact, even in the presence of various attacks or image processing operations.

Due to the good energy compaction property of Hadamard, it is used by several techniques in digital watermarking. Bhatnagar and Raman (2009) used *SVD* is used for proposing a multi resolution Walsh Hadamard transformation, which improves both imperceptibility, reversibility and

robustness. *SVD* is used for systematic breakdown of variance and eliminating colinearity. Multi resolution Walsh Hadamard, transforms the host image for the watermark embedding into the singular values at the finest and the coarsest level sub-bands.

2.2.4 Reversible Watermarking in Frequency Domain

Reversible watermarking in the frequency domain is a technique used in medical imaging to embed watermarks in a manner that allows for the complete recovery of the original, unwatermarked image during the extraction process. It operates in the frequency domain, utilizing transform techniques. The goal of reversible watermarking is to embed the watermark while minimizing the distortion introduced to the original image. In the frequency domain, this is achieved by modifying the frequency coefficients in a reversible manner. Reversible watermarking techniques ensure that the original image can be perfectly reconstructed after the extraction of the watermark, without any loss of image quality.

It is particularly useful in medical imaging applications where preserving the integrity and diagnostic value of the image is crucial. It allows for the secure embedding of additional information, such as patient identifiers, study details, or copyright information, while guaranteeing the ability to obtain the original image without any degradation. It offers a balance between watermark capacity and image quality preservation in medical imaging. They enable secure and tamper-resistant communication and storage of medical images, ensuring the authenticity and integrity of the image content while providing opportunities for data protection and ownership verification.

Tian (2003) discusses a reversible watermarking technique, where the original image can be completely restored after watermark extraction. It uses histogram shifting to embed the watermark in the wavelet domain while preserving reversibility. By modifying the histogram of wavelet coefficients, the watermark bits are embedded in the image. Xuan et al. (2004b) presented a reversible data hiding technique that uses a compression and expansion processing pair approach in the IWT domain. The method avoids overflow and underflow issues through histogram modification applied after embedding the data in the high-frequency subbands. This technique achieves low distortion and outperforms the method proposed by Tian (2003). In a separate work, Xuan et al. (2004a) described a lossless data hiding technique based on IWT and the threshold embedding technique. The method uses the LSB to embed the high-frequency CDF (2, 2) low-magnitude value compared to threshold integer wavelet coefficients. The technique also applies histogram modification to prevent overflow/underflow issues.

Xuan et al. (2005) described a lossless data hiding method that uses IWT and threshold embedding technique. Histogram modification is used before embedding to prevent underflow/overflow. The data is first embedded into high-level frequency subbands. Arsalan et al. (2017) proposed a reversible watermarking IRW-Med technique to protect patient's information. The technique uses the concept of companding function to reduce distortion, IWT to achieve reversibility, histogram modification to prevent underflow and overflow and Genetic Programming (GP) to select an intelligent wavelet coefficient. GP can learn itself, thus help in finding suitable tradeoff between the imperceptibility and payload. The method achieves low distortion, finds hidden information and can recover an image.

Lee et al. (2007) introduced an Information Theoretic Index (ITI) wavelet-based reversible watermarking technique.. The method partitions the input image into non-overlapping blocks and embeds the watermark into the high-frequency wavelet coefficients of each block. The approach also includes side information with a small size compared to the embedding capacity, which is added

to the payload along with the message. High embedding capacity and low distortion are achieved through this method.

2.2.5 Ridgelet Transform Watermarking in Frequency Domain

RT watermarking in the frequency domain is a technique used in medical image processing to embed watermarks in medical images by utilizing the *RT*. *RT* is a multi-resolution representation that captures and enhances linear singularities in an image, such as edges and ridges. It is particularly effective in representing highly directional features commonly found in medical images, such as blood vessels or anatomical structures.

It first transformed into the ridgelet domain using the *RT*. The transform decomposes the image into a set of ridgelet coefficients, which capture the local directional information at different scales and orientations. These coefficients represent the image's frequency content in a sparse and directional manner. The selection of the coefficients to modify and the magnitude of the modifications are determined by watermarking algorithms designed to balance the trade-off between watermark invisibility and robustness against attacks. It exploits the directional and sparse nature of medical images, allowing for efficient representation and manipulation of image features. *RT* provides a compact and robust representation that can enhance the watermarking capacity and the watermark's resistance to attacks. Campisi et al. (2004) proposed a multiplicative watermarking scheme for the ridgelet domain. The approach involves performing the *RT* to identify the best direction for embedding the watermark in the corresponding image block with straight edges. The circular harmonic function is then used to obtain an associated edge image by employing filter bank design. This method is highly robust and maintains perceptual invisibility.

Uzun and Amira (2005) proposed Finite Ridgelet Transform (FRIT) method Field Programmable Gate Array (FPGA) implementation for image processing applications. Finite Radon Transform (FRAT) and 1-D Discrete Bi-orthogonal Wavelet Transform (DBWT) are used as building blocks. The paper provides insight into the *FRIT* programming and how the *RT* work. Chen and Kégl (2007) described an image denoising scheme using *RT* combined with dual-tree complex wavelet. Gaussian white noise can be removed by using digital complex *RT*. The method provides better results for denoising than VisuShrink and wiener2, also sharp edges are preserved while removing white noise.

Zhu and Wang (2008) proposed a robust Watermarking Scheme in *FRIT* Domain. Maximum a Posterior (MAP) estimate based on the Laplacian probability distribution function is used to find the most suitable *FRIT* coefficients to embed the watermark. Kalantari et al. (2010) described a robust image watermarking method in *RT*. Ridgelet coefficients representing the most energetic direction are modified to embed watermark data in selected blocks. Watermark extraction is done using the universal optimum decoder. In each block, it uses the variance of the ridgelet coefficients of the most energetic direction. Robust noise estimation method is also proposed to perform decoding by decoder using noise variance.

Sadreazami and Amini (2012) proposed a robust spread spectrum based image watermarking method. *RT* is performed on every image block to show optimal performance for images with line singularities. Blocks having best directions (highest variance intensity) are selected to embed the watermark bits. The method is highly robust against common attacks. Huang et al. (2016) propoed an adaptive digital *RT* multiscale algorithm. Both line and curve information are adaptively dealt by this method by considering its underlying structure first. Wavelet transform is applied to decompose

curve parts into finer scales. Better image denoising is achieved by applying adaptive *RT*.

Ismail and Ali (2023) introduced a quality improvement technique for watermarked videos using the *RT*. The technique aims to improve the visual quality of watermarked videos while preserving the robustness of the watermark. Experimental results demonstrate that this is effective in achieving high-quality watermarked videos with minimal visual distortion. The study suggests that the proposed technique has potential to enhance the performance of watermarking techniques in medical video applications.

2.3 Compressed Domain Watermarking

Compressed domain watermarking in medical images refers to the technique of embedding watermarks directly into the compressed representations of medical images, such as *JPEG* or *DICOM* formats. It takes advantage of the specific characteristics and structures present in compressed medical images to efficiently embed and extract watermarks without the need for full decompression. This approach allows for copyright protection, authentication, and tamper detection of medical image data while minimizing storage requirements and computational complexity.

Dong et al. (2015) introduced an innovative watermarking algorithm that operates in the encrypted domain, incorporating the use of *DCT* and a logistic chaotic map. The algorithm utilizes a zero watermarking technique to ensure the authenticity and integrity of medical images. By working in the encrypted domain, the algorithm aims to maintain the security and confidentiality of the original medical image while providing robust watermarking capabilities. The utilization of *DCT* and the logistic chaotic map indicates the adoption of frequency domain-based techniques, where the watermark is embedded within the transformed coefficients.

Haddad et al. (2020) proposed a unique scheme that integrates watermarking, encryption, and compression to safeguard medical images. Unlike conventional methods, this scheme allows access to watermarking-based security services from encrypted and compressed image bitstreams without requiring decryption or decompression. It employs bit substitution watermarking modulation, *JPEG-LS* compression, and *AES* block cipher encryption in *CBC* mode. The scheme adheres to the medical image standard *DICOM*, enabling image tracing, integrity and authenticity verification, and control of image reliability in encrypted and compressed domains. Experimental results on Retina and ultrasound medical images demonstrate the scheme's ability to securely transmit messages while minimizing image distortion. Furthermore, the scheme has the capacity to support multiple security services simultaneously.

Li et al. (2022) tackle the issue of copyright protection in multimedia data transmission within the context of integrated data sensing, communication, and computing for the *IoT*. They propose a robust reversible watermarking algorithm that operates in the compression domain. The algorithm employs multilayer embedding techniques, where a robust watermark is embedded in mid-frequency coefficients. Additionally, auxiliary information is incorporated to facilitate the reverting of the embedding process in high-frequency coefficients. To enhance the algorithm's performance, a coefficient selection method is introduced, taking into account the complexity of texture. Experimental results showcase the superior performance of the proposed algorithm when compared to existing reversible robust watermarking methods.

2.4 Hybrid Domain Watermarking

Hybrid domain watermarking in medical images involves the integration of two or more distinct domains, such as spatial, frequency, or compressed domains, to embed and extract watermarks. By leveraging the strengths of multiple domains, hybrid domain watermarking aims to achieve enhanced robustness, imperceptibility, and security in medical image protection. This approach combines the advantages of different domains to create a more effective and adaptable watermarking technique for applications such as copyright protection, content authentication, data integrity verification, tamper detection and localization in medical imaging.

Acharya et al. (2004) enhanced their interleaving process specifically for *JPEG* standard of image storage. Spatial domain watermarking technique along with Frequency domain watermarking is tested. *DCT* coefficients are selected and the *LSB* are replaced by the watermark data bits for embedding. The test result of interleaving process shows that normalized root mean square error (NRMSE) is less than 5%. Alvarez et al. (2007) gives a method for medical images, to obtain a secure system for storage and transmission interleaved with patients' data. Standard encryption algorithms such as Triple data encryption standard (DES), *AES etc.* are used to further strengthen the interleaving process.

Khor et al. (2016) presented a watermarking technique for medical images using multiple frames. To optimize processing time, the technique employed multicores technology. Experimental results showed that parallel watermarking processing significantly reduced the elapsed time compared to sequential processing, while maintaining imperceptibility and robustness. The utilization of parallel processing techniques is a characteristic of hybrid watermarking approaches, which aim to leverage the strengths of different domains or technologies to achieve improved performance. Giakoumaki et al. (2006a) described a method to simultaneously protect, retrieve, and authenticate the source and data. Multiple watermarks are embedded to achieve efficiency and transparency.

2.4.1 Wavelet based Watermarking in Hybrid Domain

Wavelet-based watermarking in the hybrid domain refers to a technique that combines the advantages of both wavelet transform and another domain, such as spatial, frequency, or compressed domain, to embed and extract watermarks in medical images. Wavelet transforms are applied to decompose the image into different frequency bands, allowing for efficient embedding of the watermark in the selected domain. This hybrid approach aims to achieve robustness against various attacks, while maintaining the desired level of imperceptibility and preserving the diagnostic information in medical images. Usman et al. (2009) described a lossless data hiding method based on intelligent coefficient selection scheme using *GP* and *IWT*. Least significant bit-plane having high-frequency wavelet coefficients selected via *GP* module is used to embed the information.

Sharma et al. (2015) presented a watermark embedding technique that employed wavelet transform. The cover and watermark images were transformed to the frequency domain using the first-level *DWT*. From the watermark image, the *LL* subband was selected and processed using modulus functions. To address patient identity theft concerns in telemedicine, the watermarked image underwent encryption using stream cipher cryptographic techniques, providing two levels of security. This approach combined frequency domain-based embedding (wavelet transform) with encrypted domain-based security (stream cipher encryption), aiming to enhance the security of watermarking in telemedicine applications.

Mohananthini and Yamuna (2015) introduced an algorithm for watermarking using the *DWT* and *SVD*. The algorithm decomposed the Red Green Blue (RGB) components of original images into two-level *LL* subbands using *SVD*. The watermark incorporated various patient information, including identification number, name, age, sex, diagnosis, treatment details, and doctor's signature. The algorithm exhibited favorable performance in the presence of salt and pepper noise, robustness, Gaussian noise, Gaussian blur, median filtering, *JPEG* compression with a quality of 50, rotation, smoothening, sharpening, intensity transformation, and row-column blanking.

In their research, Shaji and Prakash (2015) introduced a distinctive method for enhancing the security of medical images using Chaos Game Representation (CGR). This approach ensures image integrity by treating the image as a series of numbers in the *CGR* algorithm, which serves as an alternative to traditional hashing algorithms. The *CGR* watermark is then embedded into the medical image using the *DWT* algorithm. As *DWT* is a reversible technique, the original medical image can be restored at the receiver's end without any distortion. This combination of *CGR* and *DWT* provides a unique and effective approach to watermarking, with *CGR* operating in the spatial domain while *DWT* operates in the frequency domain.

2.4.2 ROI/RONI based Watermarking in Hybrid Domain

ROI/RONI-based watermarking in the hybrid domain refers to a technique that focuses on embedding and extracting watermarks specifically in *ROI* or *RONI* in medical images. These regions are identified based on their importance in preserving diagnostic information or protecting sensitive data. By incorporating the hybrid domain, such as spatial, frequency, or compressed domain, the watermarking process can be optimized to achieve targeted embedding and extraction in specific regions, ensuring both robustness and preservation of important information in medical images. Shih and Wu (2005) described a robust watermarking technique. In this, the watermark is embedded using improved genetic algorithms in *ROI* of the image. A fragile watermark is embedded in the frequency domain in *RONI* part to detect the unauthorized modification.

Giakoumaki et al. (2006b) proposed a watermarking technique based on multiple watermarks using wavelet transform. *ROI* of the image is protected along with authentication and retrieval of data. Hybrid coding is used to increase robustness.

A hybrid watermarking approach for *DICOM* images is introduced by Al-Qershi and Khoo (2011), in which difference expansion is used to enclose patient's data in the *ROI*, while *RONI* is used to embed recovery data and data for tamper detection using *DWT*. The proposed technique ensures complete retrieval 100% of the *ROI*.

Al-Qershi and Khoo (2011) presented a method for watermarking *DICOM* images that utilize a hybrid approach. The patient data is embedded in the *ROI* through difference expansion. In contrast, the tamper detection and recovery data is embedded in the *RONI* using *DWT*. This technique ensures the complete retrieval of 100% of the *ROI*.

Shih and Zhong (2016) gives a method of allowing multiple *ROI* to be selected for data preservation and kept lossless, and all regions of non-interest are used for digital watermarking. High capacity is achieved using *DCT* coefficients, in embedding of secret data.

2.4.3 Tamper Detection based Watermarking in Hybrid Domain

Tamper detection-based watermarking in the hybrid domain is a technique that aims to detect and localize tampering or unauthorized modifications in medical images. It combines the advantages of

watermarking in multiple domains, such as spatial, frequency, or compressed domain, to enhance the detection accuracy and robustness. By embedding tamper-evident watermarks that are sensitive to image alterations, this approach enables the identification of tampered regions and provides an additional layer of security for medical image integrity. The hybrid domain nature of this watermarking technique allows for efficient and reliable tamper detection, enabling the detection of both subtle and severe image manipulations. In order to prevent unauthorized disclosure of patient information, Woo et al. (2005) proposed multiple watermarking techniques that embed both fragile and annotation watermarks in the image for tamper detection and privacy control, respectively.

Thabit and Khoo (2017) presented a combination of recovery and data-hiding techniques with tamper detection. The technique embeds data in the *ROI* and *RONI* using the *SLT* algorithm. Moreover, the presented technique is robust against multiple attacks, including salt, pepper noise, and *JPEG* compression. The *IWT* coefficient is utilized in order to recover the information from the *ROI*.

2.4.4 Reversible Watermarking in Hybrid Domain

Reversible watermarking in the hybrid domain is a technique that allows for the embedding and extraction of watermarks in medical images while maintaining the original image data integrity. It combines the benefits of reversible watermarking, where the original image can be perfectly restored after watermark extraction, with the advantages of the hybrid domain, such as spatial, frequency, or compressed domain. This approach ensures that the embedded watermark does not cause any irreversible changes to the image, enabling both watermark detection and accurate restoration of the original image without any loss of information. It is particularly useful in applications where reversible watermarking and hybrid domain techniques are required to balance data integrity and watermark robustness. Chiang et al. (2008) introduced a lossless data embedding method that includes two detection and restoration systems. One of the systems allows for complete restoration of the image, while the other system only restores the *ROI* with improved visual quality. While the first system can recover an almost identical original image, the second system can recover the *ROI* without any loss.

Al-Qershi and Khoo (2009) described a lossless watermarking technique for *DICOM* images. *ROI* is embedded with patient data while *RONI* is embedded with recovery data as a watermark. Without tampering, 100% recovery is possible. However, with tampering, localization of tampered area is done in *ROI*, and a good quality image is extracted. Arsalan et al. (2012) described an intelligent reversible watermarking method Genetic Algorithm-based Reversible Watermarking (GA-RevWM). *GA* and *IWT* are the basis of *GA-RevWM* approach. Higher *PSNR* is achieved in a given effective payload using controlled threshold value. Lei et al. (2014) proposed a reversible watermarking method that provides a secure environment for transmission of medical images. Original image is embedded with signature information and textual data based on the recursive dither modulation (RDM) algorithm. *SVD*, *WT* is applied before *RDM* algorithm. The strength of the watermark is controlled using Differential Evolution (DE) by designing quantization steps (QSs). The method is highly robust and imperceptible.

The article by Mao et al. (2015) proposes a reversible watermarking technique with a high payload, which generates high-quality images. In their work, an embedding algorithm is introduced called distortion-oriented minimized (DOM), specifically focusing on minimizing distortion. Moreover, the authors use the Cascading Trellis Coding (CTC) algorithm further to reduce alterations to the host

coefficients as a whole. By using this approach, certain designated host coefficients are maintained unchanged. To achieve reversibility with high quality, they utilize scaling and wavelet coefficients in conjunction with the *DOM* and cascading trellis coding algorithm while avoiding overflow and underflow issues. Wu et al. (2015b) proposed a *RDH* method similar to Wu et al. (2015a) for medical images. In this, the primary grey-scale values are identified by performing background segmentation. The contrast of *ROI* is selectively enhanced. The original image is recovered 100% with side information hidden within the watermarked image.

A technique proposed in Xiao et al. (2015) for reversible image authentication uses two watermarks and Compressive Sensing (CS). The two watermarks used in the technique are classified as short and long. In order to authenticate image integrity as perception Hash, the short watermark is used, whereas in order to do recovery and tamper localization, the long watermark is utilized. Moreover, the authors modified the discrete Haar wavelet coefficient's histogram for embedding purposes. In order to recover the image, a short watermark is performed. Once the authentication is achieved, the image is completely recovered with a success rate of 100%. On the other hand, in order to recover and tamper the localization of the image. The long watermark is used if the authentication fails.

2.4.5 Discrete Cosine Transform based Watermarking in Hybrid Domain

DCT based watermarking in the hybrid domain for medical images is a technique that combines the *DCT* with the advantages of the hybrid domain. The *DCT* is applied to decompose the image into frequency components, and the watermark is embedded in the selected *DCT* coefficients. By operating in the hybrid domain, the watermark can be embedded and extracted efficiently while preserving the frequency characteristics of the medical image. This approach offers robustness against various attacks and provides effective protection for medical image integrity and authenticity. Rayachoti (2023) demonstrate a watermarking technique for telemedicine that is both robust and has a high embedding capacity. The technique combines the *DCT* and *SVD* to embed a watermark in the telemedicine image. Experimental results demonstrate that the proposed technique achieves high robustness against various attacks and has a high embedding capacity, indicating its potential to improve the security of telemedicine applications.

2.4.6 Ridgelet Trasnform Watermarking in Hybrid Domain

RT watermarking in the hybrid domain for medical images is a technique that combines the *RT* with the advantages of the hybrid domain. The *RT* is applied to the image to capture the directional information and enhance the representation of medical features. By incorporating the *RT* into the hybrid domain, the watermark can be embedded and extracted efficiently while preserving the directional characteristics of the medical image. This approach enables robust watermarking that can withstand various attacks and provides effective protection for medical image integrity and authenticity. Yang et al. (2008) combined *RT* with feed Forward Neural Network (FNN). Ridgelet act as an activation function, and structure is determined using an incremental constructive method. *GA* is used to determine the ridgelet neuron's optimal directions.

Mangaiyarkarasi and Arulselvi (2011) described robust watermarking scheme based on *RT*. In this scheme, extraction is done using Independent Component Analysis (ICA) which uses blind source separation technique to extract the watermark in a spatial domain directly without using any transformation process and original image. Liu et al. (2022) proposes a secure watermarking algorithm for medical images that combines ridgelet-*DCT* and Tent-Henon-Map (THM) double

chaos. The algorithm encrypts the original medical image with *THM* double chaos and embeds a watermark using the ridgelet-*DCT* transform. The results of experiments demonstrate the high robustness of the algorithm against various attacks, such as compression, filtering, and cropping. These findings suggest that the proposed algorithm has the potential to enhance the security of medical image transmission and storage.

2.5 Gaps in Medical Image Watermarking

While medical image watermarking techniques have made significant progress, there are still some gaps and challenges that researchers and developers continue to address. Some of the key gaps in medical image watermarking from literature survey include:

1. **Robustness:** Medical images often undergo various transformations and processing steps, such as compression, cropping, filtering, and enhancement. Watermarking techniques need to be robust enough to withstand these operations without significant degradation or loss of the embedded watermark. Ensuring robustness in the presence of common medical image manipulations remains a challenge.

2. **Security:** Medical image watermarking should provide robust security to protect patient privacy and sensitive medical information. Unauthorized access, tampering, or removal of watermarks should be prevented to maintain the integrity and authenticity of the medical images. Strengthening the security measures in medical image watermarking techniques is crucial to safeguard patient data.

3. **Capacity and Efficiency:** Medical images often contain large amounts of data, requiring watermarking techniques with sufficient capacity to embed meaningful information without compromising the image quality. The challenge lies in developing efficient and scalable algorithms that can handle the high data volumes of medical images while maintaining acceptable performance.

4. **Clinical Relevance and Interpretability:** Medical image watermarks should be designed in a way that does not interfere with the clinical interpretation of the images. Watermarks should be unobtrusive and should not affect the diagnostic quality or visual perception of the medical images. Ensuring that watermarks do not introduce any false positives or negatives in medical diagnosis is a critical aspect to consider.

5. **Standardization and Interoperability:** There is a lack of standardized watermarking techniques and formats specifically tailored for medical images. Interoperability among different systems, software, and devices is essential to ensure seamless integration and compatibility. Establishing standardized protocols and formats for medical image watermarking would enhance interoperability and promote widespread adoption.

6. **Ethical and Legal Considerations:** Medical image watermarking should comply with ethical and legal regulations regarding patient privacy, data protection, and copyright. It is important to address legal aspects, such as intellectual property rights and ownership of watermarked medical images, to ensure proper usage and adherence to legal frameworks.

Addressing these gaps in medical image watermarking requires ongoing research and development efforts. Collaborative work between researchers, healthcare professionals, and regulatory bodies can

help overcome these challenges and advance the field of medical image watermarking. This research work is done to contribute in the same.

2.6 Objectives of the thesis

On the basis of gaps identified in the literature survey, following objectives are proposed for this work.

1. To review existing watermarking techniques.
2. To develop efficient watermarking technique(s) for medical images.
3. To validate and compare developed techniques(s) with existing medical watermarking techniques.

2.7 Methodology

- **Literature Review:** Conduct an extensive review of the existing literature on medical watermarking techniques, data compression, image feature extraction, security, tamper detection, and related areas. Identify the limitations and challenges in the field and explore the state-of-the-art methods and technologies.
- **Data Collection:** Gather a diverse dataset of medical images from reliable sources that cover various modalities and imaging techniques. Ensure the dataset represents a wide range of medical conditions and imaging scenarios to provide a comprehensive evaluation of the proposed techniques.
- **Feature Extraction and Transform Techniques:** Implement the *SLT*, *FWT*, *ANN*, *PSO* and *RT* algorithms. Develop modules or utilize existing libraries to perform image feature extraction using *SLT* and explore the capabilities of *FWT* and *RT* in image compression and feature preservation. Verify the suitability and effectiveness of these techniques for medical image watermarking.
- **Watermark Embedding and Extraction:** Design and implement the watermark embedding and extraction algorithms based on the selected transforms (*SLT*, *FWT*, *RT*) and RS vector embedding. Develop the necessary techniques to ensure robust and secure embedding, imperceptibility, and authentication. Implement the necessary modules to handle cryptographic algorithms, compression algorithms and biometric thumbprints for enhanced security (e.g., *MD5*, *AES*, *SHA-3*, Lempel-Ziv-Welch (LZW).
- **Performance Evaluation:** Define performance metrics such as *NC*, *SIM*, *SNR*, *PSNR*, *bpp*, and time complexity. Evaluate and compare the proposed watermarking techniques with existing methods using the collected dataset and performance metrics. Analyze the results to demonstrate the superiority and effectiveness of the proposed techniques.
- **Experimental Validation:** Conduct extensive experiments to validate the proposed techniques. Evaluate the embedding capacity, security, robustness against attacks, imperceptibility, tamper detection, and recovery capabilities. Generate visual quality assessments and conduct statistical analyses to validate the improvements achieved by the proposed methods.

- **Real-Time Implementation and Optimization:** Implement the proposed techniques in a real-time environment, considering the computational requirements and execution time constraints. Optimize the algorithms and procedures to achieve efficient and practical implementations suitable for real-time medical imaging applications.
- **Discussion and Interpretation:** Analyze and interpret the results obtained from the experiments and evaluations. Discuss the strengths and limitations of the proposed techniques and provide insights into the potential applications and future directions. Provide recommendations for further research and development.

Chapter 3

Slantlet based Hybrid Watermarking Technique for Medical Images

3.1 Introduction

This chapter introduces a novel reversible robust hybrid watermarking technique specifically designed for medical images, with the aim of supporting *MIS* and *HIS*. The proposed technique addresses the limitations and challenges associated with existing watermarking techniques in medical imaging.

The research proposes a watermarking technique that offers high efficiency in terms of source and patient authentication, medical image integrity, and patient information confidentiality. It provides services such as source and patient authentication, medical image integrity, and patient information confidentiality. The technique is reversible, allowing for the retrieval of the original medical image and watermark without distortion.

Existing watermarking techniques for medical images face constraints due to the critical nature of medical image data and the need to prevent data tampering. These techniques often suffer from limitations such as insufficient embedding capacity, vulnerability to network attacks, inadequate watermark recovery, low *BER*, limited applicability to color images, lack of protection for the *ROI*, inability to recover corrupted watermarks, and compromised invisibility [1].

To address these limitations, the proposed technique focuses on enhancing watermark security, robustness, invisibility, and embedding capacity simultaneously. It incorporates the *SLT* for data embedding, which increases the energy percentage of the compressed image/signal, thereby enhancing the embedding capacity. *SLT* outperforms other transformations like *DWT* and *DCT* in noise removal and compression performance, resulting in improved *BER*.

Additionally, the technique utilizes the *RS* vector for hybrid embedding, which increases the embedding capacity and security. The use of *SLT*, which employs three filters, contributes to the high robustness of the technique. Moreover, the proposed technique demonstrates reduced execution time and improved visual quality and smoothness of watermarked images.

Security concerns are extensively addressed through the implementation of techniques such as *MD5*, *AES*, and biometric thumbprints of patients. The proposed technique also provides tamper detection and localization capabilities.

Experimental results validate the effectiveness of the proposed technique, showing superior performance in terms of correlation, *SIM, SNR, PSNR, BPP*, and time complexity compared to existing techniques.

By addressing the limitations and challenges of existing watermarking techniques and achieving the desired objectives, the proposed technique contributes to the advancement of medical image watermarking, providing enhanced data integrity and security for medical information systems. The

[1] **Contents of the work presented in this chapter have been published in *Multimedia Tools and Applications*, Vol. 77, pp. 12493–12518, 2017 (SCI Indexed)**

chapter is structured as: Section 3.2, the proposed medical image authentication technique is described and in Section 3.3, the experimental results are illustrated. Finally in section 3.4, the proposed work is concluded.

3.2 Proposed Watermarking Technique

In this section, review of *SLT*, watermark creation algorithm, embedding algorithm, extraction algorithm, overflow and underflow handling process are discussed.

3.2.1 Slantlet Transform

The *DWT* has found applications in various fields due to its effectiveness in describing piecewise smooth signals. However, its performance can be enhanced by focusing on two important criteria: time-localization and smoothness characteristics. To strike a balance between these criteria, Selesnick (1998), Selesnick (1999) introduced the *SLT* as an alternative form of the *DWT*. The *SLT* offers improved time-localization and smoother properties by controlling the lengths of discrete-time basis functions and their moments. It provides a viable solution for achieving a better trade-off between time-localization and smoothness compared to the conventional *DWT*.

The *SLT* utilizes the equivalent form of the filter bank representation of the DWT to determine the filter coefficients. The 2-scale filter banks, as shown in Figure 3.1, are employed in this process. The *SLT* filter bank is implemented using a parallel structure, and it uses different filters instead of filter products. As a result, the filters used in the *SLT* filter bank have shorter lengths compared to those used in the traditional *DWT*.

The purpose of implementing the *SLT* matrix Selesnick (1999) was to demonstrate the orthogonality of this transform. In this research technique, inspired by Mulcahy's image transformation method Mulcahy (1997), the matrix is employed to calculate the *SLT* of image blocks, deviating from the conventional *SLT* approach. By utilizing the *SLT* matrix, the researchers aimed to examine and confirm the orthogonality properties of the transform.

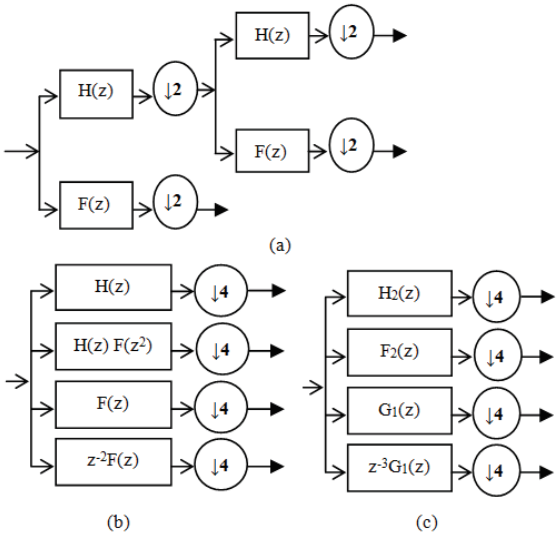


Figure 3.1: Decomposition structures for: (a) DWT, (b) equivalent structure of DWT, and (c) SLT.

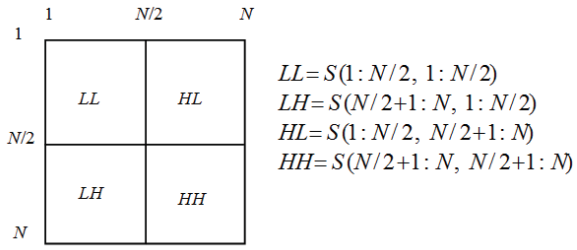


Figure 3.2: Decomposition of the SLT coefficients into 4-subbands.

$$S = SLT_N \ \mathbf{s} \ SLT_N^T \tag{3.1}$$

The SLT of the original signal, represented as S, is obtained using an $N \times N$ Slantlet matrix denoted as SLT_N. It is worth noting that s, S, and SLT_N have the same size. The SLT coefficients in the matrix S are divided into four subbands: LL, HL, LH, and HH, as illustrated in Figure 3.2. This approach is employed to extract the SLT coefficients for each image block in the process. The inverse SLT transform (ISLT) can be obtained by:

$$s = SLT_N^T \ \mathbf{S} \ SLT_N \tag{3.2}$$

The SLT has been widely utilized in diverse applications, consistently showcasing superior performance compared to previous methods specific to each application. For example, in studies conducted by Selesnick (1998, 1999), the SLT was employed as an alternative to the DWT for noise reduction in signals. The results demonstrated that the SLT outperformed the DWT in terms of noise removal, highlighting its effectiveness in this particular application.

The study conducted by Panda et al. (2002) demonstrated that the SLT outperformed the DCT and DWT methods in signal compression. It was observed that the SLT-based algorithm retained a higher percentage of energy in the compressed image or signal compared to the DWT approach. Similarly, in the research by Mutt and Kumar (2009), the SLT was employed in a steganography scheme and exhibited superior performance in terms of both the visual quality of the stego-image and the execution time of the algorithm compared to the DWT.

The utilization of the SLT after applying Eqs. 3.1 and 3.2 in signal classification systems was investigated in the studies by Abou-Loukh et al. (2010); Abou-Loukh and Gatea (2011). The findings demonstrated the superiority of SLT-based schemes over DWT-based schemes in terms of signal classification accuracy. Similarly, in the field of image watermarking, the SLT outperformed DWT-based schemes in terms of visual quality and robustness, as indicated in the works of Mohammed and Khoo (2012) and Lafta and Alwan (2011). The research by Mohammed and Khoo (2012) specifically presents a preliminary study on SLT, highlighting a robust irreversible image watermarking method. The reversible watermarking methods in the transform domain are based on the integer wavelet transform An et al. (2012), Xuan et al. (2002), Xuan et al. (2005), Xuan et al. (2006), Xuan et al. (2009), Mohanty (1999), Zou et al. (2004).

In the study by Thabit and Khoo (2014), a robust reversible watermarking scheme based on the SLT is proposed. The algorithm divides the image into non-overlapping blocks and applies the SLT matrix for block transformation. A high frequency subband (either HL or LH) is chosen to carry the watermark bits. The algorithm scans the blocks to identify the maximum mean value

Figure 3.3: Biometric watermark with MD5

PATIENT ID: DANILKRVII6114
ADDRESS: 37 DEFENCE COLONY ROOP NAGAR INDIA
HOSPITAL ID: 1312SUJATA2412SUM
HOSPITAL NAME: CH. SUBE SINGH HOSPITAL
DOCTOR ID: 3219SAHIL0401
DISEASE: MRI SCAN FOR TUMOUR SIGNS

Figure 3.4: "Text Watermark".

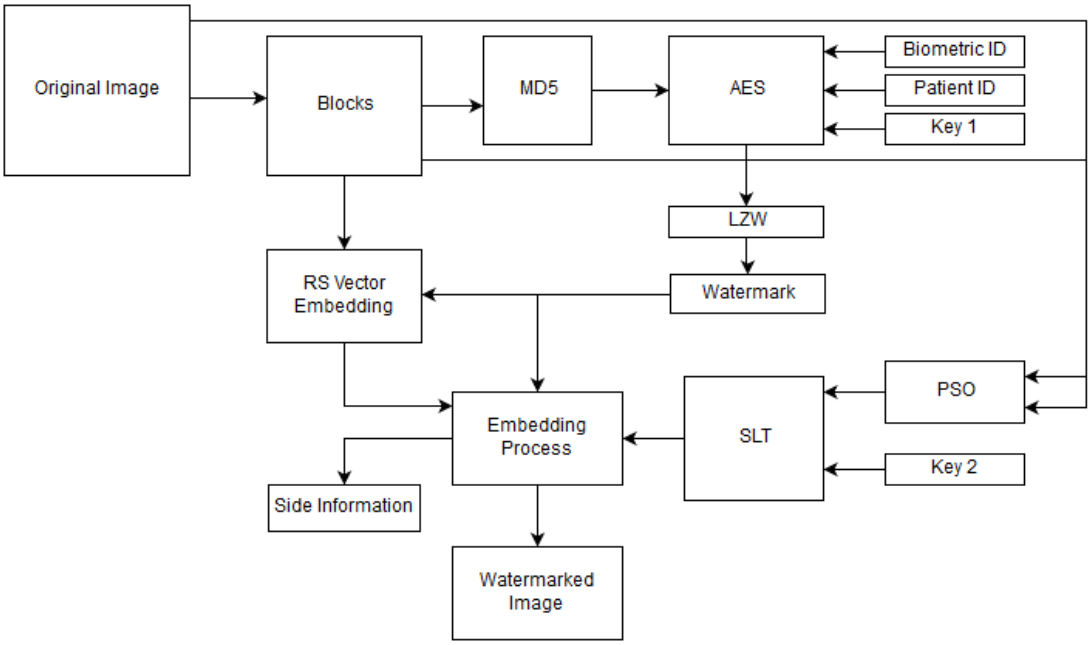


Figure 3.5: Proposed Watermark embedding technique.

of the carrier subband, which is used to set a threshold value. A pre-processing step is performed on the original image blocks using this threshold value before the watermark embedding process. During embedding, if the watermark bit is '1', the mean value of the carrier subband is shifted by the same value used in the pre-processing step. At the receiver side, the mean value of the carrier subband is compared to the threshold value to extract the watermark bits. The scheme in Thabit and Khoo (2014) demonstrates improved performance compared to previous methods. However, there is room for further improvement in terms of capacity and visual quality. It is worth noting that the pre-processing step employed in the scheme may degrade the visual quality of the watermarked image, especially for medical images. Furthermore, the watermark embedding method based on the maximum mean value sets limitations on the capacity of the scheme. Future research is required to address these limitations and enhance the overall performance of the watermarking scheme.

Step 1. **Division of Original image**: The original image is divided into non-overlapping blocks (NB) of 8×8.

Step 2. **Apply MD5**: Apply Message-Digest algorithm 5 on each block of original image for 128-bit resulting hash value Rivest (1992). An example of *MD5* encryption of biometric thumbprint is shown is Figure 3.4.

Step 3. **Apply AES**: Apply 14 rounds of *AES* with key size of 256 bits on the output of Step 2 along with the concatenation of patient's biometric *ID*, key1 and patient *ID* (Figure 3.5).A round has several processing steps which includes transposition, substitution, mixing of the input plaintext and transform it into the final output of cipher text.

3.2.2 Watermark Creation Algorithm

In this subsection, the algorithm used to generate the watermark is explained:

Step 4. **LZW**: Apply *LZW* on the output of Step 3 to compress the watermark bits. Lempel *et al.* Welch (1984) described *LZW* as a table-based lookup algorithm used to compress file into smaller files.

Step 5. **Watermark**: The output from step 4 is the final watermark.

3.2.3 Watermark Embedding Algorithm

The watermark embedding algorithm, shown in Figure 3.3, is summarized in the following steps:

Step 1. **Division of Original image:** The original image is divided into non-overlapping blocks, NB_i, where i is the index of the block. Each of these blocks are transformed by using *SLT* Eq. (3.1) to get four subbands- *HH*, *HL*, *LH* and *LL*. High frequency subbands *HL* and *LH* are used for the watermark embedding in proposed technique.

Step 2. **Calculating the threshold value:** *PSO* (Eberhart and Kennedy Kennedy and Eberhart (1995)) is used for calculating threshold *Th*, for each and every block and T for the whole image, by using the following Eqs. (3.3) and (3.4).

$$V_i^{k+1} = (w \times V_i^k) + (c_1 \times rand_1(....) \times x \times (pbest_i - s_i^k)) + (c_2 \times rand_2(....) \times x \times (gbest - s_i^k)) \tag{3.3}$$

$$s_i^{k+1} = s_i^k + V_i^{k+1} \tag{3.4}$$

where, V_i^k : velocity of agent i at iteration k,
w: weighting function,
c_j: weighting factor,
rand : uniformly distributed random number between 0 and 1,
s_i^k : current position of agent i at iteration k,
$pbest_i$: pbest of agent i,
gbest: gbest of the group.

Step 3. **Embedding watermark:** To embed a watermark bit in each selected block, the mean values of the *SLT* coefficients in the high frequency subbands (*HL* and *LH*) are modified. If the watermark bit is '1', the mean value of the *HL* subband is increased compared to the *LH* subband. Conversely, if the watermark bit is '0', the mean value of the *LH* subband is increased compared to the *HL* subband.

Let's consider a watermark sequence (w) as a vector of bits w = [w_1,...,w_j,...,w_{len}], where j ranges from 1 to *len* and *len* represents the length of the watermark sequence. To embed a specific watermark bit *wj* in a block, the previously determined threshold T (from step 2) is

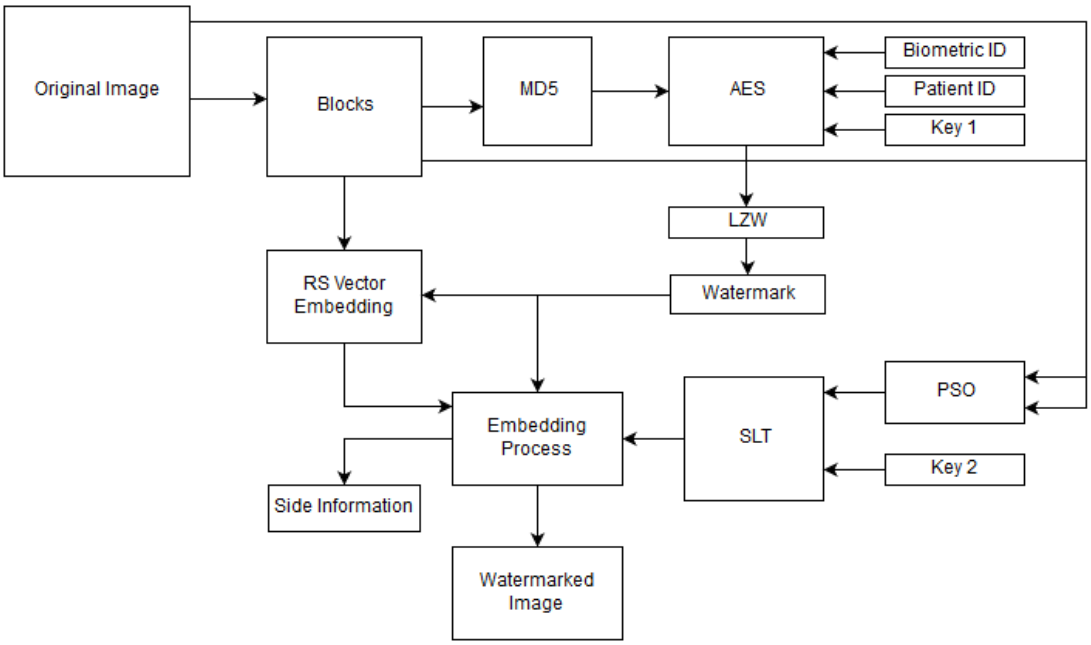


Figure 3.6: Proposed Watermark embedding technique.

used along with the alteration factors specified in Eqs. (3.5) (3.6). The following rules define the embedding process:

If w_j=1 and (μ^{HL} - μ^{LH}) ≥T, then the block remains unchanged.
If w_j=1 and (μ^{HL} - μ^{LH}) <T, then $\mu^{HL}_{new} = \mu^{HL} + A_1$ and $\mu^{LH}_{new} = \mu^{LH}$ - A_1.
If w_j=0 and (μ^{LH} - μ^{HL})≥T, then the block remains without change.
If w_j=0 and (μ^{LH} - μ^{HL}) <T, then $\mu^{HL}_{new} = \mu^{HL}$ - A_2 and $\mu^{HL}_{new} = \mu^{HL} + A_2$
Alteration factors,A_1 andA_2, have been calculated as

$$A_1 = [T - (\mu^{HL} - \mu^{LH}]/(2 \times Th) \tag{3.5}$$

$$A_2 = [T - (\mu^{LH} - \mu^{HL})]/(2 \times Th) \tag{3.6}$$

Because of the reversibility requirements, the difference between the mean values of selected subbands will be saved as side information when the mean values are changed to embed the watermark bit.

Step 4. **Applying the ISLT**: The process of watermark embedding is executed until all the watermarked bits are embedded. The original subbands are substituted by the modified subbands and *ISLT* is applied through matrix multiplication process by in Eq. (3.2). Now, to ensure the reversibility, the resulted output must be rounded up to integer numbers. Thus, the original image and the watermarked image can be resynthesized exactly the same at the receiver end.

Step 5. **Embedding through RS vector:** The image is partitioned into sets of four pixels, treating each set as a single value. Prior to creating these sets, it is necessary to define the Discrimination and Flipping functions.

The Discrimination Function (f) is employed to represent the state of each set, and its calcu-

lation is as follows:

$$f(group) = \sum_{i=1}^{i=3} |x_{i+1} - x_i| \tag{3.7}$$

Where: Group = $\{x_1, x_2, x_3, x_4\}$, x_i is the value of the pixel i in the current group.
The Flipping function is utilized to alter the pixel value by flipping the *LSB* of the two middle pixels within each block. The Discrimination function is then computed for each group before (fr) and after (fs) applying the flipping function. The state of each group is determined as follows, using Eq. (3.7) :
RG Group: if $fs > fr$
SG Group: if $fs < fs$
UG Group: if $fs = fr$
The RS Vector is generated by assigning a single value to each group of pixels in the image. Regular groups (RG) have a watermark bit '1' embedded, while Singular groups (SG) have a watermark bit '0' embedded. Unused groups (UG) are disregarded as they are unaffected by the flipping function. The resulting *RS* Vector is a sequence of bits, representing the states of the pixel groups in the image. It comprises zeros and ones, indicating the presence or absence of watermarking in each group. Finally, the watermarked image is created by combining the pixel groups with the corresponding side information, resulting in the embedded watermark.

3.2.4 Handling the Overflow and Underflow

To handle the issue of underflow and overflow in pixel values during the watermark embedding process, previous methods have employed histogram modification techniques Thabit and Khoo (2014), Thodi and Rodríguez (2007). These techniques involve narrowing the image histogram from both ends before embedding the watermark. This approach has been commonly used in various watermarking techniques. However, a new and enhanced approach was proposed to address this problem. Instead of applying histogram modification as a pre-processing step, the modification is performed only when necessary. This optimized histogram modification process ensures that pixel values are adjusted only if they exceed the desired range Tian (2003). In this method, the modified pixel values are stored as side information and transmitted along with the watermarked image to the receiver. This allows the receiver to accurately extract the watermark by utilizing the side information to restore the original pixel values. This approach enhances the overall performance and reversibility of the watermarking technique.

In a study by Coatrieux et al. (2000), an investigation was conducted on the impact of modifying wavelet coefficients on pixel values, specifically focusing on selecting the highest scale pixel change. This led to the development of a pixel adjustment method to address issues of underflow and overflow in pixel values before the watermark embedding process. Instead of using pixel adjustment as a preprocessing or post-processing step, the proposed technique incorporates it as a side-processing step during the watermark embedding process itself.

This approach avoids the degradation of visual quality caused by the shifting process involved in traditional methods. By integrating pixel adjustment within the watermark embedding process, the proposed technique aims to improve the overall visual quality of the watermarked image.

In the proposed technique, the watermark embedding process takes into account the specific pixel values that experience overflow or underflow. These problematic pixel values are adjusted to ensure

the effective application of the desired watermarking formulae. By making these adjustments, the visual quality of the watermarked image is improved. The adjusted pixel values and their associated information are saved as part of the side information. This approach ensures that the watermarking process is performed accurately while preserving the visual integrity of the image.

$$Iw(i,j) = \begin{cases} 255 & if \quad Iw(i,j)>255 \\ 0 & if \quad Iw(i,j) < 0 \end{cases}$$

The total overhead of the algorithm consists of several components, including Key1, Key2, the block size, the difference in mean values of the blocks, and the number of bits in overflow/underflow. The size of the side information depends on the image size and watermark size, and is inversely proportional to the number of blocks NB_i. For example, in the case of a 512×512 image with a block size of 4×4, the side information is approximately 2096 bytes. This side information, along with the block size, needs to be transmitted alongside the watermarked image to the receiver. The variations in total overhead are illustrated in Table 3.6 using the original image (4) from Table 3.1 as an example.

3.2.5 Watermark Extraction Algorithm

Step 1. **Dividing the image:** At receiver's side, firstly read the watermarked image along with the side information and then the pixels that were adjusted are relocated back to their original locations. Now, non-overlapping blocks are formed from the watermarked image.

Step 2. **Applying SLT:** Transform each and every block by using *SLT* to obtain its subbands.

Step 3. **Extraction of SLT based Watermark:** For each and every block, the coefficient mean values in the high frequency subbands *i.e.* *HL* and *LH* are calculated and the desired watermark bits are extracted according to the following equations:
$w_j^* = 1$, if $\mu_{new}^{HL} \geq \mu_{new}^{LH}$
$w_j^* = 0$, if $\mu_{new}^{HL} < \mu_{new}^{LH}$
where w_j^* is the extracted bit. Here, μ_{new}^{HL} is the mean values of the slantlet transformation coefficients in high frequency *HL* subband and μ_{new}^{LH} is the mean values of the slantlet transformation coefficients in high frequency *LH* subband.

Step 4. **Extraction of RS Vector based Watermark**: Create groups of 4 pixels. Determine f and F for each RS vector. Extract the embedded watermark by determining *RG*, *SG* and *UG*.

Step 5. **Recovery of the Original Image:** To restore the original image, the watermark bits and the difference values obtained from the side information are employed. By performing the reverse procedure used during the watermark embedding phase, the original mean value of each block can be retrieved. This entails reversing the shifting of the mean values and rearranging the image blocks accordingly. Through this process, the blocks containing the difference value, extracted watermark value, and original mean value are reconstructed, ultimately resulting in the recovery of the original image.

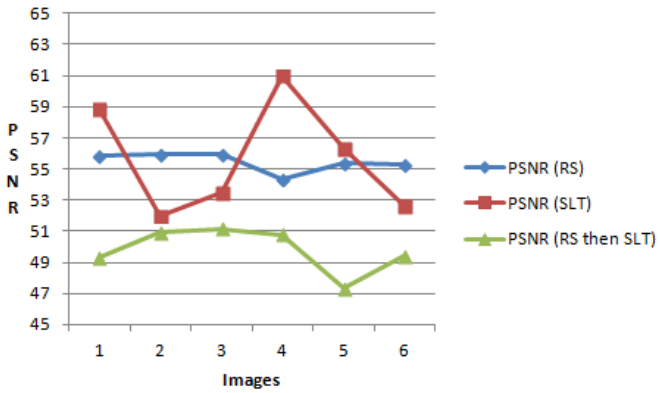


Figure 3.7: PSNR comparison for medical images.

3.3 Experimental Results

The proposed watermarking technique was evaluated through a series of experiments to assess its performance in different aspects. A dataset of 100 medical images was used for the evaluation, with all images converted to grayscale and resized to a resolution of 512×512 pixels. Various parameters were considered to evaluate the performance, including image quality preservation, security, integrity, confidentiality, tamper detection and localization, invisibility, robustness, capacity, reversibility, and the impact of block size and threshold values.

3.3.1 Invisibility Evaluation

To evaluate the visual quality (*i.e.*, the invisibility) of the watermarked images, the *PSNR* between the original and the watermarked image is calculated as by Eq.1.1, 1.2, 1.3. Table 3.1 shows the *PSNR* value for Lena image as 51.0727 dB and *PSNR* values for different medical images after all three cases *i.e.*.

i. *PSNR* of the image through the embedding with *RS* vector having 30,720 hidden bits.

ii. *PSNR* of the image only embedding though *SLT* with 30,720 hidden bits.

iii. *PSNR* of the image after the proposed technique after embedding 61,440 bits.

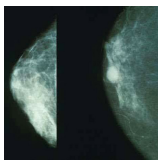
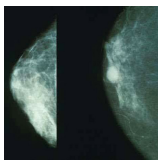
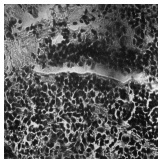
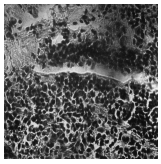
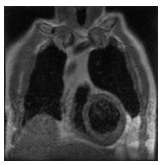
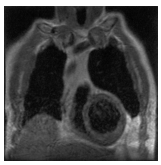
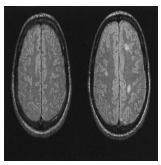
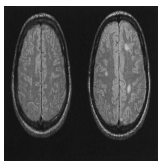
Comparison of the above cases is shown in Figure 3.6 with corresponding watermarked images from Table 3.1 .

3.3.2 Capacity Evaluation

The capacity of the watermarking scheme is determined by the size of the image and the number of hidden bits. In this case, for an image with dimensions $H \times W$ and a spatial domain block size of $h \times w$. For an image I_m with size $H \times W$ and a spatial domain block with size bsize=$h \times w$, the pure capacity can be calculated by:

$$Capacity(C) = (H/h) \times (W/w) \tag{3.8}$$

Table 3.1: Watermarked images along with PSNR (dB)

Original image	Watermarked Image	PSNR(RS)	PSNR(SLT)	PSNR(RS then SLT)
a.			55.8439	50.7585	51.0727
1.			55.8782	58.8271	49.3297
2.			55.9123	51.9748	50.9343
3.			55.9184	53.4858	51.1411
4.			54.3898	60.9701	50.7663
5.			55.3495	56.3128	47.3072
6.			55.2765	52.6306	49.4132

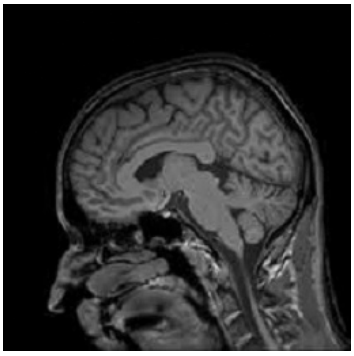


Figure 3.8: MRI brain image(256×256).

If the block size in the transform domain (Bsize) is $r \times s$, where $r = h/2$, and $s = w/2$, then the relationship between the capacity and the block size can be calculated as follows:

$$Capacity(C) = (H/2 \times r) \times (W/2 \times s) \tag{3.9}$$

The capacity of the watermarking scheme, expressed in bits-per-pixel (bpp), can be determined by dividing the value of parameter C, which represents the total number of bits that can be embedded in the image for a given block size, by the total number of pixels in the image. Proposed technique in transform domain has the capacity of 0.0625 bpp using Eq. (3.9) and the capacity from RS vector embedding is calculated by Eq. (3.13) is 1.06 bpp. Table 3.2 is constructed by taking Figure 3.7 as original image, showing embedding capacity for each channel. The capacity is calculated after compression by *LZW*.

Table 3.2: PSNR, Capacity(bits), BPP for different channels.

No of Channels	Average PSNR(dB)	Capacity	BPP
R	50.1308	61,440	1.1225
RG	50.1347	1,22,880	2.2450
RGB	50.1392	1,84,320	3.3675

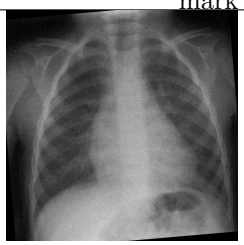
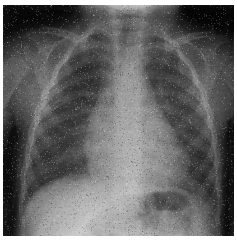
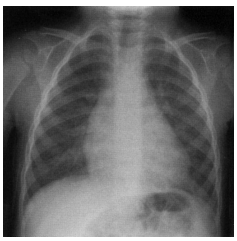
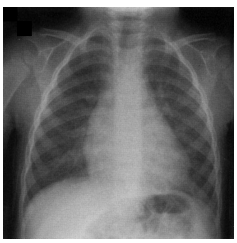
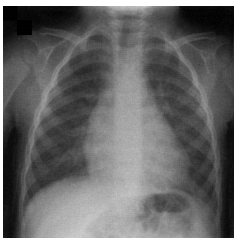
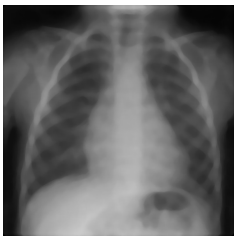
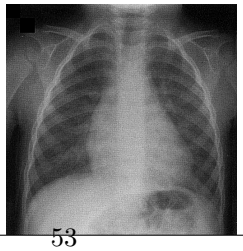
3.3.3 Reversibility Evaluation

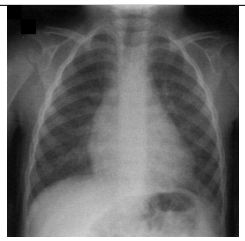
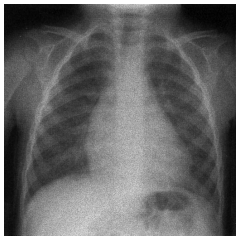
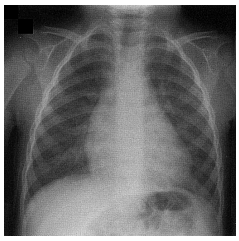
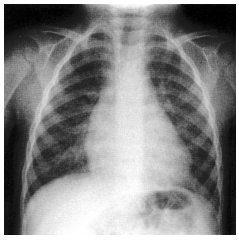
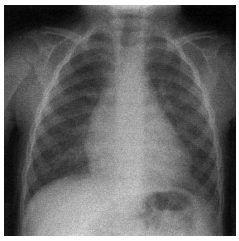
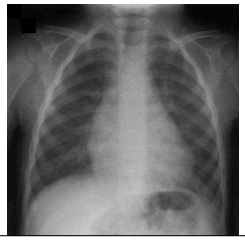
The reversibility of the proposed technique was evaluated using the Image Error Rate (IER). The IER measures the ratio of successfully recovered images without any errors to the total number of test images. In the case of the proposed technique, the IER was found to be zero, indicating that all cover images and the embedded watermark were successfully recovered without any loss of data or errors.

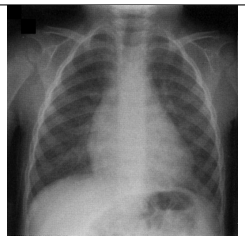
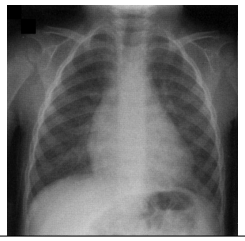
3.3.4 Robustness Evaluation

For robustness evaluation, watermarked images are tested against many attacks and watermarks are extracted after attacks along with *PSNR* values as shown in Table 3.3, against three types of unintentional attacks. Attacks like *JPEG* compression is done with the quality factor equals to (20, 30,..., 100), Additive Gaussian Noise (AGN) with zero-mean and a variance equals to (0.001, 0.002,...., 0.01). Resistance against these attacks show the strength of proposed technique.

Table 3.3: Types of attacks with extracted watermark and PSNR

Type of Attack	Image after Attack	Extracted Watermark	PSNR
A. Rotation(5 degree)			30.2142
B. Salt and Pepper			32.03
C. Filtering(average)			49.5695
D. Cropping(128×128)			42.2059
E. JPEG Comprssion			38.0628
F. Median Filter			32.6737
G. Smoothening			34.2089

Type of Attack	Image after attack	Extracted watermark	PSNR
H. Gaussian			41.7804
I. Speckle noise			29.98
J. Sharpening			30.8433
K. Histogram Equalization			15.7809
L. Poission attack			31.02
M. Blurring			34.6018
N. Motion Blur			39.6919

Type of Attack	Image after attack	Extracted watermark	PSNR
O. Resize(1.2)			25.1450
P. Wiener Attack			39.9482
Q. Scaling			30.1988

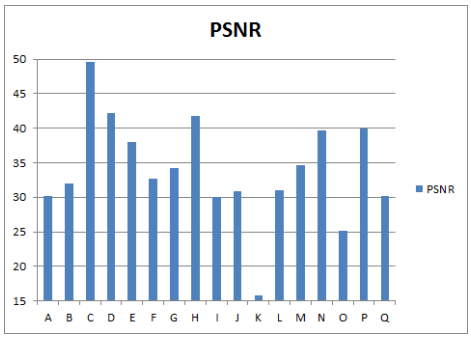


Figure 3.9: PSNR variation after attacks on watermarked image.

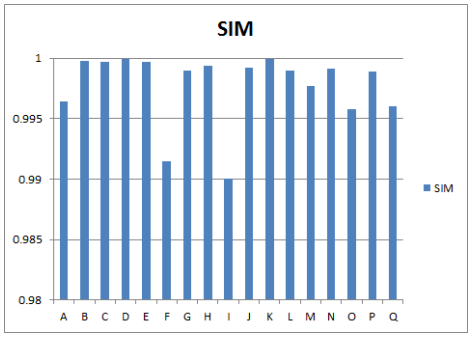


Figure 3.10: SIM after attacks on watermarked image.

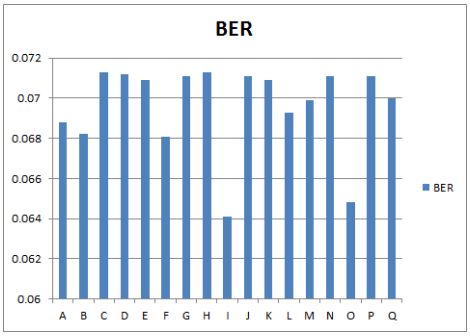


Figure 3.11: BER after attacks on watermarked image.

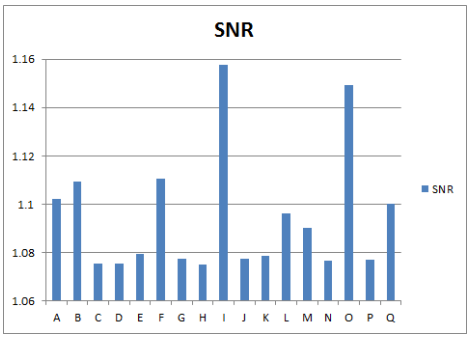


Figure 3.12: Signal to noise ratio after attacks on watermarked image.

Figure 3.9 shows variation on the *PSNR* values after attacks as the *PSNR* value of the watermarked image before attacks was $50.76dB$ and the least destruction was done with average filter attack. Similarly Figs. (3.10 - 3.13) show the variations in the values of *SIM*, *BER*, *SNR* and *NC* with the images from Table 3.3. *BER* is 'ZERO' for Gamma correction(0.5) and sharpening alpha(0.2) attacks. Results show that the proposed technique have high strength and good recovery of watermark after attacks.

3.3.5 Authenticity and Integrity

In the case of medical images, security and authenticity are most important criteria because if there is any tampering with the contents of the image than it can damage the *ROI* whereas maintaining the integrity of the image is equally viable. So, the proposed technique can be used for checking the authenticity and integrity of the medical image.

Tamper Detection and localization: If the watermarked image is tampered within the network or by intruders, it is detectable and can be localized through the proposed technique. As, it creates an encrypted watermark by using three components *i.e.* the biometric *ID*, patient *ID* for the purpose of checking integrity and original image blocks from *ROI*. Patient *ID* is in the form of text watermark which secures the personnel details of the patient for confidentiality. Biometric *ID* *i.e.* thumbprint is the unique identification mark of the patient which secures the authenticity and integrity of the patient. *ROI* blocks from the original image help in tamper detection and localization of the corrupted region of medical image. Experimental results shown in Table 3.4, for image(4.) from Table 3.1, prove the efficiency of the proposed technique.

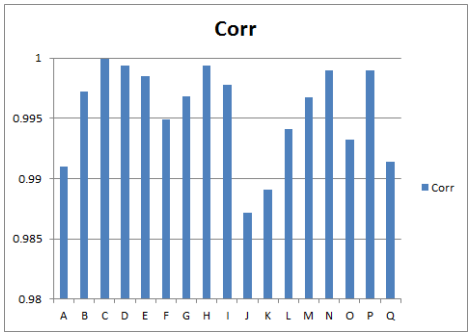


Figure 3.13: Correlation values after attacks on watermarked image.

Table 3.4: Extracted watermarks with original and tampered image.

Image Type	Watermarked Image	Original image watermark	Biometric ID watermark	Text watermark
Untampered				PATIENT ID: DANILKRVII6114
Tampered				PA=09ET01D:D12IL5HV6I314

3.3.6 Security of the watermark

MD5 and *AES* are very efficient cryptographic algorithms used for security of digital data. As, watermark used in proposed technique consists of four parts *i.e.* blocks of original image, biometric *ID* of the patient, patient *ID* as text watermark and key1. The original image blocks are encrypted with MD5, giving abundant security while generation hash functions. The hash values are then fused with other three components of watermark, which are encrypted using *AES-256*. It does provide a defence against the possibility of Quantum Computers, specifically Grovers' Algorithm which can reduce the search space by effectively half. There is the protection for encrypted watermarks for more than 50+ years against any kind of cryptographic attacks like collision attacks, bruteforce attack, algebraic attacks, exhaustive key searching, boomerang attacks meet-in-the-middle attack and bicliques attack.

3.3.7 Effects of Parameters

In this section, an examination was carried out to analyze the effects of two parameters: block size (Bsize) and threshold values (T and Th). Adjusting the block size has an impact on the capacity, invisibility, robustness, and software runtime. Similarly, altering the threshold values influences the invisibility and robustness of the watermark. The proposed scheme was subjected to testing using various threshold values (T = 1, 2, ...) and block sizes to assess its performance under different settings.

Threshold

Adjusting the threshold value influences the visibility and robustness of the watermark, while it has no effect on the capacity. As the threshold value increases, the *PSNR* decreases and the *BER* decreases. It should be noted that the choice of threshold value (Th) depends solely on the block sizes utilized in the scheme.

Block size

The capacity of the watermarking scheme was calculated for different block sizes, assuming an original image size of 256×256. As shown in Table 3.5, the capacity decreases as the Bsize increases. The *PSNR* value tends to increase with larger block sizes, indicating better image quality. Moreover, larger block sizes result in reduced running time, as there are fewer blocks to process. The *BER* also varies with block size, with a lower *BER* observed for larger block sizes.

Table 3.5: Block Size in transform domain with Capacity(bits).

Block Size	Capacity
2×2	16384
4×4	4096
8×8	1024

Furthermore, proposed technique allows flexible adjustment on the Bsize and threshold that controls the tradeoff between image fidelity and embedding capacity.

3.3.8 Overall Execution Time

Execution time is computed for the program at different block sizes. Overall execution time includes the time taken for watermark creation, embedding with Rs vector as well as *SLT* and watermark extraction. The results have been calculated on the personnel computer with processor: Intel(R) Core(TM)i7-4510U CPU @ 2.00 GHz 2.60GHz and 8GB memory. Matlab(R2015a) have been used to record the programs run time in seconds with the tic and toc commands. The average execution time for 100 medical test images have been calculated and the results are shown in Table 3.6 for original image(4.) from Table 3.1. The recorded results illustrate that the execution time in transform domain is inversely proportional to the Bsize due to the higher number of bits that are embedded in the image and higher number of blocks increase the repetition of embedding process. Total overhead created by the proposed technique is reduced with the increase in block size.

Table 3.6: Block size wise Overall Execution Time (in seconds) and Total Overhead(in Bytes).

Block Size	Embedding Time	Extraction Time	Overall Time	Total Overhead
2×2	1.4998	0.9562	5.4966	8240
4×4	0.4008	0.2132	3.6546	2096
8×8	0.1592	0.0631	3.2629	560
16×16	0.0723	0.0287	3.1416	176
32×32	0.0598	0.0125	3.11308	80

3.3.9 Comparison with Existing Techniques

In this section, the performance of the proposed scheme is compared with existing robust reversible medical watermarking techniques.

Table 3.7: Comparison with existing techniques

Techniques	PSNR(dB)	BPP	Execution Time
Alattar (2004)	29.23	0.74	Low
Shih and Zhong (2016)	48.53	1.10	–
Shih and Wu (2005)	38.0	1.00	High (240 sec.)
Thodi and Rodríguez (2007)	29.39	0.99	–
Tian (2003)	31.48	0.49	Low
Wakatani (2002)	22.36	2.00	–
Wang et al. (2013)	51.24	0.54	Low
Zain and Clarke (2011)	31.70	1.06	–
Zhao et al. (2011)	44.64	0.22	–
Proposed Algorithm	50.14	1.1225	Low (3.65 sec.)

These comparisons indicate that the proposed technique has significantly achieved high quality and high capacity. In addition, the comparison is conducted by embedding a watermark into 256×256 *MRI* brain image with block size of 4×4. As compared to Alattar (2004), the proposed technique can improve *PSNR* to 71.536%, *BPP* to 51.689% and has low time complexity as quad based algorithm is applied once on the image data. As compared to Shih and Zhong (2016), the proposed technique can improve *PSNR* to 3.317% and *BPP* to 2.045%. As compared to Shih and Wu (2005), the proposed technique can improve *PSNR* from to 31.947%, *BPP* to 12.25% and high time complexity as it takes 4 minutes for embedding . As compared to Thodi and Rodríguez (2007), the proposed technique can improve *PSNR* to 70.602% and *BPP* to 13.383%. As compared to Tian (2003), the proposed technique can improve *PSNR* to 59.275%, *BPP* to 129.081 and low time complexity as it uses difference expansion with a low computational complexity.%.As compared to Wakatani (2002), the proposed technique can improve *PSNR* to 124.239%. Although *BPP* is 43.875% lower, it could be increased if the block size is reduced to 2×2. As compared to Wang et al. (2013), *PSNR* is lowed by 2.146% for the proposed technique but *BPP* is improved by 107.870% and possess low time complexity. As compared to Zain and Clarke (2011), the proposed technique can improve *PSNR* up to 58.170% and *BPP* to 5.896%. As compared to Zhao et al. (2011), the proposed technique can improve *PSNR* to 12.320% and *BPP* to 410.227%. The above comparison is performed by considering only one channel of the image for the proposed technique. If all three channels are considered then capacity of the proposed technique is increased by 211.67 % approximately than all existing techniques shown in Table 3.7, with *BPP* 3.3675 *i.e.* 206.13 % higher than Shih and Zhong (2016). Time complexity for the embedding process is low *i.e.* 3.6546 seconds and it improves with the increase in block size as shown in Table 3.6. Also, '–' is used for the existing algorithms, which have not discussed the time complexity.

In summary, the proposed technique maintains visual quality of watermarked images while simultaneously increasing the capacity for medical image watermarking because proposed techniques uses the advantages of embedding in both transform and spatial domains.

3.4 Conclusion of the Chapter

Medical images are very high resolution images so it is difficult to secure such images through watermark. This work is proposed for the security of watermark and the cover image. Slantlet transformation along with *RS* vector is used for watermark embedding in selected blocks of the cover image. Cryptographic techniques *MD5* and *AES*. are used for watermark security along with the compression techniques for increasing the capacity. *PSNR* between cover and watermarked image is improved through the proposed technique as compared with existing techniques. Also many attacks done on the watermark and watermarked image which gave very promising results as compared to the existing medical watermarking techniques. Biometric security is applied for the integrity of the designed watermark.

Chapter 4

Dual Hybrid Medical Watermarking using Walsh-Slantlet Transform

4.1 Introduction

A hybrid robust lossless data hiding algorithm is proposed in this chapter by using the SVD with FWT and SLT for image authentication. These transforms possess good energy compaction with distinct filtering, which leads to higher embedding capacity from 1.8 bit per pixel (bpp) up to 7.5bpp. In the proposed algorithm, ANN is applied for region of interest (ROI) detection and two different watermarks are created. Embedding is done after applying FWH by changing the SVD coefficients and by changing the highest coefficients of SLT subbands. In dual hybrid embedding first watermark is the ROI and another watermark consists of three parts, *i.e.*, patients' personal details, unique biometric ID and the key for encryption. [1]. Comparison of the proposed algorithm is done with the existing watermarking techniques for analyzing the performance. Experiments are simulated on the proposed algorithm by casting numerous attacks for testing the visibility, robustness, security, authenticity, integrity and reversibility. The resultant outcome proves that the watermarked image has an improved imperceptibility with a high level of payload, low time complexity and high $PSNR$ against the existing approaches.

SLT is used for high energy compaction with multi-resolution decomposition with each filter bank. The method provides high data embedding capacity and uses PSO technique to calculate the optimum thresholds for selecting blocks. ROI region holds the Watermark. RS vector is used to embed the data. Watermark is compressed using LZW technique and encryption is done using AES. The existing medical watermarking algorithms work ordinarily but lack in taking all the important aspects of medical image watermarking into consideration equidistantly. The objective of the proposed research is to consider every possible parameter to their best capability and provide a secure algorithm in medical image watermarking. Proposed algorithm basically focuses on robustness and authentication of the medical image without compromising invisibility, time complexity and reversibility. Tamper detection, localization and recovery is another highlight of the proposed algorithm.

[1] **Contents of the work presented in this chapter have been published in *Multimedia Tools and Applications*, Vol. 78, pp. 17899–17927, 2019 (SCI Indexed)**

The chapter is organized as: Section 4.3and 4.2 explains the basics of *WHT* and *ANN*. Section 4.4, the proposed medical image authentication technique is illustrated and in Section 4.5, the experimental results are illustrated. Finally in section 4.6, the conclusion of the proposed work is summarized.

4.2 Walsh Hadamard Transform

WHT is non-sinusoidal, easily applicable,dyadic symmetry and orthogonal transformation (with only two values as +1 or -1) technique which is used in area of signal processing. A signal is decomposed into a set of orthogonal, rectangular waveforms called Walsh functions with transform matrix is efficiently formed by addition and subtraction without any multiplication while computing the values. *WHT* is chosen as it is one of the simplest and well suited transformation techniques because the transformation matrix is +1 and -1. Thus, it only requires addition and subtraction operations without performing multiplication operations which reduces processing time with high energy compaction. *WHT* can be perfectly reconstructed as no quantization error is executed in the encrypted domain. The *2D*-Hadamard transform is commonly used in image processing and is defined in Eq. (4.1):

$$H = H^T = H^* = H^{-1} \tag{4.1}$$

Where, H is Hadamard matrix, H^T stands for transpose of Hadamard matrix, H^* stands for conjugate Hadamard matrix, H^{-1} is the inverse Hadamard matrix. Walsh matrix each row can derive its sequence number by applying gray code and bit reversal conversion to Hadamard matrix.

Hadamard matrix H_n of size n is made using Kronecker product that exist between H_1 and H_{n-1}, where $n=2^N$, and N is an integer number. 4×4 Hadamard matrix is obtained by multiplying two H_2.

Sequency of the row is defined as the total number of times the sign *i.e.*, positive to negative or vice versa changes on each row of the matrix. These rows can be viewed as rectangular wave samples with *1/n* units sub period. Such continuous functions are known as Walsh's functions. The following relation Eq. (4.2) is satisfied as normalized Hadamard matrix is an orthogonal matrix.

$$H_h \times H_h^T = I \tag{4.2}$$

Here, H_h is a Hadamard matrix, I is a unitary matrix and H_h^T is a inverse Hadamard matrix. Using Fast *WHT*, Hadamard transform is calculated in $n= \log_2 N$ operations. The fast *WHT* (FWHT) and inverse *WHT* (IWHT) are as follows Eq. (4.3) and (4.4):

$$WHT\,(y) = Y = H_w y \tag{4.3}$$

Table 4.1: Conversion to Hadamard Order.

Type of Order	Symbolism			
Binary	00	01	10	11
Sequency Order	0	1	2	3
Gray code	00	01	11	10
Bit reverse	00	10	11	01
Hadamard order	0	2	3	1

$$IWHT\,(Y) = y = H_w Y \tag{4.4}$$

$$H_h = \frac{1}{2}\begin{bmatrix} 1 & 1 & \vdots & 1 & 1 \\ 1 & -1 & & 1 & -1 \\ \cdots & \cdots & & \cdots & \cdots \\ 1 & 1 & \vdots & -1 & -1 \\ 1 & -1 & & -1 & 1 \end{bmatrix} \begin{matrix} 0 \\ 3 \\ \\ 1 \\ 2 \end{matrix} \tag{4.5}$$

$$H_w = \frac{1}{2}\begin{bmatrix} 1 & 1 & \vdots & 1 & 1 \\ 1 & 1 & & -1 & -1 \\ \cdots & \cdots & & \cdots & \cdots \\ 1 & -1 & \vdots & -1 & 1 \\ 1 & -1 & & 1 & -1 \end{bmatrix} \begin{matrix} 0 \\ 1 \\ \\ 2 \\ 3 \end{matrix} \tag{4.6}$$

$$Y_w\,(k) = \sum_{N=0}^{n-1} y\,(N)\, w_n\,(k, N) \tag{4.7}$$

$$Y_w\,(k) = \sum_{N=0}^{n-1} y\,(N) \prod_{i=0}^{M-1} (-1)^{N_i k_{M-1-i}},\ k = 0, 1,\ \ldots,\ n-1 \tag{4.8}$$

$$y\,(N) = \frac{1}{n} \sum_{k=0}^{n-1} Y_w\,(k)\, w_n(k, N) \tag{4.9}$$

$$y\,(N) = \frac{1}{n} \sum_{k=0}^{n-1} Y_w\,(k) \prod_{i=0}^{M-1} (-1)^{N_i k_{M-1-i}},\ N = 0, 1,\ \ldots,\ n-1 \tag{4.10}$$

Where,H_h is a Hadamard matrix, Y is a spectrum vector and y is a signal vector. The $WHT(y)$ is the forward and $IWHT(Y)$ is the inverse of WHT_h, and H_w is the Walsh ordered matrix. H_w is retrieved by reordering rows of H_h as shown in Eqs. (4.5)-(4.10) and Hadamard ordered is retrieved by converting sequency to binary and from gray scale to bit reverse symbolism, as shown in Table 4.1. Where n=2^N, M=$\log_2 n$, and N_i is the i-th bit in the binary representation of N.

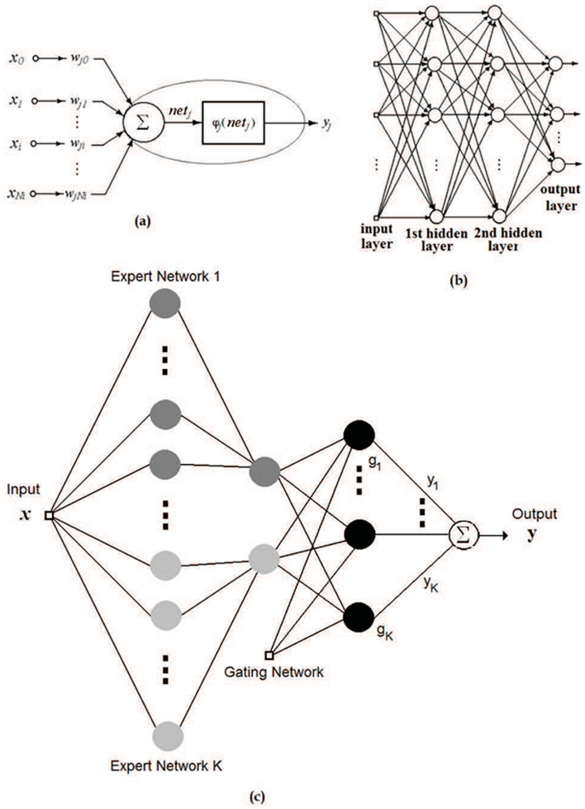


Figure 4.1: (a) Rosenblatt Perceptron; (b) Two hidden layers in *FNN*; (c) Dynamic Modular *ANN* with K experts

4.3 Artificial Neural Network

The machine learning process is increased when a problem has natural decomposition of data at simple functions. Kumar et al. (2022) discusses the role of Machine Learning (ML) and Artificial Intelligence (AI) in healthcare, highlighting their potential to improve decision-making, diagnosis, and treatment for major diseases. Kumar and Kumar (2022) addresses the challenges and opportunities associated with *ML* in healthcare, emphasizing its ability to analyze data and provide actionable insights for better patient care. Doull et al. (2021) investigates the factors affecting the detection of poachers using drones in conservation efforts and explores the effectiveness of *ML* for automated detection. Experimental tests analyzed the impact of camera type, time of day, camera angle, canopy density, and subject movement on detection probability. Both manual analysis by volunteers and *ML*-based automated detection software were employed. Results showed that a thermal infrared (TIR) camera, particularly at dawn with a 90°camera angle, improved detection probability. *ML* software achieved a detection probability of 0.558, but with higher false positives compared to manual analysis. Despite this, the advantages of *ML*-based automated detection make it a promising tool for anti-poaching strategies, offering potential for successful integration into conservation efforts. A global contextual residual convolutional neural network (GC-ResCNN) is proposed in Xu et al.

(2022) to address the challenges of motor fault diagnosis under variable-speed conditions, utilizing hierarchical structures, global context modules, and multi-feature fusion layers to improve feature representation and discriminant capability. The field of *AI* surgery (AIS) is advancing with the development of *ML*, deep learning, computer vision, and natural language processing, enabling the potential for more autonomous actions in surgery, Gumbs et al. (2021). Surgeons are increasingly interested in technology and robotics, with the goal of achieving greater autonomy in procedures. Haptics, although important, may not be the primary focus for developing autonomous robots, and embracing *AI* in surgery is crucial for future advancements in the field. Ferrag et al. (2021) presents a comprehensive study and experimental analysis of federated deep learning for cyber security in *IoT* applications, reviewing federated learning-based security systems, discussing the use of federated learning with blockchain and malware detection, identifying vulnerabilities, and evaluating the performance of centralized and federated learning models using real *IoT* traffic datasets, showcasing the effectiveness of federated deep learning in preserving privacy and detecting attacks.

Multilayer perceptrons (MLP) are used to construct modular machine architecture and implement experts. *ANN* is very useful for extracting feature from the medical image. In Thompson et al. (2020), a hybrid model combining a Convolutional Neural Network (CNN) and a *MLP* is proposed for the automated detection of obstructive Sleep Apnoea (OSA) using single-channel ECG signals. The *CNN* component extracts prominent features from the signals, which are then utilized by the *MLP* for classification. The hybrid model achieves high classification results, demonstrating its effectiveness in accurately identifying the presence of OSA and providing valuable insights for clinical diagnosis. *ANN* and wavelets have been used extensively in science and practical applications, pattern recognition for example. *ANN*s learn from a training set. Vector of descriptors are created with the help of Wavelet transforms which can compress as well as extract the most important characteristics of the image. *ANN* then optimize pattern recognition using vector of descriptors created by Wavelet transforms. Image content can be accurately described by values stored in array of descriptors which takes less space than pixel by pixel representation. However, generation of vector is a difficult process. It requires *ROI* to be well described. *ANN* is most commonly used machine learning technique in stock market prediction. The proposed *ANN* algorithm is used to extract features like Information measure of correlation, information measure of correlation, Autocorrelation, Sum entropy, Sum variance, Sum average, Sum of squares, Difference variance, Cluster Shade, Difference entropy and Dissimilarity Energy.

Based on nonlinear model in *ANN* configuration, Artificial neuron - Rosenblatt Rosenblatt (1958) perceptron, is most commonly used. *ANN* for the proposed technique is dynamically self programming and continuously adaptable. Artificial neurons are signal processing units compiled using an adder, set of input connections (weights) and an activation function (linear / non-linear) as shown

in Figure 4.1.a wherein adder is used for adding input signals of a neuron having linear combiner based on respective synapses.

net_j is the level of internal activity of a neuron as described in Eq. (4.11).

$$net_j = \sum_{i=0}^{N_i} w_{ji} \; . \; x_i \tag{4.11}$$

where, x_i is the input signal. When, i = 0 and value of $x_0 = +1$, then it is considered as the neuron's polarization potential. y_j is the output signal as defined in Eq. (4.12) as activation function $\varphi()$ response to net_j Silva et al. (2010) .

$$y_j \; = \; \varphi\left(net_j\right) \tag{4.12}$$

The multilayer perceptron (MLP) is utilized to implement the experts in the modular machine architecture. The self-organizing map (SOM) or Kohonen Neural Network can reduce dimensionality while maintaining the input data's topology. *SOM*s are particularly useful for visualization problems. In *SOM*, an input vector $\alpha \in H^i$ is provided for each neuron, which has a weight vector $weg \in H^i$. Neuron d is selected to fire whenever an input vector is provided to the network, as shown in Eq. (4.13). The neuron d is selected based on the weight vector that is most similar to that of the input vector.

$$d = arg\ min(\parallel \alpha - weg \parallel^2) \tag{4.13}$$

The modified equation as shown in Eq. (4.14) has firing neuron d with weight vectors w and neighbouring neurons j where j=1, ... , n

$$weg_j(c+1) = weg_j(c) + l_{jd}(\parallel s_j - s_d \parallel, c) \times (\alpha(c) - weg_j(c)) \tag{4.14}$$

On a neural network, a kernel $l_{jd}(\parallel s_j - s_d \parallel, c)$ is defined as a function of distance $\parallel s_j - s_d \parallel$ between d and j, and time c is the number of iterations. Depending upon the distance from d, j modifies w so that they resemble the data point (input vector). However, their strength depends upon the distance from d.

In Feed Forward neural network (FNN), every neuron in a layer is linked to the neuron in former layer as shown in Figure 4.1.b. Signals pass through the hidden layers of *FNN* while they broadcast from input to output layer. Neural network response is generated through output neurons while the input characteristics are represented by hidden neurons Hykin (1999).

In modular *ANN*, a set of sub-tasks are generated from an excessive and elaborated task which are thus easy to solve. In other words, a group of experts combine their conclusions to achieve better

Table 4.2: Architecture of *ANN* with training parameters.

Architecture	
Activation Function	Rectified Linear Units
Input Neurons	14
Hidden layer Neurons	50
Output Neurons	12
Parameters for training	
Training Rule	Decision Tree
Training Rate	0.1
EPOCHS	2500
Error Measurement	MSE

resolutions when done individually. Modular *ANN* is a set of learning machine which is either static or dynamic. A dynamic modular *ANN* is shown in Figure 4.1.c.A global response is generated by controlling network from the input signal. The learning speed of modular *ANN* is much higher than other neural networks.

4.4 Proposed Watermarking Technique

In this section, watermark creation algorithm, embedding algorithm, extraction algorithm; overflow and underflow handling process are discussed.

4.4.1 Watermark Creation Algorithm

All the three channels are used to increase the capacity of the proposed technique, but the watermarks are same for *RGB* to increase the security and for tamper localization/detection. Watermark 1 and Watermark 2 are generated from the following steps:

Step 1. **Division of Original image**: Divide the image into its three channels *RGB*.

Step 2. ***ROI* Selection** : *ANN* is trained first with different images, as it has adaptive training with neurons topologically ordered within a field. Table 4.2 gives the architecture and the training parameters for the *ANN* used. Trained *ANN* is then used for feature extraction, to separate *ROI* from *RONI* for *RGB* separately by following steps:

i Neurons Grid is made by selecting 30 rows and 100 columns *i.e.*, (30×100).

ii Extract pixels from the geometrical shape (i.e., bordered cylindrical, rectangle or pentagon) surface depending upon the structure and type of the *ROI* in original medical image. These extracted pixels are called coordinate sets.

iii Initial weights of the grid neurons are set to the value same as to the coordinate sets.

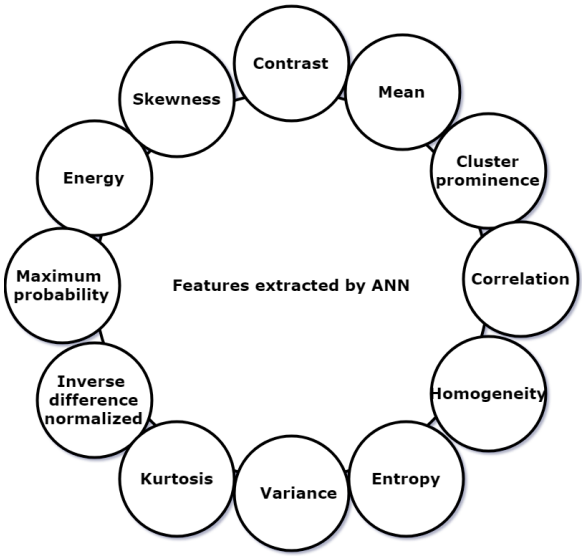


Figure 4.2: Parameters of medical image extracted by ANN

iv Finally, input is given in neural network with Eqs. (4.11) and (4.12), which is the cartesian coordinates of pixel value set which is to be triangulated.

v *ANN* is trained adaptively with decision tree framework.

vi Repeat i-v until neuron grid is made for all the rows of the original image.

Figure 4.2 gives the features extracted by the proposed *ANN*, which further creates the distinction of *ROI* and *RONI*. XORing is done in a bitwise fashion of the *ROI* obtained form *RGB* to get a combined *ROI*.

Step 3. **Watermark 1**: *SHA3-512* with 576 bits block size is applied on *ROI* with 'a' bits with padding function pattern 10^*1 i.e., a one bit, followed by zero bits ($maximum\ 'a-1'$) and one bit at the end, to get first watermark.

Step 4. **Apply *AES***: Apply *AES* with the unique key *i.e.*, key 1 (256 bits) on the output of Step 3 along with the concatenation of biometric *ID* and patient's *ID*.

Step 5. **Apply *LZW***: Apply *LZW* on the output of Step 4 to compress the watermark bits.

Step 6. **Watermark 2**: The output from step 5 is the second watermark.

4.4.2 Watermark Embedding Algorithm

Watermark embedding algorithm as shown in Figure 4.3 is summarized as follows:

Step 1. **Channel Division** The original image is divided to its colour bands *RGB* and the following steps are applied to each colour band separately.

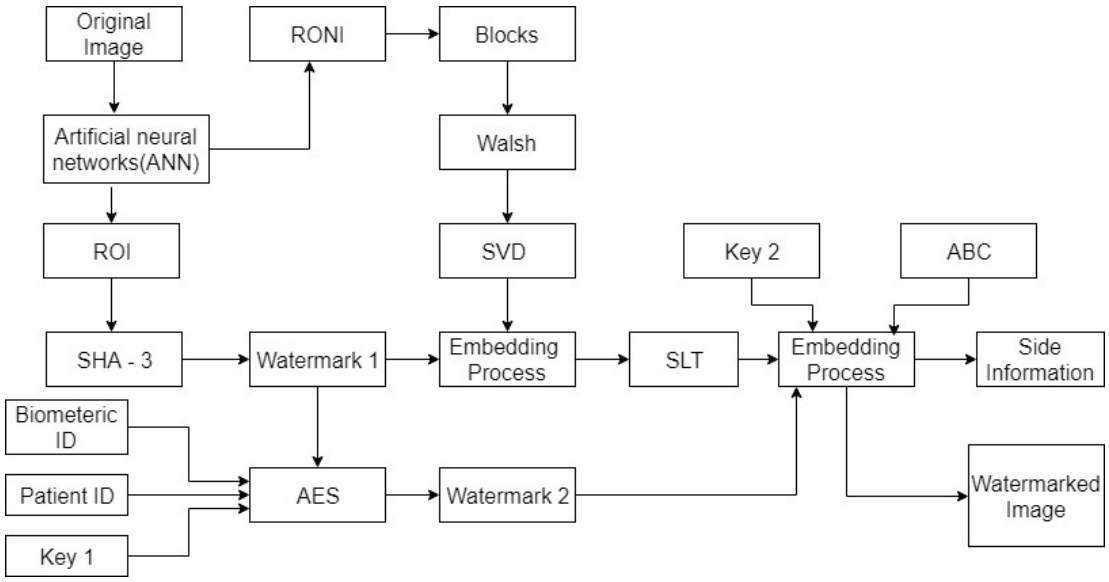


Figure 4.3: Block diagram representation of the proposed watermarking scheme.

Step 2. **Apply Walsh transform:** Split *RONI* part of the image into non-overlapping chunks of 8×8 and apply *FWH* . Calculate the relation of sequency number with correlation *i.e.*, P_z, where z is the order number of the block and store as side information as described in Table 4.1.

Step 3. **Calculating the threshold value:** Artificial Bee Colony (ABC) Karaboga and Basturk (2007) is used for calculating threshold *Th*, for each and every block and T for the whole image, by using the following Eqs. (4.16), (4.15) and (4.17).

$$T_{ij}(t+1) = \sum_{0}^{nb_i} (q_{ij}(t) + p(q_{ij}(t) - q_{kj}(t)))/nb_n \tag{4.15}$$

$$Th_{ij}(t+1) = q_{ij}(t) + p(q_{ij}(t) - q_{kj}(t)) \tag{4.16}$$

$$q_{ij} = q_{j\ min} + r \times (q_{j\ max} - q_{j\ min}) \tag{4.17}$$

where, nb_i : block number, T_i : The position of the onlooker bee, t : The iteration number, q_k: The randomly chosen employed bee, p: A series of random variable in the range. $i \in$ [-1,1], j : The dimension of the block, r : a random number between 0 and 1. T_{ij} and Th_{ij} are used for pixel section for embedding while preserving the quality of the original image. Where ij is the selected position co-ordinate.

Step 4. **Applying *SVD*:** *SVD* is applied to the *HH* block after *FHT* to divide all the high valued coefficients into three parts Tian et al. (2003) as in Eq. (4.18):

$$S = [USV] \tag{4.18}$$

Step 5. **Watermark1 Embedding:**Apply step 1 to step 4 on the watermark and get the S_s value as in Eq. (4.19):

$$S_s = [U_u S_s V_v] \tag{4.19}$$

where S_s is the singular value after applying SVD on watermark. For watermark embedding process. Obtain $S^{'}$ as in Eq. (4.20):

$$S^{'} = S + ((Th_{ij} \times S_s)/T_{ij}) \tag{4.20}$$

Side information is obtained by computing mean and standard deviation of the block. Thresholds are used to decrease the change in $S^{'}$.

Step 6. **Applying Inverse *SVD* (*ISVD*):** Apply $ISVD$ with $S^{'}$ as shown in Eq. (4.21):

$$S = [US^{'}V] \tag{4.21}$$

Step 7. **Applying the *SLT*:** The SLT matrix Selesnick (1999) by applying Eq. (3.1) to transform the red component. The SLT coefficients in matrix (S) are divided into 4-subbands (LL, HL, LH, and HH). The high frequency subband (HH) is used for the watermark embedding process.

Step 8. **Embedding watermark 2:** To embed watermark bits in each block, the difference between the mean values of the SLT coefficients in the high frequency subband (*i.e.*, HH) of that block is modified. Obtain A and $A^{'}$ *i.e.*, the highest two coefficients of each block, before and after applying SLT. Suppose, A_1 is the mean and A_2 is the standard deviation of the block. Also, let R be the ratio between (A_1, A_2) and (A , $A^{'}$). Let p_1 and p_2 be the inverse of two pseudo random number sequences of sequency order to hadamard order from P_z (demonstrated in Table 4.1, for example order number 3 will be 1.), *i.e.*, $p_1^{'}$ and $p_2^{'}$ are used to implant the watermark bits in A and $A^{'}$ by the following Eq. (4.22).

$$A_w = \begin{cases} A^{'} + (Th \times ((\sqrt{M}U_1 p_1^{'}))/T), & if \quad W = 0 \\ A^{'} + (Th \times ((\sqrt{M}U_2 p_2^{'}))/T), & if \quad W = 1 \end{cases} \tag{4.22}$$

where A_w is the modified highest coefficient of each block, W stands for the watermark bits and the watermark is of size $M \times M$, ($M = 2^c$; $c = 1, 2,..$), U_1= R and U_2= (1-R), T and Th are the threshold values from step 2. The coefficients U_1 and U_2 contribute in the improvement of the visual quality of the watermarked image, as R is constructed by both mean and standard deviation of each block retaining the change to be minimal. $\sqrt{M}$ helps

in retaining the watermark size and helps in watermark recovery. Eq. (4.22) is constructed in accordance with the properties of Wash as it has good energy compaction, real, orthogonal and symmetric.

Step 9. **Applying Inverse Slantlet (*ISLT*) and Inverse Walsh (*IWH*):** The process of watermark embedding is executed until all the watermarked bits are embedded. The original subbands are substituted by the modified subbands and *ISLT* Selesnick (1999) is applied through matrix multiplication process by in Eq. (3.2).

IWH is applied on the output after *ISLT*. Now, to ensure the reversibility, the resulted output must be rounded up to integer numbers. Thus, the original image and the watermarked image can be re-synthesized exactly the same at the receiver end. Also, to increase the capacity upto three times, the above steps are repeated in the same manner for embedding in both G and B channels as well.

Step 10. **Overflow and Underflow Condition:** The pixel values which are suffering from the condition information, is saved along with side information and then these pixel values will be adjusted as follows:

$$OU_w^{'}(a,b) = \begin{cases} 255 & if \;\; OU_w(a,b) \;>\; 255 \\ 0 & if \;\; OU_w(a,b) \;<\; 0 \end{cases} \tag{4.23}$$

where OU_w is the watermarked image before pixel adjustment, (a, b) are the coordinates of the pixels, whose value becomes below '0' and above '255' after embedding. $OU_w^{'}$ (a, b) is the modified pixel value after applying Eq. (4.23).

Step 11. **Side Information:** The side information along with key 1 and key 2 is encrypted with *AES-256*. Encrypted side information is then, embedded into the *LSB's* of the shortest spanning path WEI and KERN (1989) in the image of non overlapping blocks.

4.4.3 Watermark Extraction Algorithm

Step 1. **Dividing the image:** Divide the watermarked image into *RGB*, read the individual channel along with side information from the *LSB's* of the shortest spanning path of the image, decrypt it and then relocate back the pixels that were adjusted to their original locations. From the watermarked image, non-overlapping blocks are formed.

Step 2. **Applying *SLT*:** Apply *SLT* on the watermarked image and divide the image into 4×4 blocks.

Step 3. **Extraction of Watermark 2:** Let $A^{'''}$ be the *ISLT* coefficient of A, and correlation coefficients are then calculated between the $A^{'''}$, $p_1^{''}$ and $p_2^{''}$ for each block of the watermarked image.

Correlation coefficient are calculated and compared, *i.e.*, x($A^{'''}$,$p_1^{''}$), x($A^{'''}$,$p_2^{''}$) and x($p_1^{''}$,$p_2^{''}$). The recovered watermark is then constructed by comparing the correlation coefficients using '*Th*' as shown in Eqs. (4.24) and (4.25) using side information.

$$Th = \sqrt{M} \times C \times (U_1 \times U_2) \tag{4.24}$$

$$W_2^{''} = \begin{cases} 1, & if \quad x(A^{'''}, p_1^{''}) < x(A^{'''}, p_2^{''}) \\ 0, & otherwise \end{cases} \tag{4.25}$$

where $W_2^{''}$ is the recovered watermark, x is the corresponding correlation coefficients value and C is the weighted value of R.

Step 4. **Applying *FWT*:** Apply FWT on the 8×8 blocks of watermarked image.

Step 5. **Extraction of Watermark 1:** Apply SVD on the output of step 4 by applying Eqs. (4.19-4.21), as we need to calculate S_s after obtaining S, Th_{ij}, T_{ij} and $S^{'}$. W_1 is extracted with the use of corresponding U and V components from side information.

Step 6. **Recovery of the Original Image:** The difference value stored in side information, the original mean value of each block will be recovered by enforcing the inverse process that was applied in the watermark embedding side. Every block that contains the correlation coefficient value, extracted watermark value and the original mean value can be recovered through shifting back, the mean values, standard deviation values and hence the original image will be obtained by re-arranging the image blocks by adding or subtracting the difference.

4.5 Experimental Results

Some of the experiments have been conducted to measure the basic requirements of the watermarking schemes, which are maintaining the image quality parameters, security, integrity, confidentiality, tamper detection and localization, invisibility, robustness, capacity, reversibility and the effect of block size with threshold values. The invisibility refers to the ability of hiding the watermark into the cover image without degrading the visual quality. The basic parameter used to assess the invisibility is *PSNR*. The ability of the watermark to withstand image distortions is known as robustness. Capacity of watermarking scheme is the ultimate limit of the watermark/secret data bits that are embedded in a single cover image at a specific size. As, the capacity increases, security and *PSNR* decreases. The ability to recover original image after watermark extraction is known as reversibility. Performance evaluation of the proposed technique is done by performing several kinds of tests on 300 medical images. Attacks are performed on the watermarked image and results are

PATIENT ID: ANIL1104DANIELB
ADDRESS: 37 DEFENCE COLONY ROOP NAGAR INDIA
HOSPITAL ID: 2412SUJATARAM
HOSPITAL NAME: CH. SUBE SINGH HOSPITAL
DOCTOR ID: DR.SUNNYRSINGROHA2611
DISEASE: MRI SCAN FOR TUMOUR SIGNS

Figure 4.4: Text Watermark.

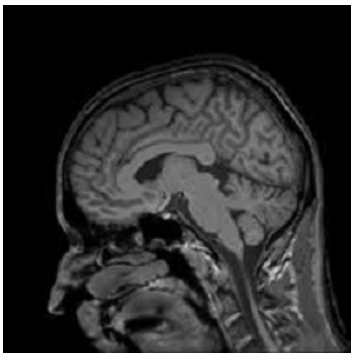


Figure 4.5: MRI image of brain (256×256 with embedding area of 36,276).

shown between the attacked image and the original image. To make the comparison easier, all the images are converted to grayscale and resized to (512×512 pixels). The parameters that have been calculated for performance evaluation are explained as follows:

4.5.1 Assessment on Invisibility

Invisibility level *i.e.*, how much distortion is created by the embedding in the original image, is calculated by the Peak Signal to Noise Ratio (PSNR) value of the original and watermarked images from Eq. 1.1. Table 4.3 shows the $PSNR$ value for Lena image as 53.64 dB. This is done on the images of size 512×512 with block size for FWT as 8×8 and block size after SLT as 4×4 with the total of 66,048 hidden bits. The average $PSNR$ of worst, average and the best values for the proposed technique are 47.82 dB, 51.93 dB and 54.26 dB respectively.

4.5.2 Tamper Detection and Localization

Medical images are highly sensitive in terms of security and authenticity as if there is any tampering with the contents of the image then it could damage the ROI whereas maintaining the integrity of the image is equally viable.

Authenticity and Integrity In the case of tampering of the watermarked image by the intruders or within the network. The proposed algorithm detects it and even localize the tempered pixels. It is possible because the proposed algorithm creates an encrypted watermark by using three components

Table 4.3: Original image, watermarked image and recovered image after watermark extraction along with *PSNR*.

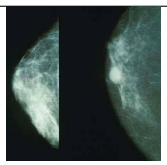
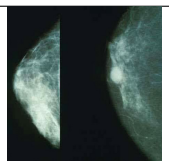
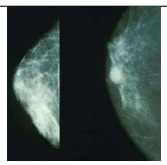
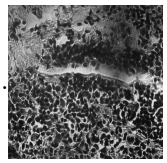
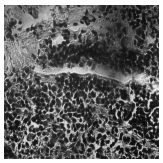
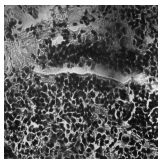
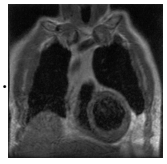
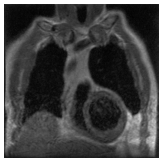
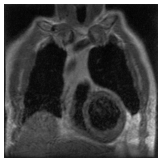
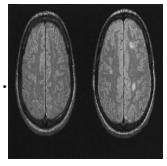
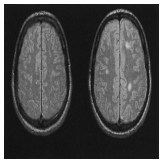
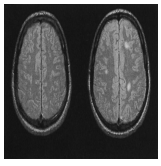
	Original image	Watermarked image	PSNR	Recovered image
1.			53.8014	
2.			54.0554	
3.			54.5383	
4.			53.7501	
5.			53.8454	
6.			52.8659	
7.			49.6742	
8.			53.6426	

Table 4.4: Tamper localization and recovery of *ROI*.

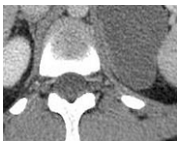
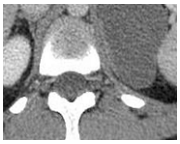
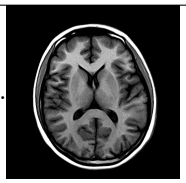
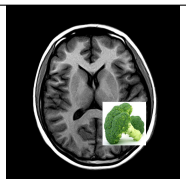
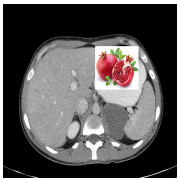
	Tampered Image	ROI(tamper localization)	ROI (tamper recovery)
1.			
2.			

Table 4.5: Extracted watermarks with original and tampered image.

	Original Image	Tampered Image	ROI tamper recovery	Biometric ID	Text
1.					PATIENT ID: ANIL1104DANIELB
2.					PATIENT ID: 0501BALBIRVIDYA

i.e., original image blocks from *ROI* for the purpose of security, the biometric *ID* for the purpose of integrity and patient's *ID* (Figure 4.4) for the purpose of checking authenticity. Both image and text watermarks are used. Text watermark is the patient's *ID* which undertakes the personnel details of the patient whereas image watermarks are *ROI* and Biometric *ID* *i.e.*, thumbprint. Thumbprint is considered as the unique identification mark of the patient which resolves all security issues. Tamper detection and localization of the corrupted region of medical image is done with the help of hidden *ROI* blocks. As, watermark 1 and watermark 2 contains *ROI* along with *ROI* of the original image left non tampered during embedding. Hence, there are three copies of *ROI* at the receiver's end for comparison for tampering detection, localization and recovery. Table 4.4 shows the tampering localization and recovery for *ROI* of the watermarked image because of sharpening in

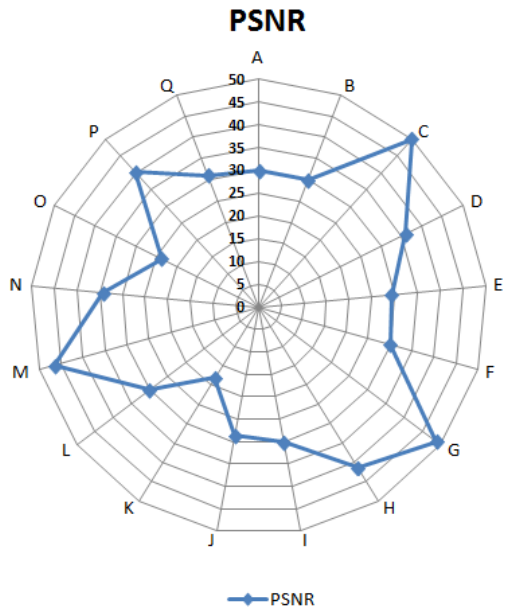


Figure 4.6: Peak Signal to Noise ratio (dB) after attacks A-Q from Table 4.6.

image *1.* and due to salt and pepper attack in image *2.*, respectively. Table 4.5 shows an example of visible tampering and tamper recovery is done for all the three parts *i.e.*, *ROI* part of watermarked image, biometric *ID* and text *ID*. This proves the efficiency of the proposed algorithm in the tamper detection and recovery.

4.5.3 Assessment on Reversibility

Reveresibility of the technique depends upon the value of image error rate. *IER* is the ratio of the sum of all the images recovered with errors to the total number of the test images of each kind. *IER* value of the proposed technique is Zero in the case where there are no attacks done on the watermarked image. As embedding is done by R between A_1 and A_2 of each block as dividend along with usage of watermark size $\sqrt{M}$ and again reducing the change by using T_{ij} as divisor. Therefore, the change is minor as it is done in the frequency domain of *SLT* and Walsh. Also, the change is completely reversible at the receiver's end without any data loss. Table 4.3 shows the recovered image after watermark extraction from the watermarked image with zero *IER*.

4.5.4 Assessment on Watermark Security

Dual hybrid scheme doubles the security. As, *ROI* is secured twice. Firstly, in watermark 1 and embedding through Walsh transform. Secondly, encrypted in watermark 2 and embedding through *SLT*. Hence, the most important part of a medical image is fully secured because of hybrid and dual nature of the proposed algorithm. In this method, *SHA-3* and *AES* are used for security of the image data. These techniques are highly efficient cryptographic algorithms. Watermark has

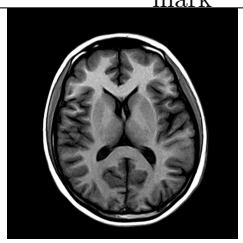
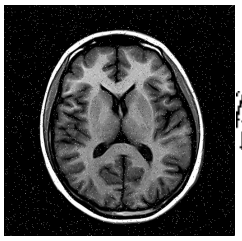
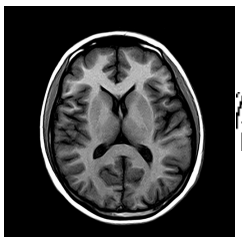
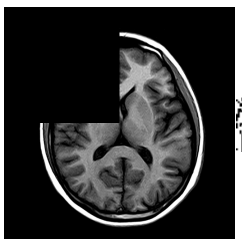
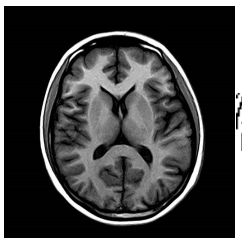
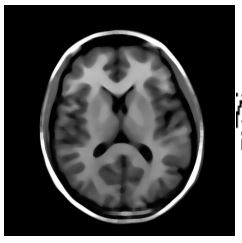
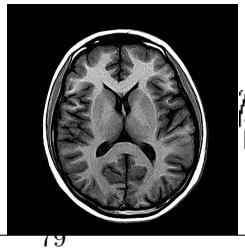
four parts *i.e.*, *ROI* blocks, patients' biometric *ID*, text watermark in the form of patient's *ID* and key1. *SHA-3(512)* is used to encrypt *ROI* blocks while the hash values are combined with remaining parts of watermark which are encrypted using *AES-256*. The use of *SHA-3* and *AES-256* provide security against algorithms like Grovers' Algorithm which can cut down search space by effectively half. There is the protection for encrypted watermarks for more than 50+ years against any kind of cryptographic attacks like collision attacks, preimage attack, bruteforce attack, side-channel attack, algebraic attacks, birthday attack, exhaustive key searching, boomerang attacks, rainbow table, bicliques attack and length extension attack. Caching induces the time variation for the fetchers. In table-lookup, caching and optimizations are disabled. Also, uniform base having either 32-bits or 64-bits are used to perform addressing calculations, which results in table-lookup performance to be slower. However, it is time constant thus it performs faster than the Galois Field (GF) (2^8) mathematics for every time the Substitution box (S-Box) is used. Hence provides better results with all types of timing attacks including nice timing to 88% secure. *AES* with 14 rounds undertakes high complexity of 2^{40} chosen plain text of size with the processing complexity of the attack is $2^{254.4}$ and meet-in-the-middle attack on chosen plain text of size with 2^{120} and 2^{203} memory complexities. Man in the middle attack for *ROI* is 100% detectable as the proposed algorithm is acceptable for tamper detection. Denoising attack can be reversed by thresholding with *SLT*.Compromised key attack can utmost breaks 11 rounds of *AES-256* but it has 14 rounds. Table 4.7 shows resistance of the proposed algorithm against different cryptographic and signal processing attacks with the evidential proof in Biryukov et al. (2009) Biryukov et al. (2010).

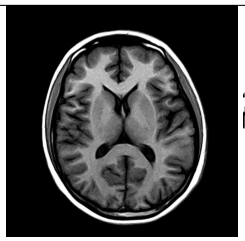
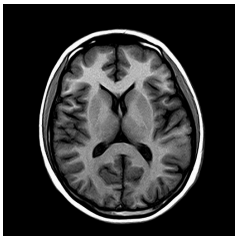
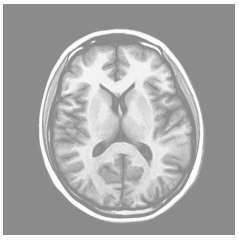
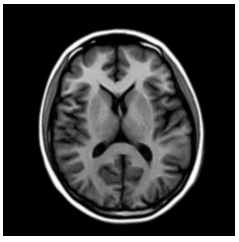
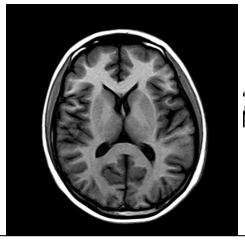
4.5.5 Assessment on Robustness

Robustness shows the resistance of the extracted watermark and the extracted original image against various attacks. Watermarked images got tested against more than 35 attacks and watermarks are extracted after attacks along with the *PSNR* and Structural SIMilarity (*SSIM*) index values as shown in Table 4.6, against different types of unintentional attacks like poisson, motion blurr, gaussian, histogram equalization, *JPEG* compression, salt and pepper, cropping *etc.* Resistance against these attacks show the strength of proposed algorithm. Normal Co-relation *NC* is calculated by the cross-correlation in the the frequency domain, local sums by pre-computing, running sums and by using local sums for normalizing the cross-correlation, hence getting the *NC* coefficients.

Table 4.7 illustrates *BER* for the extracted watermark and *NC* after many cryptographic/signal processing attacks on extracted *ROI* after attacked watermark image. Expanding attack is done by expanding *S*-boxes in *AES* by using small input-injective quadratics which gives the length expansion factor of 2 to 4 for *S*-boxes, which gives *BER* of 0.032. The image used for Tables 4.6, 4.7 and 4.8 is a *MRI* scan of size 512×512 with *NC* value is '1', *BER* value is '0' and 66,048 hidden bits.

Table 4.6: Types of attacks with extracted watermark, PSNR(dB) and SSIM

Type of Attack	Image after Attack	Extracted Water-mark	PSNR(dB)	SSIM
A. Rotation(5 degree)			29.9297	0.981
B. Salt and Pepper			30.0444	0.935
C. Filtering(average)			49.8827	0.991
D. Cropping(128×128,256×)256			35.9698	0.999
E. JPEG Compression			29.2960	0.978
F. Median Filter			30.0422	0.974
G. Smoothening			48.9215	0.952

Type of Attack	Image after attack	Extracted watermark	PSNR	SSIM
H. Gaussian			41.3355	0.964
I. Speckle noise			30.0420	0.961
J. Sharpening			28.6619	0.959
K. Histogram Equalization			18.2224	0.847
L. Poisson attack			30.0447	0.959
M. Blurring			46.4742	0.956
N. Motion Blur			34.2643	0.942

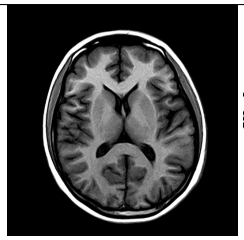
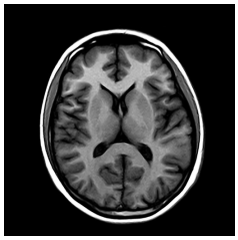
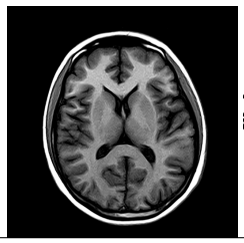
Type of Attack	Image after attack	Extracted watermark	PSNR	SSIM
O. Resize(2.5)			23.8125	0.948
P. Wiener Attack			40.2473	0.953
Q. Scaling			31.0447	0.955

Table 4.7: *ROI* robustness against cryptographic and signal processing attacks

Attacks	BER (dB)	NC
No attack	0	1
Nice Timing	0.033	0.986
Meet-in-the-middle	0	1
Man-in-the-middle	0	1
De-noising	0	1
Compromised-Key	0	1
Echo addition	0.023	0.98
Expanding S-box	0.062	0.99
Pitch shifting	0	1
Eavesdropping	0	1
Differential Cryptanalysis	0	1
Linear Cryptanalysis	0	1
Jittering	0.063	0.98
Rotational	0.064	0.99
Brute-force attack	0	1
Low-pass filtering	0	1
Re-quantization	0	1
Boomerang	0	1

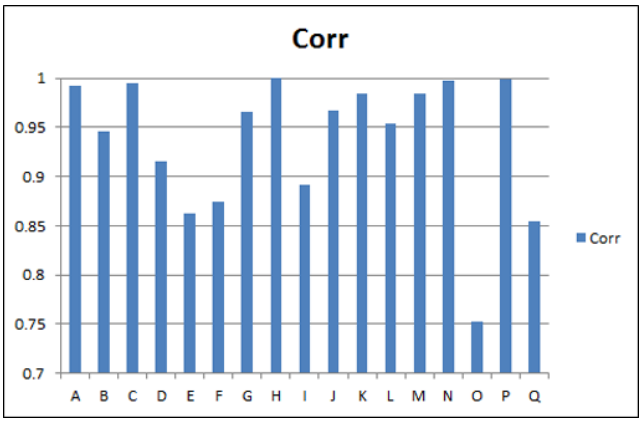


Figure 4.7: Normal Correlation after attacks A-Q from Table 4.6 on watermarked image.

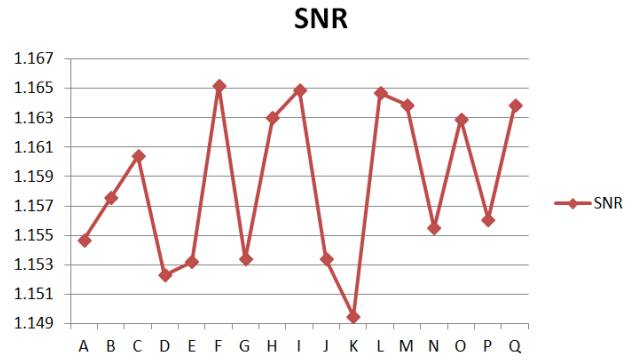


Figure 4.8: Signal to Noise Ratio (dB) after attacks A-Q from Table 4.6 on watermarked image.

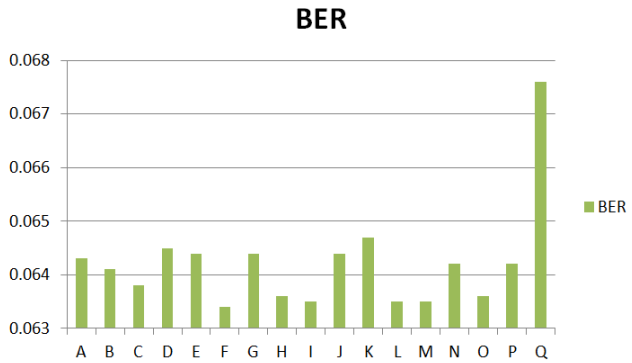


Figure 4.9: Bit Error Rate (dB) after attacks A-Q from Table 4.6 on watermarked image.

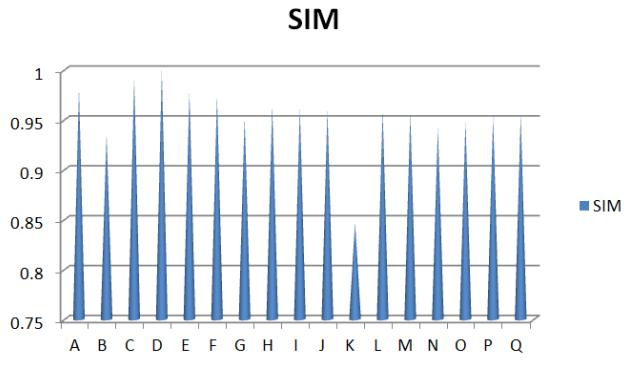


Figure 4.10: Similarity Index after attacks A-Q from Table 4.6 on watermarked image.

Table 4.8: Simulation results for side information after transmitting through AWGN channel.

SNR (dB)	Total corrupted bits	Corrupted hidden data bits
0	40072	105
1	20072	62
2	10946	30
3	6198	11
4	3258	1

Figure 4.6 shows variation on the *PSNR* values after attacks as the *PSNR* value of the watermarked image before attacks was 50.76 dB and the least destruction was done with average filter attack. Similarly Figures 4.7 - 4.10 show the variations in the values of *SIM*, *BER*, *SNR* and correlation with the type of attacks/results from Table 4.6. BER is 'ZERO' for sharpening alpha(0.2) and Gamma correction(0.5) attacks. Table 4.8 shows the results of *AWGN* on the watermarked image for the side information *LSB* hiding. With the increase in Signal to Noise Ratio (SNR) the effect of *AWGN* is reduced. As, illustrated corrupted hidden bits are not high because hiding is done through shortest spanning path, which solves the data reorganization problem as well. Stimulated results prove that the proposed algorithm is highly robust.

4.5.6 Assessment on Capacity

Capacity is defined in Eq 1.4. The pure capacity can be calculated by Eq. (3.13) and the block size (Bsize) can be calculated from Eq. (3.9):

Table 4.9: PSNR, Capacity(bits) and *bpp* for Figure 4.5.

Capacity	Average PSNR(dB)	*bpp*
66,048	48.8942	1.8207
1,03,424	45.3497	2.8510
1,45,424	44.9758	4.0088
2,31,936	43.5295	6.3936
2,72,448	43.0724	7.5104

The Capacity calculates the total amount of data that can be inserted in the cover image at

different block sizes or on a particular block size. Capacity is divided by the sum of all the pixels in the cover image to calculate capacity in terms of (*bpp*). Proposed algorithm in transform domain has the capacity in bits is from 66,048 to 2,72,448 and 1.8207 to 7.5104 *bpp* through Eq.((1.4)). Table 4.9 and 4.10 are constructed by taking Figure 4.5 as original image, showing embedding capacity for all three channels. The capacity is calculated after compression by *LZW*.

Table 4.10: PSNR, Capacity(bits) and *bpp* for Figure 4.5

No of Channels	Average PSNR(dB)	Capacity	bpp
R	48.8942	66,048	1.8207
RG	48.8929	1,32,096	1.8207
RGB	48.8907	1,98,144	1.8207

4.5.7 Assessment on the effects of parameters

The proposed algorithm working could be altered by the alteration of some of the important parameters, which could lead to the different results. The effects of following two parameters are analysed:

- **Block Size (Bsize)** Bsize is the size of *SLT* coefficients subband. Capacity, robustness, invisibility and time complexity are influenced by the changes in Bsize. The Capacity has been calculated using Eq.(3.9) for different block sizes for single time loop execution when the original image size is (256×256) as shown in Table 4.11. Capacity and *BER* are inversely proportional to the Bsize while *PSNR* is directly proportional to Bsize. Running time decreases with the increase in Bsize as total number of blocks are reduced.

Table 4.11: Block Size in transform domain with Capacity for single time loop execution.

Block Size	Capacity
2×2	16384
4×4	4096
8×8	1024

- **Threshold values (T and Th)** It is the strength of the watermark. Invisibility and robustness are effected by the change in threshold value. However, it has no effect on Capacity. *PSNR* and *BER* are inversely proportional to threshold value. Threshold value depends on Bsize completely.

  The proposed scheme has been tested for different threshold values (T=1, 2,...) and different block sizes. Furthermore, proposed technique allows flexible adjustment on the Bsize and threshold that controls the tradeoff between image fidelity and embedding capacity.

Table 4.12: Block size with Execution Time (in seconds).

Block Size(Walsh)	Block Size(SLT)	Embedding Time	Extraction Time
2×2	4×4	34.3151	18.8758
4×4	4×4	21.7216	12.3733
8×8	4×4	21.1383	10.8263
16×16	4×4	21.0460	10.4377
32×32	4×4	20.3200	10.3129
2×2	8×8	19.3051	10.0212
4×4	8×8	9.9552	5.8390
8×8	8×8	6.5411	3.9572
16×16	8×8	5.5218	3.6428
32×32	8×8	5.3223	3.2567
2×2	16×16	16.3916	8.04721
4×4	16×16	5.3719	3.2106
8×8	16×16	2.6898	1.2513
16×16	16×16	1.6777	1.0266
32×32	16×16	1.4671	0.9265
2×2	32×32	15.5246	7.2108
4×4	32×32	4.6411	2.4236
8×8	32×32	1.6578	0.9862
16×16	32×32	1.4239	0.8340
32×32	32×32	0.5261	0.2414

4.5.8 Assessment on Execution Time

The proposed algorithm is based on different block sizes, hence the execution time will be different for all the sizes. The personnel computer with processor: Intel(R) Core(TM)i7-4510U CPU @ 2.00 GHz 2.60GHz and 8GB memory have been used to calculate the results. Run time is calculated in seconds with the tic and toc commands in Matlab(R2015a). The average run time for 300 medical test images have been calculated and the results are shown in Table 4.12 for image(1.) from Table 4.5. Maximum time taken for embedding is 34.31 sec. and extraction is 18.87 sec. in worst case scenario and 0.52 sec./0.24 sec. in best case.Run time is inversely proportional to the block size *i.e.*, higher the block size, lower will be the embedding and extraction time.

4.5.9 Comparisons with Existing Technologies

The proposed scheme is highly robust withholding more capacity in comparison with existing robust reversible medical watermarking techniques based on their performances. The comparison has been conducted for the invisibility, robustness, capacity and reversibility.

These comparisons indicate that the proposed technique has significantly achieved high quality and high capacity. In addition, the comparison is conducted by embedding a watermark into 256×256 *MRI* brain image *i.e.*, Figure 4.5 with block size of 4×4 for *SLT* and 8×8 for *FWT*.

As compared to Alattar (2004), the proposed technique can improve *PSNR* to 67.259%, *bpp* to

Table 4.13: Comparison with existing techniques

Techniques	PSNR(dB)	BPP	Time Complexity
Alattar (2004)	29.23	0.74	Low
Shih and Zhong (2016)	48.53	1.63	–
Shih and Wu (2005)	38.0	1.00	High
Thodi and Rodríguez (2007)	29.39	0.99	–
Tian (2003)	31.48	0.49	Low
Wakatani (2002)	22.36	2.00	–
Wang et al. (2013)	51.24	0.54	Low
Zain and Clarke (2011)	31.70	1.06	–
Zhao et al. (2011)	44.64	0.22	–
Bamal and Kasana (2018)	50.14	1.122	Low
Proposed	48.89	1.819	Low

145.810% and has low time complexity as quad based algorithm is applied once on the image data. As compared to Shih and Zhong (2016), the proposed technique can improve *PSNR* to 0.74180919% and *bpp* to 65.363%. As compared to Shih and Wu (2005), the proposed technique can improve *PSNR* to 28.657%, *bpp* to 81.9% and with high time complexity as it takes 4 minutes for embedding. As compared to Thodi and Rodríguez (2007), the proposed technique can improve *PSNR* to 66.349% and *bpp* to 83.737%. As compared to Tian (2003), the proposed technique can improve *PSNR* to 55.304%, *bpp* to 271.224% and low time complexity as it uses difference expansion with a low computational complexity. As compared to Wakatani (2002), the proposed technique can improve *PSNR* to 118.649%. Although *bpp* is 9.05% lower, it could be increased if the block size is reduced to 2×2. As compared to Wang et al. (2013), *PSNR* is lowed by 4.586% for the proposed technique but *bpp* is improved by 236.851% and possess low time complexity. As compared to Zain and Clarke (2011), the proposed technique can improve *PSNR* up to 54.227% and *bpp* to 71.603%. As compared to Zhao et al. (2011), the proposed technique can improve *PSNR* to 9.520% and *bpp* to 726.818%.

Bamal and Kasana (2018) uses single embedding process with *SLT* using RS vector but the proposed technique uses hybrid embedding using both Walsh with *SVD* for watermark 1 and *SLT* for watermark 2. Hybrid watermarking increases security and robustness, making proposed technique more resistible to attacks than Bamal and Kasana (2018) while increasing the embedding capacity. Hence, *PSNR* of the proposed technique is decreased by 2.49% but *bpp* is increased from 62.08% to 569.04%. The above comparison with existing techniques are shown in Table 4.13, with *bpp* 1.819 to 7.510 as shown in Table 4.9. Also, '–' is used for the existing algorithms, which have not discussed the time complexity. Figure 4.11 shows the comparison of *NC* with 8 different attacks and 8 different embedding techniques for two 64×64 watermarks Lei et al. (2014) Bamal and Kasana (2018). Projections in Figure 4.11 proves the proposed algorithm is highly robust. In summary, the proposed technique maintains quality while simultaneously increasing the capacity and robustness for medical image watermarking because proposed technique uses the advantages of hybrid dual

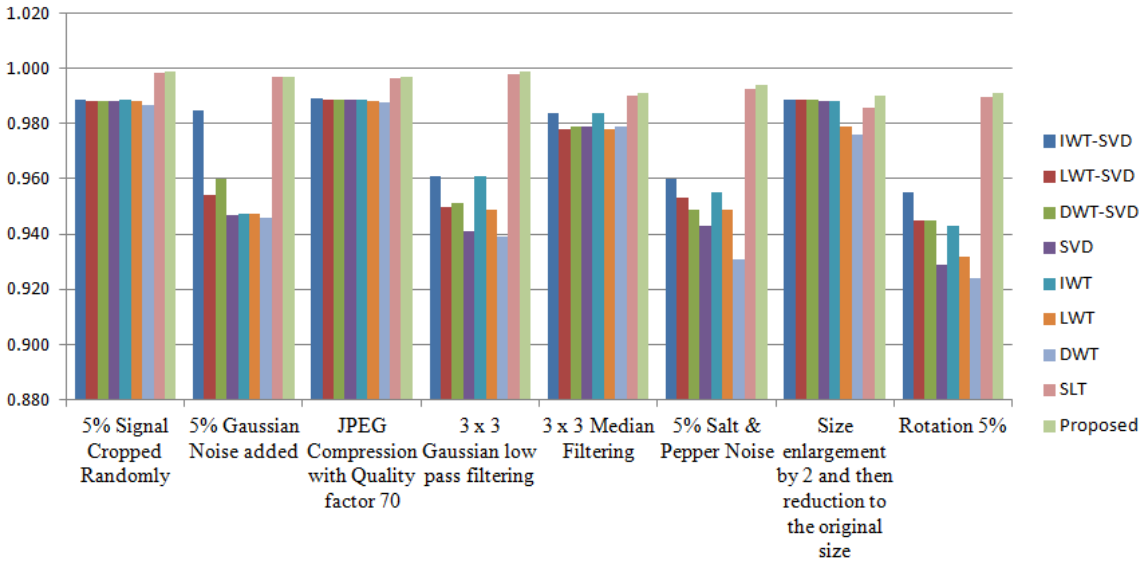


Figure 4.11: Robustness comparison of NC values with different attacks on existing techniques for two 64×64 watermarks.

embedding in transform domain.

4.6 Conclusion of the Chapter

This chapter introduces a novel digital watermarking technique that combines Walsh-Hadamard transform, *SLT*, and *SVD* to enhance various properties and parameters for effective watermarking. The technique utilizes *FWT* and *SLT* for data embedding, resulting in increased embedding capacity, improved robustness, and reduced *BER* for medical images. Additionally, an *ANN* is employed for feature extraction, facilitating region classification and enabling tamper detection and localization. The technique adopts a hybrid approach for dual embedding, enhancing capacity, security, and robustness. It achieves reduced execution time by leveraging *SLT*'s filters and the computational efficiency of *FWT*. Strong security measures such as *SHA-3, AES,* and biometric thumbprints are implemented. The technique ensures full reversibility and lossless functionality, as evidenced by an *IER* of zero. Experimental results demonstrate its superiority in terms of metrics like *SIM, PSNR, NC*, *bpp*, time complexity, and *SNR*. The watermarked images generated exhibit high visual quality, invisibility, and smoothness. Overall, the proposed technique contributes to the advancement of digital watermarking, particularly in the context of protecting and securing medical images.

Chapter 5

Reversible Medical Image Watermarking for Tamper Detection using ANN and SLT

5.1 Introduction

Internet is also known as an information superhighway that connects millions of people, who share information (data) among each other. The tremendous growth of information and communication technologies have made multimedia an indispensable characteristic of the Internet. However, as the size of multimedia data increases, the exposure to various attacks increase (Cox *et al.*, Cox et al. (1997)). Therefore, protecting private information, content, claim of ownership and its confidentiality has become extremely important. Medical images, which reveal hidden portion inside the body are no aloof from digital data integrity and tampering problem. Corruption of information stored in a medical image can affect the life of a living being. Medical images are shared among hospitals; patients and physicians over the image sharing software. When transmitting a medical image digitally, security of information and integrity of data are considered as most important aspects. Some of the hospitals integrate their systems with images sharing software like Health Information Exchange (HIE) and Picture Archiving & Communication Systems (PACS) *etc.* Generally, medical image sharing is done through data transmission on to the hospital network systems. *DICOM* standard is the commonly used image format in medicine. *DICOM* can be stored on cloud. Medical images require higher amount of security due to the growing use of patients' sensitive information in the form of medical images on the Internet which are vulnerable to exposure and attacks over the world wide web.

Medical Images can be accessed electronically with the advancement in technology. Corruption of medical images may lead to wrong diagnoses & treatments and can affect a person's life. Therefore, the security of medical images is essentially important for patients' privacy and life.

The conventional state-of-the-art watermarking techniques have shown effectiveness in addressing specific parameters, but they often fall short in simultaneously improving all of these parameters. However, the proposed technique overcomes these limitations and enhances multiple parameters simultaneously. It utilizes *SLT* for data embedding, resulting in improved compression efficiency,

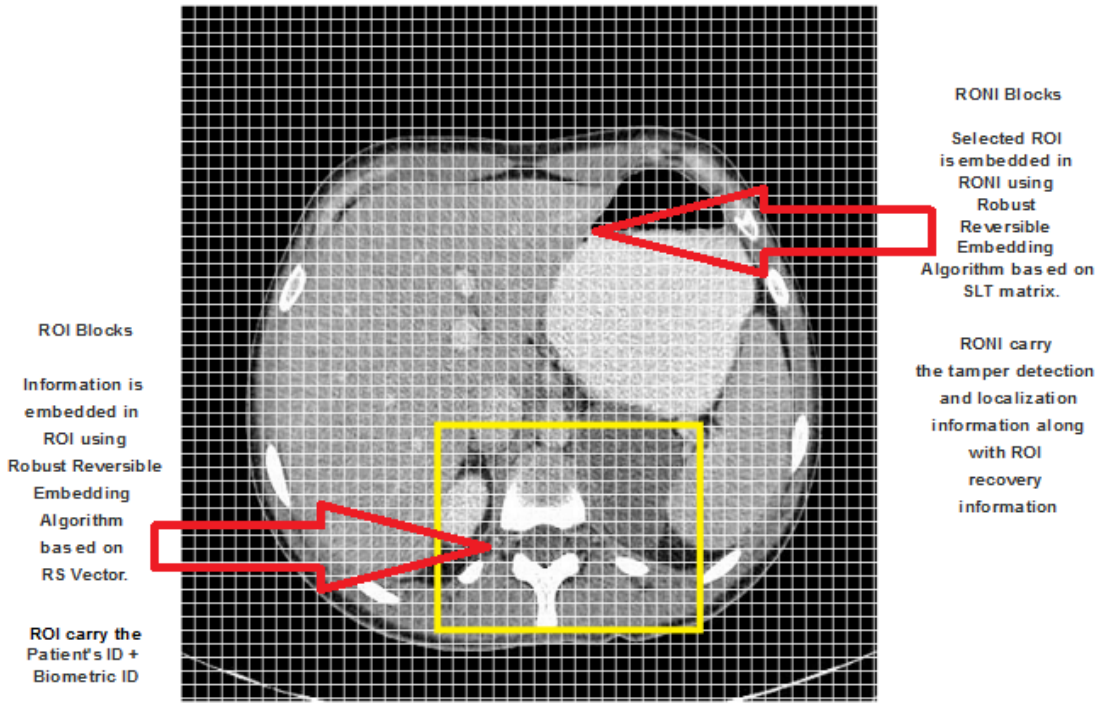


Figure 5.1: Medical image is divided into a grid showing *ROI* and *RONI*. The data sets enclosed by a yellow border are considered the *ROI*.

reduced bit error rate, and decreased execution time. The technique also incorporates the RS vector through a hybrid approach, enhancing both security and watermark capacity. Feature extraction using an *ANN* facilitates region classification, tamper localization, and recovery. Furthermore, the proposed technique significantly enhances the perceptibility and quality of watermarked images, including improvements in smoothness and contrast. It demonstrates robustness against over 20 different types of attacks, such as *JPEG* compression, speckle, motion blur, median filtering, additive Gaussian noise, cropping, erasing, salt-and-pepper noise, and more. The technique achieves a zero *IER*, highlighting its fully reversible and lossless capabilities. Robust security measures are incorporated using *AES, LZW,* and *SHA-3*. The paper provides quantitative values such as *PSNR* and NC (Normalized Correlation) for watermarked images, considering both recovered *ROI* and the biometric watermark. The importance of medical imaging security, particularly during crises such as the *COVID-19* pandemic, has been highlighted in recent literature. The proposed technique demonstrates superior robustness, contrast enhancement, no visual perception, and no distortion when compared to existing techniques, as demonstrated through experimental results in related studies Islam et al. (2020); Muhammad et al. (2020); Islam et al. (2021); Rahman et al. (2020); Al-Rakhami et al. (2021); Rahman et al. (2021); Asraf et al. (2020).

The chapter is structured in four sections: section 5.2 describes the proposed medical image authentication algorithm. In Section 5.3.1, The results from the experiments are presented and discussed. Finally, the last section 5.4 provides a conclusion for the proposed work.

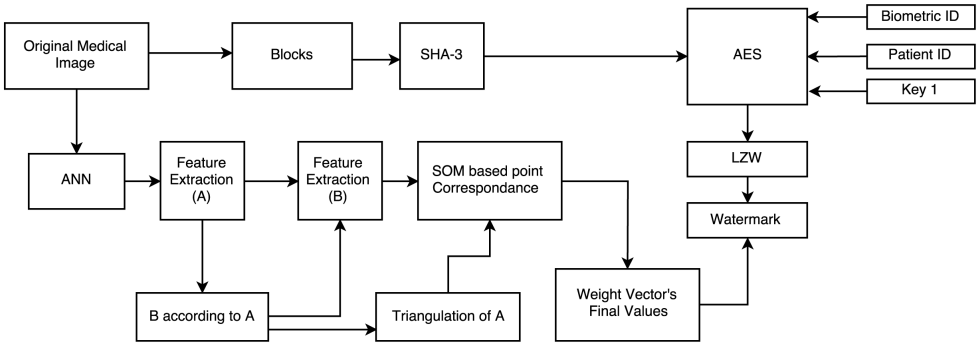


Figure 5.2: Watermark Creation with *ANN* feature extraction diagram.

5.2 Proposed Reversible Medical Watermarking Technique

Medical image constitutes two basic subparts: *ROI* and *RONI*. Hence, the authentication intactness of *ROI* is severely important for accurate diagnosis. The proposed robust reversible hybrid algorithm is based on the idea of protecting *ROI*. *ROI* and *RONI* are extracted by *ANN*. Then, different hiding schemes are used on both subparts for watermark embedding. *ROI* itself is used as watermark as shown in Figure 5.1. In this section, the creation of a watermark and extracting features for *ROI* and *RONI*, watermark embedding, and lossless watermark extraction algorithms are discussed along with the technique to eliminate overflow and underflow conditions.

5.2.1 Ahead-Preparations for Lossless Data Recovery

There are many techniques for data recovery at the receiver's end. Previous techniques generally use the average of pixel values of any size of the block. As Zain and Fauzi (2007) undertook an average for 2×2 block size for data recovery. Chiang et al. (2008),Kulkarni and Patil (2012),Zain and Fauzi (2006) uses 4×4 block size while Xiao et al. (2015) uses 8×8 for the tampered information. JPEG2000 of the *ROI* is also used by a few methods like Al-Qershi and Khoo (2009) and Al-Qershi and Khoo (2011), where the visual quality is compromised for the cover image. Although Thabit and Khoo (2017) used *IWT* for feature extraction and data recovery but robustness is only for few attacks like *JPEG* compression, *AGN*, salt and pepper. Firstly, feature extraction is done for the proposed technique, followed by watermark creation from the medical cover image itself.

- **Feature Extraction Algorithm**

  Figure 5.2 shows the Feature extraction (A) and feature extraction (B) after applying *ANN* to the medical cover image. This is the step-wise demonstration of how modules *A* and *B* are extracted by applying *ANN* while separating *ROI* and *RONI*. The following steps are used for

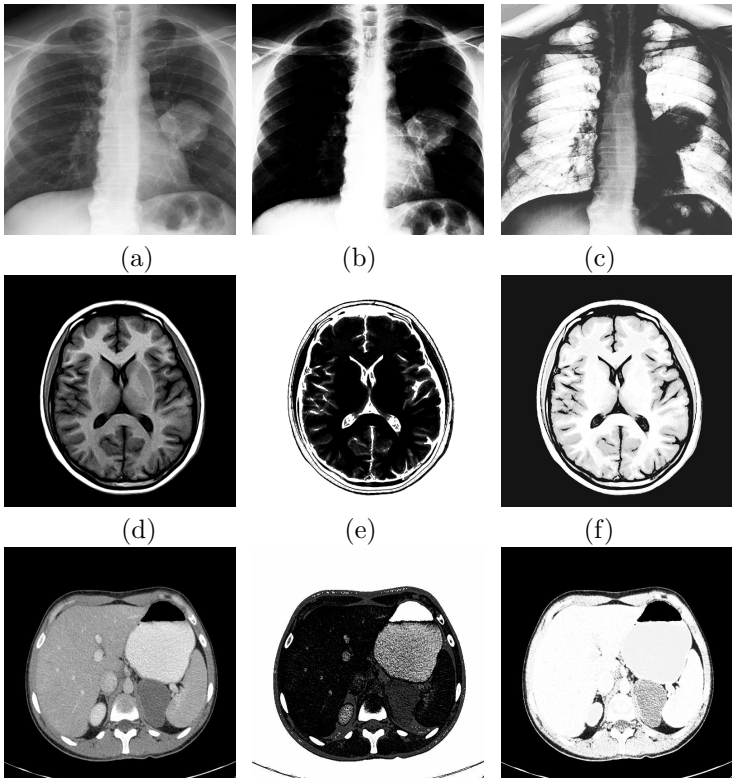


Figure 5.3: Examples to manifest medical cover images used while showing the difference in *ROI* and *RONI* by darkening the regions. (a) Original image 1, (b) *ROI* Region for image 1, (c) *RONI* Region for image 1, (d) Original image 2, (e) *ROI* Region for image 2, (f) *RONI* Region for image 2, (g) Original image 3, (h) *ROI* Region for image 3, (i) *RONI* Region for image 3.

feature extraction:

Step 1. Triangulation of A is done by defining a *SOM* according to the following:

- i 100 columns and 30 rows are selected to create a neurons grid *i.e.* (30×100).
- ii Initial weights of the grid neurons and *i.e.* a pentagonal, rectangular, or cylindrical bordered extracted pixels of the coordinate set are synchronized to same values.
- iii Finally, the neural network's input is the pixel value cartesian coordinates set from (4.11) and (4.12), and this needs to be triangulated with its topology.

Step 2. Topology of A is used to establish *SOM* from (4.13),(4.14) and *SOM's* are trained by using B:

- i **Topology of A :** The input layer of a *SOM* prototype is used for searching the corresponding points, which is necessary for replicating the topology of the set A.
- ii **Cartesian coordinates:** Each node of the wired frame is assigned one neuron, and the connections are the same between the wired frame and neurons. Neurons that aren't connected on the float set can't be connected within themselves. Corresponding wired frame node's (3D space) cartesian coordinates is the initial weight vector.

iii **Training of the network:** This is done by selecting points randomly from reference set B. The closest weight vector neuron is chosen to fire. The firing neuron's weight vector is well adjusted compared to its neighbouring neurons (window of 3×3).

Table 5.1: *ANN* extracted features and values for the image shown in Figure 5.1.

Number	Name	Values
1	Information measure of correlation	-0.0299
2	Difference entropy	1.8900
3	Maximum probability	0.6869
4	Entropy	2.7361
5	Inverse difference normalized	0.9017
6	Cluster Prominence	38.2978
7	Sum entropy	140.9200
8	Dissimilarity Energy	0.8989
9	Difference variance	1.9921
10	Correlation	0.1599
11	Sum of squares	0.2001
12	Autocorrelation	48.0001
13	ClusterShade	4.1927
14	Sum variance	14.5774
15	Homogeneity	0.6264
16	Contrast	1.8835
17	Sum average	48.0021

Table 5.1 gives the name of the features and feature values extracted from the proposed *ANN* algorithm.

- **Data Recovery from extracted features** Feature extraction and recovery are made on the medical cover image by applying *ANN*. A few examples of the output after feature extraction applied on the whole image rather than a window of 20×100 are shown in Figure 5.3. The demonstration of 3 medical cover images with the differences in *ROI* and *RONI* regions is reflected in Figure 5.3. The black regions in Figure 5.3 b, 5.3 e and 5.3 h shows the *ROI* of the images and the dark part in Figure 5.3 c, 5.3 f and 5.3 i illustrates the *RONI* of the same images with respect to medical cover image 5.3 a.

Step 1. During the triangulation of A, the *SOM* network converges, resulting in a triangulated subset of points referred to as *A1*. Each node in *A1* corresponds to a neuron in the *SOM* network (30×100 neurons), with an initial weighting vector (p_0, q_0, r_0) that matches the node's initial cartesian coordinates. Upon displacement, each node is assigned a final weighting vector (p_1, q_1, r_1), which coincides with a point in B.

Step 2. A one-to-one point correspondence is generated between neurons while *SOM* lateral interactions. Many points from A may correspond to a single point in B. To prevent such mismatches, a distance threshold criterion is employed. This criterion excludes corre-

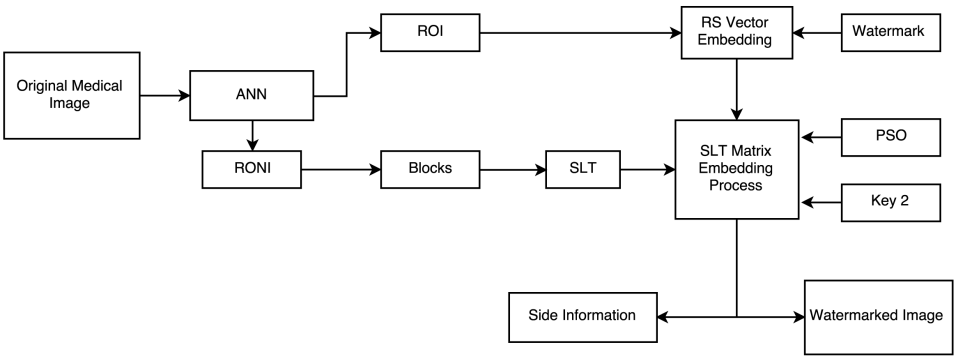


Figure 5.4: Watermark Embedding Technique.

sponding points more than five voxels apart, which helps avoid excessive deformation of the final warped image. As a result, the number of successful corresponding points is reduced to around 500 pairs of points for all patient data.

5.2.2 Watermark Creation Technique

Following are the summarized steps of the watermark creation algorithm, as depicted in Figure 5.2 :

Step 1. **Medical cover image division**: the medical cover image is categorized into its three *RGB* channels *i.e.* Red, Blue and Green.

Step 2. **Division into blocks**: the medical cover image is partitioned into 8×8 blocks.

Step 3. **Watermark**: Apply *SHA-3* on *ROI* to get encrypted *ROI*.

Step 4. **Apply *AES***: *AES* is applied to the output generated from third step with the concatenation of the key1, patient *ID* and biometric *ID*.

Step 5. ***LZW***: Finally, the watermark bits are compressed using LZW on the result of Step 4.

Step 6. **Watermark**: Result generated in the previous step is concatenated with final weight vectors for constructing the final watermark used in the medical cover image.

5.2.3 Watermark Embedding Technique for *RONI*

Following are the steps for the proposed watermark embedding technique, illustrated in Figure 5.4 :

Step 1. **Medical cover image division:** The medical cover image is partitioned into non-overlapping blocks denoted by NB_i, where i is the block index. Each of these blocks is subjected to the *SLT*

transformation (3.1), which results in four sub-bands: *LL, HL, HH* and *LH*. It is important to note that *s*, *S*, and SLT_N are of the same size. Sub-bands *HL* and *LH* are used to embed the watermark, while the high-frequency subband *HH* is not used for the proposed technique.

Step 2. **Calculating the threshold value:** The determination of threshold values *Th* for each block and *T* for the entire image is carried out using the *PSO* algorithm Kennedy and Eberhart (1995) using (3.3) and (3.4).

Step 3. **Watermark Embedding:** To embed a watermark bit in a selected block, the pixel values of the *SLT* coefficients in the high-frequency sub-bands, namely *HL* and *LH*, are modified by computing their difference. Specifically, when the watermark bit is '1', the pixel value of the *SLT* coefficients in the *HL* subband is increased compared to that in the *LH* subband. On the other hand, when the watermark bit is '0', the pixel value of the *LH* subband is increased compared to that in the *HL* subband.

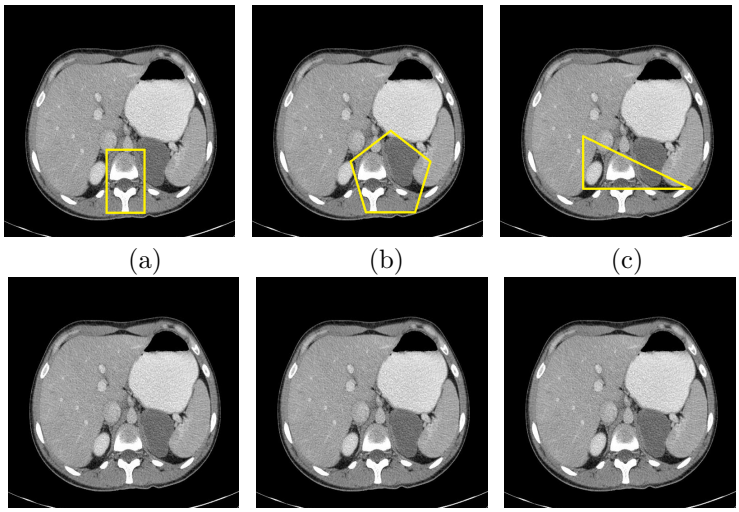


Figure 5.5: Images depicting watermark invisibility for image 1 with highlighted *ROI* in various shapes. The images of medical cover: (a) region 1 in image 1, (b) region 2 in image 1, and (c) region 3 in image 1. The images with watermarked: (d) region 1 in image 1, (e) region 2 in image 1, and (f) region 3 in image 1

To illustrate the embedding process, suppose there is a watermark sequence denoted by *w*, which is a sequence of bits represented as a vector w=[w_1,...,w_j,...,w_{len}]. Here, j =1, 2, ..., *len*, where *len* denotes the length of the watermark sequence *w*. To embed a watermark bit w_j into a given block, a threshold value denoted by T from step 2 is utilized. Additionally, the alteration factors described in (3.3) and (3.4) are employed with each watermark bit w_j. The following rules are used for embedding:

If w_j=1 and (ρ^{HL} - ρ^{LH}) ≥T, then the block remains unchanged.
If w_j=1 and (ρ^{HL} - ρ^{LH}) <T, then $\rho^{HL}_{new} = \rho^{HL} + ATF_1$ and $\rho^{LH}_{new} = \rho^{LH}$ - ATF_1.

If w_j=0 and (ρ^{LH} - ρ^{HL})≥T, then the block remains without change.

If w_j=0 and (ρ^{LH} - ρ^{HL}) <T, then $\rho^{HL}_{new} = \rho^{HL}$ - ATF_2 and $\rho^{HL}_{new} = \rho^{HL} + ATF_2$

Alteration factors, ATF_1 and ATF_2, have been calculated as:

$$ATF_1 = [\rho^{HL} + \phi] - [T - (\rho^{HL} - \rho^{LH})/(Th)] \tag{5.1}$$

$$ATF_2 = [\rho^{LH} + \phi] + [T - (\rho^{LH} - \rho^{HL})/(Th)] \tag{5.2}$$

The variable ϕ represents the ratio between each block's mean and standard deviation. It is important to note that the difference between the pixel values of the selected sub-bands is saved as side information in order to ensure reversibility when embedding the watermark bit.

Step 4. **ISLT**: The embedding process for the watermark continues until all bits have been embedded. The modified sub-bands replace the original sub-bands, and the *ISLT* is applied to the modified sub-bands using matrix multiplication as shown in (3.2).

In order to maintain reversibility, the output of the previous step must be rounded up to integers. This guarantees that the watermarked image and the medical cover image can be restored to the recipient just like the original.

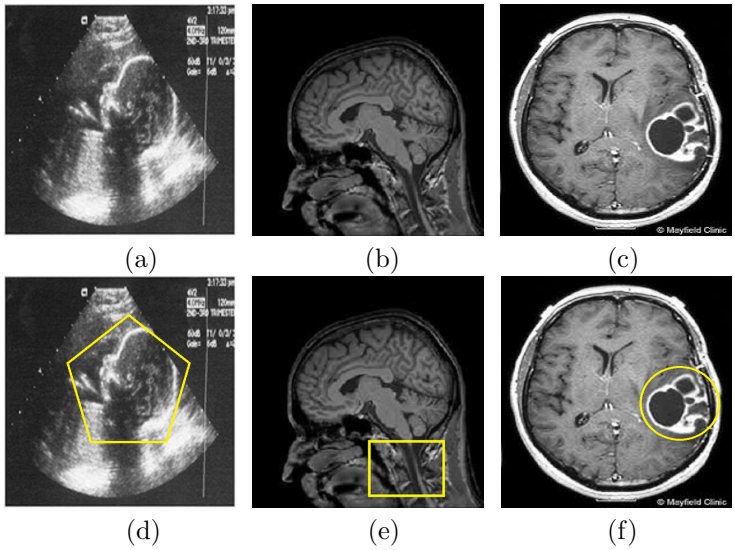


Figure 5.6: Three Images showing the visual quality. (a) Medical cover image 2, (b) Medical cover image 3, (c) Medical cover image 4, (d) Watermarked image 2 with *ROI* in pentagon, (e) Watermarked image 3 with *ROI* in rectangle, and (f) Watermarked image 4 with *ROI* in circle .

5.2.4 Watermark Embedding Technique for ROI

Step 1. **Watermark embedding using RS vector:** In this method, the image is partitioned into groups of four pixels. Each group is considered a single value for embedding the watermark.

Step 2. **Discrimination Function:** Prior to forming groups, a Discrimination Function (f) and a Flipping function (FF) must be defined. The Discrimination Function is used to describe the state of the group and is calculated using the Eq. (5.3) as follows:

$$f(group) = \sum_{i=1}^{i=3} |x_{i+1} - x_i| \tag{5.3}$$

where Group = $\{x_1, x_2, x_3, x_4\}$, and the notation x_i is used to represent the pixel value of the ith pixel within the current group.

Step 3. **Flipping Function:** FF is applied to alter the pixel values of an image. It is applied within each bock by flipping the *LSB* of the two middle pixels. To determine the state of each group before (fo) and after (fu) applying the FF, the discrimination function is calculated using Eq. (5.3). The state of each group is determined based on the following criteria:

- *RG* Group: if $fu > fo$
- *SG* Group: if $fu < fo$
- *UG* Group: if $fu = fo$

Step 4. **Creating RS Vector:** The RS Vector is created by assigning a single value to each group of pixels in the image. Watermark bit '1' is embedded in the Regular group (RG), '0' in the Singular group (SG), and the Unused group (UG) remains unaltered as the FF does not impact it. Consequently, the RS Vector comprises a series of bits (0s and 1s), each denoting the state of a specific group of pixels. Finally, the watermarked image is formed by merging the groups and the accompanying side information.

5.2.5 Overflow and Underflow

To prevent underflow or overflow of pixel values during the watermark embedding process, the proposed technique employs pixel adjustment as a concurrent step. The adjustment is performed by shifting the value of each target pixel, enhancing the watermarked image's visual quality. Overflow or underflow condition of the pixel values modifies the watermarking formulas, and the corresponding information is stored as side information. The adjustment applied to these pixels involves the following transformation using Equation $I_w(i, j)$ from subsection 3.2.4.

5.2.6 Watermark Extraction Technique for *RONI* and *ROI*

Step 1. **Image division:** To retrieve the watermark at the receiver's end, the watermarked image is read along with the side information, and the pixels that are previously adjusted during

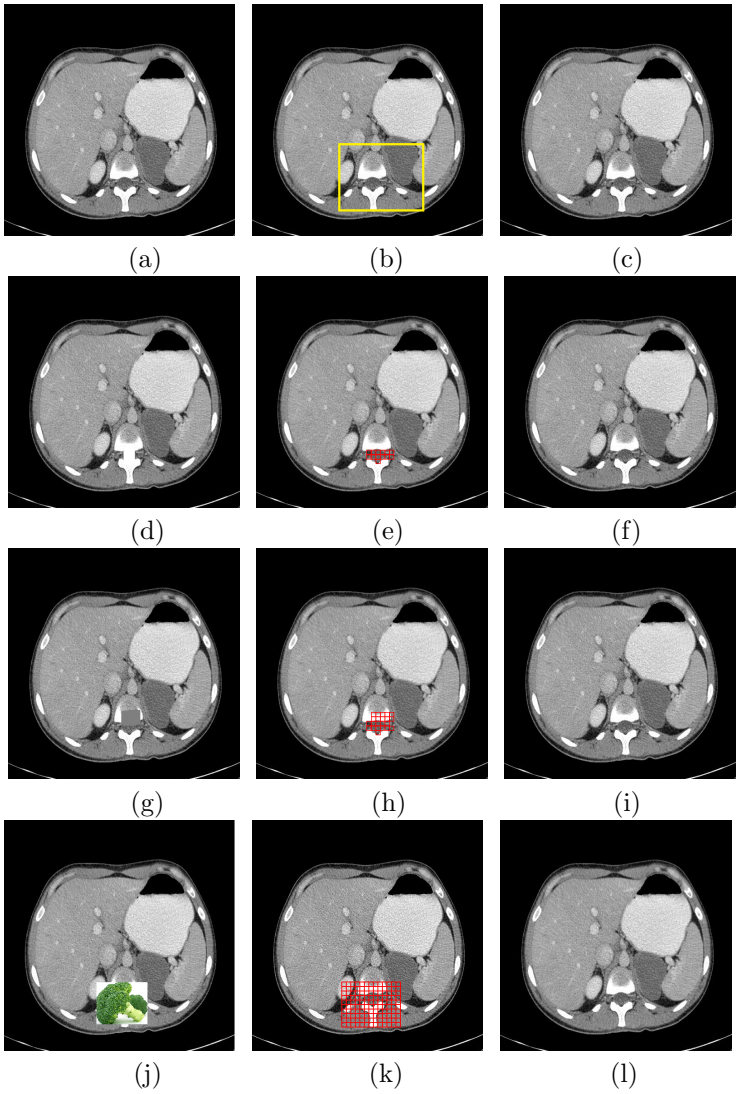


Figure 5.7: Different types of tempering, temper detection, localization, and recovery for the medical image. (a) image with medical cover, (b) Image with selected *ROI*, (c) Image with Watermarked, (d) Tampering1 (erasing data from *ROI*), (e) Tampering1 and its localization, (f) Recovery of data from Tampering1, (g) Tampering2 (copy and paste), (h)Tampering2 and its localization, (i) Recovery of data after Tampering2,(g) Tampering3 (adding new substance), (h) Tampering3 and its localization, (i) Recovery of original data after Tampering3

the watermark embedding process are relocated to their original positions. Subsequently, the watermarked image is divided into non-overlapping blocks.

Step 2. **SLT application:** The next step involves applying the *SLT* to each block to obtain its sub-bands.

Step 3. **SLT-based Watermark Extraction:** To extract the watermark, the ratio between the mean and standard deviation values of the coefficients in the high-frequency sub-bands, i.e., *HL* and *LH*, is computed for each block and the following equations are used for watermark extraction:

$$w_j^* = 1, \text{ if } (\rho_{new}^{HL} - \phi^{'}) \geq (\rho_{new}^{LH} - \phi^{'})$$
$$w_j^* = 0, \text{ if } (\rho_{new}^{HL} - \phi^{'}) < (\rho_{new}^{LH} - \phi^{'})$$

In the above equation, w^*j represents the extracted bit. The variables $\rho^{HL}new$ and ρ_{new}^{LH} denote the pixel values of the slantlet transformation coefficients in the high-frequency sub-bands *HL* and *LH*, respectively. The variable $\phi^{'}$ represents the difference between the ϕ value of the original image and the ϕ value of the watermarked image.

Step 4. **RS Vector based Watermark Extraction**: The image is divided into groups of four pixels. For each *RS* vector, f and F are determined. The embedded watermark is then extracted by identifying the *RG*, *SG*, and *UG*.

Step 5. **Medical cover image recovery:** To recover the medical cover image, the extracted watermark bits and saved ϕ values from the side information are used to restore the original pixel values of each block. This is achieved by reversing the process used during watermark embedding. Each block containing the extracted watermark and different values can be used to recover the original mean value by shifting back the mean values. Finally, rearranging the image blocks can reconstruct the medical cover image.

5.3 Experimental Results

The proposed watermarking technique has been assessed based on several criteria: visual quality, confidentiality, security, capacity, integrity, invisibility, robustness, reversibility, and tamper detection and localization. In addition, the effect of size of the block and threshold values on the technique's quality is also analyzed. The watermark's invisibility is assessed using the *PSNR* parameter, which measures the ability of the watermark to remain undetectable without degrading the perceptibility of the medical cover image. The term "robustness" in the context of watermarking refers to the capability of the watermark to remain detectable even after the watermarked image has been subjected

Table 5.2: *PSNR*(dB) with capacity(bits) for the proposed technique from Figures 5.5 and 5.6.

Image	Total Capacity	RONI	ROI	PSNR(dB)
image 1, region 1	63,440	52,933	10,507	57.82
image 1, region 2	62,520	32,766	29,754	56.25
image 1, region 3	62,980	49,420	14,560	56.64
image 2	56,200	19,095	37,105	50.83
image 3	63,256	45,016	18,240	56.87
image 4	64,320	58,318	6,002	59.26

to various types of image distortions, such as noise or compression. Capacity, on the other hand, depicts the maximum amount of data bits that can be embedded into a single host image while still maintaining the watermark detectable. As the watermarking capacity increases, there is a trade-off between security and *PSNR*. The reversibility of the watermarking technique, is indicated by the capability of the lossless recovery of the original medical cover image after watermark extraction. It is an important factor in evaluating the proposed technique. In this research, the proposed technique is tested on a data-set comprising 300 medical images that are transformed and resized into 512×512 pixels gray-scaled images to ensure consistency in the comparison. The effectiveness of the proposed technique is checked using several metrics outlined in the following subsections.

5.3.1 Invisibility Evaluation

The term "invisibility" in the watermarking world refers to the effectiveness of a watermarking technique to embed a watermark into an image without causing any noticeable visual degradation. The difference in the *PSNR* value between the watermarked and original images determines the image quality or invisibility, as illustrated in Eq. 1.1.

Measuring the information volume that can be encoded into the host image is one way to evaluate the capacity of the watermarking technique. This should be done without any noticeable visual degradation or significant decrease in the *PSNR*.

To calculate the capacity of each medical cover image, Eq. (1.4) is employed, which considers the image's height and width.

Table 5.2 presents the experimental results for the proposed watermarking technique applied to the *ROI* and *RONI* regions of medical images. Eq. (1.4) is utilized to estimate the capacity of the watermark. *PSNR* is calculated in decibels (dB) which is reported in the table as a measure for evaluating the watermarked image's quality.

The selected *ROI* and corresponding watermarked images are shown in Figure 5.5 and 5.6, respectively. The *ROI* bits are obtained after compressing the patient's text *ID* and biometric *ID* before adding them to the *ROI* region. On the other hand, the *RONI* bits are obtained after compressing the *ROI* region and the final weight vector values. To further compress the *ROI* bits,

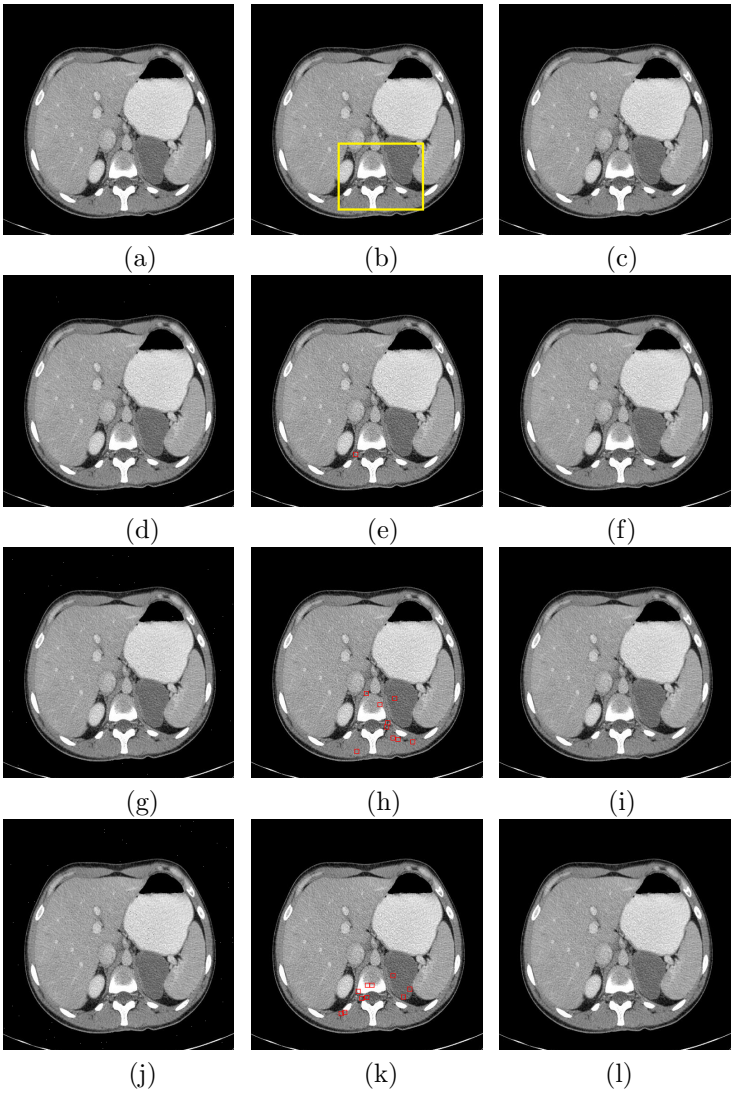


Figure 5.8: Robustness against salt-and-pepper (SP) noise is depicted for the medical cover image (a). (b) Selected *ROI*, (c)Watermarked image, (d) SP (0.0002), (e) Localization of SP(0.0002), (f) Recovery of SP (0.0002), (g) SP (0.0005), (h) Localization of SP (0.0005), (i) Recovery of SP (0.0005) (j) SP (0.0008), (k) Localization of SP (0.0008), (l) Recovery of SP (0.0008)

the *LZW* algorithm is applied before creating the final watermark.

Table 5.2 demonstrates the feasibility of the proposed watermarking technique, with total capacities ranging from 56,200 to 64,320 bits for the *ROI* and *RONI* regions. The achieved *PSNR* values are above 50 *dB*, indicating that the watermark is not detectable by the human eye. In conclusion, the proposed watermarking technique can effectively embed a significant number of bits in medical images while preserving their visual quality.

5.3.2 Authenticity and Integrity

Regarding medical images, ensuring security and authenticity is of utmost importance. Modifying the image content can potentially damage the *ROI*, emphasizing the criticality of preserving the image's integrity. The proposed method provides a means for verifying the genuineness and reliability of

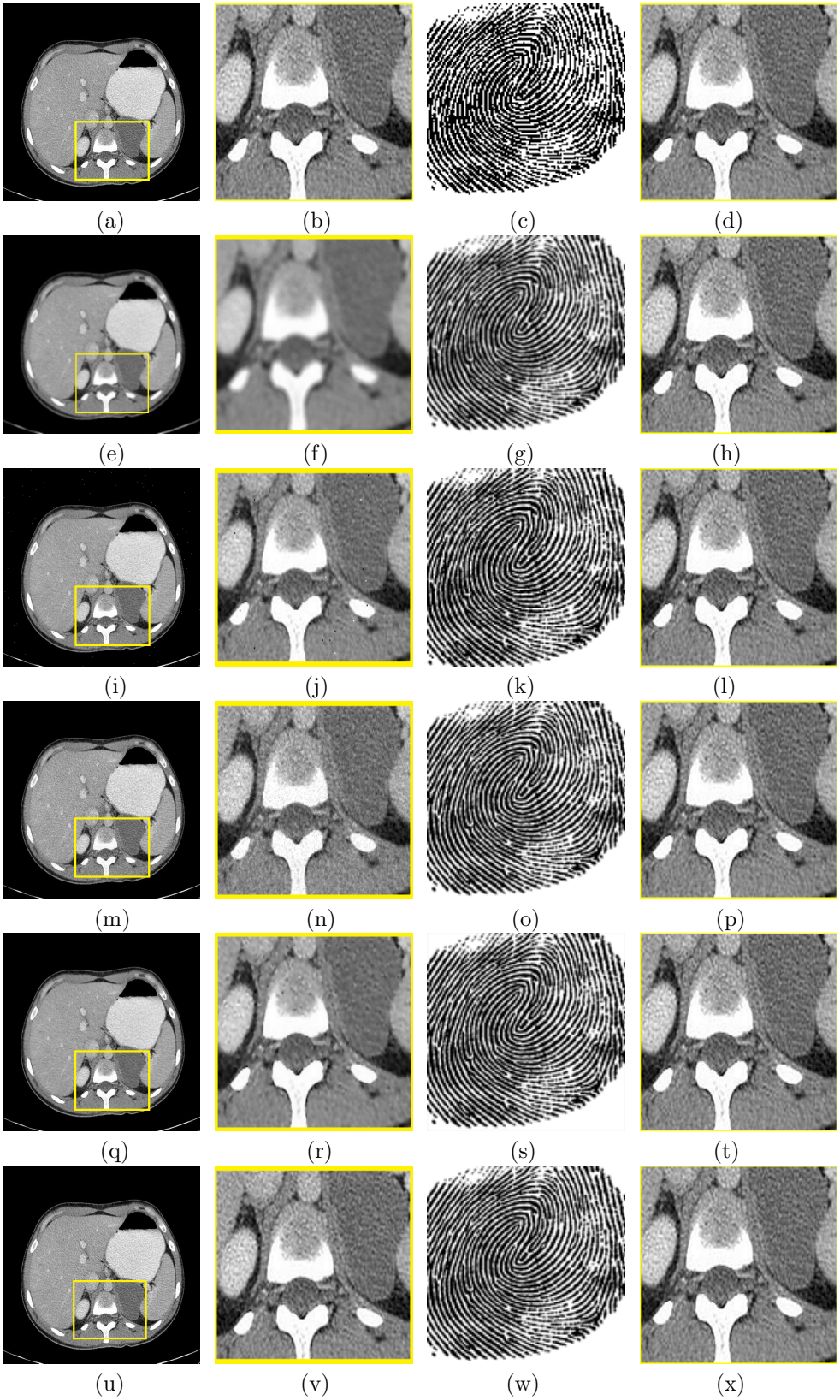


Figure 5.9: Attacks to demonstrate *ROI* and biometric ID extracted and tamper recovery. (a) Watermarked image without attacks, (b) Selected *ROI* (without attacks) (c) Extracted Biometric ID, (d) Extracted *ROI*, (e) Tamper (A) Blurr, (f) Selected *ROI* after Tamper (A), (g) Extracted Biometric ID after Tamper (A), (h) Recovery of Tamper (A), (i) Tamper (B) SALT and PEPPER (0.01), (j) Selected *ROI* after Tamper(B),(k) Extracted Biometric ID (B), (l)Recovery (B),(m) Tamper(C) POISSON Attack, (n) Selected *ROI* (C), (o) Extracted Biometric ID (C), (p) Recovery (C) (q) Tamper(D) WEINER Attack, (r) Selected *ROI* (D),(s) Extracted Biometric ID (D), (t) Recovery (D) (u) Tamper (E) RESIZE, (v) Selected *ROI* (E),(w) Extracted Biometric ID (E), (x) Recovery (E)

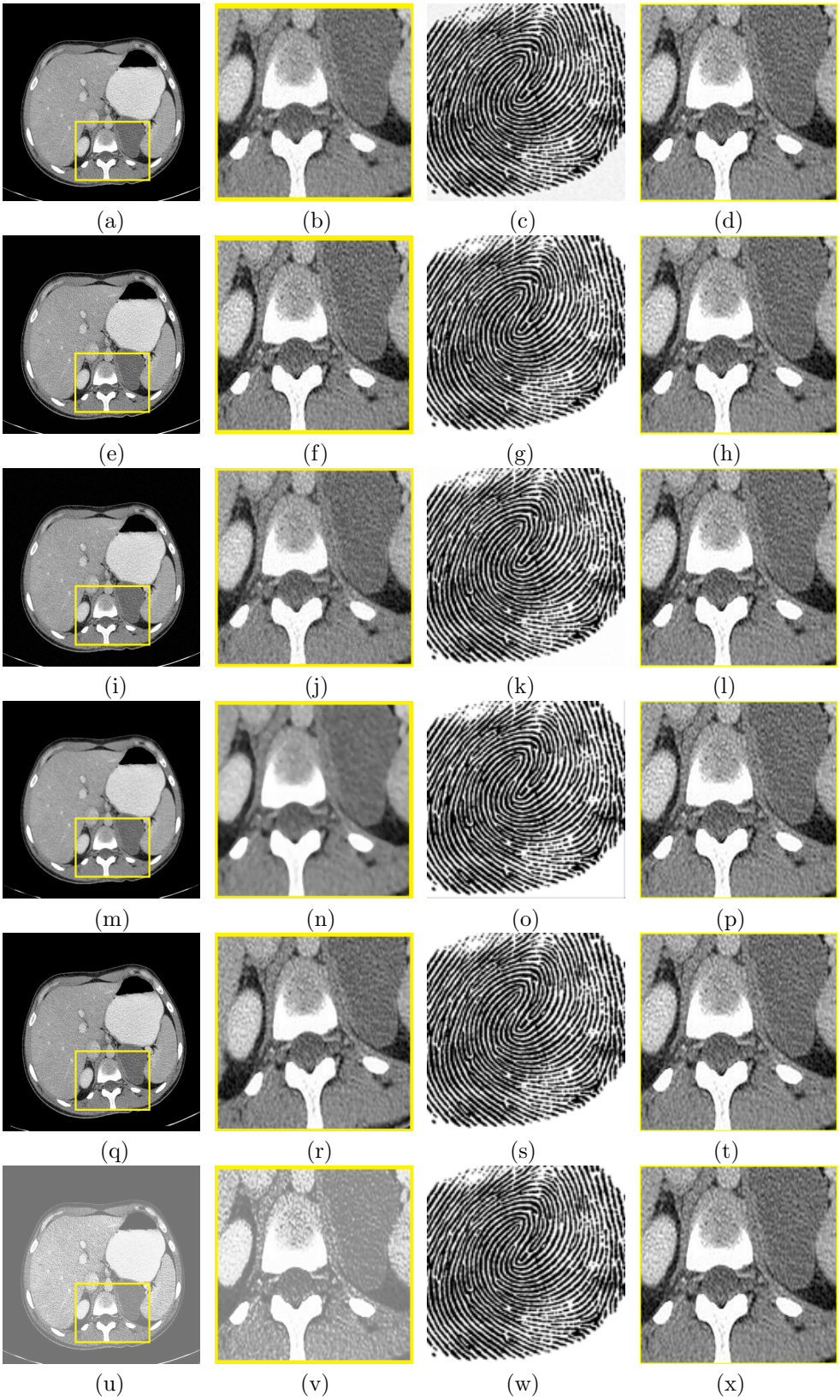


Figure 5.10: Attacks to demonstrate *ROI* and biometric ID extracted and tamper recovery. (a) Tamper (F) SPECKLE Attack, (b) Selected *ROI* after Tamper (F) (c) Extracted Biometric ID after Tamper (F), (d) Recovery of Tamper (F), (e) Tamper (G) *JPEG* compression 70%, (f) Selected *ROI* (G), (g) Extracted Biometric ID (G), (h) Recovery (G), (i) Tamper (H) AGN (0.0008), (j) Selected *ROI* (H),(k) Extracted Biometric ID (h), (l) Recovery (H),(m) Tamper(I) MEDIAN filter (4×4), (n) Selected *ROI* (I), (o) Extracted Biometric ID (I), (p) Recovery (I) (q) Tamper(J) GEOMETRIC ROTATION, (r) Selected *ROI* (J),(s) Extracted Biometric ID (J), (t) Recovery (J) (u) Tamper (K) HISTOGRAM EQUALIZATION, (v) Selected *ROI* (K),(w) Extracted Biometric ID (K), (x) Recovery (K)

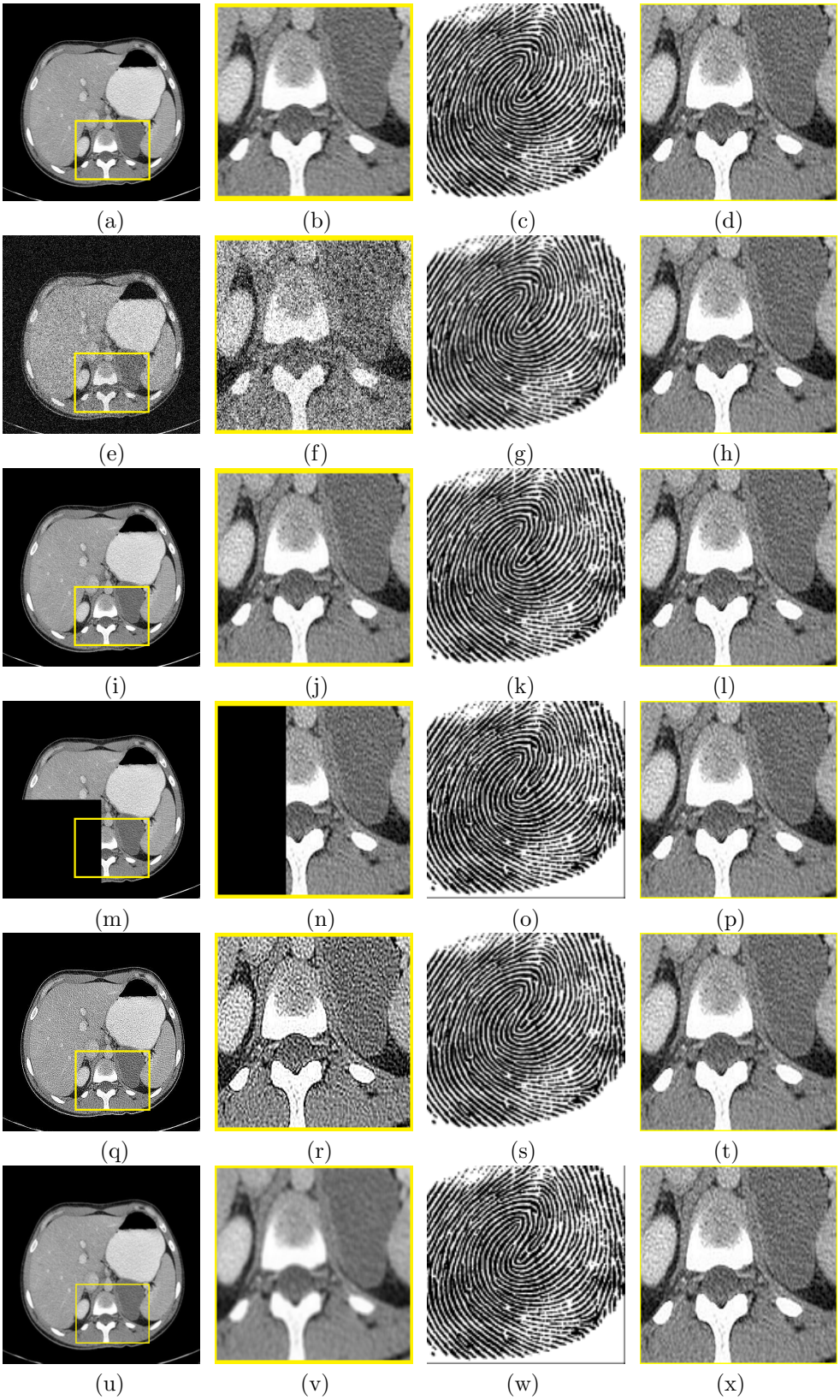


Figure 5.11: Attacks to demonstrate *ROI* and biometric ID extracted and tamper recovery. (a) Tamper (L) MOTION BLUR, (b) Selected *ROI* after Tamper (L) (c) Extracted Biometric ID after Tamper (L), (d) Recovery of Tamper (L), (e) Tamper (M) ADJUST, (f) Selected *ROI* (M), (g) Extracted Biometric ID (M), (h) Recovery (M), (i) Tamper (N) GAUSSIAN Filter, (j) Selected *ROI* (N),(k) Extracted Biometric ID (N), (l) Recovery (N),(m) Tamper(O) CROPPING (64×64), (n) Selected *ROI* (O), (o) Extracted Biometric ID (O), (p) Recovery (O) (q) Tamper(P) SHARPENING, (r) Selected *ROI* (P),(s) Extracted Biometric ID (P), (t) Recovery (P) (u) Tamper (Q) AVERAGE(4×4), (v) Selected *ROI* (Q),(w) Extracted Biometric ID (Q), (x) Recovery (Q)

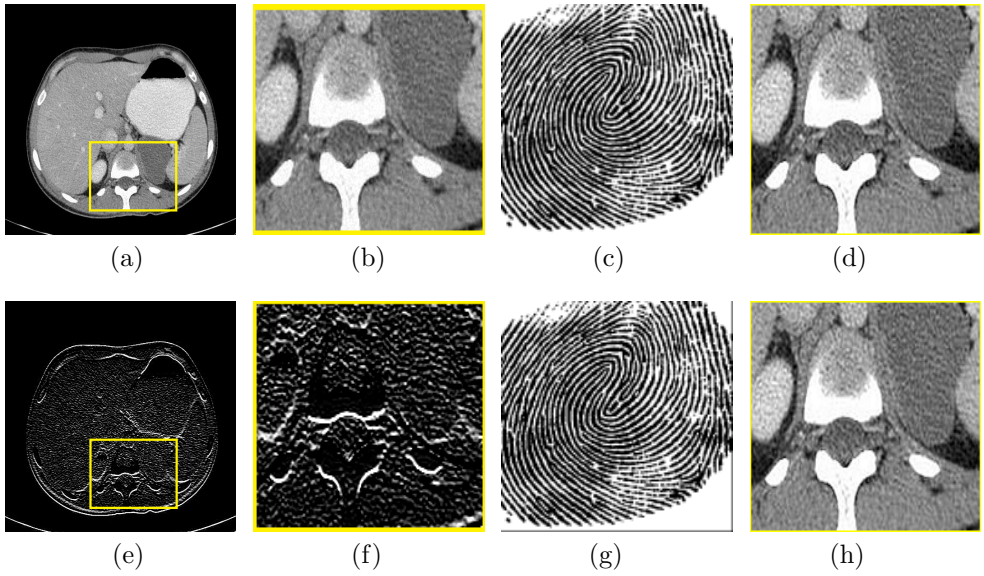


Figure 5.12: Attacks to demonstrate *ROI* and biometric ID extracted and tamper recovery. (a) Tamper (R) SMOOTHENING, (b) Selected *ROI* after Tamper (R) (c) Extracted Biometric ID after Tamper (R), (d) Recovery of Tamper (R), (e) Tamper (S) SOBEL, (f) Selected *ROI* (S), (g) Extracted Biometric ID (S), (h) Recovery (S).

medical images.

Tamper Detection and localization: The proposed technique is remarkable for detecting and pinpointing tampering in medical images. It offers significant benefits in assuring patient information's authenticity, integrity, and confidentiality. The technique employs a watermarking approach that utilizes three components to create an encrypted watermark for detecting and localizing unauthorized changes to the image. The first component is the patient's biometric *ID* (e.g., thumbprint), which serves as a unique identification mark to ensure the patient's authenticity and integrity. The second component is the patient *ID*, represented as a text watermark, which safeguards the confidentiality of the patient's personal information.The third element comprises the *ROI* blocks extracted from the medical coverage image, which facilitate identification and pinpointing of any corrupted areas in the medical image.

The proposed technique offers several advantages over existing tamper detection and localization methods. Firstly, it provides higher security and confidentiality for patient data by utilizing a biometric *ID* and text watermark for the patient's identification and personal details. Secondly, the use of *ROI* blocks enables the identification and localization of corrupted regions in the image, thereby facilitating the timely detection and correction of any errors. Finally, the proposed technique is highly efficient and scalable, making it ideal for large-scale medical image datasets. Overall, the proposed technique offers a robust and secure solution for detecting and localizing tampering in medical images., making it highly suitable for clinical and research applications.

Figure 5.7 depicts the demonstration of tamper localization and recovery. Figure 5.7 is the step

wise illustration of the medical cover image, then selection of *ROI* in yellow square region (Figure 5.7 c) is the Watermarked image. There various types of tempering done with the watermarked image like erasing Figure 5.7 d, copy/paste Figure 5.7 j and new addition of broccoli image in the medical cover image (Figure 5.7 g). Figures 5.7 e, 5.7 h, 5.7 k shows working of the proposed technique with the localization of the erased area and Figures 5.7 f, 5.7 i, 5.7 l illustrates working of the proposed robust algorithm in recovery of the lost data.The proposed technique demonstrates remarkable robustness to salt-and-pepper noise, with noise values ranging from 0.0002 to 0.00008. as demonstrated in Figure 5.8. The results clearly illustrate the technique's effectiveness in tamper detection and localization. The effectiveness of the suggested method is visually demonstrated by the experimental results presented in Figures 5.7 and 5.8. These findings indicate that the technique is a promising solution for addressing the problem of unauthorized image tampering in medical imaging applications.

5.3.3 Reversibility Evaluation

The *IER* is calculated to evaluate the proposed technique's reversibility. The *IER* is obtained by dividing the sum of all the images with erroneous recoveries (i.e., those containing pixels with values different from the expected ones) by the total number of test images of each category. Impressively, the suggested approach achieved an *IER* value of "ZERO," indicating that all cover images and watermarks are retrieved without any data loss or errors. This outcome highlights the technique's robustness and its capability to retrieve the medical cover image and watermark with high accuracy.

5.3.4 Robustness Evaluation

In order to evaluate the efficacy of the proposed technique, a range of tests are implemented on the watermarked images using various intentional and unintentional attacks. These attacks comprised *JPEG* compression with different quality factors and variances, and other typical image processing operations like rotation, cropping, and resizing. After extracting the watermarks from the tampered images, their *NC* and *PSNR* values are used to evaluate the resulting images. The data presented in Figure 5.13 supports the claim that the proposed technique is robust. The results indicate that the watermarked images remain resistant to these attacks and can be retrieved with high *NC* and *PSNR* values.

In addition to intentional attacks, the suggested technique underwent testing to against unintentional attacks such as, speckle noise, salt-and-pepper noise, and gaussian noise. Figures 5.9 to 5.12 illustrate these attacks on the watermarked images, along with the selected regions of interest (*ROI*) used for tamper localization. The proposed technique is found to be highly effective in localizing and detecting any tampering with the watermarked images, with the recovery of the *ROI*

Table 5.3: Comparision of *PSNR* (dB), BPP and time complexity(TC) (in seconds) of the Proposed Technique with Existing Techniques.

Techniques	PSNR	BPP	TC
Alattar (2004)	29.23	0.74	Low
Shih and Zhong (2016)	48.53	1.10	–
Shih and Wu (2005)	38.0	1.00	High (240s)
Thodi and Rodríguez (2007)	29.39	0.99	–
Tian (2003)	31.48	0.49	Low
Wakatani (2002)	22.36	2.00	–
Wang et al. (2013)	51.24	0.54	Low
Zain and Clarke (2011)	31.70	1.06	–
Zhao et al. (2011)	44.64	0.22	–
Bamal and Kasana (2018)	50.14	1.122	Low(3.65s)
Bamal and Kasana (2019)	48.89	1.81	Low (34.31s)
Proposed Algorithm	51.62	1.1225	Low (48.28s)

and biometric *ID* of the patient providing a high level of security and authenticity. The results of these experiments provide compelling evidence of the effectiveness and dependability of the proposed technique in protecting sensitive medical images from unauthorized access and tampering. Naming of the attacks are done from Figures 5.9 - 5.12 like A-blurred attack, B-salt and pepper, C-poission attack, D-weiner, E-resize(1.02), F-Speckle(0.01), G-JPEG compression (70%), H-additive gaussian noise (AGN), I-median filter 4×4, J-geometric rotation (5 degrees), K-histogram equalization(256), L-motion blur, M-adjust (0.3, 0.7), N-gaussian filter, O-cropped 64×64, P-sharpen,Q-average, R-smooth and S-sobel. The data presented in Figure 5.13 depicts the values of *PSNR* and *NC* for the original medical cover image, which is obtained after extracting the watermark from an attacked watermarked image. It is worth noting that the *PSNR* of the watermarked image prior to the attacks is 57.55 dB. The image used to get histogram and graph in Figures 5.13 are taken from Figures 5.9 - 5.12. Histogram in Figure 5.13 clearly depicts that *PSNR* value is directly proportional to *NC*. For example, N-gaussian filter has *PSNR* 49.82 dB for cover image and 32.52 dB for the extracted biometric watermark with $0.99NC$ for both whereas, after S-sobel *PSNR* reduces to 16.11 dB, 14.36 dB with 0.34,0.26 *NC*, respectively. The proposed technique does not work best with attacks like resizing the image and sobel.

5.3.5 Security of the watermark

To ensure digital data security, this technique uses two efficient cryptographic algorithms, namely *SHA-3* and *AES*. The watermark used in the proposed technique is made from four components: patient *ID* as a text watermark block of *ROI*, patient biometric *ID*, and key1. First, the blocks of *ROI* are encrypted using *SHA-3* with a 512-bit key for high-level security. Next, the hash values obtained from the encryption process are combined with the other three watermark components and

Table 5.4: Comparison with state of the art and proposed technique against different methodologies. Authentication data (AD), Patient's Data (PD), Recovery Data (RD)

Techniques	Objectives	*ROI* based	Embedding Technique	Embedded Data
Woo et al. (2005)	Authentication and data hiding	No	DWT + LSB	AD and PD
Giakoumaki et al. (2006a)	Authentication and data hiding	Yes	DWT in Transform domain	AD and PD
Giakoumaki et al. (2006b)	Authentication and data hiding	Yes	DWT in Transform domain	AD and PD
Zain and Fauzi (2006)	Authentication	No	LSB in Spatial domain	AD and RD
Zain and Clarke (2007)	Authentication	Yes	LSB in Spatial domain	AD
Zain and Fauzi (2007)	Authentication	Yes	LSB in Spatial domain	AD and RD
Chiang et al. (2008)	Authentication	No	Modified DE	AD and RD
Wu et al. (2008)	Authentication	No	DCT in Transform domain	AD and RD
Guo and Zhuang (2009)	Authentication and data hiding	Yes	Modified DE	AD and PD
Al-Qershi and Khoo (2009)	Authentication and data hiding	Yes	DE + Modified DE	AD, RD, and PD
Memon (2010)	Authentication and data hiding	Yes	LSB in Spatial domain	AD and PD
Tian et al. (2011)	Authentication and data hiding	Yes	DCT	AD
Al-Qershi and Khoo (2011)	Authentication and data hiding	Yes	DWT + Modified DE	AD, RD, and PD
Kulkarni and Patil (2012)	Authentication and data hiding	Yes	DE	AD, RD, and PD
Naseem et al. (2013)	Authentication and data hiding	Yes	LSB in Spatial domain	AD
Dragoi and Coltuc (2015)	Data hiding	No	Spatial domain Prediction	secret message
Mao et al. (2015)	Data hiding	No	Distortion-oriented, minimized + DWT	secret message
Li et al. (2015)	Authentication and data hiding	No	Rhombus Prediction + Histogram Modification	secret message
Wu et al. (2015a)	Authentication and data hiding	No	Modified pixel value + LSB	AD and side information
Wu et al. (2015b)	Authentication and Data Hiding	Yes	Pixel replacement	AD and side information
Xiao et al. (2015)	Authentication	No	Histogram modification of discrete Haar wavelet coefficients	AD
Gao et al. (2017)	Authentication and data hiding	Yes	Histogram modification	secret message and side information
Luo et al. (2021)	Authentication and data hiding	Yes	SLT in transform domain	AD, RD, and PD
Thabit and Khoo (2017)	Authentication and data hiding	No	IWT + SVD	AD and RD
Proposed technique	Authentication and data hiding	Yes	SLT (transform)+ RS Vector (spatial)	AD, RD, and PD

Table 5.5: Comparison with sate-of-the-art and proposed technique against desirable parameters.

Techniques	Tamper Localization	Tamper Recovery	Reversibility	Robustness	Contrast Enhancement	Visual Perception Distortion
Woo et al. (2005)	No	No	No	Fragile	No	No
Giakoumaki et al. (2006a)	No	No	No	Robust against JPEG compression	No	No
Giakoumaki et al. (2006b)	No	No	No	Robust against JPEG compression	No	No
Zain and Fauzi (2006)	Yes	Average of 4×4 blocks	No	Fragile	No	Yes
Zain and Clarke (2007)	No	No	Yes	Fragile	No	No
Zain and Fauzi (2007)	Yes	Average of 2×2 blocks	No	Fragile	No	Yes
Chiang et al. (2008)	Yes	Average of 4×4 blocks	Yes	Fragile	No	No
Wu et al. (2008)	Yes	JPEG compression of the blocks	Yes	Not Tested	No	No
Guo and Zhuang (2009)	No	No	Yes	Fragile	No	No
Al-Qershi and Khoo (2009)	Yes	JPEG2000 of the ROI	Only ROI	Fragile	No	Yes
Memon (2010)	No	No	No	Fragile	No	Yes
Tian et al. (2011)	Yes	No	No	Robust to Filtering and JPEG compression attacks	No	No
Al-Qershi and Khoo (2011)	Yes	JPEG2000 of the ROI	Only ROI	Robust against Salt and Pepper	No	No
Kulkarni and Patil (2012)	Yes	Average of 4×4 blocks	Only ROI	Fragile	No	No
Naseem et al. (2013)	No	No	Only ROI	Fragile	No	No
Dragoi and Coltuc (2015)	No	No	Yes	Fragile	No	No
Mao et al. (2015)	No	No	Yes	Fragile	No	No
Li et al. (2015)	No	No	Yes	Fragile	No	No
Wu et al. (2015a)	No	No	Yes	Fragile	Yes	No
Wu et al. (2015b)	No	No	Yes	Fragile	Yes	No
Xiao et al. (2015)	Yes	Average of 8×8 blocks	Yes	Fragile	No	No
Gao et al. (2017)	Yes	No	Yes	Robust against tampering attacks like copy-paste, text-addition, and content-removal	Yes	No
Thabit and Khoo (2017)	Yes	IWT applied on ROI to modify selected coefficients	Only ROI	Robust against attacks like Salt and Pepper, AGN and JPEG Compression	No	No
Proposed technique	Yes	Selected and modified feature extracted ANN bits of ROI	Yes	Robust against attacks in Figure 10-13	Yes	No

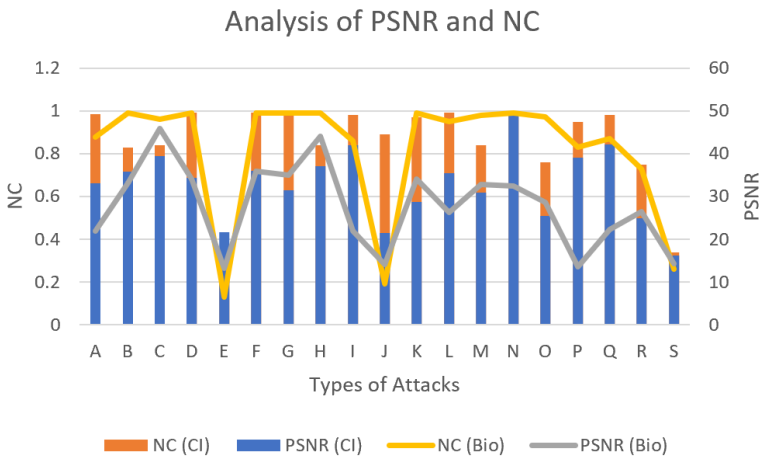


Figure 5.13: Analysis of *PSNR* *d*B and*NC* values of the cover image9 (CI) after attacks and extracted biometric (Bio) ID after various attacks. Attacks, namely A-S are from Figures 10-13

AES-256 encryption.

The *AES* algorithm employs 14 rounds of encryption, making breaking it highly complex. It uses a key expansion process to generate round keys each time. *AES* 256-bit is virtually impenetrable even with brute force attack after 2^{124} operations approximately. The best feasibility of an attack being successful after *AES-256* is side-channel attacks, which is not an issue with image watermarking. On the other hand, the biclique attack can take at most 4 bits off the key space, still leaving security in 124 bits minimally. The proposed technique ensures perfect resistance against a man-in-the-middle attack. On the other hand, threshold with *SLT* makes the denoising attack reversible. In the case of a compromised key attack, the *AES-256* algorithm used in the proposed technique can withstand such attacks as it employs 14 rounds of encryption.

5.3.6 Comparison with Techniques

The proposed technique is compared to other state-of-the-art reversible watermarking techniques in the medical field. The results show that it outperforms its counterparts in quality and capacity by a significant margin. To be specific, a watermark consisting of 61,440 bits of information are embedded into a 256×256 *MRI* brain image (image 3 from Figure 5.6) using a block size of 8×8.

The proposed technique enhances the *BPP* by as much as 410.227% when compared to Zhao et al. (2011). It is worth mentioning that the evaluation is performed solely on one channel of the *RGB* image. Nevertheless, when considering all three channels, the capacity of the proposed technique exceeds that of all other previously existing techniques listed in Table 5.3 by over 200%.

An acknowledgment for the execution time of the proposed technique that may vary based on the block size used and the system used for calculations. All the experiments concerning this research are executed on a computational data machine featuring an Intel(R) Core(TM) i7-4510U CPU clocked

at a frequency range of 2.00 GHz to 2.60 GHz, coupled with 8 GB of memory. Matlab(R2015a) is used to code and calculate the runtime duration of the experiments by using the tic and toc commands. It is a high-level numerical computing software for data analysis and scientific research. While the proposed technique may take more time than some of the existing work, it offers additional advantages in terms of security and resistance to various attacks compared to Bamal and Kasana (2018) and Bamal and Kasana (2019).

Table 5.4 projects the comparison of the difference in the type of proposed technique to existing ones. As shown, (Zain and Fauzi (2006), Chiang et al. (2008), Wu et al. (2008), Dragoi and Coltuc (2015), Mao et al. (2015), Li et al. (2015), Wu et al. (2015a), Xiao et al. (2015)) are the authentication or data hiding algorithms but are not *ROI* based techniques. The proposed technique is *ROI* based on three types of embedding data *i.e.* authentication data (*ROI*), recovery data (key1 and side information) and patients' data (text *ID* and biometric *ID*). Table 5.5 illustrates the comparison for the factors like tamper localization and recovery, reversibility, contrast enhancement, visual perception, and distortion. Thabit and Khoo (2017) is a reversible algorithm capable of tamper localization and recovery, robustness against three attacks with no distortion but no contrast enhancement. Only the proposed technique has achieved all factors desirably.

In conclusion, the proposed technique demonstrates superior performance in terms of robustness against more than 20 attacks while maintaining the perceptibility of the watermarked images with a good capacity. Contrast enhancement is done by using *RS* vector on *ROI*, which is highly important for image analysis by medical personnel. The advantages of the proposed work are achieved by leveraging the transformed sub-bands and using both the spatial and transform domains for watermark embedding. The proposed technique is a promising solution for secure, reversible, and robust medical image watermarking.

5.4 Conclusion of the Chapter

The secure watermarking of high-resolution medical images is a challenging task, which has been addressed in this work. The proposed technique employs a combination of slantlet transformation and *RS* vector for watermark embedding in selected grids of the medical images. Notably, this research focuses on detecting, pinpointing, and restoring tampering for *ROI*, essential for watermarking medical images. Compared to existing techniques, the proposed technique improves the *PSNR* while preserving the *ROI*. It is possible to achieve strong resilience to over 20 different attacks, all while maintaining the visual fidelity of the watermarked medical image and ensuring the lossless recovery of the *ROI*. Furthermore, this research work incorporates biometric *ID*, a unique identification, to ensure the integrity of the watermark. Overall, this research offers a comprehensive solution for

secure medical image watermarking.

For future work, the algorithm's complexity could be reduced by removing *AES* and *SHA-3* if security is not needed in a particular region. Also, *ANN* could be trained to find *ROI* in all possible medical images for feature extraction while accounting for time complexity. Also, alternatives to *PSO* could be explored to achieve less execution time. There is always scope to increase capacity while maintaining good *PSNR* with new futuristic technologies and experiments.

Chapter 6

Reversible Robust Austere Viable Watermarking Medical Images using Ridgelet Transform

6.1 Introduction

Internet and its applications have been tremendously growing over the years. With the advent rise of computation power, multimedia and medical imaging applications over the Internet, security and integrity are an important concern. Multimedia has become an essential part of everyone's life directly or indirectly, approximately 4.54 billion people around the world are connected to the Internet Mulaydinov (2021). Softwares like *PACS* and *HIE* which use *DICOM* image format, are used to share medical images digitally between the hospitals and also store them over the cloud Popov and Mihanović (2022).

Digital watermarking, is commonly used for multimedia data security. It imperceptibly modifies the original data (host) which is in the form of image, audio or video by embedding covert information (watermark). While using this technique with medical images, necessary steps are taken to ensure the image follows *DICOM* standard. The hidden information can later be extracted as and when required to trace the ownership or protect privacy. Medical images are generally divided into two regions, *i.e. ROI* which is considered important and *RONI* Eswaraiah and Sudhir (2022) which is the remaining part of the image other than ROI. Thus, digital watermarking is usually required for *ROI* part of the image. Digital watermarking is generally categorized based on two strategies spatial and frequency domains. Watermark is directly inserted into the original image while working in a spatial domain by correlation between pixels just like as in difference expansion approach. This technique relatively undertakes low computational cost and is comparatively easy to implement but fragile as computer analysis can reveal the embedded information easily. In frequency / transform domain methods, watermark is embedded by changing the coefficients of original image in the frequency domain. Transformations like *DFT*, *DCT*, and *DWT* are the commonly used frequency domain techniques. Spatial domain, however, has higher capacity than the frequency domain. *DFT* is the frequency domain portrayal of finite sequenced input. It is an invertible, orthogonal, and periodic transform. The *DCT*, which is a cosine-modulated version of the *DFT*, is an asymmetric transform

that places less energy in higher frequency coefficients than the *DFT*. This property makes it well-suited for watermark embedding, as it avoids visible boundary artifacts. On the other hand, the *DFT* is commonly used for general spectral analysis and finds applications in various fields. The *DWT*, which provides a time-frequency representation of an image, captures both the frequency and temporal location information.

Candes (1998) proposed a novel method of ridgelets which is used to construct finite approximations or prediction to overcome the problem of dimensionality with neural networks and to improve efficiency and capability of neural networks. The continuous and discrete *RT* are formed to derive new approximation bounds. Ridgelets can be used for representing objects with singularities across hyperplanes. Tian (2003) proposed a reversible data embedding method to attain high embedding capacity and low distortion. This method proposes the *DE* technique to explore the redundancy of digital content by reversibly embedding a payload into digital images. With the increase in DE, difference values also increase for high capacity and low distortion. Donoho and Flesia (2003) studied the effect of *RT* for digital data using true ridge functions. The Fast Slant Stack (FSS) method is combined with the Fast 2-D Wavelet Transform (WT) to construct discrete objects that exhibit inter-relationships that are analogous to those in the continuum ridgelet theory. Lin and Otoya (2023) introduces an innovative approach to pose-invariant face recognition, departing from the conventional holistic perspective. Instead of relying on deep convolutional neural networks (DCNNs), this method employs ensemble learning and local feature descriptors to build a face recognition system. Each person's recognition ensemble consists of base learners, each trained on specific facial landmarks. Three classification models are utilized as base learners. The methodology introduces a novel face pose descriptor called the Face Angle Vector (FAV), used by a head pose classification model. The system selects facial landmarks based on this pose information for local feature descriptor extraction. This approach holds promise for a wide range of real-world applications requiring robust face recognition in varying conditions. Wang et al. (2020) proposes a temporal-spatio graph-based technique for bearing fault detection and diagnosis, leveraging the correlation information in the spatial and temporal dynamics of frequencies. The method extracts short-time periodograms and constructs a temporal-spatio graph to map the spectrum and identify principal frequencies related to the bearing's health condition. Fault detection is performed by monitoring changes in the principal frequency, while fault type identification is achieved using a K-nearest neighbor classifier with a specific graph distance metric.

The proposed technique utilizes the *RT* instead of *DWT* due to the limitations of DWT in representing straight lines and edges in images. *RT* proves to be more effective in handling singularities and representing line and curve singularities in 2-D. The technique benefits from the *SSIM* increment achieved through *RT*, which offers advantages over straightforward discretizations of the

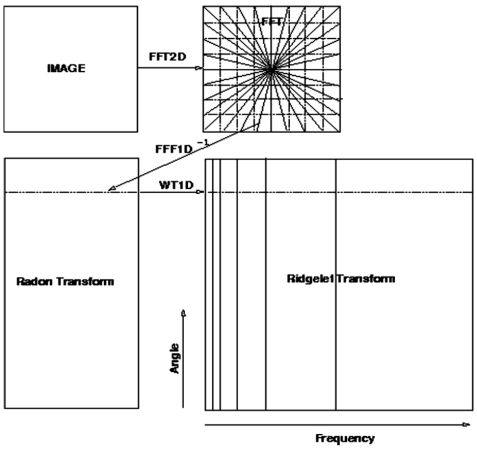


Figure 6.1: Discrete ridgelet transform flowchart. Radial lines present in the Fourier domain are processed separately. Along with radial lines, 1-D inverse FFT is calculated first and then 1-D wavelet transform later.

Fourier plane. The use of pseudopolar *FFT* allows for one-dimensional *FFT*s and significantly reduces processing time. Experimental results demonstrate the superiority of the proposed technique compared to various other methods such as *IWT, SVD, DWT*, lifting wavelet transform (LWT), *SLT, IWT-SVD, LWT-SVD, DWT-SVD,* differential expansion, Bit plane, Spread spectrum, etc. Figure 6.1 shows the discrete ridgelet transform flowchart. The radial lines present in the Fourier domain are processed separately. Along with radial lines, 1-D inverse *FFT* is calculated first and then 1-D wavelet transform later. Whereas, Figure 6.2 shows the flowchart representation of computation of finite *RT*.

The proposed technique exhibits resistance against more than 16 attacks and shows improvements in capacity, *BPP, PSNR, SSIM, NC*, and a reduction in Standard Deviation Error (SD Error) and processing time. Key properties of the proposed algorithm include its reversibility, fast processing time (O(N log(N))), increased invisibility and capacity due to RT, complexity reduction through sparse representation, robustness against wrap-around artifacts, enhanced security through multiple watermark embedding approaches, utilization of *AES-256* and *SHA-3* for cryptographic attacks security, inclusion of patient biometric *ID* and personal information for unique identification security, protection of *ROI*, tamper detection and recovery capabilities, and improved imperceptibility achieved during the *RT* process.

In summary, the proposed watermarking technique utilizes *RT* to overcome the limitations of DWT and achieves improvements in various parameters, resulting in enhanced security, capacity, imperceptibility, and resistance against attacks.

The chapter is structured as follows: Section 6.2 presents the preliminaries used in the proposed technique. In Section 6.3, we describe the proposed medical image authentication technique. Section 6.4 illustrates the experimental results, while in Section 6.5, we summarize the conclusion of our work.

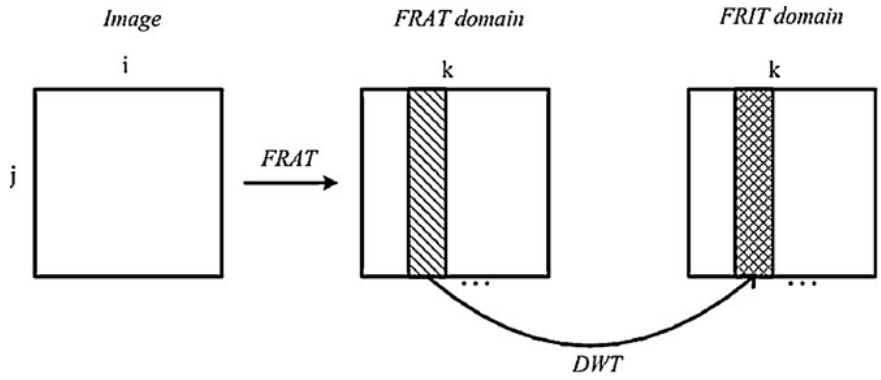


Figure 6.2: Computation of Finite Ridgelet Transform

6.2 Ridgelet Transform

Candes (1998) in his thesis proposed a new tool known as 'Ridgelet' to represent and analyze the multivariate functions. According to Candes, ridgelet is the best approximation method to represent an object which has a discontinuity across a line. RT is better than other transformation techniques like Fourier transform FT and WT. While WT represents objects along isolated points, ridgelets is used to represent objects with singularities across hyper-surface that are smooth along lines. Thus addition of 1D Wavelet along lines is RT. RT are highly directional sensitive and anisotropic.

In 2D, WT is incapable of finding smoothness along the edges. At every step of decomposition, The 2D WT produces large wavelet coefficients making it difficult to perform denoising of noisy images. Thus in 2D, Radon transform is used to combine points (WT) and lines (RT).

Ordinary RT is obtained as :

1. 2D FFT is calculated from the image.
2. FT on a square lattice can be replaced by sampled values on a polar lattice.
3. A one-dimensional inverse FFT is performed on each angular line.
4. Ridgelet coefficient is obtained by performing 1D scalar WT on the resulting angular lines.
5. The Radon transform is utilized to map a linear singularity in the 2D domain into a point.
6. Radon projection's output (each row of radon transformed image) is passed through the wavelet transform.
7. Field Programmable Gate Array (FPGA)/ Very Large Scale Integration (VLSI) implementations of the RT are needed for real-time applications.
8. In place lifting DWT is performed in the second output buffer containing the FRAT vectors.

In essence, the *RT* is the result of applying the 1D *WT* to fragments of the Radon transform. More specifically, the Finite Radon Transform (FRAT) of a real function *f*, which is defined on a finite grid $Z^2 prime$ where $Zpm = 0, 1, ..., pm - 1$ and Pm is a prime number, can be obtained.

$$r_k[l] = FRAT(k,l) = \frac{1}{\sqrt{Pm}} \sum_{(l,Pm \epsilon L_{k,l})} f[x,y], \quad k \epsilon Z^*_{Pm}, \quad l \epsilon Z_{Pm} \tag{6.1}$$

where $Z^*_{Pm} = (0, 1, ...Pm - 1, Pm)$. $L_{k,l}$, the lattice line is comprised of a group of points on the lattice that together form a line. Z^2_{Pm} , specifically

$$\begin{cases} L_{k,l} = \{(x,y) : y = kx + l \pmod{Pm},\ x \in Z_{Pm}\}, \quad 0 \leq k < Pm \\ L_{Pm,l} = \{(l,y) : y \in Z_{Pm}\} \end{cases} \tag{6.2}$$

The previously mentioned *FRAT* method utilizes a set of (Pm + 1) normal vectors, denoted by uk, where [uk = (-k, 1), k = 0, 1,..., Pm-1] union [up = (0, 1)], with k representing the line direction and l representing its intercept. An important feature of *FRAT* is its invertibility through the use of finite back-projection (FBP), which enables a representation of a generic image. The *FBP* operator is defined as the summation of radon coefficients of all lines passing through a given point, described as follows:

$$FBP_r(x,y) = \frac{1}{Pm} \sum_{(k,l \epsilon Px_{xy})} r_k[l], \quad (x,y)\ \epsilon\ Z^2_{Px} \tag{6.3}$$

where Px_{xy} denotes the set of indices of all the lines that go through a point $(x,y)\ \epsilon\ Z^2_{Pm}$. More specially, using (2) we can write:

$$Px(xy) = [(k,l) :\ l\ =\ y\ -\ kx\ (modp),\ k \epsilon\ Z_p] \cup [(p,x)] \tag{6.4}$$

substituting Eq. 6.1 into Eq. 6.3, we obtain

$$FBP_r(x,y) = \begin{cases} \frac{1}{Pm} \sum_{(k,l \in Px_{xy})} \sum_{(x',y' \in L_{k,l})} f[x',y'] \\ \frac{1}{Pm} \left(\sum_{(x',y' \in Z^2_{Px})} (f[x',y'] + Pm \cdot f[x,y]) \right) = f[x,y] \end{cases} \tag{6.5}$$

RT is mainly used in image denoising, analysis, watermarking, enhancement, authentication, texture classification and fusion, *etc.* *RT* provides one of the best representation for smooth objects and objects with edges.

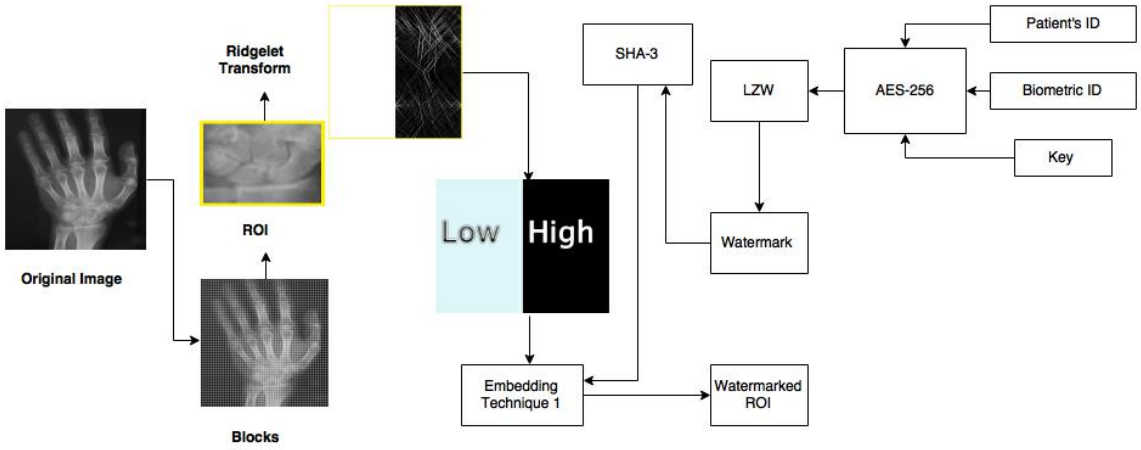


Figure 6.3: Proposed technique block diagram Representation

6.3 Proposed Reversible Medical Watermarking Algorithm

This section covers various topics including the creation of a watermark algorithm, embedding algorithm, extraction algorithm, and how to handle overflow and underflow during the process.

6.3.1 Watermark Creation Algorithm

The first step of the watermark creation process involves applying *AES* encryption to the concatenated biometric *ID*, key, and patient *ID*. The second step then involves compressing the resulting watermark bits using *LZW* compression. Finally, the third step is simply obtaining the watermark (W) from the output of the second step.

6.3.2 Unique Identity Document-Austere Viable Watermarking (UID-AVW)

The algorithm for embedding watermarks in the *ROI* part of an image is illustrated in Figure 6.3. For each 4×4 block of the W in 8-bit medical images, a recovery data set of 128 bits is created by collecting the bits of pixels inside the watermark block. The two *LSB*s of each pixel in the mapped *ROI* block are used to embed this recovery data. Similarly, in 12-bit and 16-bit medical images, the recovery data sets have sizes of 192 and 256 bits, respectively. For each *ROI* block in 12-bit and 16-bit medical images, the three and four *LSBs* of pixels in the mapped *ROI* block are used to embed the recovery data, respectively. Finally, the information of the watermark and the hash value of the watermark are embedded into the *LSBs* of the border pixels of the *ROI*. Here, the information refers to the number of vertices and the coordinates of vertices of an enclosing rectangle, and the border is defined as the outer three lines of pixels in the image. The detailed algorithm for embedding is as follows.

Step 1. **Selection of ROI:** The original image is partitioned into two parts, namely, *ROI* and *RONI*, by using connected-component analysis Shih (2017).

Step 2. **Channel Division:** *ROI* is divided into its three basic components Red Green Blue (RGB).

Step 3. **Apply Ridglet:** Low(L) and High(H) bands are obtained after applying *RT* on the red component of *ROI*.

Step 4. **Apply SHA-256:** $H_{\triangle}$ is calculated by applying *SHA-256* on the W part.

Step 5. **Blocks of ROI:** The L-band of *ROI* is then partitioned into non-overlapping 8×8 chunks.

Step 6. **Blocks of Watermark:** W is partitioned into non-overlapping 4×4 chunks.

Step 7. **Calculating the threshold value:** The calculation of the threshold T for the entire image is performed using *PSO* Kennedy and Eberhart (1995), which involves using Eqs. (3.3) and (3.4).

Step 8. **Mapping:** The mapping of each block in the W to a block in the L band of *ROI* is performed using Eqs. 3.13 and 3.9, assuming that the number of blocks in W is smaller than the number of blocks in *ROI*.

$$Æ_{ROI} = [((\alpha * Æ_W) mod B_N) + 1]/T \tag{6.6}$$

where $Æ_{ROI}$ is a block number in *ROI*, α is a secret key and is a prime number between 1 and B_N, $Æ_W$ is block number in W, B_N is the number of blocks in W and T is the threshold value.

Step 9. **Side Information:** Fetch bits of 16 pixels inside each W block as recovery data.

Step 10. **Recovery data:** The recovery data of each block in W is embedded into 2, 3, or 4 *LSBs* of the pixels in the corresponding mapped *ROI* block, depending on the bit depth.

Step 11. **Encrypt:** The collection of bits that indicate the hash value ($H_{\triangle}$) and information of W should be encrypted using a secret key $\alpha 1$.

Step 12. **Border pixels:** The next step is to embed the encrypted bits into the *LSBs* of border pixels of the *ROI*.

Step 13. **Inverse Ridgelet:** Apply inverse *RT* on the output of step 11.

Step 14. **Watermarked ROI:** Repeat steps 3-13 for green and blue components of *ROI* to get watermarked *ROI*.

6.3.3 Region Of Interest-AVW and Tamper Detection/Recovery-AVW

Watermark embedding algorithm *i.e.* Region Of Interest - Austere Viable Watermarking (ROI-AVW) and Tamper Detection/Recovery - Austere Viable Watermarking (TDR-AVW) for RONI part of the image is as shown in Figure 6.4 is explained as follows:

Step 1. **Channel Division** *RONI* is divided into its three basic components *RGB*.

Step 2. **Apply Ridglet:** Low(L) and High(H) bands are acquired after applying *RT* on the red component of *RONI*.

Step 3. **Blocks of RONI:** L band of *ROI* part of the image is divided into non-overlapping chunks of 4×4.

Step 4. **Threshold values:** Threshold *Th*, for every single block and T for the overall image is calculated by *PSO* through Eqs. (3.3) and (3.4).

Step 5. **Block and coefficient selection:** . High energy coefficients of low frequency band (L) are used for the watermark embedding process.

Step 6. **ROI-AVW:** The watermark bits (W) are embedded in the first quarter of the L band for each block, by modifying the differences between the mean values of the ridgelet coefficients in the selected low frequency band. The highest coefficients of each block, before and after applying the *RT*, are denoted by ϑ and $\vartheta^{'}$, respectively. The mean and standard deviation of the block are represented by μ and δ, respectively. The ratio of the μ and δ between ϑ and $\vartheta^{'}$ is denoted by R. The two pseudo-random number sequences which are used to implant watermark bits in ϑ and $\vartheta^{'}$ using Eq. 6.7 are η and $\eta^{'}$.

$$\vartheta_W = \begin{cases} \vartheta^{'} + (Th \times ((\sqrt{N} R \eta_1))/T), & if \;\; W = 0 \\ \vartheta^{'} + (Th \times ((\sqrt{N} V \eta_2))/T), & if \;\; W = 1 \end{cases} \tag{6.7}$$

where ϑ_W is the modified highest coefficient of each block, W stands for the watermark bits and the watermark is of size $N \times N$, ($N = 2^c$; $c = 1, 2,..$), V= (1-R), T and Th are the threshold values from step 4. The coefficients R and V contribute in the improvement of the visual quality of the watermarked image.

Step 7. **TDR-AVW:** W bits are embedded in the fourth quarter of L band for each block. Implantation f the watermark bits in ϑ and $\vartheta^{'}$ are accomplished by the this Eq. (6.8).

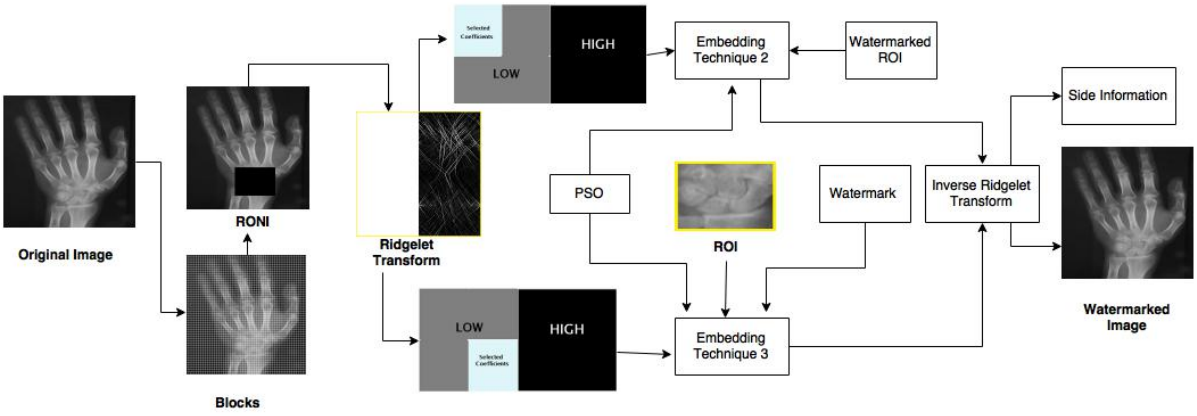


Figure 6.4: Proposed watermarking scheme Block diagram representation

$$\vartheta_W = \begin{cases} \vartheta^{'} - (T \times ((\sqrt{N} R \eta_1))/Th), & if \quad W = 0 \\ \vartheta^{'} - (T \times ((\sqrt{N} V \eta_2))/Th), & if \quad W = 1 \end{cases} \tag{6.8}$$

where ϑ_W is the modified highest coefficient of each block, W stands for the watermark bits and the watermark is of size $N \times N$, ($N = 2^c$; $c = 1, 2,..$), V= (1-R), T and Th are the threshold values from step 4. The coefficients R and V contribute in the improvement of the visual quality of the watermarked image.

Step 8. **Applying Inverse Ridgelet:**The watermark embedding process continues until all the watermark bits are embedded. The modified subbands replace the original subbands, and then the inverse RT is applied. To ensure reversibility, the resulting output is rounded up to integer values, allowing for exact reconstruction of the original image and the watermarked image at the receiver end. Furthermore, to increase the watermarking capacity up to three times, the above steps are repeated in the same manner for embedding in both the G and B channels.

Step 9. **Handling the Underflow & Overflow:** When pixel values are affected by overflow or underflow, the watermarking process is adjusted to account for this and the relevant information is saved as side information. The pixel values are then adjusted accordingly with Eq. (3.2.4).

6.3.4 Watermark Extraction Algorithm for UID-AVW

The steps described are for the extraction of watermark from a watermarked medical image. During the extraction phase, the watermarked image is divided into two parts: *ROI* and *RONI*. Here is a brief description of each step:

Step 1. The encrypted bits are extracted from the *LSB*s of the border pixels.

Step 2. The extracted bits are decrypted to obtain the watermark information W and the hash value $H_{\triangle}$ of the watermark.

Step 3. Using the information of W, the pixels belonging to W and ROI are identified in the received medical image.

Step 4. The hash value of W ($H^1_{\triangle}$) is calculated using the SHA-3 technique.

Step 5. $H_{\triangle}$ is compared with $H^1_{\triangle}$.

Step 6. If $H_{\triangle} = H^1_{\triangle}$, the extraction procedure stops; otherwise, it proceeds to the next step.

Step 7. W and ROI are divided into blocks of sizes 4×4 and 8×8, respectively.

Step 8. For each block B inside W, the following steps are repeated to identify tampered W blocks

Step 9. The average (a1) and variance (v1) values of block B are calculated.

Step 10. The bits of pixels of W block B are extracted from the 2^{nd}, 3^{rd}, or 4^{th} LSBs of pixels in the mapped ROI block, depending on the bit depth.

Step 11. The average (a2) and variance (v2) of the extracted pixel values are calculated.

Step 12. The W block B is marked as tampered if $a1 \neq a2$ or $v1 \neq v2$.

Step 13. Each tampered W block is replaced with the bits of pixels extracted from the corresponding mapped ROI block to obtain the original W block.

6.3.5 Watermark Extraction Algorithm for ROI-AVW and TDR-AVW

RONI part of the image is considered for extraction with *ROI-AVW* and *TDR-AVW*.

Step 1. **Dividing the RONI:** Upon receiving the watermarked image, the receiver begins by reading the image and the accompanying side information. The pixels that were previously adjusted during the embedding process are then moved back to their original locations to reconstruct the image. Next, the watermarked image is divided into non-overlapping blocks.

Step 2. **Applying Ridgelet:** The watermarked $RONI$ is subjected to RT, and the resultant image is divided into non-overlapping blocks of size 4×4.

Step 3. **Extraction ROI-AVW:** The inverse ridgelet coefficient $\vartheta^{'''}$ is calculated, and correlation coefficients are computed between $\vartheta^{'''}$ and $\eta^{''}_1$, as well as between $\vartheta^{'''}$ and $\eta^{''}_2$ for each block in the first quarter of the L-band of the watermarked image. The correlation coefficients are compared using a predefined threshold value 'Th', i.e., x($\vartheta^{'''}$,$\eta^{''}_1$), x($\vartheta^{'''}$,$\eta^{''}_2$) and x($\eta^{''}_1$,$\eta^{''}_2$), and

the recovered watermark is then constructed using the side information and Eqs. (6.10) and (6.10).

$$Th = \sqrt{N} \times Weg \times (R \times V) \tag{6.9}$$

$$W_{tech2}^{''} = \begin{cases} 1, & if \quad x(\vartheta^{'''}, \eta_1^{''}) < x(\vartheta^{'''}, \eta_2^{''}) \\ 0, & otherwise \end{cases} \tag{6.10}$$

The recovered watermark is denoted as $W_{tech2}^{''}$ and the corresponding correlation coefficient value is denoted by x. The weighted value of R is denoted by Weg.

Step 4. **Extraction TDR-AVW:** The watermark recovery process involves calculating the correlation coefficients between the inverse ridgelet coefficient $\vartheta^{'''}$, $\eta_1^{''}$ and $\eta_2^{''}$ for each block of the fourth quarter of the L band of the watermarked image. The watermark is then recovered by comparing these correlation coefficients using a threshold value denoted by 'Th' as shown in Eqs. (6.9) and (6.11) with the help of the side information.

$$W_{tech3}^{''} = \begin{cases} 1, & if \quad x(\vartheta^{'''}, \eta_1^{''}) > x(\vartheta^{'''}, \eta_2^{''}) \\ 0, & otherwise \end{cases} \tag{6.11}$$

where $W_{tech3}^{''}$ is the recovered watermark.

Step 5. **Applying Inverse Ridgelet:** The inverse RT is applied to the $RONI$ portion of the watermarked image, which remains after the watermark extraction process.

Step 6. **Recovery of the Original Image:** After the watermark extraction, the difference value stored in the side information is used to recover the original mean value of each block by applying the inverse process that was used during watermark embedding. Then, each block that contains the correlation coefficient value, extracted watermark value, and the original mean value can be recovered by shifting back the mean and standard deviation values. Finally, the original image is generated by rearranging blocks of the image and concatenating recovered ROI and $RONI$ parts.

6.4 Experimental Results

The proposed approach is tested on several standard images, including Lena, Baboon, Barbara, and Gold hill, each with a size of 512×512. Additionally, 300 medical images were used for average

(a)

PATIENT ID: DANILKRVII6114
ADDRESS: 37 DEFENCE COLONY ROOP NAGAR INDIA
HOSPITAL ID: 1312SUJATA2412SUM
HOSPITAL NAME: CH. SUBE SINGH HOSPITAL
DOCTOR ID: 3219SAHIL0401
DISEASE: MRI SCAN FOR TUMOUR SIGNS

(b)

Figure 6.5: Watermarks used for the proposed algorithm. (a) Biometric Watermark, (b) Text Watermark.

results. The algorithm's performance was evaluated by testing it on various images, as illustrated in Figure (6.6). The authors also compared their proposed technique with other published results using conventional images such as Lena, Goldhill, Barbara, Lake, Plane, and Baboon. In the experiments, a watermark image containing patient information and biometric *ID* was used, as shown in Figure (6.5).

6.4.1 Imperceptibility

Watermarking imperceptibility is evaluated with the following factors:

1. *PSNR*, which is given by Eq. 1.1.
2. The capacity of the proposed watermarking scheme is determined by image size whereas the size of hidden bits can be calculated using Eq. 1.4.
3. *SSIM* is computed for various windows of an image. The measure between two windows p and q of the same size $N \times N$ is given by eq. 1.5.
4. *BPP* is calculated by Eq. 1.6.

Table 6.1 and Table 6.2 shows the values for *PSNR* (dB), capacity, *SSIM*, *BPP* by, Time and *SD* Error for the images from Figures 6.6 and 6.5. Table 6.1 shows three different embedding techniques are proposed for medical images: *UID-AVW, ROI-AVW,* and *TDR-AVW*. For each technique, the capacity, *BPP*, *PSNR*, and *SSIM* are reported for various medical images including Hand, Knee,

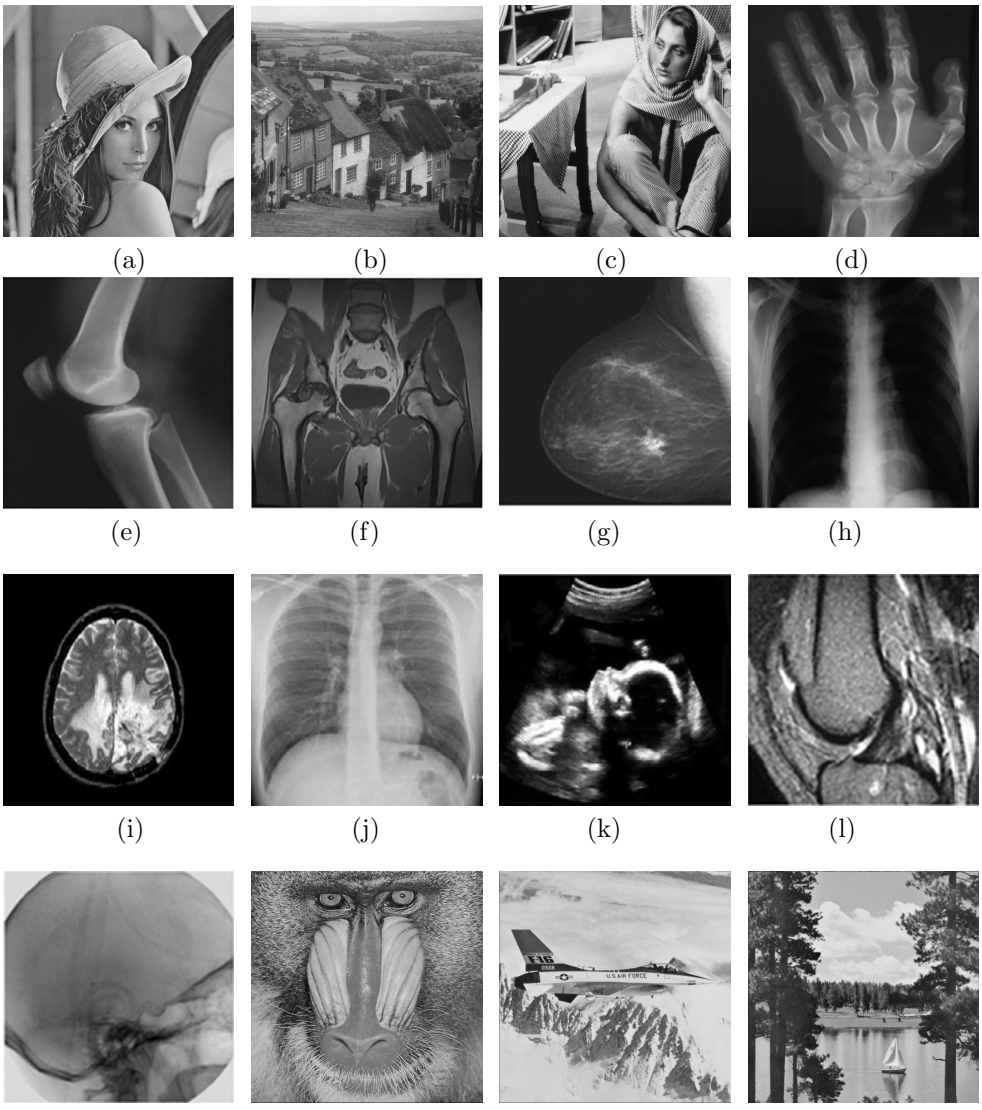


Figure 6.6: Host (commonly referred & medical) images for embedding. (a) Lena, (b) Goldhill, (c) Barbara, (d) Hand, (e) Knee, (f) Belly, (g) Breast, (h) X-ray Posteroanterior (PA) chest view, (i) MRI, (j) X-Ray normal view,(k) Ultrasound (US), (l) ACL-side-views,(m) Angiography Mask, (n) Baboon, (o) Plane, (p) Lake

Belly, Breast, Xray (PA), *MRI*, X-Ray, *US*, *ACL*, and Mask. *UID-AVW* refers to the embedding technique that uses unique image identifiers to embed the data. *ROI-AVW* refers to the embedding technique that uses region of interest (ROI) information to embed the data. *TDR-AVW* refers to the embedding technique that uses texture and data redundancy to embed the data. From the table 6.1, it can be seen that for most of the images, the *TDR-AVW* technique provides the highest capacity, but at the cost of lower PSNR and SSIM values compared to the other two techniques. The *UID-AVW* technique provides the lowest capacity but the highest *PSNR* and *SSIM* values. The *ROI-AVW* technique provides a good balance between capacity and image quality. The BPP value decreases as the capacity increases, which is expected as more data is embedded in the image.

In table 6.2 the results for *Bpp* variation from 0.1 to 0.7, capacity (bits) for all the images. As the *Bpp* increases, the capacity of the watermark increases as well, but the standard deviation error also increases. For Lena and Barbara images, as the *Bpp* increases, the time required to embed the watermark also increases. However, for Goldhill, Hand, and Knee images, the time required to embed the watermark initially increases and then decreases. Lena and Barbara images have lower capacity and require more time for watermark embedding compared to the other images. Hand and Knee images have the highest capacity and lower standard deviation error, making them good candidates for watermarking. Goldhill and Barbara images have relatively higher standard deviation error compared to the other images.

Thus proving the effectiveness of the watermarking scheme and the masking procedure. It is evident that the watermark is hidden by all three techniques, *i.e. UID-AVW, ROI-AVW* and *TDR-AVW.*

6.4.2 Authenticity and Integrity

Authenticity and integrity of the watermark are determined by the following experimental results of the proposed watermarking technique:

1. **Mole addition:** During the transmission process, the watermarked medical mole is added to the watermarked image. Thus making the block (covering added mole) noisy.

2. **Histogram equalization:** The mapping of the embedding technique is altered by equalizing the histogram of the image.

3. **Border cropping:** The block borders are cropped which jams the communication between the watermark and the feature map which produces a noisy difference map.

4. **Wrong key insertion:** Upon usage of incorrect key, each decrypted watermark blocks would be faulty. Thus, resulting in incorrect recovery of watermark and noisy.

Table 6.1: PSNR (dB), Maximum Capacity(bits), BPP and SSIM for all three proposed embedding techniques for medical images.

Image	Embedding Type	Capacity	BPP	PSNR	SSIM
Hand	UID-AVW	140,715	0.5368	57.6388	0.9883
	ROI-AVW	784,820	2.9938	55.1787	0.9719
	TDR-AVW	1,178,796	4.4967	53.9845	0.9658
Knee	UID-AVW	140,505	0.5359	56.3033	0.9927
	ROI-AVW	572,336	2.1832	52.3835	0.9754
	TDR-AVW	1,107,454	4.2246	51.6596	0.9629
Belly	UID-AVW	140,723	0.5368	59.5075	0.9892
	ROI-AVW	858,446	3.2747	55.0609	0.9725
	TDR-AVW	1,215,488	4.6367	53.9089	0.9596
Breast	UID-AVW	140,615	0.5364	59.5928	0.9915
	ROI-AVW	846611	3.2295	55.6256	0.9711
	TDR-AVW	1,225,400	4.6745	53.8440	0.9690
Xray (PA)	UID-AVW	140,683	0.5366	56.7056	0.9875
	ROI-AVW	710,154	2.7090	53.2007	0.9707
	TDR-AVW	1,184,222	4.5174	51.7783	0.9599
MRI	UID-AVW	140,794	0.5370	66.9933	0.9998
	ROI-AVW	812,636	3.1000	63.7931	0.9754
	TDR-AVW	1,183,129	4.5132	60.7852	0.9618
X-Ray	UID-AVW	140,758	0.5369	57.1008	0.9997
	ROI-AVW	792,712	3.0239	54.6318	0.9766
	TDR-AVW	1,182,358	4.5103	52.4635	0.9610
US	UID-AVW	140,764	0.5369	63.1380	0.9996
	ROI-AVW	834,238	3.1823	60.7208	0.9776
	TDR-AVW	1,203,544	4.5912	58.5301	0.9657
ACL	UID-AVW	140,760	0.5369	57.3225	0.9969
	ROI-AVW	779,420	2.9732	55.9594	0.9789
	TDR-AVW	1,143,702	4.3629	54.2256	0.9587
Mask	UID-AVW	140,776	0.5370	59.3062	0.9975
	ROI-AVW	699,620	2.6688	58.9811	0.9879
	TDR-AVW	1,150,592	4.3892	56.3298	0.9645

Table 6.2: Results for Bpp variation from 0.1 to 0.7, Capacity (bits), Standard Deviation Error and Time (Seconds) for some conventional watermarking images and medical images.

Image	Payload	0.1	0.2	0.3	0.4	0.5	0.6	0.7
Lena	Bpp	0.1400	0.2097	0.3183	0.4200	0.5049	0.6065	0.7019
	SD Error	0.2810	0.2873	0.2876	0.2888	0.2916	0.2955	0.2989
	Time	24.961	27.868	31.119	38.572	44.740	50.373	56.952
	Capacity	36,706	54,980	83,466	110,112	132,380	159,003	183,999
Goldhill	Bpp	0.1709	0.2010	0.3419	0.4003	0.5767	0.6065	0.7190
	SD Error	0.2882	0.2900	0.2914	0.2922	0.2937	0.2949	0.29672
	Time	18.775	20.674	27.226	32.226	40.089	45.006	53.666
	Capacity	44,809	52,709	89,636	104,941	151199	159,000	188493
Barbara	Bpp	0.1068	0.2137	0.3204	0.4657	0.5342	0.6412	0.7050
	SD Error	0.2243	0.2238	0.2399	0.2459	0.2464	0.2501	0.2662
	Time	20.431	22.332	30.901	36.151	42.714	49.844	54.150
	Capacity	27,998	56,028	83,994	122,087	140,035	168,097	184,824
Hand	Bpp	0.1246	0.2493	0.3738	0.4774	0.5440	0.6236	0.7482
	SD Error	0.1801	0.1888	0.2231	0.2242	0.2283	0.2379	0.2515
	Time	20.239	24.894	30.552	35.810	42.354	50.784	57.106
	Capacity	32,656	65,342	97,978	125,152	140,715	163,466	196,141
Knee	Bpp	0.1817	0.2714	0.3636	0.4017	0.5450	0.6254	0.7780
	SD Error	0.2584	0.2639	0.2676	0.2896	0.2898	0.2902	0.2977
	Time	20.495	24.951	30.487	37.762	43.119	50.733	56.539
	Capacity	47,620	71,158	95,317	105,307	142,858	163,965	203,965
Belly	Bpp	0.1590	0.2557	0.3186	0.4028	0.5095	0.6067	0.7017
	SD Error	0.1916	0.2133	0.2240	0.2268	0.2294	0.2361	0.2424
	Time	18.723	21.694	30.687	35.810	40.629	46.772	52.008
	Capacity	41,694	67,020	83,506	105,602	133,565	159,065	183,965
Breast	Bpp	0.1386	0.2048	0.3397	0.4022	0.5166	0.6246	0.7085
	SD Error	0.1398	0.1402	0.1621	0.1764	0.1868	0.2072	0.2272
	Time	25.332	29.364	34.095	40.651	46.995	50.102	56.064
	Capacity	36,351	53,704	89,052	105,455	135,445	163,753	185,753
X-ray (PA)	Bpp	0.1011	0.2157	0.3023	0.4146	0.5023	0.6047	0.7000
	SD Error	0.2091	0.2114	0.2375	0.2401	0.2541	0.2375	0.2394
	Time	21.112	22.788	28.894	34.093	40.541	45.528	52.852
	Capacity	26,520	52,842	79259	108,693	131,683	158,524	183,524

5. **Un-watermarked:** If watermark is not embedded, then the watermark extraction process will generate a meaningless watermark at the receiving side which would be random noisy unexpected image.

6. **Scaling:** The process of scaling alters both embedded watermark and recovered cover image. Thus, the decrypted watermark is different than expected.

Besides scaling and cropping, this scheme can also detect geometrical transformations which result in changes to the image size without even knowing the original image size.

Table 6.3: PSNR (dB) values after various attacks on Images

ATTACKS	Lena	Goldhill	Barbra	Baboon	Plane	Lake	Hand	Knee	Belly	Breast	PA	MRI	Xray	US	ACL	Mask
Speckle	44.2207	44.6772	44.1135	43.6768	41.5165	44.3966	48.8906	48.4026	47.8234	48.987	48.0123	49.8574	41.1782	50.0196	45.6984	41.6187
Salt and Pepper	44.4016	43.2882	45.6402	43.8811	43.6297	43.5516	45.9273	43.8531	44.9884	45.7777	44.1244	44.0153	42.367	43.0803	45.1079	41.8954
Gaussian	39.5696	39.5497	39.7226	39.4211	39.3052	39.7637	39.8322	39.7372	39.7304	39.8853	39.7524	41.5331	38.5416	40.8514	39.7901	38.5478
Poission	37.165	27.6781	27.2013	26.977	25.5617	27.1743	30.0701	30.2719	29.59	29.9122	30.3294	32.0323	36.2799	32.4438	30.8342	29.8613
Median Filter	50.3726	50.1351	52.9759	48.8967	47.7168	53.2967	55.2677	52.6414	52.7814	58.014	53.3152	64.2038	44.2191	58.5917	54.2001	44.1797
Rotate	35.0469	29.7482	28.7486	27.919	28.1213	31.6869	35.8399	36.8068	32.7373	36.1814	26.9484	34.0201	27.9432	29.8645	26.3477	35.3152
Croppped	40.3726	39.5497	36.8612	36.9047	31.8706	37.9317	39.814	39.7372	39.7304	39.8853	39.7524	41.5331	38.5416	40.8514	39.7901	38.5478
JPEG Compression	37.1999	35.0915	33.4048	30.4246	37.7521	34.0878	46.8239	47.4666	44.2719	46.9014	47.2634	45.3294	45.1191	45.5493	44.688	45.4218
Low Pass Gaussian Filter	41.9689	39.632	31.0418	39.7929	40.8308	38.2912	55.0888	49.8011	47.3055	55.2778	52.9839	53.6955	47.602	53.1707	53.1089	47.7222
Resize	39.5702	39.5497	39.7226	39.4211	39.3052	39.7637	39.814	39.7372	39.7304	39.8853	39.7524	41.5331	38.5416	40.8514	39.7901	38.5478
Average	50.3726	50.1351	52.9759	48.8967	47.7168	53.2967	55.2677	52.6414	52.7814	58.014	53.3152	64.2038	44.2191	58.5917	54.2001	44.1797
Weiner	37.5216	34.0902	29.6935	27.3844	37.8935	33.8898	51.2046	49.3024	43.5306	48.7942	49.6084	48.6432	48.3921	48.5545	46.6614	48.3652
Histogram Equalization	30.3856	27.7566	33.4776	27.8264	31.7513	24.2684	30.967	30.3329	31.0148	30.8927	30.7916	25.7962	35.5773	28.0295	28.2176	27.2808
Blurr	33.9877	28.0355	30.8499	31.2106	27.3622	25.9862	41.3908	34.8797	31.1039	39.2076	38.8037	35.5439	43.7848	35.8092	36.6232	42.5539
Motion Blurr	39.1466	33.2698	33.3352	37.9365	35.3411	32.8929	50.2806	42.9443	40.0608	52.8329	52.3061	46.8271	48.9189	50.2935	47.9915	48.8103
Sharpen	33.0821	30.6523	32.0328	32.77	30.981	39.3267	37.5371	30.9874	28.332	36.395	34.6282	34.4885	30.7166	34.1524	34.746	30.396

Table 6.4: NC values after various attacks on Images

ATTACKS	Lena	Goldhill	Barbra	Baboon	Plane	Lake	Hand	Knee	Belly	Breast	PA	MRI	Xray	US	ACL	Mask
Speckle	0.9996	0.9997	0.9998	0.9995	0.9992	0.9997	0.9998	0.9998	0.9997	0.9999	0.9999	0.9999	0.9992	0.9999	0.9997	0.9994
Salt and Pepper	0.9996	0.9995	0.9999	0.9995	0.9996	0.9997	0.9996	0.9993	0.9993	0.9997	0.9997	0.9997	0.9996	0.9996	0.9997	0.9995
Gaussian	0.9986	0.9986	0.9994	0.9982	0.9984	0.9992	0.9984	0.9981	0.9973	0.9987	0.999	0.9995	0.9979	0.9994	0.9988	0.9982
Poission	0.9739	0.978	0.9883	0.9658	0.9588	0.9851	0.9846	0.9832	0.9714	0.9866	0.9911	0.9955	0.99555	0.9954	0.9808	0.9658
Median Filter	0.9999	0.9999	1	0.9998	0.9997	1	1	0.9999	0.9999	1	1	1	0.9992	1	1	0.9993
Rotate	0.9558	0.97432	0.915	0.9695	0.97238	0.97457	0.9958	0.9861	0.9489	0.9678	0.94801	0.9971	0.9678	0.9916	0.9724	0.97477
Croppped	0.9958	0.92	0.9901	0.9781	0.96341	0.9772	0.9973	0.9869	0.9746	0.9971	0.9967	0.9976	0.9832	0.9971	0.9966	0.9844
JPEG Compression	0.9973	0.9958	0.9971	0.9836	0.9973	0.9969	0.9997	0.9997	0.999	0.9997	0.9998	0.9998	0.9994	0.9998	0.9996	0.9995
Low Pass Gaussian Filter	0.9991	0.9986	0.9953	0.9893	0.9987	0.9988	1	0.9998	0.9996	1	1	1	0.9996	1	0.9999	0.9997
Resize	0.9954	0.996	0.9945	0.9965	0.9927	0.9933	0.9991	0.9972	0.9968	0.9941	0.9928	0.9986	0.9932	0.9917	0.9911	0.9901
Average	0.9999	0.9999	1	0.9998	0.9997	1	1	0.9999	0.9999	1	1	1	0.9992	1	1	0.9993
Weiner	0.9975	0.9948	0.9935	0.9678	0.9975	0.9968	0.9999	0.9998	0.9989	0.9998	0.9999	0.9999	0.9997	0.9999	0.9998	0.9997
Histogram Equalization	0.992	0.9662	0.9977	0.989	0.9753	0.9861	0.9461	0.9413	0.94084	0.9349	0.9245	0.9853	0.99878	0.98357	0.98	0.98658
Blurr	0.9829	0.9788	0.96473	0.98522	0.971	0.9799	0.9989	0.994	0.9807	0.9985	0.9987	0.998	0.9991	0.998	0.9978	0.999
Motion Blurr	0.9958	0.9937	0.9706	0.98709	0.9954	0.9959	0.9999	0.9991	0.9974	0.9999	0.9999	0.9999	0.9997	0.9999	0.9998	0.9998
Sharpen	0.9477	0.9602	0.9348	0.97129	0.95238	0.99337	0.9973	0.9869	0.9746	0.9971	0.9967	0.9976	0.9832	0.9971	0.9966	0.9844

It is possible due to the fact that geometrical transformations results in significant changes in the extraction mapping process and mess up the embedded watermark.

6.4.3 Robustness Evaluation

This research tests the proposed technique very harshly on many images with various attacks. The table 6.3 shows the *PSNR* values after various attacks on 16 different medical images. The 16 different types of attacks include Speckle, Salt and Pepper, Gaussian, Poission, Median Filter, Rotate, Cropped, *JPEG* Compression, Low Pass Filter Gaussian, and Resize. For each image and attack, the *PSNR* value in dB is provided. Higher *PSNR* values indicate better image quality, as it means that the image is closer to the original, undistorted image. The table shows that the *PSNR* values vary widely across different images and attacks, with some attacks causing more distortion than others. For example, the Poission attack consistently results in the lowest *PSNR* values, indicating the highest level of distortion. In contrast, the Median Filter and Low Pass Filter Gaussian attacks result in the highest PSNR values, indicating the lowest level of distortion.

The table 6.4 contains the *NC* values of various image attacks on different images.,The images used in the experiment include Lena, Goldhill, Barbra, Baboon, Plane, Lake, Hand, Knee, Belly, Breast, *PA*, *MRI*, Xray, *US*, *ACL*, and Mask. The *NC* values indicate the similarity between the original and attacked images, with a value of 1 indicating perfect similarity and 0 indicating no similarity. Overall, the table shows that the Median Filter and Low Pass Filter Gaussian attacks have the highest *NC* values across most of the images, indicating that they have the least impact on the similarity between the original and attacked images. On the other hand, the Poisson and Rotate attacks have the lowest *NC* values, indicating that they have the most impact on the similarity between the original and attacked images. The *NC* values of the other attacks fall somewhere in between, with some showing higher similarity and others showing lower similarity between the original and attacked images. The table provides valuable information for researchers and practitioners in the field of image processing and can be used to compare the effectiveness of different attacks on different images.

To evaluate the robustness, the watermarked images were subjected to various attacks and the watermarks were extracted after the attacks. The average value of *PSNR* and *NC* for 300 medical images against various types of unintentional attacks is shown in Table 6.5. Attacks such as *JPEG* compression are performed by adding *AGN* with a zero-mean value, where the quality factor is set to (20, 30,..., 100) and the variance is set to (0.001, 0.002,...., 0.01). The strength of the proposed algorithm can be demonstrated by the resistance against these attacks. Among all the attacks, the highest average PSNR of 54.7 0dB was achieved by the Median Filter, followed by Low Pass Filter Gaussian with 51.67 dB. On the other hand, the Poisson attack resulted in the lowest average *PSNR*

of 31.48 dB. In terms of average NC values, Median Filter again had the highest value of 0.99990, followed by Average with the same value. The lowest average NC was obtained from Histogram Equalization with 0.96228. Overall, Median Filter performed the best in terms of both $PSNR$ and NC values, while Poisson and Histogram Equalization performed the worst.

Table 6.5: Average PSNR and Average NC values after various attacks on 300 Images

ATTACKS	Average PSNR	Average NC
Speckle	47.34002	0.99983
Salt and Pepper	44.77480	0.99967
Gaussian	40.62898	0.99862
Poission	31.47847	0.98508
Median Filter	54.57367	0.99990
Rotate	33.09083	0.97509
Croppped	40.43318	0.99120
JPEG Compression	46.71164	0.99993
Low Pass Gaussian Filter	51.67268	0.99987
Resize	40.45932	0.99474
Average	54.70212	0.99990
Weiner	48.78966	0.99981
Histogram Equalization	30.49517	0.96228
Blurr	38.47841	0.99637
Motion Blurr	48.69653	0.99964
Sharpen	33.77685	0.99127

6.4.4 Security of the watermark

In order to ensure security of digital data, the proposed technique uses cryptographic algorithms *SHA-3* and *AES*. The proposed technique consists of four parts of the watermark which are: Key1, the blocks of the *ROI*, the biometric *ID* of the patient and the unique identification number of the patient as a text watermark. The *ROI* blocks are encrypted using *SHA-3*(512) to provide sufficient security. The encrypted components of the watermark using *AES-256* are merged with the hash values. In order to offer high complexity and resistance to various attacks namely: man-in-the-middle or chosen plain text attacks, the *AES* with 14 rounds. In addition, the proposed algorithm is capable of detecting tampering attempts with 100% accuracy. Denoising attacks can be reversed by applying thresholding with SLT, and compromised key attacks can only break a maximum of 11 rounds of *AES-256*, which is less than the 14 rounds used in this technique.

6.4.5 Reversibility Evaluation

In order to assess the proposed method's ability to be reversed, the *IER* was calculated. The *IER* measures the proportion of test images that were recovered with errors compared to the total number of test images. Results showed that the *IER* was zero, which indicates that all cover and watermark images were restored successfully without any loss of data.

6.4.6 Overall Execution Time

In order to measure the overall execution time, a *PC* or personal computer is used with Intel(R) Core(TM) i7-4510U CPU @ 2.00 GHz 2.60GHz and 8GB memory specifications. To record the program's runtime in seconds, Matlab(R2015a) is used using the tic and toc commands. The measurement of the proposed technique execution time is done at different block sizes which include the time taken to create the watermark, *SLT*, embedding with *RS* vector and watermark extraction.

6.4.7 Comparison with Existing Techniques

This section provides a brief comparison with respect to the performance of the proposed watermarking scheme with existing robust reversible medical watermarking techniques. To prove that *RT* is better than other transformations, comparison is done with the exiting transformations and techniques. Table 6.6 shows the proposed technique results are better than the existing transforms. For example: an X-Ray normal view *PSNR* with respect to proposed technique are 19.15%, 18.98%, 18.93%, 18.57%, 19.00%, 18.97%, 18.97%, and 35.88% higher than those of the *IWT, LWT, DWT, IWT-SVD, LWT-SVD, DWT-SVD, SVD,* and Kumsawat et al. techniques, respectively. Similarly, the Mean Structural Similarity Index (MSSIM) values for the proposed technique were 0.55%, 0.68%, 0.78%, 0.41%, 0.63%, 0.64%, 3.69%, and 3.07% higher than those of the aforementioned techniques, respectively. Finally, the Normal Correlation Average (NCA) values for the proposed method were 3.03%, 3.37%, 3.48%, 0.87%, 3.02%, 2.92%, 4.16%, and 1.32% higher than those of the same techniques, respectively. One can conclude that the proposed technique outperforms existing techniques for robust reversible medical watermarking.

Table 6.7 compares the proposed technique with the methods proposed by Xuan et al. (2004b) and Arsalan et al. (2017) in terms of *PSNR* and *SSIM* for different payloads (in bits per pixel or bpp) ranging from 0.1 to 0.7. The comparison is done for various images such as Lena, Goldhill, Barbara, Hand, Knee, X-ray, and Breast. The average difference between existing methods and proposed technique varies from 15% to 18% for payload 0.1 to 0.7. The results suggest that the proposed technique outperforms the other two methods in terms of both *PSNR* and *SSIM* for most of the images and payload values.

Table 6.6: Comparison of PSNR(dB), MSSIM (Mean Structural Similarity), and NCA (Normal Correlation Average) for medical images with various existing methods

Med Image	Method	PSNR	MSSIM	NCA
MRI	IWT Lei et al. (2014)	48.02	0.9912	0.9542
	LWT Lei et al. (2014)	47.91	0.9908	0.9436
	DWT Lei et al. (2014)	47.23	0.9902	0.9428
	IWT-SVD Lei et al. (2014)	48.31	0.992	0.968
	LWT-SVD Lei et al. (2014)	47.94	0.992	0.9549
	DWT-SVD Lei et al. (2014)	48.08	0.9917	0.9513
	SVD Lei et al. (2014)	47.99	0.9915	0.9499
	GA Kumsawat et al. (2005)	41.32	0.9724	-
	Proposed Method	66.7915	0.9986	0.9999
X-Ray	IWT Lei et al. (2014)	48.28	0.9936	0.9719
normal	LWT Lei et al. (2014)	47.96	0.992	0.9652
view	DWT Lei et al. (2014)	47.88	0.9912	0.9662
	IWT-SVD Lei et al. (2014)	48.39	0.9934	0.9738
	LWT-SVD Lei et al. (2014)	48.06	0.9924	0.9623
	DWT-SVD Lei et al. (2014)	48.03	0.9924	0.9615
	SVD Lei et al. (2014)	48.03	0.9621	0.9604
	GA Kumsawat et al. (2005)	42.25	0.9687	-
	Proposed Method	57.2445	0.99875	0.9999
Ultrasound	IWT Lei et al. (2014)	48.12	0.9931	0.9675
	LWT Lei et al. (2014)	48.21	0.9925	0.9587
	DWT Lei et al. (2014)	48.03	0.9918	0.9578
	IWT-SVD Lei et al. (2014)	48.35	0.993	0.9679
	LWT-SVD Lei et al. (2014)	48.47	0.9934	0.9612
	DWT-SVD Lei et al. (2014)	48.43	0.9934	0.9608
	SVD Lei et al. (2014)	48.42	0.9935	0.9588
	GA Kumsawat et al. (2005)	42.12	0.9815	-
	Proposed Method	63.5296	0.99845	0.9999

Table 6.8 compares the performance of three different methods for watermarking in medical images. The methods are evaluated based on three metrics: Time (in seconds), *PSNR* (dB) and *SD* error. The results are compared against Xuan's method in Xuan et al. (2004b) and Arsalan's method in Arsalan et al. (2017). The payload size varies from 0.1 to 0.75. In terms of time, the proposed method outperforms Xuan's method and is significantly faster than Arsalan's method. For example, at a payload of 0.1, the proposed method takes only 19.3659 seconds, while Xuan's and Arsalan's methods take 0.6068 seconds and 208.0176 seconds, respectively.

Table 6.7: Comparison for PSNR (dB) and SSIM vs. payload (bpp) and Effective Payload (EP) for Xuan et al. Xuan et al. (2004b) and Arsalan et al. Arsalan et al. (2017)

with the corresponding data from Table 6.2

Image	Payload	0.1		0.2		0.3		0.4		0.5		0.6		0.7	
	Technique	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
Lena								EP (bpp) - 0.58							
	Xuan et al. (2004b)	49.80	0.9966	46.20	0.9933	43.40	0.9896	42.20	0.9860	41.20	0.9729	40.30	0.9682	39.00	0.9633
	Arsalan et al. (2017)	50.86	0.9968	46.71	0.9943	45.20	0.9910	44.30	0.9890	43.60	0.9783	42.60	0.9707	41.87	0.9707
	Proposed	56.66	0.9980	56.01	0.9960	55.98	0.9957	55.98	0.9955	55.08	0.9951	54.89	0.9946	54.16	0.9931
Goldhill								EP (bpp) - 0.4							
	Xuan et al. (2004b)	50.00	0.9956	46.60	0.9918	44.40	0.9886	42.90	0.9851	41.80	0.9815	40.90	0.9786	40.20	0.9746
	Arsalan et al. (2017)	52.59	0.9976	49.26	0.9957	47.92	0.9937	46.67	0.9924	46.22	0.9915	44.83	0.9885	44.11	0.9869
	Proposed	56.52	0.9986	56.50	0.9984	56.36	0.9980	55.83	0.9972	55.12	0.9960	54.90	0.9932	53.74	0.9915
Barbara								EP (bpp) - 0.48							
	Xuan et al. (2004b)	48.60	0.9966	45.60	0.9933	43.30	0.9896	41.20	0.9860	40.60	0.983	39.70	0.9793	38.60	0.9744
	Arsalan et al. (2017)	50.24	0.9968	47.30	0.9943	45.68	0.9910	44.81	0.9890	44.11	0.9869	43.10	0.9832	42.43	0.9811
	Proposed	58.91	0.9973	58.94	0.9966	57.56	0.9856	57.55	0.9940	56.54	0.9928	55.53	0.9897	54.36	0.9872
Hand								EP (bpp) - > 0.6							
	Xuan et al. (2004b)	56.28	0.9982	51.98	0.9953	49.76	0.9925	48.28	0.9896	47.22	0.9867	46.37	0.9837	45.69	0.9806
	Arsalan et al. (2017)	56.79	0.9984	52.28	0.9955	50.38	0.9927	49.2	0.9905	48.10	0.9876	47.27	0.9853	46.67	0.9836
	Proposed	61.59	0.9987	60.98	0.9965	59.97	0.9936	58.28	0.9915	57.51	0.9883	57.00	0.9859	56.69	0.9846
Knee								EP (bpp) - 0.58							
	Xuan et al. (2004b)	54.73	0.9973	51.56	0.9943	49.35	0.9905	47.86	0.9867	46.80	0.9832	45.96	0.9794	45.25	0.9756
	Arsalan et al. (2017)	56.41	0.9981	52.97	0.9957	50.53	0.9925	49.49	0.9906	48.58	0.9879	47.6	0.9851	46.59	0.9819
	Proposed	57.63	0.9995	57.06	0.9982	56.33	0.9962	56.33	0.9949	56.15	0.9926	55.33	0.9885	53.97	0.9863
Belly								EP (bpp) - > 0.6							
	Xuan et al. (2004b)	51.29	0.9955	47.97	0.9907	45.96	0.9863	44.32	0.9823	43.17	0.9781	42.38	0.9735	41.70	0.9683
	Arsalan et al. (2017)	52.12	0.9961	48.94	0.9927	47.37	0.9891	46.55	0.9872	45.83	0.9848	44.93	0.9813	44.20	0.9785
	Proposed	59.37	0.9989	58.90	0.9983	58.72	0.9972	58.00	0.9951	57.58	0.9900	57.05	0.9874	56.31	0.9850
Breast								EP (bpp) - > 0.6							
	Xuan et al. (2004b)	56.00	0.9986	51.70	0.9960	49.10	0.9929	47.30	0.9895	45.90	0.9861	44.90	0.9831	44.20	0.9799
	Arsalan et al. (2017)	56.20	0.9983	51.60	0.9958	49.90	0.9936	48.80	0.9917	47.70	0.9896	47.00	0.9872	46.20	0.9854
	Proposed	62.79	0.9994	62.70	0.9969	60.43	0.9952	60.28	0.9946	59.88	0.9921	58.98	0.9902	57.85	0.9886
X-ray (PA)								EP (bpp) - > 0.6							
	Xuan et al. (2004b)	53.80	0.9971	50.00	0.9928	48.10	0.9886	46.00	0.9843	45.60	0.9801	44.80	0.9760	44.10	0.9719
	Arsalan et al. (2017)	54.43	0.9971	50.70	0.9932	49.03	0.9903	48.11	0.9878	47.28	0.9853	46.29	0.9817	45.53	0.9783
	Proposed	59.21	0.9994	59.02	0.9986	58.60	0.9934	57.51	0.9916	56.85	0.9880	55.60	0.9863	54.53	0.9848

Table 6.8: Comparison of average for 300 medical images with Xuan et al. (2004b) and Arsalan et al. (2017) for Time (Seconds), PSNR and Standard Deviation Error.

Payload	Time (secs)			PSNR (dB)			SD error		
	Xuan *et al.*	Arsalan *et al.*	Proposed Technique	Xuan *et al.*	Arsalan *et al.*	Proposed Technique	Xuan *et al.*	Arsalan *et al.*	Proposed Technique
0.1	0.6068	208.0176	19.3659	54.81	56.25	59.4315	1.1	0.33	0.2081
0.2	0.6485	219.4836	21.4722	51.53	53.05	59.0392	0.9	0.29	0.2159
0.3	0.6472	219.4837	28.8286	49.48	51.38	58.1549	0.68	0.34	0.2352
0.4	0.7149	219.4838	33.7514	47.97	50.31	57.4206	0.51	0.38	0.2438
0.5	0.7884	219.4839	40.1951	46.79	49.35	56.9849	0.42	0.43	0.2500
0.6	0.8367	219.4840	45.9219	45.86	48.21	56.2720	0.37	0.38	0.2541
0.7	0.8688	219.4841	52.0009	45.10	47.33	55.4766	0.35	0.31	0.2640
0.75	0.9085	219.4842	55.6732	44.74	46.95	55.1470	0.35	0.25	0.2788

In terms of *PSNR*, the proposed method outperforms both Xuan's and Arsalan's methods at all payload sizes. At a payload of 0.1, the proposed method achieves a *PSNR* of 59.4315 *d*B, while Xuan's and Arsalan's methods achieve *PSNR*s of 54.81 *d*B and 56.25 *d*B, respectively. In terms of *SD* error, the proposed method outperforms Xuan's method, but is slightly worse than Arsalan's method. For example, at a payload of 0.1, the proposed method achieves an *SD* error of 0.2081, while Xuan's and Arsalan's methods achieve *SD* errors of 1.1 and 0.33, respectively. Overall, the proposed method outperforms both Xuan's and Arsalan's methods in terms of time and *PSNR*. However, Arsalan's method has a slightly better *SD* error performance

Furthermore, Table 6.9 depicts the comparison of proposed technique with watermarked images with varied *BPP* and capacity values with 6 existing methods for medical images for *PSNR* and *SSIM*. The methods are compared based on their performance on two types of medical images, namely, ACL-side-views and angiography masks. Overall, the proposed technique achieves higher capacity and better compression efficiency (lower *BPP*) compared to the existing methods. It also provides significant improvements in terms of *PSNR* and *SSIM*, achieving up to 7.6% higher *PSNR* from proposed technique and up to 0.8% higher *SSIM* of proposed technique compared to the best-performing existing method. The proposed technique achieves higher *PSNR* and *SSIM* values compared to existing methods when applied to both types of medical images. In particular, the proposed technique achieves a capacity of 38,900 bits and a *BPP* of 0.3428 for *ACL*-side-views, while achieving a capacity of 38,900 bits and a *BPP* of 0.3428 for angiography masks. Compared to the best-performing existing method, the proposed technique achieves improvements of up to 4.3% in terms of *PSNR* and up to 0.8% in terms of *SSIM* for *ACL*-side-views, and improvements of up to 5.1% in terms of *PSNR* and up to 0.8% in terms of *SSIM* for angiography masks.

Table 6.10 gives the comparison with *GA* Naheed et al. (2014), *PSO* Naheed et al. (2014), and Interpolation Luo et al. (2010) methods for the commonly referred images. These four commonly used images are evaluated for maximum capacity, *PSNR*, *BPP*, and *SSIM*. The proposed technique achieves significantly better results than the other methods in terms of capacity and *PSNR*, with an

Table 6.9: Comparison with existing methods for Capacity(bits), BPP, PSNR 1(dB) and SSIM 1 for existing methods () and PSNR 2(dB) and SSIM 2 for the proposed techniqe.

Medical Images	Method	Capacity	BPP	PSNR 1	PSNR 2	SSIM 1	SSIM 2
ACL-side-views	GA Naheed et al. (2014)	38,700	0.342793	49.011976	58.5276	0.998578	0.9986213
	PSO Naheed et al. (2014)	38,390	0.340074	49.004725	58.5278	0.998566	0.9986208
	Luo et al. (2010)	36,060	0.319409	48.946455	58.5317	0.998580	0.9987929
	Tian (2003)	12,217	0.108215	41.198559	60.2273	0.990596	0.9998638
	Xuan et al. (2005)	14,614	0.128260	48.143731	60.2204	0.998047	0.9998685
	Lee et al. (2007)	10,882	0.096390	48.420868	61.8481	0.998843	0.9999858
Angiography Mask	GA Naheed et al. (2014)	38,700	0.342793	49.011976	59.8704	0.998578	0.9986540
	PSO Naheed et al. (2014)	38,390	0.340074	49.004725	59.8867	0.998566	0.9986569
	Luo et al. (2010)	36,060	0.319409	48.946455	60.1552	0.998580	0.9987144
	Tian (2003)	12,217	0.108215	41.198559	61.5857	0.990596	0.9999453
	Xuan et al. (2005)	14,614	0.128260	48.143731	61.5802	0.998047	0.9999454
	Lee et al. (2007)	10,882	0.096390	48.420868	62.0724	0.998843	0.9999467

Table 6.10: Comparison of maximum capacity values with Naheed et al. GA Naheed et al. (2014) (GA), Naheed et al. PSO Naheed et al. (2014) (PSO), and Luo et al. Interpolation Luo et al. (2010) (IN) methods for the commonly referred images with proposed method (RT).

Med Images	Methods	Capacity	PSNR	BPP	SSIM
Plane	GA	87,415	49.00	0.99777	0.33346
	PSO	87,390	49.00	0.99778	0.99856
	IN	84,434	48.96	0.99784	0.32209
	RT	1,062,628	51.23	4.05360	0.96838
Lena	GA	73,231	48.85	0.99754	0.27935
	PSO	73,206	48.86	0.99753	0.27925
	IN	71,609	48.84	0.99756	0.27316
	RT	1,053,064	51.26	4.01712	0.96962
Lake	GA	39,600	48.55	0.99801	0.15106
	PSO	39,547	48.55	0.99801	0.15080
	IN	38,704	48.53	0.99800	0.14764
	RT	1,057,192	51.30	4.03286	0.96981
Baboon	GA	23,598	48.55	0.99863	0.09001
	PSO	23,374	48.55	0.99863	0.08916
	IN	22,709	48.50	0.99859	0.08662
	RT	1,048,960	51.25	4.00146	0.95994

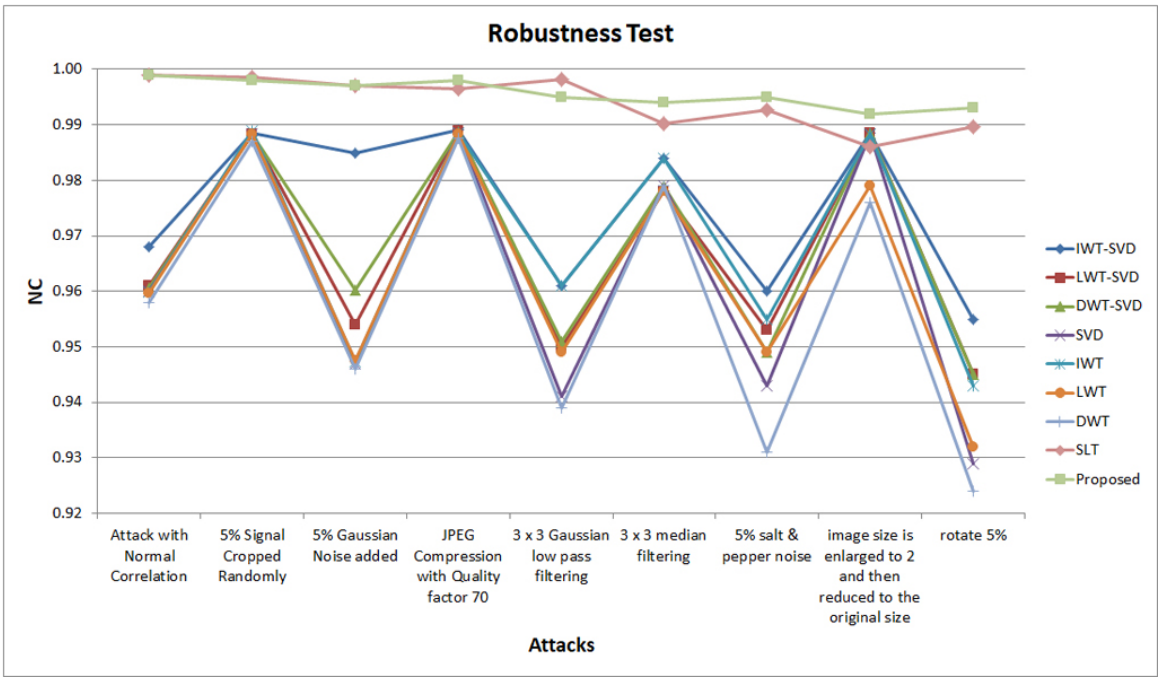


Figure 6.7: Comparison of NC with existing techniques from Lei et al. (2014) and Bamal and Kasana (2018) for two 64×64 watermarks.

average improvement of 98.8% and 4.2 dB, respectively. In terms of *BPP*, the proposed method performs worst than the other methods, but still achieves a reasonable compression ratio in comparison to the capacity. Finally, the *SSIM* values are high for all methods, indicating that the reconstructed images after using proposed technique are visually similar to the original images. As, the proposed technique uses *PSO* for threshold, which boosts the results than existing ones.

Figure 6.7 gives the comparison results of 9 attacks on lena with various transforms from from Lei et al. (2014) and Bamal and Kasana (2018) proving the proposed technique is mostly better. *SLT* Bamal and Kasana (2018) technique has better results for 3×3 gaussian low pass filter attack than the proposed technique. It can be due to the usage of low frequency bands for data embedding, but this is beneficial against all other attacks. Hence, it becomes the natural choice for data embedding.

Figure 6.8 references to the results that show that the proposed technique with *RT* is better than many state-of-the-art methods. For example the approximate percentage differences between the proposed technique with *RT* and the existing techniques at a payload of 0.5 bpp: Difference Expansion by Tian (2003)- 10.9%, Spread spectrum described by Xuan et al. (2004a)- 9.4%, Lee et al. (2007)- 10.9%, Bit-plane by Coltuc (2011)- 9.8%, Usman et al. (2009)- 9.0%, Xuan et al. (2005)- 7.0%, Arsalan et al. (2017)- 4.1%, *GA-RevWM* described by Arsalan et al. (2012)- 6.2%, Sachnev et al. (2009)- 7.3% and Siddiqa and Khan (2015)- 6.3%.

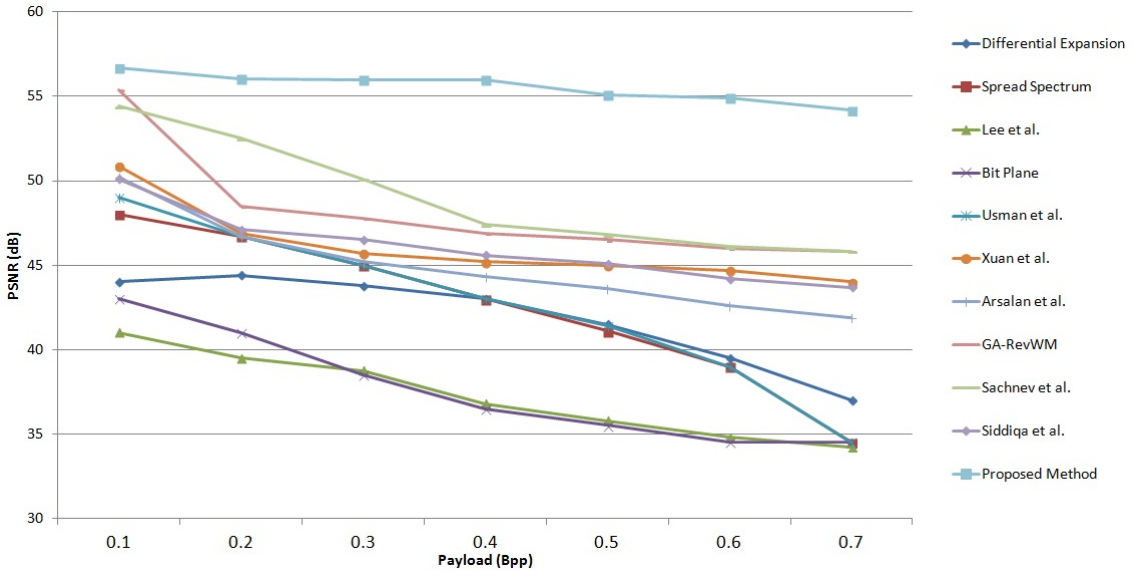


Figure 6.8: Comparison of PSNR(dB) with existing techniques for Lena.

6.5 Conclusion of the Chapter

A new approach is introduced for ridgelet-based blind watermarking that utilizes manifold techniques to enhance the technique's robustness. The watermarking process begins by partitioning the original image into *ROI* and *RONI*, which are then divided into non-overlapping blocks to effectively leverage *RT* characteristics for straight edges. The ridgelet coefficients matrix is constructed by selecting the best directions for embedding the watermark bits using *PSO* based on mean value's variance intensity and highest energy coefficients of each direction. Experimental results demonstrate that the proposed technique is highly robust, with no discernible differences between the original and watermarked images. The proposed techniques leverages techniques such as AES-256, SHA-3, and *RT* characteristics to improve watermark extraction robustness. The superiority of the proposed technique is demonstrated by comparing its results with those of other published works. The proposed technique exhibits high robustness against a variety of attacks, including speckle, salt and pepper noise, *JPEG* compression, blur, resizing, rotation, Weiner, cropping, Gaussian noise, Poisson, median, average, and Gaussian filtering.

Chapter 7

Conclusions and Future Directions

7.1 Conclusions

The research work embodied in this thesis has addressed the authentication, integrity and confidentiality of the medical images. Four novel efficient medical watermarking techniques are proposed in this research work. Various aspects of the research problem are investigated and the main findings are summarized below.

Watermarking in medical images is a crucial aspect due to the high importance of the data contained within these images. Existing watermarking techniques in the medical field suffer from various limitations such as low embedding capacity, vulnerability to network attacks, inadequate watermark recovery, low *BER*, limited applicability to color images, insufficient protection of *ROI*, inability to recover corrupted watermarks, and compromised invisibility. Therefore, there is a clear need for a techniques that addresses these challenges and provides high embedding capacity, security, robustness against attacks, full reversibility, and preservation of the *PSNR* value.

This research highlights the shortcomings of existing techniques and proposes an innovative approach that simultaneously improves multiple parameters essential for watermarking. The utilization of *SLT* for data embedding proves advantageous, as it increases the energy percentage of the image after compression, thereby enhancing the embedding capacity. *SLT* outperforms other transformations like *DWT* and *DCT* in terms of noise removal and signal compression, which in turn improves the *BER*. Moreover, *SLT* can extract image features for region classification, contributing to the overall effectiveness of the proposed technique. *SLT* also proves to be effective in image feature extraction, facilitating region classification and tamper detection. The inclusion of *RS* vector embedding further enhances capacity and security.

The employment of advanced cryptographic techniques, such as *MD5, AES,* and biometric thumbprints, addresses security concerns and ensures the confidentiality, integrity, and authenticity of embedded data. Additionally, the proposed technique addresses limitations in execution time, visual quality, and imperceptibility, providing faster processing, improved visual quality, and imperceptible watermarked images.

The first hybrid embedding approach incorporating *RS* vector further enhances the embedding capacity and security, offering a robust solution. The usage of *SLT*, with its implementation of three filters, ensures high robustness against various attacks. Additionally, this proposed technique demonstrates significantly reduced execution time, making it suitable for real-time applications. The visual quality of watermarked images is notably improved, with enhanced smoothness and preservation of visual details. The research also addresses security concerns by implementing techniques such as *MD5, AES,* and biometric thumbprints of patients. These measures effectively enhance the security and integrity of the watermark and cover image. Furthermore, the proposed technique provides tamper detection and localization capabilities. By employing *SLT* and *RS* vector for watermark embedding in selected blocks of the cover image, along with cryptographic techniques like *MD5* and *AES* for watermark security and compression techniques to increase capacity. The proposed technique demonstrates superior performance compared to several existing techniques in terms of *PSNR* and *BPP*. For example, when compared to Alattar (2004), the proposed technique improves *PSNR* by 71.536% and *BPP* by 51.689%, while also having a lower time complexity. Compared to Shih and Zhong (2016), the proposed technique achieves a 3.317% improvement in *PSNR* and a 2.045% improvement in *BPP*. The average improvement in *PSNR* for the proposed algorithm compared to the existing techniques is approximately 15.15 dB. The average improvement in *BPP* for the proposed algorithm compared to the existing techniques is approximately 0.2025.

The second technique presents a digital watermarking technique that combines Walsh-Hadamard transform, *SLT*, and *SVD* to address the challenges in watermarking medical images. The proposed technique offers improvements in embedding capacity, robustness, *BER*, and execution time, providing a comprehensive solution for secure watermarking. By incorporating *FWT* and *SLT* for data embedding, the proposed technique achieves increased embedding capacity, robustness against attacks, and improved *BER*. Both transforms exhibit favorable properties, such as energy compaction and lossless reversibility, contributing to enhanced performance. The proposed technique demonstrates reduced execution time due to the computational efficiency of *FWT* and *SLT*. The integration of *AES* and *SHA-3* further enhances watermark security, while compression techniques increase capacity. The proposed algorithm demonstrates improved PSNR between the cover and watermarked images compared to existing techniques. Additionally, it exhibits robustness against various attacks, surpassing existing medical watermarking techniques. The incorporation of biometric security measures ensures the integrity of the designed watermark. The average improvement in *PSNR* for the proposed algorithm compared to the existing techniques is approximately 13.55 dB and the average improvement in *BPP* is approximately 0.8378 for 256×256 *MRI* brain image *i.e.*, Figure 4.5 with block size of 4×4 for *SLT* and 8×8 for *FWT*.

The third technique undertakes the inclusion of *ANN* enables effective feature extraction, region

classification, tamper detection, and localization. This utilization of *ANN* enhances the overall security and integrity of the watermarking process. A hybrid approach is adopted for dual embedding, further enhancing the capacity, security, and robustness of the watermarked image. To ensure high security, the algorithm incorporates *SHA-3, AES*, and the biometric thumbprint of the patient. These cryptographic techniques enhance the security, compression, and reliability of the watermark and cover image. The average improvement in *PSNR* for the proposed algorithm compared to the existing techniques is approximately 13.37 dB and for *BPP* is approximately 0.1266 for a 256×256 *MRI* brain image (image 3 from Figure 5.6) using a block size of 8×8.

The fourth proposed watermarking technique addresses the limitations of existing methods by utilizing RT instead of traditional methods like *DWT*. *RT* overcomes the weaknesses of wavelets in representing straight lines and edges in images, particularly in higher dimensions. The use of RT leads to advantages such as improved SSIM and vectorizability through pseudopolar *FFT*. This proposed technique incorporates a dual output buffer configuration, enabling simultaneous execution of the Radon Transform and DWT on the chip. This configuration reduces the overall processing time. Experimental results validate the superiority of the proposed technique over other methods such as *IWT, SVD, DWT, LWT, SLT, IWT-SVD, LWT-SVD, DWT-SVD*, differential expansion, bit plane, spread spectrum, etc. The average improvement in PSNR for the proposed method compared to the existing methods Lei et al. (2014) from *MRI* image is approximately 19.66 dB. The average improvement in *MSSIM* for the proposed method compared to the existing methods Lei et al. (2014) from *MRI* image is approximately 0.0109 and average improvement in *NCA* is approximately 0.1958.

Overall, the proposed watermarking techniques address the limitations and challenges associated with existing medical image watermarking methods. It provides a comprehensive solution that improves capacity, security, robustness, execution time, visual quality, and imperceptibility. By leveraging advanced techniques such as *SLT, RT,* Radon Transform, Walsh Transform, and *ANN,* the proposed techniques demonstrate superior performance and effectiveness in securing medical images. These proposed techniques demonstrates resilience against more than 16 different attacks, while simultaneously increasing capacity, *BPP, PSNR, SSIM,* and reducing Standard Deviation Error (*SD* Error). The experimental results highlight the effectiveness of the proposed technique in terms of robustness, capacity, perceptibility, and processing time. The technique outperforms more than 30 existing methods and provides a selective and useful approach for secure watermarking. The experimental results validate the effectiveness and efficiency of the proposed technique, demonstrating its superiority through various performance metrics. The broader motivation for this research lies in the importance of medical imaging security, especially in critical situations like the *COVID-19* pandemic. By addressing the limitations of existing methods and providing enhanced robustness, contrast enhancement, tamper detection, and recovery capabilities, this research contributes to the

overall advancement and security of medical imaging practices. This research contributes to the advancement and security of medical imaging applications, addressing the critical need for reliable and secure watermarking techniques in the medical field.

7.2 Scope for future study

These future scopes aim to further advance the proposed watermarking technique, address emerging challenges, and explore new opportunities to enhance the security, performance, and applicability of medical image watermarking in diverse healthcare scenarios.

* **Deep learning-based watermarking:** Incorporating deep learning techniques, such as convolutional neural networks (CNNs) or generative adversarial networks (GANs), can further enhance the performance and robustness of the watermarking technique. Deep learning models can learn complex image features and patterns, allowing for more effective and secure embedding and extraction of watermarks.

* **Blockchain-based watermarking:** Integrating blockchain technology into the watermarking process can provide an immutable and decentralized system for storing and verifying watermarks. Blockchain can enhance the security and integrity of watermarked images by creating a transparent and tamper-proof record of the watermarking process.

* **Fusion of multiple watermarking techniques:** Exploring the fusion of different watermarking techniques, such as combining the proposed ridgelet-based technique with other existing methods, can lead to improved performance and robustness. The fusion of complementary techniques can leverage their individual strengths to overcome limitations and enhance the overall watermarking process.

* **Adaptive watermarking:** Developing adaptive watermarking techniques that can dynamically adjust the embedding strength, capacity, and robustness based on the specific requirements of different medical imaging applications. Adaptive watermarking can optimize the trade-off between imperceptibility and robustness, ensuring optimal performance for various scenarios.

* **Real-time watermarking:** Extending the proposed technique to support real-time watermarking applications, such as streaming medical images or live video feeds. Real-time watermarking requires efficient and low-latency algorithms to embed and extract watermarks in real-time, enabling secure and reliable watermarking for time-sensitive applications.

* **Watermarking for 3D medical imaging:** Expanding the proposed technique to support watermarking of three-dimensional (3D) medical images, such as CT scans or MRI volumes.

3D medical imaging presents unique challenges and opportunities for watermarking, and developing specialized techniques for securing volumetric data can have significant implications in healthcare and medical research.

* **Robustness against advanced attacks:** Continuously evaluating and enhancing the proposed technique's robustness against emerging and advanced attacks, such as deep learning-based image manipulations, adversarial attacks, or content-aware tampering. Staying ahead of potential vulnerabilities and ensuring the effectiveness of the watermarking technique against evolving attack methods is crucial for long-term security.

* **Standardization and integration:** Collaborating with relevant standardization bodies, such as the International Organization for Standardization (ISO), to establish standardized protocols and guidelines for medical image watermarking. Standardization promotes interoperability, consistency, and widespread adoption of watermarking techniques across different healthcare systems and institutions.

* **Improved watermarking techniques:** Further research and development can focus on refining the proposed watermarking technique to address any remaining limitations and challenges. This could involve optimizing the algorithm parameters, exploring alternative transformations or fusion approaches, and fine-tuning the embedding and extraction processes. The goal is to continuously enhance the performance, robustness, and efficiency of the watermarking technique.

* **Integration with emerging imaging technologies:** As medical imaging technologies continue to advance, such as with the introduction of new modalities or imaging devices, there is a need to adapt the watermarking technique to support these emerging technologies. Future work could focus on integrating the proposed technique with technologies like 3D imaging, hyperspectral imaging, or advanced imaging modalities to ensure compatibility and security across a wide range of medical imaging applications.

* **Application in telemedicine and remote healthcare:** With the growing adoption of telemedicine and remote healthcare, there is a need for secure and reliable transmission and storage of medical images. Future research could explore how the proposed watermarking technique can be applied in telemedicine scenarios to ensure the integrity, authenticity, and privacy of medical images during transmission and remote storage. This could involve considering challenges related to bandwidth constraints, network vulnerabilities, and remote authentication. **Enhanced security measures:** Continuing advancements in security measures can further strengthen the proposed watermarking technique. Future work could explore incorporating

advanced encryption algorithms, multi-factor authentication techniques, or biometric-based security measures to enhance the overall security of the watermark and cover image. This would provide additional layers of protection against unauthorized access or tampering attempts.

* **Standardization and adoption:** To facilitate widespread adoption and interoperability of the proposed watermarking technique, future efforts could focus on standardizing the technique through collaboration with relevant standardization bodies, medical imaging organizations, and regulatory authorities. Developing industry-wide standards and guidelines would ensure consistent implementation and evaluation of medical image watermarking techniques across different healthcare systems and institutions. **Evaluation under real-world conditions:** While the proposed technique has demonstrated promising results in experimental settings, future research could focus on evaluating its performance under real-world conditions. This could involve conducting large-scale studies involving diverse medical image datasets, different healthcare settings, and a variety of watermarking scenarios. Real-world evaluations can provide valuable insights into the practical effectiveness, limitations, and potential areas for improvement of the proposed technique.

* **Ethical and legal considerations:** As medical image watermarking involves sensitive patient data, future research should also consider the ethical and legal implications of implementing the proposed technique. This includes addressing issues related to patient consent, data privacy, compliance with regulations such as HIPAA (Health Insurance Portability and Accountability Act), and ensuring transparency and accountability in the watermarking process.

Bibliography

Abou-Loukh, S. and Gatea, S. (2011). Spoken word recognition using slantlet transform and dynamic time warping. *Nahrain University, College of Engineering Journal*, 14(1):34–45.

Abou-Loukh, S., Zeyad, T., and Thabit, R. (2010). Ecg classification using slantlet transform and artificial neural network. *Journal of Engineering*, 16(1):4510–4528.

Acharya, R., Bhat, P. S., Kumar, S., and Min, L. C. (2003). Transmission and storage of medical images with patient information. *Computers in Biology and Medicine*, 33(4):303–310.

Acharya, R., Niranjan, U., Iyengar, S. S., Kannathal, N., and Min, L. C. (2004). Simultaneous storage of patient information with medical images in the frequency domain. *Computer Methods and Programs in Biomedicine*, 76(1):13–19.

Ahlawat, P. and Dave, M. (2021). An attack resistant key predistribution scheme for wireless sensor networks. *Journal of King Saud University-Computer and Information Sciences*, 33(3):268–280.

Al-Qershi, O. M. and Khoo, B. (2009). Authentication and data hiding using a reversible roi-based watermarking scheme for dicom images. In *Proceedings of International Conference on Medical Systems Engineering*, pages 829–834.

Al-Qershi, O. M. and Khoo, B. E. (2011). Authentication and data hiding using a hybrid roi-based watermarking scheme for dicom images. *Journal of Digital Imaging*, 24(1):114–125.

Al-Rakhami, M. S., Islam, M. M., Islam, M. Z., Asraf, A., Sodhro, A. H., and Ding, W. (2021). Diagnosis of covid-19 from x-rays using combined cnn-rnn architecture with transfer learning. *MedRxiv*, pages 2020–08.

Al-Zewairi, M., Almajali, S., and Ayyash, M. (2020). Unknown security attack detection using shallow and deep ann classifiers. *Electronics*, 9(12):2006.

Alattar, A. M. (2004). Reversible watermark using the difference expansion of a generalized integer transform. *IEEE transactions on image processing*, 13(8):1147–1156.

Alvarez, G., Li, S., and Hernandez, L. (2007). Analysis of security problems in a medical image encryption system. *Computers in Biology and Medicine*, 37(3):424–427.

An, L., Gao, X., Li, X., Tao, D., Deng, C., and Li, J. (2012). Robust reversible watermarking via clustering and enhanced pixel-wise masking. *IEEE Transactions on image processing*, 21(8):3598–3611.

Anand, D. and Niranjan, U. (1998). Watermarking medical images with patient information. In *Engineering in Medicine and Biology Society, 1998. Proceedings of the 20th Annual International Conference of the IEEE*, volume 2, pages 703–706. IEEE.

Arsalan, M., Malik, S. A., and Khan, A. (2012). Intelligent reversible watermarking in integer wavelet domain for medical images. *Journal of Systems and Software*, 85(4):883–894.

Arsalan, M., Qureshi, A. S., Khan, A., and Rajarajan, M. (2017). Protection of medical images and patient related information in healthcare: Using an intelligent and reversible watermarking technique. *Applied Soft Computing*, 51:168–179.

Asraf, A., Islam, M., Haque, M., et al. (2020). Deep learning applications to combat novel coronavirus (covid-19) pandemic. *SN Computer Science*, 1(6):1–7.

Balasamy, K., Dharshini, M., Gayathri, S., and Geetha, M. (2016). Image authentication system using fused watermarking technique. *International Journal of Innovative Research in Computer and Communication Engineering*, 4(1):189–193.

Bamal, R. and Kasana, S. S. (2018). Slantlet based hybrid watermarking technique for medical images. *Multimedia Tools and Applications*, 77(10):12493–12518.

Bamal, R. and Kasana, S. S. (2019). Dual hybrid medical watermarking using walsh-slantlet transform. *Multimedia Tools and Applications*, 78(13):17899–17927.

Bhatnagar, G. and Raman, B. (2009). Robust watermarking in multiresolution walsh-hadamard transform. In *Advance Computing Conference, 2009. IACC 2009. IEEE International*, pages 894–899. IEEE.

Biryukov, A., Dunkelman, O., Keller, N., Khovratovich, D., and Shamir, A. (2010). Key recovery attacks of practical complexity on aes-256 variants with up to 10 rounds. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 299–319. Springer.

Biryukov, A., Khovratovich, D., and Nikolić, I. (2009). Distinguisher and related-key attack on the full aes-256. In *Advances in Cryptology-CRYPTO 2009*, pages 231–249. Springer.

Campisi, P., Kundur, D., and Neri, A. (2004). Robust digital watermarking in the ridgelet domain. *IEEE signal processing letters*, 11(10):826–830.

Candes, E. J. (1998). *Ridgelets: theory and applications*. PhD thesis, Stanford University.

Chen, G. and Kégl, B. (2007). Image denoising with complex ridgelets. *Pattern Recognition*, 40(2):578–585.

Chiang, K.-H., Chang-Chien, K.-C., Chang, R.-F., and Yen, H.-Y. (2008). Tamper detection and restoring system for medical images using wavelet-based reversible data embedding. *Journal of Digital Imaging*, 21(1):77–90.

Coatrieux, G., Maitre, H., Sankur, B., Rolland, Y., and Collorec, R. (2000). Relevance of watermarking in medical imaging. In *Information Technology Applications in Biomedicine, 2000. Proceedings. 2000 IEEE EMBS International Conference on*, pages 250–255. IEEE.

Coatrieux, G., Quantin, C., Montagner, J., Fassa, M., Allaert, F.-A., and Roux, C. (2008). Watermarking medical images with anonymous patient identification to verify authenticity. In *MIE*, volume 136, pages 667–672.

Coltuc, D. (2011). Improved embedding for prediction-based reversible watermarking. *IEEE Transactions on Information Forensics and Security*, 6(3):873–882.

Cox, I. J., Kilian, J., Leighton, F. T., and Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. *IEEE transactions on image processing*, 6(12):1673–1687.

Cruz, R. M., Peixoto, H. M., and Magalhães, R. M. (2011). *Artificial neural networks and efficient optimization techniques for applications in engineering*. INTECH Open Access Publisher.

Dong, J., Li, J., and Duan, Y. (2015). A robust watermarking algorithm for encrypted medical images based on dct encrypted domain. In *International Conference on Electronic Science and Automation Control*, pages 140–143. Citeseer.

Donoho, D. L. and Flesia, A. G. (2003). 1-digital ridgelet transform based on true ridge functions. *Studies in Computational Mathematics*, 10:1–30.

Doull, K. E., Chalmers, C., Fergus, P., Longmore, S., Piel, A. K., and Wich, S. A. (2021). An evaluation of the factors affecting 'poacher'detection with drones and the efficacy of machine-learning for detection. *Sensors*, 21(12):4074.

Dragoi, I.-C. and Coltuc, D. (2015). On local prediction based reversible watermarking. *IEEE Transactions on Image Processing*, 24(4):1244–1246.

Eswaraiah, R. and Reddy, E. S. (2014). Medical image watermarking technique for accurate tamper detection in roi and exact recovery of roi. *International journal of telemedicine and applications*, 2014:13.

Eswaraiah, R. and Sudhir, T. (2022). Recovering roi of medical image through curvelet transform-based watermarking method. In *Evolution in Computational Intelligence*, pages 223–232. Springer.

Fakhari, P., Vahedi, E., and Lucas, C. (2011). Protecting patient privacy from unauthorized release of medical images using a bio-inspired wavelet-based watermarking approach. *Digital Signal Processing*, 21(3):433–446.

Ferrag, M. A., Friha, O., Maglaras, L., Janicke, H., and Shu, L. (2021). Federated deep learning for cyber security in the internet of things: Concepts, applications, and experimental analysis. *IEEE Access*, 9:138509–138542.

Gao, G., Wan, X., Yao, S., Cui, Z., Zhou, C., and Sun, X. (2017). Reversible data hiding with contrast enhancement and tamper localization for medical images. *Information Sciences*, 385:250–265.

Garcia-Hernandez, J. J., Gomez-Flores, W., and Rubio-Loyola, J. (2016). Analysis of the impact of digital watermarking on computer-aided diagnosis in medical imaging. *Computers in biology and medicine*, 68:37–48.

Giakoumaki, A., Pavlopoulos, S., and Koutsouris, D. (2006a). Multiple image watermarking applied to health information management. *IEEE Transactions on Information Technology in Biomedicine*, 10(4):722–732.

Giakoumaki, A., Pavlopoulos, S., and Koutsouris, D. (2006b). Secure and efficient health data management through multiple watermarking on medical images. *Medical and Biological Engineering and Computing*, 44(8):619.

Gumbs, A. A., Frigerio, I., Spolverato, G., Croner, R., Illanes, A., Chouillard, E., and Elyan, E. (2021). Artificial intelligence surgery: How do we get to autonomous actions in surgery? *Sensors*, 21(16):5526.

Guo, X. and Zhuang, T.-g. (2009). A region-based lossless watermarking scheme for enhancing security of medical data. *Journal of digital imaging*, 22(1):53–64.

Haddad, S., Coatrieux, G., Moreau-Gaudry, A., and Cozic, M. (2020). Joint watermarking-encryption-jpeg-ls for medical image reliability control in encrypted and compressed domains. *IEEE Transactions on Information Forensics and Security*, 15:2556–2569.

Hamdan, S., Almajali, S., Ayyash, M., Salameh, H. B., and Jararweh, Y. (2023). An intelligent edge-enabled distributed multi-task learning architecture for large-scale iot-based cyber–physical systems. *Simulation Modelling Practice and Theory*, 122:102685.

Huang, Q., Hao, B., and Chang, S. (2016). Adaptive digital ridgelet transform and its application in image denoising. *Digital Signal Processing*, 52:45–54.

Hykin, S. (1999). Neural networks: A comprehensive foundation. printice-hall. *Inc., New Jersey*.

Islam, M. M., Karray, F., Alhajj, R., and Zeng, J. (2021). A review on deep learning techniques for the diagnosis of novel coronavirus (covid-19). *Ieee Access*, 9:30551–30572.

Islam, M. Z., Islam, M. M., and Asraf, A. (2020). A combined deep cnn-lstm network for the detection of novel coronavirus (covid-19) using x-ray images. *Informatics in medicine unlocked*, 20:100412.

Ismail, R. and Ali, S. M. (2023). Design of quality improvement technique through ridgelet transform on watermarked video. *Iraqi Journal For Computer Science and Mathematics*, 4(1):204–210.

Kalantari, N. K., Ahadi, S. M., and Vafadust, M. (2010). A robust image watermarking in the ridgelet domain using universally optimum decoder. *IEEE Transactions on circuits and systems for video technology*, 20(3):396–406.

Karaboga, D. and Basturk, B. (2007). A powerful and efficient algorithm for numerical function optimization: artificial bee colony (abc) algorithm. *Journal of global optimization*, 39(3):459–471.

Kennedy, J. and Eberhart, R. (1995). Particle swarm optimization. In *Neural Networks, 1995. Proceedings., IEEE International Conference on*, volume 4, pages 1942–1948 vol.4.

Khor, H. L., Liew, S.-C., and Zain, J. M. (2016). Parallel digital watermarking process on ultrasound medical images in multicores environment. *Journal of Biomedical Imaging*, 2016:4.

Kishore, P., Kishore, S., Kumar, E. K., Kumar, K., and Aparna, P. (2015). Medical image watermarking with dwt-bat algorithm. In *Signal Processing And Communication Engineering Systems (SPACES), 2015 International Conference on*, pages 270–275. IEEE.

Kulkarni, M. B. and Patil, R. T. (2012). Tamper detection & recovery in medical image with secure data hiding using reversible watermarking. *Int J Emerg Technol Adv Eng*, 2(3):370–373.

Kumar, S. and Kumar, T. V. (2022). Artificial intelligence for healthcare: Issues, challenges and opportunities. *AIJR Abstracts*, page 77.

Kumar, T. V. et al. (2022). Machine learning for healthcare. In *Synergistic Interaction of Big Data with Cloud Computing for Industry 4.0*, pages 133–147. CRC Press.

Kumsawat, P., Attakitmongcol, K., and Srikaew, A. (2005). A new approach for optimization in image watermarking by using genetic algorithms. *IEEE Transactions on Signal Processing*, 53(12):4707–4719.

Lafta, M. M. and Alwan, I. M. (2011). Watermarking in image using slantlet transform. *Iraqi Journal of Science*, 52(2):225–230.

Lee, S., Yoo, C. D., and Kalker, T. (2007). Reversible image watermarking based on integer-to-integer wavelet transform. *IEEE Transactions on Information Forensics and Security*, 2(3):321–330.

Lei, B., Tan, E.-L., Chen, S., Ni, D., Wang, T., and Lei, H. (2014). Reversible watermarking scheme for medical image based on differential evolution. *Expert Systems with Applications*, 41(7):3178–3188.

Li, M., Poovendran, R., and Narayanan, S. (2005). Protecting patient privacy against unauthorized release of medical images in a group communication environment. *Computerized Medical Imaging and Graphics*, 29(5):367–383.

Li, Q., Wang, X., Pei, Q., et al. (2022). Compression domain reversible robust watermarking based on multilayer embedding. *Security and Communication Networks*, 2022.

Li, X., Zhang, W., Gui, X., and Yang, B. (2015). Efficient reversible data hiding based on multiple histograms modification. *IEEE Transactions on Information Forensics and Security*, 10(9):2016–2027.

Lin, S., Kuo, Y.-C., and Huang, Y.-H. (2006). An image watermarking scheme with tamper detection and recovery. In *First International Conference on Innovative Computing, Information and Control - Volume I (ICICIC'06)*, volume 3, pages 74–77.

Lin, S. D. and Otoya, P. E. L. (2023). Pose-invariant face recognition via facial landmark based ensemble learning. *IEEE Access*.

Lin, S. D. and Otoya, P. L. (2022). Large pose detection and facial landmark description for pose-invariant face recognition. In *2022 IEEE 5th International Conference on Knowledge Innovation and Invention*, pages 143–148. IEEE.

Liu, Z., Li, J., Ai, Y., Zheng, Y., and Liu, J. (2022). A robust encryption watermarking algorithm for medical images based on ridgelet-dct and thm double chaos. *Journal of Cloud Computing*, 11(1):1–20.

Luo, L., Chen, Z., Chen, M., Zeng, X., and Xiong, Z. (2010). Reversible image watermarking using interpolation technique. *IEEE Transactions on information forensics and security*, 5(1):187–193.

Luo, Y., Li, L., Liu, J., Tang, S., Cao, L., Zhang, S., Qiu, S., and Cao, Y. (2021). A multi-scale image watermarking based on integer wavelet transform and singular value decomposition. *Expert Systems with Applications*, 168:114272.

Manasrah, T. and Al-Haj, A. (2008). Management of medical images using wavelets-based multi-watermarking algorithm. In *Innovations in Information Technology, 2008. IIT 2008. International Conference on*, pages 697–701. IEEE.

Mangaiyarkarasi, P. and Arulselvi, S. (2011). A new digital image watermarking based on finite ridgelet transform and extraction using ica. In *Emerging Trends in Electrical and Computer Technology (ICETECT), 2011 International Conference on*, pages 837–841. IEEE.

Mao, Q., Li, F., and Chang, C.-C. (2015). Reversible data hiding with oriented and minimized distortions using cascading trellis coding. *Information Sciences*, 317:170–180.

Memon, N. A. (2010). *Watermarking of medical images for content authentication and copyright protection.* PhD thesis, Ghulam Ishaq Khan Institute of Engineering Sciences & Technology, Swabi.

Milanova, M. G., Ford, C., Kountchev, R., and Kountcheva, R. (2003). Digital watermarking for medical images. In *METMBS*, pages 509–520.

Mohammed, R. T. and Khoo, B. E. (2012). Image watermarking using slantlet transform. In *Industrial Electronics and Applications (ISIEA), 2012 IEEE Symposium on*, pages 281–286. IEEE.

Mohananthini, N. and Yamuna, G. (2015). A study of dwt-svd based multiple watermarking scheme for medical images. *IJ Network Security*, 17(5):558–568.

Mohanty, S. P. (1999). Digital watermarking: A tutorial review. *URL: http://www. csee. usf. edu/˜ smohanty/research/Reports/WMSurvey1999Mohanty. pdf.*

Muhammad, L., Islam, M., Usman, S. S., Ayon, S. I., et al. (2020). Predictive data mining models for novel coronavirus (covid-19) infected patients' recovery. *SN Computer Science*, 1(4):1–7.

Mulaydinov, F. (2021). Digital economy is a guarantee of government and society development. *Ilkogretim Online*, 20(3):1474–1479.

Mulcahy, C. (1997). Image compression using the haar wavelet transform. *Spelman Science and Mathematics Journal*, 1(1):22–31.

Mutt, S. and Kumar, S. (2009). Secure image steganography based on slantlet transform. In *Methods and Models in Computer Science, 2009. ICM2CS 2009. Proceeding of International Conference on*, pages 1–7. IEEE.

Naheed, T., Usman, I., Khan, T. M., Dar, A. H., and Shafique, M. F. (2014). Intelligent reversible watermarking technique in medical images using ga and pso. *Optik-International Journal for Light and Electron Optics*, 125(11):2515–2525.

Naseem, M., Qureshi, M., Cheema, A., and Rahman, A. (2013). Hash based medical image authentication and recovery using chaos and residue number system. *the Journal of Basic and Applied Scientific Research*, 3(6):488–495.

Panda, G., Dash, P., Pradhan, A., and Meher, S. (2002). Data compression of power quality events using the slantlet transform. *IEEE Transactions on power delivery*, 17(2):662–667.

Popov, M. and Mihanović, F. (2022). Hl7 functionalities in ris/pacs/his system integration. *Radiološki vjesnik: radiologija, radioterapija, nuklearna medicina*, 46(1):12–18.

Priya, R. L. and Sadasivam, V. (2015). Protection of health imagery by region based lossless reversible watermarking scheme. *The Scientific World Journal*, 2015.

Rahman, M. M., Islam, M., Manik, M., Hossen, M., Al-Rakhami, M. S., et al. (2021). Machine learning approaches for tackling novel coronavirus (covid-19) pandemic. *Sn Computer Science*, 2(5):1–10.

Rahman, M. M., Manik, M. M. H., Islam, M. M., Mahmud, S., and Kim, J.-H. (2020). An automated system to limit covid-19 using facial mask detection in smart city network. In *2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, pages 1–5. IEEE.

Rahouti, M., Ayyash, M., Jagatheesaperumal, S. K., and Oliveira, D. (2021). Incremental learning implementations and vision for cyber risk detection in iot. *IEEE Internet of Things Magazine*, 4(3):114–119.

Rayachoti, E. (2023). A robust and high embedding capacity watermarking technique for telemedicine. *The Imaging Science Journal*, pages 1–12.

Rivest, R. (1992). The md5 message-digest algorithm. *URL: https://www.ietf.org/rfc/rfc1321.txt*.

Rosenblatt, F. (1958). The perceptron: A probabilistic model for information storage and organization in the brain. *Psychological review*, 65(6):386.

Sachnev, V., Kim, H. J., Nam, J., Suresh, S., and Shi, Y. Q. (2009). Reversible watermarking algorithm using sorting and prediction. *IEEE Transactions on Circuits and Systems for Video Technology*, 19(7):989–999.

Sadreazami, H. and Amini, M. (2012). A robust spread spectrum based image watermarking in ridgelet domain. *AEU-International Journal of Electronics and Communications*, 66(5):364–371.

Selesnick, I. W. (1998). The slantlet transform. In *Time-Frequency and Time-Scale Analysis, 1998. Proceedings of the IEEE-SP International Symposium on*, pages 53–56. IEEE.

Selesnick, I. W. (1999). The slantlet transform. *IEEE transactions on signal processing*, 47(5):1304–1313.

Shaji, V. and Prakash, V. V. (2015). Medical image watermarking using cgr. *International Journal of Engineering Research and General Science*, 3(5):580–586.

Sharma, A., Dave, M., Singh, A. K., and Ghrera, S. (2015). Encryption based medical image watermarking against signal processing attacks. In *Proceedings of International Conference on Future Computational Technologies (ICFCT 2015)*, pages 82–88.

Shih, F. Y. (2017). *Digital watermarking and steganography: fundamentals and techniques*. CRC Press.

Shih, F. Y. and Wu, Y.-T. (2005). Robust watermarking and compression for medical images based on genetic algorithms. *Information Sciences*, 175(3):200–216.

Shih, F. Y. and Zhong, X. (2016). High-capacity multiple regions of interest watermarking for medical images. *Information Sciences*, 367:648–659.

Siddiqa, A. and Khan, A. (2015). High capacity reversible image watermarking using error expansion and context-dependent embedding. *Electronics Letters*, 51(13):985–987.

Silva, P. d. F., Cruz, R. M., and D Assuncao, A. G. (2010). Neuromodeling and natural optimization of nonlinear devices and circuits. *System and Circuit Design for Biologically-Inspired Intelligent Learning*, 1969067189.

Singh, A. K., Dave, M., and Mohan, A. (2014). Wavelet based image watermarking: futuristic concepts in information security. *Proceedings of the National Academy of Sciences, India Section A: Physical Sciences*, 84:345–359.

Srivastava, G. and Khari, M. (2021). *Bioelectronics and Medical Devices: Applications and Technology*. CRC Press.

Thabit, R. and Khoo, B. E. (2014). Robust reversible watermarking scheme using slantlet transform matrix. *Journal of Systems and Software*, 88:74–86.

Thabit, R. and Khoo, B. E. (2017). Medical image authentication using slt and iwt schemes. *Multimedia Tools and Applications*, 76(1):309–332.

Thodi, D. M. and Rodríguez, J. J. (2007). Expansion embedding techniques for reversible watermarking. *IEEE transactions on image processing*, 16(3):721–730.

Thompson, S., Fergus, P., Chalmers, C., and Reilly, D. (2020). Detection of obstructive sleep apnoea using features extracted from segmented time-series ecg signals using a one dimensional convolutional neural network. In *2020 International Joint Conference on Neural Networks*, pages 1–8. IEEE.

Tian, J. (2003). Reversible data embedding using a difference expansion. *IEEE transactions on circuits and systems for video technology*, 13(8):890–896.

Tian, L., Zheng, N., Xue, J., Li, C., and Wang, X. (2011). An integrated visual saliency-based watermarking approach for synchronous image authentication and copyright protection. *Signal Processing: Image Communication*, 26(8):427–437.

Tian, Y., Tan, T., Wang, Y., and Fang, Y. (2003). Do singular values contain adequate information for face recognition? *Pattern recognition*, 36(3):649–655.

Umamageswari, A. and Suresh, G. (2015). Analysis of secure medical image communication with digital signature and reversible watermarking. *Indonesian Journal of Electrical Engineering and Computer Science*, 15(3):544–553.

Usman, I., Khan, A., Ali, A., and Choi, T.-S. (2009). Reversible watermarking based on intelligent coefficient selection and integer wavelet transform. *International Journal of Innovative Computing, Information and Control*, 5(12).

Uzun, I. S. and Amira, A. (2005). Design and fpga implementation of finite ridgelet transform [image processing applications]. In *Circuits and Systems, 2005. ISCAS 2005. IEEE International Symposium on*, pages 5826–5829. IEEE.

Wakatani, A. (2002). Digital watermarking for roi medical images by using compressed signature image. In *System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on*, pages 2043–2048. IEEE.

Wang, T., Liu, Z., Lu, G., and Liu, J. (2020). Temporal-spatio graph based spectrum analysis for bearing fault detection and diagnosis. *IEEE Transactions on Industrial Electronics*, 68(3):2598–2607.

Wang, Z.-H., Lee, C.-F., and Chang, C.-Y. (2013). Histogram-shifting-imitated reversible data hiding. *Journal of systems and software*, 86(2):315–323.

WEI, J. C. and KERN, G. M. (1989). Commonality analysis: A linear cell clustering algorithm for group technology. *The International Journal Of Production Research*, 27(12):2053–2062.

Welch, T. A. (1984). A technique for high-performance data compression. *Computer*, 6(17):8–19.

Woo, C.-S., Du, J., and Pham, B. L. (2005). Multiple watermark method for privacy control and tamper detection in medical images.

Wu, H.-T., Dugelay, J.-L., and Shi, Y.-Q. (2015a). Reversible image data hiding with contrast enhancement. *IEEE signal processing letters*, 22(1):81–85.

Wu, H.-T., Huang, J., and Shi, Y.-Q. (2015b). A reversible data hiding method with contrast enhancement for medical images. *Journal of Visual Communication and Image Representation*, 31:146–153.

Wu, J. H., Chang, R.-F., Chen, C.-J., Wang, C.-L., Kuo, T.-H., Moon, W. K., and Chen, D.-R. (2008). Tamper detection and recovery for medical images using near-lossless information hiding technique. *Journal of Digital Imaging*, 21(1):59–76.

Xiao, D., Deng, M., and Zhu, X. (2015). A reversible image authentication scheme based on compressive sensing. *Multimedia Tools and Applications*, 74(18):7729–7752.

Xu, Y., Yan, X., Sun, B., and Liu, Z. (2022). Global contextual residual convolutional neural networks for motor fault diagnosis under variable-speed conditions. *Reliability Engineering & System Safety*, 225:108618.

Xuan, G., Shi, Y. Q., Chai, P., Teng, J., Ni, Z., and Tong, X. (2009). Optimum histogram pair based image lossless data embedding. In *Transactions on Data Hiding and Multimedia Security IV*, pages 84–102. Springer.

Xuan, G., Shi, Y. Q., Yang, C., Zheng, Y., Zou, D., and Chai, P. (2004a). Lossless data hiding using integer wavelet transform and spread spectrum. In *IEEE International Workshop on Multimedia Signal Processing*. Citeseer.

Xuan, G., Shi, Y. Q., Yang, C., Zheng, Y., Zou, D., and Chai, P. (2005). Lossless data hiding using integer wavelet transform and threshold embedding technique. In *Multimedia and Expo, 2005. ICME 2005. IEEE International Conference on*, pages 1520–1523. IEEE.

Xuan, G., Yang, C., Zhen, Y., Shi, Y. Q., and Ni, Z. (2004b). Reversible data hiding using integer wavelet transform and companding technique. In *International Workshop on Digital Watermarking*, pages 115–124. Springer.

Xuan, G., Yao, Q., Yang, C., Gao, J., Chai, P., Shi, Y. Q., and Ni, Z. (2006). Lossless data hiding using histogram shifting method based on integer wavelets. In *International Workshop on Digital Watermarking*, pages 323–332. Springer.

Xuan, G., Zhu, J., Chen, J., Shi, Y. Q., Ni, Z., and Su, W. (2002). Distortionless data hiding based on integer wavelet transform. *Electronics Letters*, 38(25):1646–1648.

Yang, S., Wang, M., and Jiao, L. (2008). Incremental constructive ridgelet neural network. *Neurocomputing*, 72(1):367–377.

Zain, J. and Clarke, M. (2005). Security in telemedicine: issues in watermarking medical images. In *International conference: science of electronic, technologies of information and telecommunications*.

Zain, J. M. and Clarke, M. (2007). Reversible region of non-interest (roni) watermarking for authentication of dicom images. *IJCSNS*, 7(9):19.

Zain, J. M. and Clarke, M. (2011). Reversible region of non-interest (roni) watermarking for authentication of dicom images. *arXiv preprint arXiv:1101.1603*.

Zain, J. M. and Fauzi, A. R. (2006). Medical image watermarking with tamper detection and recovery. In *Engineering in Medicine and Biology Society, 2006. EMBS'06. 28th Annual International Conference of the IEEE*, pages 3270–3273. IEEE.

Zain, J. M. and Fauzi, A. R. (2007). Evaluation of medical image watermarking with tamper detection and recovery (aw-tdr). In *Engineering in Medicine and Biology Society, 2007. EMBS 2007. 29th Annual International Conference of the IEEE*, pages 5661–5664. IEEE.

Zhao, Z., Luo, H., Lu, Z.-M., and Pan, J.-S. (2011). Reversible data hiding based on multilevel histogram modification and sequential recovery. *AEU-International Journal of Electronics and Communications*, 65(10):814–826.

Zhu, R. and Wang, X. (2008). Robust watermarking scheme in finite ridgelet transform domain. In *Computational Intelligence and Industrial Application, 2008. PACIIA'08. Pacific-Asia Workshop on*, volume 1, pages 588–592. IEEE.

Zou, D., Shi, Y. Q., and Ni, Z. (2004). A semi-fragile lossless digital watermarking scheme based on integer wavelet transform. In *IEEE 6th Workshop on Multimedia Signal Processing, 2004.*, pages 195–198.