

ANALYSIS AND DESIGN OF A MULTILEVEL SECURITY MECHANISM FOR DATA COMMUNICATION NETWORKS

THESIS

Submitted in fulfillment of the requirement of degree of

DOCTOR OF PHILOSOPHY

to

The Faculty of Engineering and Technology

by

SANGEETA DHALL

(Registration No.: 17-YMCA-904010)

Under the Supervision of

Dr. SHAILENDER GUPTA



Department of Electronics Engineering
J.C. Bose University of Science and Technology, YMCA, Faridabad
Sector-6, Mathura Road, Faridabad-121006, Haryana, INDIA

July 2023

DEDICATIONS

GOD the most courteous and sympathetic: who gave me the power, well-being, nerves and provided me with all the people to whom I am offering this hard work, which took a lot of fortitude and period until it came to light.

My Parents: I would like to dedicate the fruitful outcome of this work to my respectable mother and father, who always put in a lot of confidence and belief in me and encouraged me at every hardship and hurdle of life. My gratitude, love, respect, and thanks go to my dearest mother. Without her blessings, prayers, and pure love, I would have attained nothing in life.

My Brothers: My gratitude and appreciation to my brothers for their continuous support, encouragement, and patience during each instance of my life and study.

My Husband: My affectionate thanks go to my husband for his sustained support, patience, and thoughtful all the way through the interval of my study time.

My Daughters: I would like to bestow this thesis and all my accomplishments in life to my lovely daughters, who have been my steady source of hope and fortitude to go on despite the difficult times I have encountered. Their smiles have repeatedly pushed me to put in my best potential efforts to be an improved individual.

My supervisor: I would like to express my sincerest gratefulness towards my supervisor Dr. Shailender Gupta for providing me the opportunity to work in the challenging areas of multimedia security. Dr. Gupta has been an inexorable source of inspiration and support all through my Ph.D. duration. Devoid of his supervision, stimulus, and support, this thesis would never come to radiance. I would also like to thank him for his valuable comments, suggestions, and discussions.

My friends and colleagues: Before I finish, I wish to thanks all friends, fellow students, and staff in the Department of Electronics Engineering in the J.C. Bose University of Science and Technology, YMCA, for their back-up and support during the time of this course. I want to express my special thanks to Dr. Lalit Rai, the Assistant Professor in the department, for his encouragement and constructive dialogue. Also, my special thanks go to Prof. Pradeep Kumar Dimri, the Chairperson in the department, for his valuable advice and recommendations that significantly improve the thesis's clarity and soundness.

DECLARATION

I hereby declare that the thesis entitled **ANALYSIS AND DESIGN OF A MULTILEVEL SECURITY MECHANISM FOR DATA COMMUNICATION NETWORKS** by **SANGEETA DHALL**, being submitted in fulfillment of the requirements for the Degree of Doctor of Philosophy in **ELECTRONICS ENGINEERING** under Faculty of Engineering and Technology of J.C. Bose University of Science and Technology, YMCA, Faridabad, Haryana during the academic year 2022-23, is a bona fide record of my original work carried out under the guidance and supervision of **Dr. SHAILENDER GUPTA, ASSOCIATE PROFESSOR, DEPARTMENT OF ELECTRONICS ENGINEERING** and has not been presented elsewhere.

I further declare that the thesis does not contain any part of any work which has been submitted for the award of any degree either in this university or in any other university. .

(Sangeeta Dhall)

Registration No.: 17-YMCA-904010

CERTIFICATE

This is to certify that this Thesis entitled **ANALYSIS AND DESIGN OF A MULTILEVEL SECURITY MECHANISM FOR DATA COMMUNICATION NETWORKS** by **SANGEETA DHALL**, submitted in fulfillment of the requirement for the Degree of Doctor of Philosophy in **ELECTRONICS ENGINEERING** under Faculty of Engineering and Technology, J.C. Bose University of Science and Technology, YMCA, Faridabad, Haryana during the academic year 2022-23, is a bonafide record of work carried out under my guidance and supervision.

I further declare that to the best of my knowledge, the thesis does not contain any part of any work which has been submitted for the award of any degree either in this university or in any other university. .

Dr. Shailender Gupta
Associate Professor
Department of Electronics Engineering
Faculty of Engineering and Technology
J.C. Bose University of Science and Technology, YMCA
Faridabad, Haryana

Dated:

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to my Supervisor **Dr. Shailender Gupta** for giving me the opportunity to work in this area. It would never be possible for me to take this thesis to this level without his innovative ideas and his relentless support and encouragement.

I want to thank all the colleagues in the Department of Electronics Engineering at the University for their Endorsement during the course. My special gratitude to Prof. Pradeep Kumar Dimri, the Chairperson in the department, for his valuable recommendations that significantly helped me throughout my journey. I want to express my special thanks to Prof. Munish Vashishath, Prof. Neelam Turk, Mr. Bharat Bhushan, Ms. Archana Agarwal, and Ms. Archana Agarwal in the Department of Electronics Engineering for their encouragement and constructive dialogue.

(Sangeeta Dhall)

Registration No.: 17-YMCA-904010

ABSTRACT

With the increase in the number of internet users, intact communication of covert information is the vital requirement of all the applications like medical, defence, education, business transactions. For that matter need for a proficient security mechanism is apparent. Widely used techniques are cryptography and steganography. The primary goal of the former is to change data into some other form understandable only by the intended users, and in later mechanisms, data is hidden in a cover image for protection. However, these techniques alone has inadequacy; in cryptography, if the intruder has access to the cryptographic key, he can easily decrypt the message, as the algorithms are openly obtainable. In steganography, if the intruder suspects the existence of a message in a cover file, then additional analysis and application of the algorithm can result in the exposure of the secret data.

To enhance security, researchers focused their attention on using multiple levels of security mechanisms. Various researchers have tried several amalgamations of protection methods, but still, instances of online data breaches are increasing, thus demanding further improvements in existing mechanisms. In most multilevel approaches, the data is first encrypted and then embedded in a cover file. Even if the intruder suspects the message's existence in the cover file, a cryptographic key is still needed to decrypt the secret message. Along with these two techniques in secured schemes, the compression process also has a vital role. It increases the embedding capacity of data because confidential data is firstly compressed then followed by encoding and embedding. Any security mechanism for ensuring security in communication should meet the essential network security requirements and stipulations of the applications for which employed, and majorly these are classified as; confidentiality, authenticity, integrity, reproducibility, imperceptibility, and optimized implementation time. This research work is devoted to investigate superlative steganography and cryptography mechanisms so that multiple stages of protection can be incorporated to enhance the security of secret information. There is an extensive literature survey of these mechanisms; many spatial and frequency transform domains have been studied and implemented for steganography. Similarly, comprehensive studies and comparisons of traditional, Chaos based, and Quantum-chaos based algorithms as per the defined performance parameters are carried out in encryption mechanisms.

The main objectives of the work conducted in this research are the design, development, and testing of the proposed security mechanisms to provide optimum values of vital performance metrics. Before devising the security mechanism, existing multilevel schemes are studied and implemented to understand better the available combinations and gaps between the methods' required and actual performance. After

reviewing the literature two protection mechanisms are designed. Out of which, first, provides confidentiality, integrity, imperceptibility, reproducibility, and authenticity, specifically for medical applications. This proposal portrays a multi-layer, highly secured healthcare security model that will protect the patient's medical information; Electronic Patient Record (EPR) consists of text information of the patient and medical images like X-Rays, CT-scan, and MRI, etc. Firstly, in this plan, EPR is compressed using the Huffman compression algorithm to reduce its size for increasing embedding capacity and imperceptibility. This compressed EPR is encrypted using a cryptography scheme based on the Quantum logistic map to obtain encoded records. For authentication, the IRIS of the authorized person is captured and converted to a binary template. Hash algorithm (SHA-256) is used to calculate the hash value of this template, which is also embedded in cover medical image to maintain the system's integrity. The medical image to be secured is used as a cover image to hide this modified EPR and hash value of the biometric template, thus resulting in WaterMarked Medical Image (WMMI). This WMMI undergoes diverse stages for protection and is finally ready to move in an open network without giving even little indication to any unauthorized individual.

Another innovative approach involves designing, developing, implementing, and validating a multilevel security mechanism, focusing on confidentiality, imperceptibility, reproducibility, and execution speed. This proposal has incorporated Quantum based robust key scheduling algorithm, which generates keys for different stages of the given scheme like confusion, diffusion, and steganography. The key generation algorithm uses Quantum logistic maps for the generation of keys. This map has chosen because of its features of high randomness and sensitivity towards initial keys. Information to be secured is initially checked for its randomness or frequency for deciding on the inclusion of the compression stage in the protection system and then moves towards the next stage, bit-level confusion. This process is done using a random array generated with the help of a seed taken from randomly generated keys by the centralized algorithm. This confusing data is then diffused using a simple XOR operation of each bit with a separate key generated centrally. This highly random resultant information is then embedded into the cover image. The carrier image is processed by transforming it into the frequency domain for embedding. Lifting wavelet frequency transformation is chosen because of its simplicity and lossless recovery. The resultant secret data is stored in random locations of one of the bands of the LWT-transformed image. These random locations are also chosen from random keys generated centrally.

These proposals show optimized values for most parameters regarding confidentiality, the perceptibility of the stego image, randomness, speed of execution, and complete information recovery.

TABLE OF CONTENTS

CANDIDATE’S DECLARATION	i
CERTIFICATE	ii
ACKNOWLEDGEMENT	iii
ABSTRACT	iv
TABLE OF CONTENTS	vi
LIST OF TABLES	x
LIST OF FIGURES	xii
LIST OF ALGORITHMS	xv
LIST OF ABBREVIATIONS	xvi
1 INTRODUCTION	1
1.1 MOTIVATION AND RESEARCH PROBLEM	1
1.2 RESEARCH BACKGROUND	4
1.2.1 Single Level Security Mechanisms	5
1.2.2 Dual-Level Security Mechanisms	7
1.2.3 Multilevel Security Mechanisms	9
1.3 PROBLEM DEFINITION	11
1.4 OBJECTIVES	11
1.5 TOOL USED	12
1.6 PERFORMANCE METRICS	12
1.6.1 Parameters for Steganography/Invisible Watermarking Mechanisms	12
1.6.2 Parameters for Cryptography Mechanisms	15
1.7 SIMULATION SET-UP PARAMETERS	17
1.8 THE PROPOSED MECHANISMS	18

1.8.1	Proposal 1: Multilayered Highly Secure Authentic Watermarking Mechanism for Medical Applications	18
1.8.2	Proposal 2: Quantum based Robust and Swift Hybrid Security Mechanism	23
1.9	OUTCOMES	27
1.10	ORGANIZATION OF THE THESIS	30
2	LITERATURE SURVEY - SINGLE LEVEL SECURITY	31
2.1	STEGANOGRAPHY/INVISIBLE WATERMARKING MECHANISMS	31
2.1.1	Spatial Domain Steganography	32
2.1.2	Transform Domain Steganography	38
2.1.3	Comparison of Steganography Mechanisms	43
2.2	CRYPTOGRAPHY MECHANISMS	47
2.2.1	Traditional Encryption Mechanisms	48
2.2.2	Chaos Based Encryption Mechanism	55
2.2.3	Quantum Chaos Based Encryption Techniques	60
2.2.4	Comparison of Cryptography Mechanisms	64
3	LITERATURE SURVEY - MULTILEVEL SECURITY	69
3.1	DUAL-LEVEL SECURITY MECHANISMS	70
3.1.1	Image Security using Steganography and Cryptographic Techniques	71
3.1.2	An Adaptive Pseudorandom Stego-Crypto Technique for Data Communication	71
3.1.3	ROI Based Medical Image Watermarking with Zero Distortion and Enhanced Security	72
3.1.4	An Efficient Filtering based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography .	73
3.1.5	On the Implementation of a Secured Watermarking Mechanism based on Cryptography and Bit Pairs Matching	74
3.1.6	A Hybrid Security Mechanism based on DCT and Visual Cryptography for Data Communication Networks	75
3.1.7	A Secure Image Steganography using Advanced Encryption Standard and Discrete Cosine Transform	76
3.1.8	High Embedding Capacity Data Hiding Technique Based on EMSD and LSB Substitution Algorithms	76
3.1.9	A PVD based High Capacity Steganography Algorithm with Embedding in Non-sequential Position	78

3.1.10	Design of Hybrid Cryptography System based on Vigenère Cipher and Polybius Cipher	79
3.2	COMPARISON OF DUAL-LEVEL SECURITY MECHANISMS	80
3.3	MULTILEVEL SECURITY MECHANISMS	82
3.3.1	Hybrid Technique for Robust and Imperceptible Multiple Watermarking using Medical Images	83
3.3.2	Robust and Secure Multiple Watermarking for Medical Images	84
3.3.3	A Novel Hybrid Security Mechanism for Data Communication Networks	85
3.3.4	Secure Medical Data Transmission Model for IoT-Based Healthcare Systems	86
3.3.5	A Novel Visual Medical Image Encryption for Secure Transmission of Authenticated Watermarked Medical Images	87
3.3.6	Hybrid Cryptography and Steganography Method to Embed Encrypted Text Message within Image	88
3.3.7	Achieving Data Integrity and Confidentiality using Image Steganography and Hashing Techniques	88
3.3.8	An Efficient Algorithm for Confidentiality, Integrity and Authentication using Hybrid Cryptography and Steganography	89
3.3.9	A New Approach to Hiding Data in the Images using Steganography Techniques based on AES and RC5 Algorithm Cryptosystem	90
3.4	COMPARISON OF MULTILEVEL SECURITY MECHANISMS	91
4	MULTILAYERED SECURE MECHANISM	93
4.1	CONTRIBUTION	93
4.2	PROPOSED MECHANISM	94
4.2.1	Huffman Compression	96
4.2.2	Encryption	98
4.2.3	Biometric Recognition	100
4.2.4	Hashing Algorithm	103
4.2.5	Watermarking Mechanism	104
4.2.6	Scrambling	106
4.3	SIMULATION SET-UP PARAMETERS	108
4.4	RESULTS	108
4.4.1	Imperceptibility Analysis	108
4.4.2	Confidentiality Analysis	112
4.4.3	Authenticity Analysis	120
4.4.4	Integrity Analysis	122

4.4.5	Reproducibility or Data Extraction Analysis	122
4.5	CONCLUSION	124
5	QUANTUM BASED SECURITY MECHANISM	125
5.1	CONTRIBUTION	125
5.2	THE PROPOSED MODEL	126
5.2.1	Key Scheduling Algorithm	127
5.2.2	Conditional Compression	129
5.2.3	Bit-Level Confusion	130
5.2.4	Bit-Level Diffusion	131
5.2.5	Steganography Mechanism	132
5.3	SIMULATION SET-UP PARAMETERS	134
5.4	RESULTS	136
5.4.1	Imperceptibility Analysis	136
5.4.2	Confidentiality Analysis	138
5.4.3	Computational Time analysis	146
5.4.4	Reproducibility analysis	146
5.5	CONCLUSION	147
6	OVERALL CONCLUSION AND FUTURE SCOPE	149
6.1	OVERALL CONCLUSION	149
6.2	FUTURE SCOPE	151
	REFERENCES	152
	REFERENCES	153
	BRIEF PROFILE	163
	LIST OF PUBLICATIONS	165

LIST OF TABLES

1.1	Simulation Set-up Parameters	18
1.2	Comparison of Proposed Mechanism with References on Diverse Parameters of Steganography/Watermarking and Cryptography	20
1.3	Comparison of Proposed Mechanism with References for Authenticity, Integrity, Reproducibility and Computational Time	21
1.4	Comparison of Proposed Mechanism with References for Imperceptibility	22
1.5	Comparison of Proposed Mechanism with References on Diverse Parameters of Steganography/Watermarking and Cryptography	25
1.6	Comparison of Proposed Mechanism with References for Reproducibility and Computational Time	25
1.7	Comparison of Proposed Mechanism with References for Imperceptibility	26
2.1	Performance parameters taken for literature Survey of Steganography Techniques	44
2.2	Comparison of Spatial Domain Steganography Mechanisms	45
2.3	Comparison of Frequency Domain Steganography Mechanisms	46
2.4	Performance Parameters for Literature Survey of Cryptography Techniques	65
2.5	Comparison of Cryptography Mechanisms	66
3.1	Security Parameters used in Literature Survey	80
3.2	Literature Survey of Dual-level Security Mechanisms	81
3.3	Literature Survey of Multilevel Security Mechanisms	92
4.1	Compression Rate using Huffman Compression	97
4.2	Advantages of IRIS Recognition	101
4.3	Set-up Parameters	108
4.4	Results for Different Stages of Medical Images	109
4.5	Results for Different Stages of Reference Images	110
4.6	Recorded PSNR Values	112
4.7	Recorded MSE Values	113
4.8	Recorded Jaccard Index Values	114
4.9	Recorded UIQI Values	115

4.10	Recorded Correlation Coefficient Values	116
4.11	Recorded Bhattacharya Coefficient Values	117
4.12	Recorded Intersection Coefficient Values	118
4.13	Bit Error Rate for Minor Change in Key Input	119
4.14	Number of Pixel Change for One Pixel Change in Plain Text	119
4.15	Key-space for Encryption Techniques	119
4.16	Comparison of Proposed Mechanism with References on Diverse Parameters of Cryptography	120
4.17	Authenticity Mechanism Comparisons	121
4.18	Comparison of Proposed Mechanism with References for Authenticity .	121
4.19	BER for Retrieved EPR	123
4.20	BER for Retrieved Medical Image	123
5.1	Set-up Parameters	135
5.2	Images and References Taken for Comparative Analysis	135
5.3	Stego-images for Different Hybrid Mechanisms	137
5.4	Recorded PSNR and MSE Values	139
5.5	Recorded JI, BC, IC, UIQI and CC Values	143
5.6	BER for Encrypted Data	144
5.7	Bit Error Rate for Minor Change in Initial Conditions	145
5.8	Comparison of Proposed Mechanism with References on Diverse Parameters of Cryptography	145
5.9	BER for Recovered Data	147

LIST OF FIGURES

1.1	Annual Numbers of Data Compromises in US from 2015 to 2022	3
1.2	Cyber Security Incidents in India	3
1.3	Global Average Total Cost of Data Breach	3
1.4	Security Levels for Data Protection	4
1.5	Proposal 1: Multilayered Highly Secure Authentic Mechanism for Medical Applications	19
1.6	Proposal 2: Quantum based Robust and Swift Hybrid Security Mechanism	24
2.1	Steganography/ Invisible Watermarking mechanisms	32
2.2	Block Diagram for LSB Steganography	33
2.3	Block Diagram for Pseudorandom LSB Steganography	33
2.4	Block Diagram for Visual Cryptography Mechanism	34
2.5	Block Diagram for Distortion Steganography	35
2.6	Block Diagram for BPCS Steganography	36
2.7	Block Diagram for LSB based Steganography using Secret Key	37
2.8	Block Diagram for DCT Steganography	38
2.9	Block Diagram for DWT Steganography	39
2.10	Block Diagram for LWT Steganography	40
2.11	Block Diagram for DFT Steganography	41
2.12	Block Diagram for SWT Steganography	42
2.13	Block Diagram for FrFT Steganography	43
2.14	Cryptography Mechanisms	47
2.15	Block Diagram for AES Cryptography	48
2.16	Block Diagram for DES Cryptography	49
2.17	Block Diagram for TDES Cryptography	50
2.18	Block Diagram for Vigenère Cryptography	51
2.19	Block Diagram for RSA Cryptography	52
2.20	Block Diagram for RC4 Cryptography	53
2.21	Block Diagram for Hierarchical Visual Cryptography	54
2.22	Block Diagram for Chaos Encryption 1	55
2.23	Block Diagram for Chaos Encryption 2	57
2.24	Block Diagram for Chaos Encryption 3	57

2.25	Block Diagram for Chaos Encryption 4	58
2.26	Block Diagram for Chaos Encryption 5	59
2.27	Block Diagram for Quantum Chaos Encryption 1	61
2.28	Block Diagram for Quantum Chaos Encryption 2	62
2.29	Block Diagram for Quantum Chaos Encryption 3	62
2.30	Block Diagram for Quantum Chaos Encryption 4	63
2.31	Block Diagram for Quantum Chaos Encryption 5	64
3.1	General Structure of Dual-level Security Mechanism	69
3.2	Dual-level Security Mechanisms	70
3.3	Image Security using Steganography and Cryptographic Techniques . .	71
3.4	An Adaptive Pseudorandom Stego-Crypto Technique	72
3.5	ROI Based Medical Image Watermarking with Zero Distortion and Enhanced Security	73
3.6	An Efficient Filtering based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography	74
3.7	On the Implementation of a Secured Watermarking Mechanism based on Cryptography and Bit Pairs Matching	74
3.8	A Hybrid Security Mechanism based on DCT and Visual Cryptography	75
3.9	A Secure Image Steganography using Advanced Encryption Standard and Discrete Cosine Transform	76
3.10	High Embedding Capacity Data Hiding Technique Based on EMSD and LSB Substitution Algorithms	77
3.11	A PVD based High Capacity Steganography Algorithm with Embedding in Non-sequential Position	78
3.12	Design of Hybrid Cryptography System based on Vigenère Cipher and Polybius Cipher	79
3.13	Multilevel Security Mechanisms	82
3.14	Hybrid Technique for Robust and Imperceptible Multiple Watermarking using Medical Images	83
3.15	Robust and Secure Multiple Watermarking for Medical Images	84
3.16	A Novel Hybrid Security Mechanism for Data Communication Networks	85
3.17	Secure Medical Data Transmission Model for IoT-Based Healthcare Systems	86
3.18	A Novel Visual Medical Image Encryption for Secure Transmission of Authenticated Watermarked Medical Images	87
3.19	Hybrid Cryptography and Steganography Method to Embed Encrypted Text Message within Image	88

3.20	Achieving Data Integrity and Confidentiality using Image Steganography and Hashing Techniques	89
3.21	An Efficient Algorithm for Confidentiality, Integrity and Authentication using Hybrid Cryptography and Steganography	90
3.22	A New Approach to Hiding Data in the Images using Steganography Techniques based on AES and RC5 Algorithm Cryptosystem	91
4.1	Proposed Model for Sender Side	95
4.2	Proposed Model for Receiver Side	97
4.3	Advantages of Quantum Chaos Encryption mechanism	99
4.4	SHA-256 Algorithm	103
4.5	Advantages of Lifting Wavelet Transform Watermarking Mechanism	104
4.6	Filter Banks used in Wavelet Transform	105
4.7	Watermarking Scheme Embedding Customized EPR and Hash Code in Medical Image	106
4.8	Steganography Scheme Embedding Three Planes of Medical Image in Reference Image	106
4.9	Different Stages of Images in the Proposal	109
4.10	PSNR Comparisons	112
4.11	MSE Comparisons	113
4.12	Jaccard Similarity Index Comparison	114
4.13	UIQI Comparisons	115
4.14	Correlation Coefficient Comparisons	116
4.15	Bhattacharya Coefficient Comparisons	117
4.16	Intersection Coefficient Comparison	118
4.17	Testing of SHA-256	122
5.1	The Proposed Model for Sender Side	127
5.2	Centralized Key Generation	129
5.3	PSNR Comparisons	139
5.4	MSE Comparisons	140
5.5	Bhattacharya Coefficient Comparisons	140
5.6	Intersection Coefficient Comparisons	141
5.7	UIQI Comparisons	141
5.8	Correlation Coefficient Comparisons	142
5.9	Jaccard Index Comparisons	142
5.10	BER Comparison for Encryption	144
5.11	Computational Time Comparisons	146

LIST OF ALGORITHMS

1	Pseudocode for Huffman Compression	98
2	Pseudocode for Huffman Decompression	98
3	Pseudo-code for Quantum Chaos Encryption Mechanism	100
4	Pseudocode for Watermarking Mechanism	107
5	Key Scheduling Algorithm	128
6	Pseudocode for Compression	129
7	Pseudocode for Decompression	130
8	Pseudocode for Bit-Level Confusion	130
9	Pseudocode for Reverse Process of Confusion	131
10	Pseudocode for Bit-Level Diffusion	131
11	Pseudocode for Reverse Process of Diffusion	132
12	Pseudocode for Embedding Algorithm	133
13	Pseudocode for Retrieval Algorithm	134

LIST OF ABBREVIATIONS

Symbols	Meaning
AES	Advanced Encryption Standard
BC	Bhattacharya Coefficient
BER	Bit Error Rate
BPCS	Bit Plane Complexity Segmentation
CA	Coefficient Approximation
CC	Correlation Coefficient
CD	Coefficient Detailed
CH	Coefficient Horizontal
CV	Coefficient Vertical
DCT	Discrete Cosine Transform
DES	Data Encryption Standard
DFT	Discrete Fourier Transform
DWT	Discrete Wavelet Transform
EMSD	Enhanced Modified Signed Digit
EPR	Electronic Patient Record
FrFT	Fractional Fourier Transform
HH	High High
HieVC	Hierarchical Visual Cryptography
HL	High Low
IC	Intersection Coefficient
IWT	Integer Wavelet Transform
JI	Jaccard Index
KSA	Key Scheduling Algorithm
LH	Low High
LL	Low Low
LSB	Least Significant Bit
LWT	Lifting Wavelet Transform
LZW	Lempel Ziv Welch
MAC	Message Authentication Code
MD5	Message Digest 5

MSB	Most Significant Bit
MSE	Mean Square Error
NBC	Number of Bits Change
NPCR	Net Pixel Changes Rate
NROI	No Region Of Interest
PPN	Pixel Position Number
PSNR	Peak Signal to Noise Ratio
PVD	Pixel Value Difference
RC4	Rivest Cipher 4
RC5	Rivest Cipher 5
ROI	Region Of Interest
RONI	Region Of No Interest
RSA	Rivest, Shamir and Adelman
SHA	Secure Hash Algorithm
SVD	Singular Value Decomposition
SWT	Stationary Wavelet Transform
TDES	Triple Data Encryption Standard
UACI	Unified Average Changing Intensity
UIQI	Universal Image Quality Index
VC	Visual Cryptography

Chapter 1

INTRODUCTION

The advancements in technology are increasing at a swift pace. David House, an Intel colleague, had figured out that integrated circuits would double their performance every 18 months [1]. Thus, processing capabilities have greatly improved, which has changed users' lives and empowered hackers to use them for their benefit. The reports from Statistics [2] and business today [3] revealed this fact by illustrating that the number of cyber security attacks and data exposure has risen significantly in US and India, respectively. This research work is performed to explore the ways of inculcating security in information interchange. The step-by-step approach is employed to suggest the solution to this escalating problem, commencing with exploring the existing mechanisms by studying and implementing the literature under the research background. Then research gaps (problems) are identified amongst existing descriptions and necessary validations. Further, the research objectives are identified based on the recognized research problem and security requirements. These objectives include implanting confidentiality, integrity, authenticity, reproducibility, imperceptibility and optimum speed in security solutions.

This chapter briefly describes all the steps, and at the end, the organization of the rest of the thesis is presented.

1.1 MOTIVATION AND RESEARCH PROBLEM

In the current scenario, digitalization has become an inseparable part of everyone's life, resulting in a more handy system for online transactions and data sharing over the Internet. The development in digital communication technology and the escalation of computer power and storage has led to ease in data exchange and difficulties in ensuring individuals' privacy. The hike in electronic information usage has adversely resulted in the intimidation of thefts and content copyright. In the present cyber world, no sector is safe, as cybercriminals rely on sophisticated technologies; due to this, organizations

often experience misery, as their confidential data and significant assets fall prey to malicious attacks. The data-centric world in today's time emphasizes data security for the apparent objective of safeguarding valuable and confidential information in diverse sectors like medical, defence, education, business and many more.

According to reports by Health Insurance Portability and Accountability Act (HIPAA) journal [4], more than 40 million healthcare records have been exposed or disclosed without acquiescence in 12 months between July 2020 and June 2021. Also, an average of 3,343,448 healthcare records were infringed each month. As per reports by Diplomatist [5], the enormity of threats can be gauged in the defense sector, as the national cyber security budget has increased from Rs. 30,000 crores in 2013 to Rs. 80,000 crores in 2019-20. This is separate from what individuals and organizations spend on cyber security for their personal systems. According to the latest report by Kaspersky [6], the educational sector persists in drawing the attention of cybercriminals on the Internet. It is illustrated that 270,171 users came across diverse threats from July to December 2020. The reports demonstrated a 60 percent increase compared to the first half of last year. In the document published by Security Intelligence [7], it is stated that cyber-security is becoming more critical for businesses and agencies of every size, in nearly every industry, as in the year 2020, ransomware cases grew by 150 percent. A data breach caused rising costs in banking and finance. Statistica reveals this fact through a report on "data breaches recorded in the United States by the number of breaches and records exposed" [2] and "Incidents of cyber attacks in India from 2015 to 2022" [3].

Statistica is an advanced analytics software package initially developed by StatSoft, acquired by Dell in March 2014 [8]. Figure 1.1 presents the recorded number of data compromises in the United States between 2015 and 2022. Over 155.8 million individuals were affected by data exposures that indicate unintended disclosure of sensitive information due to inadequate information security. Figure 1.2 shows occurrences of cyber-attacks in India between 2015 and 2022. It is showing an escalation in the figures compared to the previous years. Also, the country was among the top five with the most cyber security incidents that year.

Additionally, India ranked third in terms of internet user numbers [3]. Figure 1.3 demonstrates the global average total cost of a data breach [9]. The consolidated average total cost in the 2022 study was 4.35 million dollars, a significant increase from 3.86 million dollars in 2020. All these figures are significantly high. To embark upon such a scenario, various network security mechanisms are needed. Therefore, researchers must search for innovative security mechanisms to protect users' data. One way of securing data is by using a standalone single-layer technique like steganography and cryptography. These mechanisms no doubt ensure the safety of data to a great extent, but with technology advancements [10], the security level must

be enhanced. These methods are used per network security requirements [11] and application areas for protection such as business, military/defense, education, or any other.

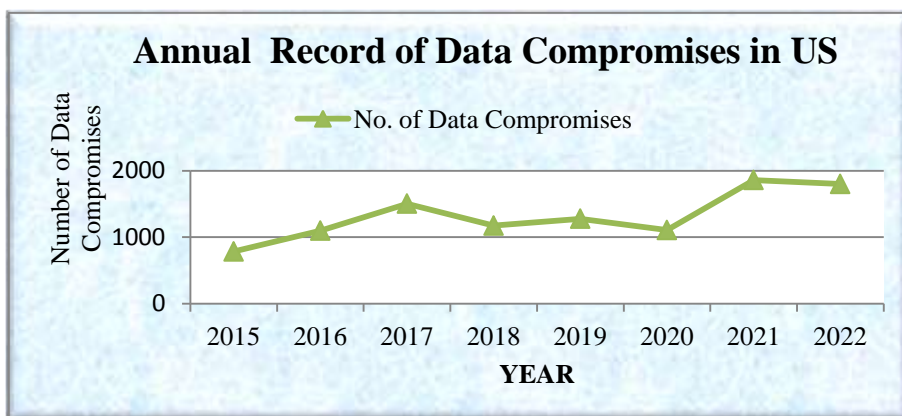


Figure 1.1: Annual Numbers of Data Compromises in US from 2015 to 2022

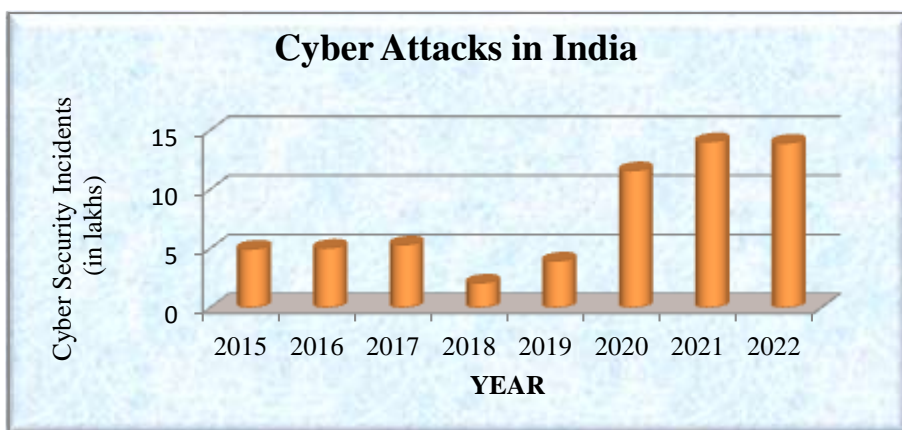


Figure 1.2: Cyber Security Incidents in India



Figure 1.3: Global Average Total Cost of Data Breach

Network security requirements include message confidentiality, which ensures

meaningful data communication between the intended sender and receiver, for all others, the message is meaningless. Message integrity ensures data reception at the receiver without any alteration, as the sender sent it. Message authentication ensures the identity of the sender to avoid data communication with pretenders. Message non-repudiation ensures that the transfer of data from the sender should not be denied, and entity authentication ensures the verification of the user before accessing the system resources. Furthermore, different application areas need diverse conditions like optimum imperceptibility of hidden protected data in the carrier in the case of steganography and watermarking or highly different encrypted output in cryptography for the safety of confidential information. Another is retrieving confidential information by the recipient using a suitable decryption mechanism in the case of cryptography or using an appropriate extraction algorithm for steganography or watermarking to get original data. Finally, the security mechanism should be implemented with the minimum possible computational time requirements.

The scope of this research work covers message confidentiality, integrity, authentication, imperceptibility, reproducibility and reasonable time requirements by identifying, designing, analysing and validating efficient security mechanisms. The upcoming section demonstrates the existing mechanisms for protection.

1.2 RESEARCH BACKGROUND

In order to secure data and other records, the most admired security solutions are cryptography, steganography and watermarking mechanisms.

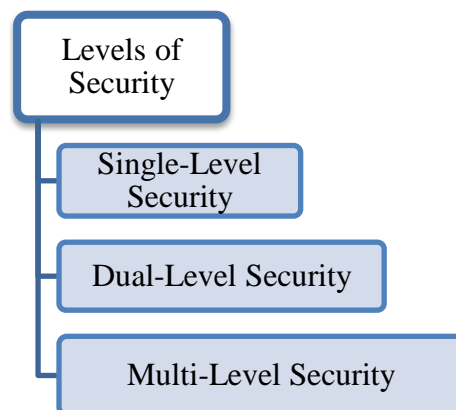


Figure 1.4: Security Levels for Data Protection

The cryptography deals with changing the appearance of information to conceal its identity and steganography masks the information by hiding it in certain carriers (image, audio, video, etc.). Watermarking also hides information (like a signature, hologram and text) in important documents or manuscripts for copyright protection.

The subsequent section enlists numerous algorithms for each mechanism available in the literature. Figure 1.4 shows the levels of security employed in literature for enhancing the overall protection of the system. Each of these categories is listed as follows.

1.2.1 Single Level Security Mechanisms

These techniques include steganography, watermarking, or cryptography used to protect secret information, i.e., text, image, or document.

(a) **Steganography Technique:** It is the art and science of hiding messages so that no one suspects their existence apart from the sender and intended recipient [12–19]. It involves altering the image so that only the purposeful entities can detect the message sent through it. It is about concealing the existence of messages. Steganography is typically invisible.

(b) **Watermarking Technique:** It refers to hiding the secret message (text, audio, image, logo, signature) in the document to provide authentication. It follows the methodology in which the information that verifies the owner is embedded into the signal [20–25]. This signal could be either video, image, or audio. It is about establishing the identity of information to prevent unauthorized use. Watermarking is of two types; visible and invisible.

Steganography and invisible watermarking employ similar implementation algorithms. These are broadly classified into two categories: Spatial domain and Frequency domain.

(i) **Spatial Domain:** In this category of algorithms, certain bits of the image pixels are modified or updated, in the spatial domain, for embedding the information without prior transformation. Many of these algorithms are listed here.

- Least Significant Bit (LSB) Substitution
- Pseudorandom LSB
- Bit Plane Complexity Segmentation (BPCS)
- Distortion Steganography
- Visual Cryptography (VC)
- Image Steganography using Secret Key

(ii) **Frequency Domain:** In the frequency or transform domain steganography mechanisms, the information is embedded in the image after transformation in the frequency domain. Many transformations can be used for the image before hiding the secret data; these are listed below.

- Discrete Cosine Transform (DCT)
- Discrete Wavelet Transform (DWT)
- Lifting Wavelet Transform (LWT)
- Stationary Wavelet Transform (SWT)
- Discrete Fourier Transform (DFT)
- Fractional Fourier Transform (FrFT)

The steganography and invisible watermarking methodology are identical, but the application areas are distinct. The former is used to protect confidential data by inserting them in one of the carriers, which may be an image, video, or audio and the latter is used to authenticate documents/manuscripts by inserting a watermark/signature into them. Consequently, both algorithms deal with inserting or hiding information into some cover (plain image or manuscript). Invisible watermarking is the same as steganography.

(c) **Cryptography Techniques:** It is another widely accepted security mechanism employed in data communication networks. It encodes secret information to move it safely to the communication channel. These mechanisms use various algorithms, broadly classified as Traditional [26–32], Chaotic [33–37] and Quantum Chaotic [38–42] maps-based algorithms, all are taken for study and implementation.

(i) **Traditional Encryption Techniques:** These long-established algorithms were fundamental, straightforward and comparatively less random and largely dependent on the substitution, shifting and round-based procedures. Many of these algorithms are listed here.

- Advanced Encryption Standard (AES)
- Data Encryption Standard (DES)
- Triple DES (TDES)
- Vigenère Cryptography
- Rivest, Shamir and Adelman (RSA)
- Rivest Cipher 4 (RC4)
- Hierarchical Visual Cryptography (Hie VC)

(ii) **Chaos Based Encryption Techniques:** Chaotic maps are extensively used in cryptography due to chaotic properties like ergodicity, mixing and sensitivity to initial conditions. The application of chaos in cryptography introduces confusion and diffusion properties in the cipher. Many such algorithms are listed below.

- A new image encryption scheme based on a chaotic function
- A novel image cipher based on mixed transformed logistic maps
- An efficient image encryption scheme based on a Peter De Jong chaotic map and a RC4 stream cipher
- An intertwining chaotic maps based image encryption scheme
- An innovative image encryption scheme based on chaotic map and Vigenère scheme

(iii) ***Quantum Chaos Based Encryption Techniques:*** Quantum chaos theory becomes a tool that can be used to improve the quality of pseudorandom number generators. The randomness and non-periodicity of the quantum-chaotic map are successfully verified by statistical complexity and the normalized Shannon entropy, thus used extensively in cryptography applications. Many Quantum chaos based algorithms are listed below.

- A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces
- An image encryption scheme based on quantum logistic map
- A novel color image encryption algorithm based on quantum chaos sequence
- Bit-level quantum color image encryption scheme with quantum cross-exchange operation and hyper-chaotic system
- Quantum image encryption using intra and inter bit permutation based on logistic map

The subsequent section introduces dual/twin-level security techniques.

1.2.2 Dual-Level Security Mechanisms

These techniques attempt to combine two different protection mechanisms or use identical techniques in cascading to enhance defense for secret information. The diverse dual/twin level protection mechanisms available in the literature are listed below.

- Image Security using Steganography and Cryptographic Techniques
- An Adaptive Pseudorandom Stego-Crypto Technique for Data Communication
- ROI Based Medical Image Watermarking with Zero Distortion and Enhanced Security
- An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography

- On the Implementation of a Secured Watermarking Mechanism based on Cryptography and Bit Pairs Matching
- A Hybrid Security Mechanism Based on DCT and Visual Cryptography for Data Communication Networks
- A Secure Image Steganography using Advanced Encryption Standard and Discrete Cosine Transform
- High Embedding Capacity Data Hiding Technique Based on EMSD and LSB Substitution Algorithms
- Design of Hybrid Cryptography System Based on Vigenère Cipher and Polybius Cipher
- A PVD Based High Capacity Steganography Algorithm with Embedding in Non-Sequential Position

Escalation in security threats is the motivation behind combining the above-said techniques, as standalone algorithms provide security up to a specific limit. As per existing amalgamation, increased layers of appropriately chosen security mechanisms ensure a highly protected system; this is the stimulus behind adding multiple layers to form a highly secure system, as demonstrated by various researchers [43–51].

The literature survey is done based on security parameters which are the essential network security requirements and stipulations of the applications for which they are employed and majorly these are classified as; confidentiality, authenticity, integrity, reproducibility, imperceptibility and optimized implementation time. A concise literature survey of dual-level security mechanisms is presented below.

- All of the studied mechanisms prioritize and guarantee the utmost level of confidentiality, as it stands as the core driving force behind these proposals. The primary focus is safeguarding sensitive information and ensuring it remains secure and protected at all times. By employing an encryption technique and another layer of security, these proposals create a solid foundation that upholds the highest standards of confidentiality.
- The available mechanisms cannot adequately address message integrity and authenticity requirements, which are fundamental to ensure information security. These mechanisms fall short of measuring or providing the necessary safeguards to guarantee the trustworthiness and validity of transmitted messages. These critical information security requirements demand more substantial and sophisticated measures to combat the increasingly complex and pervasive threats in today's digital landscape.

- Only a few mechanisms can effectively measure and ensure message reproducibility and image imperceptibility, which are crucial for maintaining information security. To address these challenges, researchers and practitioners must invest in innovative approaches that balance preserving the original message content and rendering images imperceptible to the human eye.
- In information security applications, the significance of time requirements cannot be overstated. However, it is imperative to note that only some existing mechanisms effectively measure or provide computational time comparisons. The absence of mechanisms capable of quantifying and comparing computational time impedes the evaluation and optimization of security systems and hinders the development of efficient solutions.

The subsequent section introduces multilevel security techniques.

1.2.3 Multilevel Security Mechanisms

To effectively safeguard against potential security breaches, it is recommended to implement multiple layers of security mechanisms. As an illustration, the first layer of protection on a computer system might be a password-based authentication system. However, if the password is discovered, this can be readily bypassed. Consequently, an extra layer of security, like two-factor authentication, can be introduced to increase protection. The diverse existing multilevel security mechanisms proposed by numerous authors are listed below.

- Hybrid Technique for Robust and Imperceptible Multiple Watermarking using Medical Images
- Robust and Secure Multiple Watermarking for Medical Images
- A Novel Hybrid Security Mechanism for Data Communication Networks
- Secure Medical Data Transmission Model for IoT-Based Healthcare Systems
- A Novel Visual Medical Image Encryption for Secure Transmission of Authenticated Watermarked Medical Images
- Hybrid Cryptography and Steganography Method to Embed Encrypted Text Message within Image
- Achieving Data Integrity and Confidentiality using Image Steganography and Hashing Techniques

- An Efficient Algorithm for Confidentiality, Integrity and Authentication using Hybrid Cryptography and Steganography
- A New Approach to Hiding Data in the Images using Steganography Techniques Based on AES and RC5 Algorithm Cryptosystem

These techniques attempt to join the multiple levels of different protection techniques to protect secret information. This offers potency to reduce the effects of threats. The existence of wide varieties of threats, intruders and attacks resulted in the evolution of numerous multilevel mechanisms so that different methods can be opted as per requirement, applications and environment of working [52–60].

A concise literature survey of multilevel security mechanisms is presented below.

- The studied mechanisms strongly emphasize prioritizing and ensuring the highest confidentiality level, which is the fundamental driving force behind these proposals. The primary objective revolves around safeguarding sensitive information, leaving no room for compromise regarding security and protection.
- The comprehensive mechanisms explored in this study surpass dual-level mechanisms in effectively addressing crucial requirements such as message integrity, reproducibility and authenticity. These requirements serve as the bedrock for establishing a resilient information security framework.
- In the field of information security applications, the importance of time requirements must be emphasized more. However, it is crucial to acknowledge that only a few studied mechanisms accurately measure or offer computational time comparisons. The lack of mechanisms capable of quantifying and comparing computational time hampers the evaluation and optimization of security systems, impeding the development of efficient solutions.

There needs to be more than the standalone technique, steganography, watermarking or cryptography, as the attacks have grown more sophisticated and occurrences of online data threats are escalating. Therefore, researchers have tried to combine multiple security layers to provide better security. As seen from the concise literature survey of dual and multilevel security mechanisms, ample schemes are designed to protect secret information (text/image) completely. However, not even a single mechanism is proficient enough to optimize or evaluate all the objectives. This gap between requirement and availability motivates new designs of such protection mechanisms to optimize the defined goals. As per the severity of security need, researchers had put in lots of effort to propose numerous combinations of different security mechanisms to form a scheme that can save fragile information in diverse application areas like medical, education, defense, business and many more, so that all sectors can flourish.

1.3 PROBLEM DEFINITION

Intact communication of covert information is the key requirement of all the applications like medical, military, education and business transactions. For that matter, the need for a proficient security mechanism is apparent. According to the security needs in diverse fields [10, 11, 55], it is observed that confidentiality, imperceptibility, reproducibility (data extraction), authenticity, integrity, with minimum computational time are the foremost objectives. As per the literature studied in this work, no such mechanism is available which can primarily optimize these requisites. In order to fulfil most of the requirements, the following problems are identified for the research work:

- The inadequacy of an efficient cryptography algorithm to optimize the vital performance metrics like key-space, execution time, entropy, correlation coefficient and key sensitivity for providing confidentiality to the protection mechanism.
- The scarcity of the proficient invisible watermarking or steganography algorithm for confidential data or watermark to optimize numerous parameters like confidentiality, reproducibility, execution speed and imperceptibility.
- Insufficiency of competent multilevel security mechanisms to optimize the required goals of confidentiality, authentication, imperceptibility, reproducibility, integrity and high computational speed for the diverse applications

The motivation behind this work is to accomplish all the goals, which are described in the next section.

1.4 OBJECTIVES

In order to address all the impediments listed in the problem definition, following objectives are devised for this research work:

1. To study and implement diverse compression, encryption, steganography and watermarking mechanisms available in literature.
2. To identify efficient compression algorithm for the secret data or watermark to be embedded.
3. To design and implement efficient cryptography algorithm which has optimum values of brute force search, execution time, key-space, correlation coefficient, entropy and key sensitivity.

4. To design and implement efficient watermarking or steganography algorithm for secret data or watermark with optimum values of robustness and security parameters
5. To propose/ develop an efficient multilevel security mechanism considering the dynamic nature of today's computer network environment incorporating trade-off among assorted mechanisms.

All implementations, analysis and validation are done through the software simulation tool provided in the next section.

1.5 TOOL USED

For the implementation of all the mechanisms, MATLAB IDE- R2014a is used because of its various advantages, some of which are listed below:

- It is an interpreted language for mathematical computations. It supports carrying out numerical calculations and envisages the outcomes with high precision.
 - This software tool aids in data analysis, algorithm development and conveniently creating models and applications.
 - The built-in diverse functions enable programmers to investigate several approaches and accomplish solutions swiftly compared to spreadsheets or traditional programming languages.
 - Its environment permits to handle data interactively, facilitating the tracking of files and variables and simplifying familiar programming/debugging tasks.
- In order to analyze and validate numerous mechanisms, some measurement parameters are needed. A distinct set of such metrics is defined for diverse algorithms in a subsequent section.

1.6 PERFORMANCE METRICS

The performance and strength of various techniques is evaluated based on various performance metrics and criterion's which are defined as follows [10,61]:

1.6.1 Parameters for Steganography/Invisible Watermarking Mechanisms

The required metrics are described below.

- **The confidentiality** of the mechanisms can be evaluated by investigating image quality before and after embedding. It can be done using numerous metrics categorized into robustness and security analysis; all are described below. The robustness of a steganography technique can be measured by calculating the PSNR and MSE of the stego image relative to the original image. The security analysis compares the pixel values, probability distribution and histograms between the cover and stego images. An assortment of parameters measures the similarity or dissimilarity between both images. These are described below:

- **Peak Signal to Noise Ratio (PSNR):** This parameter is used to compare each pixel of the image before and after embedding. The higher value of PSNR means the low error thus ensure the high confidentiality of stored information. It can be calculated as under.

$$PSNR = 10 \times \log_{10} \left(\frac{\max^2}{MSE} \right) \quad (1.1)$$

Where, \max represents the maximum value of the pixel of the image, MSE is Mean Squared Error.

- **Mean Squared Error (MSE):** It stands for cumulative squared error between the two images (before and after embedding). The lower value of MSE means lower error. It can be calculated as under.

$$MSE = \frac{1}{m \times n} \sum_{k=1}^m \sum_{j=1}^n [(B(k, j) - A(k, j))]^2 \quad (1.2)$$

Where, B and A represent images before and after embedding respectively, m and n give row and column size of the image.

- **Jaccard similarity Index (JI):** The Jaccard similarity index or Jaccard similarity coefficient compares elements of two sets to spot shared and distinct components. It's a measure of similarity for the two sets of data, with a range from 0 to 1. A higher value signifies more similar populations. It can be calculated as follows:

$$JI(B, A) = \frac{|A \cap B|}{|A \cup B|} \quad (1.3)$$

Where, B and A represent images before and after embedding respectively, $|A \cap B|$ indicates the value in both images, $|A \cup B|$ tells the quantity in either image.

- **Universal Image Quality Index (UIQI):** It is a measure of image

deformation with respect to the Human Visual System (HVS). As in an image, pixel values existing at diverse locations show the different impact on HVS. If some deformation is initiated in the image, such alterations are calculated as a combination of three factors; Loss of Correlation (LC), Contrast Distortion (CD) and Luminance Distortion (LD).

$$LC(B,A) = \frac{2 \times SD_{AB}}{SD_A + SD_B} \quad (1.4)$$

$$CD(B,A) = \frac{2 \times SD_A \times SD_B}{SD_A^2 + SD_B^2} \quad (1.5)$$

$$LD(B,A) = \frac{2 \times M_A \times M_B}{M_A^2 + M_B^2} \quad (1.6)$$

$$UIQI(B,A) = LC(B,A) \times CD(B,A) \times LD(B,A) \quad (1.7)$$

Where, B and A represent images before and after embedding respectively, M and SD are mean and standard deviation respectively of images (A and B),

SD_{AB} is covariance between A and B .

- **Correlation Coefficient (CC):** This parameter is a measure of the linear correlation between two images A and B . Its range is between -1 to $+1$ both inclusive, where 1 signifies perfect match and -1 signifies inversion of image. The correlation coefficient can be calculated as:

$$CC(B,A) = \frac{SD_{AB}}{SD_A \times SD_B} \quad (1.8)$$

Where, B and A represent images before and after embedding respectively, SD_{AB} is the covariance between A and B ,
 SD is a standard deviation (for images A and B).

- **Bhattacharya Coefficient (BC):** This parameter gives an estimated measure of the count of overlapping between two arithmetical samples which are two images (before and after embedding). It measures the relative closeness between these images. Bhattacharyya Coefficient can be

calculated as follows

$$BC(B,A) = \sum_{i=1}^N \sqrt{B1(i) \times A1(i)} \quad (1.9)$$

Where, B and A represent images before and after embedding respectively, $B1$ and $A1$ are probability distributions of these two images respectively. N is total number of elements in an image.

- **Intersection Coefficient (IC):** This parameter provides a count of the same value of pixels between two histograms. If the probability distribution of two images is taken as $B1$ and $A1$ respectively, then Intersection coefficient is given by

$$IC(B,A) = \sum_{i=1}^N \min[B1(i), A1(i)] \quad (1.10)$$

Where, B and A represent images before and after embedding respectively, N is total number of elements in an image.

The range of values for this coefficient is between 0 to 1. Where 0 represents complete mismatch and 1 represents exactly match.

- **Imperceptibility** for a technique can be gauged by visual inspection of snapshots recorded before and after embedding of secret information in the image. It is also termed as qualitative analysis of the results.
- **Reproducibility or data extraction** is verified by calculating the Bit Error Rate (BER) between the original message at the sender side and the retrieved message at the receiver end. The low value of BER is desirable; ideally, it should be 0.
- **Computational time** gives the measure of the time duration required to accomplish the process. It is defined as the total processing time on the receiver or receiver and transmitter sides. The computational time relies on variables like the system configuration, information size and the image type/size used.

1.6.2 Parameters for Cryptography Mechanisms

To analyze these mechanisms, various metrics are used, which are described below:

- **The confidentiality** of the cryptography mechanism can be judged by analysing key-size and randomness introduced by the algorithm. The Key-space analysis is

done by gauging key-size and entropy is the measure of randomness. Both are illustrated below.

- **Key-Space Analysis:** It defines the range of combinations for the key. With the increase in key-size, the complexity of the cryptanalyst will increase for its identification. Key-size is one of the important parameters used to test a cryptography mechanism, as it is the only secret factor to be kept safe.
- **Information Entropy Analysis:** It defines the randomness in the encrypted image. Entropy is calculated between encrypted and original image.

$$Entropy = \sum_{k=1}^m \sum_{j=1}^n P(i, j) \times \log_2 \left[\frac{1}{P(i, j)} \right] \quad (1.11)$$

Where $P(i,j)$ is the probability of each pixel in an image.

m and n are the row and column of an image.

If image is completely randomised then the maximum value of entropy is equal to 8.

- **Differential Attack Analysis:** This attack is performed to find out the secret key or original image by comparing the variations in the input with deviations in the encrypted output. It measures the sensitivity of the algorithm under test. High sensitivity to small changes in the plain image provides excellent resistance to differential attacks. NPCR and UACI are its measures.

- **Number of Pixel Changes Rate (NPCR):** It implies the rate of alteration in number of pixels of the encoded image when the original and pixel altered plain-images are compared. The encryption procedure should be sensitive in relation to keys and original images. The slight change in key and original image should result into completely different encrypted image. Let $C1$ and $C2$ be the encoded images for the first and pixel changed plain image. NPCR is given as:

$$NPCR = \frac{\sum_{i=1}^m \sum_{j=1}^n D(i, j)}{m \times n} \times 100\% \quad (1.12)$$

Where, m and n are the row and column of the images.

D is defined as:

$$D(i, j) = \begin{cases} 0 & \text{for } C1(i, j) = C2(i, j), \\ 1 & \text{for } C1(i, j) \neq C2(i, j) \end{cases} \quad (1.13)$$

- **Unified Average Changing Intensity (UACI):** It is the difference in

average intensity between the plain and encrypted image. Let $C1$ and $C2$ be the encoded images for the first and pixel changed plain image. UACI is given as:

$$UACI = \frac{1}{m \times n} \left[\sum_{i=1}^m \sum_{j=1}^n \frac{|C1(i, j) - C2(i, j)|}{2^L - 1} \right] \times 100\% \quad (1.14)$$

Where, L is the number of the bits representing respective red, green and blue channels,

m and n are the row and column of the images.

Optimize values of NPCR and UACI shows sensitivity to small changes in plain image and excellent resistance towards differential attack and provide a mechanism with high confidentiality.

- **Computational time** is defined as the total processing time on the receiver or receiver and transmitter sides. It depends on memory size, CPU structure, Operating system and many more.
- **Imperceptibility** is judged by the quantitative and qualitative analysis of results. The resultant image/data should be dissimilar from the original one. Quantitatively the PSNR and MSE can be used to investigate this diversion. The low value of PSNR is desirable in the case of the encryption mechanism but undesirable for the steganography mechanism. The comparison of snapshots of original and encrypted information provides qualitative analysis.
- **Reproducibility or data extraction** is verified by calculating the Bit Error Rate (BER) between the data/ image before and after encryption. The high value of BER is desirable; the encrypted and original information should be entirely dissimilar.

1.7 SIMULATION SET-UP PARAMETERS

The Set-up parameters used for recording results for existing mechanisms as well as proposed mechanisms are shown in Table 1.1. This table provides information regarding the dataset used for experimentation purposes, which includes the size and type of images. Different sizes of confidential data used for hiding are also mentioned. Also, the configuration of hardware and software systems used for experimentation is

described in the table. The software tool used for implementation is also mentioned. The numerous techniques in the literature are implemented using these specifications and the defined tool.

Table 1.1: Simulation Set-up Parameters

Parameters	Values
Sizes of Cover Image	128x128x3, 192x192x3, 256x256x3, 512x512x3 (Set of sample images of each size are taken for results)
Image Category	Coloured and Greyscale Images (jpg Format)
Secret Data (in bytes)	10, 25, 80, 150, 300 and 500 bytes
Programming Tool version	MATLAB
Processor	1.90Ghz, Intel (R) Core (TM i3-3227U)
Memory	4GB RAM

The following section provides all the proposed mechanisms, which are the primary outcomes concerning the defined objectives of the research work.

1.8 THE PROPOSED MECHANISMS

The utmost objectives of the work conducted in this research are the design, development and validation of the performance of proposed security mechanisms to provide optimum values of vital performance metrics. After reviewing the literature on existing multilevel techniques, two protection mechanisms are designed, as described below.

1.8.1 Proposal 1: Multilayered Highly Secure Authentic Watermarking Mechanism for Medical Applications

This proposal portrays a multi-layer, highly secured healthcare security model that protects the patient's medical information; Electronic Patient Record (EPR) consists of text information of the patient and medical images like X-Rays, CT-scan, MRI, etc. Figure 1.5 shows the design, which consists of multiple stages.

In the first step, data to be secured, EPR is compressed using the Huffman compression algorithm to reduce its size for minimizing locations to be modified and improve imperceptibility. This compressed EPR is then encrypted using a cryptography scheme based on a Quantum logistic map to obtain encoded records. For authentication, the IRIS of the authorized person (Doctor) is captured and converted to a binary template. The hash algorithm, Secure Hash Algorithm-256 (SHA-256), is used to calculate the hash value of this template, which is also embedded in the cover

medical image to maintain the system's integrity. The medical image to be secured is used as a envelop for hiding this modified EPR and hash value of the biometric template. All planes (R, G, B) of the cover image are separated and then Lifting Wavelet Transform (LWT) is applied on each plane for transforming into different frequency bands (Low Low, High Low, Low High, High High). As per the size of information, either two or more bands can be utilized to store customized records and hash values, resulting in WaterMarked Medical Image (WMMI). This WMMI is separated into three color planes and then each plane is scrambled using Arnold transformation, a permutation algorithm. Then, each shuffled plane is compressed using a lossless Huffman compression algorithm to decrease the number of locations to be modified for enhancing imperceptibility. All compressed planes are partitioned into two shares before embedding into a reference image. The reference image is used for hiding modified WMMI.

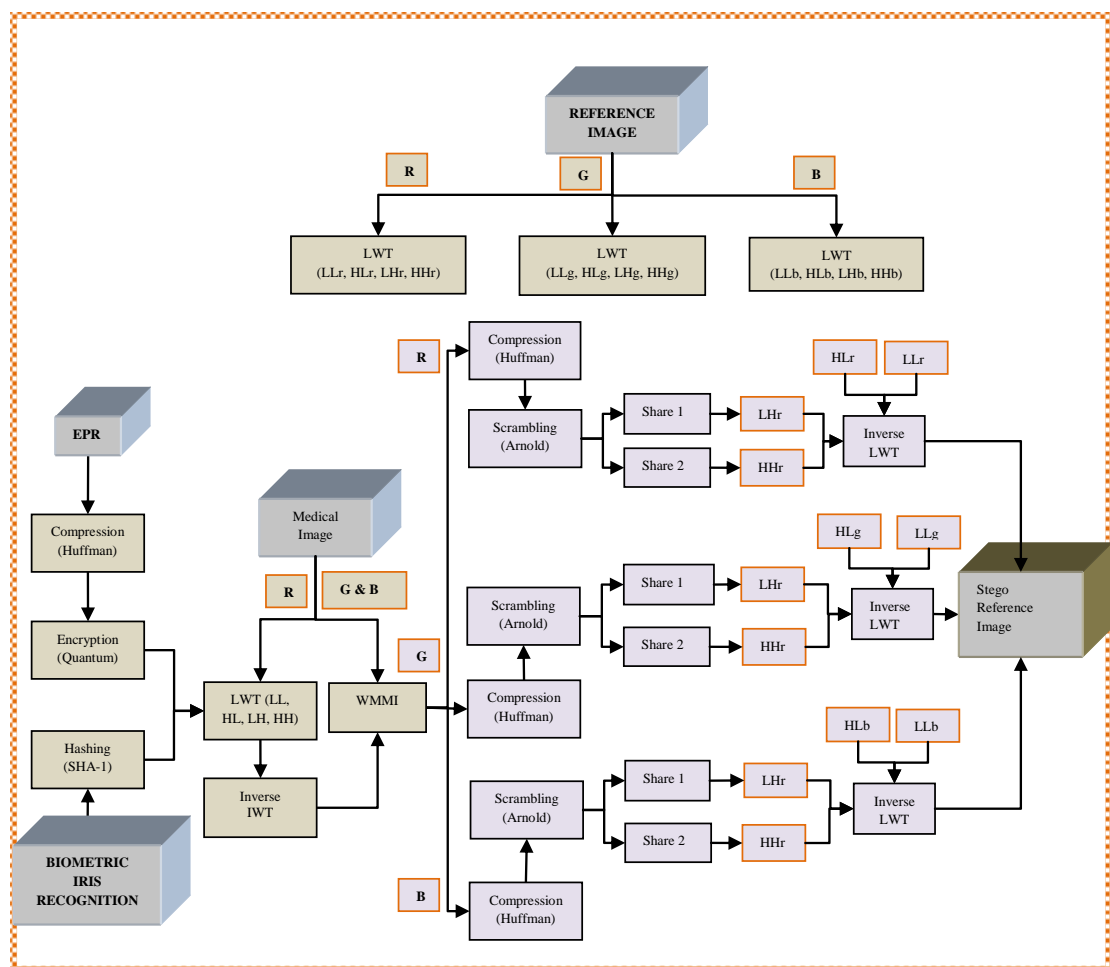


Figure 1.5: Proposal 1: Multilayered Highly Secure Authentic Mechanism for Medical Applications

This cover image is prepared firstly by partitioning into different color planes and then transforming each plane into a frequency domain to form diverse frequency bands

using the LWT steganography algorithm. All the resultant shares of WMMI are embedded into selected frequency bands (HH and LH) to sustain the perceptibility of the reference image. Embedding is followed by inverse LWT and grouping of all color planes, which results in a stego-reference image.

The receiver side consists of all stages in reverse order to get back the EPR for the intended recipient.

Results:

The proposed mechanism is motivated by the medical application described in [55], so all the results are compared with the method proposed by [55] (Ref2) and another medical application based work [54] (Ref1).

Table 1.2: Comparison of Proposed Mechanism with References on Diverse Parameters of Steganography/Watermarking and Cryptography

CONFIDENTIALITY			
Comparison of diverse steganography parameters (REFERENCE and STEGO REFERENCE IMAGE)			
PARAMETERS	Ref1 [54]	Ref2 [55]	PROPOSED
PSNR	29.2536	31.6149	37.3033
MSE	77.2178	44.8317	12.0989
JI	0.9747	0.9997	0.9947
UIQI	0.9938	0.9970	0.9998
CC	0.9877	0.9940	0.9997
BC	0.9974	0.9986	0.9998
IC	0.9462	0.9668	0.9875
Comparison of diverse steganography parameters (MEDICAL and RECONSTRUCTED MEDICAL IMAGE)			
PSNR	29.2536	39.4489	52.8208
MSE	77.2178	7.3822	0.3396
JI	0.9747	0.9959	0.9924
UIQI	0.9938	0.9964	0.9990
CC	0.9877	0.9929	0.9980
BC	0.9974	0.9991	0.9985
IC	0.9462	0.9759	0.9617
Comparison of diverse cryptography parameters(Medical Records)			
MECHANISM USED	AES (For odd positions) RSA (For even positions)	IWT and equation based encryption	Quantum logistic map based mechanism
KEY-SIZE	128 Bits for odd, 1024 for even	37^n (n-levels of decompositions)	448 Bits
KEY-SPACE	$2^{128}, 2^{1024}$	37^n	2^{448}

- **Confidentiality Analysis:** For checking confidentiality of records image quality is examined before and after embedding. The excellence of a technique is judged by comparing the pixel values, probability distribution and histograms between the medical image and WMMI, also among reference image and stego-reference

image. In brief, different parameters of steganography/ watermarking and cryptography algorithms used in the multilevel mechanisms are compared. Table 1.2 provides comparison of proposed mechanism with references on diverse parameters of steganography/watermarking and cryptography.

- **Authenticity Analysis:** For incorporating authenticity, the validation of the biometric identification process is employed. The IRIS detection as a biometric solution has many advantages over other biometric solutions [62]; that is why it is preferred in the current mechanism. Table 1.3 compares the authenticity method incorporated by different protection schemes.





Table 1.3: Comparison of Proposed Mechanism with References for Authenticity, Integrity, Reproducibility and Computational Time

TECHNIQUE IMPLEMENTED	AUTHENTICITY	INTEGRITY	REPRODUCIBILITY	COMPUTATIONAL TIME
	Mechanism used	Mechanism used	BER (Original and Retrieved Records)	Time for Execution (Seconds)
Ref1 [54]	No mechanism	No mechanism	0	5.87 seconds
Ref2 [55]	Finger print (biometric)	No mechanism	0	3.15 seconds
Proposed Mechanism	IRIS detection (biometric)	Hash function (SHA-256)	0	102.5 seconds

- **Integrity Analysis:** To ensure the reception of unaltered data or maintain the information's integrity, one of the best ways is to send a hash code along with the primary information. SHA-256 is employed in the proposed mechanism, which generates a hash code of 256 bits. It alters 50 percent bits for a single bit change in input data. Table 1.3 compares the method of integrity incorporated by different protection schemes.
- **Reproducibility or Data Extraction Analysis:** Another critical parameter to gauge a security mechanism is its capability for data extraction, i.e., the records which were modified and hidden in some carriers should be reproduced in original form for their usage. The BER is measured for retrieved information for analyzing this factor. As seen from the Table 1.3, all the mechanisms provide perfect reproducibility of records.
- **Computational Time Analysis:** The time requirements for implementing different algorithms are given in the table. As seen from the Table 1.3, the inclusion of multiple layers of security results in higher time requirements for the proposed mechanism than the existing methods.
- **Imperceptibility Analysis:** It is gauged by visual inspection of snapshots recorded before and after embedding secret information in the image, giving a

qualitative analysis of the results. Table 1.4 shows the stego-image snapshots for all the mechanisms. As seen from the results, the imperceptibility of all the algorithms is admirable.

Table 1.4: Comparison of Proposed Mechanism with References for Imperceptibility

IMPERCEPTIBILITY			
Original Image	Ref1 [54]	Ref2 [55]	Proposed Mechanism
			

Tables 1.2 to 1.4 illustrate the comparison of the proposal with two reference mechanisms. Almost every outcome of comparison shows that most of the parameters of the proposed mechanism have optimized values in contrast to formally accepted techniques available in the literature; this is due to the fact of employing Lifting Wavelet Transform (LWT) steganography and the choice of appropriate frequency bands for the embedding of information. Before embedding, the amendment of records (EPR and Medical Image) grants add-on protection. However, the inclusion of multiple layers of security results in higher time requirements than existing mechanisms. So, optimization of execution time is the area to be worked upon for striving towards perfection. A new proposal is demonstrated in the next section in consideration of this area.

Conclusion:

With the increased medical data transversal over insecure networks and other interconnected networks, demand for security of such crucial data has also raised manifold. The proposed mechanism illustrates a multi-layer security architecture that is used to protect the medical images along with patient information. This mechanism provides the following desirable security characteristics:

- **Confidentiality** of electronic patient records is achieved by employing compression, encryption followed by hiding in the medical cover image and for WMMI security layers used are scrambling, compression and then residing into LWT transformed planes of the reference image.
- **Imperceptibility** of hidden information (medical image and EPR) is attained by choosing suitable frequency bands in lifting wavelet transformed medical image and reference image.

- **Biometric authentication** is accomplished by capturing IRIS pattern at both ends (sender and receiver) and then providing access to secret information after comparing and verifying.
- **Integrity** is achieved by generating hash code for the captured IRIS template and its comparison with respective code on the receiver side for granting access to records.
- Perfect **reproducibility** of records is attained by hiding information in such locations from where it can be retrieved without any loss. This is verified by extracting EPR with zero bit error and medical images with acceptable bit changes.
- For the resultant stego reference image, it is tough to distinguish it from its original version resulting in a **visually meaningful encrypted image**.

Compared to the existing security techniques, the proposed method provides high protection by getting the higher values of diverse security and other parameters. The following section demonstrates the second proposed mechanism.

1.8.2 Proposal 2: Quantum based Robust and Swift Hybrid Security Mechanism

This multilevel secure, robust and fast, authentic mechanism is proposed to secure secret records and to fulfil the protection issues in diverse applications. Figure 1.6 shows the projected mechanism 2. In this proposal a multilayered design containing Quantum-based confusion and diffusion processes followed by Lifting Wavelet Transform (LWT) steganography mechanism is projected. Moreover, a provisional compression mechanism is also employed. Secret data is initially checked for the frequency of characters, which is the decisive factor for the inclusion of compression operation. After decision-making, either compressed or unchanged data undergoes a bit-level confusion stage with the help of a random key generated by a Quantum-based key scheduling algorithm. The subsequent process is diffusion in which each perplexed bit undergoes XOR operation with random keys generated by a centralized key generation mechanism. Finally, this data is embedded into lifting wavelet transformed cover image. The mingled data bits are stored at random locations of carrier image, which is then ready to commune in insecure site.

The hallmarks of the given mechanism are Centralized Key Scheduling Algorithm, Conditional Compression, Bit-Level Confusion, Bit-Level Diffusion and Frequency Domain Lifting Wavelet Transform Steganography. The heart of the mechanism is key scheduling algorithms, from which three keys are used for all three processes. As a

seed for random number generation in the confusion process. The data size keys for the diffusion and steganography processes.

The usage of simple and effective stages is providing remarkable time efficiency, imperceptibility and power of confidentiality in an extremely effectual way in comparison to available mechanisms.

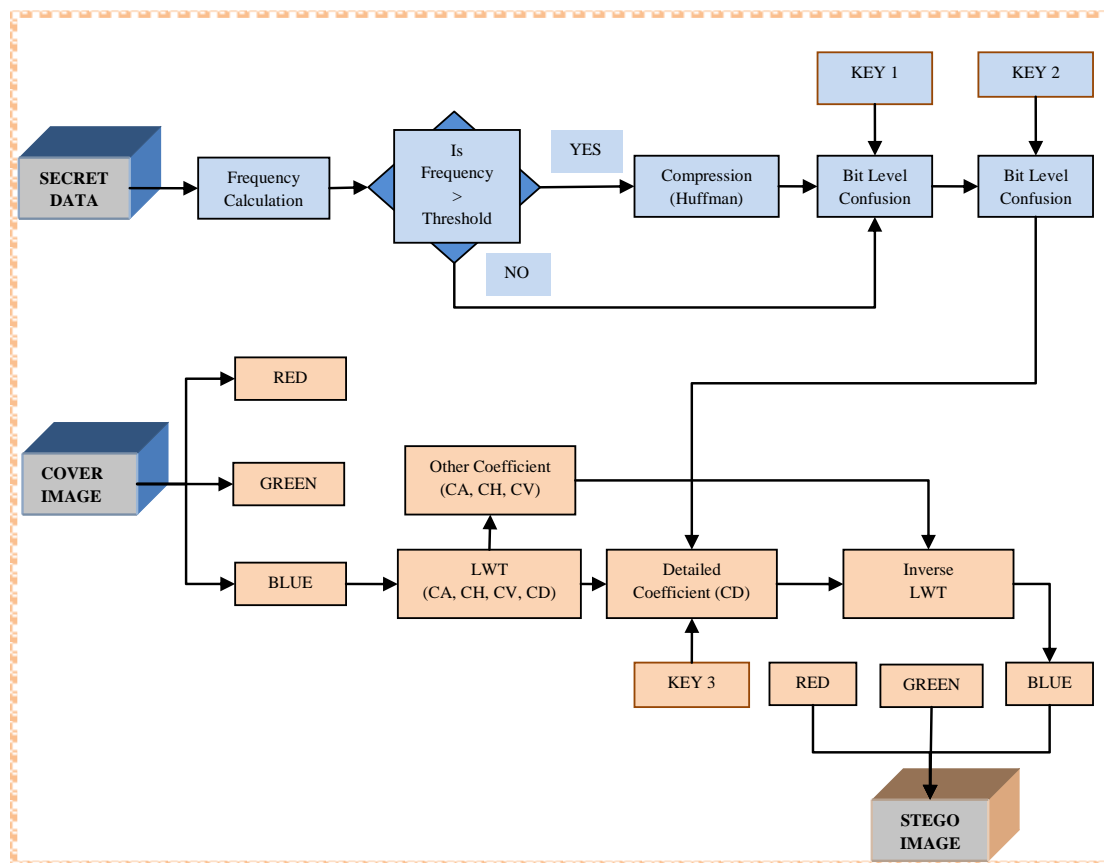


Figure 1.6: Proposal 2: Quantum based Robust and Swift Hybrid Security Mechanism

Results:

All the results of proposed mechanism are compared with the method recommended by [63] as (Ref1), [64] as (Ref2) and [48] as (Ref3).

- **Confidentiality Analysis:** Image quality is examined before and after embedding to check the confidentiality of records. The excellence of a technique is judged by comparing the pixel values, probability distribution and histograms between the original image and the stego-image for assessment of steganography. The comparison is based on key-size and space for the evaluation of cryptography mechanisms. In brief, different parameters of steganography and cryptography algorithms used in the multilevel schemes are compared in Table 1.5.
- **Reproducibility or Data Extraction Analysis:** Another critical parameter to gauge a security mechanism is its capability for data extraction, i.e., the records

which were modified and hidden in some carriers should be reproduced in original form for their usage. The Bit Error Rate is (BER) measured for retrieved information for analyzing this factor. As seen from the Table 1.6, all the mechanisms provide perfect reproducibility of records.

Table 1.5: Comparison of Proposed Mechanism with References on Diverse Parameters of Steganography/Watermarking and Cryptography

CONFIDENTIALITY				
Comparison of diverse steganography parameters (COVER and STEGO IMAGE)				
PARAMETERS	PROPOSED MECHANISM	Ref1 [63]	Ref2 [64]	Ref3 [48]
PSNR	72.98000	47.22000	62.77000	22.39000
MSE	0.018100	1.252000	0.035200	377.1000
JI	0.999927	0.999825	0.999964	0.971388
UIQI	0.999996	0.999695	0.999994	0.923630
CC	0.999992	0.999410	0.999989	0.861999
BC	0.999988	0.993210	0.999985	0.983279
IC	0.997705	0.938950	0.996516	0.933170
Comparison of diverse cryptography parameters				
MECHANISM USED / PARAMETERS	Quantum logistic map based mechanism	Symmetric Key Cryptography	Hierarchical Visual Cryptography	AES
KEY-SIZE	448 Bits	4 digits	Data length L	128 Bits
KEY-SPACE	2^{448}	2^{32}	2^L	2^{128}

Table 1.6: Comparison of Proposed Mechanism with References for Reproducibility and Computational Time



TECHNIQUE IMPLEMENTED	REPRODUCIBILITY	COMPUTATIONAL TIME
	BER (Original and Retrieved Records)	Time for Execution (Seconds)
Ref1 [63]	0	23.43
Ref2 [64]	0	6.19
Ref3 [48]	0	132.56
PROPOSED MECHANISM	0	4.54

- **Computational Time Analysis:** The time requirements for implementing different algorithms are given in the table below. In many data communication and security applications, time restriction is very prominent, requiring prompt data for further action. For reducing the time of execution, straightforward and effective processes are used and even one stage is conditional, i.e., it will be used as per the want of data to be secured.

Table 1.6 shows the time required for embedding secret data in image using various algorithms. As observed from table, the execution time for the proposed model is optimum in comparison to other renowned mechanisms. These values are recorded for the sender side process, used for inserting 300 bytes of secret data. Usage of simple processes for confusion and diffusion of confidential data results in a reduced amount of time complexity.

- **Imperceptibility Analysis:** Table 1.7 shows the stego-image snapshots for all the mechanisms. As seen from the results, imperceptibility for all the algorithms is excellent.

Table 1.7: Comparison of Proposed Mechanism with References for Imperceptibility

IMPERCEPTIBILITY				
ORIGINAL IMAGE	Ref1 [63]	Ref2 [64]	Ref3 [48]	PROPOSED MECHANISM
1. 	2. 	3. 	4. 	5. 

Tables 1.5 to 1.7 illustrate the comparison of the proposal with other renowned mechanisms available in the literature. As observed from the readings, almost every outcome of comparison shows that most of the parameters of the proposed mechanism have optimized values in contrast to formally accepted techniques available in the literature; this is due to the fact of employing LWT steganography and also the choice of appropriate frequency bands for the embedding of information. The "int2int" wavelet is a reversible transform, meaning it does not introduce any loss of information during the embedding process. It provides a higher level of security compared to floating-point wavelets. Floating-point operations may introduce rounding errors that could be exploited by an attacker, whereas the "int2int" wavelet is more resistant to such attacks. It is computationally efficient and requires less memory compared to other wavelet transforms. It offers a reasonable embedding capacity while maintaining image quality. It allows for hiding significant data in the cover image without causing noticeable visual artifacts. Alteration of confidential data before embedding grants add-on protection, as it introduces multifold security measures; thus, it is conferred that the proposed technique is immensely secured.

Conclusion:

With the increased information transversal over insecure networks and other

interconnected networks, demand for crucial data protection has also elevated. The proposal exemplifies a hybrid security model used to protect the confidential data used for diverse applications. The proposed scheme offers a highly secured mechanism by inculcating manifold security for data. These are conditional compression followed by dual-stage encryption and finally embedding the modified version of records in Lifting Wave Transformed cover image. This mechanism achieves the following security measures:

- Better confidentiality by modifying the secret data and finally hiding in random locations of frequency-transformed Images.
- Enhanced perceptibility of stego-image by choosing suitable frequency bands in lifting wavelet transformed cover image and conditional compression of the data.
- Perfect reproducibility of retrieving records with zero bit error.
- Improved randomness by adopting the use of Quantum logistic maps for key generation at all the stages of confusion and diffusion processes.
- High speed of execution with the usage of simple yet effective processes at each stage along with the conditional compression phase.

The proposed method provides high visibility by getting the optimized values of diverse security and other parameters like PSNR, JI, CC, IC, BC and computational time. This section presented the second proposal to achieve confidentiality, optimum time requirements, randomness, reproducibility and authenticity. The mechanism improved in many aspects and can be used for applications, as per the strength areas of the method. The following section summarizes the research work by presenting the outcomes of the given research work.

1.9 OUTCOMES

The objectives and respective outcomes are mapped as follows:

Objective 1: To study and implement diverse compression, encryption and steganography/watermarking mechanisms available in literature.

Outcome 1: Numerous existing compression, steganography/ Invisible watermarking and encryption mechanisms enlisted in section 1.2 are studied and implemented to identify an efficient method.

Related Publications:

- ❖ “Comparative Analysis of Data Compression Algorithms”, in “International Conference on Advances in Sustainable Energy, Environment and Engineering” ICASEE-2021

Objective 2: To identify efficient compression algorithm for the secret data or watermark to be embedded.

Outcome 2: After comparative analysis of various compression mechanisms such as Arithmetic, Huffman and LZW compression, which can be used in data communication network following inferences are given:

- Compression rate of Huffman and Arithmetic mechanisms are optimum.
- Speed of processing of LZW method is most favourable.
- Entropy values are high for Huffman and Arithmetic mechanisms.
- Out of all mechanisms Huffman mechanism is most suitable for Information security applications as it provides output in the form of bits in contrast to arithmetic method which provides tag value in floating point data type.
- A lossless compression technique has been identified, Huffman compression having compression of approximately 40%, as verified on numerous data set.

Related Publications:

- ❖ “Comparative Analysis of Data Compression Algorithms”, in “International Conference on Advances in Sustainable Energy, Environment and Engineering” ICASEE-2021

Objective 3: To design and implement efficient cryptography algorithm which has optimum values of brute force search, execution time, key-space, correlation coefficient, entropy and key sensitivity.

Outcome 3: An efficient encryption mechanism has been designed and analyzed, which has optimized values of key-size, key-space, entropy and correlation coefficient. It consists of two stages: confusion and diffusion. Both operations are performed at bit level. Key used at both stages is generated using centralized key scheduling algorithm. This method is employed in Proposal 2.

Related Publications:

- ❖ “Quantum Based Robust and Swift Hybrid Security Mechanism”, Published in Multimedia Tools and Applications, Springer Nature 2022, vol. 81, no. 30, pp 43727–43752, May 2022, <https://doi.org/10.1007/s11042-022-13244-w>, SCIE

Objective 4: To design and implement efficient watermarking or steganography algorithm for secret data or watermark with optimum values of robustness and security parameters.

Outcome 4: An efficient steganography/ Invisible watermarking mechanism has been identified, which has optimized values of various security (PSNR, MSE) and robustness (BC, CC, JI, UIQI) parameters. Lifting Wavelet Transform (LWT) with Integer to Integer (Int2Int) wavelet transform is considered due to the enormous advantages and features. This method is used in both proposals.

Related Publications:

- ❖ "A Multilevel Steganography Mechanism Using Quantum Chaos Encryption", Published in Multimedia Tools and Applications, Springer Nature 2019, vol. 79, no. 3-4, pp 1987–2012, November 2019, <https://doi.org/10.1007/s11042-019-08223-7>, SCIE

Objective 5: To develop/propose an efficient multilevel security mechanism considering the dynamic nature of today’s computer network environment incorporating trade-off among assorted mechanisms.

Outcome 5: Two different multilevel security mechanisms are proposed and developed. First, with the motive of providing confidentiality, integrity, authenticity, imperceptibility and reproducibility and second for providing confidentiality, imperceptibility, reproducibility with prime focus on speed of execution, for protecting secret information and documents considering the dynamic nature of today’s computer network environment.

Related Publications:

- ❖ "Multilayered Highly Secure Authentic Watermarking Mechanism for Medical Applications", Published in Multimedia Tools and Applications, Springer Nature 2021, vol. 80, no. 12, pp 18069-18105, February 2021, <https://doi.org/10.1007/s11042-021-10531-w>, SCIE
- ❖ “Quantum Based Robust and Swift Hybrid Security Mechanism”, Published in Multimedia Tools and Applications, Springer Nature 2022, vol. 81, no. 30, pp 43727–43752, May 2022, <https://doi.org/10.1007/s11042-022-13244-w>, SCIE

1.10 ORGANIZATION OF THE THESIS

The thesis is structured as follows:

Chapter 1 provides a brief introduction of the complete research work.

Chapter 2 gives a literature survey on single-level security mechanisms. It describes existing solutions for secure communication mechanisms, namely cryptography, invisible watermarking and steganography, highlighting their objectives and significance to information security. In addition, it explains various categories of all the techniques.

Chapter 3 presents the need for multiple levels of security to develop highly secure mechanisms. It describes the hybrid security mechanisms, categorized into dual-level and multilevel algorithms.

Chapter 4 presents the first proposed multilayer protection technique to fulfil the objectives of confidentiality, integrity, imperceptibility, reproducibility and authenticity along with set-up parameters that are taken into consideration for carrying out experimentation and its comparative analysis with the existing state-of-the-art mechanisms.

Chapter 5 projects another multilevel security mechanism, focusing on confidentiality, imperceptibility, reproducibility and computational speed along with set-up parameters that are taken into consideration for carrying out experimentation and validation of work by comparing with existing mechanisms for the respective technique.

Chapter 6 supplies the work's conclusions and potential directions for future research, followed by references, which are referred throughout the work. At last, a list of papers published regarding the above work is attached.

The following chapter details all renowned mechanisms studied and implemented to have insights into the security requirements.

Chapter 2

LITERATURE SURVEY - SINGLE LEVEL SECURITY

This chapter presents a reasonable amount of background information about the available security solutions relevant to the objectives and challenges of information security. Firstly, the classification and corresponding implementation of steganography/invisible watermarking mechanisms is described. Further classification of categories and consequent implementation of encryption mechanisms are performed. It helps to understand the strength of a single layer of protection and the need for developing a suitable security methodology that meets the comprehensive and dynamically varying requirements of a highly vulnerable society for efficient tools.

2.1 STEGANOGRAPHY/INVISIBLE WATERMARKING MECHANISMS

Steganography is an art and technique of hiding secret data in some carrier, i.e., image, audio, or video file. Various such techniques are available for hiding data in an image with their respective pros and cons [65–69]. Steganography is typically invisible, but Watermarking is visible and invisible; out of these later is same as steganography. The methodology used for steganography and invisible watermarking is identical, but the application areas are distinct. Former is used to protect confidential data by inserting them in one of the carriers and latter is used for authentication of documents/manuscripts by inserting watermark/signature into them. Broadly, these techniques are classified as spatial domain and transform domain. Each technique is further classified into different types depending on their actual implementation. Figure 2.1 shows diverse steganography/ invisible watermarking mechanisms available in literature. Many of these algorithms are illustrated here.

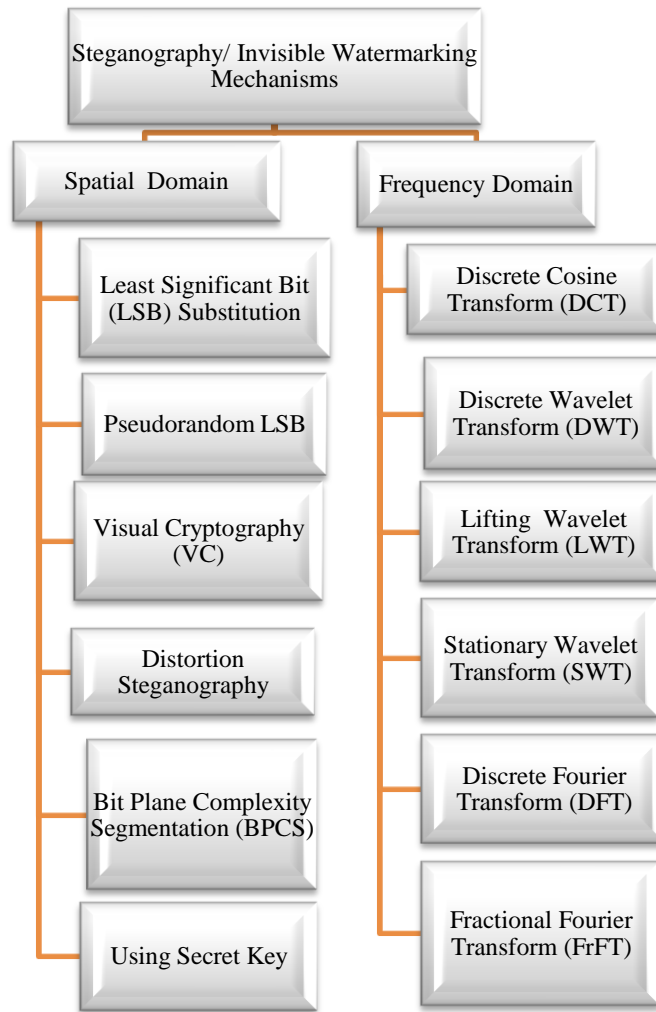


Figure 2.1: Steganography/ Invisible Watermarking mechanisms

2.1.1 Spatial Domain Steganography

In the spatial domain steganography techniques, image pixel values are converted into binary values and some bits are changed to hide confidential data. Many categories of spatial domain techniques differ mainly based on manipulating different bits in pixel values. Some of the respective mechanisms are described below:

- (a) **Least Significant Bit Substitution Mechanism:** The methodology of the Least Significant Bit (LSB) steganography technique is LSB replacement for the pixels of an image. Since only LSB is changed, the difference between the cover (i.e., original) image and the stego-image is hardly noticeable [18, 70]. Figure 2.2 shows the block diagram for the mechanism. In the first step of this technique, the cover image is separated into different color planes and the red plane is selected for embedding. In the next step, the binary value of the pixels in the image and the secret message is computed. The LSB of the pixel is then replaced with the corresponding bit of the binary transformed secret data.

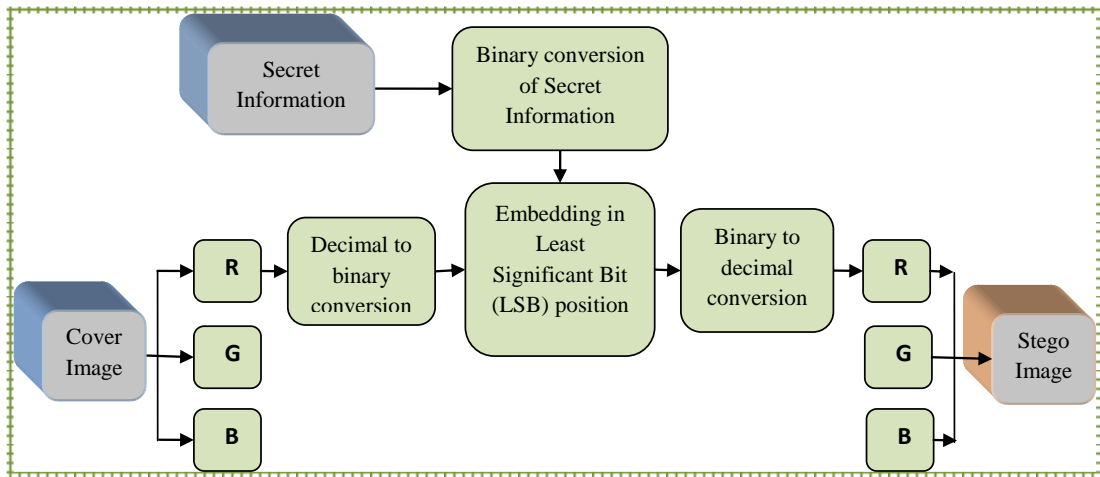


Figure 2.2: Block Diagram for LSB Steganography

The complete message length is traversed for embedding in corresponding pixels' LSB until the message reaches the end. The rest of the pixels in the image are unchanged. On the receiver side, after reading the stego image, it is separated into different color planes. The pixel values of the modified red plane are converted into binary and the least significant bits are retrieved from it for the defined size of binary converted secret message. These are finally converted into characters for getting original secret data.

- (b) ***Pseudorandom Least Significant Bit Substitution Mechanism:*** In this technique, a key chooses the pixels randomly where message bits will be stored.

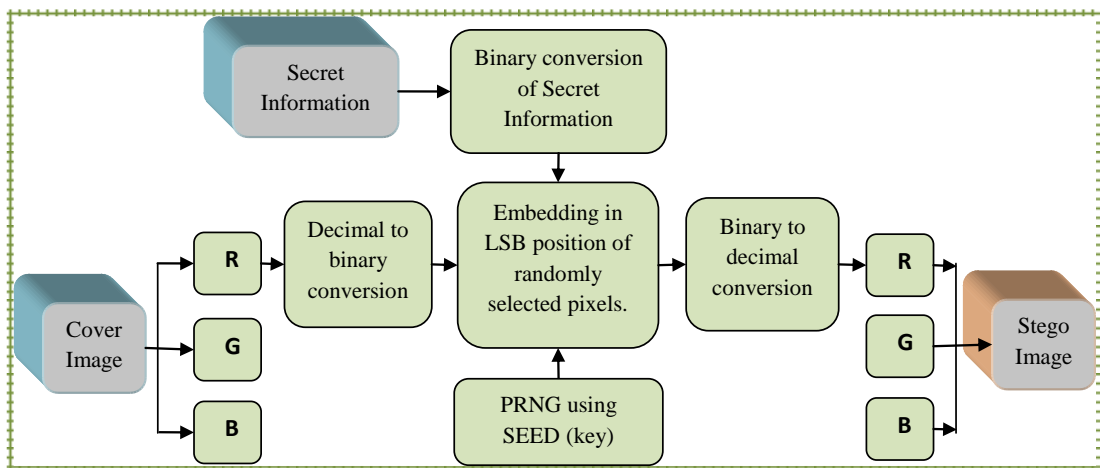


Figure 2.3: Block Diagram for Pseudorandom LSB Steganography

A random key is used as a seed for a pseudorandom number generator for selecting pixel locations in an image for hiding the secret message bits [12, 70]. Figure 2.3 shows the block diagram for the pseudo-random LSB substitution steganography mechanism. In the first step of this technique, the cover image is

separated into different color planes and the red plane is selected for embedding. Further, with the help of seed value, random locations are identified and used for embedding binary-converted secret message bits into the LSB of binary pixels. These random locations are made non-repetitive. The whole message length is traversed for embedding in randomly selected pixels' LSB until the message ends. On the receiver side, after reading the stego image, it is separated into different color planes. Using the same seed as the key exact random locations are generated. Then pixel values of the modified red plane are converted into binary and the least significant bits are retrieved for the defined size of binary converted secret message. These are finally converted into characters to get original secret data.

(c) **Visual Cryptography Mechanism:** In this mechanism, multiple shares of the cover image are created, so the secret message cannot be retrieved with the help of a single share. Visual Cryptography (VC) can be implemented in diverse ways, either as a cryptography mechanism, steganography technique, or combined with other mechanisms for enhancing security. One of the versions of VC is described here [13, 70]. Figure 2.4 shows the block diagram for the Visual Cryptography (VC) mechanism. In the first step, the colored image is converted

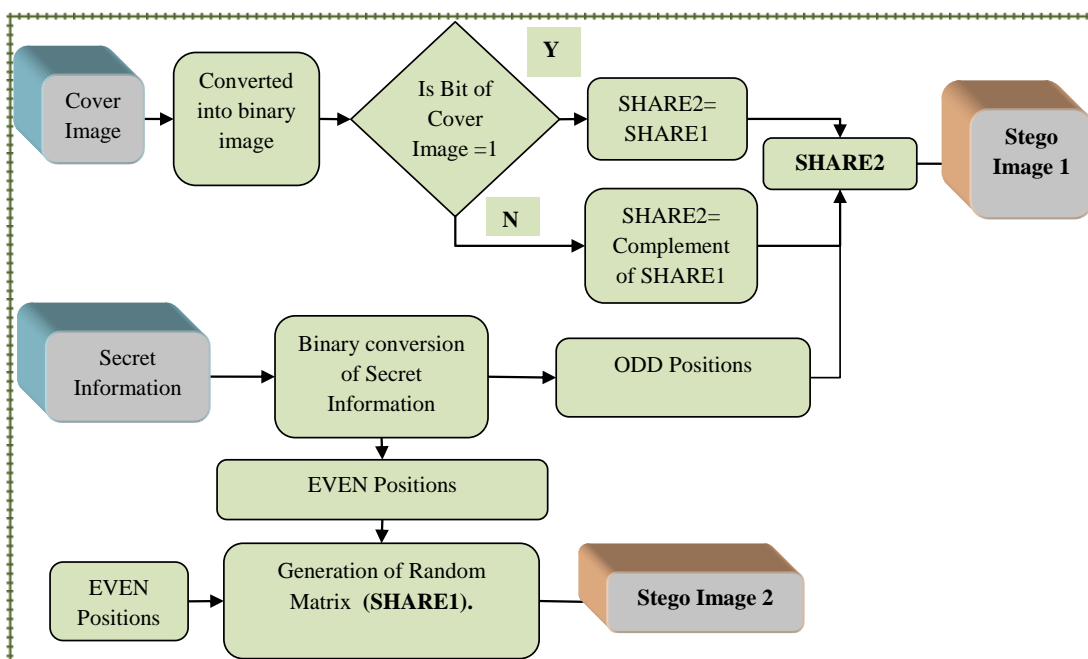


Figure 2.4: Block Diagram for Visual Cryptography Mechanism

into a binary image. A random matrix of the same size as a cover image is generated, considered SHARE 1. In the next step, as per the value of the bit of the cover image, a second random matrix is formed and is termed SHARE 2. If the pixel value is 1, the pixel value of the new matrix is the same as SHARE 1; if

the pixel value is 0, the pixel value of the new matrix is a complement of SHARE 1. The secret data bits are embedded in both shares in the next step. Alternate binary converted secret data bits are stored in both shares, even position bits in SHARE 1 and odd in SHARE 2. These shares are sent from the sender as stego-images (Stego Image 1 and Stego Image 2). These shares are read on the receiver side and finally converted into characters to get original secret data.

- (d) **Distortion Steganography Mechanism:** This technique is a variation of the LSB substitution technique. In this method, modification in the pixel value is made if the value of the secret bit is 1; else pixel value will remain unchanged [14, 15]. It uses an approach similar to pseudorandom LSB to use a pseudorandom number generator to select the pixel. Figure 2.5 shows the block diagram for the

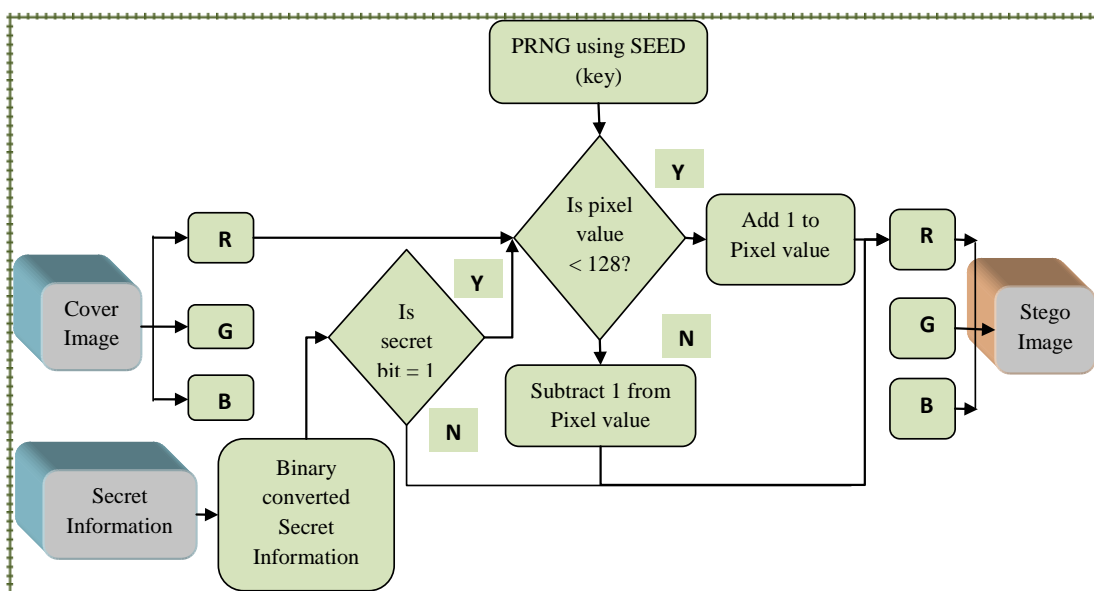


Figure 2.5: Block Diagram for Distortion Steganography

distortion steganography mechanism. In this process, firstly, the secret message is converted into bits. Then, the random key is initialized and used to identify the cover image's pixels. As per the value of each message bit, i.e., 0 or 1, the pixel value of the randomly located pixel will be modified; If secret bit=1, then; Pixel value is checked; if the pixel value < 128, increase the pixel value by x where $x=1$. If pixel overflows (value ≥ 128), decrease pixel value by x . A cover image is needed at the receiver end to retrieve message bits. The pixel value of the stego-image is compared with the corresponding value of the cover image. If the value is identical, the message bit is 0, else 1; this way, complete information is extracted.

- (e) **Bit Plane Complexity Segmentation Steganography Mechanism:** BPCS stands

for Bit Plane Complexity segmentation [17, 72–74]. This technique has a special feature of high embedding capacity and data is embedded into noise-like regions that the human eye cannot differentiate.

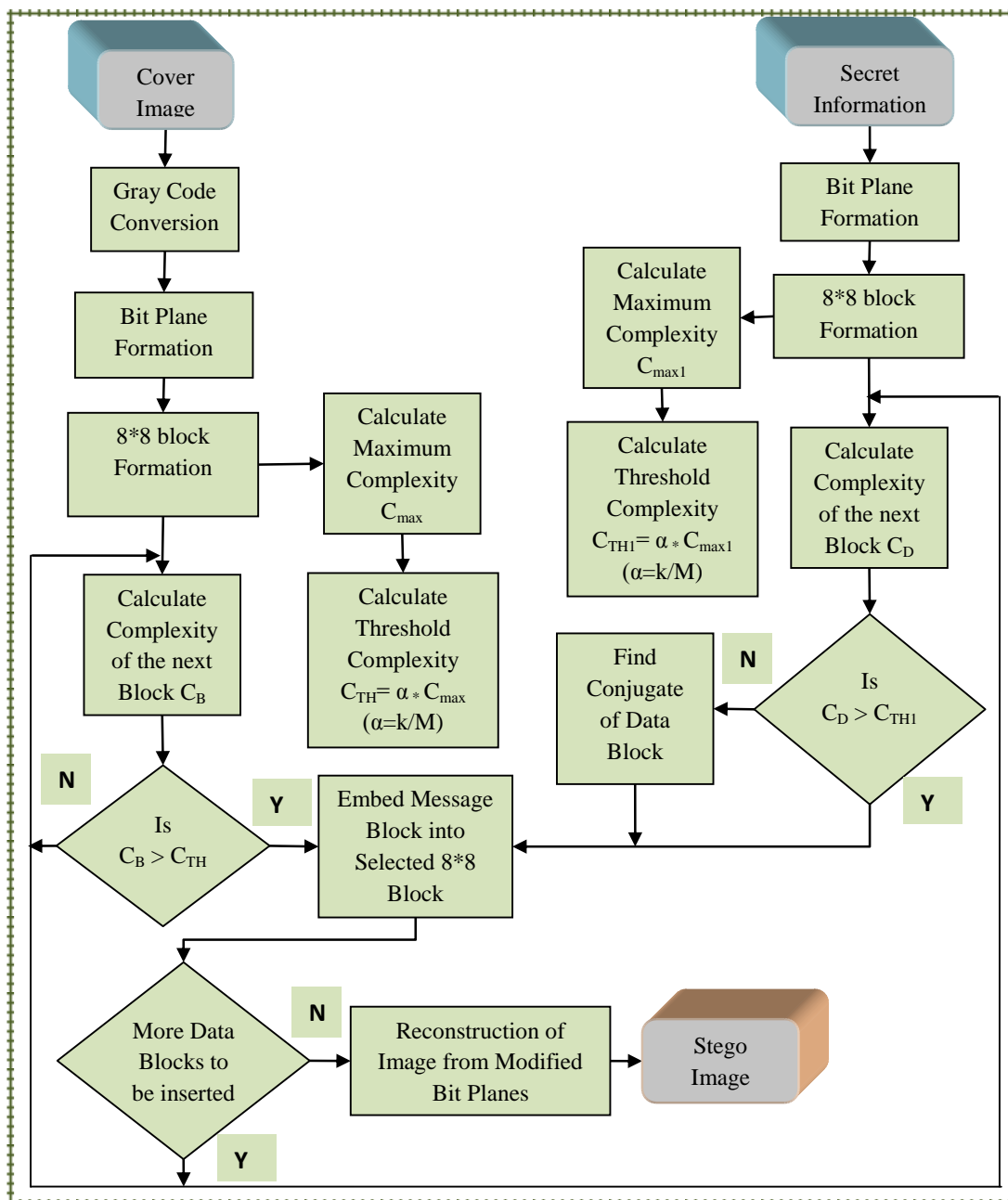


Figure 2.6: Block Diagram for BPCS Steganography

These noises-like regions have maximum possible changes in adjacent pixel values, i.e., black and white pixels, thus termed complex regions. Figure 2.6 shows the block diagram for Bit Plane Complexity Segmentation (BPCS) mechanism. The First step in BPCS is canonical gray code conversion of the pure binary codes of the cover image. After conversion, bit planes are formed for all the bit positions of the cover image and secret information. Then blocks

of 8×8 are formulated for the last plane of both. Threshold Complexity (C_{TH}) and (C_{TH1}) are now calculated for the cover image and binary-converted secret data, respectively. Both cover image and data blocks are compared with corresponding threshold values for further action. If the cover image block's complexity is higher than C_{TH} , it is considered for embedding. If data block complexity is higher than (C_{TH1}), it will be inserted without alteration; otherwise, its conjugate will be calculated. After insertion of all data blocks into cover image blocks using the defined algorithm, all bit planes are converted back to image planes and the stego image is constructed. On the receiver side, all the processes are employed reversely to reconstruct the original secret information from retrieved data blocks.

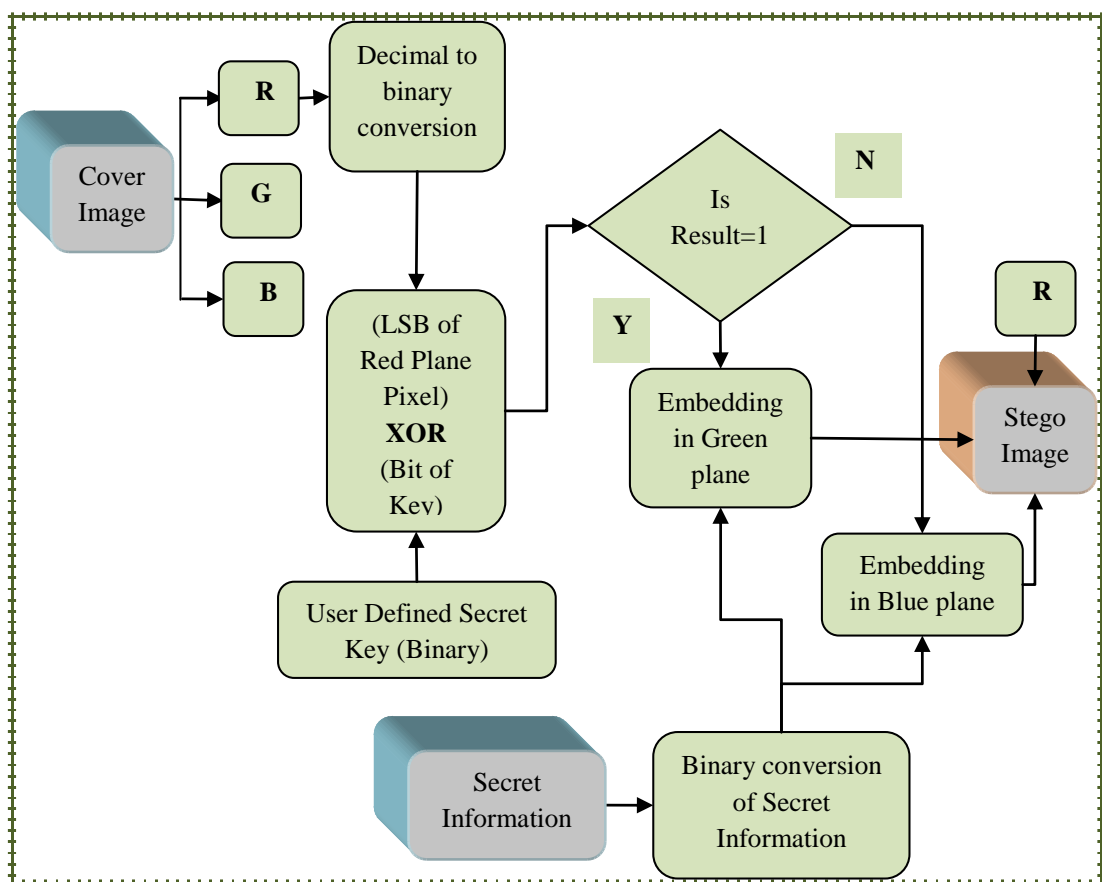


Figure 2.7: Block Diagram for LSB based Steganography using Secret Key

- (f) **LSB based Image Steganography using Secret Key:** Figure 2.7 shows the block diagram for LSB based image steganography using a secret key. In this steganography mechanism, a user-defined secret key and the red plane are employed for decision-making to hide the information into either the Green plane or the Blue plane [16]. The cover image is separated into different color planes in the first step. The circular shift operation is applied to the user-defined

key to make it dynamic and suitable for all sizes of messages. For decision-making on embedding, the LSB of the pixel value of the red plane is XORed with one bit of key. If the result is 1, then the secret message bit will store in the green plane; otherwise, it will get stored in the blue plane's pixel value. On the receiver side, bits will be retrieved from the least significant green or blue plane bits for the defined size of binary converted secret message, as per the XORed value of the red plane and secret key bits. These are finally converted into characters to get original secret data.

2.1.2 Transform Domain Steganography

In the transform domain steganography mechanisms, the message is embedded in the cover image, transformed in the frequency domain. The message bits are inserted into the transformed coefficients of the image. Many different transformations can be used for the cover image before hiding the secret data [19–25, 75–79]. This steganography method gives more robustness against attacks, as the confidential data is stored in the image at those areas that are not directly exposed and will remain unchanged after cropping or resizing the image. Numerous respective mechanisms are described below.

- (a) **Discrete Cosine Transform Steganography Mechanism:** In this steganography technique, the image is converted into frequency domain [19, 21, 22]. Discrete Cosine Transform (DCT) deals only with DFT's real or cosine parts. Since an image is a signal with no complex value, DCT is used instead of DFT to convert the spatial domain to the frequency domain.

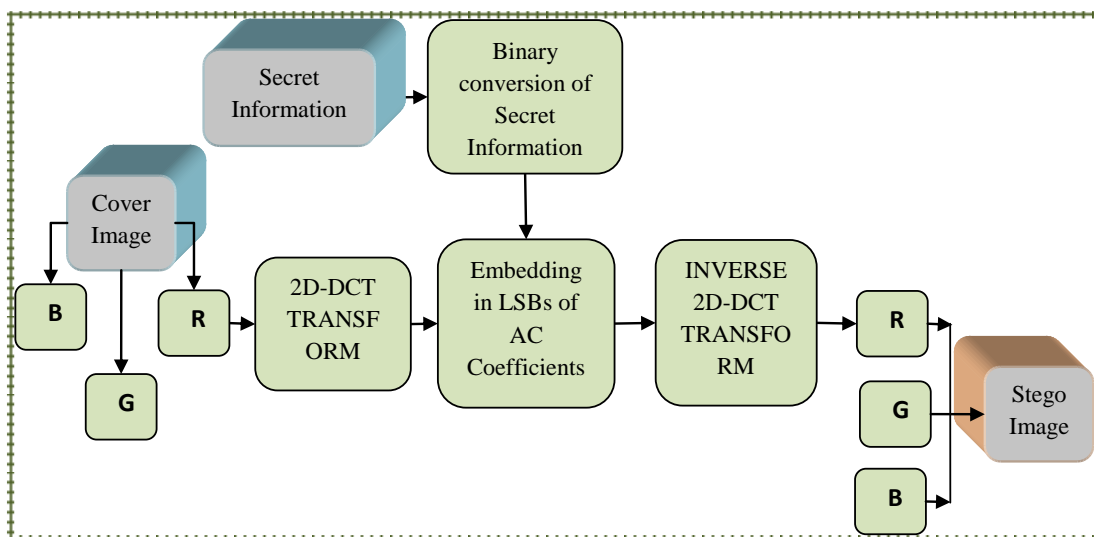


Figure 2.8: Block Diagram for DCT Steganography

This transformation is mainly used when the stego-image is prone to image modification processes like compression, cropping, etc. Figure 2.8 shows the

block diagram for DCT image steganography. In the first step of this technique, the cover image is separated into different color planes. Then 2D-DCT transformation is applied on the selected red plane to transform it into the frequency domain to convert the whole plane into DC and AC coefficients. In the next step, as per the size of secret data, bits are stored in the LSB of each AC coefficient of frequency transformed red plane of the cover image. In the last step, the modified red plane is transformed back to its original form using inverse 2D- DCT transform and combined with the other two planes to form a stego image. On the receiver side, the same procedure is employed for retrieving bits from DCT transformed red plane to get back the secret information.

- (b) **Discrete Wavelet Transform Steganography Mechanism:** Discrete Wavelet Transform (DWT) steganography is another frequency domain transformation proposed by 'Haar'. This technique is divided into two operations, horizontal and vertical operation.

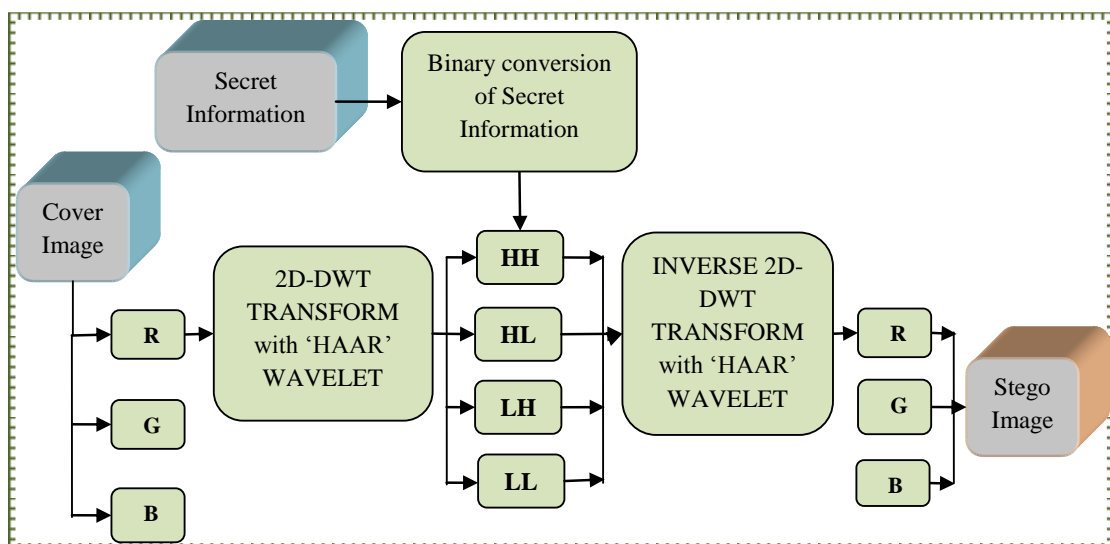


Figure 2.9: Block Diagram for DWT Steganography

Various steps of the procedure are as follows: Step 1: The pixels in a row are scanned from left to right and addition and subtraction operations are performed on neighboring pixels. On the left-hand side summation of the pixels is stored and on the right-hand side difference value is stored. This process is repeated for all the rows. The addition of pixels gives the low-frequency component and the difference of pixels gives the high-frequency component of the original image. Step 2: The pixels are scanned, in the vertical direction, from top to bottom. The sum and difference are calculated on neighboring pixels. The summation of pixels in the column is stored at the top and the difference value is stored at the bottom. This process is repeated for all the columns. The information is converted into

four sub-bands: LL, HL, LH and HH. The LL sub-band looks very similar to the original image as it is the low-frequency portion [23, 77].

Figure 2.9 shows the block diagram for DWT image steganography. In the first step of this technique, the cover image is separated into different color planes. Then 2D-DWT transformation with 'Haar' wavelet decomposition is applied on the selected red plane to convert it into the frequency domain so that the whole plane is converted into different frequency bands: LL, LH, HL and HH. In the next step, bits are stored in the HH band as per the size of the secret data. After embedding, in the last step, all the bands of the red plane are transformed back to their original form using inverse 2D- DWT transform and combined with the other two planes to form a stego image. The same steps are employed on the receiver side to get back the original secret data.

(c) **Lifting Wave Transform Steganography Mechanism:** Lifting Wave Transform (LWT) mechanism performs 2-D lifting wavelet decomposition with respect to a particular lifted wavelet that is specified or chosen.

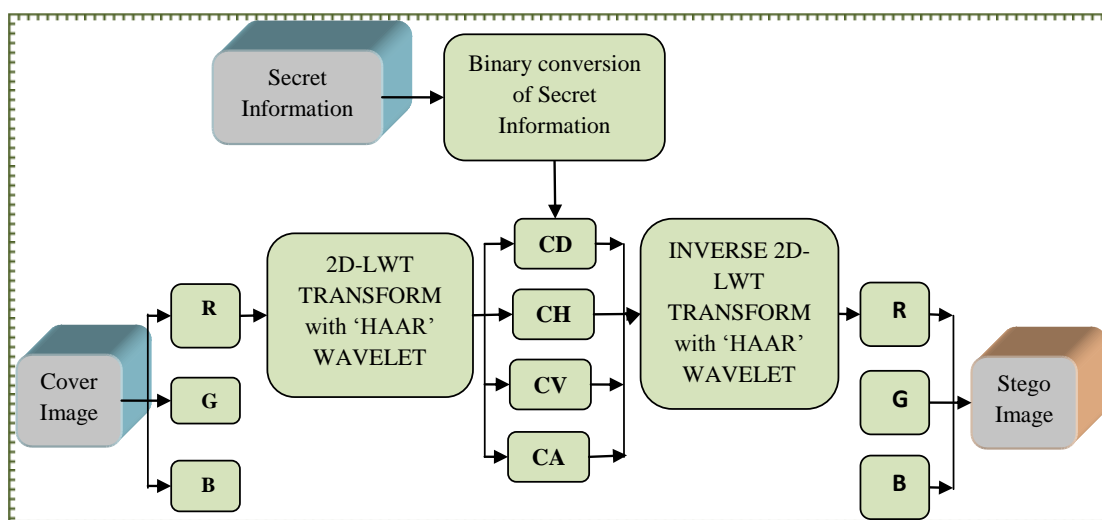


Figure 2.10: Block Diagram for LWT Steganography

This transformation segregates the given image into different coefficients; these are approximation coefficient (CA) and detailed coefficient (CH, CV, CD) by sorting out the frequencies into low and high frequencies. A multi-scale filter bank arrangement is used in Wavelet Transform, which splits the approximate and detailed frequencies [75, 79, 80]. Figure 2.10 shows the block diagram for LWT image steganography. In the first step of this technique, the cover image is separated into different color planes. Then 2D-LWT transformation with 'Haar' wavelet decomposition is applied on the selected red plane to convert it into the frequency domain so that the whole plane is converted into different frequency bands: CA, CH, CV and CD. In the next step, as per the size of the secret data,

bits are stored in the CD band of frequency transformed red plane of the cover image. In the last step, all the bands of the red plane are transformed back to their original form using inverse 2D- LWT transform and combined with the other two planes to form a stego image. The same steps are employed on the receiver side to get secret data from the transformed stego image.

- (d) **Discrete Fourier Transform Steganography Mechanism:** This mechanism transforms the continuous function into a frequency domain which gives complex values consisting of both magnitude and phase. It is robust against attacks like scaling, rotation and geometry [24, 25]. FFT (Fast Fourier transform) is an efficient algorithm to implement DFT, which converts spatial to the frequency domain. It is an image-processing tool that decomposes the image into cosine and sine components. Figure 2.11 shows the block diagram for DFT

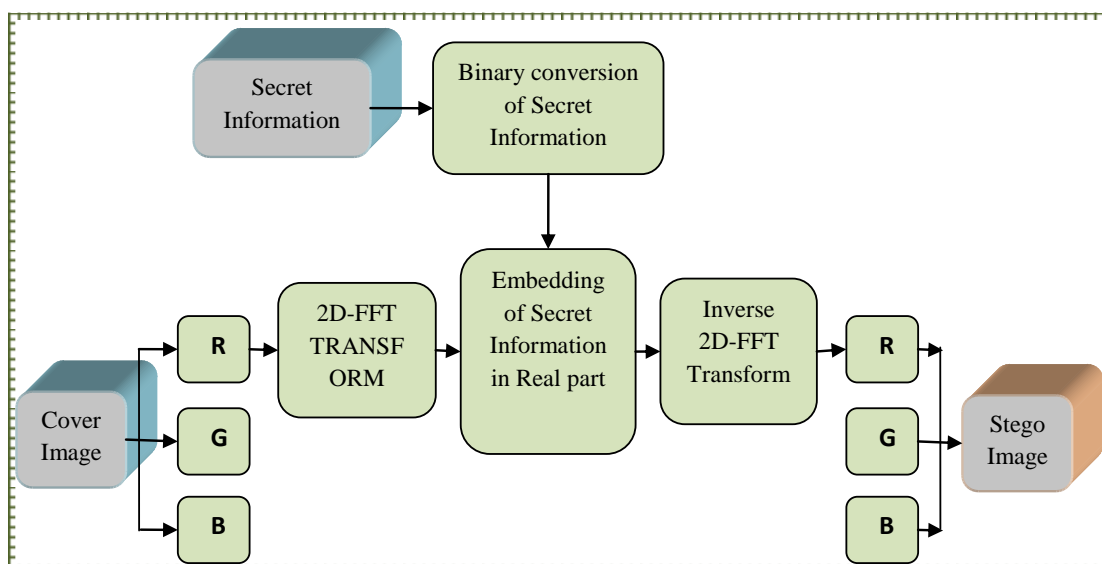


Figure 2.11: Block Diagram for DFT Steganography

image steganography. In the first step of this technique, the cover image is separated into different color planes. Then 2D-FFT transformation is applied on the selected red plane to convert it into the frequency domain Discrete Fourier Transformation (DFT). In the next step, as per the size of the secret data, bits are stored in the real part of the frequency-transformed red plane of the cover image. In the last step, all the bands of the red plane are transformed back to their original form using inverse 2D- FFT transform and combined with the other two planes to form a stego image. The same method is employed on the receiver side to retrieve the original secret data.

- (e) **Stationary Wavelet Transform Steganography Mechanism:** This mechanism decomposes an image into four subbands: A (coefficients of approximation), H,

V and D (coefficients of details; horizontal, vertical, diagonal). It performs a multilevel 2-D stationary wavelet decomposition using a specific orthogonal wavelet. Stationary Wavelet Transform (SWT) is a linear, invariant, undecimated technique [78]. Figure 2.12 shows the Block Diagram for SWT image steganography.

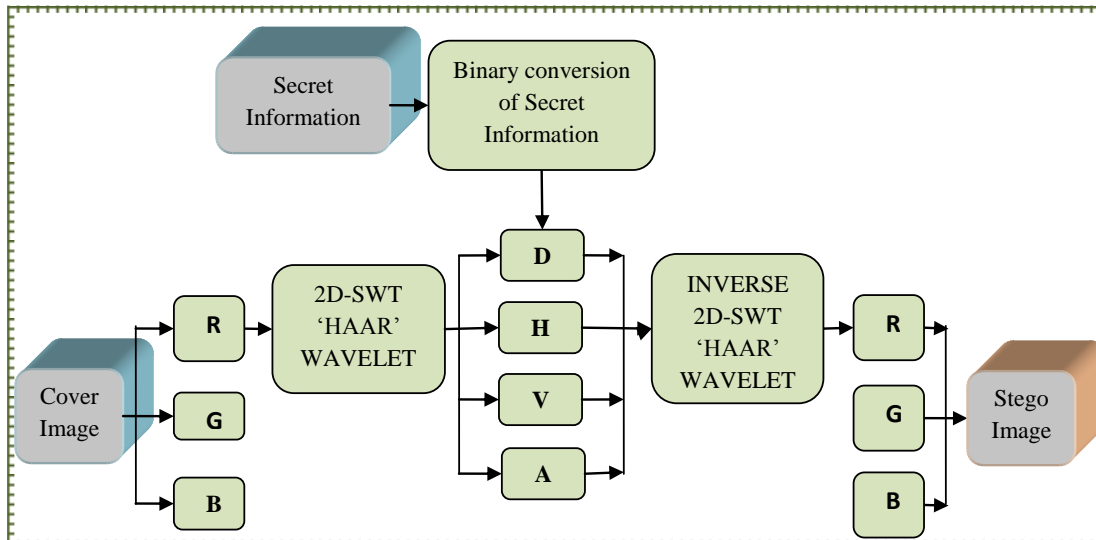


Figure 2.12: Block Diagram for SWT Steganography

In the first step of this technique, the cover image is separated into different color planes. Then, 2D-SWT transformation with 'Haar' wavelet decomposition is applied on the selected red plane to convert it into the frequency domain so that the whole plane is converted into different frequency bands; these are A, H, V and D. In the next step, as per the size of secret data, bits are stored in the D band of frequency transformed red plane of the cover image. In the last step, all the bands of the red plane are transformed back to their original form using inverse 2D- SWT transform and combined with the other two planes to form a stego image. The same method is employed on the receiver side to retrieve the original secret information.

- (f) **Fractional Fourier Transform Steganography Mechanism:** The Fractional Fourier Transform (FrFT) is a generalization of the classical Fourier transform introduced in mathematics literature to solve differential equations in quantum mechanics. The FrFT is defined for the entire time-frequency plane and the angle parameter ' α ' associated with FrFT governs the rotation of the signal to be transformed in the time-frequency plane [20, 76]. Figure 2.13 shows the block diagram for FrFT image steganography. In the first step of this technique, the cover image is separated into different color planes. Then, FrFT transformation is applied on the selected red plane to convert it into the frequency domain discrete Fractional Fourier Transformation (FrFT).

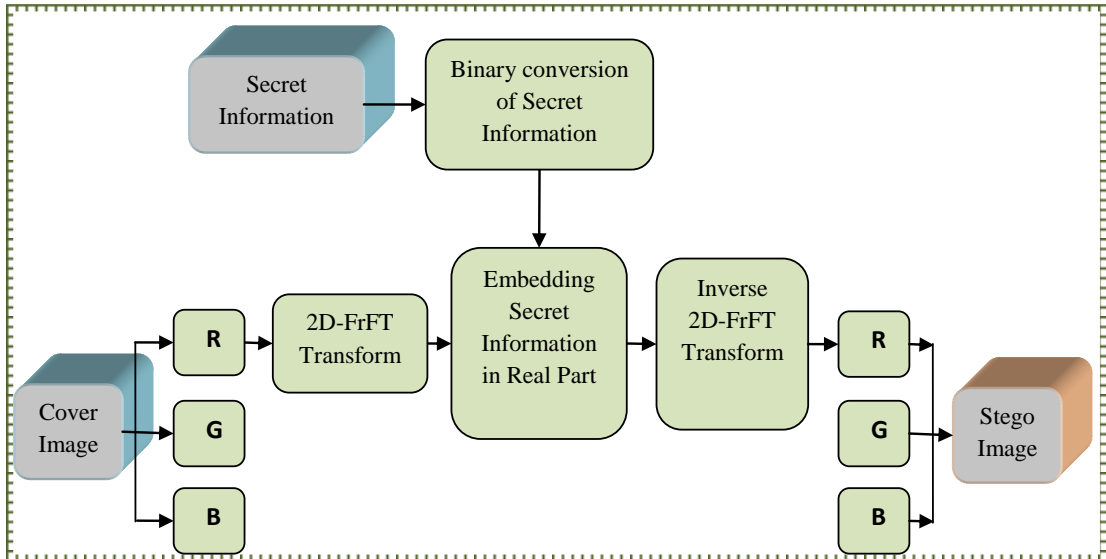


Figure 2.13: Block Diagram for FrFT Steganography

In the next step, as per the size of the secret data, bits are stored in the real part of the frequency-transformed red plane of the cover image. In the last step, all the bands of the red plane are transformed back to their original form using inverse FrFT transform and combined with the other two planes to form a stego image. On the receiver side, after separating the modified red plane from the stego-image, the FrFT transform is applied to it to retrieve data bits.

2.1.3 Comparison of Steganography Mechanisms

In exploring a secure protection mechanism, numerous single-layer security mechanisms available in the literature are studied and implemented. The performance evaluation of these techniques is performed with the help of parameters as described in Table 2.1. These are broadly categorized as the analysis of the imperceptibility of the image after embedding, confidentiality provided to secret information, time taken for implementation and capability of the technique to read back the information stored in the cover image. These are all essential network security requirements. The comparison of diverse steganography mechanisms discussed in this chapter is shown in Tables 2.2 and 2.3, illustrating for spatial domain and transform domain, respectively. As seen from the tables, it can be inferred that different mechanisms provide varying values of defined performance metrics. The choice of a steganography mechanism should be guided by the specific requirements of the intended application. Factors such as data type, security needs and available computational resources play a crucial role in determining the most suitable mechanism. By considering the performance metrics highlighted in the tables, practitioners can select the optimal steganography technique for their particular use case.







Table 2.1: Performance parameters taken for literature Survey of Steganography Techniques

Parameters of Comparison	Performance Metrics	Range (Optimized)
Imperceptibility Analysis (IMP): The stego image is analyzed visually to determine any type of deformity in the image.	Snapshots	Visual Inspection
<p>Confidentiality of the mechanisms can be evaluated by investigating image quality before and after embedding. It can be done using numerous metrics categorized into robustness and security analysis.</p> <p>Robustness Analysis (RA): This is Quantitative analysis, performed by investigation of image values before and after embedding.</p> <p>Security Analysis(SA): It compares the pixel values, probability distribution and histograms between the cover and stego images i.e. before and after embedding</p>	Peak Signal to Noise Ratio (PSNR)	Its value should be higher than 30db (High).
	Mean Square Error (MSE)	It should be minimum, ideally 0 (Low).
	Correlation Coefficient (CC)	Its value lies in the range [-1, +1]. +1 signifies perfect match and 0 signifies entirety mismatch. (Positive)
	Jaccard similarity Index (JI)	Its value lies in the range [0, 1]. The higher value signifies more similar populations (High).
	Universal Image Quality Index (UIQI)	Its value lies in the range [0, 1] High values signify lower impact on the Human Visual System (High).
	Intersection Coefficient (IC)	The range of values for this coefficient is between 0 to 1. Where 0 represents complete mismatch and 1 represents exactly match (High).
	Bhattacharya Coefficient (BC)	Its value lies in the range [0, 1]. The high value signifies the relative closeness between the images (High).
Computational time (CT): It is defined as the total processing time on receiver side or receiver and transmitter side.	Execution time (in Seconds)	The computational time should be as low as possible for practical applications. (Low)
Reproducibility (REP): It indicates complete retrieval of the confidential information by the recipient.	Bit Error Rate (BER)	The BER should be as low as possible, ideally it should be 0. (Low)

It is evident from the results; the spatial domain techniques provide high readings in robustness and security analysis compared to frequency-domain algorithms. Instead,

transform domain methods hide messages in significant areas of the cover image and are, therefore, less sensitive to small changes in the image. Transfer domain methods are preferred because strategies of threat and steganalysis are increasing and spatial domain algorithms are elementary and straightforward to be broken.







Table 2.2: Comparison of Spatial Domain Steganography Mechanisms

Steganography Mechanisms	CONFIDENTIALITY (Robustness Analysis and Security Analysis)							CT	REP	IMP
	PSNR	MSE	CC	JI	UIQI	IC	BC	Time (S)	BER	Visual Check
SPATIAL DOMAIN STEGANOGRAPHY/ WATERMARKING MECHANISMS										
LSB Substitution [18]	62.29 High	0.0380 Low	0.999998 Highest	99.9912 High	0.999999 Highest	0.998899 Highest	0.999998 Highest	2.79 Lowest	0	
Pseudorandom LSB [70]	68.25 High	0.0097 Low	0.999998 Highest	99.9995 Highest	0.999999 Highest	0.998667 High	0.999997 High	10.82 Highest	0	
Visual Cryptography [13]	24.16 Lowest	249.12 Highest	0.460500 Lowest	83.0800 Lowest	0.626398 Lowest	0.878070 Lowest	0.6673 Lowest	6.33 Low	0	
Distortion [14]	68.35 Highest	0.0095 Lowest	0.999998 Highest	99.9994 High	0.999999 Highest	0.998575 High	0.999997 High	5.19 Low	0	
Bit Plane Complexity Segmentation [71]	65.28 High	0.0190 Low	0.999987 High	98.7548 High	0.999987 High	0.992789 High	0.99987 High	10.50 High	0	
Secret Key Based LSB Substitution [16]	67.25 High	0.0122 Low	0.999998 Highest	99.9933 High	0.999999 Highest	0.997741 High	0.999993 High	8.077 High	0	

As seen from the comparison table of spatial domain steganography mechanisms, LSB substitution, pseudorandom LSB and distortion techniques provide the highest values for different parameters for the evaluation of confidentiality. For computational time, LSB and VC provide the best results. Reproducibility is best for all the mechanisms. Apart from VC, all others give good-quality output images for imperceptibility. The comparison table of frequency domain steganography mechanisms shows that LWT-based frequency transformation provides the highest values for different parameters to evaluate confidentiality. For computational time, DFT based schemes provide the best results. Reproducibility is best for all the

mechanisms. Apart from DFT and FrFt-based techniques, all others give good-quality output images for imperceptibility.

Table 2.3: Comparison of Frequency Domain Steganography Mechanisms

Staganography Mechanisms	CONFIDENTIALITY (Robustness Analysis and Security Analysis)							CT	REP	IMP
	PSNR	MSE	CC	JI	UIQI	IC	BC	Time (S)	BER	Visual Inspection
FREQUENCY DOMAIN STEGANOGRAPHY/ WATERMARKING MECHANISMS										
DCT Based Steganography [19]	28.96 Low	82.48 High	0.945900 High	99.86 High	0.970059 High	0.934 High	0.995 High	6.29 High	0	
DWT Based Steganography [77]	48.21 High	0.981 Low	0.999805 High	99.98 High	0.999902 High	0.994 High	0.999 Highest	8.54 Highest	0	
LWT Based Steganography [79]	48.52 Highest	0.916 Lowest	0.999828 Highest	99.99 Highest	0.999914 Highest	0.993 High	0.999 Highest	4.76 Low	0	
SWT Based Steganography [78]	43.74 High	2.75 Low	0.915112 High	81.77 Lowest	0.868005 Low	0.644 Lowest	0.868 Lowest	5.48 High	0	
DFT Based Steganography [24]	24.22 Lowest	245.9 Highest	0.538987 Lowest	82.03 Low	0.677102 Lowest	0.923 High	0.719 Lowest	4.17 Lowest	0	
FrFT Based Steganography [20]	28.08 Low	101.0 High	0.891007 Low	99.97 High	0.939245 High	0.990 High	0.898 Low	6.46 High	0	

Among the array of steganography mechanisms under comparison, the Lifting Wavelet Transform (LWT) utilizing the Integer to Integer (Int2Int) wavelet transform emerges as the prime choice for integration into the proposed mechanism. This selection is grounded in several compelling reasons that affirm its suitability for the intended application. One of the standout advantages of LWT is its utilization of a fixed-point arithmetic configuration. LWT's fixed-point structure is significantly more memory-efficient than its floating-point arithmetic counterpart. This characteristic is especially pivotal in constrained memory resources, enabling efficient implementation even in resource-limited environments. In domains such as image processing, the input pixel values are inherently integers. The crux of the matter arises during the wavelet transform process, where filtering operations can introduce fractional values due to inherent mathematical computations. The Int2Int wavelet transform, integral to LWT, adeptly addresses this concern. Ensuring that the output remains in the integer domain

effectively mitigates the propagation of rounding errors that can undermine the fidelity of the steganographic process.

The following section details another prevalent security solution.

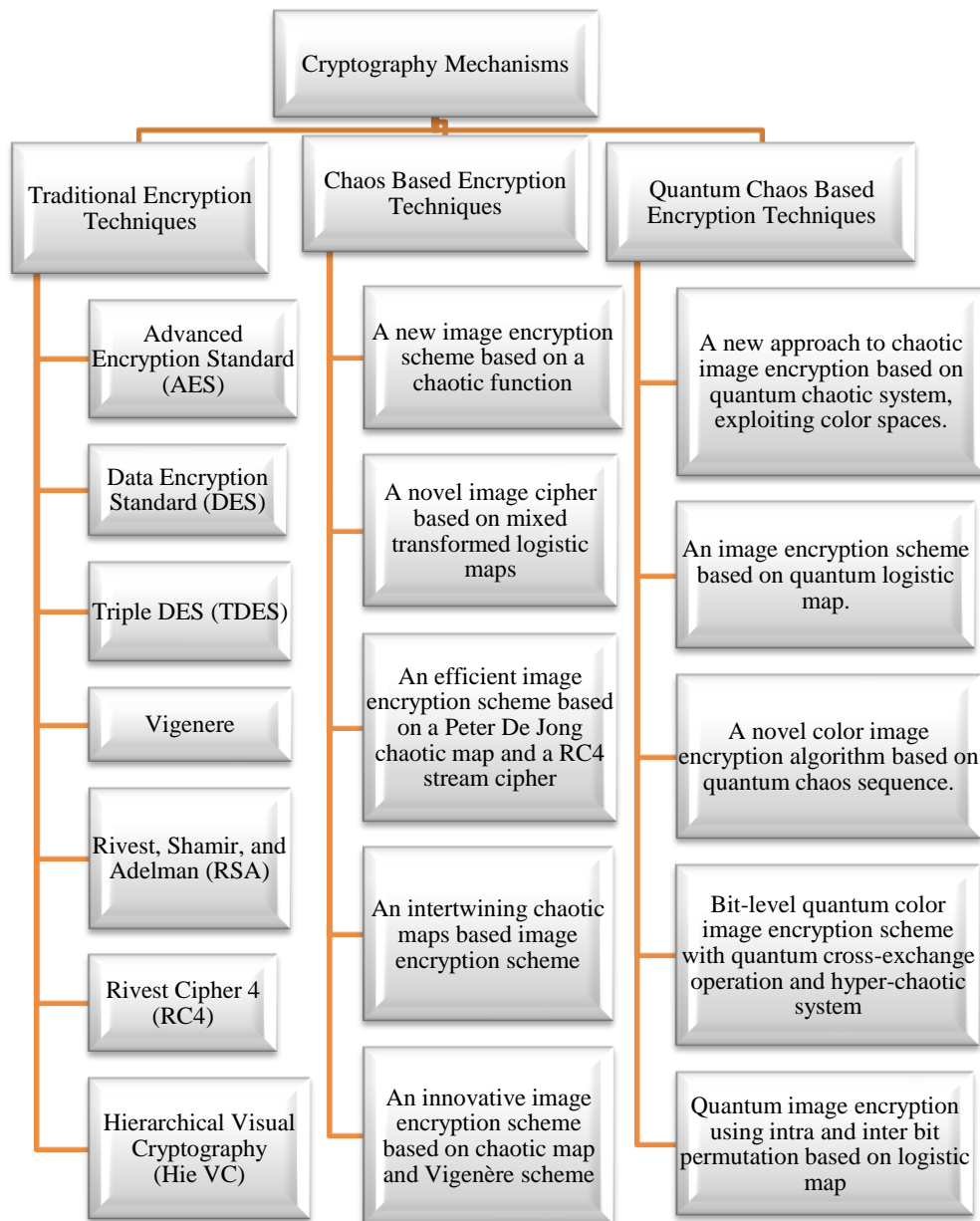


Figure 2.14: Cryptography Mechanisms

2.2 CRYPTOGRAPHY MECHANISMS

For securing any information, cryptography is admired and widely used choice. It is used to encode the message so that it can be safely moved on the communication channel. Although many algorithms are available in the literature, in the current era, widespread studies are going on in the field of chaos and quantum-chaos based

cryptography schemes [81, 82]. Many of these algorithms are illustrated here. Figure 2.14 demonstrates various existing encryption algorithms and all are taken for study and implementation.

2.2.1 Traditional Encryption Mechanisms

Traditional, classic, or conventional algorithms were the primary and straightforward algorithms that were dependent on the shifting, transposition, or substitution, round-based practices [26–30]. For instance, vigenère’s encryption plot substituted plain content from a predefined table called the vigenère table, while several employed shuffling letters, like Caesar techniques. The techniques possessed low randomness and consumed large processing time to encrypt images while small key-space leads to an easy intruder attack. These algorithms can be effectively decoded utilizing the frequency distribution of the ciphered data or with attacks such as brute force attack, chosen plaintext attack, known plaintext attack. But these mechanisms were widely used in the past. However, most of them were broken by the unauthorized user. Many of the respective mechanisms are described below:

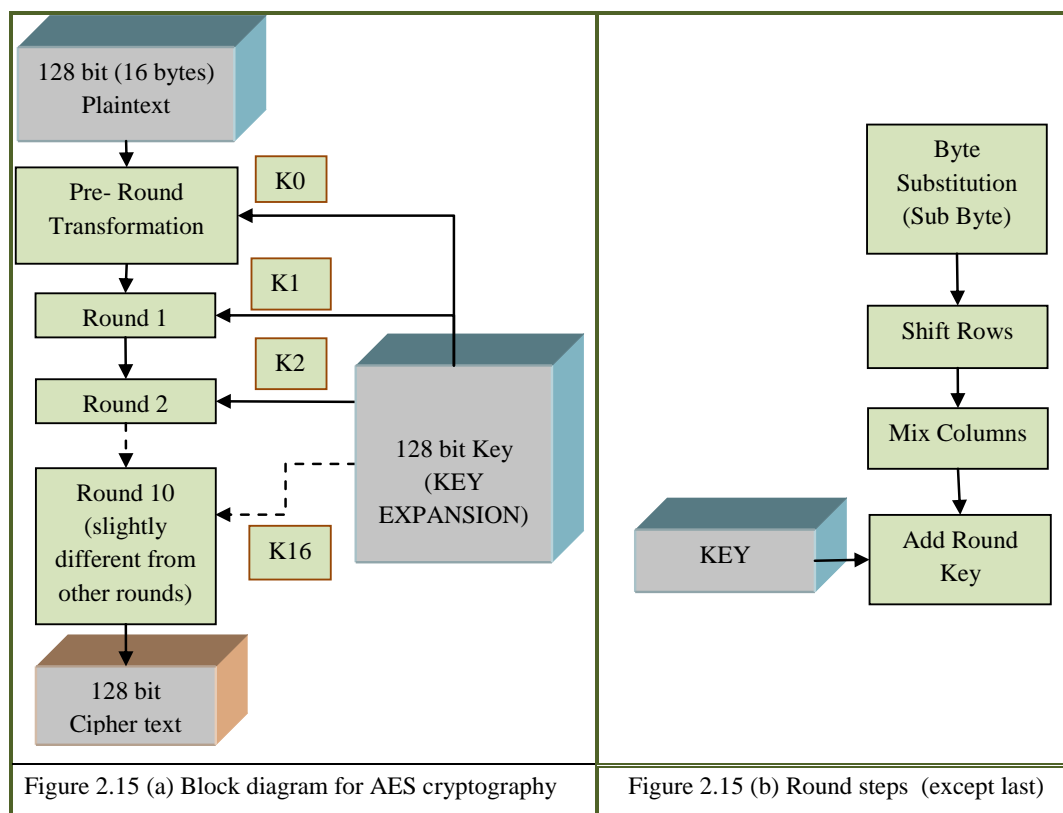


Figure 2.15: Block Diagram for AES Cryptography

- (a) **Advanced Encryption Standard:** It is a symmetric-key method having a place in the Rijndael cipher family. It is a block cipher, which means the number of

bytes it encrypts is fixed. It can encrypt blocks of 16 bytes or 128 bits at a time. The number of rounds of the algorithm depends on the key-size. For the key-size of 128 bits or 16 bytes, the number of rounds is 10; for the key-size of 192 bits or 24 bytes, the number of rounds is 12; and for the key-size of 256 bits or 32 bytes, the number of rounds is 14. The selected key is expanded into individual sub-keys, a dedicated sub-key for each operation round. This process is called key expansion. AES and most encryption algorithms are reversible, which means that almost the same steps are performed to complete both encryption and decryption in reverse order [29, 82]. Figure 2.15 shows a block diagram for the AES encryption process along with the steps performed in each round (except the last round). The structure of AES is based on a substitution permutation network. The input data undergoes multiple rounds of encryption process depending on the size of the key. Each round consists of byte substitution, shift rows, mix columns and key addition operations. The only exception is that the mix column step is not performed in the last round to make the algorithm reversible during decryption. After completing all rounds, except that there is no mix column function for the last one, the final round will provide the cipher text, which is the same size as plain text, 128 bytes. For decryption, all the rounds and respective steps are followed in reverse order to retrieve the plaintext.

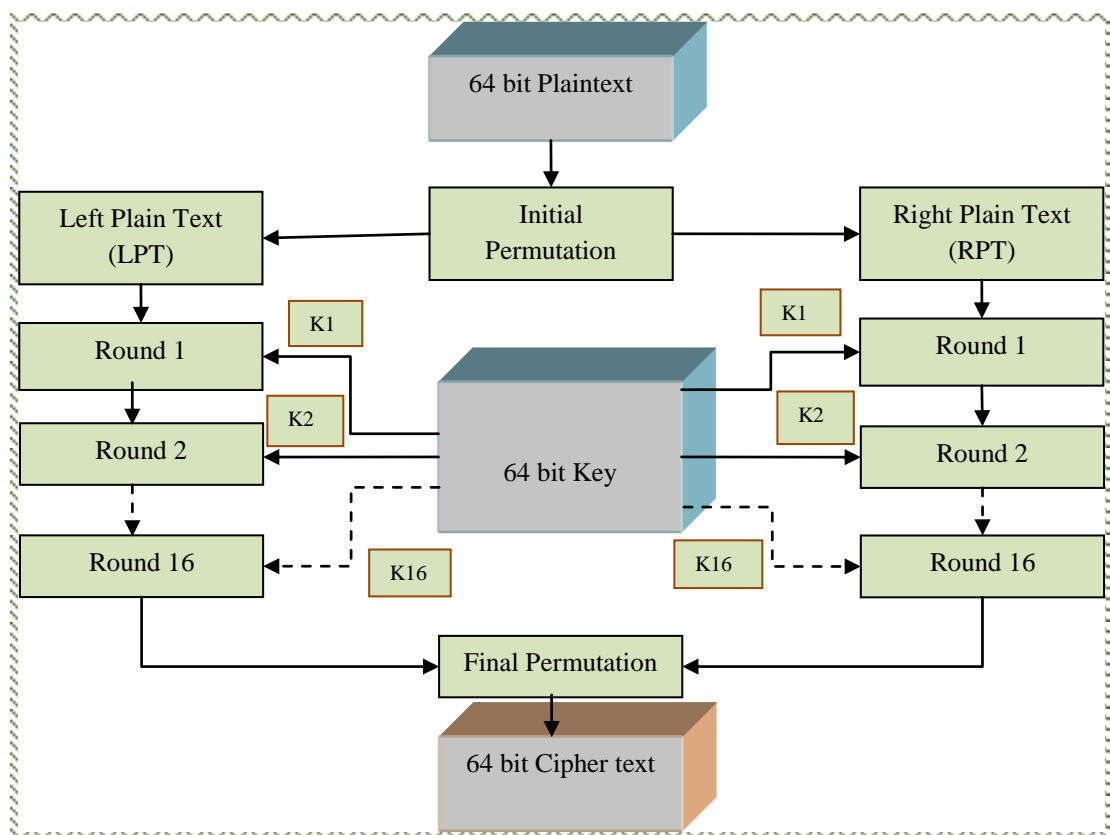


Figure 2.16: Block Diagram for DES Cryptography

(b) **Data Encryption Standard:** It is one of the earliest block cipher encryption schemes created in the 1970s at IBM [26]. It is based on the two fundamental attributes of cryptography; substitution (confusion) and transposition (diffusion) [82]. DES uses 16 rounds. Figure 2.16 shows the block diagram for the DES encryption process. The first step is key transformation, in which the initial key of a 64-bit is transformed into a 48-bit key using different steps. After getting keys, the next step in plain text encryption is handing over the 64-bit plain text block to an initial Permutation (IP) function. The Initial permutation (IP) happens only once, before the first round. After IP, the resulting 64-bit permuted text block is divided into two half blocks; Left Plain Text (LPT) and Right Plain Text (RPT). Each half-block consists of 32 bits and goes through 16 rounds of the encryption process. After applying these rounds, the RPT is expanded from 32 bits to 48 bits using the expansion permutation. In the end, LPT and RPT are rejoined and a Final Permutation (FP) is performed on the combined block. The same algorithm and key are used for encryption and decryption, with minor differences. On the encryption side, round 1 used k1 and round 16 used k16; at the decryption site, round 1 used k16 and round 16 used k1.

(c) **Triple Data Encryption Standard:** It is a symmetric key block cipher that applies the DES cipher in triplicate by encrypting with the first key (k1), decrypting with the second key (k2) and encrypting with the third key (k3). A two-key variant also exists, where k1 and k3 are the same.

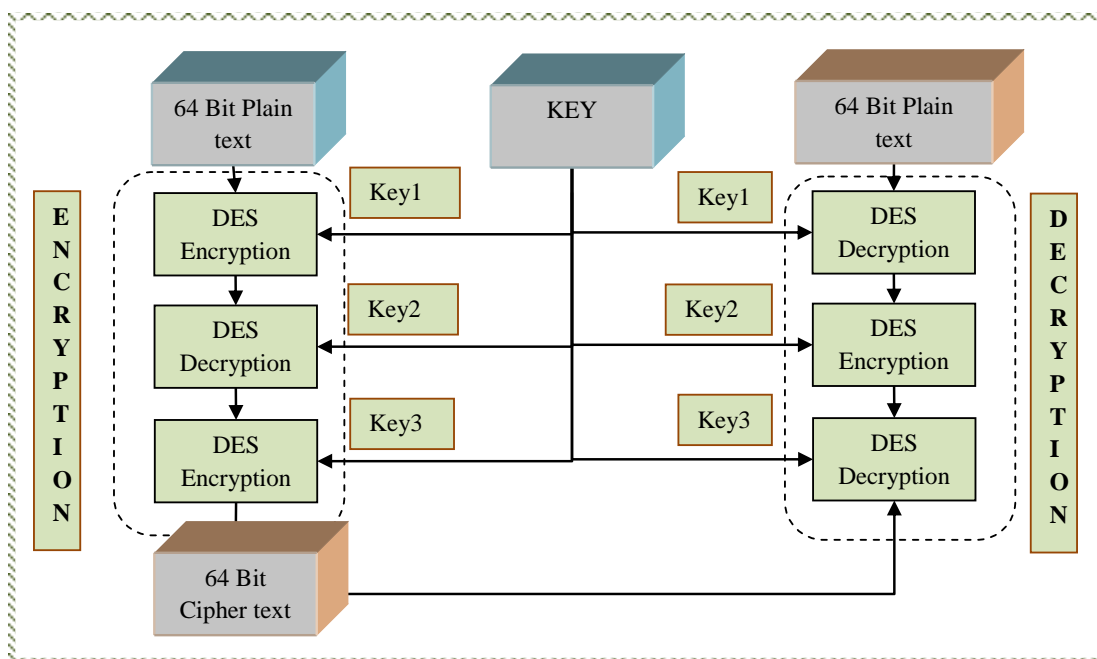


Figure 2.17: Block Diagram for TDES Cryptography

It is an encryption technique that uses three instances of DES on the same plain text. It has the advantage of proven reliability and a longer key length. TDES uses three 56-bit keys for the encryption and decryption processes [27]. Three key alternatives as shown as defined; Key choice 1: All three keys are independent. It is the most excellent keying alternative and is not vulnerable to any known practical attacks, Key choice 2: K1 and K2 are autonomous, while K3 is the same as K1. It is safe against meet-in-the-middle attacks but is powerless against attacks like chosen plaintext. It is otherwise known as 2DES, Key choice 3: All three keys are indistinguishable. It is the weakest keying alternative.

Figure 2.17 shows the block diagram for TDES encryption and decryption processes. The first step is key transformation, in which the initial key of a 64-bit is transformed into three independent 48-bit keys by using different steps. Then by using different keys, alternatively DES encryption and decryption algorithms are employed. On the receiver side also, after the generation of three keys, reverse alternatives are used, i.e., decryption followed by encryption.

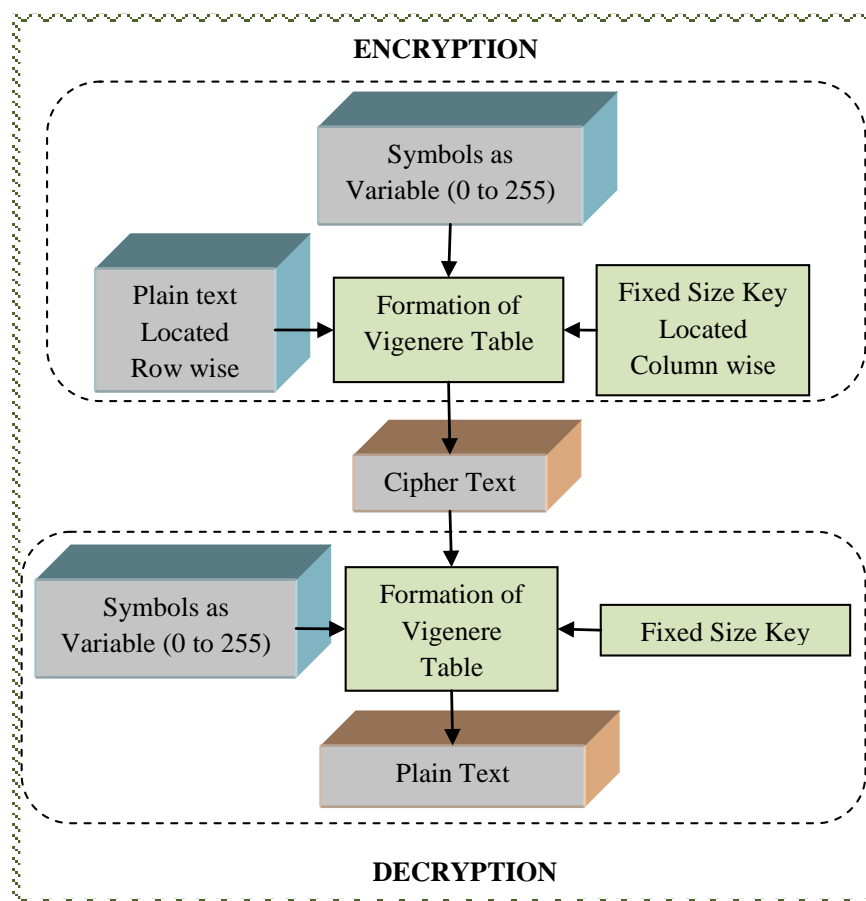


Figure 2.18: Block Diagram for Vigenère Cryptography

- (d) **Vigenère Cryptography:** It is a polyalphabetic substitution cipher that uses two or more cipher alphabets. They have one to many correspondences between each

letter and its substitutes. The first step in this encoding process is to form a vigenère table. In this table, each row is formed by shifting the sequence of characters toward the left cyclically. The key is of fixed size and value; every character will be located on the column side and characters of secret data will be located on the row side. The interaction of these two will give encrypted data. Data decryption is also done using the same symmetric table [28, 37]. Figure 2.18 shows the block diagram for vigenère cryptography. For encryption and decryption, the first step is forming a Vigenère table. For encoding data, Vigenère table and a key is required. This Key will be of fixed size and value, which the receiver and transmitter will share. If the data to be encoded is larger than the number of characters of Key, then the repetition of key elements is used. The key elements are located column-wise in this generated table and the data characters to be encoded are found row-wise. The intersection of these two gives encoded character. The Vigenère table and Key are needed for data decryption and the complete plain text is retrieved.

- (e) **Rivest, Shamir and Adelman Cryptography:** Rivest, Shamir and Adelman (RSA) were the technique’s inventors.

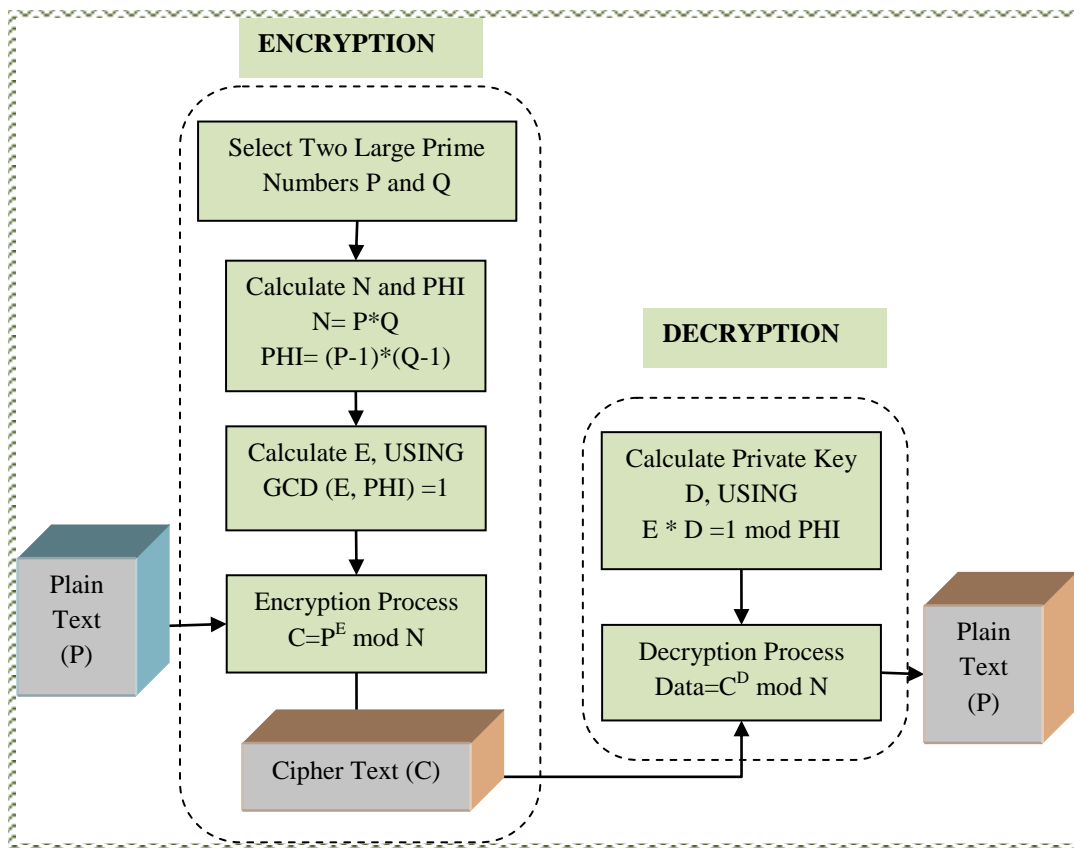


Figure 2.19: Block Diagram for RSA Cryptography

RSA algorithm is an asymmetric cryptography algorithm, which means it works

on two different keys, i.e., Public Key and Private Key. The public key consists of two numbers, where one is the multiplication of two large prime numbers. Moreover, the private key is also derived from the same two prime numbers. Therefore, the strength of encryption relies on the key-size and if the key-size is doubled or tripled, the strength of encryption increases exponentially. RSA keys can be typically 1024, 2048, or 4096 bits long [83, 84]. Figure 2.19 shows the block diagram for RSA cryptography. For encryption and decryption, the initial procedure begins with selecting two prime numbers, P and Q and then calculating their product N and PHI. On the sender side, the public keys used for encryption are E and N. So, E is calculated using selected prime numbers. Thus, the ciphertext is calculated using the relation Cipher text = $P^E \text{ mod } N$, where P is plain text and E and N are public keys. For decryption, private key D is required at the receiver side, calculated using E, P and Q. Finally, plain text is retrieved using the relation Data = $C^D \text{ mod } N$, where C is cipher text and Data is plaintext.

- (f) **RC4 Cryptography:** It is a stream cipher designed in 1987 by Ron Rivest. It is a variable-length key stream cipher with byte-oriented operations. This algorithm [30] encrypts one byte at a time and is based on a random permutation. Figure 2.20 shows the block diagram for RC4 cryptography. The S-array (State array)

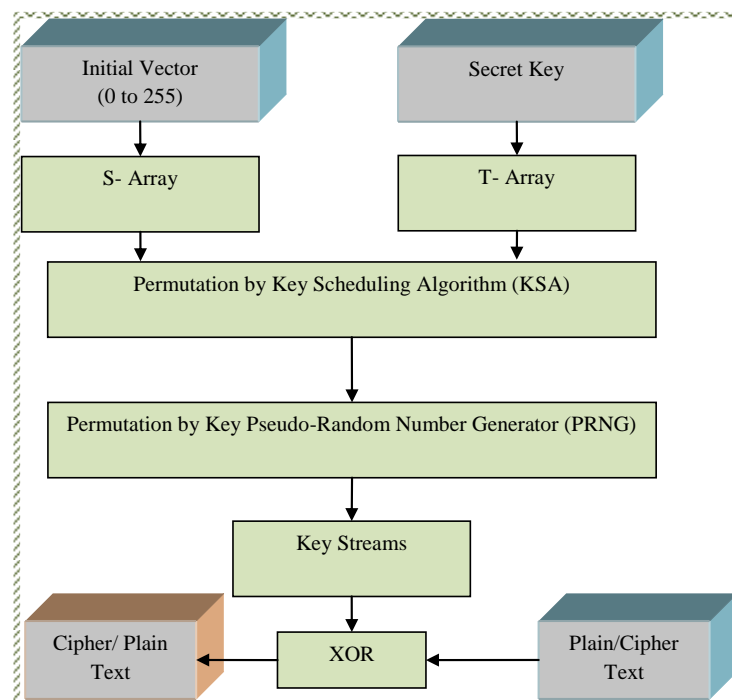


Figure 2.20: Block Diagram for RC4 Cryptography

and T-array (Temporary array) are key components used in the RC4 algorithm to generate a pseudorandom stream of bytes. The S-array is an array of 256 bytes

used to initialize the permutation of the RC4 state. The initial values of the S-array are determined by the secret key provided for the encryption process. The T-array, also known as the key-scheduling array, is another array of 256 bytes. It is derived from the secret key by repeating and extending it to match the length of the S-array. The values in the T-array are used to modify the permutation of the S-array during the initialization process.

The RC4 algorithm operates by swapping elements of the S-array based on the values from the T-array. This process is called the Key Scheduling Algorithm (KSA). After the initialization, the S-array generates a pseudorandom byte stream by repeatedly swapping elements and producing output bytes using a process known as the pseudorandom generation algorithm (PRGA). Finally, bitwise XOR operation of the key streams with the subsequent byte produces either ciphertext or plaintext.

(g) **Hierarchical Visual Cryptography Mechanism:** The key idea behind Hierarchical Visual Cryptography (HieVC) is segregating the secret information into several levels called shares [85]. HieVC requires all the shares while decrypting the information [61]. Figure 2.21 shows the block diagram for Hierarchical Visual Cryptography. In this scheme, data is converted into 2

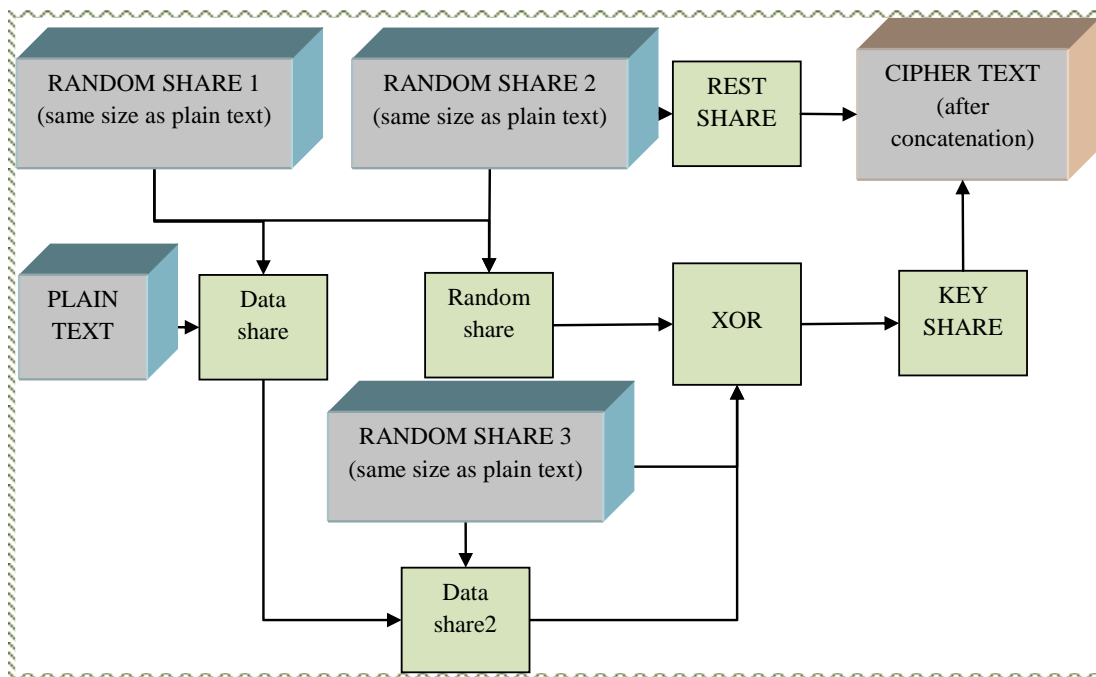


Figure 2.21: Block Diagram for Hierarchical Visual Cryptography

Shares: Rest Share and Key share, where a share is defined as a component of data that contains partial information and appears as noise to unauthorized users. First, RANDOM SHARE 1, generated as part of key generation, generates another sequence (Data Share) based on the idea. If the data bit is 1, the

complement of RANDOM SHARE 1 is written into Data Share. Else, a bit of RANDOM SHARE 1 is copied into Data Share. As the name suggests, a hierarchical relationship is followed; hence three shares, Random Share, RANDOM SHARE 3 and Data Share 2, are further generated based on the same functionality stated above. These three shares are XOR to generate the Key Share. RANDOM SHARE 2 will act as Rest Share. These two resultant shares are then transmitted further by the sender. On the receiver side, for performing the decryption process, there is only a need to XOR the key share and rest share to retrieve the original information.

2.2.2 Chaos Based Encryption Mechanism

Security of records (text, image and video) is rising extensively for many applications. Due to their intrinsic features, such as the strong correlation between pixels and bulky data capacity, images, in particular, are generally not suitable for processing by conventional encryption algorithms. These traditional techniques are unsuitable for image encryption due to high redundancy, strong correlation and high computation complexity. In recent years, various encryption schemes based on chaotic systems have been suggested to meet the requirements for robust image encryption applications [33–35]. The chaos-based cryptosystems are suitable for the secure transmission of images due to the intrinsic features of chaotic systems such as ergodicity, random-like behaviors, sensitive dependence on initial conditions and system parameters. Chaos-based cryptographic algorithm is an efficient encryption algorithm, first proposed in 1989. The properties of such systems are of immense importance in cryptographic confusion and diffusion processes. Hence chaotic-based encryption is receiving increasing interest from cryptographers [36, 37].

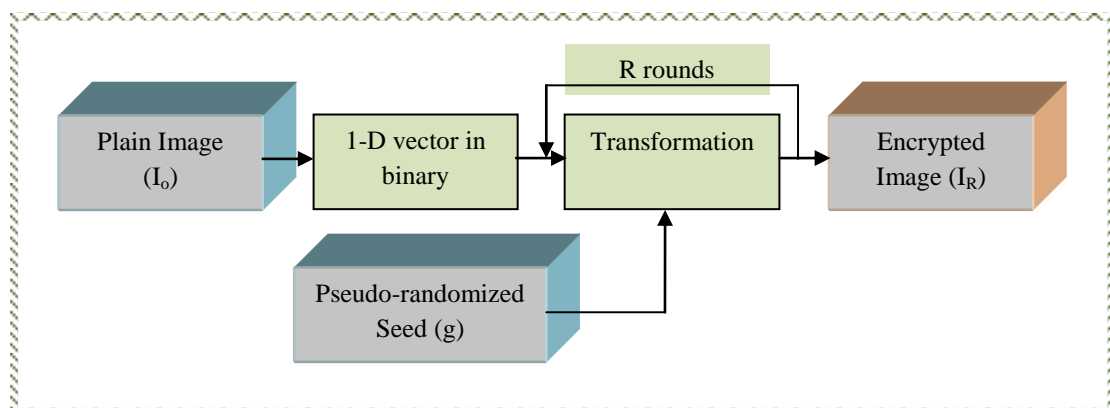


Figure 2.22: Block Diagram for Chaos Encryption 1

- (a) *A New Image Encryption Scheme Based on a Chaotic Function - Chaos Encryption 1*: This is a new chaos-based image encryption scheme based on a

coupling of chaotic function and XOR operator [33]. Figure 2.22 shows the block diagram for chaos encryption 1. Here, a pseudo-randomized seed g initiates the relation of recurrence given by:

$$X_{(n+1)} = \text{mod}(((\text{mod}(X_n^2, S)) \times X_n) + X_g, S) \quad (2.1)$$

where the initial position $X_0=g$ and $X_g=g^2$, the seed g is in the range $1, \dots, L$ and L being the binary size of the image I_0 . The value S is initialized to $L-1$ and decremented after each iteration. It shows the chaotic behavior due to which this function is used for pseudo random number generation by shuffling the starting positions $1, \dots, L$, by considering initial seed X_0 . In this scheme, information to be encrypted is the plain-image (I_0), which is first transformed into its one-dimensional equivalent vector. For shuffling of elements of the 1-D array, a sequence of pseudo-randomized seed key is generated, which is in the range 1 to L . Number of minimum rounds are calculated as $\text{Round} = \text{floor}(128/\log_2(L)) + 1$. A complete encryption scheme produces a cipher-image, where the Round is the value, providing total number of rounds used to encrypt the plain-image. Finally, the 1-D array of cipher image constituted back to RGB image (I_R). For decryption, the cipher-image is transformed into its 1-D equivalent vector consists of the binary sequences. The same randomized key in reverse order is used in this decryption process.

- (b) ***A Novel Image Cipher Based on Mixed Transformed Logistic Maps - Chaos Encryption 2:*** This cryptosystem is designed to encrypt color images based on transformed logistic maps. The mechanism provides good confusion and diffusion properties, ensuring incredibly high security due to mixing color pixels. Confusion works on making the relationship between the key and the ciphertext as intricate as possible. Commonly, this effect is incorporated by the permutation stage, whereas the diffusion effect is established in the pixel value diffusion stage. Figure 2.23 shows the block diagram for chaos encryption 2. In this scheme, with the help of proposed transformed logistic maps, the key has been generated and used in the diffusion process [34]. The confusion process, initial permutation, is achieved with the help of six random odd integer keys from 0 to 256 from the secret key. The nonlinear diffusion is done by a 4-bit circular shift followed by an addition between shifted value and the first chaotic key (X). Finally, the resultant values are XOR with the second chaotic key (Y). The final step is zig-zag diffusion of updated pixel values, in which the values of pixels are read in a zig-zag manner, followed by XOR operation amongst each other and XOR with a third chaotic key (Z). The procedure for zig-zag diffusion is performed for all three planes of the image and results in a cipher image (I_R).

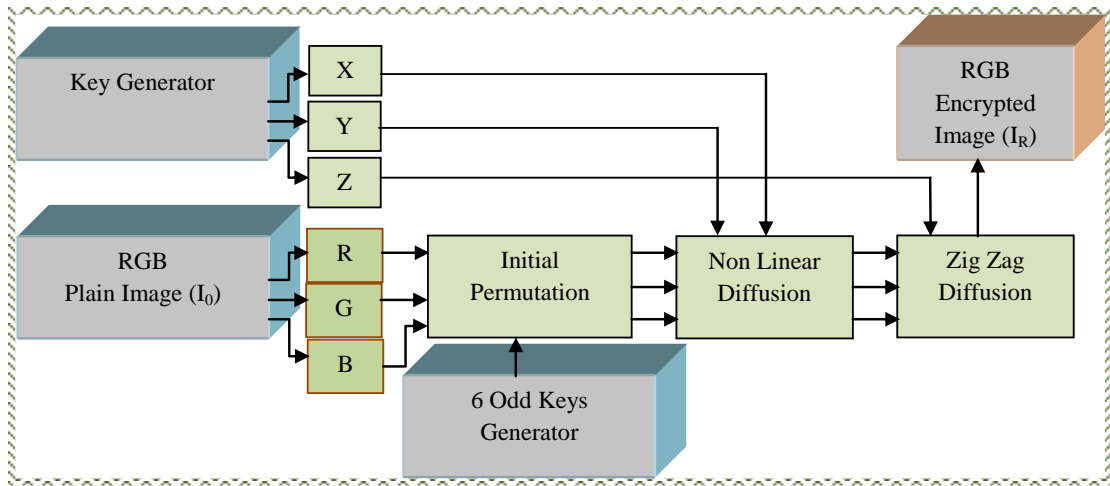


Figure 2.23: Block Diagram for Chaos Encryption 2

The decryption process follows all these processes in reverse order using the same set of keys, thus retrieved back the plain image (I_0).

- (c) **An Efficient Image Encryption Scheme Based on a Peter De Jong Chaotic Map and a RC4 Stream Cipher - Chaos Encryption 3:** This is a proficient image encryption scheme based on a Peter De Jong chaotic map and an RC4 stream cipher, wherein both these methods are employed together for image encryption. Figure 2.24 shows the block diagram for chaos encryption 3. The

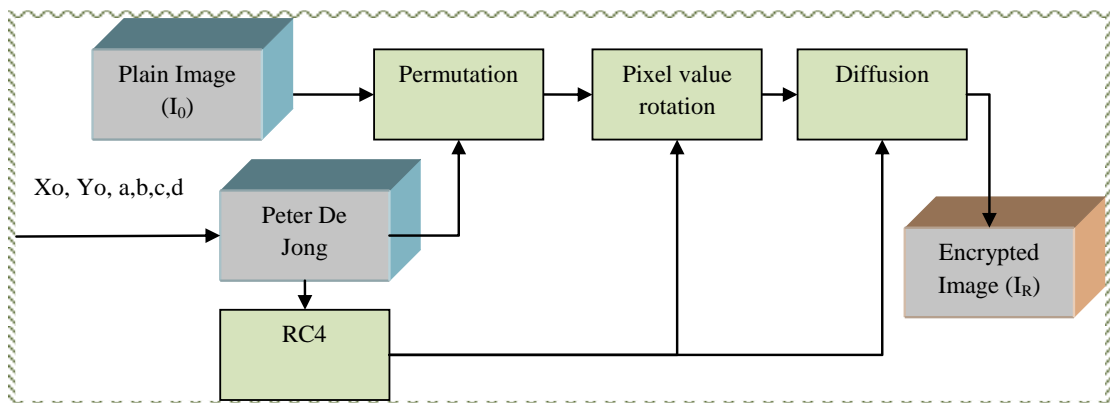


Figure 2.24: Block Diagram for Chaos Encryption 3

Peter De Jong map is used to establish the initial keys for the RC4 stream generator and permutation stage [35] as presented here:

$$X_{(i+1)} = \sin(a \times Y_i) - \cos(b \times X_i) \quad (2.2)$$

$$Y_{(i+1)} = \sin(c \times X_{(i+1)}) - \cos(d \times Y_i) \quad (2.3)$$

Where, X_i , Y_i are the current chaotic values, $X_{(i+1)}$; $Y_{(i+1)}$ are the next chaotic values and a , b , c , d are the control parameters. In this scheme, five set of keys

are given as input to Peter de Jong map to obtain the initial values for RC4 stream generator. These equations are iterated multiple times to get a key set used to determine the initial key values for the RC4 and the permutation process. The RC4 stream generator produces the pseudo-random numbers for the pixel value rotation and diffusion processes. Each round of encryption consists of three stages: permutation, pixel value rotation and diffusion. The first step is based on scrambling and circular rotations of the rows and columns in alternate orientations. The second stage circularly rotates every pixel value by utilizing $ROW \times COL$ pseudo-random numbers. In the last step, diffusion is performed twice, in two different orientations (forward and backward) with two previously diffused pixels and two pseudo-random numbers, which results in a cipher image (I_R). Decryption involves inverse steps to return the plain image (I_0).

- (d) **An Intertwining Chaotic Maps Based Image Encryption Scheme - Chaos Encryption 4:** This is an intertwining chaotic maps-based image encryption scheme in which the cipher provides good confusion and diffusion properties that ensure high security. Figure 2.25 shows the block diagram for the chaos

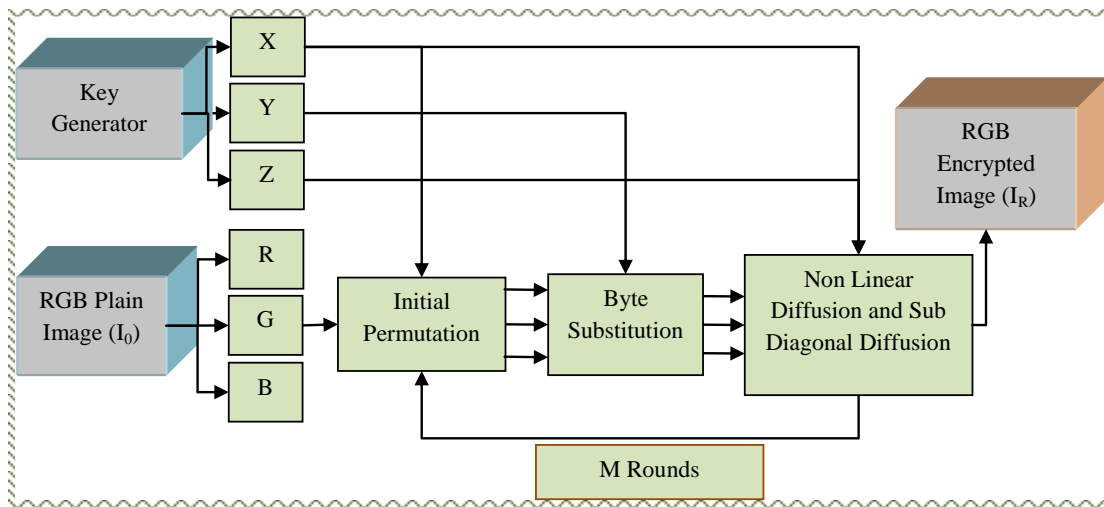


Figure 2.25: Block Diagram for Chaos Encryption 4

encryption 4 mechanism [36]. The system consists of four main phases, permutation, byte substitution, nonlinear diffusion and sub-diagonal diffusion. The permutation of pixel position, the change of pixel value and byte substitution are performed to enable the confusion process. Two rounds of operations are carried out. Six randomly chosen odd integers are used to permute in the substitution process and then XORed with the first chaotic key (X) to shuffle and alter the image pixels. Byte substitution is also applied and the resultant values are XORed with the second chaotic key (Y) to improve the security against the known/chosen-plaintext attack and increase nonlinearity. In

the diffusion process, the pixel values are changed successively with diverse operations, including nonlinear diffusion using the first chaotic key, sub-diagonal diffusion of adjacent pixels and XORing with the third chaotic key (Z), which results in Cipher Image (I_R). The decryption algorithm is just the reverse of the encryption to get the original image; pixel values of the encrypted image are XORed with the same set of secret keys to get the final plain image (I_0).

(e) **An Innovative Image Encryption Scheme based on Chaotic Map and Vigenère Scheme - Chaos Encryption 5:** The image encryption scheme is based on chaotic maps and Vigenère scheme and has each round consisting of two steps: diffusion and confusion [37]. Figure 2.26 shows the block diagram for the chaos

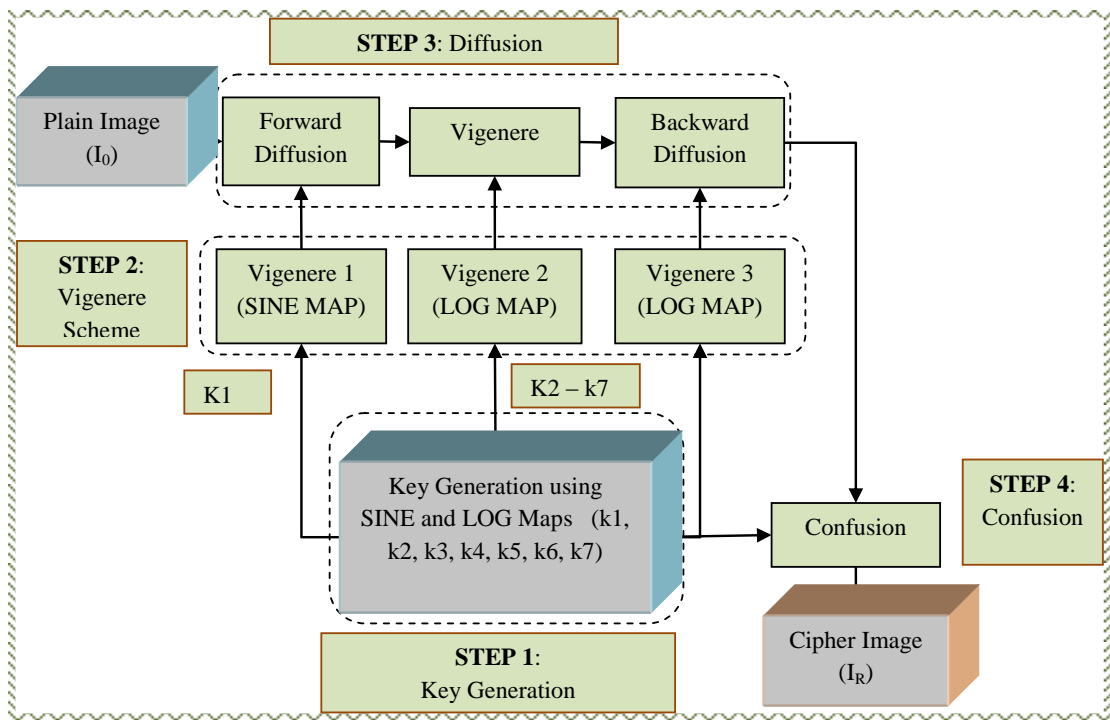


Figure 2.26: Block Diagram for Chaos Encryption 5

encryption 5 mechanism. The defined mechanism consists of four steps; Keys Generation, Vigenère Scheme, Diffusion process and Confusion process. This scheme is based on chaotic maps (Sine and Log Maps), as described below:

Log Map Equation:

$$X_{(n+1)} = r \times X_n(1 - X_n) \quad (2.4)$$

Sine Map Equation:

$$X_{(n+1)} = \sin(\pi \times X_n) \quad (2.5)$$

Where r is the parameter and x_n is the initial value used in the equation having a given range $0 < x_n < 1$ and $0 < r \leq 4$. The first step, keys generation, involves the generation of chaotic sequences using chaotic functions. These sequences will be used in subsequent steps of the process. In the second step, Vigenère Scheme, chaotic sequences are used to generate Vigenère matrices for the diffusion step. During the third, the diffusion step, the plain input image is diffused using forward diffusion, Vigenère and backward diffusion. After this step, a diffused image results and this diffused image goes through the confusion step resulting in the encrypted image (I_R). For decryption, the same set of keys and sequences are employed. However, all processes are implemented in reverse order to get back the original plain image (I_0).

2.2.3 Quantum Chaos Based Encryption Techniques

The chaos based cryptographic scheme has many brilliant advantages compared to traditional algorithms, such as sensitive dependence on initial conditions and control parameters, mixing property, high-efficiency non-periodicity and pseudorandom property. However, it is noted that available chaotic schemes are inconsistent due to some problems related to security and performance problems such as generation of the key stream, small key-space, or the required round encryption time. Since the late 1970s, there have been concerns about what happens if a classical chaotic system becomes quantized, a subject that has now come to be called "quantum chaos" [38–40]. Quantum maps are eventually quantized of classical maps. Quantum chaos theory becomes a tool that can be used to improve the quality of pseudorandom number generators. The randomness and non-periodicity of the quantum-chaotic map are successfully verified by statistical complexity and the normalized Shannon entropy. Therefore, many quantum image watermarking and image encryption schemes have been proposed in recent years [41, 42].

- (a) *A New Approach to Chaotic Image Encryption Based on Quantum Chaotic System, Exploiting Color Spaces - Quantum Chaos Encryption 1*: This is an image cipher, particularly designed for colored images, based on quantum chaotic system. Figure 2.27 shows the block diagram for Quantum Chaos 1 cryptography. The defined scheme comprises four modules: two for confusion and two for diffusion. Firstly, a new substitution scheme is attained based on toral-automorphism in integer wavelet transform by scrambling the low-frequency sub-bands Y (Luminance) component. Then two diffusion modules are applied by integrating the features of horizontally and vertically adjoining pixels with the assistance of a quantum chaotic map. Finally, substitution/confusion is attained by creating a transitional chaotic key stream

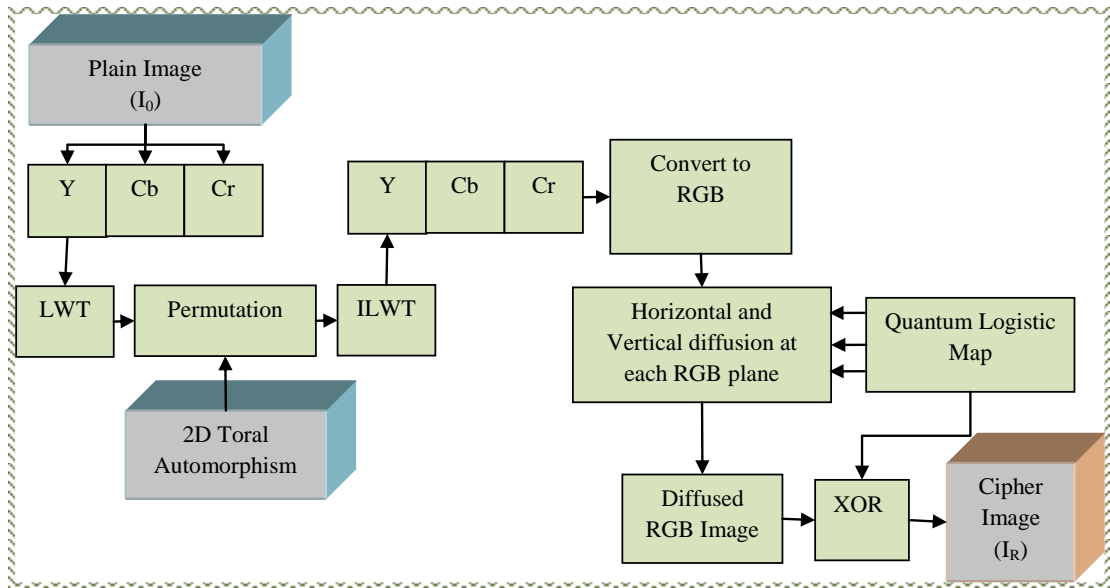


Figure 2.27: Block Diagram for Quantum Chaos Encryption 1

image with the help of a quantum chaotic system [39], which results in a cipher image (I_R). Decryption is the converse of encryption. On the receiver side, using the same round transformations and the same keys, the decryption can be easily derived from the encryption routine and finally, a plain image (I_0) will result.

- (b) **An Image Encryption Scheme Based on Quantum Logistic Map - Quantum Chaos Encryption 2:** A new image encryption algorithm, which exploits the interesting properties of three-dimensional quantum logistic map, is used in this scheme [38]. Figure 2.28 shows the block diagram for the mechanism. The image encryption algorithm consists of the following steps: Initialization phase; initially, keys are defined, same for both directions, i.e., encryption and decryption. These secret keys: x_0 , y_0 , z_0 , r , b , x_n and z_n are given as input to the Quantum chaotic map. Employing these keys, given equations are iterated 1000 times to remove the transients' effect [38]. Repetition of the map equations once, using new initial conditions to get new key values, which are then modified before combining with the plain image. The control parameter (r) is modified using Z_n and plain image values to further affect these values with the help of straightforward arithmetic operations. Each input array element is combined with both keys sequentially using XOR logical operation. This modified value of the plain image is reversed and all the previous steps are repeated to generate the latest key values from new ones. Modification and combination of these values with customized and reversed plain image occurs. Finally, this results in a cipher image (I_R). The decryption process is performed closely analogously, in reverse order to reconstruct the plain image (I_0).

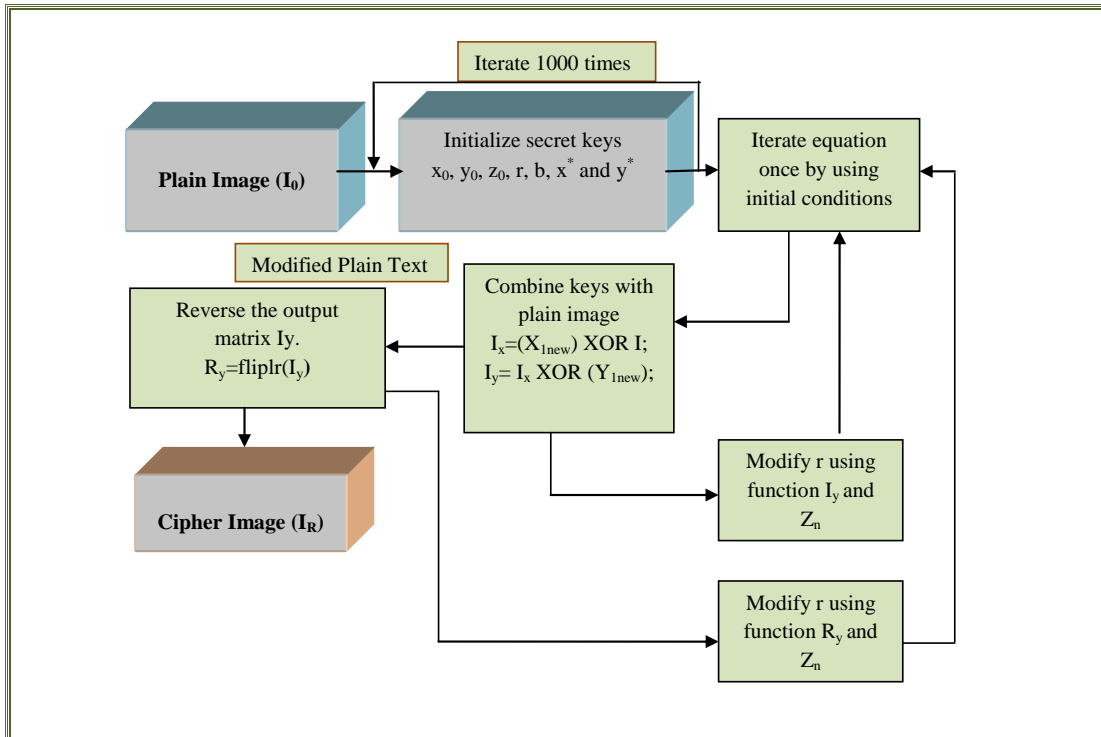


Figure 2.28: Block Diagram for Quantum Chaos Encryption 2

(c) *A Novel Color Image Encryption Algorithm Based on Quantum Chaos Sequence - Quantum Chaos Encryption 3*: This is a quantum chaos based algorithm of image encryption [40]. Figure 2.29 shows the block diagram for

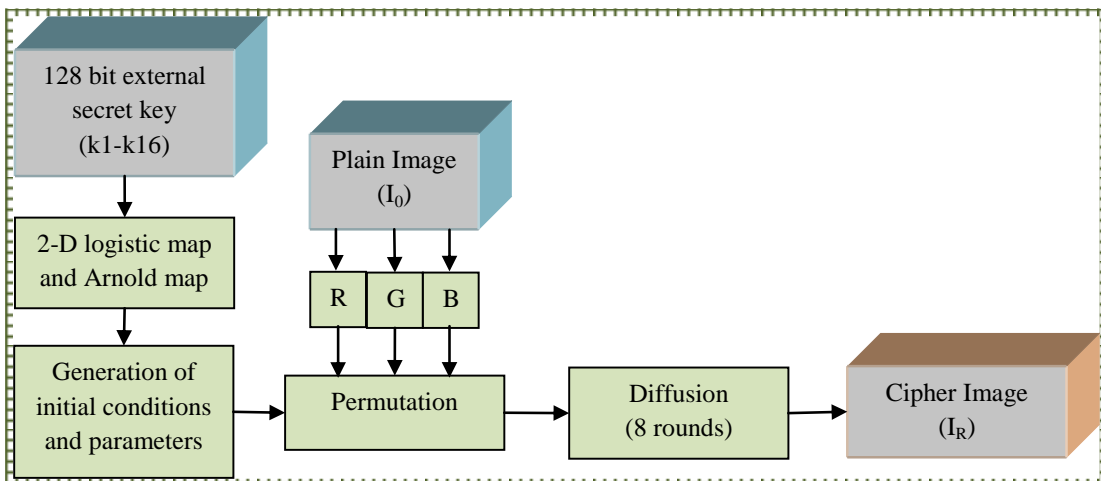


Figure 2.29: Block Diagram for Quantum Chaos Encryption 3

Quantum Chaos Encryption 3. In this scheme, the two-dimensional logistic map generates the key streams as initial conditions and parameters. Further, the general Arnold scrambling algorithm with keys is exploited to permute the pixels of color components. In the diffusion process, a unique encryption algorithm, the folding algorithm, is employed to modify the value of diffused

pixels. The creation of the key stream depends on the 128-bit external secret key, K and the size N of the plain image. Moreover, the quantum chaotic map is applied to create the key streams to modify the value of diffused pixels by “folding the picture,” which gives a cipher image (I_R). The decryption process is similar to the encryption, implemented in reverse order. In this process, opening folded matrices is the first step. Second, applying suitable relations accomplishment of encryption of Arnold transform is done to get the retrieved plain image (I_0).

- (d) **Bit-Level Quantum Color Image Encryption Scheme with Quantum Cross-Exchange Operation and Hyper-Chaotic System - Quantum Chaos Encryption 4:** This is a bit-level quantum color image encryption scheme employing quantum cross-exchange operation and a 5D hyper-chaotic system [41]. Figure 2.30 shows the block diagram for Quantum Chaos

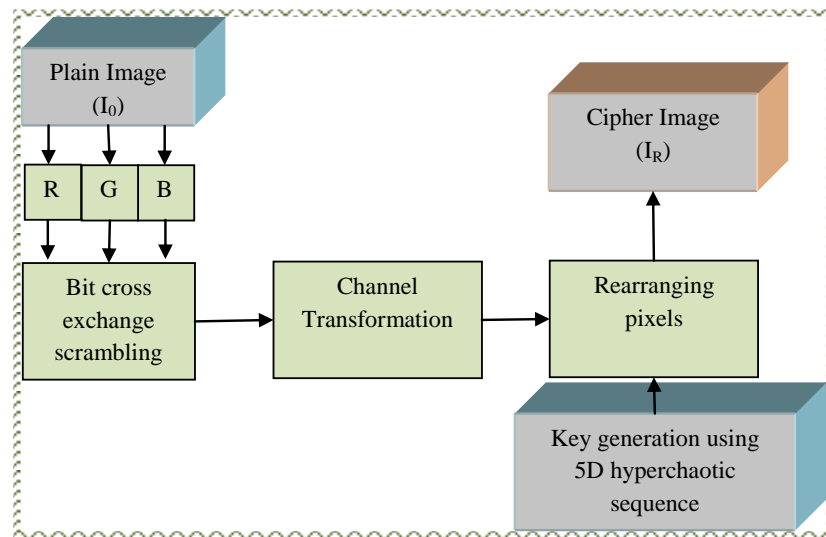


Figure 2.30: Block Diagram for Quantum Chaos Encryption 4

Encryption 4. The encryption process starts with color image representation with the new quantum RGB multi-channel representation for a digital color image. It is followed by image scrambling with the quantum cross-exchange operation, which results in the encrypted quantum color image. The next step is channel transformation. After separating the permuted quantum color image into three grayscale images and rearranging the pixels from row to column, the result is three sequences TR , TG and TB . Further, three sequences are reconstructed into three two-dimensional matrices SR , SG and SB . These three matrices are combined into a three-dimensional matrix, that results in the cipher image (I_R). The decryption process is the inverse operation of encryption. All the initial conditions are the same as encryption.

- (e) **Quantum Image Encryption using Intra and Inter Bit Permutation based on Logistic Map - Quantum Chaos Encryption 5:** This is novel quantum images encryption scheme in which logistic maps are employed along with intra and inter bit permutation operation [42].

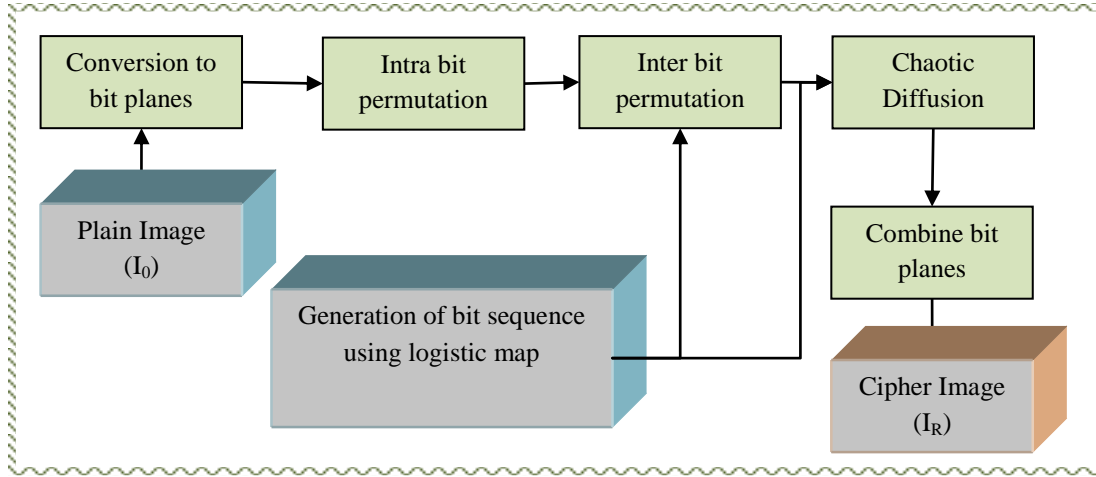


Figure 2.31: Block Diagram for Quantum Chaos Encryption 5

Figure 2.31 shows the block diagram for the Quantum Chaos Encryption 5 mechanism. The complete quantum image encryption process includes three stages, i.e., intra-bit permutation, inter-bit permutation and chaotic diffusion. A novel enhanced quantum representation model initially represents the image to be encrypted and subsequently, the intra and inter-permutation operations are consecutively performed on bit planes. The intra bit permutation is attained by categorizing the chaotic sequence and the inter-bit permutation is performed with qubit XOR operations between the two selected bit planes. The intra bit permutation is performed within each bit plane and alters the bit position. The inter-bit permutation is processed between diverse bit-planes, modifying pixel and gray information simultaneously. The cipher-text image results through a chaotic diffusion process with a quantum image XOR operation. The XOR operation is comprehended by controlling a chaotic sequence generated with a logistic map. The image decryption process is just the inverse of encryption. Therefore the original image can be precisely recovered from an encrypted image with the acceptable factors of the logistic map.

2.2.4 Comparison of Cryptography Mechanisms

In exploring a secure protection mechanism, numerous single layer security mechanisms were proposed and implemented by copious researchers and are available in the literature.

Table 2.4: Performance Parameters for Literature Survey of Cryptography Techniques

Parameters of Comparison	Performance Metrics	Range
<p>Confidentiality of the cryptography mechanism can be judged by analysing key- size and randomness introduced by the algorithm. Key-space analysis is done for gauging key-size and entropy is the measure of randomness.</p> <p>Key-space: It defines the range of combinations for key.</p> <p>Information Entropy Analysis: It defines the randomness in the encrypted image.</p> <p>Differential Attack Analysis: This attack is performed to find out the secret key or original image by comparing the variations in the input with deviations in the encrypted output. It measures the sensitivity of the algorithm under test. High sensitivity to small changes in the plain image provides excellent resistance to differential attacks.</p>	Key-size	Higher than 128 for resisting brute force search attacks [42] (High).
	Entropy	Entropy ≈ 8 (High)
	Number of Pixel Changes Rate (NPCR)	<p>Test passes at the values greater than</p> <ul style="list-style-type: none"> • $N_{*0.05}=99.5693\%$ • $N_{*0.01}=99.5527\%$ • $N_{*0.001}=99.5341\%$
	Unified Average Changing Intensity (UACI)	<ul style="list-style-type: none"> • $U_{*0.05} = [33.284\% - 33.6447\%]$ • $U_{*0.01} = [33.2255\% - 33.7016\%]$ • $U_{*0.001} = [33.1594\% - 33.7677\%]$
Computational Time (CT) is the time required by the algorithm to encrypt a plain image or data to get the resultant decrypted outcome.	Computational time (in Seconds)	The time required for execution should be as low as possible for practical applications. (Low).

Imperceptibility (IMP) is judged by the quantitative and qualitative analysis of results. The resultant image/data should be entirely dissimilar from the original one.	Pixel Signal to Noise Ratio (PSNR) for quantitative analysis. Snapshots for qualitative analysis.	PSNR value should be less than 30dB (Low). Images before and after algorithm, should be entirely dissimilar.
--	---	--

Table 2.5: Comparison of Cryptography Mechanisms

Parameters	CONFIDENTIALITY				CT Analysis	IMP Analysis
	Key-space Analysis					
Cryptography Mechanisms	Differential Attack Analysis				Execution Time (Seconds)	PSNR
	Information Entropy Analysis					
	Key-size key-space	NPCR	UACI	Entropy		
Hierarchical VC [85]	Data Length (L)/ 2^L Variable	Fail	Fail	0.999 Lowest	8.099 High	51.07 Highest
AES [29]	$128/ 2^{128}$ Large	Pass	Pass	7.986 High	1.899 Low	27.17 Low
DES [26]	$64/ 2^{64}$ Smallest	Pass	Pass	7.988 High	8.545 High	26.16 Low
TDES [27]	$168/ 2^{168}$ Large	Pass	Pass	7.950 High	24.064 High	27.13 Low
Vigenère [28]	$128/ 2^{128}$ Large	Fail	Fail	7.730 High	0.851 Low	26.51 Low
RSA [83]	$128/ 2^{128}$ Large	Pass	Pass	7.568 High	5.709 High	8.67 Lowest
RC4 [30]	$256/ 2^{256}$ Large	Pass	Pass	7.955 High	0.259 Lowest	27.20 Low
Chaos Encryption 1 [33]	$462/ 2^{462}$ Large	Pass	Pass	7.985 High	9.178 High	27.08 Low
Chaos Encryption 2 [34]	$192/ 2^{192}$ Large	Pass	Pass	7.985 High	19.199 High	27.18 Low

Chaos Encryption 3 [35]	384/ 2^{384} Large	Pass	Pass	7.963 High	0.619 Low	27.27 Low
Chaos Encryption 4 [36]	192-216/ 2^{192} - 2^{216} Large	Pass	Pass	7.985 High	37.939 Highest	27.14 Low
Chaos Encryption 5 [37]	448/ 2^{448} Largest	Pass	Pass	7.998 High	1.847 Low	26.96 Low
Quantum Chaos Encryption 1 [39]	224/ 2^{224} Large	Pass	Pass	7.984 High	0.788 Low	27.11 Low
Quantum Chaos Encryption 2 [38]	448/ 2^{448} Largest	Pass	Pass	7.999 Highest	0.369 Low	25.32 Low
Quantum Chaos Encryption 3 [40]	128/ 2^{128} Large	Pass	Pass	7.986 High	3.650 Low	27.22 Low
Quantum Chaos Encryption 4 [41]	10^{72} Large	Fail	Pass	7.975 High	9.108 High	27.17 Low
Quantum Chaos Encryption 5 [42]	100/ 2^{100} Small	Fail	Fail	7.956 High	4.846 Low	27.13 Low

The study and implementation of cryptography techniques delve into a meticulous examination of performance parameters, as elaborated in Table 2.4. In tandem, the comparison presented in Table 2.5 underscores the need for a comprehensive evaluation to identify the most efficient cryptography mechanisms. However, due to enormous advantages like very high sensitivity towards initial conditions, key-space, key sensitivity and very high entropy (randomness), having very low correlation coefficient and execution speed, along with high resistance towards brute force search attacks, differential attacks, geometric attacks and noise attacks, quantum chaos encryption mechanism is preferred for the proposed mechanism. Crucially, the encrypted output of the quantum chaos encryption mechanism exhibits a uniform histogram. This uniformity signifies that the encrypted information is distributed without any discernible pattern, rendering statistical analysis futile for intruders.

The current data security landscape presents a stark reality relying solely on standalone techniques such as steganography, watermarking or cryptography is no longer sufficient. The relentless evolution of cyber threats and the escalating occurrences of online data breaches underscore the need for a holistic and multi-faceted approach to safeguarding sensitive information. While valuable in their own right, standalone techniques can only bear the weight of modern security

challenges with help. As in steganography, if intruders recognize minor modifications in a carrier, steganalysis will intimidate data safety. In the encryption mechanism, if an intruder can guess or steal the key, he can easily decrypt the encrypted data. The increasing sophistication of attacks, ranging from advanced persistent threats to intricate social engineering tactics, demands a comprehensive defensive strategy that transcends the boundaries of individual methods. Therefore, researchers have tried to combine both to provide better security.

Next, Chapter 3 reviews the literature for research on multi level security mechanisms, featuring the dual-stage and multiple-stage algorithms.

Chapter 3

LITERATURE SURVEY - MULTILEVEL SECURITY

The previous chapter depicted the diverse security mechanisms proposed and implemented by researchers. The deployment of the individual security layer is inadequate, as the attacks have grown more complicated [2, 11]. Therefore, researchers have tried to combine multiple protection algorithms to provide a high level of security to confidential records and provide better security. The resultant mechanism encodes the data and hides the secret data, making it more difficult for the intruder to retrieve the original confidential information. Information compression plays a vital role in these mechanisms, giving special consideration to network security applications. The compression algorithm helps enhance security by reducing the size of secret information (text/data/image) so that while hiding in the image, fewer locations will be modified. Consequently, it will improve the overall result. There are possibilities of multiple levels of protection, which will result in dual/twin layers of security and multilayered/multilevel techniques described as under.

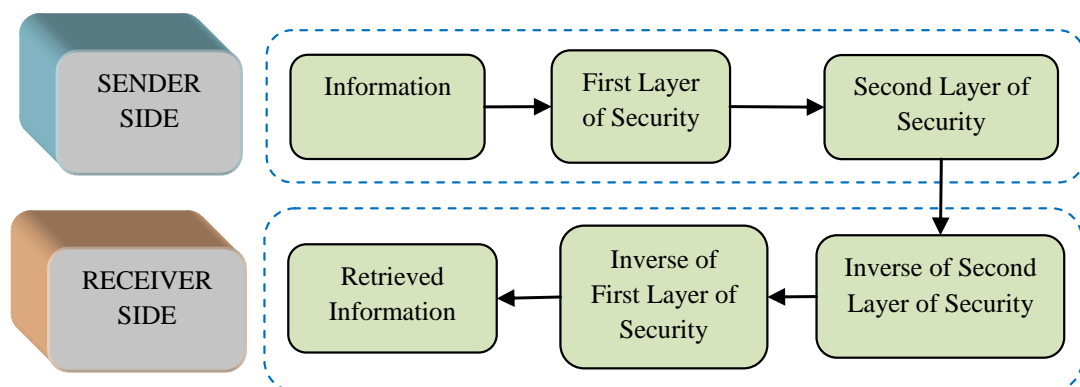


Figure 3.1: General Structure of Dual-level Security Mechanism

3.1 DUAL-LEVEL SECURITY MECHANISMS

Dual/Twin layers security mechanisms combine two divergent protection mechanisms or use identical cascading to enhance defence for secret information. An increase of security threats necessitates combining the multiple techniques, as standalone algorithms provide security up to a specific limit. As per existing mergers, increased layers of appropriately chosen security mechanisms ensure a highly protected system; this is the stimulus behind adding multiple layers to form a highly secure system. Furthermore, a blending of two methods endows with a better shield than the single layer of security, as demonstrated by various researchers [45–47, 55, 63, 86]. Figure 3.1 shows the general organization of the dual-level security mechanism. It consists of a twin level of protection for information to be secured. Figure 3.2 shows diverse dual-layer mechanisms taken for studies and execution.

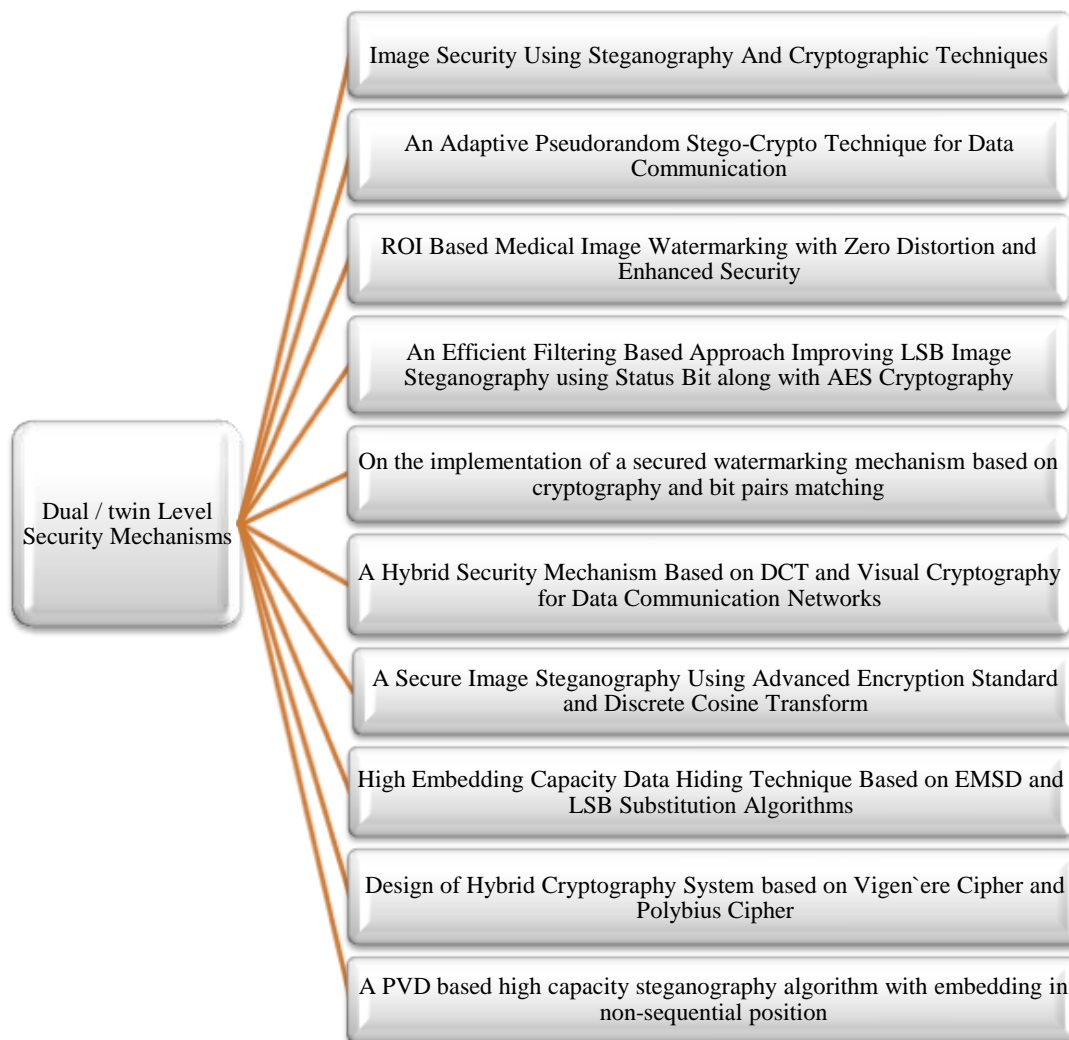


Figure 3.2: Dual-level Security Mechanisms

3.1.1 Image Security using Steganography and Cryptographic Techniques

In this scheme, the hybrid approach consists of cascading cryptography and steganography. Figure 3.3 shows the block diagram showing insight into the given scheme [43]. The first step of security is encryption accomplished by the DES algorithm, which takes an 8-bit block of plaintext and a 10-bit key to produce an 8-bit ciphertext. The second layer of security is the LSB substitution steganography

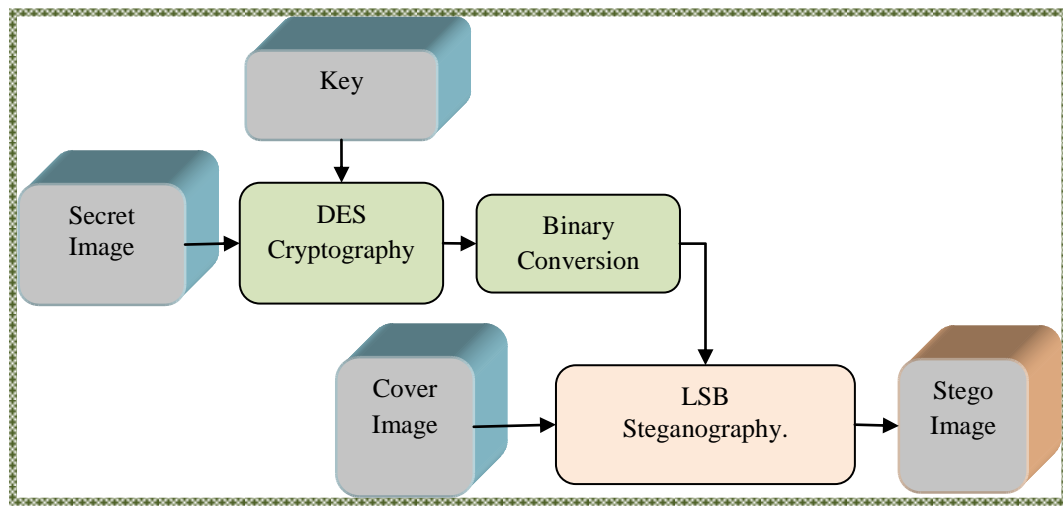


Figure 3.3: Image Security using Steganography and Cryptographic Techniques

mechanism. This is a simple approach to embed information in a cover image. The pixel values of the encrypted image are hidden in the LSB of pixels of the cover image. The proposed method provides a high correspondence between the cover and stego images as per results for better imperceptibility and robustness.

3.1.2 An Adaptive Pseudorandom Stego-Crypto Technique for Data Communication

The given mechanism is an adaptive method taking care of problems encountered in information security. Figure 3.4 shows the block diagram showing insight into the given scheme. It unites the stream cipher cryptographic technique with a modified pseudorandom LSB substitution technique to provide even distribution of ciphertext [44]. The first layer of security is the RC4 encryption mechanism used for the plain text. The second security layer utilizes the identification of the pixels of the cover image, where the ciphertext bits are to be stored. The exact process is followed for both the sender and receiver. To accomplish this, a Pixel Position Number (PPN) array is calculated in which each element indicates a distinctive pixel in the cover

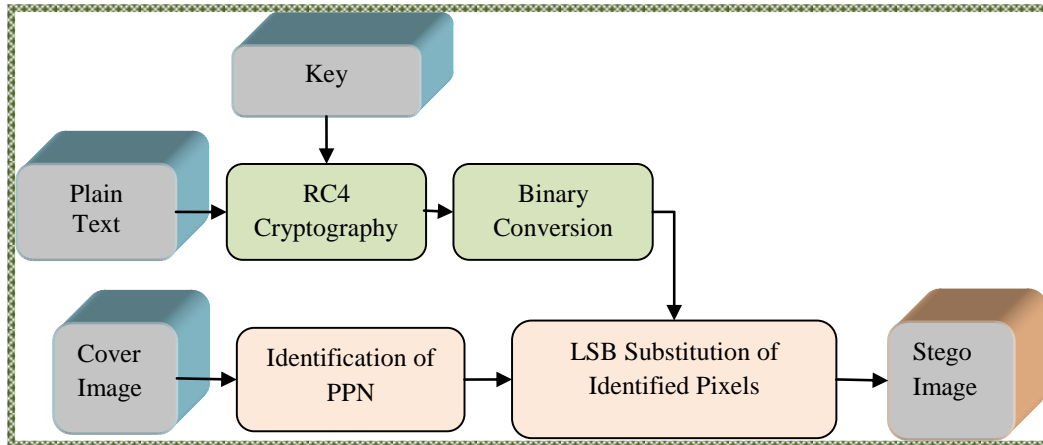


Figure 3.4: An Adaptive Pseudorandom Stego-Crypto Technique

image. This process of generating PPN has seed, length of ciphertext and parameters a , b and c as inputs. Analogous to each value of PPN, the pixel's location in the image is identified by calculating the pixel's height, width and plane, respectively. Then LSBs of the respective pixel are replaced by the encrypted data bits. This completes the embedding process on the sender side. To extract an encrypted message, the receiver needs the seed and length of the message to identify the embedded pixels in the stego-image and the key to decrypt the message can be recognized. The LSBs of these pixels are retrieved as data and decrypted using the reverse RC4 algorithm to obtain an original secret text. In this scheme, the robustness and speed of execution are evaluated/optimized, but randomness, authentication and integrity are not considered.

3.1.3 ROI Based Medical Image Watermarking with Zero Distortion and Enhanced Security

This dual-stage mechanism consists of RSA encryption followed by DWT steganography [45]. Figure 3.5 shows the block diagram showing insight into the given scheme. In this dual-stage mechanism, the RSA cryptography algorithm encrypts the watermark, which is further embedded in the DWT co-efficient of the medical image. Region Of Interest (ROI) is identified before embedding. Image enhancement is done on the cover medical image to identify ROI. The original image is subtracted from the negative image to separate ROI and RONI. The negative image is attained by subtracting the cover medical image from the maximum pixel value (255). That is followed by finding the high-intensity areas to hide the data. These areas can be identified by assigning the minimum and maximum weights. The recognized high-intensity areas are used for hiding the encrypted message. This results in a stego-image. The extraction of the secret message is done by following all the processes in reverse order. This mechanism is employed only for grayscale images and

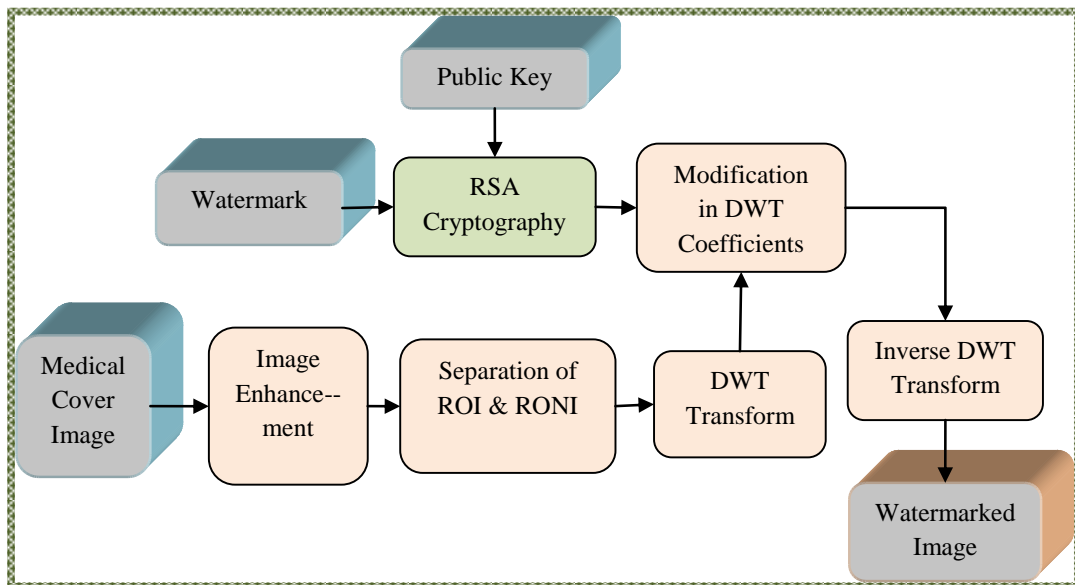


Figure 3.5: ROI Based Medical Image Watermarking with Zero Distortion and Enhanced Security

has very high time complexity due to RSA usage. The proposal is not designed for evaluating/optimizing authenticity, integrity, randomness and execution speed.

3.1.4 An Efficient Filtering based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography

In this proposal, dual-layer security is provided and it consists of two main parts; first is encryption for changing the secret message to ciphertext by AES algorithm and second, hiding the ciphertext into the cover image by a proposed steganography technique [46]. Figure 3.6 shows the block diagram showing insight into the given scheme. In the proposed technique, a new steganography technique is developed using a filtering-based algorithm, which uses MSB bits for filtering purposes. The embedding process is given here: Using the first layer of security, the original message is encrypted with the AES algorithm. The encrypted output is converted into a binary number. The cover image is checked for identification as a lighter or darker image for the second layer of security. Then, the MSB bits from all the pixel planes are taken (Red, Green, Blue) and converted into a decimal number. As per this decimal value and identification of the image as lighter and darker, all the message bits are embedded in the cover image, which results in a stego-image. The extraction of the secret message is done by following the same process of identification. The proposal evaluates/optimizes robustness, imperceptibility and embedding capacity but not authenticity, integrity, randomness and execution speed.

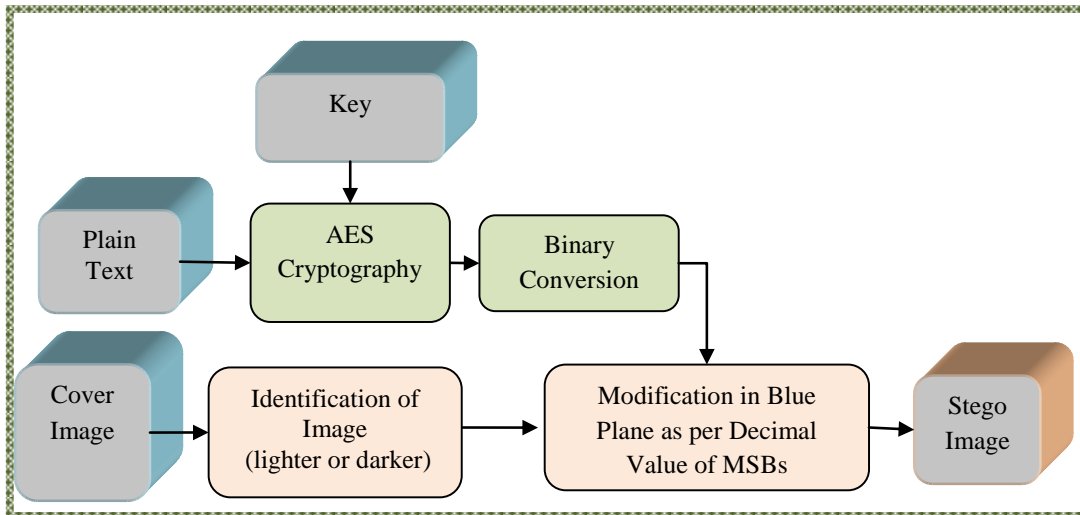


Figure 3.6: An Efficient Filtering based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography

3.1.5 On the Implementation of a Secured Watermarking Mechanism based on Cryptography and Bit Pairs Matching

In this proposal [63], a technique based on the matching of bit pairs is presented. In this, pixel bits of the cover image and the information to be embedded, i.e., watermark image, are arranged in pairs and then after comparison of pairs, replacement of bit pairs takes place with the respective matched pair. Figure 3.7 shows the block diagram

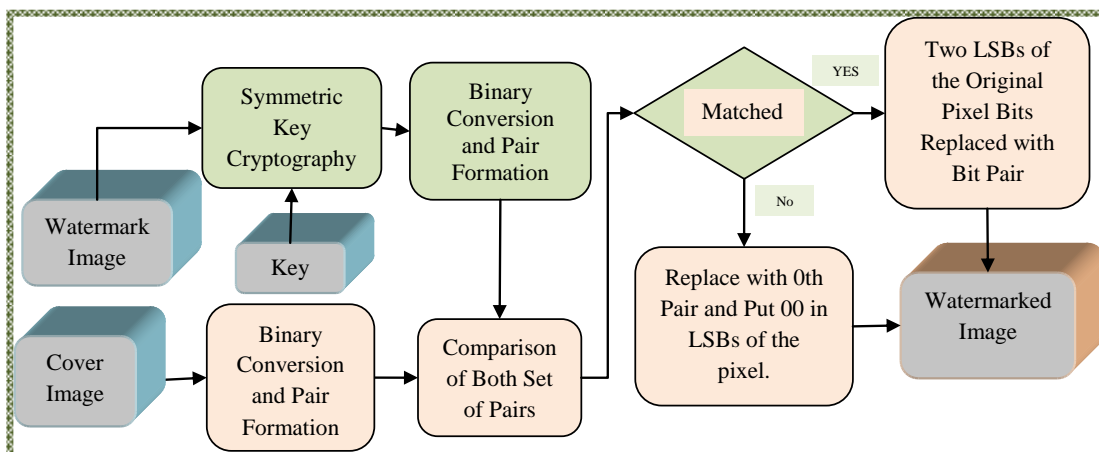


Figure 3.7: On the Implementation of a Secured Watermarking Mechanism based on Cryptography and Bit Pairs Matching

showing insight into the given scheme. Before insertion, the watermark image undergoes symmetric key encryption to enhance security; this is a simple division process with a fixed key in which the remainder and quotient form the resultant cipher. For the decryption of data, the quotient part of the encrypted data is multiplied by the

same key to produce an intermediate result, which is added to the remainder bits of the encrypted data. The second layer of security is steganography based on bit pair matching. Firstly, each pixel of encrypted data is converted to its binary equivalent and then pairs of these bits are formed. In parallel, each original image pixel is converted to its binary equivalent and then four pairs are formed. The resultant bit pairs of both are matched and as per the matching status, watermark bits are embedded in the cover image. This way watermark will be hidden in the original image to form a stego-image. The reverse process is carried out at the receiver side to extract the original watermark. The given mechanism evaluates/optimizes the robustness and embedding capacity, not the randomness and execution speed.

3.1.6 A Hybrid Security Mechanism based on DCT and Visual Cryptography for Data Communication Networks

This twin-layer mechanism introduced the combination of Visual Cryptography (VC) and frequency domain DCT mechanism to provide improved protection for secret information for communication [47]. Figure 3.8 shows the block diagram showing

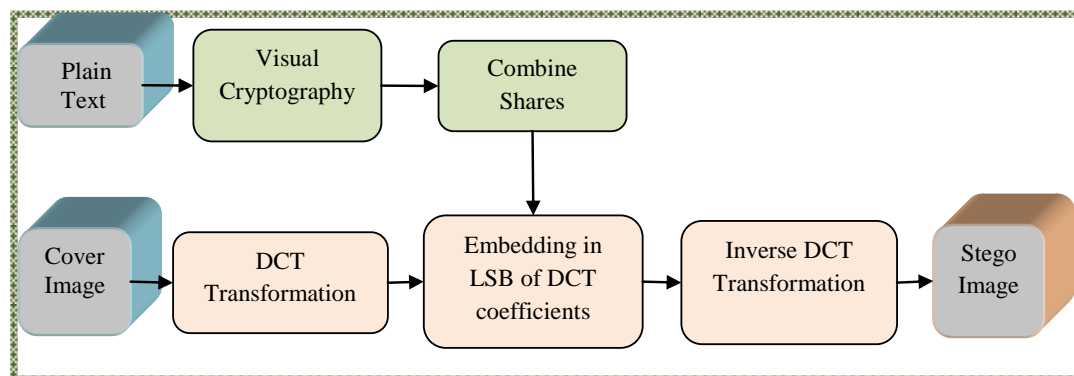


Figure 3.8: A Hybrid Security Mechanism based on DCT and Visual Cryptography

insight into the given scheme. The first stage is encrypting confidential data by dividing it into shares using VC and combined to form an encrypted message. The second layer of security is steganography, in which bits of the encrypted message are stored in the Discrete Cosine Transformed (DCT) cover image to form a stego image, which is finally transmitted over the network. The reverse process is carried out at the receiver side to extract the message again. Using a hybrid approach that combines visual cryptography and DCT (Discrete Cosine Transform) steganography can offer several advantages regarding security, capacity, and robustness for hiding information in images. Usage of this scheme evaluates/optimizes Imperceptibility, robustness and reproducibility.

3.1.7 A Secure Image Steganography using Advanced Encryption Standard and Discrete Cosine Transform

The given proposal is a multilayer security mechanism formed by AES encryption followed by DCT steganography [48]. Figure 3.9 shows the block diagram showing

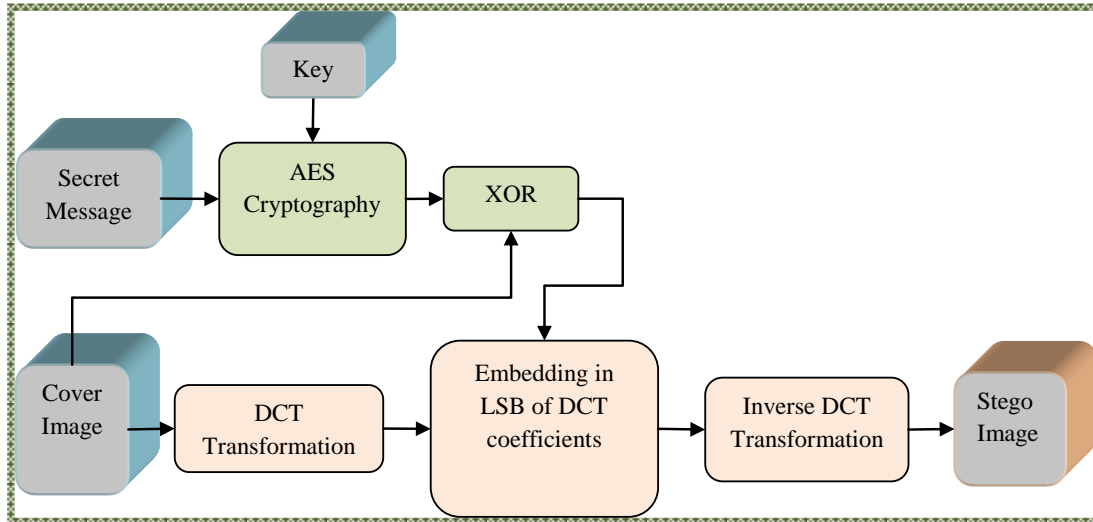


Figure 3.9: A Secure Image Steganography using Advanced Encryption Standard and Discrete Cosine Transform

insight into the given scheme. The first layer of security is formed by encrypting the secret message using the AES cryptography algorithm, which gives a cipher text. The cipher text undergoes XOR operation with the binary converted pixel values of the cover image, which results in modified encrypted data. In parallel, the cover image is frequency-transformed using Discrete Cosine Transformation (DCT). The modified encrypted message is then inserted in the binary converted LSB position of the DCT coefficients of the cover image. Finally, Inverse Discrete Cosine Transformation (IDCT) is performed to obtain a stego-image. The reversed process is carried out at the receiver side to extract the original data. The given mechanism evaluates/optimizes the robustness, imperceptibility and reproducibility but not the randomness and computational complexity.

3.1.8 High Embedding Capacity Data Hiding Technique Based on EMSD and LSB Substitution Algorithms

The Least Significant Bit (LSB) substitution and Enhanced Modified Signed Digit (EMSD) algorithm based, new hybrid image steganography is introduced in this work [49]. Figure 3.10 shows the block diagram showing insight into the given scheme. As seen from the block diagram, two algorithms are being used together; the EMSD algorithm to obtain the new pixel value and then the LSB substitution is

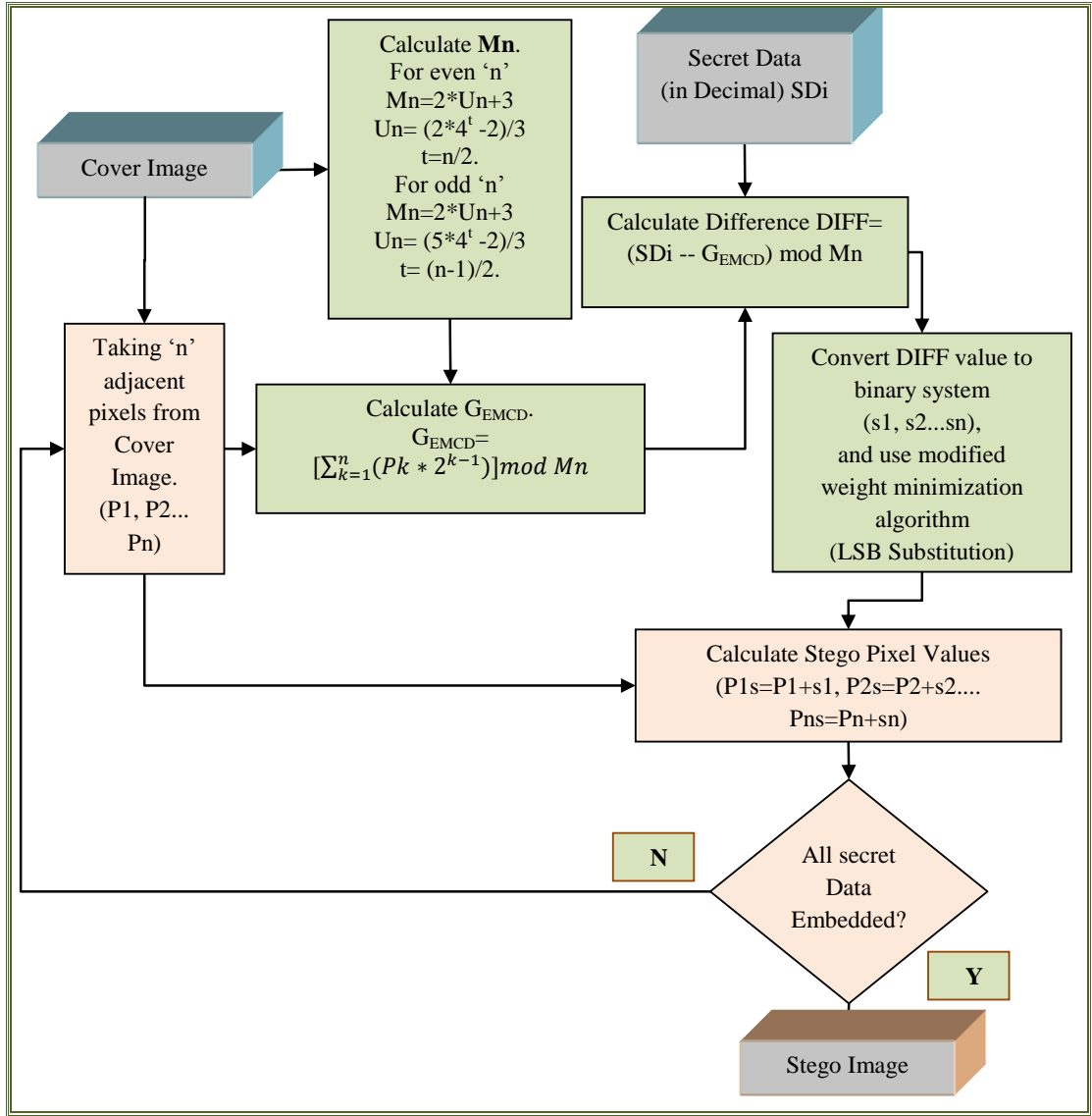


Figure 3.10: High Embedding Capacity Data Hiding Technique Based on EMSD and LSB Substitution Algorithms

implemented using the new pixel values. Initially, the number of integers (M_n) that n -bit EMSD can represent is calculated, where n is the number of adjacent pixels taken from the cover image. Different expressions are defined for even and odd values of n . The next step calculates G_{EMCD} using the given equation.

$$G_{EMCD} = \sum_{k=1}^n \text{mod}[p_k * 2^{(k-1)}, M_n] \quad (3.1)$$

Where, n is number of adjacent pixels, p_k indicates values of adjacent pixels and M_n represents number of integers. In the subsequent step, the difference between secret data in decimal SD_i and G_{EMCD} is calculated, converted to binary form and a modified weight minimization algorithm for EMSD is applied. LSB substitution is accomplished as per weights assigned and modified stego pixel values are calculated.

This way, whole secret data is embedded into the cover image. On the receiver side, the data extraction process will be performed similarly using Enhanced Modified Signed Digit (EMSD) algorithm. The given mechanism evaluates/optimizes the imperceptibility and confidentiality but not the authenticity, randomness and computational complexity.

3.1.9 A PVD based High Capacity Steganography Algorithm with Embedding in Non-sequential Position

In Pixel Value Difference (PVD) scheme, a high capacity steganography is employed in the given twin layer security mechanism. Figure 3.11 shows the block diagram showing

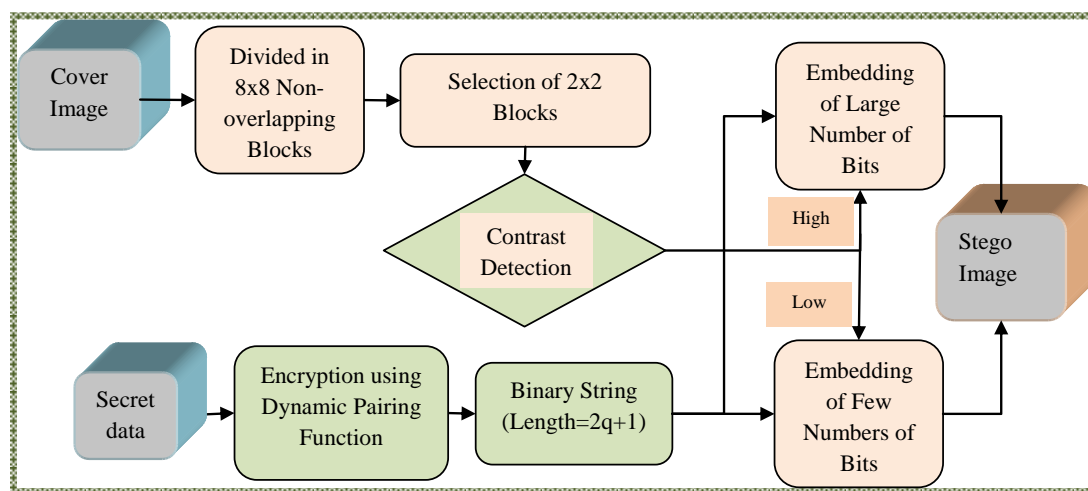


Figure 3.11: A PVD based High Capacity Steganography Algorithm with Embedding in Non-sequential Position

insight into the given scheme. In this, the embedding process utilizes both high and low contrast pixels to store information, thus focusing on PSNR and embedding capacity. Before embedding, the secret message is encrypted using dynamic pairing function methodology. The secret message is converted into a bit-stream by replacing the ASCII value of the characters with the corresponding binary equivalent. The given bit-stream is broken into blocks of $2q$ bits. Now, the encoded value is calculated using given formula:

$$c(e1, e2) = 0.5 \times (e1 + e2 + j)(e1 + e2 + j + 1) + e2 \quad (3.2)$$

Where, $e1$ is equivalent decimal value of, 1 to q bits and $e2$ is decimal equivalent of $q+1$ to $2q$ bits, here $j=1$ and c is encrypted message. Finally, c is converted in binary form of length $2q + 1$ bits resulting in the ciphertext. The second layer of security is embedding in a non-sequential manner with the help of a multi-bit PVD-based steganography algorithm. The embedding mechanism varies depending on whether the

pixel pairs are of low or high contrast. At first, the image is divided into 8×8 non-overlapping blocks. Each 8×8 block is a group of sixteen 2×2 non-overlapping smaller blocks. The smaller block is selected non-sequentially depending on the image's height (h) and width (w), as per the four cases defined here. If $h > w$ and $h \times w$ is odd, If $h > w$ and $h \times w$ is even, If $h < w$ and $h \times w$ are odd, If $h \leq w$ and $h \times w$ is even. Per the given case, a separate set of values is declared [50]. On a selected 2×2 block, embedding is done using PVD based approach. This results in a stego image. The reversed process is carried out at the receiver side to extract the original data. The given mechanism evaluates/optimizes the robustness and embedding capacity but not the randomness and computational complexity.

3.1.10 Design of Hybrid Cryptography System based on Vigenère Cipher and Polybius Cipher

The scheme demonstrated by the author [51] is the combination of two established algorithms, these are, Vigenère cipher and Polybius Square Cipher. Figure 3.12 shows

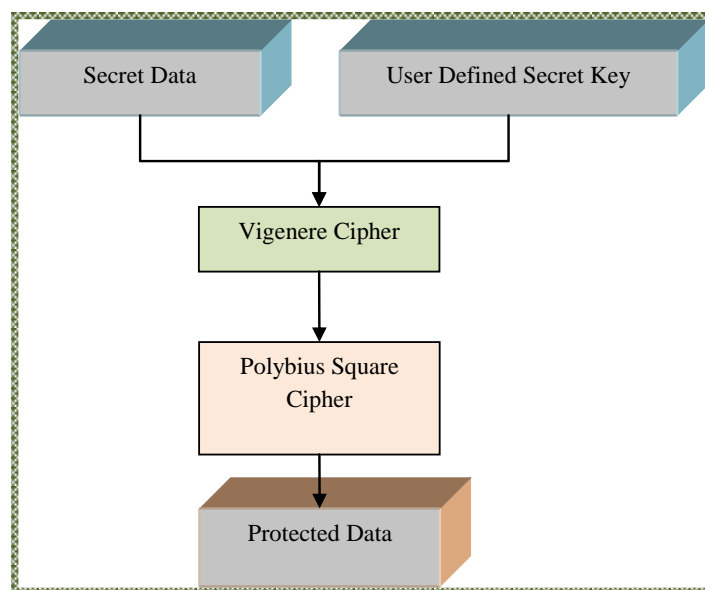


Figure 3.12: Design of Hybrid Cryptography System based on Vigenère Cipher and Polybius Cipher

the block diagram showing insight into the given scheme. The first level of security is introduced by Vigenère cipher with the help of a user-defined secret key and the subsequent level is used by turning ciphertext into a key for the Polybius Square Cipher process. The key is used to modify the plaintext to create the last ciphertext. This cascading results in the last ciphertext hard to be broken. On the receiver side, decryption is done reversely to retrieve the secret information. The given mechanism evaluates/optimizes the confidentiality of the secret information.

3.2 COMPARISON OF DUAL-LEVEL SECURITY MECHANISMS

In the exploration of a secure protection mechanism, numerous dual-level security mechanisms are proposed and implemented by researchers. The following table presents a brief study of the existing mechanism based on security parameters revealed in Table 3.1.

Table 3.1: Security Parameters used in Literature Survey

OBJECTIVES	DEFINITION	ABBREVIATIONS
Confidentiality	It means meaningful data communication between the intended sender and receiver and for all others, the message is meaningless.	CON
Integrity	It signifies data reception at the receiver without any alteration, as the sender sent it.	INT
Authenticity	It ensures the identity of the sender to avoid data communication with pretenders.	AUT
Reproducibility	It indicates complete retrieval of the confidential information by the recipient.	REP
Imperceptibility	It implies the unintended recipient does not perceive data hidden in the carrier.	IMP
Computational Time	It measures the execution time required by a particular algorithm or process.	CT

Table 3.2 presents a concise literature survey of dual-level security mechanisms. To effectively safeguard against potential security breaches, it is crucial to implement additional layers of security mechanisms. For example, a password-based authentication system might be the first layer of protection on a computer system. In case the password is discovered, this can be readily bypassed. Thus, an extra layer of security, like two-factor authentication, can be employed to increase protection. Incorporating multiple layers of security measures can reduce the dangers of security lapses and offer a more secure environment for information to be protected.

Table 3.2: Literature Survey of Dual-level Security Mechanisms

SECURITY MECHANISM	FIRST LEVEL of SECURITY	SECOND LEVEL of SECURITY	CON	INT	AUT	REP	IMP	CT
Nivedhitha, et al. [43], 2012	DES	LSB Substitution	Y	N	N	N	Y	N
Nain, et al. [44], 2013	RC4	Adaptive Pseudorandom	Y	N	N	N	N	Y
Neha Solanki and Sanjay K Malik [45], 2014	RSA	DWT	Y	N	N	N	N	N
Islam, et al. [46], 2014	AES	Status bit using LSB	Y	N	N	N	N	N
Bal, et al. [63], 2018	Symmetric Key Cryptography	Matching of bit pairs	Y	N	N	N	N	N
Jain, et al. [47], 2018	Visual Cryptography (VC)	DCT	Y	N	N	N	Y	N
Tauhid, et al. [48], 2019	AES	DCT	Y	N	N	Y	Y	N
Serdar Solak [49], 2020	Enhanced Modified Signed Digit (EMSD)	LSB Substitution	Y	N	N	N	Y	N
Vatshayan, et al. [51], 2020	Vigenère Cipher	Polybius Cipher	Y	N	N	N	N	N
Paul, et al. [50], 2020	Encryption using Dynamic Pairing Function	Pixel Value Difference (PVD) based steganography	Y	N	N	N	N	N

As demonstrated by various researchers, the amalgamation of two layers of protection endows with a better shield than the single layer of security. There is a wide variety of combinations of layers incorporated by researchers. These can be

cryptography followed by steganography or two consecutive encryption mechanisms. Each proposal provides a different set of security measures as per its capacity. The multiple layers of security provide a more robust and comprehensive approach to security, reducing the risk of data breaches and other security incidents. The above table shows that many researchers have tried diverse combinations, but most of the required objectives still need to be evaluated/ optimized. Thus, other programmers try more levels to get the required protection mechanisms.

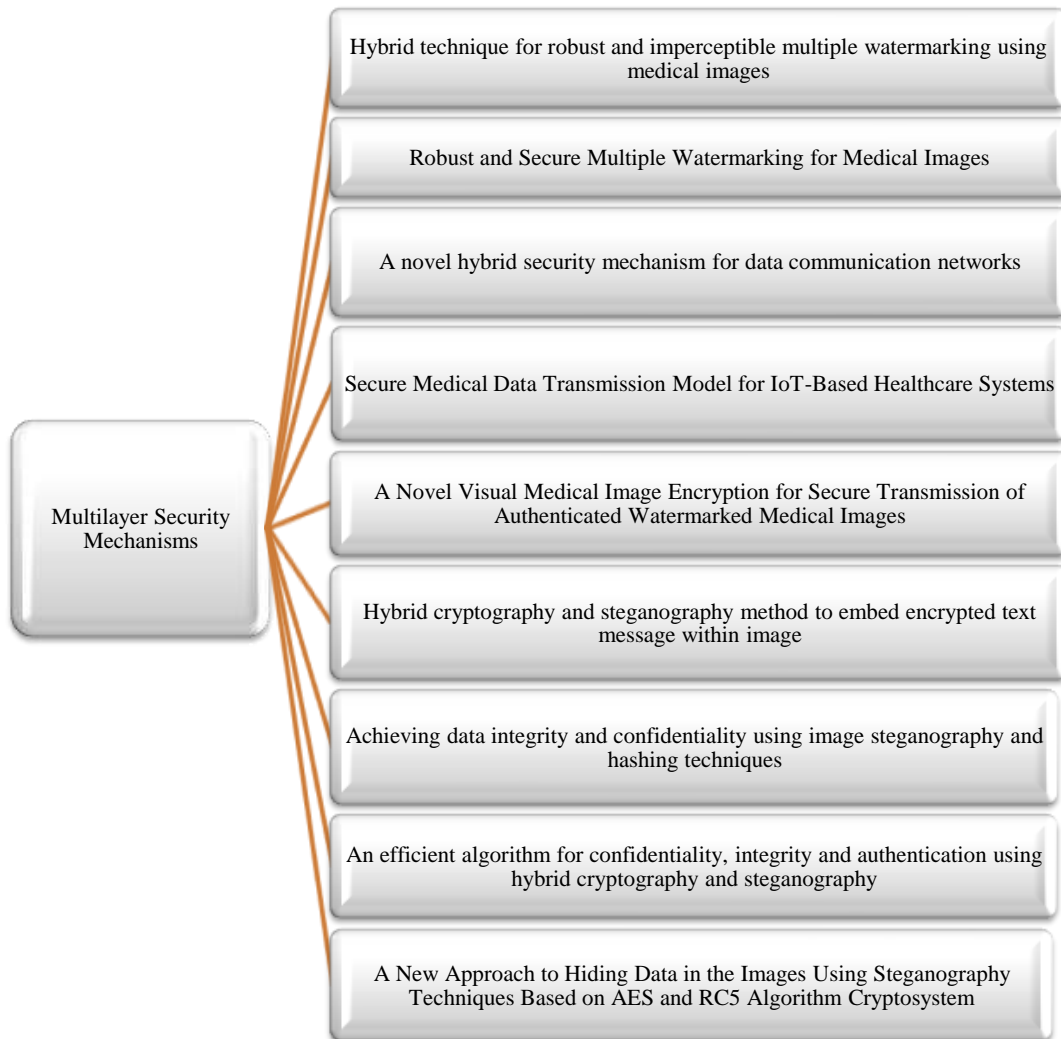


Figure 3.13: Multilevel Security Mechanisms

3.3 MULTILEVEL SECURITY MECHANISMS

As per the previous discussion, a single layer of security is not sufficient to protect vital records; hence multiple stratum are employed to attain requisite enhanced safety. Though copious dual-level mechanisms are available in the literature, with escalating

security threats, the need for further enhanced multilevel protection algorithms for given objectives is always there in the practical scenario [10]. Therefore, researchers in the literature have been proposed an assortment of multilevel schemes. Figure 3.13 gives existing multilayer security mechanisms [18, 52–56, 59, 64, 87] proposed by numerous authors. Concerning security, the requirements of the different fields and sectors include confidentiality, robustness, high speed of execution, imperceptibility and complete reproducibility of data. Next section describes the study and implementation of various mechanisms provided as per the critical requirement of security needs.

3.3.1 Hybrid Technique for Robust and Imperceptible Multiple Watermarking using Medical Images

This is a multilevel security mechanism consists of a layer of cryptography and several layers of frequency domain steganography. Figure 3.14 shows the block diagram showing insight into the given scheme. In this proposal, the application of Discrete

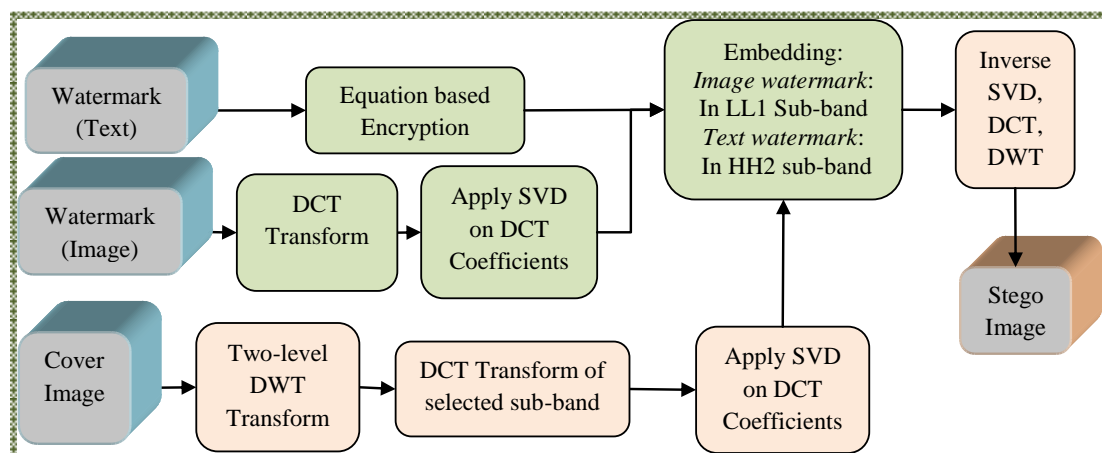


Figure 3.14: Hybrid Technique for Robust and Imperceptible Multiple Watermarking using Medical Images

Wavelet Transformation (DWT), Discrete Cosine Transform (DCT) and Singular Value Decomposition (SVD) is used on cover image [87]. Electronic Patient Record (EPR) is then embedded in singular values of DCT coefficients. EPR is encrypted using an equation-based mechanism before embedding in singular values of DCT coefficients. For identity authentication, the scheme embeds two watermarks in the cover image; one is the medical image as the image watermark and another is the EPR of the patient as the text watermark. The embedding process starts with decomposing the cover medical image up to the second level of DWT coefficients. After this step, the Low-frequency band (LL) of the transformed cover image is further transformed by DCT and SVD. In parallel, the watermark image is also transformed by DCT and

SVD. Now, the modified watermark image's singular values are inserted in the enhanced cover image's singular value. The DWT-composed cover image's second level of the high-frequency band (HH) is used to embed the encrypted text watermark. The final watermarked image is formed by applying an Inverse of SVD, DCT and DWT. On the receiver side, on similar lines, all the processes are applied reversely to retrieve the original medical image and EPR. The given mechanism evaluates/optimizes secret information's confidentiality and imperceptibility but does not provide integrity, randomness and computational time.

3.3.2 Robust and Secure Multiple Watermarking for Medical Images

In the given mechanism combination of Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) is proposed for the embedding of medical image and Electronic Patient Records (EPR) watermark simultaneously [52]. Figure 3.15 shows the block diagram showing insight into the given scheme. In this mechanism,

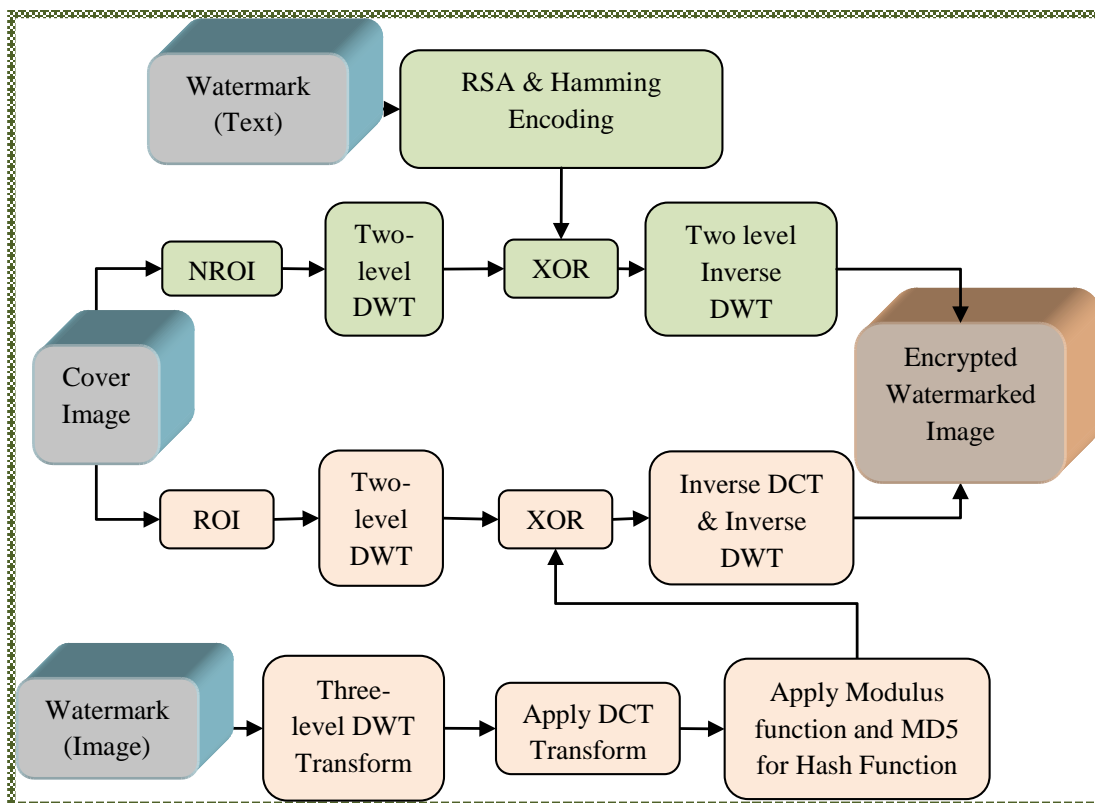


Figure 3.15: Robust and Secure Multiple Watermarking for Medical Images

the embedded process starts with encryption using the RSA algorithm and encoding using hamming coding of the text watermark (EPR), followed by decomposition of the cover image into ROI and NROI regions. Next, the two-level DWT of both regions of

the cover image is determined. In Parallel, three-level DWT and then DCT of the watermark image is calculated. The image watermark is then formatted using the modulus function, which is further used for finding hash functions using MD-5. The hash function of the modified image watermark is XORed with frequency transformed ROI region and the enhanced text watermark is XORed with the NROI region of the transformed NROI region. Finally, both are combined to get a watermarked image, which is encrypted before transmission. The extraction of watermarks is done by following all the processes in reverse order. In this mechanism, confidentiality, imperceptibility, authenticity and integrity are evaluated/optimized, but randomness and execution speed are not.

3.3.3 A Novel Hybrid Security Mechanism for Data Communication Networks

A multilayer security mechanism using Visual Cryptography (VC) followed by Status LSB substitution steganography is presented in this proposal [53]. Figure 3.16 shows

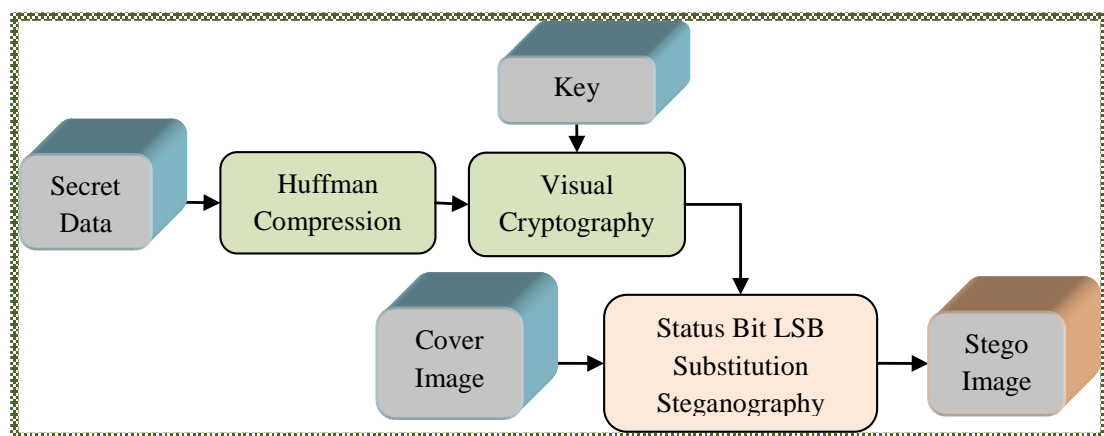


Figure 3.16: A Novel Hybrid Security Mechanism for Data Communication Networks

the block diagram showing insight into the given scheme. The first layer of security is provided by the compression technique, Huffman coding, in this proposal. The second layer is Visual Cryptography (VC), an encryption mechanism. The last layer of security is LSB substitution using the status bit steganography technique. In this scheme, the encrypted message bit is embedded in the LSB of a blue plane of the cover image. The extraction process is just the inverse of the embedding process. This mechanism provides evaluation/optimization for confidentiality, imperceptibility but not for randomness, integrity and execution speed.

3.3.4 Secure Medical Data Transmission Model for IoT-Based Healthcare Systems

This is a multilevel security mechanism that projects a combination of dual encryption and steganography [54]. Figure 3.17 shows the block diagram showing insight into the

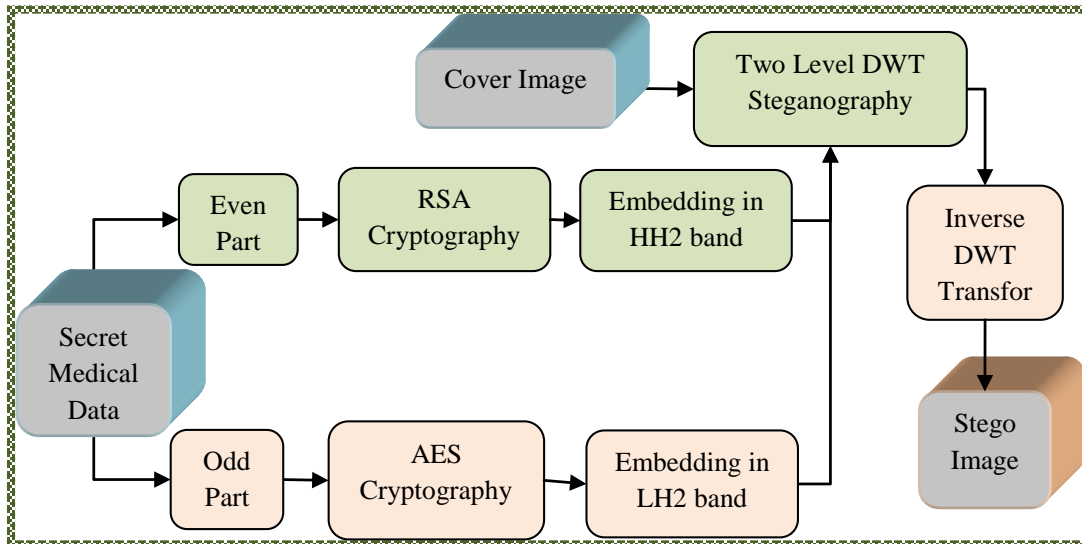


Figure 3.17: Secure Medical Data Transmission Model for IoT-Based Healthcare Systems

given scheme. For encryption, confidential data is partitioned into even and odd parts and then two separate cryptography mechanisms are employed: RSA and AES, respectively. Throughout the encryption process, the confidential data is separated into odd part $DATA_{odd}$ and even part $DATA_{even}$. The AES is used to encrypt $DATA_{odd}$ using a secret public key. The RSA is used to encrypt $DATA_{even}$ using another secret public key. The private key used in the decryption process at the receiver side is secured using the AES algorithm and transmitted in an encrypted form to the receiver to enhance the security level. For the next layer of security, a Haar-DWT steganography mechanism is employed. The odd values are hidden in vertical coefficients LH2 and the even values are inserted in diagonal coefficients HH2. After embedding both shares of encrypted secret data, inverse DWT is calculated, resulting in stego-image, which is communicated through an insecure channel. The extraction process is just the inverse of the embedding process. This mechanism provides evaluation/optimization for confidentiality, imperceptibility but not for randomness, integrity and execution speed.

3.3.5 A Novel Visual Medical Image Encryption for Secure Transmission of Authenticated Watermarked Medical Images

The proposed mechanism is a multilayer security mechanism consists of encryption and LWT steganography [55]. Figure 3.18 shows the block diagram showing insight

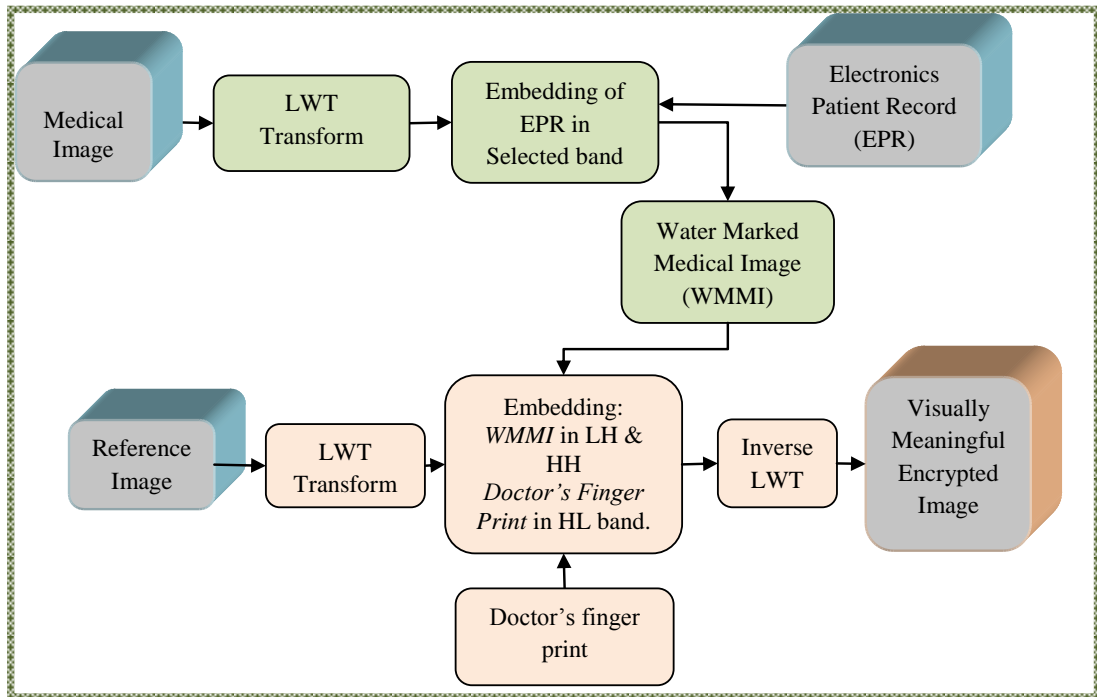


Figure 3.18: A Novel Visual Medical Image Encryption for Secure Transmission of Authenticated Watermarked Medical Images

into the given scheme. In the first layer of security, the Electronic Patient Record (EPR) is taken as a watermark and embedded in a cover medical image using LWT transform with the 'Int2Int' lifting scheme to generate a Water Mark Medical Image (WMMI). The second layer of security constitutes an enhanced visual meaningful image encryption mechanism. The usual image encryption algorithms modify it to a noise or texture-like configuration. Instead, the WMMI is encrypted as a visually significant encrypted image. This is implemented by applying a two-level Integer Wavelet Transform (IWT) on the selected reference image plane. Then the medical watermarked image and the doctor's fingerprint (F) are encrypted using the bands of the transformed image. The last layer of security is provided by authentication, using the doctor's fingerprint image. This image is changed to a binary format and then embedded in the LSB bit of the wavelet coefficients of the transformed reference image. The extraction process is just the inverse of the embedding function. This mechanism provides evaluation/optimization of imperceptibility, confidentiality, authenticity and integrity but not for randomness and execution time.

3.3.6 Hybrid Cryptography and Steganography Method to Embed Encrypted Text Message within Image

The projected model is a multi-stage security mechanism. There are four stages incorporated in this scheme: encryption of the original message using RSA algorithm, embedding the encrypted message in the cover image, extraction of the encrypted message from stego-image and finally, decryption of the ciphertext using the key of RSA algorithm [56]. Figure 3.19 shows the block diagram showing insight into the

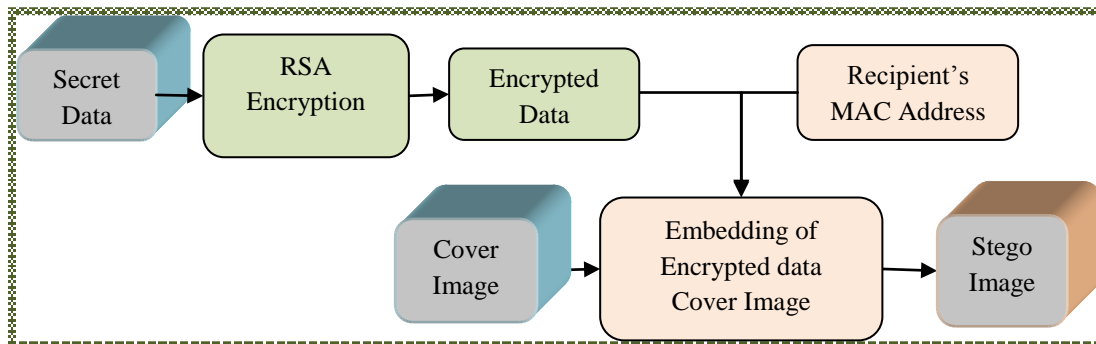


Figure 3.19: Hybrid Cryptography and Steganography Method to Embed Encrypted Text Message within Image

given scheme. As seen from the Figure, this hybrid process consists of an encryption scheme employing an RSA algorithm followed by an LSB steganography mechanism, which hides the recipient's encrypted messages and the MAC address for authentication purposes. So that, at the receiver end, the MAC-Address is checked before giving access to information to the recipient. If this address is found correct, then further process for retrieval of an encrypted message is initiated, followed by decryption of ciphertext to get back the secret message. This mechanism provides evaluation/optimization of authenticity, imperceptibility and confidentiality but not for integrity, randomness and execution time.

3.3.7 Achieving Data Integrity and Confidentiality using Image Steganography and Hashing Techniques

The projected scheme accomplished data confidentiality as well as integrity. The former is achieved by secretly embedding the data bits into the cover image and the latter is achieved using function SHA-256. Figure 3.20 shows the block diagram showing insight into the given scheme. The projected model has four stages: new image addressing, text size hashing, encoding and decoding. The image addressing process is used to reserve 512 bits to store vital information; the actual image size is obtained by subtracting 512 from the selected image size. These 512 pixels are halved

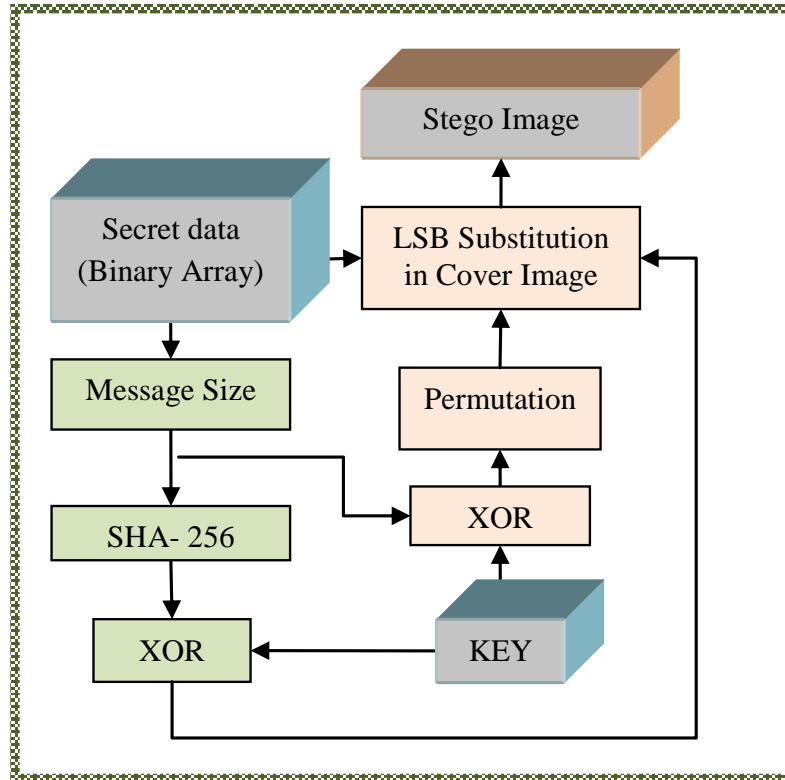


Figure 3.20: Achieving Data Integrity and Confidentiality using Image Steganography and Hashing Techniques

for storing the permuted encoded message size and the hashed message size. The text size hashing is obtained using SHA-256 and the resulting hash value is XORed with the shared key (K) and then stored in the second half of reserved pixels of the image [57]. The encoding process is categorized into two parts: calculating the address for embedding the text bit and embedding the text bits in the encoded cover image to produce a stego-image. The decoding stage is also categorized into two parts: retrieving the values of both halves stored in the last 512 pixels, extracting the message bits from the stego-image, and converting them to the original text (plaintext). In this mechanism, confidentiality, execution speed and integrity are evaluated/optimized, but randomness, imperceptibility and authenticity are not.

3.3.8 An Efficient Algorithm for Confidentiality, Integrity and Authentication using Hybrid Cryptography and Steganography

In this scheme [58], multiple security algorithms have been applied. Figure 3.21 shows the block diagram showing insight into the given scheme. A random number (X) is generated and used as a Key for the symmetric AES algorithm. The secret message is

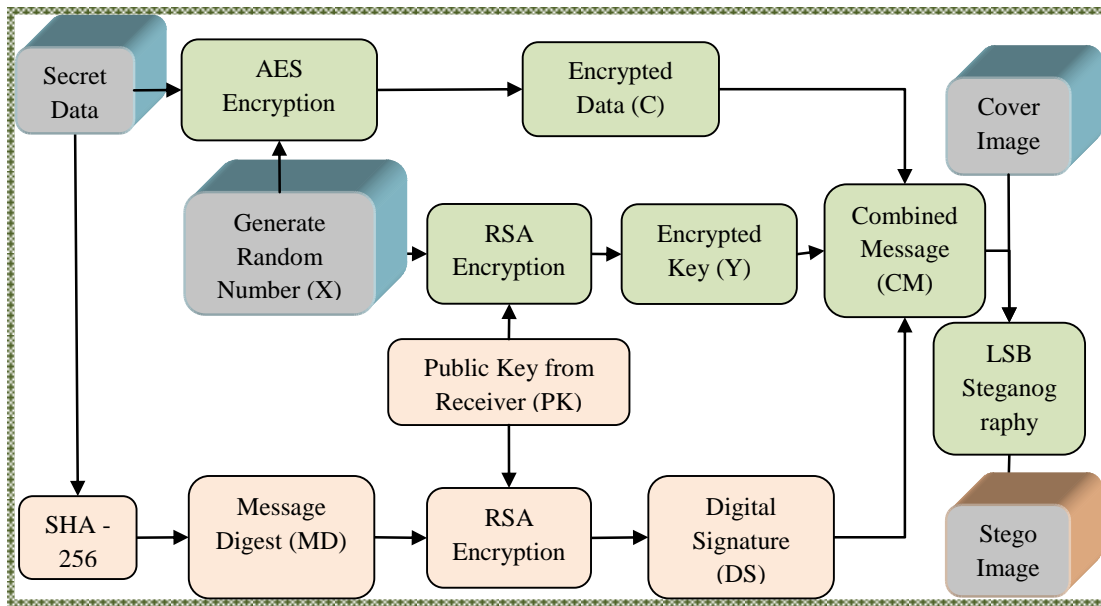


Figure 3.21: An Efficient Algorithm for Confidentiality, Integrity and Authentication using Hybrid Cryptography and Steganography

encrypted using AES and gives output Cipher-text (C). Confidential data's Message Digest (MD) is generated using the SHA-256 hash function. The key for the AES scheme (X) and Message Digest (MD) are both encrypted using RSA employing Public Key (PK), shared by the receiver, that results in an encrypted key (Y) and Digital Signature (DS), respectively. In the next step, the encrypted data (C), the Digital Signature (DS) and the encrypted key (Y) are combined to form a Complete Message (CM). Lastly, the message (CM) is embedded in the cover image using the LSB substitution steganography mechanism, which results in a stego image. For retrieval of information, all the processes are employed in reverse order. In this mechanism, confidentiality, imperceptibility, authenticity and integrity are evaluated/optimized, but randomness and execution speed are not.

3.3.9 A New Approach to Hiding Data in the Images using Steganography Techniques based on AES and RC5 Algorithm Cryptosystem

In the projected model [59], initially, the secret message undergoes dual encryption processes and later, using DCT watermarking completes the protection mechanism. Figure 3.22 shows the block diagram showing insight into the given scheme. The security process begins with a secret message encrypted with AES and RC5. When the message is encrypted, the stego object generates a watermark; subsequently, the stego object returns to the public network after employing DCT based watermarking mechanism. At the receiver end, after the arrival of the stego-object, the watermark is

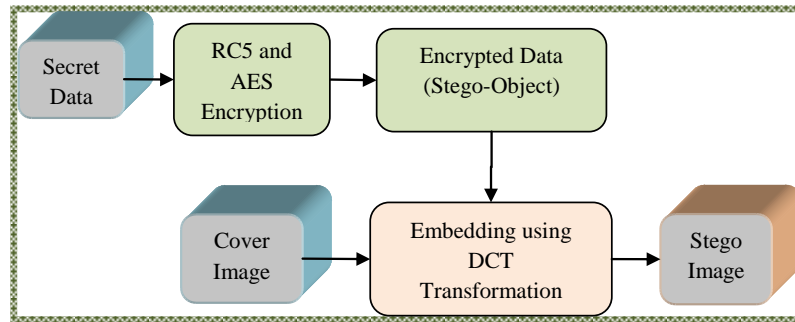


Figure 3.22: A New Approach to Hiding Data in the Images using Steganography Techniques based on AES and RC5 Algorithm Cryptosystem

removed from it and further decrypted with AES and RC5 to return the original secret message. This mechanism provides evaluation/optimization of imperceptibility and confidentiality but not for authenticity, integrity, randomness and execution time.

3.4 COMPARISON OF MULTILEVEL SECURITY MECHANISMS

In exploring a secure protection mechanism, numerous multilevel security mechanisms available in the literature are studied and implemented. The defined table presents a concise literature survey of multilevel security mechanisms based on security parameters revealed in Table 3.1. A blending of numerous methods endows with a better shield than the single layer of security, as demonstrated by various researchers. This chapter portrayed the existing dual-level and multilevel security mechanisms. As seen from Tables 3.3 and 3.2, presenting a concise literature survey of dual and multilevel security mechanisms, the schemes are designed to provide complete protection of the secret information (text/image), but still, all the objectives are not evaluated/ optimized by a single mechanism; also instances of online information exposure and data breaches are increasing.

This gap between requirement and availability motivates designing a protection mechanism to optimize all the objectives. After studying and implementing single-layer and multilayer methods in the preceding chapters, two mechanisms are presented in the following chapters to fulfill the diverse requirements of network security. The first proposal is the multilayer protection techniques designed to accomplish confidentiality, imperceptibility, reproducibility, integrity and authenticity. Another multilayer security mechanism focusing on confidentiality, imperceptibility, reproducibility and time/ speed requirements is projected in the second scheme.

Table 3.3: Literature Survey of Multilevel Security Mechanisms

SECURITY MECHANISM	FIRST LAYER of SECURITY	SECOND LAYER of SECURITY	ADDITIONAL LAYERS of SECURITY	CON	INT	AUT	REP	IMP	CT
Singh, et al. [87], 2016	Equation based Encryption	DWT Steganography	DCT and Singular Value Decomposition (SVD) Steganography	Y	N	N	N	Y	N
Sharma, et al. [52], 2017	RSA, Hamming Code	DWT	DCT, MD-5 Hashing Function	Y	Y	Y	N	Y	N
Chaudhary, et al. [53], 2016	Huffman Compression	Visual Cryptography (VC)	LSB Substitution using status bit	Y	N	N	N	Y	N
Elhoseny, et al. [54], 2018	AES Encryption (Odd part)	RSA Encryption (Even part)	Two level 2-D DWT Steganography	Y	N	N	N	Y	N
S Priya and B Santhi [55], 2019	LWT with Int2Int lifting scheme	Visual meaningful image encryption	Fingerprint Biometric Authentication	Y	Y	Y	N	Y	N
Jassim, et al. [56], 2019	RSA	LSB Substitution	MAC Address Testing	N	N	Y	N	Y	N
Hambouz, et al. [57], 2020	New Image Addressing and Confusion	Text Size Hashing (SHA-256)	Encoding (Identification of locations followed by embedding)	Y	Y	N	N	N	Y
Biswas, et al. [58], 2019	AES	LSB Substitution	RSA, Digital Signature	Y	Y	Y	N	Y	N
Hossen, et al. [59], 2020	RC5	RSA	DCT	Y	N	N	N	Y	N

Chapter 4

MULTILAYERED HIGHLY SECURE AUTHENTIC WATERMARKING MECHANISM FOR MEDICAL APPLICATIONS

In the previous chapters 2 and 3, diverse single-level and multilevel schemes were presented. This chapter initiates the research investigations by developing and testing a new scheme that combines multiple security algorithms to secure confidential information in medical applications.

4.1 CONTRIBUTION

As per the sternness of security need, researchers had put in lots of effort to propose numerous combinations of different security mechanisms to form a scheme that can save fragile medical information and the telehealthcare sector can flourish [45, 52, 54, 55, 60, 86–93]. Numerous dual-level and multilevel schemes are implemented in literature. As per the requirements of the medical healthcare field, [4, 94] it is observed that confidentiality, biometric authenticity, integrity, imperceptibility and reproducibility (data extraction) are the foremost objectives. Only some techniques are available which are fulfilling most of these agendas. The motivation behind this work is to accomplish all these goals. For that purpose, the main contributions of the proposal are:

- **Confidentiality** is achieved by hiding compressed (using lossless Huffman compression) and encrypted (using Quantum based encryption algorithm) Electronic Patient Record (EPR) in medical image and then embedding WaterMarked Medical Image (WMMI) (shuffled using Arnold transform and compressed using lossless Huffman compression) in Lifting Wavelet

Transformed (LWT) Reference image.

- **Authenticity** is acquired by including biometric verification of the doctor. Under biometric, reliable IRIS identification and then verification at the receiver side restricts access to EPR and medical image only to an authorized person.
- For **maintaining Integrity**, a hash algorithm is employed. It generates a hash function for detected IRIS value. This value is compared with the Hash value formed with biometric of doctor (IRIS value) at the receiver side. If matched that means integrity is achieved and all received information is unaffected.
- **Imperceptibility** feature ensures that the hidden information, in any case, isn't visible to the outside world. This is acquired by using appropriate algorithms (LWT watermarking and steganography) and regions (LH, HL and HH frequency bands) for embedding sensitive information. High values of PSNR and correlation coefficient confirms high imperceptibility.
- **Reproducibility** or data extraction is attained, by retrieving EPR with no Bit Error Rate (BER) at the receiver side. Also, the medical image with a very high value of PSNR and correlation coefficients and low bit error ensures this property.
- Newly introduced concept of the **visually meaningful encrypted image** is used, by transmitting reference image containing all relevant medical information (EPR and medical image) instead of the medical image containing EPR, on to the insecure channel, so that it should be considered as an ordinary image (instead of information loaded reference image). Also employing of simple encryption algorithm provides a noise-like or texture-like format. So, communication of noise-like image alarms the attackers that some information is present in the modified format which eventually leads to a large number of attacks.

The following section, 4.2, gives the detail of the proposed multilayer model, followed by explaining each building block of this technique in sections 4.3 to 4.8. Next, section 4.9 provides the setup parameters. A comprehensive analysis of results is done in section 4.10, followed by the conclusion.

4.2 PROPOSED MECHANISM

This proposal portrays a multilayer, highly secured healthcare security model that will protect the patient's medical information. Electronic Patient Record (EPR) consists of text information about the patient and medical images like X-Rays, CT-scan, MRIs, etc.

are secured with the help of this mechanism. The process for the proposed technique (sender side) is described in Figure 4.1 and explained as follows.

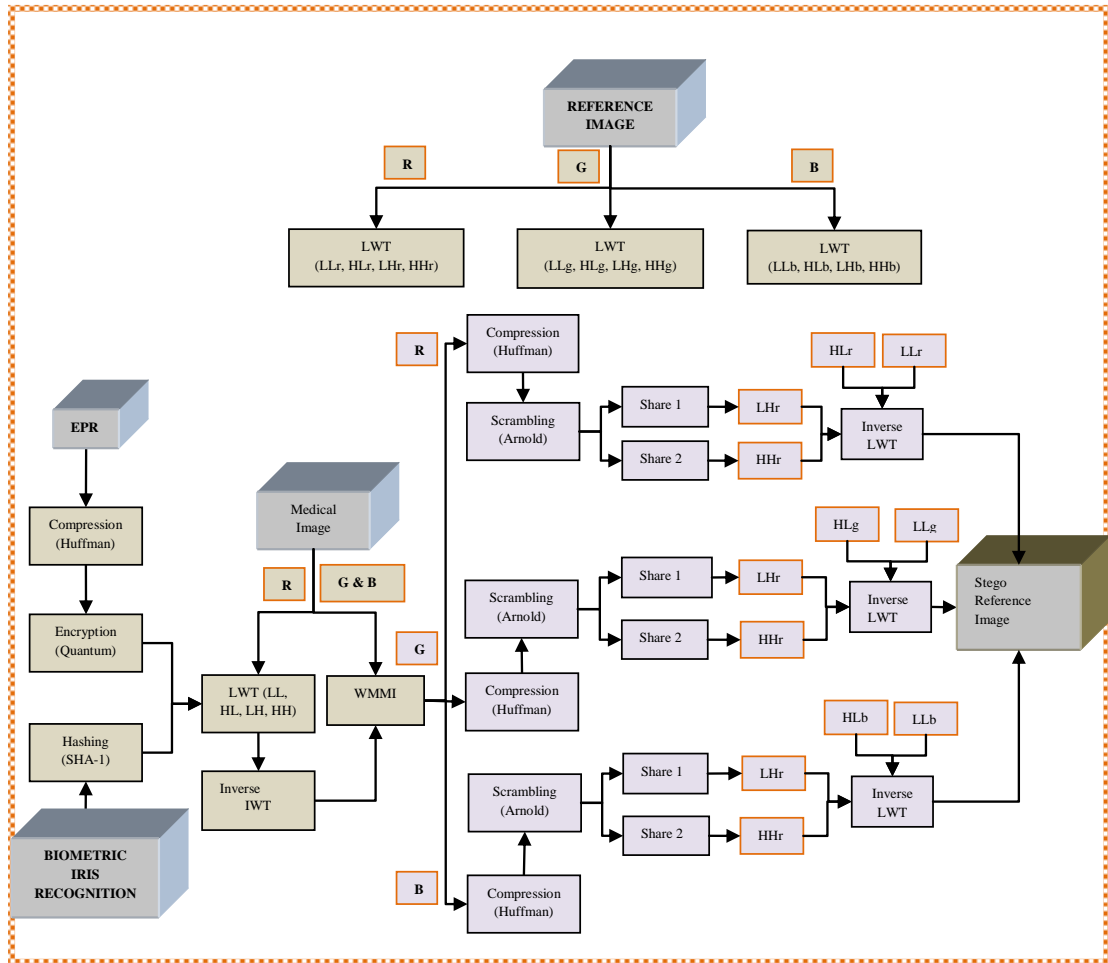


Figure 4.1: Proposed Model for Sender Side

- In the first step, data to be secured EPR is compressed using the Huffman compression algorithm to reduce its size for increasing embedding capacity and imperceptibility.
- This compressed EPR is then encrypted using a cryptography scheme based on a Quantum logistic map to obtain encoded records.
- For authentication, the IRIS of the authorized person (Doctor) is captured and converted to a binary template. The hash algorithm (SHA-256) calculates this template's hash value, which is also embedded in Cover Medical Image for maintaining the system's integrity.
- The medical image to be secured is used as a cover image for hiding this modified EPR and hash value of the biometric template.

- All planes (R, G, B) of the cover image are separated and then the Lifting Wavelet Transform (LWT) is applied on each plane for transforming into different frequency bands (LL, HL, LH, HH).
- As per the information size, either two or more bands can be utilized for storing customized records and hash values; these results in Watermarked Medical Image (WMMI).
- This WMMI is separated into three color planes and then each plane is scrambled using Arnold transformation, a permutation algorithm.
- Each shuffled plane is then compressed using a lossless Huffman compression algorithm to increase embedding capacity and imperceptibility. All compressed planes are partitioned into two shares before embedding into a reference image.
- The reference image is used for hiding modified WMMI. First, this cover image is prepared by separating it into different color planes and then transforming each plane into a frequency domain to form diverse frequency bands using the LWT steganography algorithm.
- All the resultant shares of WMMI are embedded into selected frequency bands (HH and LH) to sustain the perceptibility of the reference image.
- Embedding is followed by inverse LWT and grouping of all color planes, which results in a stego-reference image ready to move in an open network without giving even little indication to any unauthorized individual.

Receiver side consists of all stages in reverse order to get back the EPR for the intended recipient. The process for the proposed technique (receiver side) is described in Figure 4.2. The next section will describe all the blocks in detail, with the justification of the selection of each algorithm used in this proposal.

4.2.1 Huffman Compression

The first action performed in this work is the reduction of EPR using one of the popular compression techniques, Huffman compression. This method works on the principle of frequency calculation of each character or value in given data and then replacing it with code [71]. It efficiently reduces the data size by assigning shorter codes to frequently occurring symbols and more extended codes to less frequent characters. This reduced data size requires less storage space, which is advantageous in security applications with limited bandwidth and storage. Its process is explained in algorithms 1 and 2. Table 4.1 shows the compression results for text as well as image.

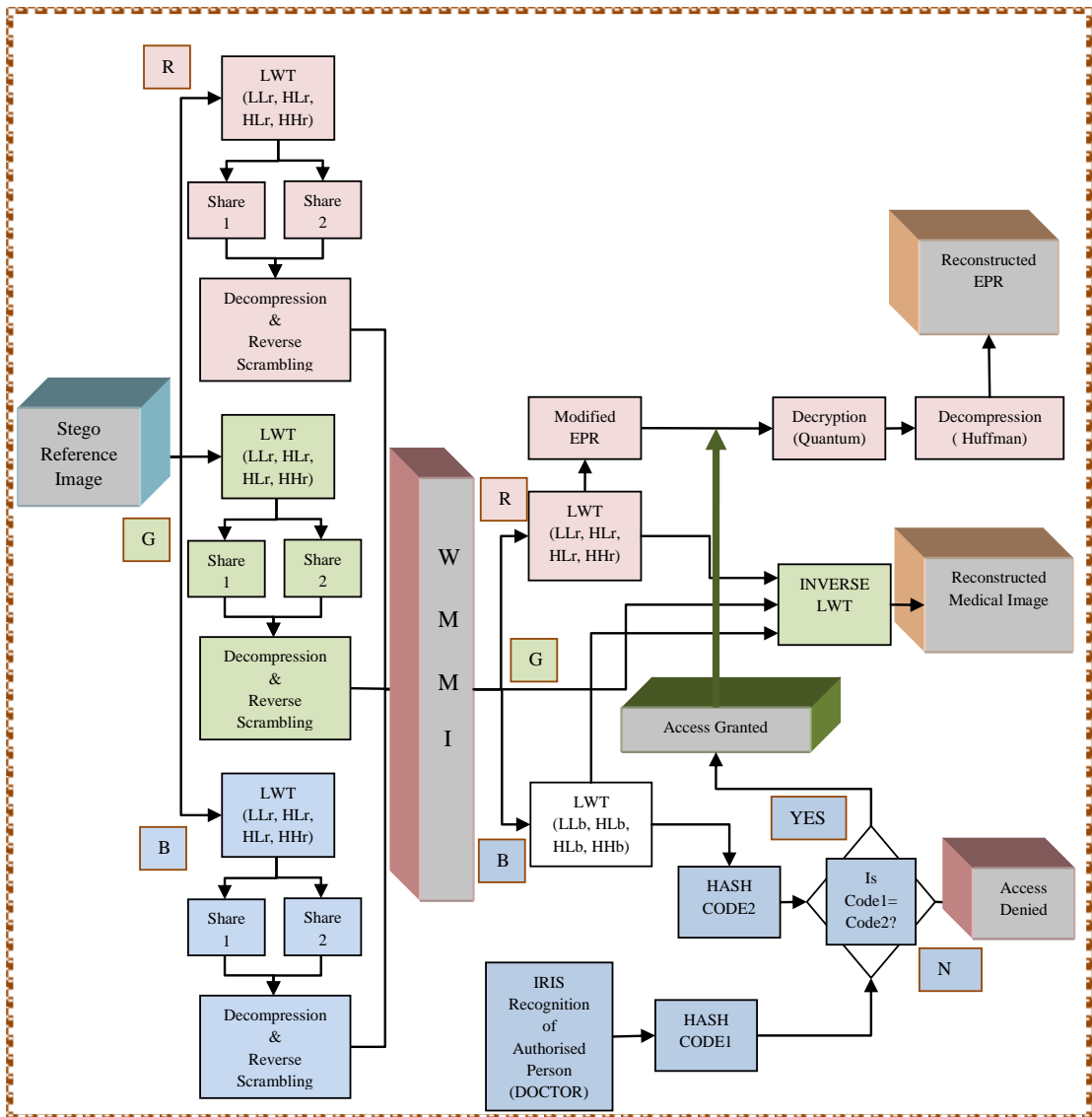


Figure 4.2: Proposed Model for Receiver Side

Table 4.1: Compression Rate using Huffman Compression

Compression Rate		
Information to be compressed	Compression rate	
Data set (text records): <ul style="list-style-type: none"> Ten set of EPR of size 110 bytes are used for testing. 	41%	
Medical Images: <ul style="list-style-type: none"> Five different medical images are used. Each colour plane is compressed separately. 	Red	35%
	Green	35%
	Blue	35%

These results justify the inclusion of this stage in the proposed model. A reduction in the size of the information to be embedded enhances the embedding capacity as

well as the perceptibility of the cover image. After reducing the size of EPR, it is encrypted before hiding in the medical image. This way, the compression mechanism also provides the first layer of security in the overall system. This algorithm is used at two positions, first in the beginning, for EPR and second for reducing all the planes of scrambled watermarked medical images.

Algorithm 1 Pseudocode for Huffman Compression

```

1: INPUT: Information to be Compressed = data
2: OUTPUT: Compressed Huffman Code = hcode
3: STEP 1: Initialize All Possible Symbols In Input Data.
4:   symbols =0:255;
5: STEP 2: Probability Of Each Symbol In Data Is Calculated
6:   prob=ones(1,length(symbols));
7:   flag1=0;
8: for J=min(symbols):max(symbols) do
9:   for I=1:LENGTH(data) do
10:    if data(I)== J then
11:      flag1=flag1+1;
12:    end if
13:  end for
14:  prob(j+1)=flag1/length(data);
15:  flag1=0;
16: end for
17: STEP 3: Dictionary Is Created With The Use Of Symbols And Probability Of Each
    Symbol In Data.
18:   dict = huffmandict(symbols,prob);
19: STEP 4: Huffman Code For Each Character Of Data Is Identified Using Data And
    Dictionary.
20:   hcode= Huffmanenco(data,dict);
21: STEP 5: Obtain The Huffman Code hcode.

```

Algorithm 2 Pseudocode for Huffman Decompression

```

1: INPUT: Compressed Huffman Code = hcode
2: OUTPUT: Original Data = recovered-data
3: STEP 1: Formation Of Dictionary Or Acquire Dictionary From Receiver Side.
4: STEP 2: Original Value Of Each Data Value Is Identified Using Huffman Code
    And Dictionary.
5:   recovered-data= huffmandeco(hcode,dict)
6: STEP 3: Obtain The Original Data recovered-data.

```

4.2.2 Encryption

Cryptography is admired and widely used for securing any information. After reducing EPR, it undergoes encryption to provide the next layer of security. Although

many algorithms are available in the literature, in the current era, widespread studies are going on in the field of chaos and quantum-chaos based cryptography schemes. Due to enormous advantages, as described in [81, 82, 95] quantum chaos encryption mechanism is used in the proposal. As shown in Figure 4.3, this scheme has optimized values of many desirable parameters.

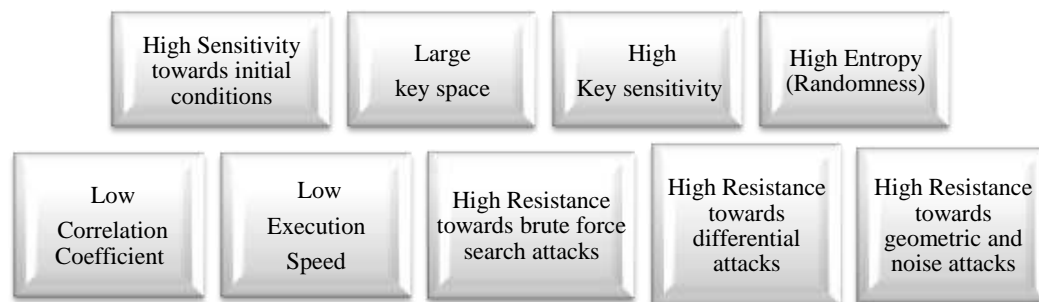


Figure 4.3: Advantages of Quantum Chaos Encryption mechanism

The encryption process is described in Algorithm 3. This mechanism offers a uniform histogram of encrypted information compared to conventional, which means the intact values in cipher text are uniformly dispersed, showing no definite pattern. Thus gives a highly uncorrelated description of the original data. That's why the correlation coefficient is also very low for this technique. Initially, keys are defined, which should remain the same for both directions, i.e., encryption and decryption. These secret keys are $X(0)$, $Y(0)$, $Z(0)$, r , b , $X'(n)$ and $Z'(n)$, which are given as input to the Quantum chaotic map [38]. Employing these keys, given equations will be iterated 1000 times to remove transients' effect. The figure 1000 is optimized value as per the experimental result of reference [96].

Decryption process is performed closely analogous, in reverse order. Keys used are same in both processes. In decoding process cipher text is firstly combined using XOR operation with the latest keys. This partial result will get reversed and then amalgamation with a new key will be done in a similar fashion. This results in reconstructed plain text. As seen from Figure 4.3 cryptography using a Quantum logistic map has numerous excellent qualities. There is one imperative criterion, given by [97], to evaluate the strength of image encryption algorithms/ciphers for differential attacks and that is the Number of Pixel Changes Rate (NPCR) and the Unified Average Changing Intensity (UACI) randomness tests. This technique cleared both these tests and proved to be one of the strongest algorithms for encoding. All the above-mentioned considerations offer the motivation to choose this mechanism for secured protection mechanism. The next part gives insight into IRIS recognition steps.

Algorithm 3 Pseudo-code for Quantum Chaos Encryption Mechanism

- 1: **Input:** Initial Keys= X(0), Y(0), Z(0), r, b, X'(n) and Z'(n); Plain Text=I;
- 2: **Output:** Cipher Text= C;
- 3: **Step 1:** Initialize All Initial Keys And Input Plain Text I.
- 4: **Step 2:** Iteration Of Following Logistic Map Equations 1000 Times, To Avoid The Transient Effect, Using The Initial Conditions And Control Parameters Initialized In The Previous Step.
- 5: **for** I = 1 to 1000 **do**

$$\begin{aligned}X(n+1) &= r \cdot (X(n) - |X(n)|^2 - r \cdot Y(n)) \\Y(n+1) &= -Y(n) \cdot e^{-2b} + e^{-b} \cdot r \cdot [(2 - X(n) - X'(n)) \cdot Y(n) \\&\quad - X(n) \cdot Z'(n) - X'(n) \cdot Z(n)] \\Z(n+1) &= -Z(n) \cdot e^{-2b} + e^{-b} \cdot r \cdot [2 \cdot (1 - X'(n)) \cdot Z'(n) \\&\quad - 2 \cdot X(n) \cdot Y(n) - X(n)]\end{aligned}$$

- 6: **end for**
 - 7: **Step 3:** Repeat The Map Equations Once Using New Initial Conditions (Calculated In Step 2) To Get New Key Values (Xnew, Ynew And Znew). These New Key Values Are Modified Before Combining With Plain Text.
 - 8: $X1\ new = \text{mod} ((\text{floor} (Xnew(1,1) * (2^{32})), 2^{32});$
 - 9: $Y1\ new = \text{mod} ((\text{floor} (Ynew (1,1) * (2^{32})), 2^{32});$
 - 10: **Step 4:** The Control Parameter (r) Is Modified Using Z And Text Values I With The Help Of Straightforward Arithmetic Operations To Affect Plain Text Values Further
 - 11: **Step 5:** Each Element Of Input Array Is Combined With Both Keys Sequentially Using Xor Logical Operation.
 - 12: $I_x = X1newxorI;$
 - 13: $I_y = IxxorY1new;$
 - 14: **Step 6:** This Modified Value Of Plain Text Is Reversed And All The Steps From 2 To 4 Are Repeated, For Generation Of Latest Key Values From New Key Values
 - 15: **Step 7:** Modification And Combination Of These Values With Customized And Reversed Plain Text Occurs. Finally, This Results In Cipher Text C.
 - 16: **Step 8:** Obtain The Cipher Text C.
-

4.2.3 Biometric Recognition

Biometric detection is a rising technology in which more attention has expanded in recent years. It utilizes mainly physiological features to identify a being. The physiological characteristics include a fingerprint, IRIS, face, thumb impression and hand geometry. Amongst these traits, the IRIS has many advantages compared to others as listed in Table 4.2 [62, 98]. However, the elevation in cost compared to traditional biometric technologies is one of the overheads for its usage. Nevertheless, no compromise authenticity makes it an obvious choice. An iris recognition system has three main stages, image pre-processing, feature extraction and template matching.

These are illustrated as follows:

- **Image Pre-Processing:** The input IRIS image necessitates being pre-processed to attain a practical iris region. This stage is divided into three steps:
 - IRIS localization: It perceives the inner and outer borders. Other undesirable parts of eyes like eyelids and eyelashes are detected and removed.
 - IRIS normalization: This stage converts iris image from Cartesian coordinates to Polar coordinates. The resultant normalized IRIS image is a rectangle image with angular resolution and radial resolution.
 - Image enhancement: The image generated after normalization stage has low contrast and inconsistent illumination due to the location of the light source, which can be surmounted by the image enhancement algorithms.

Table 4.2: Advantages of IRIS Recognition

Accuracy	It is one of the best biometric modalities in terms of accuracy. The FAR and FRR are stumpy in this modality, consequently ensuring a higher rate of correctness in results.
Scalability	Being highly scalable this technology can be used in both large and small scale programs. It has already been deployed in many large scale applications including the relevant government's biometric authentication programs in several countries across the world.
Distance	IRIS scanning can be done from an ordinary distance unlike retina scanning. It is very similar to clicking a normal photo, which can be taken from the regular distance of taking pictures.
Steady	IRIS pattern remains steady all through a person's life. It is confined by the body's own system.
Easy to use	This biometric system is plug and play in comparison to other modalities of biometric identification. Stand still position of a person is required, in front of the camera for accomplishment of capturing instantly.
Speed	Whole process of recognition requires just fraction of a second. In case the prior enrolment has taken place, it works faster than other modalities. From subsequent enrolment, a camera will capture the IRIS followed by the matching system and finally send the report instantly.
Non-intrusive and Non-invasive	For IRIS scan physical contact with the person isn't required. Due to no direct contact between camera and entity this method is non-intrusive and non-invasive.

Hard to counterfeit	The complete IRIS recognition system is hard to falsify by any ways, this makes it simple and secure. This biometric modality is deployed in a lot of countries, but data breach records of this modality are rare.
Glass/Contact lenses	Usage of contact lenses or glasses doesn't affect the iris recognition process. Although these devices are very close to the eye still the process remain unaffected.
Unpredictability	The degree of randomness of IRIS pattern is very high which makes each IRIS exclusive. As an instance, the variability IRIS has 244 degrees-of-freedom and the entropy has 3.2 bits per square-millimetre.
Pupil Size	The varying pupil size validates the accepted physiology of an iris. However it doesn't modify the IRIS pattern.
Security	As IRIS is an internal organ of the eye. That's why, IRIS pattern never alters in a life span. Being an internal organ, it is highly shielded compared to retina recognition.
Traceable	The encoding and assessment of IRIS pattern is extremely appreciable. It takes only 30 milliseconds for the image analysis and the successive encoding.

- **Feature extraction:** This stage employs texture analysis techniques to extract features from the normalized IRIS image. The important features of the iris are extracted for precise recognition intention.
- **Template matching:** Finally, template matching contrasts the user template with templates from the database using a matching process. This correspondence process will confer a measure of resemblance between two iris templates. This results in a set of values after comparison with a similar IRIS template and a different set of values when compared with the dissimilar template.

Ultimately, a conclusion of a high confidence level is made to identify whether the user is an authentic or a pretender. The source code for a Biometric Identification System Based on Iris Patterns offered by [99] is used in this proposal. The template obtained by this code is further passed through a hashing algorithm to obtain hash code for providing integrity to the overall mechanism. Hash code acquired after this algorithm will be stored in a medical image along with modified EPR so that on the receiver side hash code of the IRIS-recognized template is compared with the retrieved code. If any intentional or unintentional change has been encountered, access to the original EPR and Medical image will be denied and an error message will be displayed, "Authentication cancel-wrong Biometric detection." The subsequent section describes the hashing algorithm used in the procedure.

4.2.4 Hashing Algorithm

For providing integrity to the design, hashing algorithm is included. Integrity is an essential aspect of data security that protects data against alteration, inclusion and removal by any contender. Hashing is a procedure to convert original records into a shorter span message i.e. hash code using a hash function. Hash code is a cryptographic checksum of original record [100].

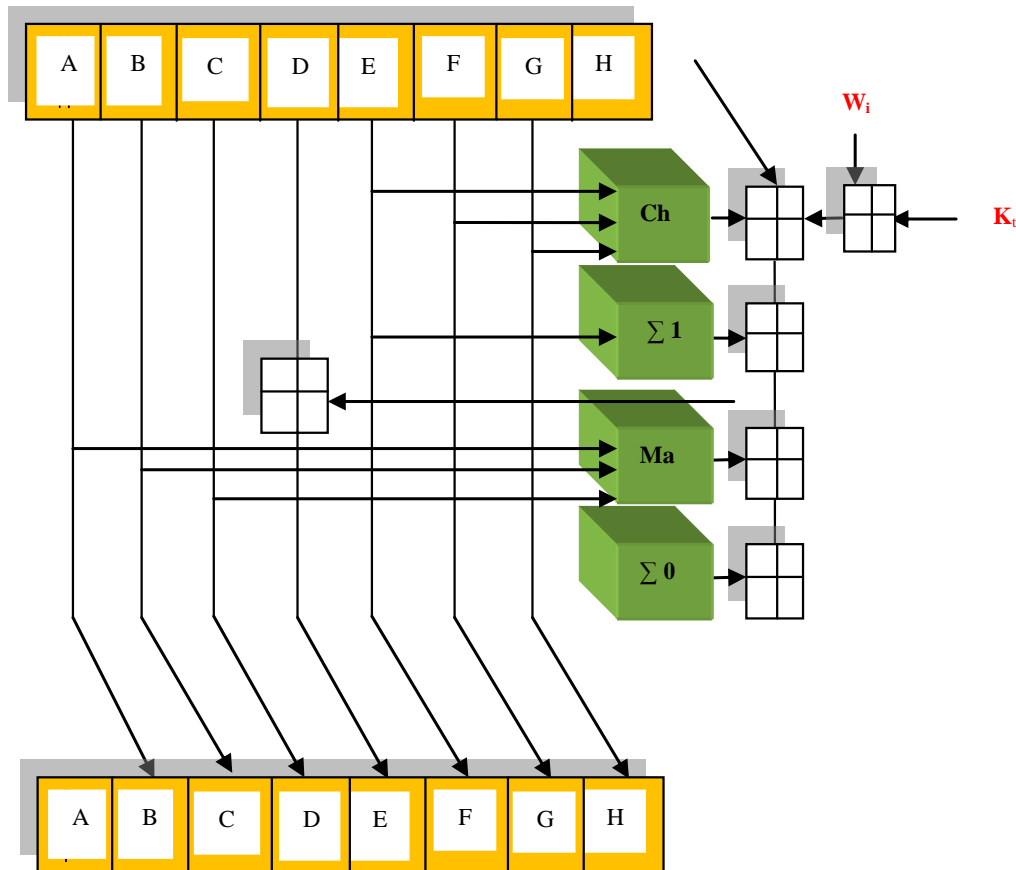


Figure 4.4: SHA-256 Algorithm

There are certain essential features of Hash functions: It must be one way only, i.e., there should be no way to reverse the hash value to obtain the original records back. It must possess weak collision resistance. It means giving a subjective message M_1 , weak collision resistance makes it challenging to construct another message M_2 , such that $\text{Hash}(M_1) = \text{Hash}(M_2)$. It must acquire strong collision resistance. That means it is complicated to locate two messages that hash to the same value, i.e., it is hard to find M_1 and M_2 such that $\text{Hash}(M_1) = \text{Hash}(M_2)$.

SHA-256 is one of the successor hash functions to SHA-1 (collectively referred to as SHA-2) and is one of the strongest hash functions available. It is defined in the NIST (National Institute of Standards and Technology) standard 'FIPS 180-4'. NIST also

provide a number of test vectors to verify correctness of implementation [101]. SHA-256 produces a 256-bit hash code known as a message digest. Figure 4.4 describes the SHA-256 algorithm in brief, in which a message digest is evaluated using padding of original message or record. The input message can be of any length and consist of text, binary data, or any other format. The SHA-256 works on fixed-size blocks of data; thus, padding is applied to the input message to ensure it can be divided into blocks of 512 bits (64 bytes). The hash values (A, B, C, D, E, F, G, H) are initialized to predetermined constants. These constants are part of the SHA-256 specification and serve as the initial state of the hash function. The padded message is divided into 512-bit blocks (16 words of 32 bits each). This is iterated over 64 rounds, performing various bitwise and arithmetic operations on the words and hash values to compute the intermediate hash values for that round. After 64 rounds, intermediate hash values are added to the initial hash values. Finally, the eight 32-bit hash values (A, B, C, D, E, F, G, H) are concatenated to form a 256-bit message digest.

This code is embedded in the selected frequency band of LWT transformed medical image along with modified EPR.

High Visual Quality	• LL band is untouched, human retina is sensitive to low frequency components.
High Computational Efficiency	• Less arithmetic operations requirement due to fixed point data type.
High Embedding Capacity	• Three out of four bands can be used for embedding (HL, LH and HH).
High Correlation Coefficient	• Frequency domain transformation and untouched LL band enhances correlation.
Low Memory Requirement	• Integer Wavelets uses fixed-point arithmetic resulting in less memory requirement in comparison to floating-point arithmetic.
Completely Reversible	• The LWT is completely reversible without any loss by transforming an integer to another integer.
High PSNR	• LWT decomposes image into approximate and detailed components. Embedding into detailed components preserves originality.
High Resistance towards Geometric and Noise Attacks	• Embedding of information into frequency transformed carrier provides resistance against many popular attacks.

Figure 4.5: Advantages of Lifting Wavelet Transform Watermarking Mechanism

4.2.5 Watermarking Mechanism

After compression and encryption, patient's secret information is stored into secure locations of a carrier. In this mechanism, the medical image is taken as a cover image

for embedding two important records (customized EPR and Hash code). Numerous watermarking mechanisms are available in the literature with their respective pros and cons along with application requirements [102]. In this proposal, LWT with Integer to Integer (Int2Int) wavelet transform is considered due to the enormous advantages listed in Figure 4.5. The wavelet transform is one of the admired processes for multi-resolution image analysis. Figure 4.6 shows the multi-scale filter bank arrangement used in Wavelet Transform [80], which split the approximate and detailed frequencies.

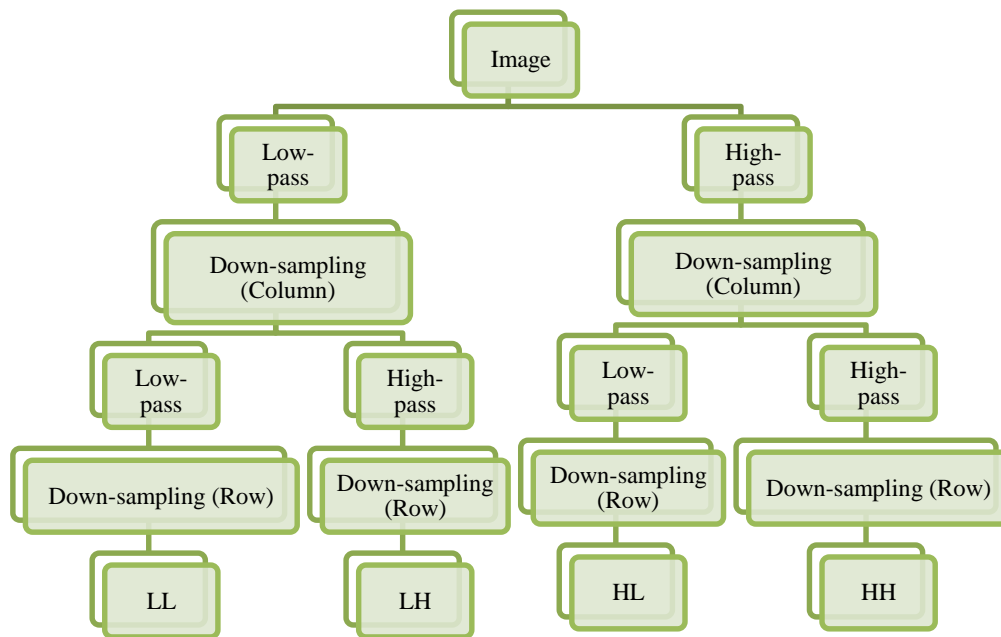


Figure 4.6: Filter Banks used in Wavelet Transform

These filter banks convolve the input image with the High Pass filter (HP) and Low Pass filter (LP) and detach both types of components pixel-wise, to get the 2-D Wavelet Transform. This results in four sub-bands: LL approximate sub-band, HL horizontal sub-band, LH vertical sub-band and HH diagonal sub-band. Integer wavelet uses a fixed-point arithmetic configuration which involves low memory requirement in comparison to use by the wavelet characterized by floating-point arithmetic. In application areas such as, image processing, the pixel values are integers which are input for the wavelet filters but, the consequential filtered output no longer consists of all integers, which at times commence rounding error. Therefore, it is stern requisite to use some wavelet transform function which returns integer value after conversion. With the same objective, the proposed method uses LWT [103, 104].

As shown in Figures 4.7 and 4.8 this mechanism is used at two locations in the proposal, at first position it is used in the watermarking mechanism for embedding customized EPR and hash code of biometric. And at the second point, it is used as steganography for embedding medical image in the reference image. Algorithm for embedding information in Image is described below in Algorithm 4.

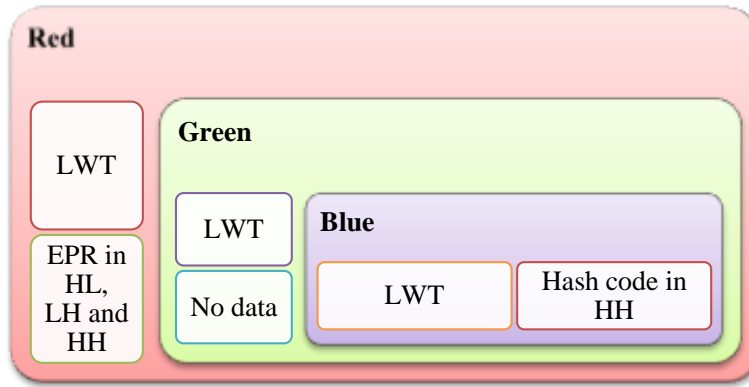


Figure 4.7: Watermarking Scheme Embedding Customized EPR and Hash Code in Medical Image

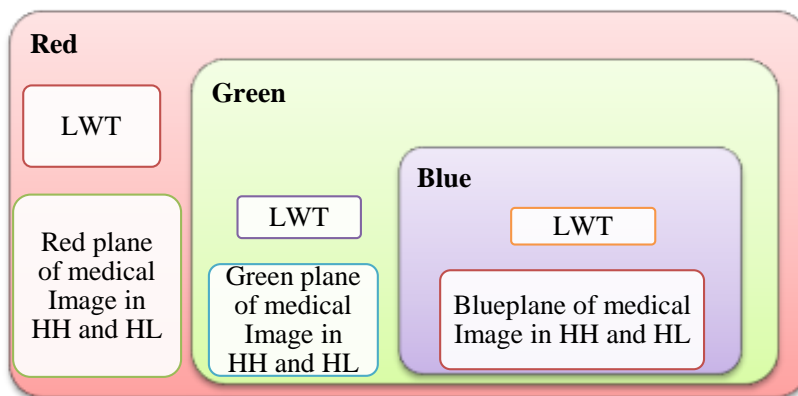


Figure 4.8: Steganography Scheme Embedding Three Planes of Medical Image in Reference Image

After embedding two important records in the medical image resultant WMMI will undergo numerous modifications before penetrating the reference image. These amendments are described in the subsequent section.

4.2.6 Scrambling

The WMMI undergoes specific changes before resting in the reference image. These alterations are, scrambling of all the separated color planes followed by compression. For scrambling the planes, Arnold transformation is used, that converts an image into an entirely different worthless image. Thus, it is used as a pre-processing stage during hiding digital image information, also known as information disguise [105,106]. Arnold scrambling algorithm features simplicity and periodicity, so it is widely used in such applications.

After permutation, all the planes of WMMI undergo Huffman compression so that the size of the planes can be reduced before embedding into the reference image. Further, each reduced plane is divided into two shares to place each in different bands

Algorithm 4 Pseudocode for Watermarking Mechanism

```
1: INPUT: Cover Medical Image = I, Secret Information = A;
2: OUTPUT: Watermarked Medical Image = I-out
3: STEP 1: Read Coloured Cover Medical Image I.
4: STEP 2: Separate All The Planes Of Image.
5:   I-RED = I(:, :, 1);
6:   I-GREEN = I(:, :, 2);
7:   I-BLUE = I(:, :, 3);
8: STEP 3: Apply 2D-LWT Transform On Each Plane With Liftwave Scheme Of
   Integer To Integer (Int2Int).
9:   LS = liftwave('db4', 'Int2Int');
10:  [llr, hlr, lhr, hhr] = lwt2(I-RED, LS);
11:  [llg, hlg, lhg, hhg] = lwt2(I-GREEN, LS);
12:  [llb, hlb, lhb, hhb] = lwt2(I-BLUE, LS);
13: STEP 4: Embedding Of Secret Information In One Or Multiple Bands Using
   Following Method. Available Bands Are hh, hl and lh.
14:   flag = 1;
15:   [M, N] = SIZE (hhr);
16:   for I do = 1:M
17:     for J do = 1:N
18:       if f then lag <= numel(A)
19:         num = de2bi(typecast(int8(hhr(i, j)), 'uint8'));
20:         num(1) = A(flag);
21:         num1 = bi2de(num);
22:         num1 = typecast(num1, 'int8');
23:         hhr(I, J) = num1;
24:         flag = flag + 1;
25:       end if
26:     end for
27:   end for
28: STEP 5: Apply Inverse Lifting Wavelet Transform On Each Plane And Combine
   All Planes To Form Watermarked Medical Image.
29:   I-RED1 = ilwt2(llr, hlr, lhr, hhr, LS);
30:   I-GREEN1 = ilwt2(llg, hlg, lhg, hhg, LS);
31:   I-BLUE1 = ilwt2(llb, hlb, lhb, hhb, LS);
32:   I-out(:, :, 1) = I-RED1;
33:   I-out(:, :, 2) = I-GREEN1;
34:   I-out(:, :, 3) = I-BLUE1;
35: STEP 6: Obtain The WaterMarked Medical Image (WMMI) I-out.
```

of integer wavelet transformed reference image. With very high visual quality, this final image is ready to move into an insecure environment. However, it provides no clue of any records available. On the receiver side, all algorithms in reverse order will be applied to retrieve all the required data. The next section provides set-up parameters followed by results.

4.3 SIMULATION SET-UP PARAMETERS

The Set-up parameters are shown in Table 4.3.

Table 4.3: Set-up Parameters

PARAMETERS	VALUES	
Size of Medical Image	64x64x3 (Set of eight images is taken for results), shown in Table 4.3	
Size of Reference Image	256x256x3 (Set of four images is taken for results), shown in Table 4.4	
Image Category	Coloured and Greyscale Images (jpg Format)	
Electronic Patient Record (EPR) (in bytes)	150, 120, 100, 80 and 60 bytes (listed in Table 4.20)	
Programming language version	MATLAB	
Processor	1.90Ghz, Intel (R) Core (TM i3-3227U)	
Memory	4GB	
Key value (Encryption Scheme)	Original Key Values x(1)=0.4523444336; y(1)=0.003453324562; z(1)=0.001324523564; r=3.99; b=6; xn=0.002; zn=0.004;	Modified Key Values xd(1)=0.4523444335; yd(1)=0.003453324562; zd(1)=0.001324523564; rd=3.99; bd=6; xnd=0.002; znd=0.004;
Specifications of Images and EPR for comparison	Medical image 2, Reference image 3 and EPR size, 60 bytes (shown in Tables 4.3 and 4.4)	

4.4 RESULTS

This section illustrates all the results based on the defined performance matrices and a comparison with available mechanisms. As the proposed mechanism is motivated by the medical application described in [55], so all the results are compared with the method proposed by [55] as (Ref2) and another medical application-based work [54] as (Ref1). While considering medical image 2, reference image 3 and EPR size 60 bytes (as mentioned in Table 4.3).

4.4.1 Imperceptibility Analysis

Figure 4.9 portrays different stages where modifications in both types of images (medical and reference images) are made and comparison is needed so that visual quality and imperceptibility can be verified. Tables 4.4 exhibits assorted medical images at different stages of the process. As observed from the results, it is incredibly hard to differentiate between all the images.

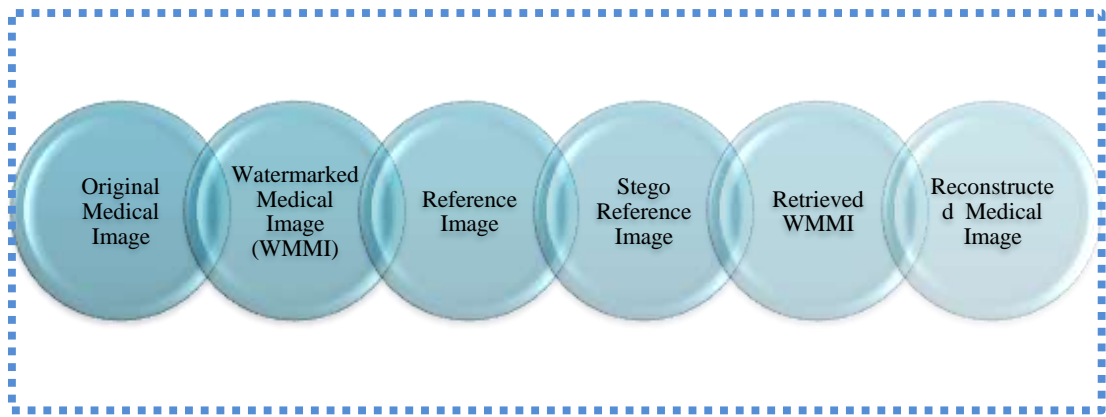

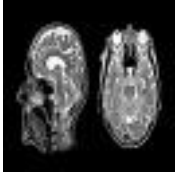
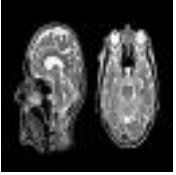















Figure 4.9: Different Stages of Images in the Proposal

Table 4.4: Results for Different Stages of Medical Images

S.No.	Original Medical Image (64 x 64 x 3)	Watermarked Medical Image (WMMI)	Retrieved WMMI	Reconstructed Medical Image
Medical Image 1	Input1 	Input2 	Output1 	Output2 
Medical Image 2	Input1 	Input2 	Output1 	Output2 
Medical Image 3	Input1 	Input2 	Output1 	Output2 
Medical Image 4	Input1 	Input2 	Output1 	Output2 













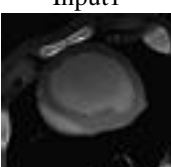

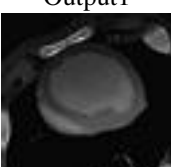



Medical Image 5	Input1 	Input2 	Output1 	Output2 
Medical Image 6	Input1 	Input2 	Output1 	Output2 
Medical Image 7	Input1 	Input2 	Output1 	Output2 
Medical Image 8	Input1 	Input2 	Output1 	Output2 

Table 4.5: Results for Different Stages of Reference Images

S. No.	Reference Image (256 x 256 x 3)	Stego Reference Image
Reference Image 1	Input 	Output 

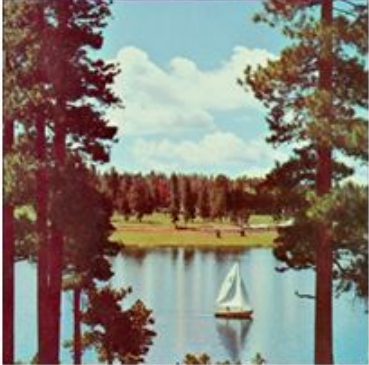



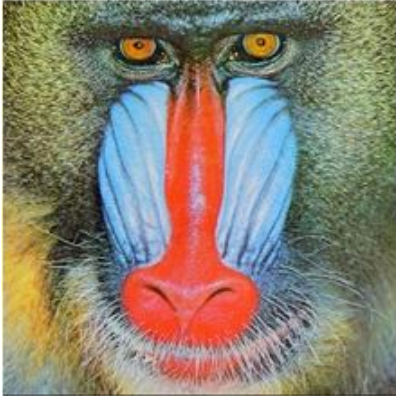
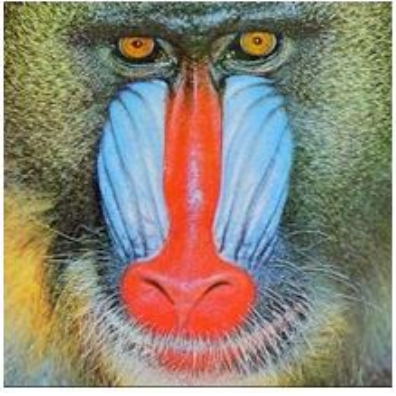
Reference Image 2	<p style="text-align: center;">Input</p> 	<p style="text-align: center;">output</p> 
Reference Image 3	<p style="text-align: center;">Input</p> 	<p style="text-align: center;">Output</p> 
Reference Image 4	<p style="text-align: center;">Input</p> 	<p style="text-align: center;">Output</p> 

Table 4.5 portrays a reference image and corresponding stego-image containing all the records (modified EPR and customized Medical Image). This result also provides excellent visual quality. The images in Table 4.5 can be termed visually encrypted meaningful images, as these images hold the WMMI in modified form. Thus the availability of these images on insecure channels can never attract intruders as these are available as a general-purpose simile.

4.4.2 Confidentiality Analysis

In evaluating the confidentiality of records, a comprehensive analysis is conducted on the images before and after the embedding procedure. The excellence of a technique is judged by comparing the pixel values, probability distribution and histograms between the medical image and WMMI, also among reference image and stego-reference image. Collectively, these analyses form a robust framework for assessing the impact of data embedding techniques on image confidentiality.

Table 4.6: Recorded PSNR Values

Image and Size of EPR	PSNR 1 (Between Reference and Stego Reference image)	Image and Size of EPR	PSNR 2 (Between Original Medical and Reconstructed Medical Image)
Reference Image 1, Medical Images 1-8	37.9233	Reference Image 1, Medical Image 1-8, EPR- 100 bytes	49.8399
Reference Image 2, Medical Images 1-8	37.9888	Reference Image 2, Medical Image 1-8, EPR- 100 bytes	51.8399
Reference Image 3, Medical Images 1-8	37.6419	Reference Image 3, Medical Image 1-8, EPR- 80 bytes	52.4899
Reference Image 4, Medical Images 1-8	37.8964	Reference Image 4, Medical Image 1-8, EPR- 120 bytes	52.5742
Average	37.8965	Average	51.6859

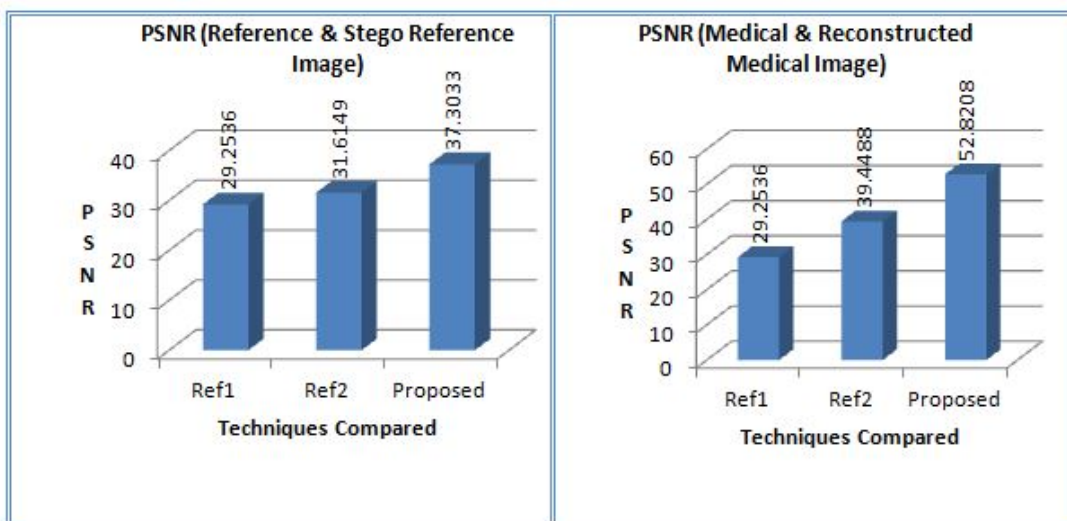


Figure 4.10: PSNR Comparisons

(a) *Comparison of diverse steganography parameters*

- *Peak Signal to Noise Ratio (PSNR)*: This parameter is used to compare each image pixel before and after embedding. The higher value of PSNR means a low error, thus ensuring the high confidentiality of stored information. Table 4.6 represents recorded PSNR values for both sets of images, i.e., amid reference and stego reference image and original and reconstructed medical image. The comparison results are shown in Figure 4.10. The proposed method gives a high PSNR value compared to the available methods.

Table 4.7: Recorded MSE Values

Image and Size of EPR	MSE 1 (Between Reference and Stego Reference image)	Image and Size of EPR	MSE 2 (Between Original Medical and Reconstructed Medical Image)
Reference Image 1, Medical Images 1-8	12.3339	Reference Image 1, Medical Image 1-8, EPR- 100 bytes	0.3015
Reference Image 2, Medical Images 1-8	12.3289	Reference Image 2, Medical Image 1-8, EPR- 100 bytes	0.3154
Reference Image 3, Medical Images 1-8	12.2828	Reference Image 3, Medical Image 1-8, EPR- 80 bytes	0.3423
Reference Image 4, Medical Images 1-8	12.3525	Reference Image 4, Medical Image 1-8, EPR- 120 bytes	0.3747
Average	12.3250	Average	0.3335

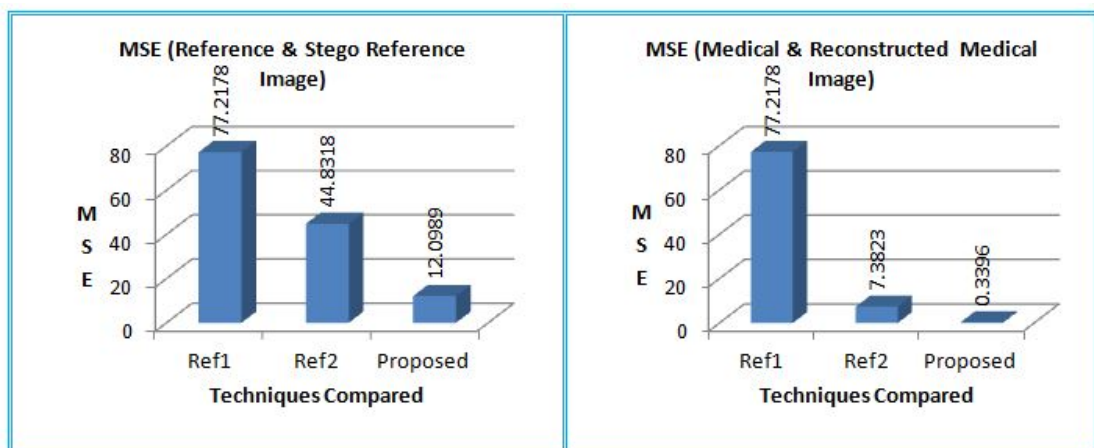


Figure 4.11: MSE Comparisons

- *Mean Square Error (MSE)*: It stands for cumulative squared error between the two images (before and after embedding). The lower value of MSE

means lower error. Table 4.7 represents recorded MSE values for both sets of images i.e. amid reference and stego reference image and amid original and reconstructed medical image and the comparison results are shown in Figure 4.11.

- *Jaccard similarity Index (JI)*: It compares elements of two sets to spot shared and distinct components. It's a measure of similarity for the two sets of data, with a range from zero to a hundred percent. A higher percentage signifies more similar populations. Table 4.8 represents recorded JI values for both sets of images i.e. amid reference and stego reference image and amid original and reconstructed medical image and the comparison results are shown in Figure 4.12

Table 4.8: Recorded Jaccard Index Values

Image and Size of EPR	J1 (Between Reference and Stego Reference image)	Image and Size of EPR	J2 (Between Original Medical and Reconstructed Medical Image)
Reference Image1, Medical Images 1-8	0.9942	Reference Image 1, Medical Image 1-8, EPR- 100 bytes	0.9900
Reference Image2, Medical Images 1-8	0.9966	Reference Image 2, Medical Image 1-8, EPR- 100 bytes	0.9900
Reference Image3, Medical Images 1-8	0.9983	Reference Image 3, Medical Image 1-8, EPR- 80 bytes	0.9926
Reference Image4, Medical Images 1-8	0.9996	Reference Image 4, Medical Image 1-8, EPR- 120 bytes	0.9925
Average	0.9969	Average	0.9938

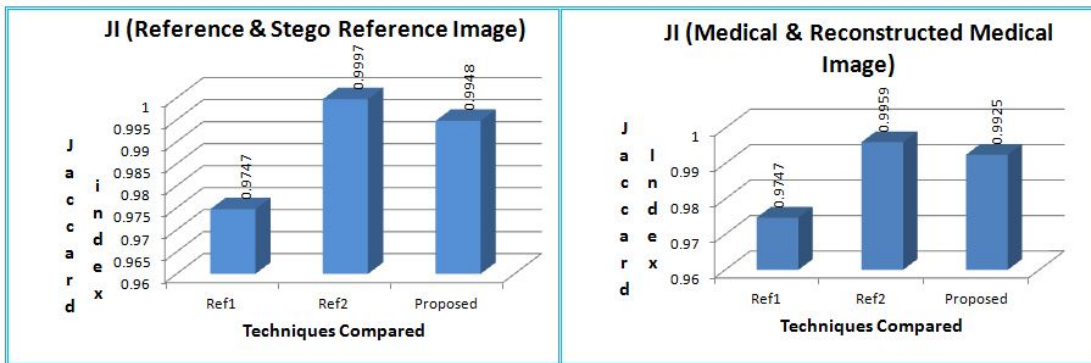


Figure 4.12: Jaccard Similarity Index Comparison

- *Universal Image Quality Index (UIQI)*: It shows the different impact of the pixels values, existing at diverse locations, on the Human Visual System (HVS). If some deformation is initiated in the image, such alterations are calculated as a combination of three factors; Loss of correlation, contrast distortion and luminance distortion. Table 4.9 represents recorded UIQI values for both sets of images i.e. amid reference and stego reference image and amid original and reconstructed medical image and the comparison results are shown in Figure 4.13

Table 4.9: Recorded UIQI Values

Image and Size of EPR	UIQI 1 (Between Reference and Stego Reference image)	Image and Size of EPR	UIQI 2 (Between Original Medical and Reconstructed Medical Image)
Reference Image 1, Medical Images 1-8	0.99993	Reference Image 1, Medical Image 1-8, EPR- 100 bytes	0.99962
Reference Image 2, Medical Images 1-8	0.99994	Reference Image 2, Medical Image 1-8, EPR- 100 bytes	0.99962
Reference Image 3, Medical Images 1-8	0.99988	Reference Image 3, Medical Image 1-8, EPR- 80 bytes	0.99969
Reference Image4, Medical Images 1-8	0.99991	Reference Image 4, Medical Image 1-8, EPR- 120 bytes	0.99962
Average	0.99992	Average	0.99964

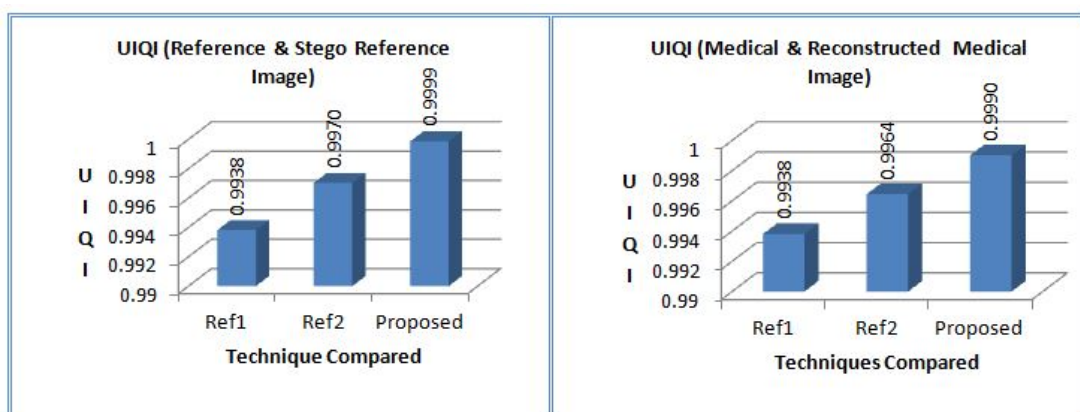


Figure 4.13: UIQI Comparisons

- *Correlation Coefficient (CC)*: This parameter measures the linear correlation between two images, A and B. Its range is between -1 to +1, inclusive, where 1 signifies perfect match, 0 signifies entirety mismatch and -1 shows

the inversion of an image. Table 4.10 represents recorded CC values for both sets of images and the comparison results are shown in Figure 4.14.

Table 4.10: Recorded Correlation Coefficient Values

Image and Size of EPR	CC 1 (Between Reference and Stego Reference image)	Image and Size of EPR	CC 2 (Between Original Medical and Reconstructed Medical Image)
Reference Image1, Medical Images 1-8	0.99987	Reference Image 1, Medical Image 1-8, EPR- 100 bytes	0.99929
Reference Image2, Medical Images 1-8	0.99989	Reference Image 2, Medical Image 1-8, EPR- 100 bytes	0.99929
Reference Image3, Medical Images 1-8	0.99977	Reference Image 3, Medical Image 1-8, EPR- 80 bytes	0.99941
Reference Image4, Medical Images 1-8	0.99982	Reference Image 4, Medical Image 1-8, EPR- 120 bytes	0.99928
Average	0.99984	Average	0.99932

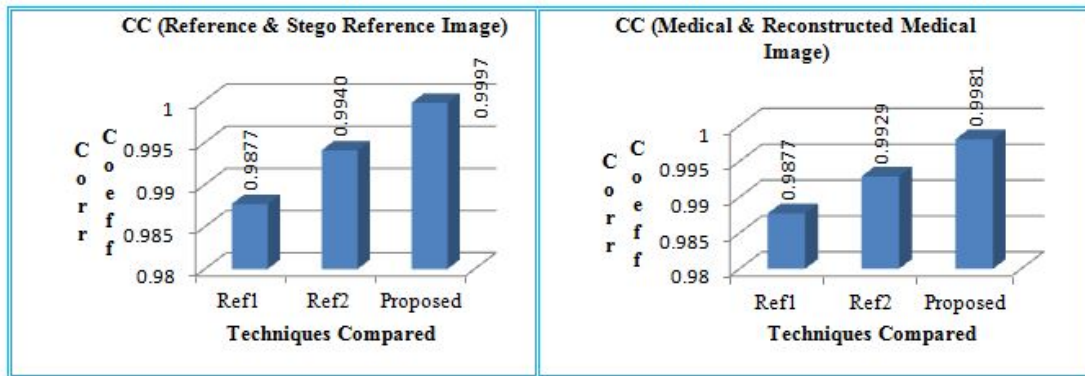


Figure 4.14: Correlation Coefficient Comparisons

- *Bhattacharya Coefficient*: This parameter gives an estimated measure of the count of overlapping between two arithmetical samples, which are two images (before (B) and after (A) embedding). It measures the relative closeness between these images. Table 4.11 represents recorded BC values for both sets of images, i.e., amid reference and stego reference image and original and reconstructed medical image and the comparison results are shown in Figure 4.15.

Table 4.11: Recorded Bhattacharya Coefficient Values

Image and Size of EPR	BC 1 (Between Reference and Stego Reference image)	Image and Size of EPR	BC 2 (Between Original Medical and Reconstructed Medical Image)
Reference Image1, Medical Images 1-8	0.98486	Reference Image 1, Medical Image 1-8, EPR- 100 bytes	0.94887
Reference Image2, Medical Images 1-8	0.98563	Reference Image 2, Medical Image 1-8, EPR- 100 bytes	0.94887
Reference Image3, Medical Images 1-8	0.98884	Reference Image 3, Medical Image 1-8, EPR- 80 bytes	0.95039
Reference Image4, Medical Images 1-8	0.98622	Reference Image 4, Medical Image 1-8, EPR- 120 bytes	0.94258
Average	0.98639	Average	0.94768

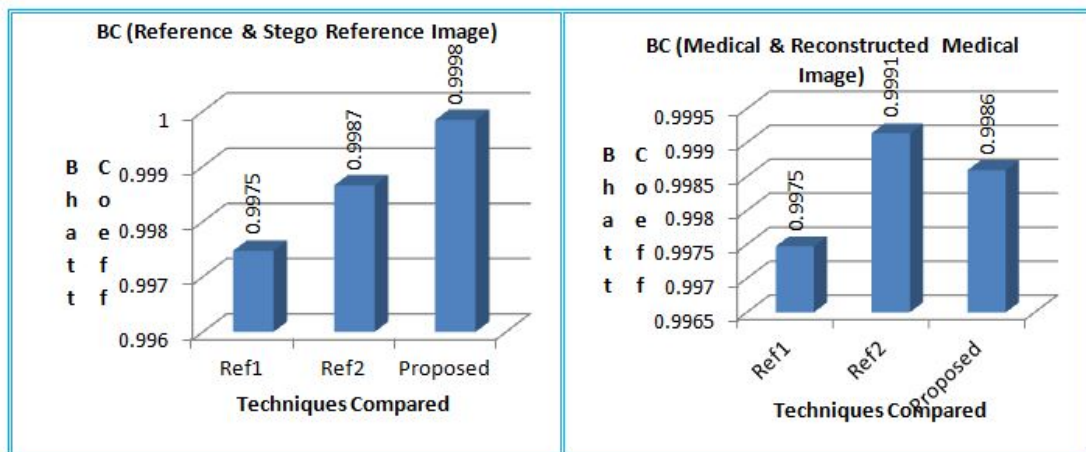


Figure 4.15: Bhattacharya Coefficient Comparisons

- Intersection Coefficient (IC):** This parameter provides a count of the same value of pixels between two histograms. When comparing histograms of different images, the intersection coefficient highlights the regions where the pixel values align and where they deviate. Its higher value signifies a more remarkable similarity in pixel value distribution, suggesting that the two histograms share a substantial number of identical values. On the other hand, a lower value indicates a significant divergence in pixel value distribution between the histograms. Table 4.12 represents recorded IC values for both sets of images, i.e., amid reference and stego reference image and original and reconstructed medical image and the comparison results are shown in Figure 4.16.

Table 4.12: Recorded Intersection Coefficient Values

Image and Size of EPR	IC 1 (Between Reference and Stego Reference image)	Image and Size of EPR	IC 2 (Between Original Medical and Reconstructed Medical Image)
Reference Image1, Medical Images 1-8	0.98759	Reference Image 1, Medical Image 1-8, EPR- 100 bytes	0.96705
Reference Image2, Medical Images 1-8	0.98069	Reference Image 2, Medical Image 1-8, EPR- 100 bytes	0.96705
Reference Image3, Medical Images 1-8	0.99883	Reference Image 3, Medical Image 1-8, EPR- 80 bytes	0.96718
Reference Image4, Medical Images 1-8	0.98015	Reference Image 4, Medical Image 1-8, EPR- 120 bytes	0.96308
Average	0.98682	Average	0.96609

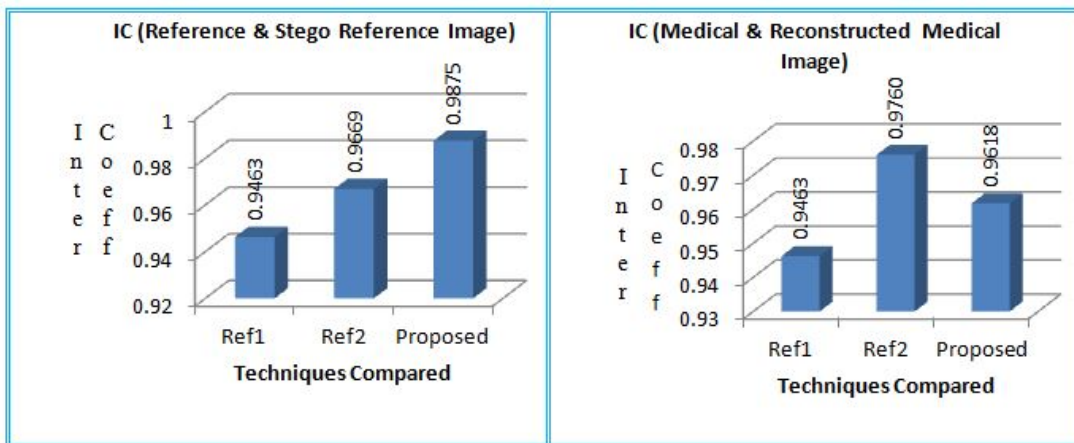


Figure 4.16: Intersection Coefficient Comparison

Results of all the parameters (PSNR, MSE, JI, CC, BC and IC) for security analysis are publicized in Tables 4.6, 4.7, 4.8, 4.9, 4.10, 4.11 and 4.12. As observed from the tables, readings for a different set of images, it is conferred that the proposed technique is immensely secured. All interpretations are in the range, which provides a perfectly secure ambiance. Tables 4.10, 4.11, 4.12, 4.13, 4.14, 4.15 and 4.16 illustrate the comparison of the proposal with the admired mechanism. Almost every outcome of comparison shows that most of the parameters of the proposed mechanism have optimized values in contrast to formally accepted techniques available in the literature; this is due to the fact of employing Integer Wavelet Transform steganography and also the choice of

appropriate frequency bands for the embedding of information. Amendment of records (EPR and Medical Image) before embedding grants add-on protection.

- (b) *Comparison of diverse cryptography parameters* EPR undergoes compression and encryption before embedding. The cryptography mechanism used in the proposal has many factors worth analyzing. These are key sensitivity analysis, key-space analysis and plain text sensitivity.

Table 4.13: Bit Error Rate for Minor Change in Key Input

Size of EPR	BER	BER ratio (in percent)
60 bytes	617	50.7
80 bytes	818	50.6
100 bytes	1029	50.01
120 bytes	1090	47.9
150 bytes	1489	49.5

Table 4.14: Number of Pixel Change for One Pixel Change in Plain Text

Size of EPR	NPCR	UACI (in percent)
60 bytes	1	28.07
80 bytes	1	33.30
100 bytes	1	29.07
120 bytes	1	30.71
150 bytes	1	29.36

Table 4.15: Key-space for Encryption Techniques

Key= X(0), Y(0), Z(0), r, b, X'(n) and Z'(n)	
Parameter	Proposed Technique
Key-size	448 Bits
Key-space	2^{448}

Tables 4.13, 4.14 and 4.15 show all the related results for analyzing the Encryption schemes. Table 4.13 illustrates changes in pixel values for minor key-value changes. The changed key value is depicted in the table of set-up parameters. It can be seen that 50% of values change in altering even very minute changes in the initial key. Table 4.14 demonstrates the Number of Pixel Changes Rate (NPCR) and the Unified Average Changing Intensity (UACI)

between the original and its encrypted EPR. These results interpret that each value of ciphertext changes with change in even only one value of the plain text [97]. Table 4.15 details the size of the initial keys used in the encryption mechanism and the key-space provided by these keys. The encryption mechanism of the proposal uses Initial Key= X(0), Y(0), Z(0), r, b, X'(n) and Z'(n), hence has key-space of 2^{448} value, which is relatively high, indicating that brute force search time for hackers is very high. This scheme provides a sizeable key spacing, can resist brute force attacks and significantly less computational time for image encryption/decryption.

Table 4.16: Comparison of Proposed Mechanism with References on Diverse Parameters of Cryptography

Parameters	REF1 [54]	REF2 [55]	PROPOSED MECHANISM
MECHANISM USED	AES (For odd positions) RSA (For even positions)	IWT and equation based encryption	Quantum logistic map based mechanism
KEY-SIZE	128 Bits for odd, 1024 bits for even	37^n (n-levels of decompositions)	448 Bits
KEY-SPACE	$2^{128}, 2^{1024}$	37^2	2^{448}

Table 4.16 provides a comparison of the proposed mechanism with existing algorithms. It shows that contemporary quantum-chaotic based encryption usage results in large key-space and highly random behavior due to its inherent nature.

4.4.3 Authenticity Analysis

For granting authenticity and integrity to the mechanism different provisions are incorporated. Authenticity verifies an appropriate recipient of the information. To incorporate this, the validation biometric identification process is incorporated. For assessment of its performance, certain metrics are required. Biometric performance metrics rates implementation of a biometric system, result or application. Diverse metrics can be used for the rationale and these are termed as Key Performance Indicators (KPI) [62, 98]. Commonly employed KPI are: The False Acceptance Rate also known as the “FAR”, The False Rejection Rate, also known as the “FRR”, The Equal Error Rate, also known as the “ERR”, The Ability to Verify Rate also known as the “AVR”, The Failure to Enroll Rate also known as the “FER”.

These all KPIs are required to be evaluated, for the systems in which biometric identification is compared with the available database and there are chances of wrong detection and correct rejection. But the proposal has a reliable identification system, as retrieved code from WMMI will get compared with the code generated from the IRIS

captured value, at the receiver end. If there is a mismatch even of the single bit then access to records will be denied. As the proposal is motivated by the medical application described in [55], in which fingerprint is used for authentication. In contrast, IRIS detection as a biometric solution has many advantages over other biometric solutions [62] as described below in Table 4.17, that's why it is preferred in the current mechanism. Table 4.18 compares the authenticity mechanism employed by other proposals.

Table 4.17: Authenticity Mechanism Comparisons

Parameters	IRIS Detection	Fingerprint Recognition	Face Recognition
Accuracy	The unique and stable patterns in the IRIS provide a robust biometric identifier, resulting in low false acceptance and false rejection rates.	It is also highly accurate, but its performance may be affected by factors like skin conditions or image quality.	It also offers reasonably good accuracy, but it may be impacted by variations in lighting and facial expressions.
Security	It is considered highly secure, as the IRIS patterns are difficult to forge or replicate.	Fake fingerprints or spoofing techniques can be employed	It can be vulnerable to spoofing attempts using photos or videos.
Uniqueness	The patterns in the iris are highly unique, even among identical twins, making it one of the most distinctive biometric traits.	Fingerprint patterns are also unique to individuals, but identical twins may have similar fingerprints.	While faces are generally unique, the level of uniqueness is lower than iris or fingerprints and face recognition may encounter challenges with identical twins.
Applications	Commonly used in secure access control systems, airports and border crossings.	Widely used in smartphones, law enforcement and attendance systems.	Used in consumer devices, surveillance systems and identity verification applications.

Table 4.18: Comparison of Proposed Mechanism with References for Authenticity

AUTHENTICITY	
TECHNIQUES	MECHANISM USED
Ref1 [54]	No mechanism
Ref2 [55]	Finger print (biometric)
Proposed Mechanism	IRIS detection (biometric)

Authentication and integrity are interrelated; its analysis is discussed in next section.

4.4.4 Integrity Analysis

To ensure the reception of unaltered information or maintain the system's integrity, one of the best ways is to send a hash code along with the primary information. This can be matched at the receiver side and further action can be defined as per the result of the matching algorithm. The SHA-256 hashing algorithm is employed in this work, which satisfies all three desirable conditions for a hashing technique: one-wayness, weak collision and strong collision resistance [100]. Its performance can be gauged by a parameter of the number of bits changed when a single bit of the message input is changed. Sensitivity to input data change is an essential feature of the hashing function, which can make it a successful detector. Figure 4.17 shows the number of bits changes for a different data set. SHA-256 generates a hash code of 256 bits. As observed from the table, more than 50% bits are changed even for a single bit change in input data.

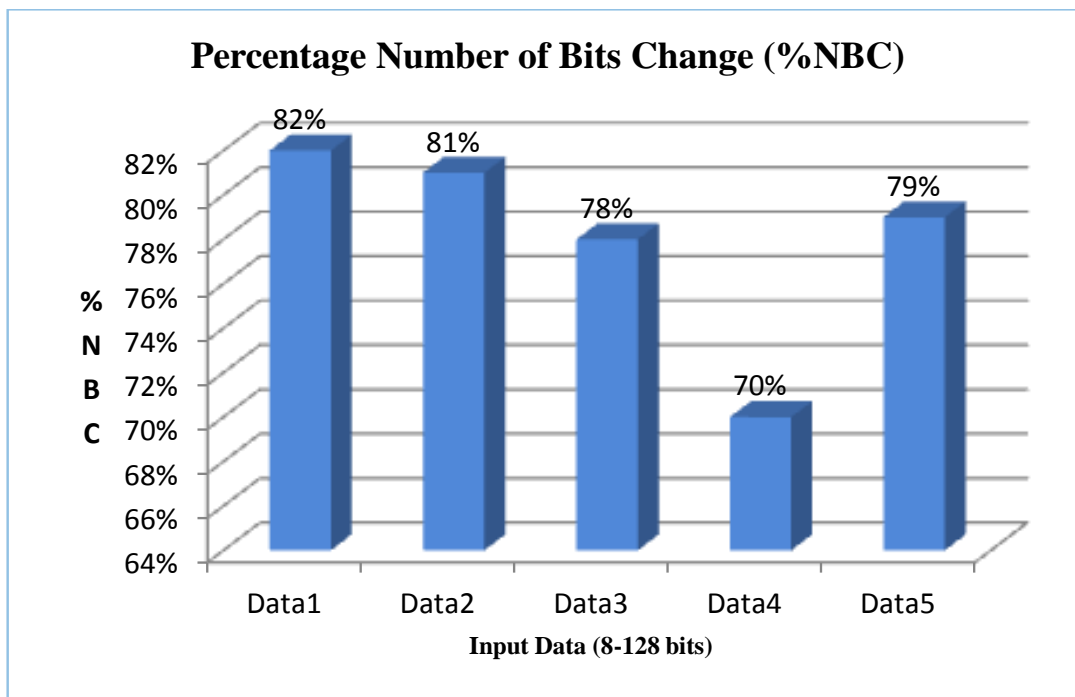


Figure 4.17: Testing of SHA-256

Consequently, even a minor change in the IRIS detection value will lead to access denial for the unauthorized person. This powerful feature of hash algorithm, contributes integrity to the proposed mechanism.

4.4.5 Reproducibility or Data Extraction Analysis

Another important parameter to gauge a security mechanism is its capability for data extraction i.e. the records which were modified and hidden in some carrier should be reproduced in original form for their usage. For analyzing this factor bit error rate is

measured for retrieved EPR and Medical image. Five sets of readings are taken for both information and recorded in Tables 4.19 and 4.20.

Table 4.19: BER for Retrieved EPR

Size of EPR	Original EPR	Retrieved EPR	BER	BER ratio
60 bytes	EPR:Patient is suffering from high sugar levels-Needs medication.	EPR:Patient is suffering from high sugar levels-Needs medication.	0	0
80 bytes	EPR:"Happiness is the key to good Health and mind,Believe in GOD and yourself" AMEN!!	EPR:"Happiness is the key to good Health and mind,Believe in GOD and yourself" AMEN!!	0	0
100 bytes	EPR:Patient is diagnosed with kidneystone of large size. Immediate surgery is recommended for followup.	EPR:Patient is diagnosed with kidneystone of large size. Immediate surgery is recommended for followup.	0	0
120 bytes	EPR: NAME-XYZ,Address,PQRST,Patient is diagnosed with minor skin problems. Regular medicines are recommended for followup.	EPR:NAME-XYZ,Address,PQRST,Patient is diagnosed with minor skin problems. Regular medicines are recommended for followup.	0	0
150 bytes	EPR: NAME-XYZ,Address,PQRST,Patient is diagnosed with major pshycological problems. Regular medicines and meditation sessions are recommended for followup.	EPR:NAME-XYZ,Address,PQRST,Patient is diagnosed with major pshycological problems. Regular medicines and meditation sessions are recommended for followup.	0	0

Table 4.20: BER for Retrieved Medical Image

Medical Image (Original and Retrieved)	BER	BER ratio (in percent)
64 x 64 x 3=98,304 bits	(Number of Bits change)	
Medical Image 1	3102	0.031555=3%
Medical Image 2	3246	0.03302=3%
Medical Image 3	6646	0.067607=6%
Medical Image 4	4128	0.041992=4%
Medical Image 5	4014	0.040833=4%
Medical Image 6	3400	0.034587=3%
Medical Image 7	3045	0.030975=3%
Medical Image 8	5042	0.05129=5%
Average Change in Pixel values (%)		3.8%

Table 4.19 shows the data extraction record for five different sizes of Electronic

Patient Record (EPR). As seen from the results, the given mechanism provides perfect reproducibility of record. Table 4.20 shows retrieval statistics for the medical image, as seen from previous results visual quality, correlation and other related coefficients for the medical image are very good. This can be verified from these results, barely 3-4% bits are altered which are not affecting the visual quality of images, hence correct diagnosis can be carried out from these received images.

4.5 CONCLUSION

With the increased medical data transversal over apprehensive networks and other interconnected networks, demand for security of such crucial data has also raised manifold. The chapter illustrates a multilayer security architecture that is used to protect the medical images along with patient information. This mechanism achieves the following security measures:

- Confidentiality by means of modifying and hiding each required record.
- Imperceptibility by choosing suitable frequency bands in Integer wavelet transformed Reference image.
- Biometric authentication by capturing and comparing IRIS pattern at both ends (sender and receiver).
- Integrity by generating hash code for the captured IRIS template and compare it with respective code on receiver side for granting access to records.
- Perfect reproducibility of records by extracting EPR with zero bit error and medical images with acceptable bit changes.
- For resultant stego reference image, it is very hard to distinguish it from its original version resulting in visually meaningful encrypted image.

In this chapter, one proposal was presented to achieve confidentiality, imperceptibility, reproducibility, integrity and authenticity. The mechanism improved in many aspects, but some vital areas need to be worked upon further for such a method to strive towards perfection — the inclusion of multiple layers of security results in higher time requirements than existing mechanisms. So, optimization of execution time is an area to be worked upon for striving toward perfection. That is why subsequent research investigations develop and test another innovative scheme that combines multiple security algorithms to secure confidential information with optimized time requirements and other vital security objectives.

Chapter 5

QUANTUM BASED ROBUST AND SWIFT HYBRID SECURITY MECHANISM

In the previous chapter, one proposal was presented to achieve confidentiality, imperceptibility, reproducibility, integrity and authenticity. In this chapter, research investigations further develop and test another innovative scheme that combines multiple security algorithms to secure confidential information.

5.1 CONTRIBUTION

The need to communicate records, text, images and other information is the mandatory action required in almost all application areas. The severity of security needs motivates researchers to put in lots of effort to propose highly protected mechanisms to save the fragile information used in diverse sectors. As in chapters 2 and 3, the study of available techniques reveals that each proposal is designed to optimize some objectives and has pros and cons for fulfilling defined goals. For security, the requests of the diverse fields and sectors include confidentiality, robustness, high speed of execution, imperceptibility and complete reproducibility of data. Due to the availability of enormous cryptography and steganography mechanisms, multiple combinations can be produced as outcomes. Each researcher tried groupings to get desired results regarding the best values of defined parameters. Most of the goals still need to be satisfied by any single proposal. The motivation behind this work is to optimize most of the mentioned goals. For that rationale, the core contributions of the proposal are:

- **Ensuring Imperceptibility:** This feature make certain that the hidden information shouldn't be visible to the third party. This is achieved by the selection of appropriate algorithms (LWT steganography) and frequency band for embedding sensitive information. Optimize results of PSNR and correlation coefficient confirms high imperceptibility.

- **Ensuring Confidentiality:** For inculcating this feature, multiple layers of security are used, to ensure that even if one layer is breached data should be protected by another one. These layers are formed by conditional compression, confusion, diffusion and finally steganography.
- **Ensuring High Speed:** Many applications are time restricted, that means need prompt data for further action. For reducing time of execution, very simple and effective processes are used and even one stage is conditional i.e. it will be used as per the want of data, to be secured.
- **Ensuring Randomness:** Encoding data in such a form which is unreadable for others can be performed by mingling it to great extent. This is introduced in proposal by using bit level confusion and diffusion processes by means of randomly generated keys using Quantum logistic maps.
- **Ensuring Reproducibility:** It is attained, by using all those algorithms at all the stages which are lossless, so that complete information is available for intended user. In mechanism compression, confusion, diffusion and steganography, all are lossless and reversible to ensure desired data reception.

The following section gives the detail of the proposed hybrid model. First, in Section 5.2, the proposed mechanism is described, pursued by explaining each building block of this technique from sections 5.3 to 5.7. Then, section 5.8 provides the setup parameters. Finally, a comprehensive analysis of results is done in section 5.9, followed by an overall conclusion.

5.2 THE PROPOSED MODEL

A hybrid security model is proposed in this chapter, which ensures the protection of the secret information used in varied applications in diverse apprehensive environments. The sender side process for the proposed model is described in Figure 5.1 and hallmarks of the same are as under:

- Centralized Key Scheduling Algorithm.
- Conditional Compression
- Bit-Level Confusion
- Bit-Level Diffusion
- Frequency Domain Lifting Wavelet Transform

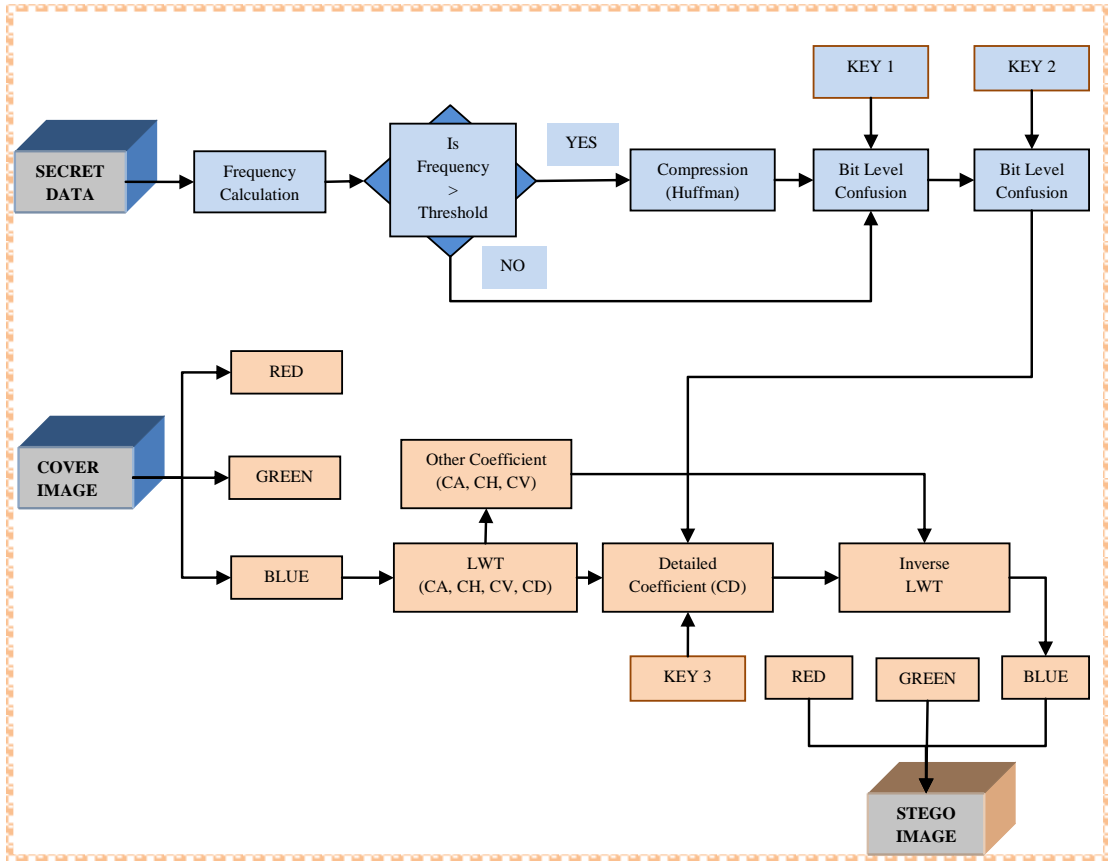


Figure 5.1: The Proposed Model for Sender Side

The subsequent section illustrates all the blocks of the proposed model, with the rationalization of the selection. Also, it is a reversible scheme; every stage can be reversed; thus, each stage is explained to demonstrate its both directions, sender side and receiver side function.

5.2.1 Key Scheduling Algorithm

For securing any information, it is required to protect it from varying facets. One of the aspects is the secret key used for the security algorithm. The proposed mechanism is a hybrid scheme consisting of different stages and each step requires a unique key for implementation. For that matter, a centralized key scheduling algorithm is used for the generation of keys for all stages, as shown in Figure 5.2. Secret keys are to be random and unique for every stage; that is why Quantum logistic Maps are employed. Due to enormous advantages, as described in [81, 95], quantum logistic maps are chosen here. Pseudo-code for key scheduling algorithm is described in Algorithm 5, which generates keys for all the stages and has the characteristics of providing highly random keys.

Algorithm 5 Key Scheduling Algorithm

- 1: **INPUT:** Initial Keys= $a(0)$, $b(0)$, $c(0)$, u , v , $a'(n)$ and $c'(n)$; Secret Data Length=LENGTH(DATA);
- 2: **OUTPUT:** KEYS: key1, key2, key3.
- 3: **STEP 1:** Initialize All Initial Keys.
- 4: **STEP 2:** Iteration Of Following Logistic Map Equations 1000 Times, To Avoid The Transient Effect, Using The Initial Conditions And Control Parameters Initialized In The Previous Step.
- 5: **for** $n = 1$ to 1000 **do**

$$\begin{aligned}a(n+1) &= u \cdot (a(n) - |a(n)|^2 - u \cdot b(n)); \\b(n+1) &= -b(n) \cdot e^{-2v} + e^{-v} \cdot u \cdot [(2 - a(n) - a'(n)) \cdot b(n) \\&\quad - a(n) \cdot c'(n) - a'(n) \cdot Z(n)]; \\c(n+1) &= -c(n) \cdot e^{-2v} + e^{-v} \cdot u \cdot [2 \cdot (1 - a'(n)) \cdot c'(n) \\&\quad - 2 \cdot a(n) \cdot b(n) - a(n)];\end{aligned}$$

- 6: **end for**
 - 7: **STEP 3:** Repeat The Map Equations Once Using New Initial Conditions (Calculated In Step 2) To Get New Key Values (aNEW, bNEW AND cNEW).
 - 8: $a1new = \text{mod}((\text{floor}(anew(1,1) * (2^{32}))), 2^{32});$
 - 9: $b1new = \text{mod}((\text{floor}(bnew(1,1) * (2^{32}))), 2^{32});$
 - 10: **STEP 4:** The Control Parameter (u) Is Modified With The Help Of Arithmetic Operations.
 - 11: **STEP 5:** This Modified Value Of Resultant Keys Is Reversed And All The Steps From 2 To 4 Are Repeated, For Generation Of Latest Key Values From New Key Values.
 - 12: **STEP 6:** Finally, These Key Values Are Manipulated As Follows To Get The Values Which Can Be Used As Keys For Different Stages:
 - 13: $H=KEYS;$
 - 14: $H1=dec2hex(H);$
 - 15: $H2=rem(numel(H1'),3);$
 - 16: $HH3=padarray(H1,[0 H2], 'replicate', 'post');$
 - 17: $H3=reshape(HH3,[],3);$
 - 18: $H4=(hex2dec(H3));$
 - 19: $H5=(H4');$
 - 20: **STEP 7:** Different Keys Are Obtained From These Values
 - 21: $Key1=H5(1);$
 - 22: $Key2=H5(2:LENGTH(DATA)+1);$
 - 23: $Key3=H5(LENGTH(DATA)+2:2 * LENGTH(DATA)+2);$
-

All the keys generated in this algorithm are used in different stages, as described in subsequent sections. The steps start from the confusion stage. Before that, a condition-based compression stage will appear. Depending on the value of frequency, the compression stage is included. Compressed information improves the embedding capacity as well as the imperceptibility of confidential data in the cover image.

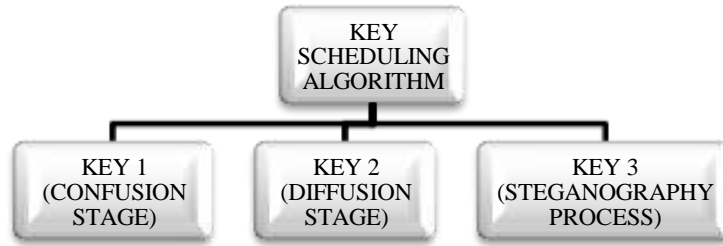


Figure 5.2: Centralized Key Generation

5.2.2 Conditional Compression

The initial action carried out in this work is identifying the need for a compression algorithm.

Algorithm 6 Pseudocode for Compression

```

1: INPUT: Information to be Compressed = data
2: OUTPUT: Compressed Huffman Code = hcode
3: STEP 1: Initialize All Possible Symbols In Input Data.
4:   symbols = 0:255;
5: STEP 2: Probability Of Each Symbol In Data Is Calculated
6:   prob = ones(1, length(symbols));
7:   flag1 = 0;
8: for J = min(symbols):max(symbols) do
9:   for I = 1:LENGTH(data) do
10:    if data(I) == J then
11:      flag1 = flag1 + 1;
12:    end if
13:  end for
14:  prob(j+1) = flag1 / length(data);
15:  flag1 = 0;
16: end for
17: STEP 3: Dictionary Is Created With Symbols And Probability Of Each Symbol In
    Data.
18:   dict = huffmandict(symbols, prob);
19: STEP 4: Huffman Code For Each Character Of Data Is Identified Using Data And
    Dictionary.
20:   hcode = Huffmanenco(data, dict);
21: STEP 5: Obtain The Huffman Code hcode.
  
```

This is done by calculating the frequency of characters appearing in confidential data. If the available frequency is higher than a threshold value, which is taken as 2 in this implementation, then compression will be favorable for reducing the data size for further processing; otherwise, it will proceed to the next stage without compression. This is because the Huffman compression algorithm uses the principle of encoding the characters as per their occurrences' in the data. If the frequency is high, then the small size of the code will be assigned to the character and inversely large size code

will be given to low-frequency characters. This algorithm is chosen because of its significant advantage of being lossless and the compression rate is very high [107, 108]. Its compression rate varies from 30 to 50%, depending on the font's occurrence in the information. The pseudocode for the compression and decompression algorithms is described in Algorithms 6 and 7, respectively.

Algorithm 7 Pseudocode for Decompression

- 1: **INPUT:** Compressed Huffman Code = hcode
 - 2: **OUTPUT:** Original Data = recovered-data
 - 3: **STEP 1:** Formation of Dictionary or Acquire Dictionary From Receiver Side.
 - 4: **STEP 2:** Original Value of Each Data Value is Identified using Huffman Code and Dictionary.
 - 5: recovered-data= huffmandeco(hcode,dict)
 - 6: **STEP 3:** Obtain the Original Data recovered-data.
-

The next stage is the confusion of the data before storing it into the carrier image.

Algorithm 8 Pseudocode for Bit-Level Confusion

- 1: **INPUT:** Compressed Secret Data or Secret Data = hcode or data (bits)
 - 2: **OUTPUT:** Confused Data = conf-data
 - 3: **INPUT:** Compressed Secret Data or Secret Data = hcode or data (bits)
 - 4: **OUTPUT:** Confused Data = conf-data
 - 5: **STEP 1:** Take Seed Value From Key Generation Algorithm.
 - 6: **STEP 2:** Unique Random Array Is Generated Using This Seed
 - 7: *SEED=KEY1;*
 - 8: *RAND-ARRAY=randperm(LENGTH(data), LENGTH(data),);*
 - 9: *A=RAND-ARRAY;*
 - 10: **STEP 3:** Permute Bits Of Compressed Data Or Data Bits Using This Generated Random Array
 - 11: **for** I **do**=1:LENGTH(hcode or data)
 - 12: ind=A(I);
 - 13: conf-data(ind)=hcode(I);
 - 14: **end for**
 - 15: **STEP 4:** Result Is The Confused Array Of Data Bits conf-data.
-

5.2.3 Bit-Level Confusion

This stage is used to permute the information available in bits from the previous step. The key for generating random numbers is taken from the key scheduling algorithm to make the permutation process more random. The pseudocode for the confusion process is given in Algorithm 8 and for reverse confusion process (receiver side) is illustrated in 9. The confusion method constitutes permutation action, wherein the permutation key is highly random, as its seed is generated using Quantum maps.

Algorithm 9 Pseudocode for Reverse Process of Confusion

```
1: INPUT: Confused Data = conf-data1
2: OUTPUT: Compressed Secret Data or Secret Data = hcode1 or data1 (bits)
3: STEP 1: Take Seed Value From Key Generation Algorithm.
4: STEP 2: Unique Random Array Is Generated Using This Seed
5:   SEED=KEY1;
6:   RAND-ARRAY=randperm(LENGTH(data), LENGTH(data),);
7:   A1=RAND-ARRAY;
8: STEP 3: Retrieve Back Bits Of Compressed Data Or Data Bits Using This
   Generated Random Array
9: for J do=1:LENGTH(conf-data1)
10:   Ind1=A(J);
11:   Hcode1(J) = conf-data1(ind1);
12: end for
13: STEP 4: Result Is The Retrieved Array Of Data Bits Hcode1 Or Data1.
```

After getting the secret data in confused form i.e. in permuted structure, the next stage is diffusion.

Algorithm 10 Pseudocode for Bit-Level Diffusion

```
1: INPUT: Confused Data = conf-data
2: OUTPUT: Diffused Data = diff-data
3: STEP 1: Take Keys From Key Generation Algorithm key2.
4: STEP 2: Bit-Wise XOR Operation Of Key With Its Own Bits And Finally With
   Confused Secret Data Bit.
5: for I do=1:LENGTH(conf-data)
6:   number=key2(I);
7:   number-bi=de2bi(number,16);
8:   for J do=1:15
9:     number-bi(J+1)=bitxor(number-bi(J), number-bi(J+1));
10:  end for
11:  diff-data(I)=bitxor(conf-data(I), number-bi(16));
12: end for
13: STEP 3: Result Is The Diffused Array Of Data Bits diff-data.
```

5.2.4 Bit-Level Diffusion

The diffusion process affects numerous ciphertext bits with alteration in each plaintext or key bit. For diffusion operation also, keys are taken from a centralized key generation algorithm. The key size is the same as confused data bits to be diffused. The pseudocode for this process is described in algorithm 10 and its reverse process (receiver side) is illustrated in algorithm 11. The diffusion process consists of the XOR operation of the bits of each key with each other and, finally, with a secret data bit. The uniqueness of

the XOR operation is the motivation behind its choice, as it gives the same output with the same operation in the reversal process.

Algorithm 11 Pseudocode for Reverse Process of Diffusion

```

1: INPUT: Diffused Data = diff-data1
2: OUTPUT: Retrieved-data = ret-data
3: STEP 1: Take Keys From Key Generation Algorithm key2.
4: STEP 2: Bit-Wise XOR Operation Of Key With Its Own Bits And Finally With
   Confused Secret Data Bit.
5: for I do=1:LENGTH(diff-data1)
6:   number=key2(I);
7:   number-bi=de2bi(number,16);
8:   for J do=1:15
9:     number-bi(J+1)=bitxor(number-bi(J), number-bi(J+1));
10:  end for
11:  ret-data(I)=bitxor(conf-data(I), number-bi(16));
12: end for
13: STEP 3: Result Is The Retrieved Array Of Data Bits ret-data.

```

After applying all the processes i.e. compression, permutation and key-wise XOR operation, next stage comprises of hiding these bits in frequency transformed cover image using steganography.

5.2.5 Steganography Mechanism

After confusion and diffusion of secret information, it is store into secure locations of a carrier. Various steganography mechanisms are available in the literature with their respective advantages along with application requirements [102–104]. Steganography is the process of hiding a secret message, by embedding it in another safe cover in such a way that only the sender and intended recipient are responsive of existence of the secret information [69, 70]. In the proposed model, Lifting Wavelet Transform (LWT) is considered due to the enormous advantages described in previous chapters.

Pseudocode for embedding information in Cover Image is described in Algorithm 12 and for retrieving information is illustrated in Algorithm 13. The embedding algorithm is followed by the retrieval process, which describes the reverse process. The wavelet transform is one of the accepted processes for multi-resolution image analysis. It separates an image using approximate and detailed analysis by sorting out the frequencies into low and high frequencies. This 2D Wavelet Transform, results in four sub-bands: CA, CH, CV, CD. LWT with lifting scheme ‘Integer wavelet’ uses a fixed-point arithmetic configuration which involves not as much memory requirement as needed by the wavelet characterized by floating-point arithmetic. In most of the application areas, the pixel values are integers which are input for the wavelet filters

but, the consequential filtered output no longer consists of all integers, which at times instigate rounding error. Therefore, it is firmly required to use some wavelet transform function which returns integer value after conversion.

Algorithm 12 Pseudocode for Embedding Algorithm

```

1: INPUT: Cover Image = Im, Secret Information = diff-data, KEY=key3;
2: OUTPUT: Stego Image = Im-out
3: STEP 1: Read Coloured Cover Image Im.
4: STEP 2: Separate All The Planes Of Image.
5:   I-RED = Im(:, :, 1);
6:   I-GREEN = Im(:, :, 2);
7:   I-BLUE = Im(:, :, 3);
8: STEP 3: Apply 2d-LWT Transform On Blue Plane With Liftwave Scheme Of
   Integer To Integer (Int2Int).
9:   LS = liftwave('db4','Int2Int');
10:  [CA, CH, CV, CD]=lwt2(I-BLUE,LS);
11: STEP 4: Embedding Of Secret Information In Selected Band Using Following
   Method. Band Chosen Is 'CD'.
12:  [M,N]=size(CD);
13:  CD1=reshape(CD,1,[]);
14:  FLAG=1;
15:  diffd=diff-data;
16: for I do=1:LENGTH(diff-data)
17:  ind123=KEY(I);
18:  num=CD1(ind123);
19:  num1=de2bi(typecast(int32(num),'uint32'));
20:  num1(1)= diff-data(flag);
21:  num2=bi2de(num1);
22:  num3=typecast(num2,'int32');
23:  CD1(ind123)=num3;
24:  FLAG=FLAG+1;
25: end for
26:  CD12=reshape(CD,m,n);
27: STEP 5: Apply Inverse Lifting Wavelet Transform On Blue Plane And Combine
   All Planes To Form Stego Image.
28:  I-BLUE=ilwt2(CA, CH, CV, CD12, LS);
29:  Im(:, :, 3)= I-BLUE;
30:  Stego-image=Im;
31: STEP 6: Result Is The Stego Image Stego-Image.

```

The "int2int" wavelet is a reversible transform, meaning it does not introduce any loss of information during the embedding process. The original cover image can be perfectly reconstructed after extracting the hidden data, ensuring no data loss. It offers a reasonable embedding capacity while maintaining image quality. With these objectives, the proposed model uses LWT [103, 104].

Algorithm 13 Pseudocode for Retrieval Algorithm

```
1: INPUT: Stego Image = stego-image, KEY=key3;
2: OUTPUT: Retrieved Secret Data = ret-data;
3: STEP 1: Read Stego Image stego-image.
4: STEP 2: Separate All The Planes Of Image.
5:   S-RED = stego-image (:,:,1);
6:   S-GREEN = stego-image (:,:,2);
7:   S-BLUE = stego-image (:,:,3);
8: STEP 3: Apply 2d-LWT Transform On Blue Plane With Liftwave Scheme Of
   Integer To Integer (Int2Int).
9:   LS = liftwave('db4','Int2Int');
10:  [CA1, CH1, CV1, CD1] = lwt2(S-BLUE,LS);
11: STEP 4: Retrieving Secret Information Bits From Selected Band Using Following
   Method. Band Chosen Is 'CD'.
12:  KEY=key3;
13:  [M,N] = size(CD);
14:  CD2 = reshape(CD1,1,[]);
15:  FLAG1 = 1;
16: for I do 1:LENGTH(data)
17:  ind12 = KEY(I);
18:  num = de2bi(typecast(int32(CD2(ind12:34)), 'uint32'));
19:  ret-data(FLAG1) = num(1);
20:  num1 = bi2de(num);
21:  num2 = typecast(num1, 'int32');
22:  CD2(ind12) = num2;
23:  FLAG1 = FLAG1 + 1;
24: end for
25: STEP 5: Result Is The Retrieved Data ret-data at the receiver side.
```

After embedding modified version of secret data in the carrier image, this resultant image is required to move through the insecure channel. Thus, it is required to study response of resultant mechanism with respect to different known parameters and its comparison with existing renowned techniques to check its efficacy and validation.

5.3 SIMULATION SET-UP PARAMETERS




The Set-up parameters used for recording results are shown in Table 5.1 and standard images taken for implementation and comparative analysis are revealed in Table 5.2. This table provides information regarding the dataset used for experimentation purposes, which includes the size and type of images. Different sizes of confidential data used for hiding are also mentioned. Also, the configuration of hardware and software systems used for experimentation is described in the table.





Table 5.1: Set-up Parameters

Parameters	Values	
Sizes of Cover Image	128x128x3, 192x192x3, 256x256x3, 512x512x3 (Set of six images for each size are taken for results)	
Image Category	Coloured Images (jpg Format)	
Secret Data (in bytes)	10, 25, 80, 150, 300 and 500 bytes	
Programming language version	MATLAB	
Processor	1.90Ghz, Intel (R) Core (TM i3-3227U)	
Memory	4GB	
Key value (Encryption Scheme)	Original Key Values a(1)=0.4523444336; b(1)=0.003453324562; c(1)=0.001324523564; u=3.99; v=6; an=0.002; bn=0.004;	Modified Key Values ad(1)=0.4523444335; bd(1)=0.003453324562; cd(1)=0.001324523564; ud=3.99; vd=6; and=0.002; bnd=0.004;
Keys for different stages	Key1: confusion, Key2: diffusion, Key3: steganography (all generated using key scheduling algorithm)	
Conditional Huffman	Threshold Frequency=2	

The table also endows with details regarding references taken for comparative analysis. These all are multilevel mechanisms, using different algorithms as a combination. Each scheme provides optimized results as per the strength of the method. All the images considered for experimentation are of varying sizes, as mentioned in Table 5.2.

Table 5.2: Images and References Taken for Comparative Analysis

Image 1	Image 2	Image 3
Leena 	Girl 	Butterfly 

<p align="center">Image 4</p>	<p align="center">Image 5</p>	<p align="center">Image 6</p>
<p align="center">Scenery</p> 	<p align="center">Flower</p> 	<p align="center">Baboon</p> 
<p align="center">Image 7</p>	<p align="center">References</p>	
<p align="center">Doll</p> 	<p align="center">REF 1 [63], REF 2 [64], REF 3 [48]</p>	

As mentioned in Table 5.2, to validate the proposed method, it is compared with available renowned multilevel mechanisms. The following section demonstrates the experimental results of the proposed mechanism and its comparison with the latest references.











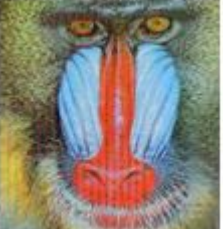





5.4 RESULTS

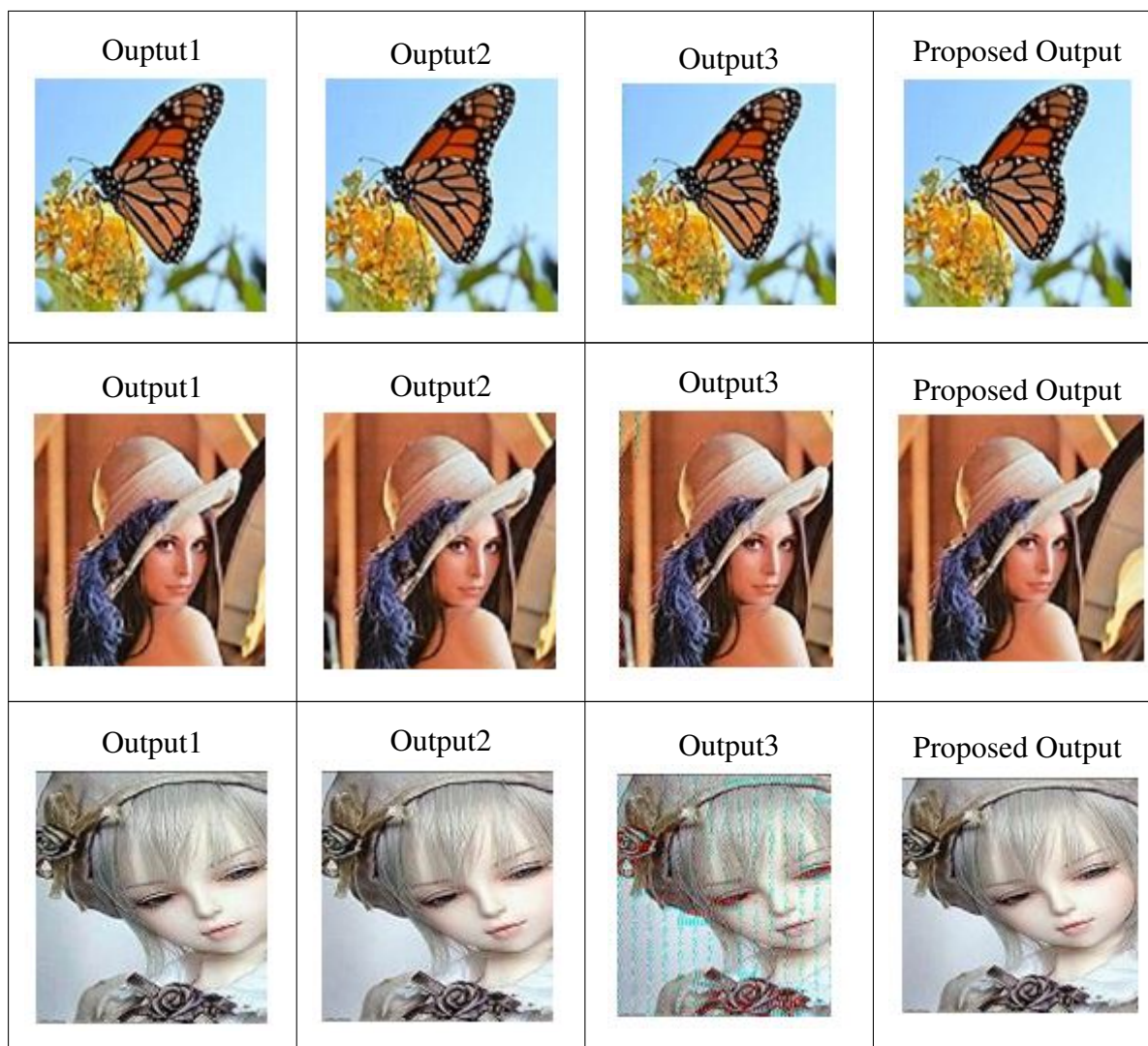
The results aid in drawing meaningful conclusions about the model's efficiency, accuracy and overall capability. The comparative analysis with existing methods further strengthens the understanding by providing benchmarks for assessing the model's uniqueness and advancements.

5.4.1 Imperceptibility Analysis

Table 5.3 portrays resultant stego-images, after implementing different algorithms. These results can be used for comparisons, so that visual quality and imperceptibility of secret data in cover image can be verified.

Table 5.3: Stego-images for Different Hybrid Mechanisms

REF 1	REF 2	REF 3	PROPOSED MODEL
<p>Ouptut1</p> 	<p>Ouptut2</p> 	<p>Ouptut3</p> 	<p>Proposed Output</p> 
<p>Ouptut1</p> 	<p>Ouptut2</p> 	<p>Ouptut3</p> 	<p>Proposed Ouptut</p> 
<p>Ouptut1</p> 	<p>Ouptut2</p> 	<p>Ouptut3</p> 	<p>Proposed Ouptut</p> 
<p>Ouptut1</p> 	<p>Ouptut2</p> 	<p>Ouptut3</p> 	<p>Proposed Output</p> 



As observed from the results, it is extremely hard to differentiate between all the images. That means all implemented mechanisms including proposed provides very fine visual quality. Several mechanisms like Ref 3 provide marks of presence of secret information in the cover image. Amount of information to be stored also marks impact on image's perceptibility.

5.4.2 Confidentiality Analysis

The confidentiality of the mechanisms can be evaluated by investigating image quality before and after embedding in both ways qualitatively and quantitatively. The former analysis is done by visual inspection of snapshots and later can be done using numerous matrices, which are described as under [10, 50, 107].

(a) *Comparison of diverse steganography parameters*

- *Peak Signal to Noise Ratio (PSNR)*: It is used to contrast each pixel of the image before and after inserting. High PSNR ensures the high confidentiality of stored information.

Table 5.4: Recorded PSNR and MSE Values

Images	Data size (bytes)	PSNR	MSE	Images	Data size (bytes)	PSNR	MSE
Image 1 to 7, 128*128	10	72.76	0.0034	Image 1 to 7, 256*256	10	79.85	0.0007
	25	69.65	0.0071		25	75.91	0.0017
	80	66.09	0.0160		80	72.98	0.0033
	150	63.57	0.0286		150	70.13	0.0065
	300	60.68	0.0557		300	67.29	0.0120
	500	59.23	0.0777		500	65.59	0.0181
Image 1 to 7, 192*192	10	75.85	0.0018	Image 1 to 7, 512*512	10	86.41	0.0002
	25	72.43	0.0040		25	82.84	0.0003
	80	70.39	0.0059		80	79.67	0.0007
	150	66.71	0.0152		150	77.09	0.0012
	300	63.68	0.0309		300	74.13	0.0025
	500	62.18	0.0434		500	72.49	0.0040

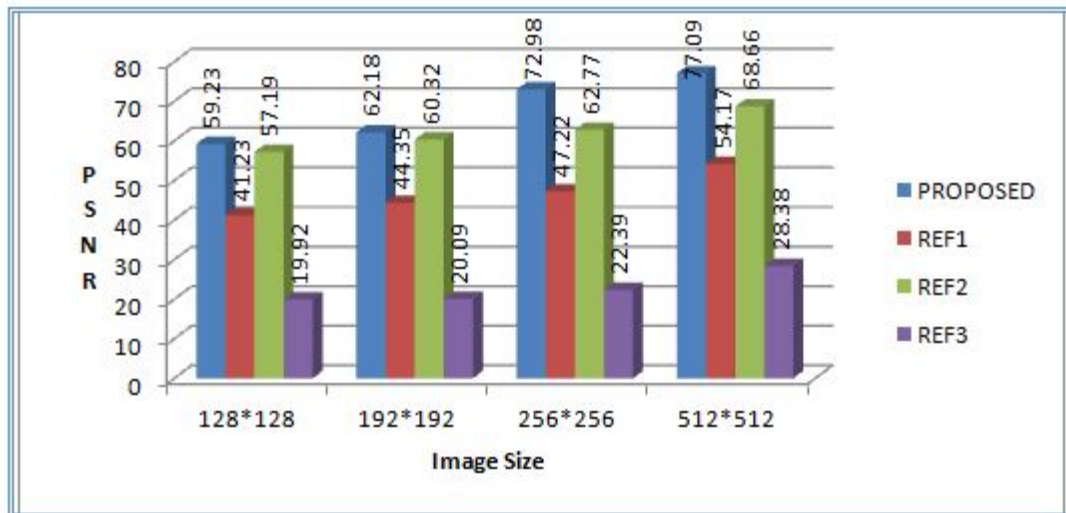


Figure 5.3: PSNR Comparisons

The proposed mechanism is compared with other renowned techniques available in literature for validation of results.

- *Mean Square Error (MSE)*: It stands for mean squared error between the two images (cover and stego). Low values of MSE ensure lower error. Seven images of varying sizes are taken for calculations of results.

Table 5.4 represents recorded PSNR and MSE values for proposed model. The comparison results are shown in Figures 5.3 and 5.4 for PSNR and MSE respectively. As observed from the results, in comparison to the available methods, the proposed model gives the high PSNR and low MSE values.

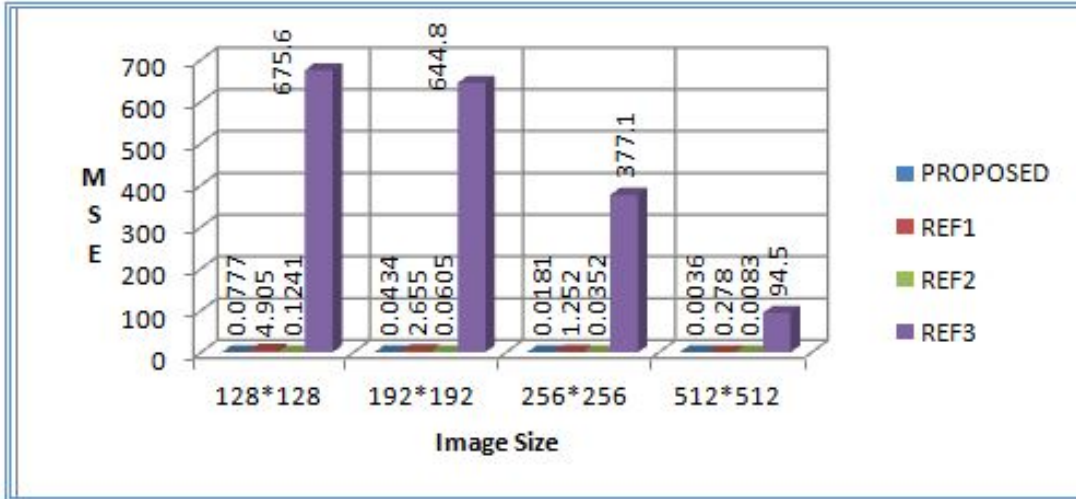


Figure 5.4: MSE Comparisons

The optimized values are accomplished by choosing the appropriate band for embedding and using the compression process before insertion of records into the cover image.

- *Bhattacharya Coefficient (BC)*: It gives an estimated measure of the count of overlapping between two images. It measures the relative closeness between the images.

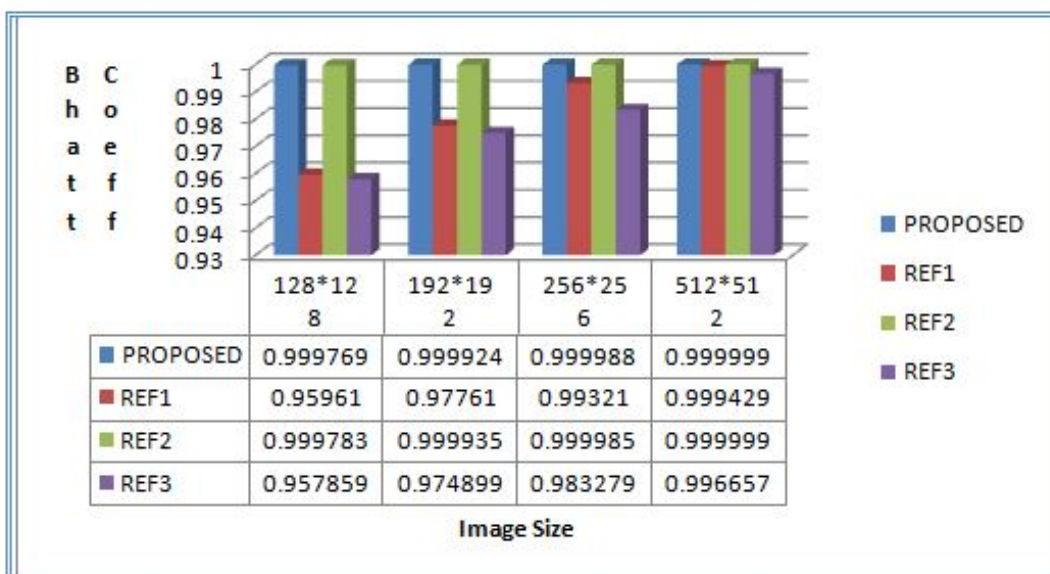


Figure 5.5: Bhattacharya Coefficient Comparisons

- *Intersection Coefficient (IC)*: It provides a count of the same value of pixels between two histograms. The range of value for this coefficient is between 0 to 1. Where 0 represents complete mismatch and 1 represents exactly match.

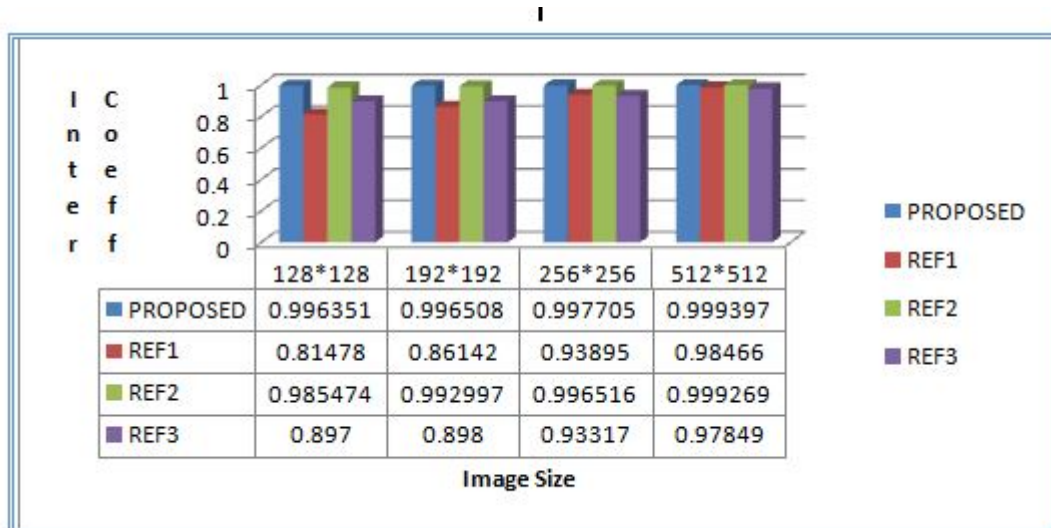


Figure 5.6: Intersection Coefficient Comparisons

- *Universal Image Quality Index (UIQI)*: It is an index which computes any kind of deformation as a combination of three factors: Loss of correlation, contrast distortion and luminance distortion. Final value is calculated by multiplying these three factors.

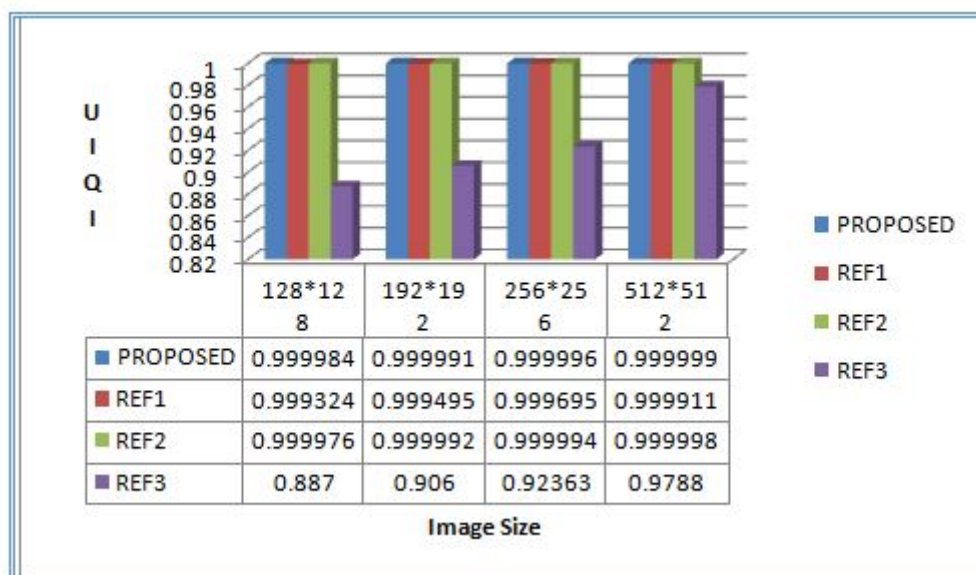


Figure 5.7: UIQI Comparisons

- *Correlation Coefficient (CC)*: It is an assessment of the linear association

between two images. It varies from -1 to $+1$ both inclusive, where 1 indicates perfect match and 0 implies entirety mismatch.

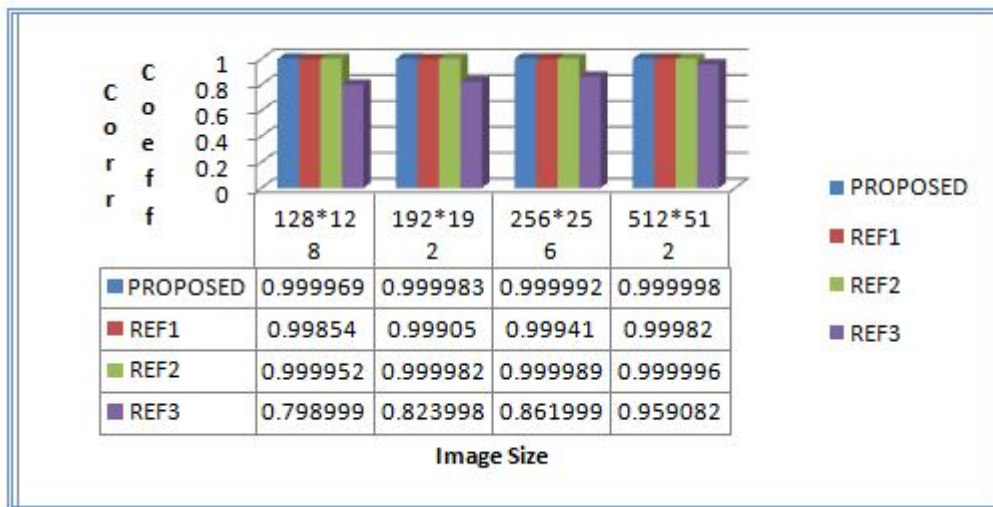


Figure 5.8: Correlation Coefficient Comparisons

- *Jaccard Index (JI)*: It is an evaluation of relationship for the two sets of data, with a range from zero to a hundred percent. High percentage indicates more similarity.

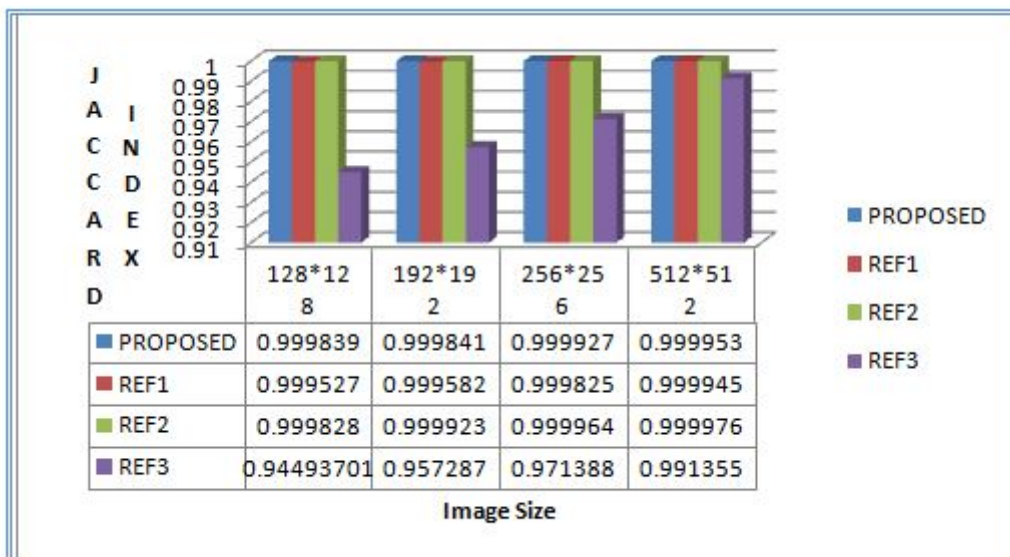


Figure 5.9: Jaccard Index Comparisons

Figures 5.5 to 5.9 provide a comparative analysis of the projected mechanism with available methods; it can be observed from the results that the proposed approach obtains optimize results in terms of most of the metrics. Consequently, it has the

competency to be more protected and offers more excellent safety towards secret information.

Table 5.5: Recorded JI, BC, IC, UIQI and CC Values

Images	Data size (bytes)	BC	IC	UIQI	CC	JI
Image 1 to 7, 128*128	10	0.999989	0.996918	0.999999	0.999999	1
	25	0.999978	0.995361	0.999999	0.999997	0.999984
	80	0.999947	0.992696	0.999997	0.999994	0.999931
	150	0.999908	0.990402	0.999994	0.999989	0.999948
	300	0.999833	0.987137	0.999989	0.999978	0.999855
	500	0.999769	0.985235	0.999984	0.999969	0.999839
Image 1 to 7, 192*192	10	0.999997	0.998417	1	0.999999	0.999998
	25	0.999992	0.997317	0.999999	0.999998	0.999981
	80	0.999992	0.997233	0.999999	0.999998	0.999972
	150	0.999997	0.99494	0.999997	0.999994	0.999953
	300	0.999943	0.992806	0.999994	0.999988	0.999876
	500	0.999924	0.991571	0.999991	0.999983	0.99984
Image 1 to 7, 256*256	10	1	0.999415	1	1	1
	25	0.999999	0.999017	1	0.999999	0.999999
	80	0.999998	0.998636	0.999999	0.999999	0.999986
	150	0.999996	0.998057	0.999999	0.999997	0.999975
	300	0.999993	0.997459	0.999997	0.999995	0.999969
	500	0.999988	0.996820	0.999996	0.999992	0.999927
Image 1 to 7, 512*512	10	1	0.999869	1	1	0.999999
	25	1	0.999782	1	1	0.999994
	80	1	0.999710	1	1	0.999993
	150	1	0.999537	1	0.999999	0.99998
	300	1	0.999366	0.999999	0.999999	0.999974
	500	0.999999	0.999247	0.999999	0.999998	0.999953

Results of all the parameters (JI, CC, BC, UIQI and IC) for security analysis are publicized in Tables 5.5 and Figures 5.3 to 5.9 shows the comparison of the proposed model with other renowned mechanisms before and after embedding secret records of 500 bytes on a different basis, i.e., values (similar and dissimilar), probability distribution, intensity, standard deviation, etc.

As observed from the figures, almost every outcome of comparison shows that all the parameters of the proposed mechanism have optimized values in contrast to formally accepted techniques available in the literature; this is due to the fact of employing Lifting Wavelet Transform steganography and also the choice of

appropriate frequency bands for the embedding of information. Alteration of confidential data before embedding grants add-on protection; thus, it is conferred that the proposed technique is immensely secured.

- (b) **Comparison of diverse cryptography parameters** As the proposed model is a hybrid mechanism having manifold stages, secret data undergo conditional compression and encryption before embedding. The cryptography mechanism used in the proposal consists of the confusion stage followed by the diffusion process. This dual process encryption has many factors worth analyzing. These are bit error rate, key sensitivity analysis, key-space analysis and plain text sensitivity.

Table 5.6: BER for Encrypted Data

Images	Data size (bytes)	BER (%)
For All Sizes of Images 1 to 7	10	49
	25	54
	80	53
	150	49
	300	52
	500	49

Table 5.6 shows the percentage of bits change when original secret data undergoes confusion and diffusion processes. More than 50% of bits are modified after the dual-stage encryption process, as seen from the results.

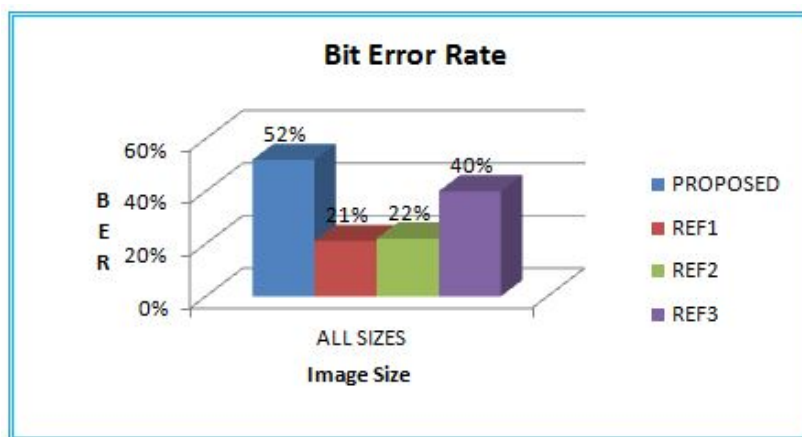


Figure 5.10: BER Comparison for Encryption

Figure 5.10 shows comparative results of encryption mechanism with existing techniques used in different hybrid models. These results are taken for encryption of 300 bytes records. As inferred from the results, randomness is

highest in the proposed model compared to other algorithms as more than 50% of bits are modified after applying the proposed mechanism. One of the main attractions of the projected mechanism is the centralized key scheduling algorithm, which is used for generating keys for different stages of hybrid model confusion stage, diffusion stage and finally for steganography stage. This algorithm is implemented using Quantum Logistic Maps, which is selected for its desirable feature of creating randomness in generated keys. The following results show the key sensitivity towards change in initial conditions. Table 5.7 demonstrates a change in key values used in different stages with a slight change in initial conditions or keys of logistic maps. Both values are declared in set up parameters, original and modified.

Table 5.7: Bit Error Rate for Minor Change in Initial Conditions

Keys	BER
Key1	48.85%
Key2	50.06%
Key3	49.77%

This resultant change in the entire key set will further modify the encryption stage values and alter the storage location in the steganography stage. The encryption mechanism of the proposal uses keys generated from a centralized key generation process which uses these Initial Key= a (1), b(1), c(1), an, bn, u, v, hence acquires key-space of 2^{448} , which is reasonably high indicating that brute force search time for hackers is very high.

Table 5.8: Comparison of Proposed Mechanism with References on Diverse Parameters of Cryptography

PARAMETERS	PROPOSED MECHANISM	REF 1	REF 2	REF 3
MECHANISM USED	Quantum logistic map based mechanism	Symmetric Key Cryptography	Hierarchical Visual Cryptography	AES
KEY-SIZE	448 Bits	4 Digits	Data length L	128 Bits
KEY-SPACE	2^{448}	2^{32}	2^L	2^{128}

Table 5.8 shows comparison of proposed mechanism with existing mechanisms. As per results, the scheme provides a sizeable key spacing, hence can resist the brute force attacks and provided a significantly less computational time for image encryption/decryption due to the usage of straightforward but effective processes.

5.4.3 Computational Time analysis

In many data communication and security applications, time restriction is very prominent, requiring prompt data for further action. For reducing the time of execution, straightforward and effective processes are used and even one stage is conditional, i.e., it will be used as per the want of data to be secured. Figure 5.11 shows the time required for embedding secret data in different images using various algorithms. As observed from Figure 5.11, the execution time for the proposed model is comparable with other renowned mechanisms. These values are recorded for the sender side process, used for inserting 300 bytes of secret data. Usage of simple processes for confusion and diffusion of confidential data results in a reduced amount of computational time.

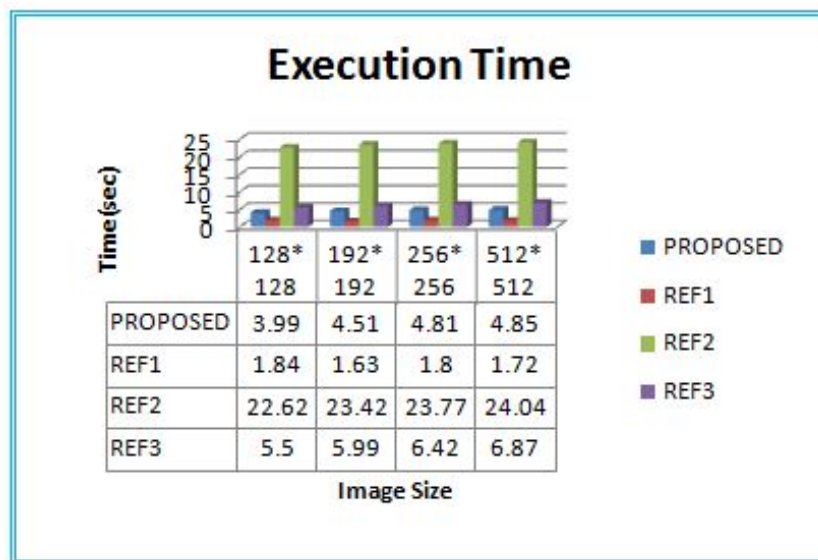


Figure 5.11: Computational Time Comparisons

5.4.4 Reproducibility analysis

Another significant consideration to judge a protection mechanism is its capability for data extraction, i.e., the encrypted secret information hidden in the cover image should be reproduced in original form for its subsequent usage. For analyzing this factor bit error rate is measured for recovered secret data. Table 5.9 shows the data recovery for different sizes of secret information and cover images. As seen from the results, the given mechanism provides perfect reproducibility of retrieved data. However, if the stego image is altered due to potential attacks or noises, then the information will not be retrieved as Huffman decompression will not allow distorted retrieved data to be converted into original form.

Table 5.9: BER for Recovered Data

Images	Data size (bytes)	BER	Images	Data size (bytes)	BER
Image 1 to 7, 128*128	10	0	Image 1 to 7, 256*256	10	0
	25	0		25	0
	80	0		80	0
	150	0		150	0
	300	0		300	0
	500	0		500	0
Image 1 to 7, 192*192	10	0	Image 1 to 7, 512*512	10	0
	25	0		25	0
	80	0		80	0
	150	0		150	0
	300	0		300	0
	500	0		500	0

In those cases, where the value of frequency of characters is less than threshold and compression is not employed, their bit error rate is more than 50% and hence original secret data cannot be taken out.

5.5 CONCLUSION

With the increased information transversal over insecure networks and other interconnected networks, demand for crucial data protection has also elevated. The proposal exemplifies a hybrid security model used to protect the confidential data used for diverse applications. The proposed scheme offers a highly secured mechanism by inculcating manifold security for data. These are conditional compression followed by dual-stage encryption and finally embedding the modified version of records in Lifting Wave Transformed cover image. This mechanism achieves the following security measures:

- Better confidentiality by modifying the secret data and finally hiding in random locations of frequency-transformed Images.
- Enhanced perceptibility of stego-image by choosing suitable frequency bands in lifting wavelet transformed cover image and conditional compression of the data.
- Perfect reproducibility of retrieving records with zero bit error.
- Improved randomness by adopting the use of Quantum logistic maps for key generation at all the stages of confusion and diffusion processes.

- High speed of execution with the usage of simple yet effective processes at each stage along with the conditional compression phase.

This chapter presented second proposal to achieve confidentiality, optimum time requirements, randomness, reproducibility and authenticity. The mechanism improved in many aspects and can be used for applications, as per strength areas of the mechanism. The next chapter summarizes the research work by presenting the overall conclusion and future research areas for the given work.

Chapter 6

OVERALL CONCLUSION AND FUTURE SCOPE

6.1 OVERALL CONCLUSION

In the existing scenario, digitalization is an inseparable part of everyone's life, consequently requiring the protection of respective electronic records. Also, data reached should be unaltered and safe in all aspects. The mechanisms used extensively are cryptography and steganography. Though, the stand-alone method of either cryptography or steganography alone provides a little shield. Thus, to offer added security to the confidential data, multiple levels of protection are preferred instead of a single-level method. The information security mechanism for ensuring safe communication should meet the given crucial requirements; confidentiality, authenticity, integrity, reproducibility and optimized implementation time. This research work is committed to finding such techniques, which can accomplish most of these requisites.

A wide range of existing algorithms are studied and implemented; for steganography, all spatial and frequency transform domain has been studied and implemented, out of which frequency transform steganography algorithms are considered for further proposals because of optimized results in terms of diverse performance metrics. From the frequency transform domain schemes, Lifting wavelet transform (LWT) with the 'Int2Int' wavelet is the algorithm chosen for blending with other mechanisms as per outcomes of various performance parameters.

On similar lines, studies and comparisons of traditional, Chaos-based and Quantum-chaos based algorithms based on defined performance parameters are carried out in encryption mechanisms. After evaluating the results of all the factors required to identify the best mechanism, the Quantum logistic map-based cryptography mechanism is chosen for multi-layer applications, as it has optimized values of almost all the parameters. The prime objectives of the work conducted in this research are the

design, development and testing of the performance of multi-level security mechanisms to provide optimum values of crucial performance metrics. Before developing the security mechanism, available schemes are studied and implemented to understand better the accessible combinations and gaps between the optimized and actual performance of the methods. Subsequent to the re-evaluation of the literature on existing multi-level techniques, two protection mechanisms are designed. The overall conclusion derived from both mechanisms in terms of providing desirable security characteristics are listed below:

- For both the mechanisms, **Confidentiality** is attained and optimized. In the first mechanism, it is achieved by employing compression, encryption followed by steganography and for watermarked medical image, security layers used are scrambling, compression and then watermarking. In the second mechanism, it is achieved by modifying the confidential data and finally employing LWT steganography at random locations.
- For both the mechanisms, **Imperceptibility** is achieved and optimized. In the first method, it is attained by choosing suitable frequency bands in LWT medical image and reference image. For the second mechanism, imperceptibility in stego-image is accomplished by choosing suitable frequency bands in lifting wavelet transformed cover image and conditional data compression.
- **Biometric authentication** is achieved in the first mechanism by capturing IRIS pattern at both ends (sender and receiver) and then providing access to secret information only after comparing and verifying.
- **Integrity** is achieved in the first mechanism by generating a hash code for the captured IRIS template and comparing it with the respective code on the receiver side for granting access to records.
- Perfect **reproducibility** of records is attained in both the mechanisms by hiding information in such locations from where it can be retrieved without any loss. For the first method, this is verified by extracting EPR with zero bit error and medical images with acceptable bit changes. In the second mechanism, reproducibility of retrieving records with zero bit error is ensured, if an intruder does not modify it. In case of any alterations, reversal of records is not possible.
- The second mechanism achieves the high **computational speed** by employing simple yet effective processes at each stage along with the conditional compression phase.

Both the proposals present optimized values of most of the parameters; this is validated by comparing methods with renowned algorithms in the literature.

6.2 FUTURE SCOPE

The work reported in this research demonstrated the viable mechanisms improved in many aspects and highlighted several potential research directions to be explored in the future. The proposed mechanisms are verified based on numerous performance metrics and validated by comparison with available renowned mechanisms. However, some vital areas need to be worked upon further for such methods to strive towards perfection. All these algorithms are highly secured with sound and complex mathematical computations that make the hacker tedious to breach the data protected by these algorithms. The hardware implementation of algorithms enhances the speed, efficiency and reliability of security standards. FPGA implementations of security algorithms are to increase the speed and decrease delays of software implementations. Millions of logic gates are clustered in FPGA; this brings innovations to existing algorithms, so in order to use these implemented techniques in working applications, hardware implementation of schemes is required so that ready-to-use portable hardware devices can be designed.

REFERENCES

- [1] R. Nambiar and M. Poess, “Transaction performance vs moore’s law: a trend analysis,” in *Technology Conference on Performance Evaluation and Benchmarking*. Springer, 2010, pp. 110–120.
- [2] Statista, “Annual number of data breaches and exposed records in the United States from 2005 to 2022,” <https://shorturl.at/loxN8>, 2022, [Online].
- [3] S. Keelery, “India: number of cyber attacks 2022,” <https://shorturl.at/arFQV>, 2022, [Online].
- [4] H. J. Steve Alder, “June 2019 Healthcare Data Breach Report,” "<https://shorturl.at/brPX3>", 2019, [Online].
- [5] Diplomatist, “Evolution of Indian Defence and Security Industry in Recent Years,” "<https://shorturl.at/FHN12>", 2020, [Online].
- [6] Kaspersky, “Threats on online learning platforms,” "<https://shorturl.at/ctyJP>", 2020, [Online].
- [7] S. Intelligence, “Security in Banking and Finance,” "<https://shorturl.at/DJQRU>", 2021, [Online].
- [8] W. Foundation, “Statistica,” "<https://en.wikipedia.org/wiki/STATISTICA/>", 2017, [Online].
- [9] IBM, “Cost of a Data Breach Report,” <https://www.ibm.com/reports/data-breach>, 2022, [Online].
- [10] S. Dhall, R. Sharma, and S. Gupta, “A multi-level steganography mechanism using quantum chaos encryption,” *Multimedia Tools and Applications*, vol. 79, no. 3, pp. 1987–2012, 2020.
- [11] B. A. Forouzan and D. Mukhopadhyay, *Cryptography and network security*. McGraw Hill Education (India) Private Limited New York, NY, USA, 2015, vol. 12.

- [12] J. Hossain, "Information-hiding using image steganography with pseudorandom permutation," *Bangladesh Research Publications Journal*, vol. 9, no. 3, pp. 215–225, 2014.
- [13] M. Pramanik and K. Sharma, "Analysis of visual cryptography, steganography schemes and its hybrid approach for security of images," *International Journal of Emerging Technology and Advanced Engineering*, vol. 6, no. 2, pp. 174–178, 2014.
- [14] C. Sumathi, T. Santanam, and G. Umamaheswari, "A study of various steganographic techniques used for information hiding," *International Journal of Computer Science & Engineering Survey (IJCSES)*, vol. 4, no. 6, pp. 9–25, 2014.
- [15] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," *Computer*, vol. 31, no. 2, pp. 26–34, 1998.
- [16] S. M. Karim, M. S. Rahman, and M. I. Hossain, "A new approach for LSB based image steganography using secret key," in *14th international conference on computer and information technology (ICIT 2011)*. IEEE, 2011, pp. 286–291.
- [17] R. Sharma, R. Ganotra, S. Dhall, and S. Gupta, "Performance comparison of steganography techniques," *International Journal of Computer Network and Information Security*, vol. 10, no. 9, pp. 37–46, 2018.
- [18] S. Gupta, A. Goyal, and B. Bhushan, "Information hiding using least significant bit steganography and cryptography," *International Journal of Modern Education and Computer Science*, vol. 4, no. 6, p. 27, 2012.
- [19] H. Sheisi, J. Mesgarian, and M. Rahmani, "Steganography: DCT coefficient replacement method and compare with JSteg algorithm," *International Journal of Computer and Electrical Engineering*, vol. 4, no. 4, pp. 458–462, 2012.
- [20] M. Patel and K. R. Patel, "Implementation of digital image watermarking using discrete fractional fourier transform," *International Journal for Scientific Research & Development*, vol. 3, no. 03, pp. 1060–1064, 2015.
- [21] T. Bhaskar and D. Vasumathi, "DCT based watermark embedding into mid frequency of DCT coefficients using luminance component," *International Research Journal of Engineering and Technology (IRJET)*, vol. 2, no. 3, pp. 738–741, 2015.

- [22] J. Abraham and V. Paul, "A DCT based imperceptible color image watermarking scheme," *International Journal of Signal Processing, Image Processing and Pattern Recognition*, vol. 9, no. 7, pp. 137–146, 2016.
- [23] S. P. Ingale and C. Dhote, "Digital watermarking algorithm using DWT technique," *International Journal of Computer Science and Mobile Computing*, vol. 5, no. 5, pp. 1–9, 2016.
- [24] N. Senthilkumaran and S. Abinaya, "Digital image watermarking using DFT algorithm," *Advanced Computing: An International Journal (ACIJ)*, vol. 7, no. 1/2, pp. 9–17, 2016.
- [25] S. B. Dar and A. B. Dar, "Watermarking in frequency domain a review," *International Journal Of Engineering And Computer Science*, vol. 3, no. 11, pp. 9215–9218, 2014.
- [26] M. Matsui, "The first experimental cryptanalysis of the data encryption standard," in *Annual International Cryptology Conference*. Springer, 1994, pp. 1–11.
- [27] E. Barker and N. Mouha, "Recommendation for the triple data encryption algorithm (TDEA) block cipher," National Institute of Standards and Technology, Tech. Rep., 2017.
- [28] Q.-A. Kester, "A hybrid cryptosystem based on vigenère cipher and columnar transposition cipher," *International Journal of Advanced Technology & Engineering Research (IJATER)*, vol. 3, no. 1, pp. 141–147, 2013.
- [29] R. Rayarikar, S. Upadhyay, and P. Pimpale, "SMS encryption using AES algorithm on android," *International Journal of Computer Applications*, vol. 50, no. 19, pp. 12–17, 2012.
- [30] A. Mousa and A. Hamad, "Evaluation of the RC4 algorithm for data encryption," *International Journal of Computer Science & Applications (IJCSA)*, vol. 3, no. 2, pp. 44–56, 2006.
- [31] R. L. Rivest, "The RC5 encryption algorithm," in *International Workshop on Fast Software Encryption*. Springer, 1994, pp. 86–96.
- [32] H. E.-d. H. Ahmed, H. M. Kalash, and O. F. Allah, "Encryption efficiency analysis and security evaluation of RC6 block cipher for digital images," in *2007 International Conference on Electrical Engineering*. IEEE, 2007, pp. 1–7.

- [33] M. Francois, T. Grosjes, D. Barchiesi, and R. Erra, "A new image encryption scheme based on a chaotic function," *Signal Processing: Image Communication*, vol. 27, no. 3, pp. 249–259, 2012.
- [34] I. S. Sam, P. Devaraj, and R. S. Bhuvaneshwaran, "A novel image cipher based on mixed transformed logistic maps," *Multimedia tools and applications*, vol. 56, no. 2, pp. 315–330, 2012.
- [35] G. Hanchinamani and L. Kulkarni, "An efficient image encryption scheme based on a Peter De Jong chaotic map and a RC4 stream cipher," *3D Research*, vol. 6, no. 3, pp. 1–15, 2015.
- [36] I. Shatheesh Sam, P. Devaraj, and R. Bhuvaneshwaran, "An intertwining chaotic maps based image encryption scheme," *Nonlinear Dynamics*, vol. 69, no. 4, pp. 1995–2007, 2012.
- [37] R. Bansal, S. Gupta, and G. Sharma, "An innovative image encryption scheme based on chaotic map and vigenère scheme," *Multimedia Tools and Applications*, vol. 76, no. 15, pp. 16 529–16 562, 2017.
- [38] A. Akhshani, A. Akhavan, S.-C. Lim, and Z. Hassan, "An image encryption scheme based on quantum logistic map," *Communications in Nonlinear Science and Numerical Simulation*, vol. 17, no. 12, pp. 4653–4661, 2012.
- [39] A. A. Abd El-Latif, L. Li, N. Wang, Q. Han, and X. Niu, "A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces," *Signal Processing*, vol. 93, no. 11, pp. 2986–3000, 2013.
- [40] H. Liu and C. Jin, "A novel color image encryption algorithm based on quantum chaos sequence," *3D Research*, vol. 8, no. 1, pp. 1–13, 2017.
- [41] N. Zhou, W. Chen, X. Yan, and Y. Wang, "Bit-level quantum color image encryption scheme with quantum cross-exchange operation and hyper-chaotic system," *Quantum Information Processing*, vol. 17, no. 6, pp. 1–24, 2018.
- [42] X. Liu, D. Xiao, and Y. Xiang, "Quantum image encryption using intra and inter bit permutation based on logistic map," *IEEE Access*, vol. 7, no. 1, pp. 6937–6946, 2018.
- [43] R. Nivedhitha, D. T. Meyyappan, and M. Phil, "Image security using steganography and cryptographic techniques," *international journal of engineering trends and technology*, vol. 3, no. 3, pp. 366–371, 2012.

- [44] A. K. Nain, S. Gupta, B. Bhushan, and R. Chawla, “An adaptive pseudorandom stego-crypto technique for data communication,” *International journal of Computer Networks & Communications*, vol. 5, no. 4, pp. 173–188, 2013.
- [45] N. Solanki and S. K. Malik, “ROI based medical image watermarking with zero distortion and enhanced security,” *International Journal of Education and Computer Science*, vol. 10, no. 6, pp. 40–48, 2014.
- [46] M. R. Islam, A. Siddiqa, M. P. Uddin, A. K. Mandal, and M. D. Hossain, “An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography,” in *2014 International Conference on Informatics, Electronics & Vision (ICIEV)*. IEEE, 2014, pp. 1–6.
- [47] Y. Jain, G. Sharma, G. Anand, and S. Dhall, “A hybrid security mechanism based on DCT and visual cryptography for data communication networks,” in *Cyber security*. Springer, 2018, pp. 131–142.
- [48] A. Tauhid, M. Tasnim, S. A. Noor, N. Faruqui, and M. A. Yousuf, “A secure image steganography using advanced encryption standard and discrete cosine transform,” *Journal of Information Security*, vol. 10, no. 3, pp. 117–129, 2019.
- [49] S. Solak, “High embedding capacity data hiding technique based on EMSD and LSB substitution algorithms,” *IEEE Access*, vol. 8, no. 1, pp. 166 513–166 524, 2020.
- [50] N. Mukherjee (Ganguly), G. Paul, S. K. Saha, and D. Burman, “A PVD based high capacity steganography algorithm with embedding in non-sequential position,” *Multimedia Tools and Applications*, vol. 79, no. 19, pp. 13 449–13 479, 2020.
- [51] S. Vatshayan, R. A. Haidri, and J. K. Verma, “Design of hybrid cryptography system based on Vigenère cipher and polybius cipher,” in *2020 International Conference on Computational Performance Evaluation (ComPE)*. IEEE, 2020, pp. 848–852.
- [52] A. Sharma, A. K. Singh, and S. P. Ghrera, “Robust and secure multiple watermarking for medical images,” *Wireless Personal Communications*, vol. 92, no. 4, pp. 1611–1624, 2017.
- [53] D. Chaudhary, S. Gupta, and M. Kumari, “A novel hybrid security mechanism for data communication networks,” *International Journal of information privacy, Security and integrity*, vol. 2, no. 3, pp. 216–231, 2016.

- [54] M. Elhoseny, G. Ramírez-González, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar, and A. Farouk, “Secure medical data transmission model for IoT-based healthcare systems,” *IEEE Access*, vol. 6, pp. 20 596–20 608, 2018.
- [55] S. Priya and B. Santhi, “A novel visual medical image encryption for secure transmission of authenticated watermarked medical images,” *Mobile networks and applications*, vol. 26, no. 6, p. 2501–2508, 2019.
- [56] K. N. Jassim, A. K. Nsaif, A. K. Nseaf, A. H. Hazidar, B. Priambodo, E. Naf’an, M. Masril, I. Handriani, and Z. P. Putra, “Hybrid cryptography and steganography method to embed encrypted text message within image,” in *Journal of Physics: Conference Series*, vol. 1339, no. 1, 2019, pp. 1–9.
- [57] A. Hambouz, Y. Shaheen, A. Manna, M. Al-Fayoumi, and S. Tedmori, “Achieving data integrity and confidentiality using image steganography and hashing techniques,” in *2019 2nd international conference on new trends in computing sciences (ICTCS)*. IEEE, 2019, pp. 1–6.
- [58] C. Biswas, U. D. Gupta, and M. M. Haque, “An efficient algorithm for confidentiality, integrity and authentication using hybrid cryptography and steganography,” in *2019 international conference on electrical, computer and communication engineering (ECCE)*. IEEE, 2019, pp. 1–5.
- [59] M. S. Hossen, M. A. Islam, T. Khatun, S. Hossain, and M. M. Rahman, “A new approach to hiding data in the images using steganography techniques based on AES and RC5 algorithm cryptosystem,” in *2020 International Conference on Smart Electronics and Communication (ICOSEC)*. IEEE, 2020, pp. 676–681.
- [60] A. K. Singh, B. Kumar, M. Dave, and A. Mohan, “Robust and imperceptible dual watermarking for telemedicine applications,” *Wireless Personal Communications*, vol. 80, no. 4, pp. 1415–1433, 2015.
- [61] N. Tayal, R. Bansal, S. Dhal, and S. Gupta, “A novel hybrid security mechanism for data communication networks,” *Multimedia Tools and Applications*, vol. 76, no. 22, pp. 24 063–24 090, 2017.
- [62] R. Saini and N. Rana, “Comparison of various biometric methods,” *International Journal of Advances in Science and Technology*, vol. 2, no. 1, pp. 24–30, 2014.
- [63] S. N. Bal, M. R. Nayak, and S. K. Sarkar, “On the implementation of a secured watermarking mechanism based on cryptography and bit pairs matching,” *Journal of King Saud University-Computer and Information Sciences*, vol. 33, no. 5, pp. 552–561, 2021.

- [64] Y. Jain, S. Dhall, and S. Gupta, "A robust multilevel security mechanism against geometric attacks," in *2019 3rd International Conference on Recent Developments in Control, Automation & Power Engineering (RDCAPE)*. IEEE, 2019, pp. 220–226.
- [65] Z. K. Al-Ani, A. Zaidan, B. Zaidan, and H. Alanazi, "Overview: Main fundamentals for steganography," *Journal of Computing*, vol. 2, no. 3, pp. 158–165, 2010.
- [66] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM systems journal*, vol. 35, no. 34, pp. 313–336, 1996.
- [67] A. A. Abdulla, "Exploiting similarities between secret and cover images for improved embedding efficiency and security in digital steganography," Ph.D. dissertation, University of Buckingham, 2015.
- [68] F. S. Abed, "A proposed method of information hiding based on hybrid cryptography and steganography," *International Journal of Application or Innovation in Engineering & Management*, vol. 2, no. 4, pp. 530–539, 2013.
- [69] M. T. Sandford II, J. N. Bradley, and T. G. Handel, "Data embedding method," in *Integration Issues in Large Commercial Media Delivery Systems*, vol. 2615, 1996, pp. 226–259.
- [70] S. Dhall, B. Bhushan, and S. Gupta, "An in-depth analysis of various steganography techniques," *International Journal of Security and Its Applications*, vol. 9, no. 8, pp. 67–94, 2015.
- [71] N. Tayal, S. Dhall, and S. Gupta, "A robust hybrid steganography mechanism for security in data communication networks," *International Journal of Computer Networks and Applications (IJCNA)*, vol. 3, no. 3, pp. 2395–0455, 2016.
- [72] P. Shi and Z. Li, "An improved BPCS steganography based on dynamic threshold," in *2010 International Conference on Multimedia Information Networking and Security*. IEEE, 2010, pp. 388–391.
- [73] S. P. Bansod, V. M. Mane, and R. Ragha, "Modified BPCS steganography using hybrid cryptography for improving data embedding capacity," in *2012 International Conference on Communication, Information & Computing Technology (ICCICT)*. IEEE, 2012, pp. 1–6.
- [74] E. Kawaguchi, "BPCS steganography-principle and applications," in *International Conference on Knowledge-Based and Intelligent Information and Engineering Systems*. Springer, 2005, pp. 289–299.

- [75] A. Chopra, S. Gupta, and S. Dhall, "Analysis of frequency domain watermarking techniques in presence of geometric and simple attacks," *Multimedia Tools and Applications*, vol. 79, no. 1, pp. 501–554, 2020.
- [76] M. Irfan, L. Zheng, and H. Shahzad, "Research article review of computing algorithms for discrete fractional fourier transform," *Research Journal of Applied Sciences, Engineering and Technology*, vol. 6, no. 11, pp. 1911–1919, 2013.
- [77] H.-J. L. Chen, "A DWT based approach for image steganography," *International Journal of Applied Science and Engineering*, vol. 4, no. 3, pp. 275–290, 2006.
- [78] M. M. Chaudhari and K. Pawar, "Stationary wavelet transform based steganography for transmitting images," *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 4, no. 12, pp. 12 064–12 069, 2015.
- [79] K. Jangde and R. Raja, "Image compression based on discrete wavelet and lifting wavelet transform technique," *International Journal of Science, Engineering and Technology Research*, vol. 3, no. 3, pp. 394–399, 2014.
- [80] M. Kalita, T. Tuithung, and S. Majumder, "A new steganography method using integer wavelet transform and least significant bit substitution," *The Computer Journal*, vol. 62, no. 11, pp. 1639–1655, 2019.
- [81] M. Kumari, S. Gupta, and P. Sardana, "A survey of image encryption algorithms," *3D Research*, vol. 8, no. 4, pp. 1–35, 2017.
- [82] A. Malik, S. Gupta, and S. Dhall, "Analysis of traditional and modern image encryption algorithms under realistic ambience," *Multimedia Tools and Applications*, vol. 79, no. 37, pp. 27 941–27 993, 2020.
- [83] W. P. Wardlaw, "The RSA public key cryptosystem," in *Coding theory and cryptography*. Springer, 2000, pp. 101–123.
- [84] B. Furht, "The RSA public-key encryption algorithm," pp. 757–757, 2006.
- [85] P. V. Chavan and M. Atique, "Design of hierarchical visual cryptography," in *2012 Nirma University International Conference on Engineering (NUiCONE)*. IEEE, 2012, pp. 1–3.
- [86] D. Bouslimi, G. Coatrieux, and C. Roux, "A joint encryption/watermarking algorithm for verifying the reliability of medical images: application to echographic images," *Computer methods and programs in biomedicine*, vol. 106, no. 1, pp. 47–54, 2012.

- [87] A. K. Singh, M. Dave, and A. Mohan, "Hybrid technique for robust and imperceptible multiple watermarking using medical images," *Multimedia Tools and Applications*, vol. 75, no. 14, pp. 8381–8401, 2016.
- [88] L.-T. Ko, J.-E. Chen, Y.-S. Shieh, H.-C. Hsin, and T.-Y. Sung, "Nested quantization index modulation for reversible watermarking and its application to healthcare information management systems," *Computational and mathematical methods in medicine*, vol. 2012, no. 1, pp. 1–8, 2012.
- [89] A. Kannammal and S. Subha Rani, "Two level security for medical images using watermarking/encryption algorithms," *International Journal of Imaging Systems and Technology*, vol. 24, no. 1, pp. 111–120, 2014.
- [90] B. Lei, E.-L. Tan, S. Chen, D. Ni, T. Wang, and H. Lei, "Reversible watermarking scheme for medical image based on differential evolution," *Expert Systems with Applications*, vol. 41, no. 7, pp. 3178–3188, 2014.
- [91] L. Bao and Y. Zhou, "Image encryption: Generating visually meaningful encrypted images," *Information Sciences*, vol. 324, no. 1, pp. 197–207, 2015.
- [92] N. A. Loan, S. A. Parah, J. A. Sheikh, J. A. Akhoun, and G. M. Bhat, "Hiding electronic patient record (EPR) in medical images: a high capacity and computationally efficient technique for e-healthcare applications," *Journal of biomedical informatics*, vol. 73, no. 1, pp. 125–136, 2017.
- [93] S. M. Mousavi, A. Naghsh, A. A. Manaf, and S. Abu-Bakar, "A robust medical image watermarking against salt and pepper noise for brain MRI images," *Multimedia Tools and Applications*, vol. 76, no. 7, pp. 10 313–10 342, 2017.
- [94] A. Umamageswari, M. F. Ukrit, and G. Suresh, "A survey on security in medical image communication," *International Journal of Computer Applications*, vol. 30, no. 3, pp. 41–45, 2011.
- [95] M. Moizuddin, J. Winston, and M. Qayyum, "A comprehensive survey: quantum cryptography," in *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*. IEEE, 2017, pp. 98–102.
- [96] K. Baeksays and T. Engerssays, "Chaos theory and the logistic map," "<https://shorturl.at/bdxS6>", 2016, [Online, Geoff Boeing].
- [97] Y. Wu, J. P. Noonan, and S. Aghaian, "NPCR and UACI randomness tests for image encryption," *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT)*, vol. 1, no. 2, pp. 31–38, 2011.

- [98] R. Y. F. Ng, Y. H. Tay, and K. M. Mok, "A review of iris recognition algorithms," in *2008 International Symposium on Information Technology*. IEEE, 2008, pp. 1–7.
- [99] L. Masek, "Matlab source code for a biometric identification system based on iris patterns," <http://people.csse.uwa.edu.au/pk/studentprojects/libor/>, 2003.
- [100] B. Chauhan, S. Dhall, and S. Gupta, "A comparison of various hashing techniques," *International Journal of Computer Networks and Applications (IJCNA)*, vol. 2, no. 4, pp. 1–6, 2015.
- [101] G. Sharma, S. Gupta, S. Dhall, and C. K. Nagpal, "Publicly verifiable watermarking scheme for intellectual property protection using quantum chaos and bit plane complexity slicing," *Multimedia Tools and Applications*, vol. 77, no. 24, pp. 31 737–31 762, 2018.
- [102] T.-G. Gao and Q.-L. Gu, "Reversible watermarking algorithm based on wavelet lifting scheme," in *2007 international conference on wavelet analysis and pattern recognition*. IEEE, 2007, pp. 1771–1775.
- [103] M. Gholipour, "Design and implementation of lifting based integer wavelet transform for image compression applications," in *International Conference on Digital Information and Communication Technology and Its Applications*. Springer, 2011, pp. 161–172.
- [104] Y. Yan and Z. Dong, "An approach to integer wavelet transform for medical image compression in PACS," *Wuhan University Journal of Natural Sciences*, vol. 5, no. 2, pp. 204–206, 2000.
- [105] L. Wu, J. Zhang, W. Deng, and D. He, "Arnold transformation algorithm and anti-arnold transformation algorithm," in *2009 first international conference on information science and engineering*. IEEE, 2009, pp. 1164–1167.
- [106] R. Shelke and S. Metkar, "Image scrambling methods for digital image encryption," in *2016 International Conference on Signal and Information Processing (IconSIP)*. IEEE, 2016, pp. 1–6.
- [107] N. Tayal, R. Bansal, S. Gupta, and S. Dhall, "Analysis of various cryptography techniques: a survey," *International Journal of Security and Its Applications*, vol. 10, no. 8, pp. 59–92, 2016.
- [108] P. Yellamma and N. Challa, "Performance Analysis Of Different Data Compression Techniques on Text File," *International Journal of Engineering Research & Technology*, vol. 1, no. 8, pp. 1–6, 2012.

BRIEF BIODATA OF THE RESEARCH SCHOLAR

Ms. Sangeeta Dhall (sangeeta_dhall@jcboseust.ac.in) received B.Tech degree in Instrumentation and Control Engineering from REC Jalandhar, and obtained M.Tech degree in Electronics and Instrumentation from J.C.Bose University of Science & Technology, YMCA Faridabad. She is pursuing her Ph. D in the area of information security from J.C.Bose University of Science & Technology, YMCA Faridabad.

Her academic interests include network security, embedded systems, and digital system design. She is currently working as an Assistant Professor in the Department of Electronics Engineering at J.C. Bose University of Science & Technology, YMCA Faridabad, India. She has presented and published more than 30 research papers in various International and National conferences and journals and has teaching experience of more than 20 years.

LIST OF PUBLICATIONS OUT OF THESIS

LIST OF PUBLISHED PAPERS

S.No	Title of Paper	Name of Journal where published	No.	Volume and Issue	Year	Pages
1.	A Multi-Level Steganography Mechanism Using Quantum Chaos Encryption	Multimedia Tools and Applications, Springer Nature 2019	1573-7721	Volume 79, Issue 3-4	November 2019	1987–2012
2.	Multilayered Highly Secure Authentic Watermarking Mechanism for Medical Applications	Multimedia Tools and Applications, Springer Nature 2021	1573-7721	Volume 80, Issue 12	February 2021	18069-18105
3.	Quantum Based Robust and Swift Hybrid Security Mechanism	Multimedia Tools and Applications, Springer Nature 2022	1573-7721	Volume 81, Issue 30	May 2022	43727–43752

LIST OF PAPERS PRESENTED IN CONFERENCE

S.No	Title of Paper	Name of Conference	No.	Volume and Issue	Year	Pages
1.	Multilevel Security Mechanism against Geometric attacks	RDCAPE-2019	IEEE, (IEEE conference ID: 47089)	Scopus	2019	10-11 October, 2019
2.	Security mechanism based on Quantum Logistic Map in Discrete Wavelet Transform Domain	TAME-2021	Department of Mechanical Engineering, JCBUST, YMCA	Under TEQIP-3	2021	18-19 March, 2021
3.	Comparative Analysis of Data Compression Algorithms	ICASEE-2021	Department of Electrical Engineering, JCBUST, YMCA Faridabad	Under TEQIP-3	2021	16-17 April, 2021