

DESIGN AND ANALYSIS OF AN EFFICIENT
SECURED MECHANISM FOR PRESERVING IMAGE
CONFIDENTIALITY

THESIS

Submitted in fulfillment of the requirement of the degree of

DOCTOR OF PHILOSOPHY

to

FACULTY OF ENGINEERING AND TECHNOLOGY

by

Manju Kumari

Regn. No.: YMCAUST/PH03/2015

Under the Supervision of

Dr. Shailender Gupta



Department of Electronics Engineering
J.C. Bose University of Science and Technology, YMCA
Faridabad-121006, (Haryana), India

APRIL 2023

Dedicated to my beloved Parents.

DECLARATION

I hereby declare that the thesis entitled “**DESIGN AND ANALYSIS OF AN EFFICIENT SECURED MECHANISM FOR PRESERVING IMAGE CONFIDENTIALITY**” by **MANJU KUMARI**, being submitted in fulfilment of the requirements for the Degree of Doctor of Philosophy in Department of Electronics Engineering under Faculty of Engineering and Technology of J.C. Bose University of Science and Technology, YMCA, Faridabad, during the academic year 2022-23, is a bonafide 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.

MANJU KUMARI

Regn. No.: YMCAUST/Ph03/2015

CERTIFICATE

This is to certify that the thesis entitled “**DESIGN AND ANALYSIS OF AN EFFICIENT SECURED MECHANISM FOR PRESERVING IMAGE CONFIDENTIALITY**” by **MANJU KUMARI**, submitted in fulfilment of the requirements for the Degree of Doctor of Philosophy in **DEPARTMENT OF ELECTRONICS ENGINEERING** under Faculty of Engineering and Technology of J.C. Bose University of Science and Technology, YMCA, Faridabad, 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

Date:

ACKNOWLEDGMENTS

First and foremost, I bow in gratitude to the **Almighty God**, who showered his gracious blessings on me by letting me through all the difficulties with imparted strength to accomplish this work. I will keep on trusting you for my future.

I would like to acknowledge and give my warmest thanks to my supervisor, **Dr. Shailender Gupta**, who made this work possible. Without his inventive ideas, unwavering support, and encouragement, I would never have been able to advance this thesis to this point.

I'd like to express my gratitude to all of my colleagues in the University's Department of Electronics Engineering for their support throughout the course. My special thanks to **Prof. Pradeep Kumar Dimri**, Chairperson of the department, for his insightful recommendations that aided me tremendously during my journey. I would like to convey my heartfelt appreciation to **Prof. Munish Vashishath** and **Prof. Neelam Turk**, in the Department of Electronics Engineering for their support and constructive discourse.

I am grateful to **Mr. Bharat Bhushan, Ms. Sangeeta Dhall, Ms. Sunita Chaudhary, Dr. Lalit Rai, Dr. Prashant Kumar** and **Ms. Nisha Yadav** for their suggestions, encouragement, and constructive dialogues during my difficult times.

I want to express my special thanks **Mr. Pranshul Sardana, Mr. Ritesh Bansal, Ms. Anjali Malik, Ms. Pratibha Rani, Mr. Gaurav , Ms. Reema,** and **Ms. Lavita Virmani** for their support during the time of this course.

Above all, words fail to express my regards for my parents, **Sh. Narender Kumar Nimesh** and **Smt. Kunti**. They consistently instilled tremendous confidence and belief in me and encouraged me to overcome every adversity and obstacle in my life. . Without your blessings, prayers, and pure love, I would have accomplished nothing in my life.

My sincere gratitude and appreciation to my brothers **Mr. Gaurav Nimesh** and **Mr. Saurav Nimesh** for their unwavering support, encouragement, and patience throughout my life and studies. without their lifetime of hard work and support, I would not have reached where I am.

All my life accomplishments to my lovely sisters **Ms. Anju** and **Ms. Madhu**, who have been a constant source of hope and fortitude in the face of adversity. Their encouragement and joyous behaviour have always motivated me to strive for greater personal and emotional growth.

I thank them above all else for helping me chase my dreams against all odds..

MANJU KUMARI

Regn. No.: YMCAUST/PH03/2015

ABSTRACT

The exponential increase in data transfer over public networks has risen multiple times in the last two decades. With this, the number of online exposed data breaches and theft has also risen resulting into huge monetary loss. About 5000 million USD were lost in the year 2021 due to all this. Therefore, it becomes mandatory for individuals and professionals to safeguard their confidential data from unauthorized access. It is thus mandatory that the information to be transferred should be transformed in such a manner that it should be meaningless to unintended users. In other words, the information must be confidential to the intended users. The widespread solution for maintaining confidential information is 'Cryptography' that is an art of transforming message to an unreadable form for intruders thus making the communication secure.

In the early stages of Cryptography simple substitution and shifting procedure were used for encryption and decryption of textual data that has low degree of correlation value among neighboring characters. With the development in the internet and multimedia technology, the contents like images and videos were also used in data transfer. Though, the Traditional Techniques were good but failed to provide good execution speed due to large size of data. Also, the Traditional Techniques were unsuccessful against statistical and differential attacks. To cater this Chaos Based Encryption Techniques were developed. These are based on mathematical Chaos Theory focusing on the study of Chaos Dynamical Systems whose apparently random states of disorder and irregularities are governed by underlying patterns and deterministic laws that are highly sensitive to initial conditions. Using this, random numbers can be generated at a very fast rate. Thus, multimedia data like image, document and video can be encrypted easily.

The Chaos Based Encryption Techniques were good in comparison to Traditional ones in terms of parameters like Key Space and Randomness. With the above things in mind, an encryption technique based on Intertwining Chaotic Maps and RC4 Stream Cipher was proposed. The scheme employed Chaotic Map for the Confusion Process and key generation for RC4 Cipher. The RC4 Cipher uses this key to generate random sequences which are used to implement an efficient Diffusion Process. The technique provides highly scrambled Cipher Images and can resist Statistical and Brute-Force Search Attacks. The Peak Signal-to-Noise Ratio values are comparable to other techniques, the Entropy Values are close to ideal value. In addition, the technique is very much practical since having lowest execution time then its counterparts. It almost outperformed all the techniques of that period in terms of many parameters but failed to pass the theoretical value of the UACI Test. The reason was that the usage of Byte Level permutation/ substitution, Diffusion in only four directions i.e. in backward and forward direction, and Logistic Maps used for generation of random key.

To further enhance security the Quantum Logistic Maps were used as these generate non-periodic random numbers. Also, Quantum Logistic Maps generate random numbers better than Chaotic Maps. Hence, an image encryption technique based on Quantum Logistic Maps was proposed which provides a good random Cipher Image. In this proposal, encryption mechanism comprised of multiple processes and each process is key dependent utilizing diverse keys to ensure high key sensitivity and resistant towards Differential Attack. The keys are generated using Quantum Chaotic Map. For the Confusion Process, Electronic Code Book (ECB), Initial Permutation (IP), Bit Plane Scrambling, and Inter-bit Plane Scrambling were employed. The ECB and IP, being matching processes are chosen for high speed of execution. Bit level permutation unlike byte level is applied to reinforce randomness, in conjunction with variable number of rounds as per the security key. For Diffusion Process, the folding technique is used along eight directions, exploiting different keys. This technique outperformed almost all its counter parts in terms of performance metrics like Key Space, PSNR and Entropy values. Also, the technique passed Differential and Statistical Attacks along with comparable execution time.

CONTENTS

DECLARATION	i
CERTIFICATE	ii
ACKNOWLEDGMENTS	iii
ABSTRACT	iv
CONTENTS	vi
LIST OF FIGURES	x
LIST OF TABLES	xiii
LIST OF ABBREVIATIONS	xiv
1 INTRODUCTION	1
1.1 INTRODUCTION TO CONFIDENTIALITY	1
1.2 CONFIDENTIALITY USING CRYPTOGRAPHY	2
1.3 CLASSIFICATION OF CRYPTOGRAPHY TECHNIQUES	4
1.3.1 Traditional Cryptography Techniques	5
1.3.2 Chaos Based Cryptography Techniques	5
1.3.3 Quantum Chaos Based Cryptography Techniques	6
1.4 LITERATURE SURVEY	7
1.5 PROBLEM DEFINITION	12
1.6 OBJECTIVES	12
1.7 TOOL USED	13
1.8 SIMULATION SET-UP PARAMETERS	13
1.9 PERFORMANCE METRICS	14
1.9.1 Image Perceptual Quality	14
1.9.2 Statistical Attack Parameters	14
1.9.3 Differential Attack Parameters	15
1.9.4 Quantitative Parameters	16
1.9.5 Key Space	17

1.9.6	Execution Time	17
1.10	PROPOSED IMAGE ENCRYPTION TECHNIQUES	17
1.10.1	Proposed Technique 1: A Novel Image Encryption Technique Based on Intertwining Chaotic Maps and RC4 Stream Cipher	18
1.10.2	Proposed Technique 2: A Superlative Image Encryption Tech- nique Based on Bit Plane Using Key-Based Electronic Code Book	22
1.11	OBJECTIVES vs OUTCOMES	26
1.12	OVERALL CONCLUSION	28
1.13	ORGANIZATION OF THESIS	29
2	LITERATURE SURVEY	31
2.1	INTRODUCTION TO CONFIDENTIALITY	31
2.2	SIMULATION SET-UP PARAMETERS FOR LITERATURE SURVEY	32
2.3	TYPES OF CRYPTOGRAPHY TECHNIQUES	33
2.4	TRADITIONAL CRYPTOGRAPHY TECHNIQUES	35
2.4.1	Vigenère Cipher	35
2.4.2	Data Encryption Standard	36
2.4.3	International Data Encryption Algorithm	38
2.4.4	Blowfish	40
2.4.5	Visual Cryptography	42
2.4.6	Rivest Cipher 4	43
2.4.7	Rivest Cipher 5	44
2.4.8	Rivest Cipher 6	46
2.4.9	Triple Data Encryption Standard	46
2.4.10	Advanced Encryption Standard	49
2.4.11	Comparison of Traditional Cryptography Techniques	51
2.5	CHAOS CRYPTOGRAPHY TECHNIQUES	53
2.5.1	Chaos 1: A New Image Encryption Scheme Based on Chaotic Function using Linear Congruence	53
2.5.2	Chaos 2: An Intertwining Chaotic Maps-based Image Encryp- tion Scheme	55
2.5.3	Chaos 3: A Novel Image Cipher Based on Mixed Transformed Logistic Map	57
2.5.4	Chaos 4: An Effective Image Encryption Scheme Based on Pe- ter De Jong Chaotic Map and RC4 Stream Cipher	58
2.5.5	Chaos 5: An Innovative Image Encryption Scheme Based on Chaotic Map and Vigenère Scheme	59
2.5.6	Comparison of Chaos Cryptography Techniques	62
2.6	QUANTUM CHAOS CRYPTOGRAPHY TECHNIQUES	64

2.6.1	Quantum Chaos 1: An Image Encryption Scheme Based on Quantum Logistic Map	65
2.6.2	Quantum Chaos 2: A New Approach to Chaotic Image Encryption Based on Quantum Chaotic System, Exploiting Color Spaces	65
2.6.3	Quantum Chaos 3: A Novel Color Image Encryption Algorithm Based on Quantum Chaos Sequence	68
2.6.4	Quantum Chaos 4: Bit Level Quantum Color Image Encryption Scheme with Quantum Cross-Exchange Operation and Hyper Chaotic System	72
2.6.5	Quantum Chaos 5: Quantum Image Encryption using Intra and Inter Bit Permuted Based on Logistic Map	74
2.6.6	Comparison of Quantum Chaos Cryptography Techniques	76
2.7	OVERALL COMPARISON	77
3	A NOVEL IMAGE ENCRYPTION TECHNIQUE BASED ON INTER-TWING CHAOTIC MAPS AND RC4 STREAM CIPHER	79
3.1	INTRODUCTION	79
3.2	PROPOSED ENCRYPTION TECHNIQUE	81
3.2.1	Key Generation using Intertwining Chaotic Map	82
3.2.2	Random Sequence Generation using RC4 Stream Cipher	84
3.2.3	Diffusion Process	85
3.2.4	Confusion Process	87
3.3	DECRYPTION	87
3.4	ALGORITHM EXPLANATION	88
3.5	SIMULATION SETUP PARAMETERS	89
3.6	RESULTS	91
3.6.1	Visual Analysis	91
3.6.2	Statistical Attack Analysis	91
3.6.3	Differential Attack Analysis	95
3.6.4	Key Space	96
3.6.5	Quantitative Analysis	97
3.6.6	Execution Time	99
3.7	CONCLUSION	99
4	A SUPERLATIVE IMAGE ENCRYPTION TECHNIQUE BASED ON BIT PLANE USING KEY-BASED ELECTRONIC CODE BOOK	101
4.1	INTRODUCTION	101
4.2	PROPOSED ENCRYPTION SCHEME	103
4.3	ENCRYPTION PROCESS	103

4.3.1	Key Generation	104
4.3.2	Confusion Process	107
4.3.3	Diffusion Process	110
5	SIMULATION SET-UP PARAMETERS AND RESULTS	113
5.1	SIMULATION SETUP PARAMETERS	113
5.2	RESULTS AND DISCUSSIONS	114
5.2.1	Visual Analysis	114
5.2.2	Statistical Attack Analysis	114
5.2.3	Differential Attack Analysis	120
5.2.4	Key Space Analysis	122
5.2.5	Quantitative Analysis	122
5.2.6	Execution Time	124
5.2.7	Cryptanalysis	124
5.3	OVERALL COMPARISON	125
6	CONCLUSION AND FUTURE SCOPE	131
6.1	OVERALL CONCLUSION	131
6.2	FUTURE RESEARCH DIRECTIONS	132
	REFERENCES	133
	BRIEF PROFILE	147
	LIST OF PAPERS PUBLISHED IN JOURNALS	149
	LIST OF PAPERS PRESENTED IN CONFERENCES	151

LIST OF FIGURES

1.1	Communication Network	1
1.2	Recorded Data Breaches or Exposed Records and Corresponding Monetary Damages Caused by Cybercrimes in United States on Annual Basis	2
1.3	Process of Cryptography	3
1.4	Classification of Cryptography Techniques	4
1.5	Proposed Cryptography Techniques	17
1.6	Block Diagram of Encryption Process of Proposed Technique 1	18
1.7	Block Diagram of Encryption Process of Proposed Technique 2	22
2.1	Block Diagram of Vigenère Cipher	36
2.2	Block Diagram of Data Encryption Standard	37
2.3	Block Diagram of International Data Encryption Algorithm	39
2.4	Block Diagram of Blowfish Algorithm	41
2.5	Block Diagram of Visual Cryptography	42
2.6	Block Diagram of Rivest Cipher 4	43
2.7	Block Diagram of Rivest Cipher 5	45
2.8	Block Diagram of Rivest Cipher 6	47
2.9	Block Diagram of Triple Data Encryption Standard	48
2.10	Block Diagram of Advanced Encryption Standard	50
2.11	Chaos Based Image Encryption Technique	53
2.12	Block Diagram of Technique Based on Chaotic Function Using Linear Congruence	54
2.13	Block Diagram of Technique Based on Intertwining Chaotic Maps	56
2.14	Zig-zag Diffusion	57
2.15	Block Diagram of Technique Based on Mixed Transformed Logistic Map	58
2.16	Block Diagram of Technique Based on Peter De Jong Chaotic Map and RC4 Stream Cipher	60
2.17	Block Diagram of Technique Based on Chaotic Maps and Vigenère Scheme	62
2.18	Chaos Based Image Encryption Technique	64
2.19	Block Diagram of Image Encryption Technique Based on Quantum Logistic Map	66

2.20	Block Diagram of Technique Based on Quantum Chaotic System, Exploiting Color Spaces	67
2.21	Block Diagram of Color Image Encryption Algorithm Based on Quantum Chaos Sequence	69
2.22	Block Diagram of Technique Based on Quantum Cross Exchange Operation and Hyper Chaotic System	73
2.23	Block Diagram of Technique Using Intra and Inter Bit Permutation Based on Logistic Map	75
3.1	Annual Number of Ransomware Families Attacks	80
3.2	Block Diagram of Encryption Process of Proposed Technique	81
3.3	Key Generation Using Intertwining Chaotic Map	83
3.4	Hierarchy of Diffusion Process	85
3.5	Confusion Process of Proposed Technique	87
3.6	Graph of Correlation Coefficient of Original and Encrypted Images of Proposed Technique	94
3.7	Graph of Comparison of Correlation Coefficients of the Proposed and Other Chaos Techniques	95
3.8	Graph of PSNR Values of the Proposed and Other Chaos Techniques	97
3.9	Graph of Information Entropy of Original and Encrypted Images	98
3.10	Graph of Execution Time of Proposed and Other Techniques	98
4.1	Block Diagram of Encryption and Decryption Process of the Proposed Technique	104
4.2	Block Diagram of Confusion Process	107
4.3	Block Diagram of Diffusion Process	110
5.1	Graph Depicting Horizontal Correlation Graphs Respectively Compared with the Chaos and Quantum Chaos Techniques for 256×256 and 512×512 Size Images	119
5.2	Graph Depicting Vertical Correlation Graphs Respectively Compared with the Chaos and Quantum Chaos Techniques for 256×256 and 512×512 Size Images	119
5.3	Graph Depicting Diagonal Correlation Graphs Respectively Compared with the Chaos and Quantum Chaos Techniques for 256×256 and 512×512 Size Images	120
5.4	Graph Comparing PSNR Values of Proposed Technique with the Chaos and Quantum Chaos Techniques for 256×256 and 512×512 Images	123
5.5	Graph Depicting Entropy Values of Proposed and Different Techniques of Different Sizes	123

5.6	Graph Depicting Execution Time of Encryption for Two Different Size Images	124
-----	--	-----

LIST OF TABLES

1.1	Performance Parameters for Literature Survey	7
1.2	Literature Survey of Traditional Techniques	9
1.3	Literature Survey of Chaos Based Encryption Techniques	10
1.4	Literature Survey of Quantum Chaos Based Encryption Techniques . . .	11
1.5	Simulation Set-up Parameters for Proposed Technique 1 and Proposed Technique 2	14
1.6	Results of Proposed Technique 1	20
1.7	Results of Proposed Technique 2	24
1.8	Comparisons of Traditional, Chaos and Quantum Chaos Based Cryptography Techniques	27
2.1	Simulation Set-up Parameters for Literature Survey	32
2.2	Vigenère Table	35
2.3	Overall Comparison of Traditional Cryptography Techniques	51
2.4	Key Scheming	59
2.5	Details of Key Generation for Encryption Process	61
2.6	Overall Comparison of Chaos Cryptography Techniques	63
2.7	List of Variables for Generation of Initial Conditions and Control Pa- rameters	68
2.8	Diffusion Process of R Plane with Eight Direction Folding	70
2.9	Quantum Bit Cross-Exchange	74
2.10	Combination Rule of 5D Hyper-Chaotic Sequence	74
2.11	Overall Comparison of Quantum Chaos Cryptography Techniques . . .	77
2.12	Overall Comparisons of Cryptography Techniques	78
3.1	Machine and Image Specifications, Initial and Modified Parameters . . .	89
3.2	Set of Images for Testing	89
3.3	Visual Analysis of Encrypted and Decrypted Images	90
3.4	Visual Assessment and Histogram of Proposed and Other Techniques . .	91
3.5	Correlation Plots of Original and Encrypted Images	93
3.6	NPCR and UACI Test for One-Bit Key Change	96
3.7	Key Space Analysis of the Proposed and Other Implemented Techniques	96

4.1	<i>h</i> Values Corresponding to Different Key Values	105
4.2	Different Keys used for Generation of Random Sequence of Varying Sizes and Values, Corresponding to the Encryption Block	105
5.1	Simulation Setup Parameters for Proposed Technique 2	113
5.2	Visual Analysis of 256×256 Size Images	115
5.3	Visual Analysis of 512×512 Size Images	116
5.4	Histogram Analysis of 256×256 Size Images	117
5.5	Histogram Analysis of 512×512 Size Images	118
5.6	Number of Pixel Change Rate Test Table	121
5.7	Unified Average Change in Intensity Test Table	121
5.8	Key Space Analysis of Various Techniques Available in Literature	122
5.9	Compiled Results of Proposed Technique 2	126

LIST OF ABBREVIATIONS

Abbreviation	Full Form
AES	Advanced Encryption Standard
2-D TAM	2-Dimensional Toral Automorphism Map
5-D HCM	5D Hyper Chaotic Map
B	Blue
BER	Bit Error Rate
BW	Black and White
CC	Correlation Coefficient
DC	Diagonal Correlation
DCT	Discrete Cosine Transform
DES	Data Encryption Standard
DFT	Discrete Fourier Transform
DWT	Discrete Wavelet Transform
G	Green
H	High
HC	Horizontal Correlation
IDEA	International Data Encryption Algorithm
IDE	Integrated Development Environment
ILWT	Inverse Linear Wavelet Transform
IP	Initial Permutation
IPES	Improved Proposed Encryption Standard
KS	Key Space
KSA	Key Scheduling Algorithm
L	Low
LSB	Least Significant Bit
LWT	Linear Wavelet Transform
M	Moderate
MATLAB	MATrix LABoratory
MSB	Most Significant Bit
MSE	Mean Square Error
NPCR	Number Pixel Change Ratio
PES	Proposed Encryption Standard
PSNR	Peak Signal to Noise Ratio
Qubit	Quantum Bit
R	Red
RB	Bottom of R plane
RC4	Rivest Cipher 4

RC5	Rivest Cipher 5
RC6	Rivest Cipher 6
S-Box	Substitution Boxes
TDEA	Triple Data Encryption Algorithm
TDES	Triple Data Encryption Standard
TDES	Triple Data Encryption Standard
UACI	Unified Average Change Intensity
USC-SIPI	University of Southern California -Signal and Image Process- ing Institute
USD	United States dollar
VC	Vertical Correlation
VH	Very High
VL	Very Low
WB	White and Black

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION TO CONFIDENTIALITY

The technological advancements [1–5] of last two decades have provided the world with systems that can transmit large amount of data like images efficiently via general public networks. This advancement has not only helped users in their day-to-day work but also assisted in fields like education, healthcare, commercial and government sectors [6]. A major problem arises while routing the data packets is that the path followed by these packets is public in nature which can be easily intercepted and read by unauthorized user leading to information leakage [7–9] as shown in Figure 1.1.

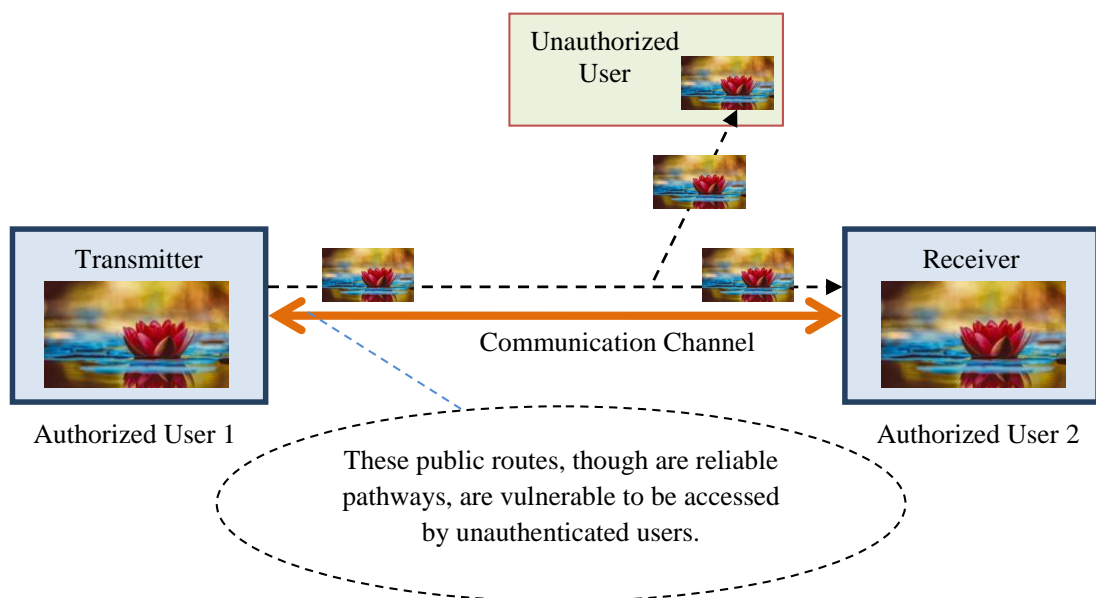


Figure 1.1: Communication Network

The exponential increase in data transfer over these public networks has risen the

number of online exposed data breaches many folds in the last few decades as can be seen from Figure 1.2. The statistica report depicts that number of exposed data breaches is escalating significantly in Figure 1.2(a) and Figure 1.2(b) depicts the monetary losses due to the exposed records [10, 11]. It shows that approximately 5000 million USD were lost in the year 2021. Therefore, it becomes mandatory for individuals and professionals to safeguard their confidential data from unauthorized access. For protecting

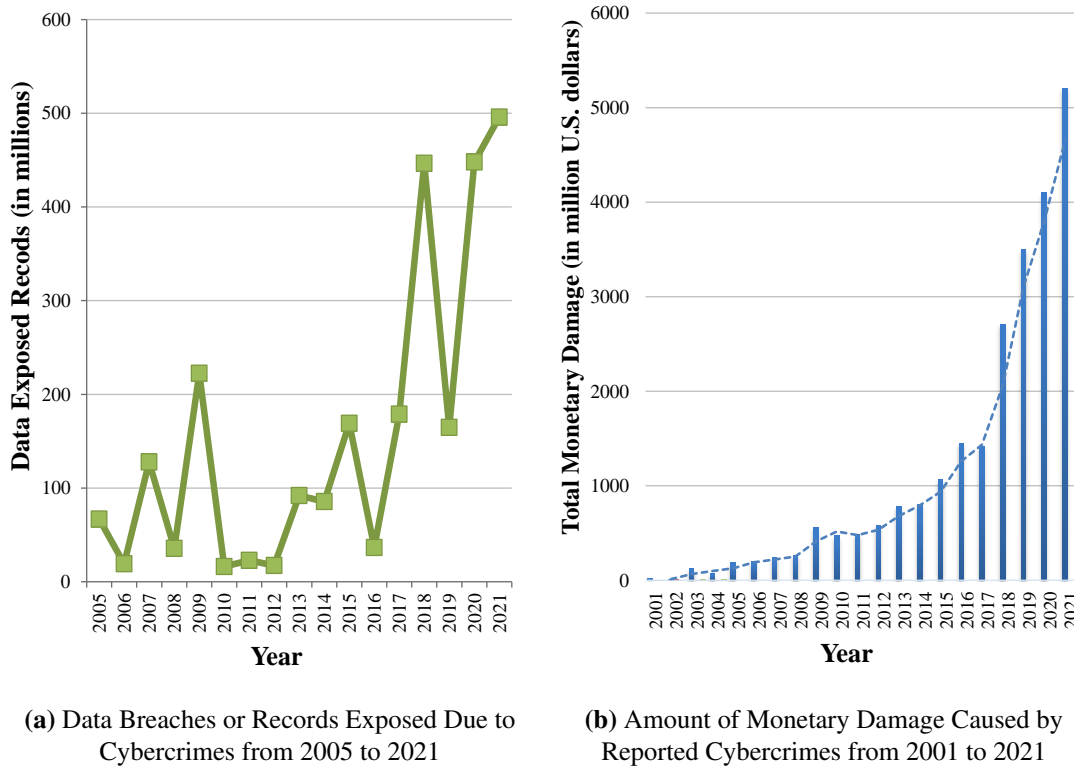


Figure 1.2: Recorded Data Breaches or Exposed Records and Corresponding Monetary Damages Caused by Cybercrimes in United States on Annual Basis

the exposed records on these public networks, the information should be transformed in such a manner that it should be meaningless to the unintended users. In other words, the information must be readable only by its intended user [12]. Thus, Confidentiality means providing privacy between sender and receiver while transferring data on the network such that no one else can read the message. The widespread solution for maintaining confidentiality is ‘Cryptography’. The next section gives details of the Cryptography process.

1.2 CONFIDENTIALITY USING CRYPTOGRAPHY

Cryptography [13] is a widely accepted method to protect confidential information (like: text, images, audio and video etc.) and records by transforming them into another form such that it cannot be read by an unauthorized user. Figure 1.3 shows that

this method is a combination of encryption and decryption processes at transmitter and receiver side respectively. Also, the transformed into Cipher Image seems like a random image on the transmission channel.

- (a) **Encryption:** Transforming original data into an unreadable form (like garbage data) before transmission using a key value.
 - (b) **Decryption:** Recovering the original data from its Cipher at the receiver end using the same key value used in encryption process.
- **Purpose of Cryptography:** To protect confidential information (text/images) and records by transforming them from one form into another such that it cannot be read by an unauthorized user.
 - **Two major functions of Cryptography are:**
 - i. The data is transformed into cipher-text which makes it difficult for the intruder to predict the exact information.
 - ii. The secret key and the method of encryption to retrieve the information are only known to the authorized user.

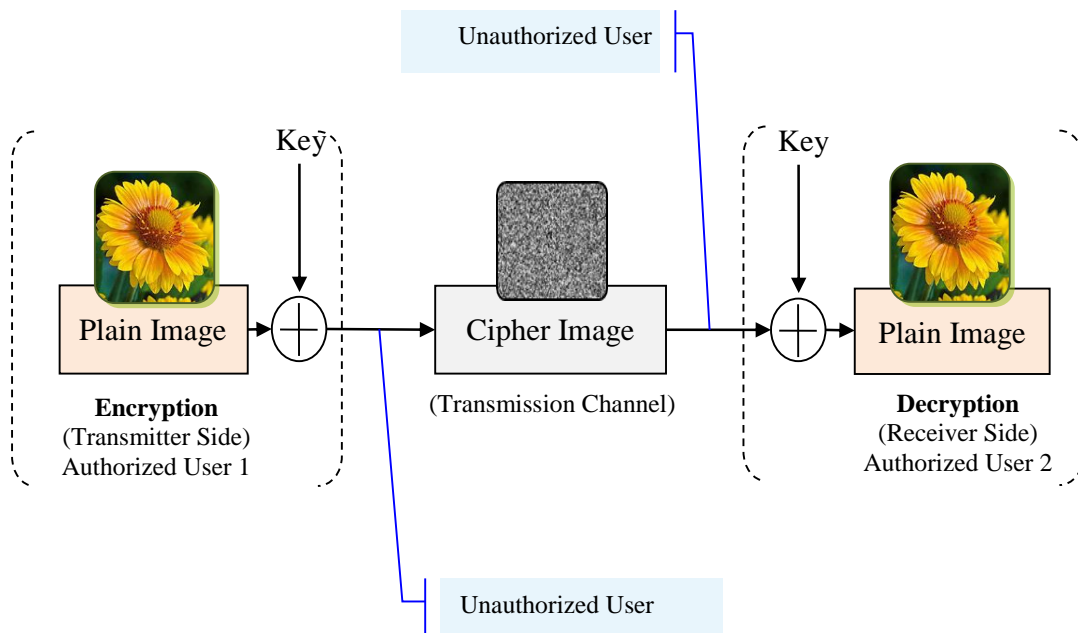


Figure 1.3: Process of Cryptography

In view of available threats and attacks, many researchers [14–26] are working in the area to introduce the mechanisms that can secure the confidential data. A large number of cryptography techniques [27–43] are available in the literature that can be classified into three categories i.e. Traditional, Chaos Based and Quantum Chaos Based techniques. The next section gives a detailed explanation of all the techniques that come under each category.

1.3 CLASSIFICATION OF CRYPTOGRAPHY TECHNIQUES

Many researchers have worked in this crucial direction to get the best solutions in terms of the protection of information i.e., data and images on public networks. This research work highlights the principle of supremacy of Confidentiality. Cryptography is one of the highly effective techniques to achieve this. All the available techniques of cryptography are classified into three categories as shown in Figure 1.4.

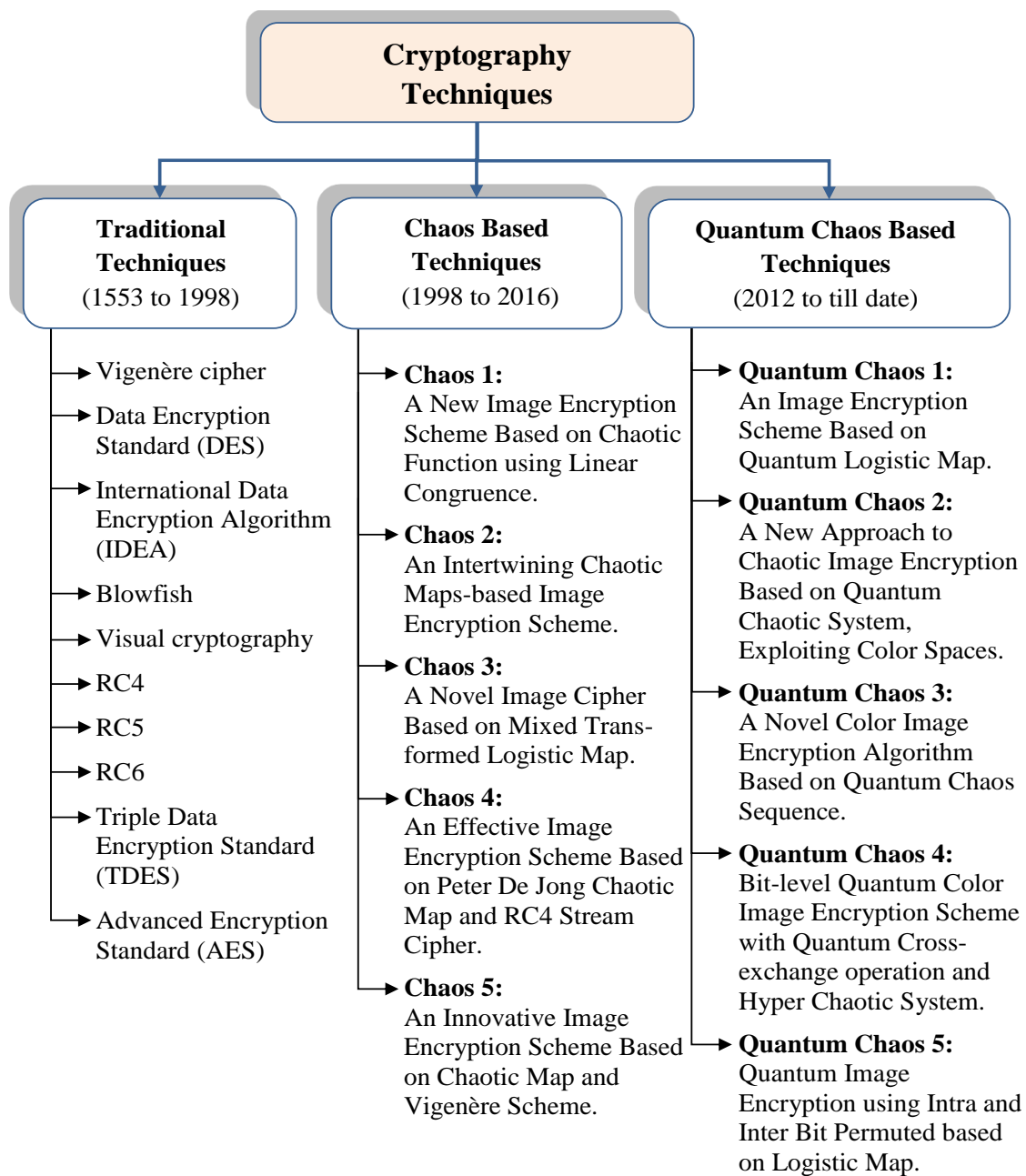


Figure 1.4: Classification of Cryptography Techniques

1.3.1 Traditional Cryptography Techniques

This category of cryptography techniques was used initially for encrypting small size textual data. Later on, with the advancements in multimedia services on internet and extensive use of social media like facebook, whatsapp, twitter and instagram etc. most of the information were exchanged in the form of images and videos. In the starting phase of this era, these traditional methods of cryptography were used for texts as well as for images. It was soon realized that the neighboring letters in textual data have low degree of the correlation value in comparison to the neighbor pixel values in an image that has high correlation value. So, these techniques [44–54] were found not suitable for the image and video encryption. Also, the size of an image is larger than textual data indicating that traditional techniques will consume more time in processing [55–59].

➤ **Problems with Traditional Encryption Techniques:**

- i. Only Compatible with Texts
- ii. Low Randomness
- iii. High Processing Delay
- iv. Small Key Space
- v. Nonresistant to Attacks

To overcome these issues Chaos Based Encryption Techniques were developed.

1.3.2 Chaos Based Cryptography Techniques

In general term chaos means highly disorganized. So, here this category of cryptography is named as Chaos Based Cryptography because it resulted a ciphered image in highly disorganized manner. It is based on mathematical Chaos Theory [60]. The Chaos based systems are highly dynamic systems which gives result in apparently random states of disorder and irregularities. These states are governed by underlying patterns and deterministic laws that are highly sensitive to initial conditions. Using this method, random numbers can be generated at a very fast rate, simply by using the direct form or modified form of Chaos-based equations i.e. Logistic Maps [61] as shown in Eq. (1.1). Thus, the system with this method can easily encrypt the multimedia data like image, text and video in highly random manner.

$$x_{n+1} = r \times x_n (1 - x_n) \quad (1.1)$$

Where,

x is the Variable and n denotes the Index of generated chaotic number.

r is Positive Constant and $r \in [0, 4]$.

x at $n=0$ is the Initial Value and $x_0 \in (0, 1)$.

This technique consists of three parts i.e. Key Generation, Confusion, and Diffusion Process [62]:

- (a) **Key Generation:** In this process, keys are generated with the help of Logistic Maps. These keys are further used at different levels of encryption.
- (b) **Confusion:** It is the process in which the pixels positions are rearranged according to the generated chaotic key values.
- (c) **Diffusion:** It is the process of pixel value modification [63] with the help of generated chaotic key values. The aim of this process is to enhance the randomness.

➤ **Problems with Chaos Based Encryption Techniques:**

The Chaos-based Encryption Technique possesses various properties like simplicity, high dependence on initial conditions, ergodicity, Confusion (pixel position scrambling), and Diffusion (pixel value modification). These procedures enhance the security on the system [64–68]. However, many of these algorithms still possess limitations like:

- i. Small Key Space
- ii. High Computation Complexity

To overcome these limitations, Quantum based encryption schemes were developed. These techniques are unquestionably more secure for image encryption than the basic and traditional techniques because of their perplexing [67] structure.

1.3.3 Quantum Chaos Based Cryptography Techniques

The Quantum Chaos Based Encryption [69–73] is done with the help of Quantum Logistic Maps. These maps were developed by utilizing uncertainty principles of Quantum Mechanics on Logistic Maps [74] and documented as a highly random equation. These maps are popular for their random response over a range of discrete numbers. The Quantum Logistic Maps has many good features like:

- (a) Key Space is large.
- (b) Generated random numbers are highly aperiodic.
- (c) Optimized value of Entropy.

Therefore, the non-periodicity and randomness of chaotic sequences are further more enhanced by utilizing it with the Quantum Logistic Maps. It acquires various kinds of Confusion and Diffusion processes same as the Chaos-based Encryption Processes. The only difference is that these two procedures are performed according to the generated random keys with the help of Quantum Logistic Maps instead of simple Logistic Maps used by Chaos Techniques as explained in previous section.

➤ **Problems with Quantum Chaos Based Encryption Techniques :**

- i. Quantum Chaos Based Logistic Maps are more complex and nonlinear than Chaotic Logistic Maps.
- ii. All the parameters like randomness, entropy, key sensitivity, image perceptual quality were improved but some techniques do not resist the statistical or differential attacks and also the execution time is significant but smaller than Chaos Based Encryption Techniques.

The next section gives the literature survey.

1.4 LITERATURE SURVEY

In search of the secure image encryption technique, numerous researchers have proposed several security mechanisms [44–54, 64–73] to achieve confidentiality. Despite of having a huge amount of encryption techniques available on the research portals, some of the popular techniques were identified as shown in Figure 1.4. The survey part of this research is done with the help of measured values of performance parameters and their specific performance metrics along with their satisfactory range of values shown in the Table 1.1.

Table 1.1: Performance Parameters for Literature Survey

Parameters of Comparison	Performance Metrics	Definition	Range
Image Perceptual Quality: The encrypted images are analyzed visually for any hidden information in it.	Snapshot	The images are interpreted by simply watching it.	Visually examined
Statistical Attack Parameters: The encrypted images are analyzed to determine the number of similarities between the pixels of the encrypted and original images [75].	Histogram	It is a graph that represents the frequency distribution of the pixel values presented in an image.	Visually examined
	Correlation Coefficient	It defines the correlation among the corresponding pixels of plain and encrypted image. It can be measured in horizontal, vertical and diagonal directions.	Its value lies in the range $[-1, +1]$. The values $+1$ represent maximum linear relation, and zero value represents no relation between adjacent pixels.

Parameters of Comparison	Performance Metrics	Definition	Range
Differential Attack Parameters: This parameter [76] helps in providing that a good encryption system must prevent a hacker from obtaining the information if the intrusion occurs in any way.	Number of Pixel Change Rate (NPCR)	It defines the average difference in pixel value between two encrypted images (the first encrypted image is produced using the original key, and the second one is obtained by modifying the original key by one bit).	Test passes at the values greater than N_{α}^* : $N_{0.05}^*=99.5693\%$ $N_{0.01}^*=99.5527\%$ $N_{0.001}^*=99.5341\%$ Where, N_{α}^* denotes critical NPCR values to reject null hypothesis with respect to the significance levels $\alpha = 0.05$, $\alpha = 0.01$ and $\alpha = 0.001$.
	Unified Averaged Changing Intensity (UACI)	It defines the average value of differential pixel values between the plain and encrypted images.	Its value must lies in the range : $U_{0.05}^*=[33.284\% - 33.6447\%]$ $U_{0.01}^*=[33.2255\% - 33.7016\%]$ $U_{0.001}^*=[33.1594\% - 33.7677\%]$ Where, U_{α}^* denotes critical UACI values to reject null hypothesis with respect to the significance levels $\alpha = 0.05$, $\alpha = 0.01$ and $\alpha = 0.001$.
Quantitative Parameters: This provides the amount of randomness or noise available in an encrypted image.	Pixel Signal to Noise Ratio (PSNR)	It is the ratio between the maximum pixel value and amount of noise available in an encrypted image.	Its value should be less than 30dB .
	Entropy	It defines the amount of randomness in the given image.	Its value should be equal to 8 for complete random image.
Key Space Assessment: A system is fully secure if the value of brute force search time to crack the key used in the encryption process is high.	Key Space	It defines the key length used in the entire process of encryption.	$2^{(\text{Length of Key})}$ bits It should be large as much as possible.
Execution Time Assessment: The time taken for the execution of entire encryption process [77].	Execution time (in Seconds)	It is the amount of time taken for an image to be encrypted.	The execution time should be as low as much can be possible.

The analyzed values of the reviewed techniques are listed in Tables 1.2, 1.3 and 1.4. Some identification marks like: low(L), very low(VL), moderate(M), high(H), very high(VH), best results among all(*), 2nd best results(**) and satisfactory range of results (highlighted by green color) are used here as the abbreviations that helps in differentiating the performance of the existing techniques.

Table 1.2: Literature Survey of Traditional Techniques

Year	Performance Metrics/ Proposed Cryptography Techniques (Authors)	Image Perceptual Quality (Snapshots)	Statistical Attack Parameters (Histogram and Correlation Coefficient (CC))	Differential Attack Parameters (NPCR and UACI)	Quantitative Parameters (PSNR and Entropy)	Key Space	Execution Time
1955	Vigene 're Cipher/ (L. D. Smith) [44]	Less Random	Histogram= Spiked CC= H	NPCR= Fail UACI= Fail	PSNR= M Entropy= M	M	L
1994	Blowfish/ (B. Schneier) [48]	Random	Histogram= Uniform CC= M	NPCR= Pass UACI= Pass	PSNR= M Entropy= H	M	H
1995	Visual cryptography/ (M. Naor and A. Shamir) [49]	Random	Histogram= Uniform CC= L	NPCR= Fail UACI= Fail	PSNR= M Entropy= H	L	L
2001	Rivest Cipher (RC4)/ (Fluhrer et al.) [50]	Highly Random	Histogram= Uniform CC= VL	NPCR= Pass UACI= Pass	PSNR= M Entropy= H	H	L
1994	Rivest Cipher 5 (RC5)/ (R. Rivest) [51]	Highly Random	Histogram= Uniform CC= M	NPCR= Pass UACI= Pass	PSNR= M Entropy= H	M	H
1998	Rivest Cipher 6 (RC6)/ (R. Rivest) [52]	Highly Random	Histogram= Uniform CC= M	NPCR= Pass UACI= Pass	PSNR= M Entropy= H	M	H
1999	Data Encryption Standard (DES)/ (NIST) [45]	Random	Histogram= Uniform CC= M	NPCR= Pass UACI= Pass	PSNR= M Entropy= H	M	M
2000	Triple data encryption standard (TDES)/ (S.S. Keller) [53]	Highly Random	Histogram= Uniform CC= M	NPCR= Pass UACI= Fail	PSNR= M Entropy= H	M	H
2001	Advanced encryption standard (AES)/ (NIST) [54]	Highly Random	Histogram= Uniform CC= M	NPCR= Pass UACI= Pass	PSNR= M Entropy= H	M	L
2007	International data encryption algorithm (IDEA)/ (H. Hoffman) [47]	Random	Histogram= Uniform CC= M	NPCR= Pass UACI= Pass	PSNR= M Entropy= H	M	H

Table 1.3: Literature Survey of Chaos Based Encryption Techniques

Year	Performance Metrics/ Proposed Cryptography Techniques (Authors)	Image Perceptual Quality (Snapshots)	Statistical Attack Parameters (Histogram and Correlation Coefficient (CC))	Differential Attack Parameters (NPCR and UACI)	Quantitative Parameters (PSNR and Entropy)	Key Space	Execution Time
2012	Chaos 1/ (François et al.) [65]	Highly Random	Histogram= Spiked CC= M	NPCR= Pass UACI= Pass	PSNR= M Entropy= H	H	H
2012	Chaos 2/ (Sam et al.) [64]	Highly Random	Histogram= Uniform CC= ** VL	NPCR= Pass UACI= Pass	PSNR= M Entropy= H	M	L
2012	Chaos 3/ (Sam et al.) [66]	Highly Random	Histogram= Uniform CC= L	NPCR= Pass UACI= Pass	PSNR= M Entropy= H	M	M
2015	Chaos 4/ (G. Hanchinamani and L. Kulkarni) [67]	Highly Random	Histogram= Uniform CC= L	NPCR= Pass UACI= Pass	PSNR= M Entropy= H	**VH	M
2016	Chaos 5/ (Bansal et al.) [68]	Highly Random	Histogram= Uniform CC= VL	NPCR= Pass UACI= Pass	PSNR= M Entropy= **H	*VH	L

Table 1.4: Literature Survey of Quantum Chaos Based Encryption Techniques

Year	Performance Metrics/ Proposed Cryptography Techniques (Authors)	Image Perceptual Quality (Snapshots)	Statistical Attack Parameters (Histogram and Correlation Coefficient (CC))	Differential Attack Parameters (NPCR and UACI)	Quantitative Parameters (PSNR and Entropy)	Key Space	Execution Time
2012	Quantum Chaos 1/ (Akshani et al.) [70]	Highly Random	Histogram= Spiked CC= M	NPCR= Pass UACI= Pass	PSNR= * L Entropy= H	H	H
2013	Quantum Chaos 2/ (Abd El-Latif et al.) [69]	Highly Random	Histogram= Uniform CC= M	NPCR= Pass UACI= Pass	PSNR= ** L Entropy= L	H	L
2017	Quantum Chaos 3/ (H. Liu and C. Jin) [71]	Highly Random	Histogram= Uniform CC= * VL	NPCR= Pass UACI= Pass	PSNR= L Entropy= * H	M	L
2018	Quantum Chaos 4/ (Zhou et al.) [72]	Highly Random	Histogram= Uniform CC= L	NPCR= Fail UACI= Pass	PSNR= M Entropy= H	M	L
2019	Quantum Chaos 5/ (Liu et al.) [73]	Highly Random	Histogram= Uniform CC= VL	NPCR= Fail UACI= Fail	PSNR= M Entropy= H	M	L

Through this study, it is found that the Quantum Chaos Based Techniques provide the best results. Still, there is a scope of improvement and parameters like randomness, key security, attack analysis and execution time can be optimized. The next section illustrate the identified existing problems in the field of confidentiality on the basis of literature survey.

1.5 PROBLEM DEFINITION

The areas that can still be improved are as follows:

- **Enhancing Security:** A system is fully secured if the value of Brute Force Search Time to crack the key used in the encryption process is too high. Though the existing schemes provide good brute force search time with increase in processing capabilities, further improvements in this area is always desirable.
- **Reducing Correlation:** The value of correlation among neighboring pixels of encrypting images must be very low in order to have good randomness. The value of entropy must be closed to eight. Though the best techniques in literature have entropy values closed to eight but improvements can still be made in this direction.
- **Good Execution Time:** Any process designed for image encryption will be practical if its speed of execution is high and the overall process takes less time to execute. Therefore, researchers keep on searching for new algorithms that have low execution time for encrypting images.
- **Pixel Sensitivity:** It is desired that if the value of one pixel is changed then it should affect the other pixels too. Though the existing mechanisms provide good value of this metric, but improvements can still be done in this direction too.
- **Resistive against Attacks:** Though the cryptography techniques provide good resistance against attacks, but improvements are still desirable in this direction.

1.6 OBJECTIVES

The objectives of the research work are as under:

- i. To study various image encryption techniques and find out their merits and demerits.
- ii. To propose a new image encryption scheme that should have low computational time complexity, high PSNR value, correlation coefficient.
- iii. To compare the proposed mechanism with the available schemes and prove its efficiency.

The next section provides the details of the tool used.

1.7 TOOL USED

For the implementation of existing and proposed mechanisms, MATLAB IDE-R2016a is used because of its diverse advantages as a modern high-performance programming language for technical computing [78]. The name MATLAB stands for MATrix LABoratory. The software package has been commercially open since 1984 and is now considered a standard tool at most universities and industries globally for research and development. It combines computation, visualization, and the programming world all together. Some of its advantages are listed below:

- It has strong built-in routines that allow a wide variety of computations.
- It has complex data structures, comprises integral editing and debugging tools, and supports object-oriented programming.
- It helps to perform numerical computations and give the results with high accuracy.
- This software tool facilitates data analysis, creating algorithms, and designing models and applications appropriately.
- The outcomes demonstrate that the suggested methods or research is a genuine advanced method for various kind of applications.
- This software also has easy-to-use graphics commands that make the visualization of results immediately available which makes the programmer to evaluate several methods.


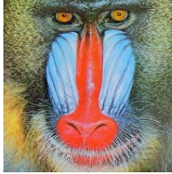
These advantages make MATLAB software an outstanding tool for teaching and research. To analyze and validate numerous techniques, a variety of performance measurement parameters are needed. With MATLAB, numerous image processing procedures may be accurately documented and repeated.

This research covered a novel image confidentiality mechanism and its quality against existing mechanisms is also evaluated with the help of MATLAB software. The subsequent section contains a distinct set of performance metrics of image encryption techniques.

1.8 SIMULATION SET-UP PARAMETERS

Table 1.5 provides the environment, key values and database used to evaluate the efficacy of the proposed schemes.

Table 1.5: Simulation Set-up Parameters for Proposed Technique 1 and Proposed Technique 2

Set up parameter	Proposed Technique 1	Proposed Technique 2
Processor	1.4 GHz dual-core Intel Core i5	1.50GHz Intel Core i3
Image type	Color Images (R, G,B)	Color Images (R,G,B)
Simulation tool	MATLAB Version R2016a	MATLAB Version R2016a
Size of Images	512 × 512	512 × 512
Images source	USC-SIPI image database [79]	USC-SIPI image database [79]
Sample Test Images	 4.2.03 (Mandrill) (512×512)	 4.2.03 (Mandrill) (512×512)
Initial condition and control parameters used for key generation	$[\mu = 3.999, xlog1 = 20.1,$ $ylog1 = 22, zlog = 19,$ $k4 = 33.5, k5 = 37.9,$ $k6 = 35.7, pix = 0.1]$	$[x = 0.4523444336,$ $y = 0.003453324562,$ $z = 0.001324523564,$ $\bar{x} = 0.002, \bar{z} = 0.004,$ $r = 3.9 \text{ and } \beta = 4.5]$

1.9 PERFORMANCE METRICS

To prove the efficacy of the proposed scheme, several performance metrics are taken into consideration as given below:

1.9.1 Image Perceptual Quality

The analysis of encrypted and decrypted images [80] is done on three images of different sizes. The encrypted image must be random in nature such that no information can be interpreted by simply watching it.

1.9.2 Statistical Attack Parameters

The encrypted images are analyzed to determine the number of similarities among the pixels of the encrypted and original images or between the adjacent pixels [81, 82]. Histogram and Correlation analysis are the two parameters used for this purpose.

- a) **Histogram:** It is a graph that represents the frequency distribution of the pixel values presented in an image. Ideally, it should be uniformly spread on the graph for encrypted image. This shows that the number of pixel values and positions are equally distributed and looks like a random image.

- b) **Correlation Coefficient:** It measures the similarities between the adjacent pixels of an image [83]. The pixels of the encrypted images must be less correlated with its corresponding decrypted image pixels. The mathematical values of correlation coefficients lie between $[-1, 1]$. The correlation coefficient $r_{\alpha\beta}$ is define in Eq. (1.2a), (1.2b), (1.2c) and (1.2d).

$$r_{\alpha\beta} = \frac{\text{cov}(\alpha, \beta)}{\sqrt{D(\alpha)}\sqrt{D(\beta)}} \quad (1.2a)$$

$$E(\alpha) = \frac{1}{N} \sum_{i=1}^N \alpha_i \quad (1.2b)$$

$$D(\alpha) = \frac{1}{N} \sum_{i=1}^N (\alpha_i - E(\alpha))^2 \quad (1.2c)$$

$$\text{cov}(\alpha, \beta) = \frac{1}{N} \sum_{i=1}^N (\alpha_i - E(\alpha)) (\beta_i - E(\beta)) \quad (1.2d)$$

Where,

α and β denote the Encrypted and Plain Images respectively.

$D(\alpha)$ is the Variance of the Image.

$E(\alpha)$ is the Mean of the pixel values of the Image.

$\text{cov}(\alpha, \beta)$ is the Covariance between Encrypted and Plain Images.

i represents the Pixel Position.

N is Total Number of Pixels in an Image.

1.9.3 Differential Attack Parameters

This test is done by modifying a single bit change in data or key value [84]. These changes must be prominent to prove a security scheme is good or not. Two parameters are used for this.

- a) **Number of Pixels Change Rate (NPCR):** It defines the rate of change in the number of pixels in two encrypted images [85]. In this, the two encrypted or cipher images are formed by original and changing one bit of the key value. The formula for NPCR is given in Eq. (1.3a) and (1.3b).

$$NPCR = \frac{\sum_{i=1}^W \sum_{j=1}^H \sum_{k=1}^L D(i, j, k)}{W \times H \times L} \times 100\% \quad (1.3a)$$

$$D(i, j, k) = \begin{cases} 0 & C1(i, j, k) = C2(i, j, k) \\ 1 & C1(i, j, k) \neq C2(i, j, k) \end{cases} \quad (1.3b)$$

Where,

$C1$ is the Cipher Image formed by Original Key.

$C2$ is the Cipher Image formed by Pixel Modified Key.

$i, j,$ and k represents the Pixel Positions of the Image.

W , H , and L are the Width, Height and Length of the Image.

D is a Bipolar Array that gives the similarities between the pixels of Images $C1$ and $C2$.

- b) **Unified Average Change in Intensity (UACI):** It defines the average value of differential intensities between two encrypted or cipher images (the first cipher image is produced using the original key, and the second cipher image is obtained by modifying the original key by one bit). The formula for UACI is given in Eq. (1.4).

$$UACI = \frac{1}{W \times H \times L} \left[\sum_{i=1}^W \sum_{j=1}^H \sum_{k=1}^L \frac{|C1(i,j,k) - C2(i,j,k)|}{2^Q - 1} \right] \times 100\% \quad (1.4)$$

Where,

$C1$ is the Cipher Images formed by Original Key.

$C2$ is the Cipher Images formed by Pixel Modified Key.

i , j , and k represents the Pixel Positions of the Image.

W , H , and L are the Width, Height and Length of the Image.

Q represents the maximum no. of bits of a pixel (in this case $Q=8$).

1.9.4 Quantitative Parameters

Two parameters are used in this study for quantitative calculation:

- a) **Peak Signal-to-Noise Ratio (PSNR):** It is the ratio between the maximum signal power component to noise [86]. For evaluation of this metric, the plain image is considered to be the signal and the encrypted image is considered as the noise. The mathematical representation of PSNR is given in Eq. (1.5a) and (1.5b).

$$PSNR = 20 \times \log_{10} \left(\frac{255}{\sqrt{MSE}} \right) dB \quad (1.5a)$$

$$MSE = \frac{1}{W \times H \times L} \sum_{i=1}^W \sum_{j=1}^H \sum_{k=1}^L [I(i,j,k) - K(i,j,k)]^2 \quad (1.5b)$$

Where,

MSE is the Mean Squared Error.

I and K are the Plain and Encrypted Images respectively.

i , j , and k represents the Pixel Positions of the Image.

W , H , and L are the Width, Height and Length of the Image.

- b) **Information Entropy:** It defines the amount of randomness in the given image [87, 88]. More is the entropy of the encrypted image better is its randomness. The formula of entropy is given in Eq. (1.6).

$$H(S) = \sum_{i=0}^{n-1} P(S_i) \log_2 \left(\frac{1}{P(S_i)} \right) \quad (1.6)$$

Where,

$H(S)$ denotes the Entropy of the image S .

n is the Total Number of Pixels in the Image.

i represents the Position of a Pixel.

S_i is the i^{th} Pixel Value and $P(S_i)$ is the Probability of occurrence of S_i in the Image.

1.9.5 Key Space

Key Space (KS) is an essential parameter for determining the quality of key used for encryption. Eq. (1.7) shows how to calculate key space [89, 90] using Length of Key (in bits). Larger the key size lesser will be the feasibility of a Brute-Force Attack.

$$KS = 2^L \quad (1.7)$$

Where,

L is the Length of Key.

1.9.6 Execution Time

It is the amount of time taken for an image to get encrypted [91]. The value of this parameter must be as low as possible. The next section provides the proposals in this dissertation work.

1.10 PROPOSED IMAGE ENCRYPTION TECHNIQUES

Two image encryption or cryptography techniques were proposed in this research work as shown in Figure 1.5. The first proposal was developed in the initial stages and was

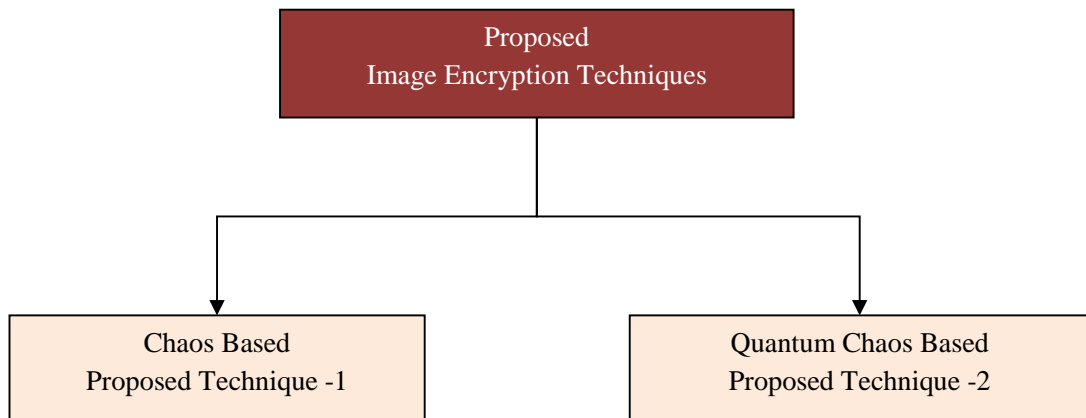


Figure 1.5: Proposed Cryptography Techniques

based on Chaos Theory. Later, with advancements in literature, a new proposal based on Quantum Chaos Theory was also proposed. Both of the Proposed Techniques are described below:

1.10.1 Proposed Technique 1: A Novel Image Encryption Technique Based on Intertwining Chaotic Maps and RC4 Stream Cipher

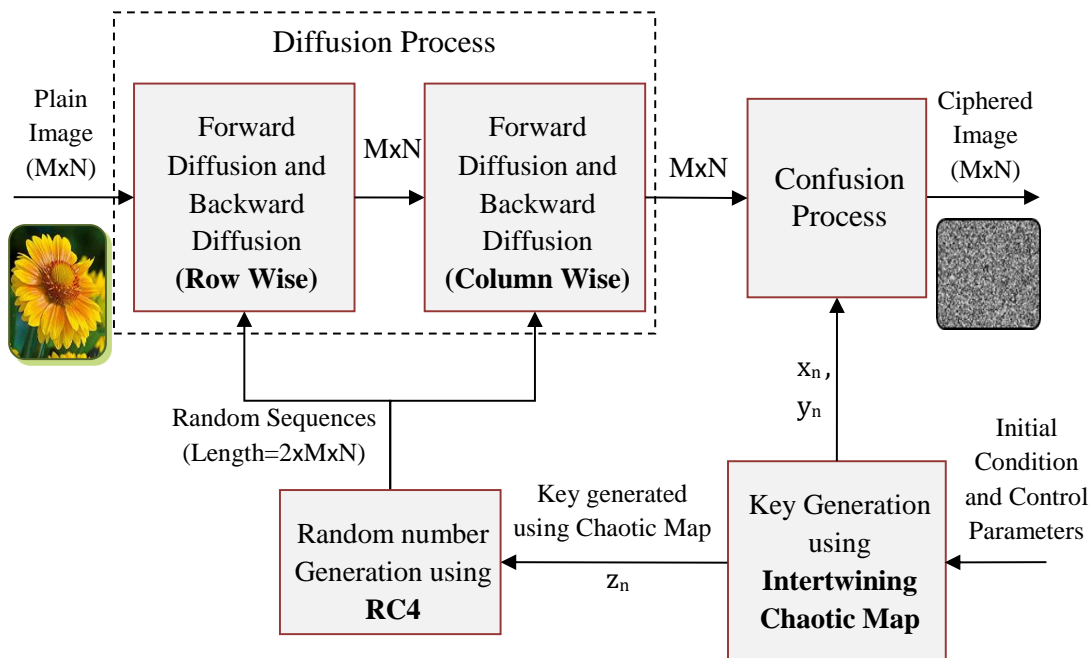


Figure 1.6: Block Diagram of Encryption Process of Proposed Technique 1

i. Proposed Mechanism

The Proposed Mechanism is designed in three major parts i.e. Key Generation, Diffusion and Confusion Process.

- **Key Generation:** This part generates all the keys used for the Diffusion and Confusion Processes.
- **Diffusion:** In this phase, the pixel values are modified with the help of keys generated from the Key Generation Process.
- **Confusion:** In this phase, the pixel values are permuted using key values generated from the Key Generation Process.

Figure 1.6 shows the block diagram of the proposed scheme. First of all, key sequences are generated using intertwining chaotic maps having best feature of randomness along with the RC4 stream cipher scheme [50].

- (a) **Key Generation Process:** Intertwining Chaotic Maps [64] shown in Eq. (1.8a), (1.8b) and (1.8c), have the best feature of randomness. Hence, in this process, the Key Sequences are generated with the help of Intertwining Chaotic Maps and also with RC4 Stream Cipher Scheme [50] in order to further enhance the randomness property of the encrypted image.

Intertwining Logistic Maps:

$$x_{n+1} = \mu \cdot k_1 \cdot y_n (1 - x_n) + z_n \quad (1.8a)$$

$$y_{n+1} = \mu \cdot k_2 \cdot y_n + z_n (1 - x_n)^2 \quad (1.8b)$$

$$z_{n+1} = \mu \cdot (x_{n+1} + y_{n+1} + k_3) \cdot \sin(z_n) \quad (1.8c)$$

Where,

x_n, y_n and z_n are the generated Chaotic Sequence at n^{th} position.

x_{n+1}, y_{n+1} and z_{n+1} are the subsequent values of Chaotic Sequence.

n varies from 1 to Length of Key.

μ is the Sequence Control Parameter.

k_1, k_2 and k_3 are Float Values as the multiplier.

x_0, y_0 and z_0 are predefined Initial Values of x, y and z respectively.

The resulting sequences are then utilized for the Diffusion (modifies the pixel values) of the image by rearranging its pixel value row-wise and then column-wise in forward and backward directions.

- (b) **Diffusion Process:** This process modifies the pixel values of the original image. It is responsible for spreading the effect of change in a pixel intensity value throughout the entire image (any change in the intensity of one pixel value will now change the encrypted image drastically). Both the images (Plain image and diffused image) will have very low resemblance with each other. In the next step, the Confusion Process (pixel position modification) is done as per the chaotic keys generated directly with the help of an intertwining logistic map [64].
- (c) **Confusion Process:** The stage shuffles the position of the pixels present in the image without making any changes in the respective pixel intensity values [61]. This ensures that an unauthorized user who tries to access the data present in the image will get no useful data about the image as the pixels are moved from their original positions. The permutation of pixel position helps to achieve lower values of correlation coefficients.

Several iterations of the Confusion and Diffusion process have been done to obtain higher order of randomness and security. The proposed scheme is very simple, consumes very little time to execute, and provides good values of parameters like PSNR and Unified Average Changing Intensity (UACI). For decryption, the same process is carried out but in a reverse manner.

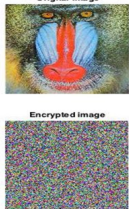
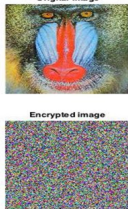
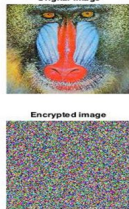

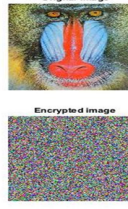
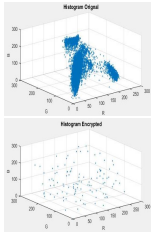
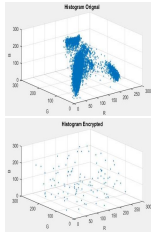
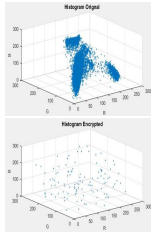
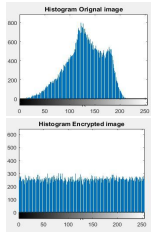
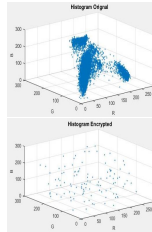
The novel features of this proposal are:

- Confidentiality is achieved by visual interpretation of the encrypted image. The resultant image is highly scrambled which ensures that no information about the original image can be extracted from the cipher image.
- The security is enhanced by lengthening the key space which makes it resistivity against the brute force attack.
- The randomness is increased with the use of highly random intertwining chaotic maps during Confusion and Diffusion processes.
- The scheme is highly resistant against the differential attacks because of row-wise and column-wise Forward and Backward Diffusion along with RC4.
- The time of execution or processing time is improved as compared to the other schemes.

ii. Results

Table 1.6 represents the supremacy of the proposed technique 1 based on evaluated performance metrics with respect to the available Chaos-based Solution. It’s performance is analyzed visually and mathematically.

Table 1.6: Results of Proposed Technique 1

Techniques/ Performance Metrics	Chaos 1	Chaos 2	Chaos 3	Chaos 4	Proposed Technique 1
Image Perceptual Quality (Snapshots)	Snapshots 	Snapshots 	Snapshots 	Snapshots 	Snapshots 
Statistical Attack Parameters (Histogram and Correlation Coefficient (H:Horizontal, V:Vertical, D:Diagonal))	Histogram 	Histogram 	Histogram 	Histogram 	Histogram 
	-0.00073(H), 0.00254(V), 0.003569(D)	-0.01616(H), -0.00815(V), -0.00592(D)	0.00063(H), -4.6E-05(V), 0.005127(D)	0.007284(H), 0.00533(V), 0.005127(D)	0.015051(H), 0.004335(V), -0.0073(D)

Techniques/ Performance Metrics	Chaos 1	Chaos 2	Chaos 3	Chaos 4	Proposed Technique 1
Differential Attack Parameters (NPCR and UACI)	99.60389 (NPCR)	99.60336 (NPCR)	99.61665 (NPCR)	99.61361 (NPCR)	99.60335(Pass) (NPCR)
	33.45831 (UACI)	33.41028 (UACI)	33.4002 (UACI)	33.50219 (UACI)	31.84106(Fail) (UACI)
Quantitative Parameters (PSNR and Information Entropy)	27.77517 (PSNR)	27.76818 (PSNR)	*27.75781 (PSNR)	28.09171 (PSNR)	28.8455 (PSNR)
	7.99941 (Entropy)	7.999372 (Entropy)	*7.99942418 (Entropy)	7.998185 (Entropy)	**7.999403 (Entropy)
Key space	2^{216}	$2^{126} - 2^{147}$	2^{192}	2^{384}	* 2^{384}
Execution Time (sec.)	13.35349	5.012986	6.103858	3.237254	*0.946774

iii. Conclusion

The proposed image encryption technique incorporates a highly random intertwining chaotic map and RC4 stream cipher for a random key generation which is utilized in the Confusion and Diffusion process. The results are evaluated on various performance metrics as shown in Table 1.6.

Following are the inferences drawn from results:

- It provides highly scrambled encrypted images that have no visual resemblance with the original images. The images obtained after decryption are visually same as the original ones. This ensures no information is revealed in visual inspection during transmission.
- As the histogram is uniformly distributed therefore this proposed technique is resistive against statistical attacks.
- The encrypted images provide very low values of the correlation coefficients and have uniform distribution of correlation graphs for all three orientations with no resemblance to the original one.
- It also provides high resistance against differential attacks since NPCR and UACI values obtained are close to the ideal values for a single bit change in the key used.
- The key space of the proposal is 2^{384} , which makes it extremely resistive against the brute force attack.
- The scheme provides PSNR value as 28.18665 which is appropriate as per the security requirements.

- The information entropy is close to ideal value i.e. 8.
- Finally, the scheme has a faster execution time as compared to the other existing image encryption techniques and hence proves the suitability in real time transmission of pictures.

1.10.2 Proposed Technique 2: A Superlative Image Encryption Technique Based on Bit Plane Using Key-Based Electronic Code Book

i. Proposed Mechanism

The second proposed encryption scheme works on similar methodologies of Quantum Chaos-based Image Encryption Techniques. Likewise, the first proposal of this technique also follows three major steps of encryption. These are Key Generation, Confusion, and Diffusion. The block diagram of the encryption process of Proposed Technique 2 is shown in Figure 1.7.

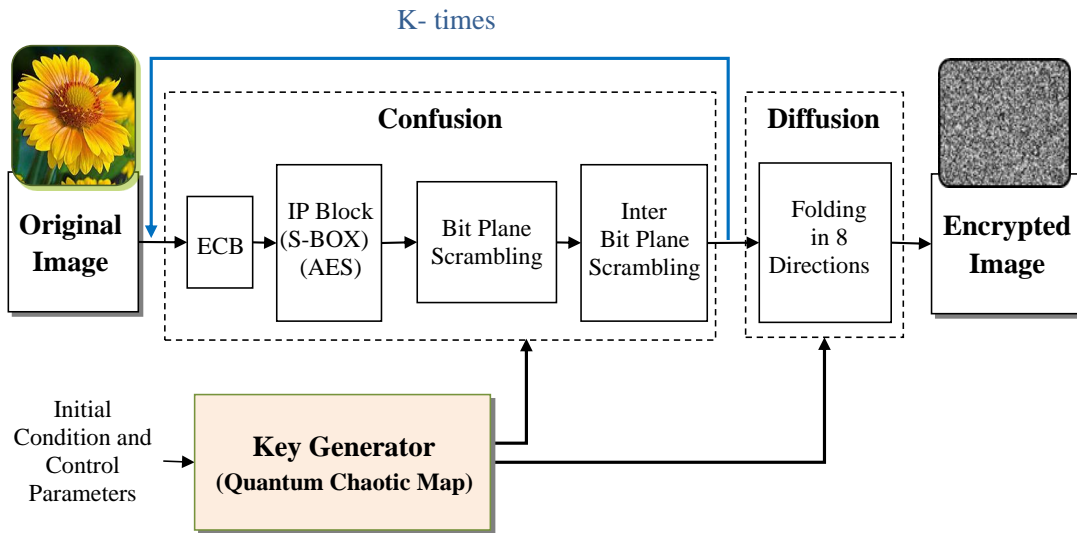


Figure 1.7: Block Diagram of Encryption Process of Proposed Technique 2

The key generator generates the random keys with the help of Quantum Logistic Maps Eq. (1.9a), (1.9b) and (1.9c).

$$x_{n+1} = r \left[\left((x_n) - |x_n|^2 \right) - y_n \right] \quad (1.9a)$$

$$y_{n+1} = -y_n e^{-2\beta} + e^{-\beta} r \left[(2 - x_n - x_n^*) y_n - x_n z_n^* - x_n^* z_n \right] \quad (1.9b)$$

$$z_{n+1} = -z_n e^{-2\beta} + e^{-\beta} r \left[(2 - x_n^*) z_n - 2x_n y_n - x_n \right] \quad (1.9c)$$

Where,

x , y and z are the Variables for arrays of random values at n number of discrete values. n varies from 1 to Length of Key. $x_0, y_0, z_0, x_n^*, z_n^*$ are the Initial Conditions.

r is positive constant taken as Control Parameter whose values must be lies in $[0, 4]$.

β is Dissipation Parameter whose value must be greater than or equals to 6 ($\beta \geq 6$).

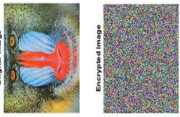
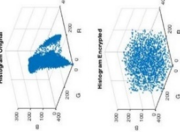
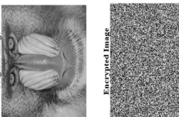
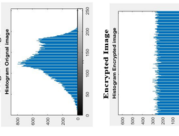
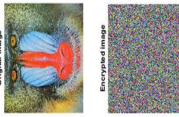
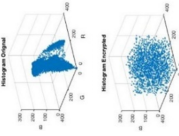
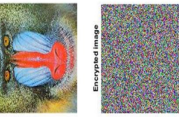
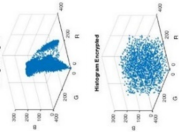
It possesses complex Confusion Processes like bit scrambling [92] on every plane of the colored images by using Electronic Code Book (ECB) [93] and Initial Permutation (IP) blocks (Similar to S-box of AES) [94]. These two ECB and IP blocks are dependent on keys and the complete process is iterated according to one of the key-value (limited to the integer range of 1 to 4) generated from the Quantum Logistic Map by which the randomness of the system increases. The folding procedure in all possible directions is done in the Diffusion phase [95]. This step helps in achieving high NPCR and UACI values [96, 97]. The decryption process is executed just in the reverse manner to recover the original image from the cipher image. The novel features of the proposed technique are:

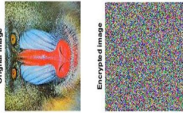
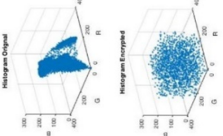
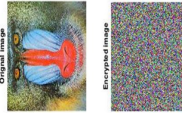
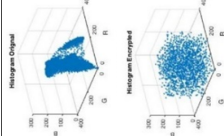
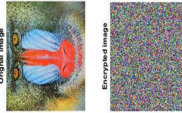
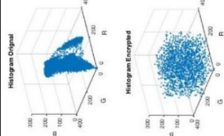
- The number of iterations for the Confusion Process is not fixed, it depends on the key which makes the encryption process more secure. As the key changes, the number of iterations also changes resulting in increased randomness.
- The folding procedure used for the Diffusion process uses different keys for different directions of folding. This not only increases key space but also increases redundancy in the process.
- In the Confusion Process, ECB and IP block are used to secure the data by altering the pixels of an image. These two processes are dependent on keys. With change of key value, the values of ECB, as well as IP block also get changed and hence enhance the image imperceptibility.
- The keys generated from the Quantum Logistic Maps are not used directly. Instead, they are used to generate a random number of iterations for final key generation.
- Bit plane manipulation of pixels is executed. Both intra and inter bit plane scrambling operations are performed on all the channels collectively instead of scrambling the bit planes of R, G, B channels individually.
- All the processes utilize different keys, resulting in dissimilar operations for a separate set of keys.

ii. Results

The simulation results are evaluated on ten images of two different sizes (256×256 and 512×512). The average results of the proposed and studied image encryption techniques for Proposal-2 are given in Table 1.7. The results are also compared with different Chaos and Quantum Chaos-Based Image Encryption Techniques available in the literature.

Table 1.7: Results of Proposed Technique 2

Performance Metrics/ Techniques	Image Perceptual Quality (Snapshots)	Statistical Attack Parameters (Histogram)	Correlation Coefficient (H: Horizontal, V: Vertical, D: Diagonal)	Differential Attack Parameters (NPCR and UACI)	Quantitative Parameters (PSNR and Entropy)	Key Space	Execution Time (in seconds)
Quantum Chaos 1			0.051004 (H) 5.91E-02 (V) 2.86E-02 (D)	NPCR= 99.6133 UACI= 33.4666	PSNR= 27.2225 Entropy= 7.99938	2^{224}	5.7863
Quantum Chaos 2			0.042315 (H) 7.93E-02 (V) 3.63E-02 (D)	NPCR= 99.6600 UACI= 33.5766	PSNR= 27.3548 Entropy= 7.99541	2^{256}	6.4392
Quantum Chaos 3			-0.00598 (H) 2.03E-03 (V) 2.46E-03 (D)	NPCR= 99.6166 UACI= 33.6133	PSNR= 27.6573 Entropy= 7.89497	2^{128}	15.4849
Quantum Chaos 4			-0.00031 (H) -1.01E-02 (V) 3.97E-03 (D)	NPCR= 51.9900(Fail) UACI= 33.5200	PSNR= 27.8223 Entropy= 7.00380	10^{72}	986.893

Performance Metrics/ Techniques	Image Perceptual Quality (Snapshots)	Statistical Attack Parameters (Histogram)	Correlation Coefficient (H: Horizontal, V: Vertical, D: Diagonal)	Differential Attack Parameters (NPCR and UACI)	Quantitative Parameters (PSNR and Entropy)	Key Space	Execution Time (in seconds)
Quantum Chaos 5			0.009587 (H) -1.46E-02 (V) 1.05E-02 (D)	NPCR= 50.3966(Fail) UACI= 25.1466	PSNR= 28.0798 Entropy= 7.99851	$> 2^{100}$	1401.44
Proposed Technique 1			-0.00397 (H) -2.72E-03 (V) -7.95E-03 (D)	NPCR= 99.6048 UACI= 30.963(Fail)	PSNR= 28.2373 Entropy= 7.99940	2^{384}	0.94677
Proposed Technique 2			0.00397 (H) -2.72E-03 (V) -7.95E-03 (D)	NPCR= 99.3633 UACI= 33.1966	PSNR= 27.5701 Entropy= 7.99938	2^{432}	5.24704

iii. Conclusion

The proposed technique utilizes a Quantum Chaotic Map for key generation used in different processes like generation of ECB, Eight Directions Folding, and a number of iterations used in overall methodologies. All the encryption processes and also the number of iterations are key dependent. The image to be encrypted is firstly confused using ECB, IP, and Inter-intra bit scrambling. The confused image is further diffused in the next stage which includes a folding process in eight directions and the number of folds for each direction depends on key values.

After analyzing the results following conclusions are inferred:

- This technique works on bit planes rather than working on bytes, which increases the entropy and randomness of the encrypted image.
- The entropy of the proposed technique is close to 8. Sharing encrypted image is random in nature.
- Due to the dependency on the original image and key generation using the Quantum Chaotic Map, our proposed technique can efficiently resist chosen plaintext attack and known plaintext attack.
- Usage of the multilevel matching process in the Confusion Process requires less time for execution. Hence, it can be used in wide applications of real time communication.
- The speed of execution of the proposed technique is less than almost all the techniques available in the literature. This parameter is dependent on the number of iterations and also on the length of key. In the proposed technique, the speed is variable because it is dependent on the key value. This feature makes our proposed technique more secure than any other technique.
- The proposed technique can resist to brute force search attack due to large key space value i.e. 2^{432} .
- The proposed technique passes all the test levels of NPCR and UACI and hence is resistant to differential attacks.

1.11 OBJECTIVES vs OUTCOMES

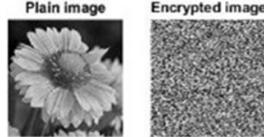


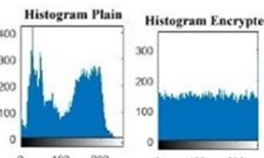
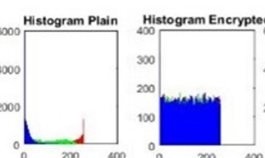
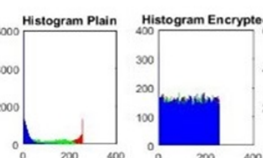
The outcomes are as follows:

- **Objective 1:** To study various image encryption techniques and find out their relative merits and demerits.

Outcome: The following steps were taken for accomplishment:

- i. Various existing image encryption techniques shown in Figure 1.4 are studied and implemented for problem identification.
- ii. The merits and demerits based on various essential performance parameters are listed in Table 1.8 for the techniques available in the literature. It can be inferred that till date Quantum Chaos-based Encryption Techniques give optimized results and having best qualities of confidentiality.

Table 1.8: Comparisons of Traditional, Chaos and Quantum Chaos Based Cryptography Techniques

Techniques/ Performance Metrics	Traditional Technique	Chaos Based Technique	Quantum Chaos Based Technique
Image Perceptual Quality (Snapshots)	Pixel Scrambling: Low 	Pixel Scrambling: High 	Pixel Scrambling: High 
Statistical Attack Parameters (Histogram and Correlation Coefficient (CC))	Histogram: Spiked 	Histogram: Uniform 	Histogram: Uniform 
	CC= Moderate	CC= Very Low	CC= Very Low
Differential Attack Parameters (NPCR and UACI)	NPCR= Fail, UACI= Fail	NPCR= Pass UACI= Pass	NPCR= Pass UACI= Pass
Quantitative Parameters (PSNR and Entropy)	PSNR= High Entropy= High	PSNR= Low Entropy= High	PSNR= Very Low Entropy= High
Key Space	Moderate	High	High
Execution Time	High	Moderate	Very Low

➤ **Objective 2:** To propose a new image encryption scheme that should have low computational time complexity, PSNR value, correlation coefficient.

Outcome: This objective is fulfilled in two phases.

- i. The first proposal was developed in the initial phases of research work and was based on Chaos Encryption Methodology. The Chaos-based Cryptography Techniques were popular due to good security features like high randomness, low correlation, PSNR, and execution time.
- ii. In the next stage, the second proposal was designed based on Quantum Chaos Encryption Methodology. It utilizes uncertainty principles of Quantum Mechanics on Logistic Maps which can enhance the randomness property of a ciphered image.

The performance metrics are calculated and analysed by comparing them with the existing techniques. The results showed optimized values of key size, key space, entropy, and correlation coefficient with low computational time.

- **Objective 3:** To compare the proposed mechanism with the available schemes and prove its efficiency.

Outcome: The proposed mechanisms (Proposed Technique 1 and Proposed Technique 2) are compared with the latest techniques as shown in Table 1.6 of Section 1.10.1 and Table 1.7 of Section 1.10.2 respectively. The proposed mechanism outperforms their counterparts.

1.12 OVERALL CONCLUSION

In this research work, the first extensive literature survey of image encryption techniques was carried out. In the initial phases of research work, the Chaos-based Encryption Techniques were surveyed, and a proposal based on the Chaos Encryption Scheme was developed which outperformed other similar techniques of that period. Afterwards, Quantum Chaos-based Cryptography Techniques were developed, and a new encryption scheme was implemented.

The overall inference of the dissertation work is as follows:

- i. **Image Perceptual Quality:** Both proposals are providing a good encrypted image, it is entirely noise-like and have no resemblance with the original image.
- ii. **Statistical Attack Parameters:** Two parameters are considered for Statistical Attack Analysis i.e. Correlation Coefficient and Histogram.
 - (a) **Correlation Coefficient:** The correlation among adjacent pixels of encrypted and plain image should be as low as possible. In both the proposals, the value is closed to zero, ensuring encrypted image is entirely different from the original one thus ensuring resistance against statistical attacks.

- (b) **Histogram:** In both the proposal the histograms were evenly distributed ensuring that both are not affected by statistical attacks.
- iii. **Differential Attacks Parameters:** The proposal passed theoretical NPCR test value, but the first proposal failed in passing the theoretical UACI value indicating that failure against differential attacks. The second proposal passed both NPCR/UACI theoretical test values hence was successful against differential attacks.
- iv. **Quantitative Parameters:** In this category, two parameters were taken named as PSNR and Entropy. Both the parameters were found to be having good values in comparison to other techniques of literature.
- v. **Key Space:** The set of all valid, possible, distinct keys of a given cryptosystem determines the key space. It must be greater than 2^{100} for resisting brute force attacks with the current computational ability of computers. Both the proposed schemes have good value of key space (Proposal-1 = 2^{384} and Proposal-2 = 2^{432}) ensuring resistance against brute force search attack.
- vi. **Execution Time:** The execution time must be as low as possible for practical usage. The first proposal nearly overpowered all other techniques of its era while the second proposal execution time was good in comparison to other techniques.

1.13 ORGANIZATION OF THESIS

The research is organized as mentioned below:

- **Chapter-2** gives the Literature Survey of image encryption techniques. It describes existing solutions to preserve image confidentiality on the communication network. In addition, it describes various categories of all the techniques.
- **Chapter-3** provides the Proposed Solution-1 based on Chaos Image Encryption Techniques. The proposed technique is also compared with its counterparts.
- **Chapter-4** provides another Proposed Solution-2 based on Quantum Chaos Image Encryption Technique. It comprises of the complete mechanism and novel features of the proposal.
- **Chapter-5** contains Simulation Set-up Parameters along with Performance Metrics used to evaluate the efficacy of the proposed encryption techniques. It also provides the results of the proposed techniques in comparison to other techniques of literature.

- **Chapter-6** gives details of accomplishment of the Objectives for research with the Overall Conclusion and Future Scope. It is followed by, References which are referred throughout the work. In the end, Published Papers in International Journals and Conferences related to the above defined research are listed.

CHAPTER 2

LITERATURE SURVEY

2.1 INTRODUCTION TO CONFIDENTIALITY


The advancements in technology in the last two decades have provided the world with systems which can transmit the big amount of data in the form of Texts, Images, Videos, and Audios efficiently via the generic public networks [98]. These public routes, though are reliable pathways but are also vulnerable to access by unauthenticated users which can altered the confidential data and misuse it. Due to the huge amount of vital information being transmitted from one node to another worldwide via internet, the risk of digital threats has also increased. Generally, the common user only pay attention towards the services and its available features but due to lack of deep knowledge of computer networking, they may not be aware that their system might get exposed to security attacks. However, there are numerous security solutions available to safeguard the interest of both individuals and organizations but still many researches are going on in this field to prevent the network from Cyber-Attacks [99] because internet is the most versatile and openly accessible to all.

To protect the data on network from intruders, it should be transformed into a secure format before transmission. This process of altering the plain data into some other form i.e. in random form which is not understood by intruders is known as Encryption while the reverse process of recovering plain data from encrypted data is known as Decryption. Cryptography refers to the entire procedure of Encryption and Decryption [100]. Lots of research is going on in this field to design and analyze the protocols that prevent third parties or the general public from accessing private messages. This chapter explains and compares all cryptography mechanisms, starting from classic to the latest techniques. This part of the research is a building block of the foundation in developing the most secure and fast image encryption technique to preserve image confidentiality on public network.

2.2 SIMULATION SET-UP PARAMETERS FOR LITERATURE SURVEY

The Simulation Set-up Parameters are given in Table 2.1 for implementation and comparison of all Cryptography Techniques. These techniques are implemented in MATLAB Software and examined with the help of various Performance Metrics.

Table 2.1: Simulation Set-up Parameters for Literature Survey

Machine	Specifications of Machine
Processor	1.4GHZ Dual-Core Intel Core I5
Memory	4GB Of 1600 MHz Lpddr3
Simulation Platform	MATLAB Version 2015
Type of data	Specifications of data
Type	Color Images
Size Of Images	256 × 256, 512 × 512
Images Source	USC-SIPI Image Database [79]
Sample Image	4.1.08 (Flower) 
Encryption Techniques	Original Values of Keys for Traditional Techniques or Initial Conditions and Control Parameters for Chaos and Quantum Chaos-based Techniques
Vigenère, AES:	[2b7e151628aed2a6abf7158809cf4f3c]
DES, Blowfish:	[133457799bbcdff1]
IDEA:	[5a14fb3e021c79e0608146a0117bff03]
RC4:	[C3f4fc9088517fba6a2dea826151e7b22b7e151628aed2a6abf7158809cf4f3c]
RC5:	[915f4619be41b2516355a50110a9ce91]
RC6:	[De37a1fd8492d8efe714f1b7cc783aad]
TDES:	[133457799bbcdff19bbcdff11334577933457799bbcdff11]
Chaos 1:	[p1= 7, p2= 31, p3= 23, p4= 9, p5= 15, p6= 21, x= 33.1, y= 37.3, z= 35.7]
Chaos 2:	g= [4713 654, 84 287, 7487, 1984, 12 314, 10, 74 120, 130 014, 95 210, 1914, 70 553, 2835, 19 800, 299 314, 83 721,610 990, 210, 65 521, 396, 1 109 094, 230 014, 63 010, 10 246]
Chaos 3:	[k1= 37.8, k2= 39.8, k3= 37.3] [oddkey1= 1, oddkey2= 5, oddkey3= 99, oddkey4= 111, oddkey5= 7, oddkey6= 77]
Chaos 4:	[a= 1.77, b= 1.67, c= -0.85, d= 2.1, X(0)= 0.6, Y(0)= 0.4]
Chaos 5:	[u= 3.99, k1= 0.01, k2= 20, k3= 22, k4= 19 , k5= 34, k6= 40, k7= 36]
Quantum Choas 1:	[Q1(0)= 0.463442266, Q2(0)= 0.004532285, Q3(0)= 0.002136285, Q*1(0)= 0.00186, Q*3(0)= 0.00398, λ= 3.99, β= 4.489, e1= 99971 and e2= 99809]

Quantum Choas 2 :	[x(1)= 0.4523444336, y(1)= 0.003453324562, z(1)= 0.001324523564, $x_nconj=0.002$, $z_nconj=0.004$, r= 3.9, $\beta=4.5$]
Quantum Choas 3:	[a= 3.3, b= 3.45, $\xi=0.001$, r= 3.99] $\beta=6$, K(1:16)= [207, 21, 42, 61, 122, 203, 97, 76, 101, 5, 7, 241, 139, 28, 98, 17]
Quantum Choas 4:	[a= 1, b= 8/3, c= 28, p= 1.3, q= 2.5, $x_1(0)=0.325$, $x_2(0)=0.0476$, $x_3(0)=0.1256$, $x_4(0)=0.0628$, $x_5(0)=0.15$]
Quantum Choas 5:	[$x_1(0)=0.5$, $x_2(0)=0.52$, $x_3(0)=0.53$, $x_4(0)=0.6$, $x_5(0)=0.37$, $x_6(0)=0.46$, $x_7(0)=0.38$, $x_8(0)=0.61$, $N_0=10000$, $\alpha=3.99999$, P(0)= 0.49]
Encryption Techniques	Modified Values (highlighted by red color) of Keys or Initial Conditions and Control Parameters used for Differential Attack Analysis)
Vigenère, AES:	[2c7e151628aed2a6abf7158809cf4f3c]
DES, Blowfish:	[143457799bbcdff1]
IDEA:	[5b14fb3e021c79e0608146a0117bff03]
RC4:	[C4f4fc9088517fba6a2dea826151e7b22b7e151628aed2a6abf7158809cf4f3c]
RC5:	[925f4619be41b2516355a50110a9ce91]
RC6:	[Df37a1fd8492d8efe714f1b7cc783aad]
TDES:	[143457799bbcdff19bbcdff11334577933457799bbcdff11]
Chaos 1:	[p1= 7, p2= 31, p3= 23, p4= 9, p5= 15, p6= 21, x= 33.11, y= 37.3, z= 35.7]
Chaos 2:	g= [4714 654, 84 287, 7487, 1984, 12 314, 10, 74 120, 130 014, 95 210, 1914, 70 553, 2835, 19 800, 299 314, 83 721, 610 990, 210, 65 521, 396, 1 109 094, 230 014, 63 010, 10 246]
Chaos 3:	[k1= 37.81, k2= 39.8, k3= 37.3] [oddkey1= 1, oddkey2= 5, oddkey3= 99, oddkey4= 111, oddkey5= 7, oddkey6= 77]
Chaos 4:	[a= 1.771, b= 1.67, c= -0.85, d= 2.1, X(0)= 0.6, Y(0)= 0.4]
Chaos 5:	[u= 3.991, k1= 0.01, k2= 20, k3= 22, k4= 19, k5= 34, k6= 40, k7= 36]
Quantum Choas 1:	[Q1(0)= 0.4634422661, Q2(0)= 0.004532285, Q3(0)= 0.002136285, $Q^*1(0)=0.00186$, $Q^*3(0)=0.00398$, $\lambda=3.99$, $\beta=4.489$, e1= 99971 and e2= 99809]
Quantum Choas 2 :	[x(1)= 0.4623444336, y(1)= 0.003453324562, z(1)= 0.001324523564, $x_nconj=0.002$, $z_nconj=0.004$, r= 3.9, $\beta=4.5$]
Quantum Choas 3:	[a= 3.31, b= 3.45, $\xi=0.001$, r= 3.99] $\beta=6$, K(1:16)= [207, 21, 42, 61, 122, 203, 97, 76, 101, 5, 7, 241, 139, 28, 98, 17]
Quantum Choas 4:	[a= 1, b= 8/3, c= 28, p= 1.3, q= 2.5, $x_1(0)=0.326$, $x_2(0)=0.0476$, $x_3(0)=0.1256$, $x_4(0)=0.0628$, $x_5(0)=0.15$]
Quantum Choas 5:	[$x_1(0)=0.51$, $x_2(0)=0.52$, $x_3(0)=0.53$, $x_4(0)=0.6$, $x_5(0)=0.37$, $x_6(0)=0.46$, $x_7(0)=0.38$, $x_8(0)=0.61$, $N_0=10000$, $\alpha=3.99999$, P(0)= 0.49]

Various types of cryptography techniques are discussed in detail in the subsequent sections.

2.3 TYPES OF CRYPTOGRAPHY TECHNIQUES

Several image encryption techniques have been proposed worldwide [30, 31, 101–103]. These techniques have undergone tremendous advancements due to an increase in the

volume of data transfer, processing speed, and threats. In the beginning, many techniques suffered different types of attacks like Differential Attacks, Statistical Attacks, Noise Attacks, Weak Key, Known Key, and Man-in-the-Middle Attacks [84]. To secure the data from these attacks many improved techniques were introduced with time. The detailed description of the same is as follows:

- i. **Traditional Encryption Techniques:** These techniques used simple substitution and shifting procedures to encrypt the data such as Advanced Encryption Standard, Blowfish, and the Data Encryption Algorithm were used to encrypt text mainly [104]. These techniques are inefficient when are used to encrypt images [105, 106] due to the inherent characteristics of the images, like high correlation, larger redundancy, and high computational cost. However, some of the techniques like RC4, AES, TDES are still in use for key protection or small size image encryption, but for large size images other techniques are preferred. In this context, Chaos-based Cryptography Techniques [60, 74, 107–113] were developed to overcome these constraints in image encryption.
- ii. **Chaos Based Encryption Techniques:** These techniques have better security than Traditional Techniques due to several characteristics like high randomness, low computation time and high key space value [114]. To effectively apply Chaos Theory in cryptography, chaotic maps must be implemented in such a way that the entropy generated by the map should produce the requisite random Ciphertext. The purpose of encrypting with Chaotic Maps is to provide a high level of security using one-dimensional [115] as well as multi-dimensional [116, 117] chaotic keys. As a result, an attacker will have a tough task to extract the information without knowing the initial values of chaotic parameters, as well as cryptography keys. However, most of these techniques have drawbacks such as limited key space and low computation speed [118] because the amount of data flow on the internet is continuously rising up. That's why Quantum Chaos-based Encryption Techniques were developed to resolve these limitations.
- iii. **Quantum Chaos Based Encryption Techniques:** These techniques [119] have enhanced efficiency and security due to large key-space, low time complexity, and high randomness. The encryption is done by utilizing Uncertainty Principles of Quantum Mechanics on Logistic Maps which increases processing efficiency. The parallelism and entanglement properties of these quantum computation systems can efficiently ramp up processing tasks and secure data transfer [120–123]. The most important feature of Quantum Chaos-based encrypted image is having a No-clone property. According to this, it is impossible to make an independent and identical replica of any unknown quantum state. Because of the No-cloning Theorem and

the Uncertainty Principle of Quantum Mechanics, this strategy is more effective in protecting image content.

2.4 TRADITIONAL CRYPTOGRAPHY TECHNIQUES

The traditional cryptography mechanisms worked efficiently for textual data but not for images as these techniques has low processing speed and randomness. As a result, these are vulnerable to attacks. Some of the popular Traditional Techniques are explained in the subsequent subsections:

2.4.1 Vigenère Cipher

Vigenère Cipher [44] is a kind of polyalphabetic ciphers which consist of a series of different Caesar Ciphers for encryption. Polyalphabetic substitution is the method of replacing each pixel of the image with the corresponding element based on the given key value. It is decided with the help of a predefined substitution table shown in Table 2.2 that is named as Vignère Table [124].

Table 2.2: Vigenère Table

		← Pixel values of Plain Image →									
		0	1	2	3	4	5	6	-----	254	255
Key Values ↑ ↓	0	0	1	2	3	4	5	6	-----	254	255
	1	1	2	3	4	5	6	7	-----	255	0
	2	2	3	4	5	6	7	8	-----	0	1
	3	3	4	5	6	7	8	9	-----	1	2
	4	4	5	6	7	8	9	10	-----	2	3
	5	5	6	7	8	9	10	11	-----	3	4
	6	6	7	8	9	10	11	12	-----	4	5
	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
	254	254	255	0	1	2	3	4	-----	252	253
	255	255	0	1	2	3	4	5	-----	253	254

The table shows a sequence of values from 0 to 255 arranged in ascending order in the first row. The same sequence is repeated in next row by shifting the sequence circularly [125] in the left direction. Similarly, each row is generated by rotating the values of previous row. During the encryption process, the Plain Image's pixels are divided into N numbers of blocks, each of which is the same length as the key.

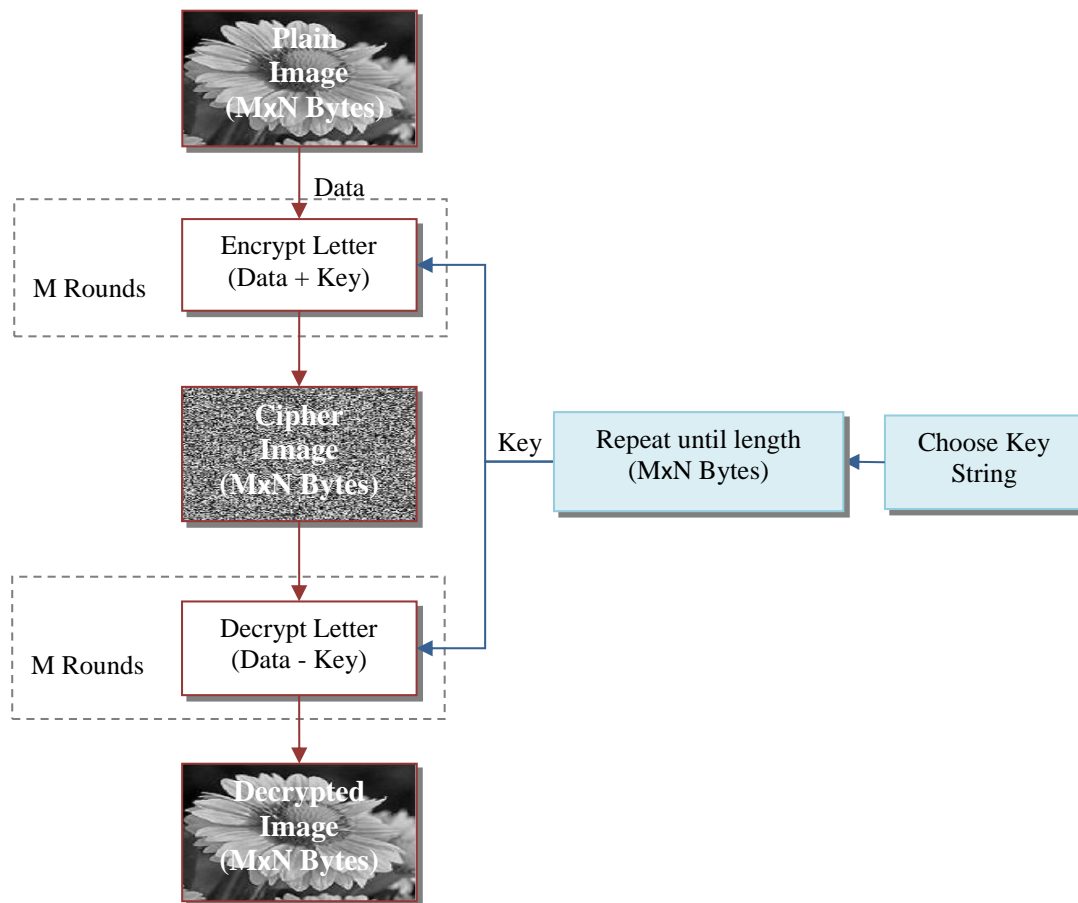


Figure 2.1: Block Diagram of Vigenère Cipher

After this, a row is chosen based on a key value, and a column is chosen based on the Plain Image's pixel value. The matching element from the Vignère Table replaces the pixel value from the Plain Image. The technique's most prominent property is that a repeated pixel value is changed into a different value, resulting in a randomly pixel distributed image. Using the same Vigenère Table, the original image may be reconstructed from the Ciphered Image. Decryption can be done by looking up the ciphered element in the row corresponding to the key value, then the column number same as the ciphered pixel value will represent the decrypted output, i.e. the original pixel value. This technique was originally developed by G. B. Bellaso [125] in 1555 and later on became popular in secret writing. The complete process of cryptography using Vigenère Cipher is shown in Figure 2.1.

2.4.2 Data Encryption Standard

Data Encryption Standard (DES) [45] is one of the earliest Block Ciphers, developed in the 1970s, at IBM and later adopted by the National Bureau of Standards. The block diagram for the DES encryption process is shown in Figure 2.2. A Plain Image is

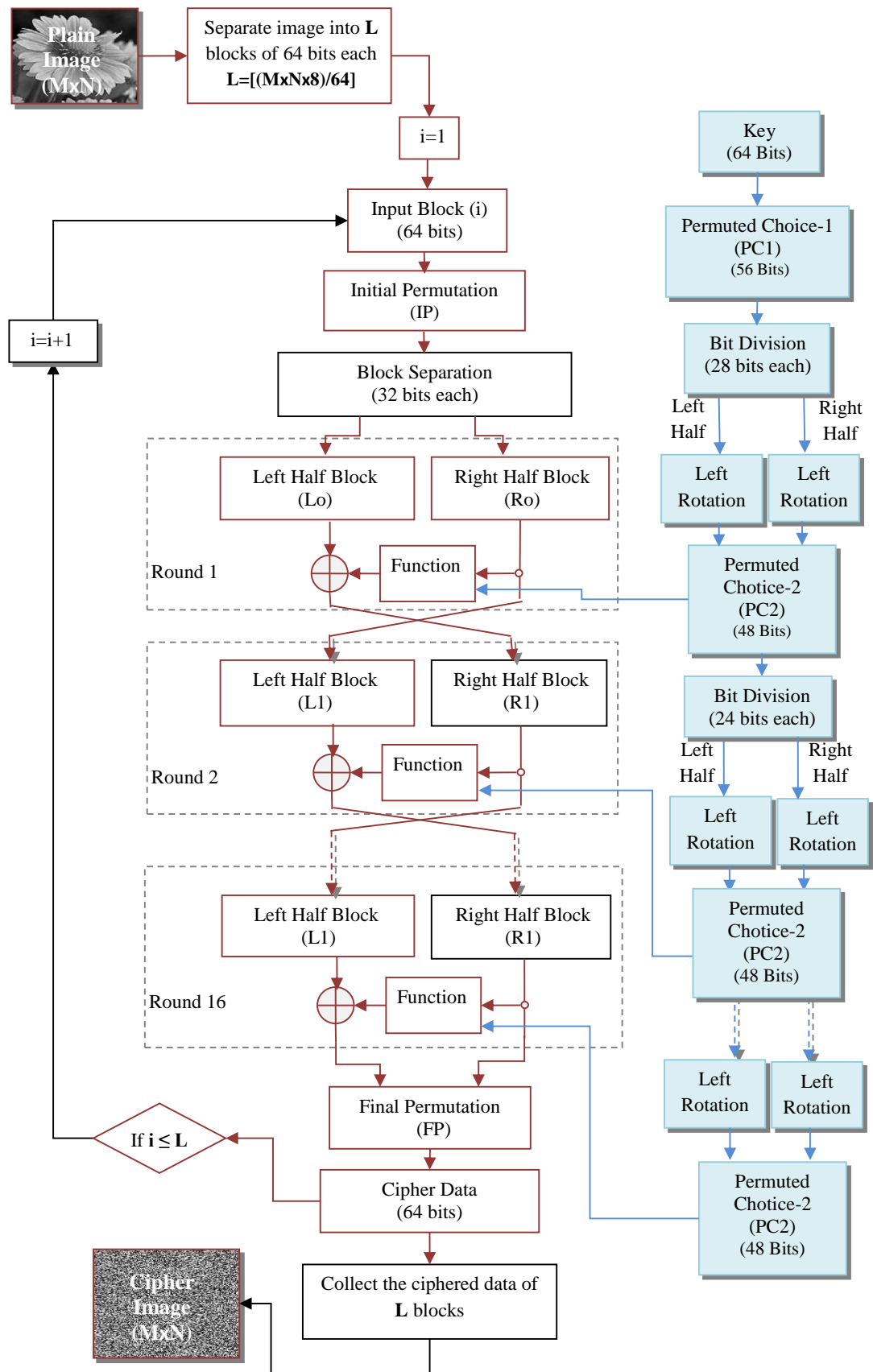


Figure 2.2: Block Diagram of Data Encryption Standard

divided into L number of blocks, each block containing 64 bits, and it employs a string of fixed length, 64 bits. Additional 0s are inserted if the last block does not have 64 bits. Each block is encoded 16 times using different permuted key versions. The initial key has a length of 64 bits, with 8 bits set aside for parity tests. Table Permuted Choice-1 is used to permute the remaining 56 bits. This is then divided into two equal portions, each with 28 bits, and cyclically rotated by one or two bits to the left. After that, combining both parts provides a permuted 56-bit result, which is then reduced to 48 bits using Table Permuted Choice-2. For round 1, this is referred to as the first Subkey applied to the encryption function. The operation is repeated up to 16 times in order to generate multiple permuted 48-bit versions, which are fed to each round as a Subkey. To begin, a single block of data (64 bits) is permuted using the Initial Permutation (IP) Table. The permuted block is split into two 32-bit halves: left and right. The right half of the block is given a function, which is then XORed with the left half of the block. The most difficult component of this encryption process is applying the function. To begin, the block's right half is enlarged from 32 to 48 bits and XORed with the first Key. The 48 bits are then separated into 8 parts, each with 6 bits evenly distributed, and 8 S-boxes are used as substitution boxes to reduce each part from 6 bits to 4 bits. As a result, the bits of eight blocks are combined and XORed with the remaining Left half block. The left and right halves of each block are then swapped in the following phase. This is performed 16 times with 16 round Keys, with the modified left and right half blocks combined to generate ciphered data in the final step. The same technique is repeated for all L-blocks, resulting in the encryption of the complete image.

Decryption follows the same mechanism of rounds as encryption does, but in reverse order with the order of subkeys inverted. Even though the encryption and decryption processes proceed in a high number of rounds, the DES security mechanism is breachable in many ways. Brute Force and Known-plain Text Attacks [126] are most common, making the technique vulnerable.

2.4.3 International Data Encryption Algorithm

International Data Encryption Algorithm (IDEA) [47] also known as Improved Proposed Encryption Standard (IPES) [127]. It is a symmetric-key block cipher and a successor of the Proposed Encryption Standard (PES) [128]. This technique entirely avoids the use of any lookup Tables or substitution boxes. It uses a fixed key size of 128-bits and a block size of 64-bits. Figure 2.3 shows the block diagram of encryption process of IDEA. The encryption and decryption structures are similar and use eight full rounds plus an additional half-round, making a total of 8.5 rounds. The various components included in each round are Bitwise Exclusive-OR (denoted by an encircled + sign= \oplus), modulo 2^{16} Addition (denoted by a squared + sign= \boxplus), and modulo

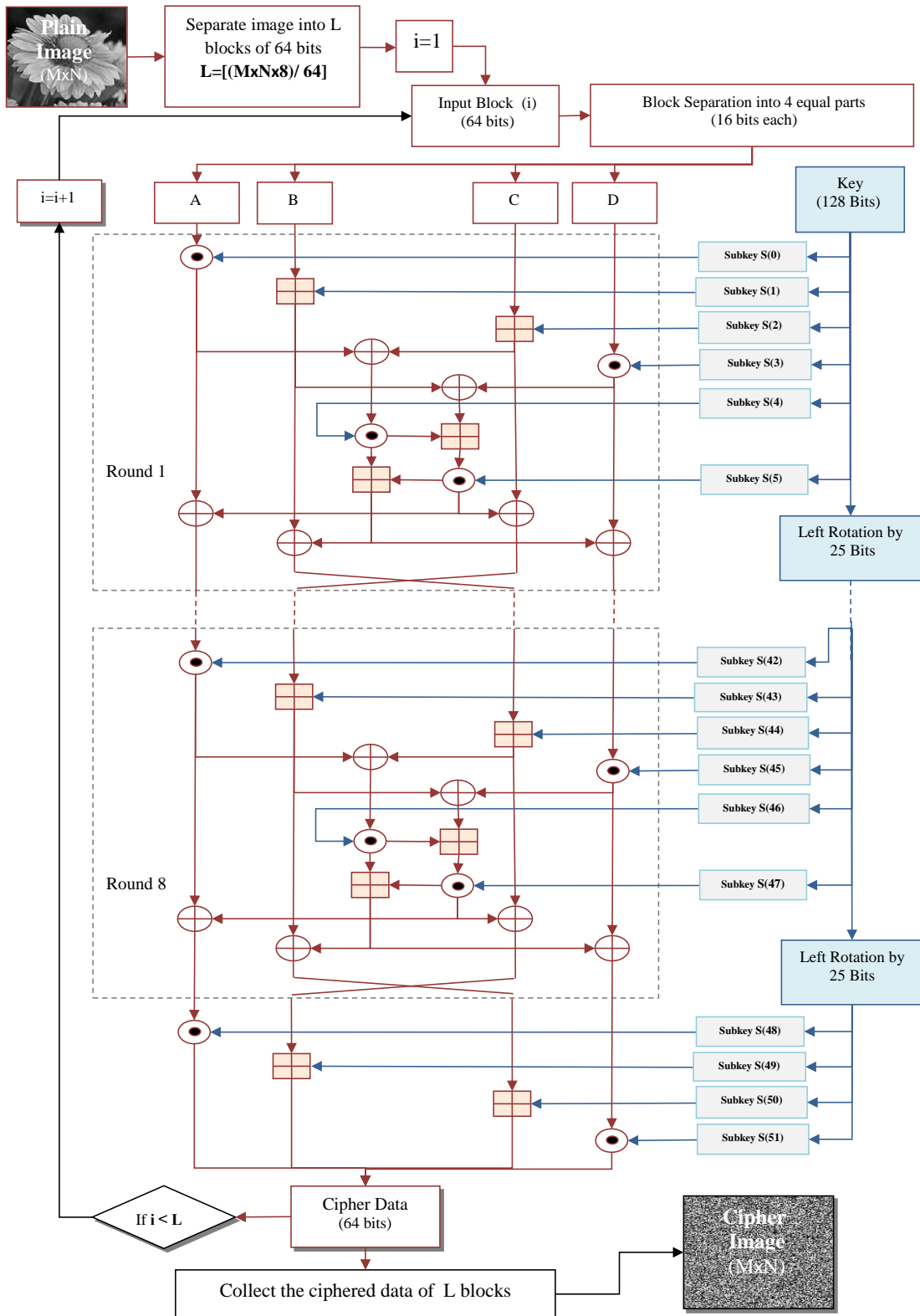


Figure 2.3: Block Diagram of International Data Encryption Algorithm

$2^{16} + 1$ Multiplication (denoted by an encircled dot= \odot). Each round uses a total of six Subkeys, while the half-round uses four Subkeys for both encryption and decryption processes. So, IDEA uses a total of 52 Subkeys which are obtained directly from the

initial key. In the Subkey Generation Process, firstly the 128-bit initial key is bifurcated into 8 parts of 16 bits each. Then these bits are cyclically rotated in 25 rounds successively in 7 rounds. By 25-bit left rotation of the key, all the bits of previous arrangement are exhausted. The 896 bits acquired during the course of these seven rounds are combined and reshaped into 56 sets. In the entire procedure, these 56 sets are used as 56 Subkeys. Now during the encryption process, the pixels of the Plain Image are separated into L blocks of 64 bits each. Then one by one every block is encrypted. The first input block is divided into 4 equal sections which are labeled as A, B, C, and D. Parts A and D are modified by modulo $2^{16} + 1$ multiplication with the help of Subkey S(0) and S(4) respectively, while parts B and C are modified by modulo 2^{16} addition with the help of Subkeys S(1) and S(2) respectively. The result of XORing modified part A with modified part C is applied to modulo $2^{16} + 1$ multiplication with Subkey S(4). The outcome is updated by modulo 2^{16} Addition with the help of XORed result of modified part B and D. This part is again modulo multiplied with Subkey S(5) and this leads to modulo addition with the previously modified part that was received from S(4). These two segments are XORed with modified parts A, B, C, and D. Part B and C are swapped and fed to the next eight similar rounds and all the subkeys are utilized. Lastly, all the encrypted blocks are collected and arranged into $M \times N$ sized images.

The same procedure is repeated in reverse order to obtain the Plain Image from the ciphered image. In this, the encryption Subkeys in the quadratic clusters, like S(0) to S(3), are substituted in an inverted order, here S(51) to S(48) respectively. While the paired Subkeys, like S(4) and S(5), are directly substituted, here S(46) to S(47) are processed in the same way. IDEA is vulnerable to various kinds of attacks like Narrow-bicliques Attack and Man-in-the-middle Attack.

2.4.4 Blowfish

Blowfish [48] is a symmetric-key block cipher algorithm. Its main component is a Feistel network, iterating 16 times. It was firstly designed by Bruce Schneier in 1993. The size of the block used is 64 bits like the DES algorithm. But, unlike DES, it uses a variable key length of 32-448 bits. Despite having a convoluted initialization, there is efficient encryption of data. The complete process is done in two parts: Key Expansion and Data Encryption. A key-expansion part extracts eighteen 32-bit Subkeys from the initial key and stores them in a P-array which are used in the XORing during encryption and decryption parts of the algorithm. Each iteration in the data encryption part consists of four 32-bit substitution boxes (S-Box) with 256-entries each.

The Plain Image is first scanned as a one-dimensional array. It is separated into L blocks of 64 bits each and entire process of the Blowfish technique is applied on each block, in sequence. The first 64-bits block is divided into two halves of 32-bits each,

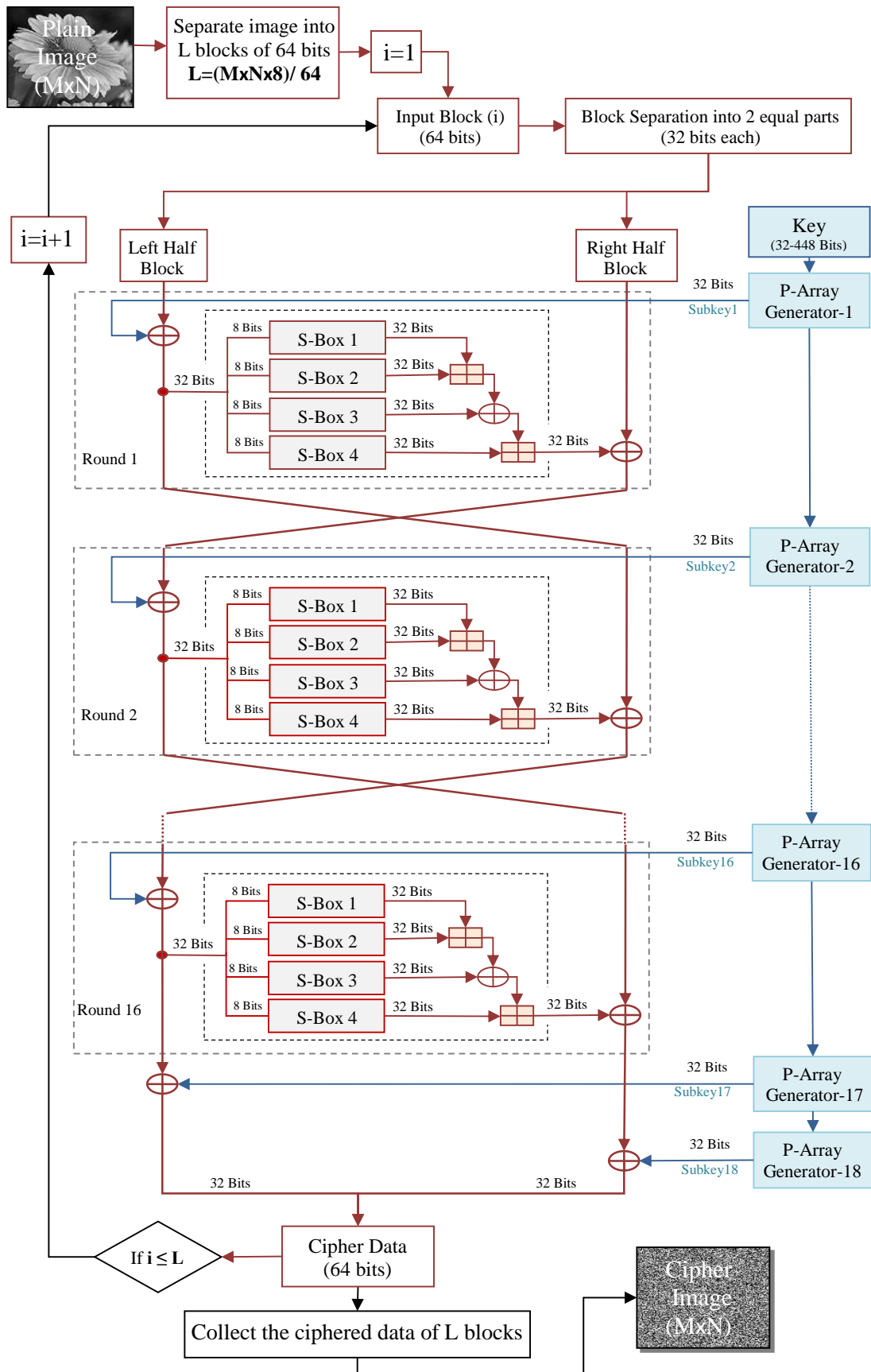


Figure 2.4: Block Diagram of Blowfish Algorithm

referred to as the left half and right half blocks. The left half of the block is XORed with first Subkey of P-array. The resulting 32 bits are divided into four parts of 8 bits each and applied to four S-boxes which expand the 8 bits into 32 bits. The first and second expanded results are added and XORed with third expanded bits. Similarly, the outcome is added with the fourth expanded bits and XORed with the remaining right half block. These modified right and left blocks are swapped and fed to the next round. The same process is repeated 16 times with the help of 16 Subkeys. The resulting left and right half blocks are XORed with Subkey 17 and Subkey 18 respectively. These bits are then combined into 64 bits. Finally, the Ciphred data from L blocks are assembled into a Plain Image of the same size. The block diagram of the encryption process is shown in Figure 2.4.

The reverse procedure is followed to decrypt the Ciphred Image into the Plain Image. This method's main drawback is that it can only be applied in circumstances where the key regularly changes, such communication links. Also, due to the small block size, files greater than 4 GB are not recommended to be encrypted.

2.4.5 Visual Cryptography

Visual cryptography [49] is the famous technique of hiding the secret messages, like: images, objects, or texts in multiple shares format. The initial research on visual cryptography was based on two share schemes and constituted only of black and white components. But in recent years, researchers have explored visual cryptography for

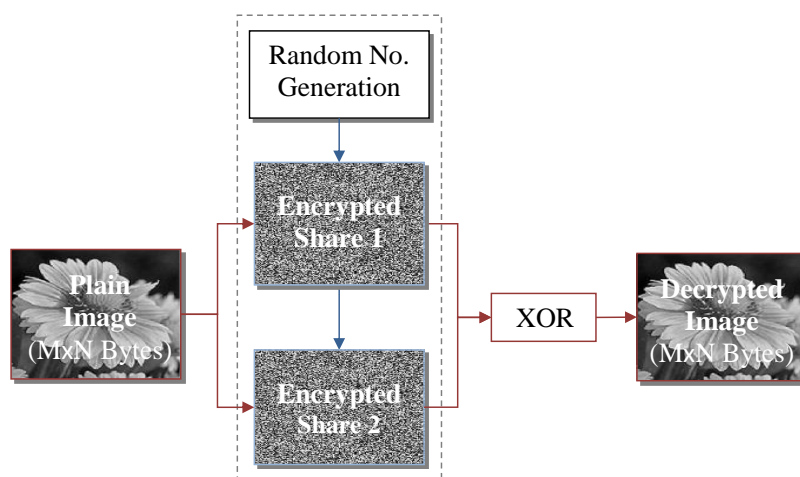


Figure 2.5: Block Diagram of Visual Cryptography

gray-scale and color images too. Along with that, the number of shares has also been increased beyond two. It is a promising alternative to other image encryption techniques because instead of using complex algorithms for securing the data it uses the

visual perception which is very simple to implement and executed. Hence, this adds an additional layer of security. Random values in the range of 0 to 255 are used to build a matrix of the same size as a Plain Image. The block diagram of visual cryptography is shown in Figure 2.5. Two shares are created with the help of this random matrix, whose pixel values are replaced with the Plain Image's pixels according to a set criterion. The two shares in the B/W picture encryption process have pixel pairs in the order BW or WB that overlap to form the final images. The overlap method is simply XORing the components, which makes the process simple and efficient. As a result, image decryption is impossible until the intruder has both the shares and the password. Though this technique is very simple and fast, yet it is vulnerable to attacks [56] since all the packets or shares passes through the same network.

2.4.6 Rivest Cipher 4

Rivest Cipher 4 (RC4) [50] is a remarkably fast and simple symmetric key stream cipher technique. It was first designed by Ron Rivest in 1987 originally as a trade secrets but was leaked a few years later in 1994 [108]. The algorithm uses a key length varying from 1-256 bytes. A pseudo-random sequence is generated to encrypt the original image using bit-wise XOR operation. In this technique, the key is fed to a pseudo-random byte

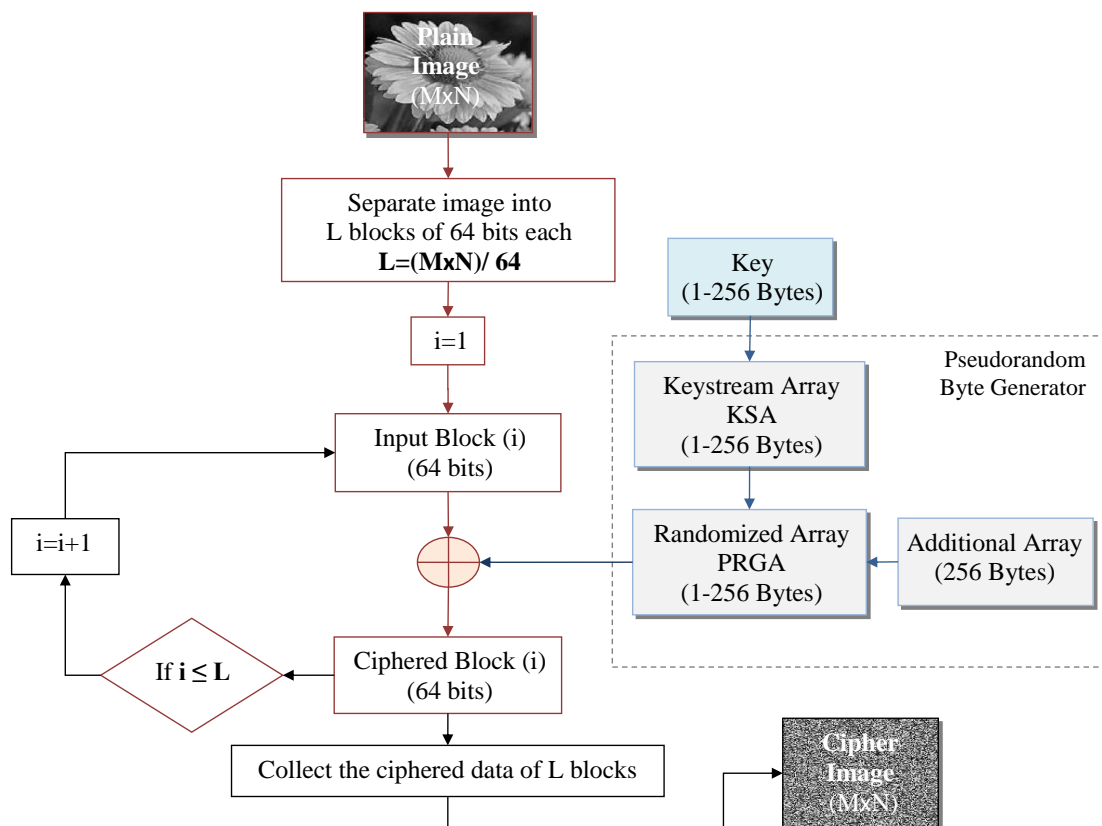


Figure 2.6: Block Diagram of Rivest Cipher 4

generator with the help of Key Scheduling Algorithm (KSA) where a randomized array is created using the key and an additional array. The additional array is the one that consists of 0 to 255 values in sequence. During encryption, the Plain Image is divided into L blocks of 64 bits each, and each block is bit-wise XORed with the pseudo-random generator's output one by one as shown in Figure 2.6.

The decryption process follows the same mechanism but in reverse order. Regardless of its simplicity, speed, and easy implementation, its applications are limited because it possess several vulnerabilities such as In-variance Weakness [50], which uses numerous partial plain-texts recovery attacks to steal data like credit card numbers, passwords, etc. To make RC4 robust against this and other types of attacks, various variants like RC4A, spritz, RC5 and RC6 have been developed.

2.4.7 Rivest Cipher 5

This Symmetric-key Block Cipher is a successor of RC4 [51]. The block diagram of Rivest Cipher 5 (RC5) is shown in Figure 2.7. RC5 was also developed by Ron Rivest, seven years after its predecessor RC4 was developed, in 1994. The encryption and decryption processes are similar to RC4 and also simple to implement. More importantly, it is a straightforward structure which is useful for memory constrained devices like smart cards. The Plain Image is divided into L blocks of 32 bits, and each part is encrypted one after another. The algorithm can use a key size varying from 0–2040 bits (with a recommended size of 128 bits), and the key schedule is more complex than its predecessor i.e. RC4. Each byte of the key is first converted into c -Words whose value is decided with the help of the key up to four decimal places. If the final value is a complex number, the rounded value is considered. This component is then mixed with two Magic Components, P_w and Q_w which are used to initialize total t -Words i.e. $2 \times (\text{no. of rounds} + 1)$. It is used for initializing the array of N number of Subkeys. These Subkeys are then utilized in N rounds of identical processes. Each round performs the mixing of secret Subkeys with original data.

During the encryption process, the first block is separated into two equal parts: A and B . The two halves are first XORed and then cyclically rotated in the left direction as per the value of corresponding Subkeys. The resultant sequence is then added with the first Subkey and subsequently, the two halves are swapped. Again, the two halves were XORed with each other and cyclically rotated with B (second half value) times and XORed with the second Subkey. This process is repeated with an N number of rounds where N is user defined. The cipher uses a variable block size, which can be 32, 64, or 128 bits, and the number of rounds varies from 0 to 255. It is recommended to use 18–20 rounds for a fast and secure implementation. Its main limitation is that a differential attack using 244 chosen plaintexts that can break 12-rounds for 64-bit block.

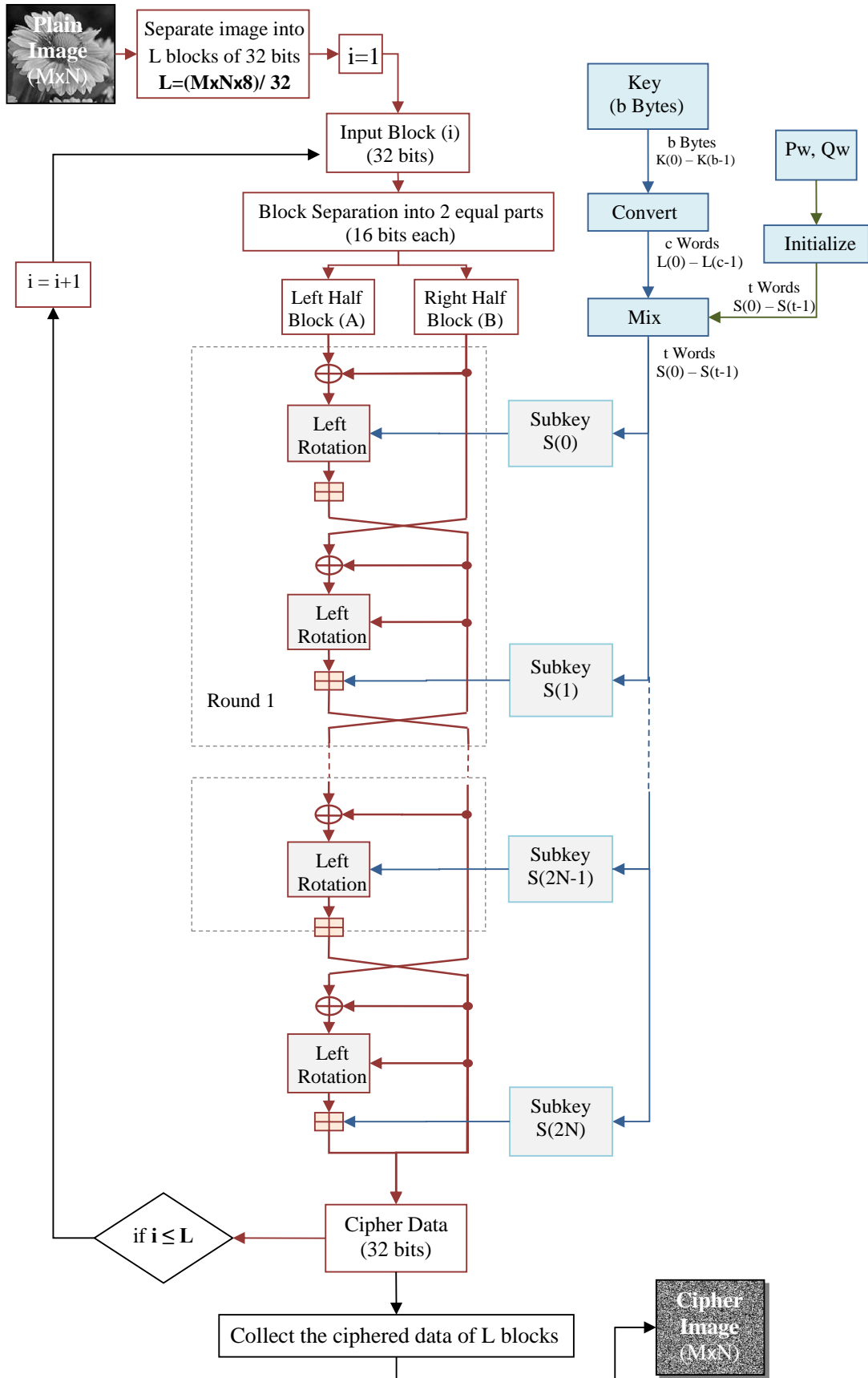


Figure 2.7: Block Diagram of Rivest Cipher 5

The decryption process is same as the encryption process but in reverse order.

2.4.8 Rivest Cipher 6

Rivest Cipher 6 (RC6) [52], a symmetric-key block cipher is a successor of the RC4 and RC5 algorithms. It was developed by Ron Rivest and others in 1998. The algorithm uses a key size of 128, 192, and 256 bits up to 2040 bits and uses a block size of 128-bits. It uses a Feistel network, the structure of which is very similar to RC5, with data-dependent rotations, modular addition, and XOR operations. RC6 could be interpreted as interweaving two parallel RC5 encryption processes, though RC6 uses an extra multiplication operation to make its rotation dependent on every bit in a word. Both the algorithms have a similar key expansion as both use a key of t words for Subkeys, which is generated from the predefined initial key. But RC6 uses four w -bit word registers instead of two. It also includes elements like a quadratic equation and integer multiplication as a part of the transformation. The Plain Image is divided into L blocks of size 64-bit each, encrypted one after another.

Key generation and encryption are the two major operations of this technique. In key generation, the same magic parts, P_w & Q_w , are taken as in RC5. These are utilized as an initial part for mixing with the original key. As a result, numerous Subkeys are generated and used at various stages of the encryption process. During the encryption process, the first half of the block is divided into four equal-length pieces A, B, C, and D. Part A is XORed with part C. The first and second Subkeys are added with parts B and D respectively. The updated parts B and D are subjected to a function in which these parts are doubled and incremented by one, and then circularly shifted to the left direction by four bits. With the XORed A and C, these results are employed by circular shift in the left direction. The next two Subkeys are then added to this result. Parts A and C have been replaced with parts B and D respectively. As shown in Figure 2.8, this process is continued until all the blocks have been encrypted.

The same process is used in reverse order to decrypt the encrypted image. The shortcomings of the predecessors of RC6 were largely overcome and there is no practical attack which can breach RC6 in a reasonable amount of time. This characteristic makes this encryption technique more efficient and secure to utilize for real time communication.

2.4.9 Triple Data Encryption Standard

Triple Data Encryption Standard (TDES) [53] also known as Triple Data Encryption Algorithm (TDEA), is a symmetric-key block cipher. As the name suggests, the algorithm utilizes the DES algorithm in all three processes i.e. encryption, decryption, and key generation processes. The Plain Image is firstly separated into L blocks of 64-bits

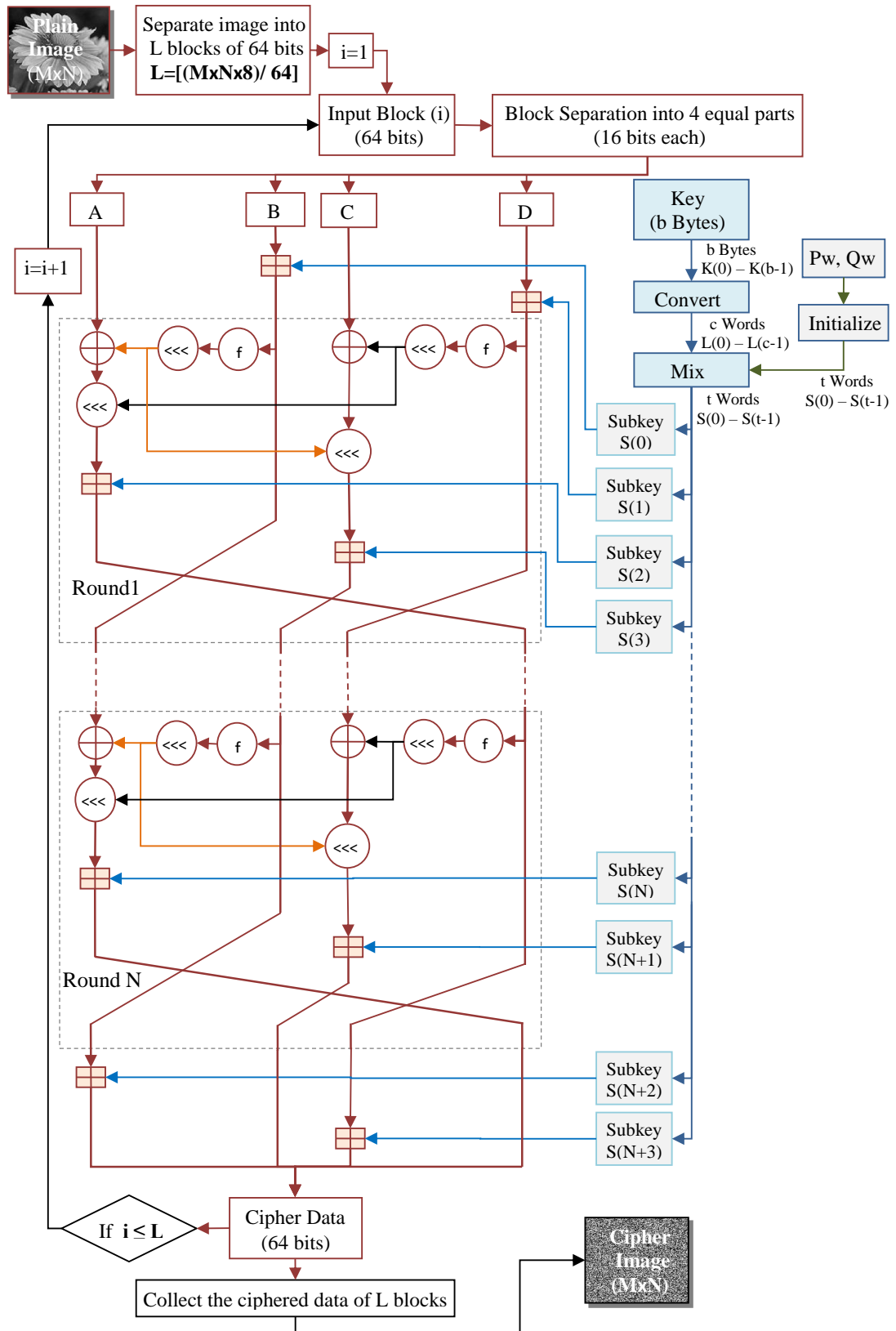


Figure 2.8: Block Diagram of Rivest Cipher 6

each and then each block is encrypted one after another. The original key, K of 56-bit is distributed to three parts of TDES, which consists of three different DES keys K1,

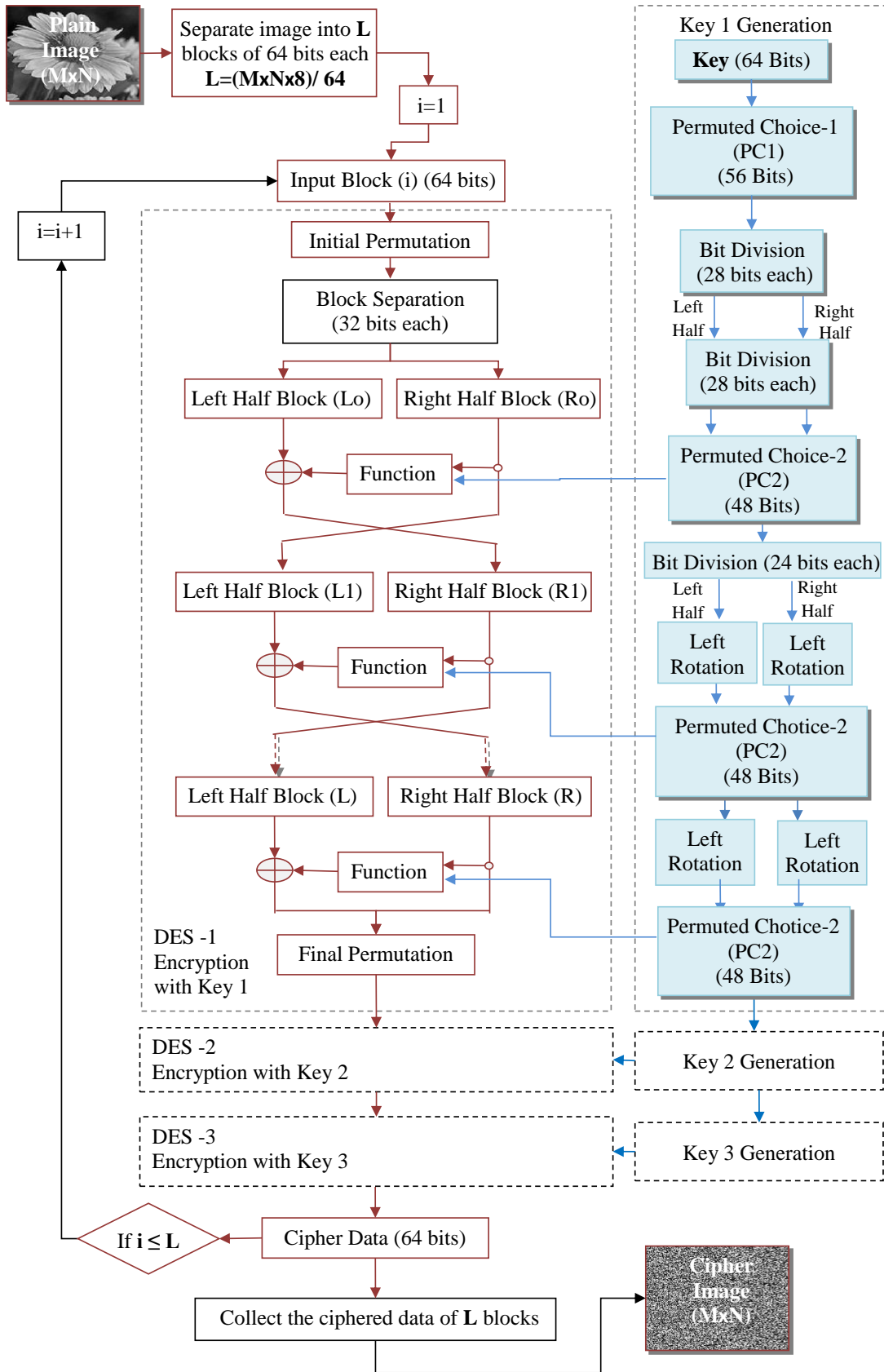


Figure 2.9: Block Diagram of Triple Data Encryption Standard

K2, and K3. The total length of three TDES keys becomes 168 bits. TDES uses these keys for the encryption and decryption processes. The process of selection of the keys is known as the keying option. The TDES process provides three keying options as follows:

- Keying option 1 – All the three keys are independent from each other. It is the most reliable keying option and is not vulnerable to any known practical attacks.
- Keying option 2 – K1 and K2 are independent, while K3 is the same as K1. It is resistant against meet-in-the-middle attack but is vulnerable to attacks like chosen-plaintext.
- Keying option 3 – All the three keys are identical. It is the weakest keying option.

Regardless of the keying options, the encryption processes of TDES use K1 to encrypt, K2 to decrypt, and K3 to encrypt the data again. Similarly, the decryption processes use the respective keys to decrypt, encrypt and decrypt the data. Figure 2.9 shows the block diagram of TDES. As the speed of data communication increases, there is a severe constraint on the TDES process to finish this in lesser and lesser time. It causes discomfort for users because it takes an unusually long time to execute. For the same reason, it is resistant to Brute Force Search Attack also.

2.4.10 Advanced Encryption Standard

Advanced Encryption Standard (AES) [54] is a symmetric-key algorithm belonging to the Rijndael cipher family. Specifically, three different members of the family were adopted by the National Institute of Standards and Technology, U.S. as AES [129]. It utilizes a substitution-permutation network structure, while the previously used DES technique was based on the Feistel network. It had an equal block size of 128-bit but had varying key sizes of 128, 192, 256-bits signifying increase in security with the increase in bits [94]. As AES is used with larger key bits, the number of cycles of repetition (rounds) increases, resulting in increase in the strength. The key expansion is the first and most important stage in creating Subkeys for each round. There is an extra Subkey for the Add Round Key phase. For key sizes of 128, 192, and 256 bits, the number of rounds required to encrypt a block of 128 bits is 10, 12, and 14 respectively. A single round is executed in four required steps are:

- i. Byte Substitution
- ii. Shift Row
- iii. Mix Column

iv. Add Round Key

These steps are executed for the first 9, 11, and 13 rounds of variable key sizes 128, 192, and 256-bits respectively. In addition, the Add Round Key step is applied at the start of the encryption process. The last round follows the same steps except for the Mix column step as shown in Figure 2.10. To begin, each Plain Image's pixel is placed

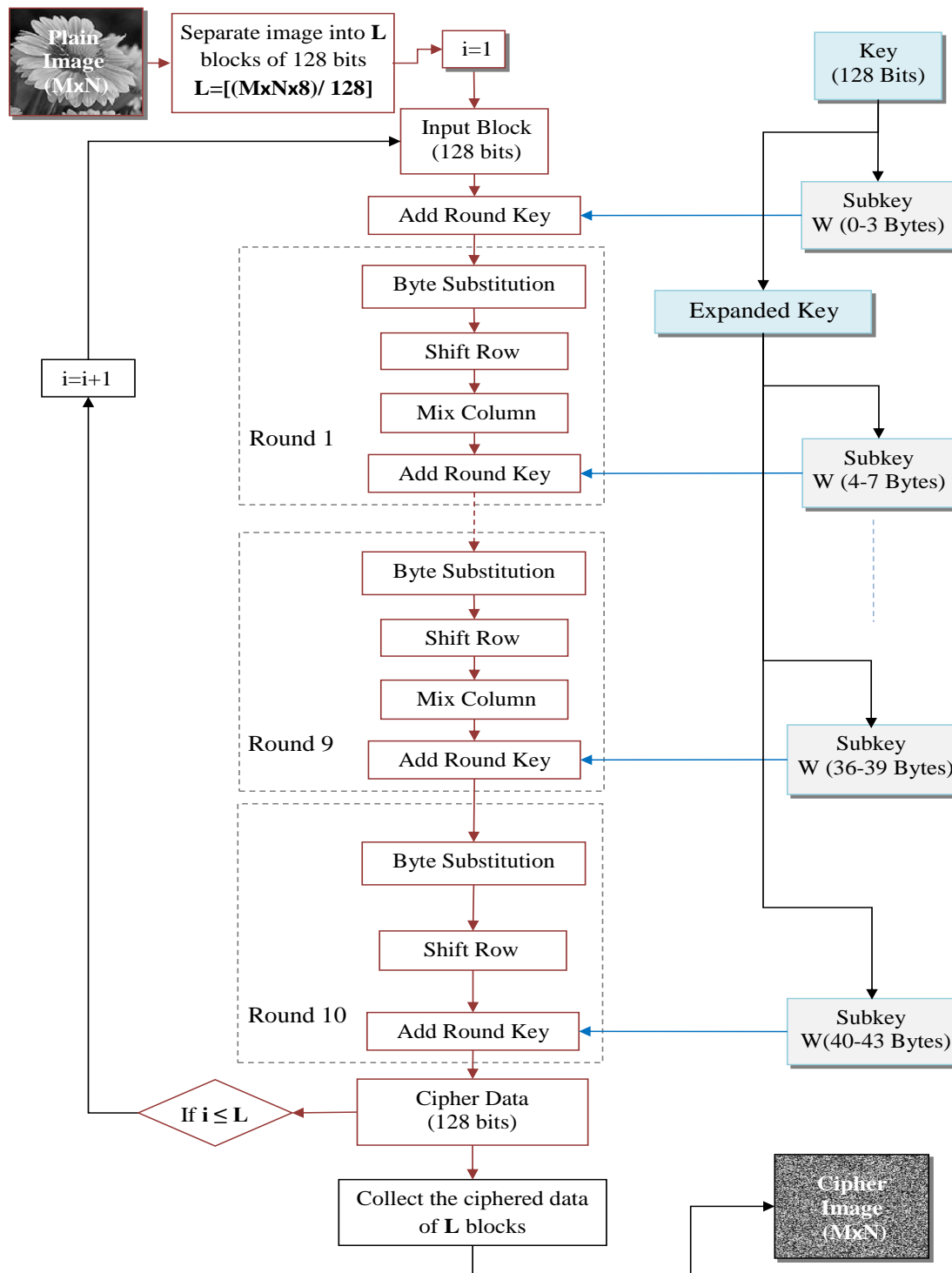


Figure 2.10: Block Diagram of Advanced Encryption Standard

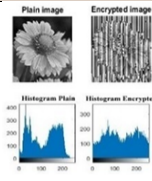
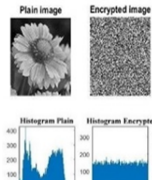
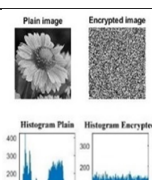
in an array and divided into L blocks of 128 bits each. Each block is encrypted one after another in succession. In the final stage, all of the encrypted pixels are collected and organized to match the Plain Image's dimensions.

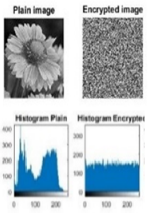
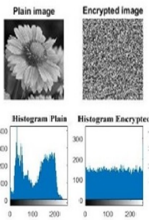
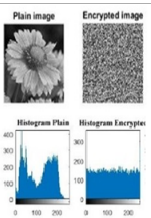
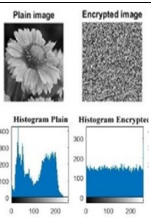
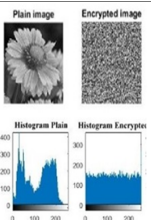
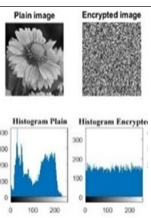
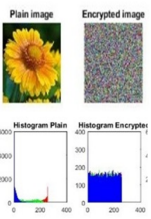
Decryption follows the same steps as encryption, but in reverse order to recover the Plain Image from the ciphered image. Researchers also introduced three different versions of AES. All three versions of AES have a very similar key schedule and use a significant number of Subkeys, such as eleven Subkeys in the 128-bit version. AES technique organizes data in two dimensions of size $M \times N$ after processing, which exhibits nonlinear effects resulting in enhanced security. Also, this technique is resistant to brute force search attack [117]. Hence AES algorithms are comparatively more secure.

2.4.11 Comparison of Traditional Cryptography Techniques

The overall comparison of traditional cryptography techniques on image data based on performance metrics is shown in Table 2.3. The highlighted values in green color specify the satisfactory or desired results which are satisfying the significant values of performance metrics.

Table 2.3: Overall Comparison of Traditional Cryptography Techniques

Cryptography Techniques	Image Perceptual Quality	Key Space	CC	NPCR	UACI	PSNR	Entropy	Execution Time (Sec.)
Vigene're Cipher		2^{128} (M)	0.2543 (H)	0.0625 (Fail)	0.0004 (Fail)	26.9690 (M)	7.8687 (M)	0.0788 (L)
DES		2^{56} (L)	0.0181 (M)	0.9967 (Pass)	0.3339 (Pass)	28.0967 (M)	7.9568 (H)	31.4582 (M)
IDEA		2^{128} (M)	0.0310 (M)	0.9950 (Pass)	0.3343 (Pass)	28.1452 (M)	7.9616 (H)	27.2763 (H)

Cryptography Techniques	Image Perceptual Quality	Key Space	CC	NPCR	UACI	PSNR	Entropy	Execution Time (Sec.)
Blowfish		2^{64} (L)	0.0219 (M)	0.9964 (Pass)	0.3355 (Pass)	28.1798 (M)	7.9576 (H)	12.9787 (M)
Visual Cryptography		Not defined	- 0.0052 (L)	3.45E-05 (Fail)	2.06E-07 (Fail)	28.1113 (M)	7.9937 (H)	0.0582 (L)
RC4		2^{256} (H)	0.0028 (VL)	0.9966 (Pass)	0.3354 (Pass)	28.0527 (M)	7.9919 (H)	0.3171 (L)
RC5		2^{128} (M)	0.0548 (M)	0.9955 (Pass)	0.3323 (Pass)	28.1598 (M)	7.9581 (H)	35.5005 (H)
RC6		2^{128} (M)	0.0216 (M)	0.9962 (Pass)	0.3362 (Pass)	28.1143 (M)	7.9870 (H)	43.2162 (H)
TDES		2^{168} (M)	0.0326 (M)	0.9952 (Pass)	0.2278 (Fail)	28.1747 (M)	7.9560 (H)	94.6852 (H)
AES		2^{128} (M)	0.0141 (M)	0.9962 (Pass)	0.3350 (Pass)	28.1161 (M)	7.9867 (H)	4.3634 (L)

From the Table, it can be seen that none of the techniques provides good results for all the performance metrics. To overcome the limitations of the traditional techniques another class of techniques known as chaotic cryptography techniques were developed. These were having good values for entropy, speed of execution as well as has large key space value. The next section provides a detailed description of few chaotic encryption techniques available in the literature.

2.5 CHAOS CRYPTOGRAPHY TECHNIQUES

As discussed above, traditionally designed encryption techniques [107] were complex and mainly compatible with texts. These techniques have low randomness, limited

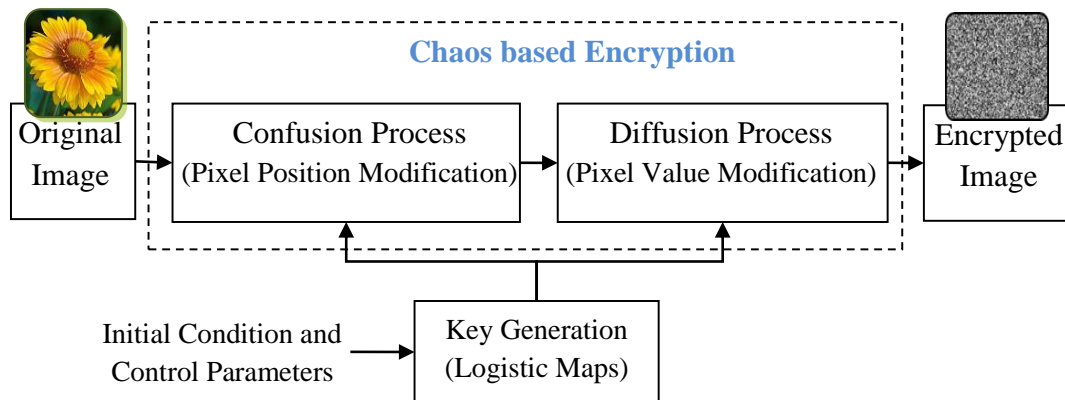


Figure 2.11: Chaos Based Image Encryption Technique

key size, and require large processing time to encrypt images. For this reason, the need for more secure and fast techniques was felt. Chaos-based techniques [68] were developed which fulfilled this objective to large extent. The logistic maps [61] are very popular for random number generation over a discrete range of input. In this kind of cryptography mechanism, secret keys are generated with the help of chaotic logistic maps and utilized at multiple levels of the encryption process, as shown in Figure 2.11. During the process, the pixel positions and values are both modified, which are termed as Confusion and Diffusion respectively. This leads to a higher degree of randomness in the encrypted images. Some of the popular Chaos-based Encryption Techniques are described in the following sub sections.

2.5.1 Chaos 1: A New Image Encryption Scheme Based on Chaotic Function using Linear Congruence

An image encryption algorithm is developed by François et al. [65] to utilize the linear congruence based chaotic function to generate large key spaces. The author mainly

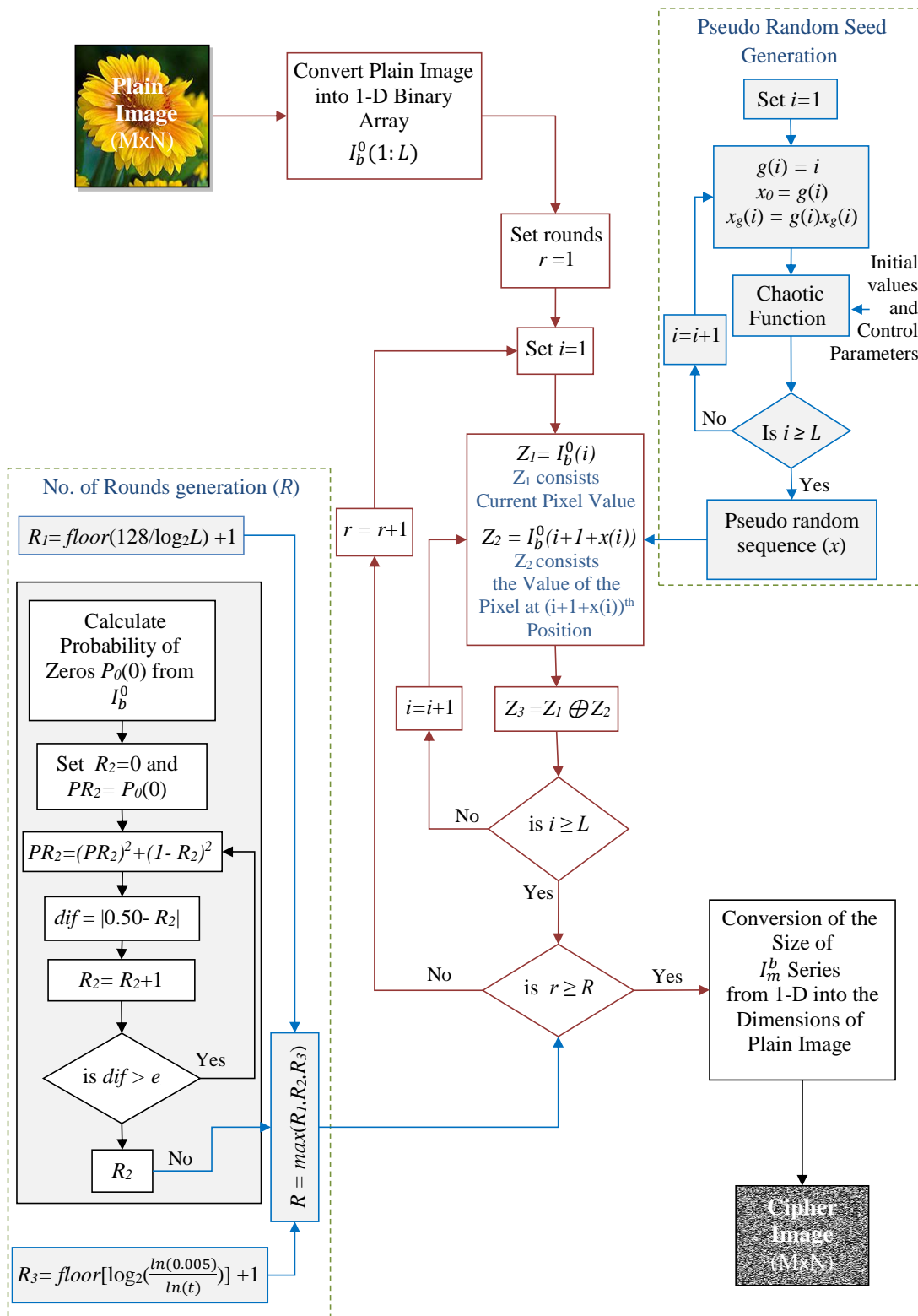


Figure 2.12: Block Diagram of Technique Based on Chaotic Function Using Linear Congruence

targeted the correlation between the neighboring pixels of the Plain Image to enhance the property of randomness in the Cipher Image. In the first step, the image is transformed into a binary one-dimensional vector I_0^b and a pseudo random seed 'g' of the same length of I_0^b is generated with the help of chaotic function [130]. The position of the pixels is modified with the help of pseudo-random seed 'g' and the scrambled pixel values are stored in vector x . Next, a new scrambled vector I_m^b is generated by adding the pixel values of I_0^b and with the pixel value of I_0^b whose position lies at value x . This process is repeated for R rounds (obtained from 3 round keys $R1$, $R2$, and $R3$) as shown in Figure 2.12 and finally the encrypted stream is reshaped as in the dimensions of the original image. In the final step, the obtained stream is reshaped to dimensions of the original image. The decryption process is carried out in exactly reverse order. The benefit of this algorithm is, it offers strong resistance against brute-force attack.

2.5.2 Chaos 2: An Intertwining Chaotic Maps-based Image Encryption Scheme

The concept of a Modified Classical Logistic Map was introduced by Sam et al. [64] in 2012 and named it Intertwining Chaotic Maps. These maps are used for the generation of Chaotic Keys utilized to perform Confusion and Diffusion Processes of encryption. These maps have highly random properties in comparison to a classical logistic map. The complete cryptosystem consists of four encryption processes i.e. Permutation to change the pixel value, Byte Substitution to enable the Confusion Process, Nonlinear Diffusion, and Sub-diagonal Diffusion along with Key Generation. Three sets of chaotic keys (x , y , and z) are generated with help of proposed intertwining chaotic maps [131] to encrypt the R, G, and B planes. Each map is iterated $M \times N$ times (size of a plane of the original image) in order to generate a random matrix of a size compatible with the Plain Image.

In the Confusion Process, initial permutation is carried out to scramble the pixel positions with the help of predefined six random values ($p1$, $p2$, $p3$, $p4$, $p5$, and $p6$) and then the resulting image is XORed with the first chaotic key(x). After this, pixel values are substituted with the help of an S-box (16×16) same as done in AES [129]. The resulting image is XORed with the second Chaotic Key (y). In the Diffusion Process, pixel values are modified in two steps i.e. Nonlinear Diffusion and Sub-diagonal Diffusion. The Nonlinear Diffusion is obtained by rotating bits of a pixel in the right direction five times and then XORing with the first Chaotic Key (x). Next, the pixel value is modified in the Sub-diagonal Diffusion step by XORing the first and second pixel. The resulting value is XORed with the third-pixel value and the similar process continues till the last pixel gets modified. In the last step, diffused image is XORed with the third chaotic key (z).

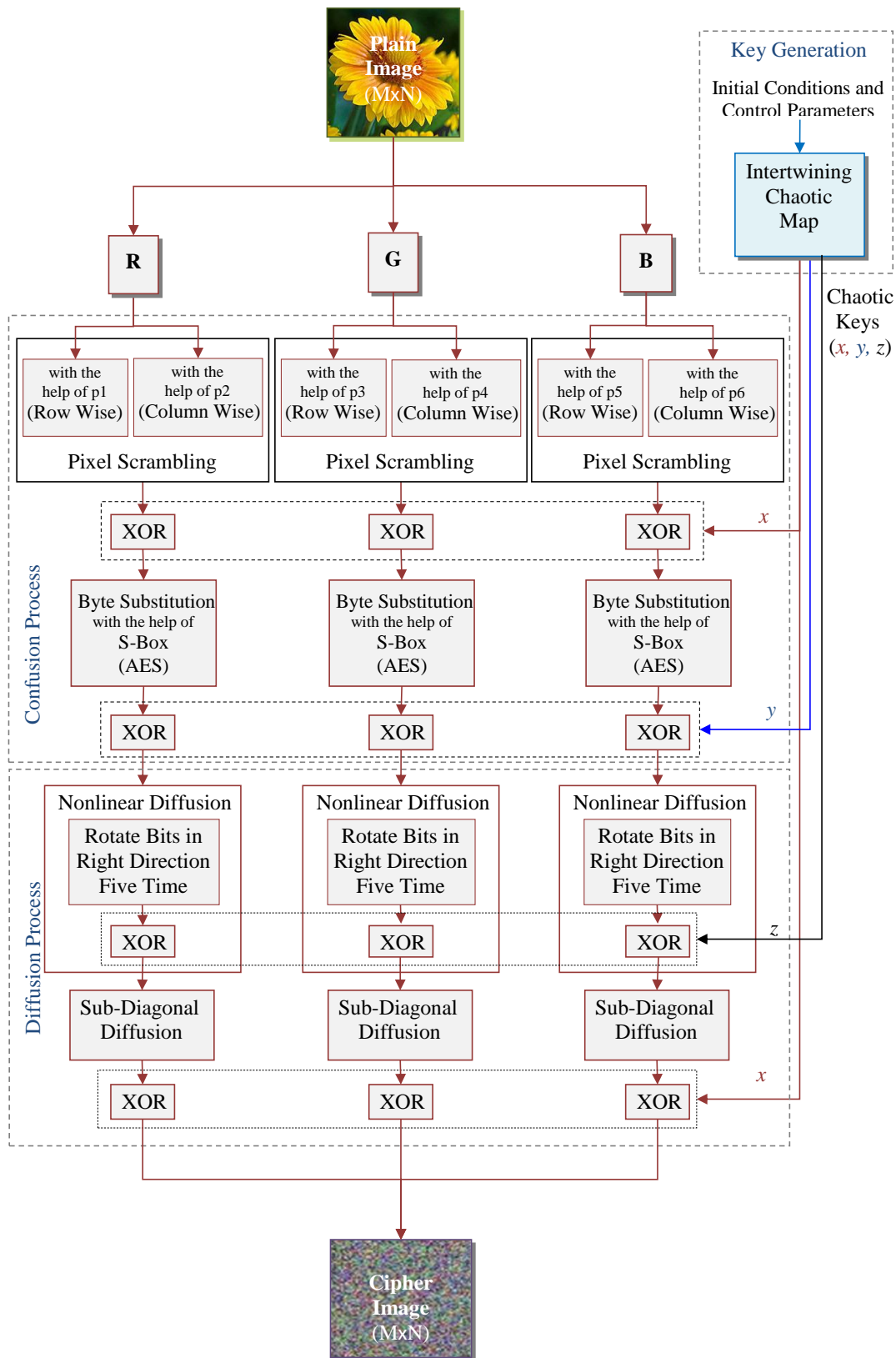


Figure 2.13: Block Diagram of Technique Based on Intertwining Chaotic Maps

Two rounds of iterations are carried out to enhance randomness. The complete encryption process is shown in Figure 2.13. The same process is carried out to decrypt the encrypted image but in reverse order. This cryptosystem is robust against known Plaintext and Brute Force Attacks. Further, it also provides good coherence in Key Space Analysis, Differential Analysis, and Statistical Analysis.

2.5.3 Chaos 3: A Novel Image Cipher Based on Mixed Transformed Logistic Map

A Mixed Transformed Logistic Map was used to design a cryptosystem for encryption of colored pixels by Sam et al. [66] in 2012. The encryption process uses nine keys, six of which are denoted as odd secret keys while the rest three (x, y, z) are Chaotic Keys. The three Chaotic Keys x, y , and z are of the same size of the Plain Image which is generated with the help of Mixed Transformed Logic Maps. Like every chaotic based encryption technique, this technique is also having Confusion and Diffusion Processes.

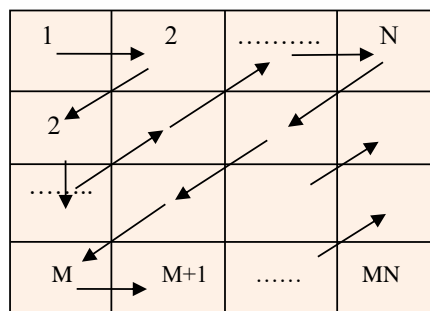


Figure 2.14: Zig-zag Diffusion

Initially, the pixel positions are permuted with the help of six odd keys and XORed with the first Chaotic Key (x). The Diffusion Process is completed in two steps i.e. Nonlinear Diffusion and Zig-Zag Diffusion. In the Nonlinear Diffusion, bits of pixels are rotated four times in the right direction and the result is XORed with a Second Chaotic Key (y). In the Zig-zag Diffusion, the colored image is separated into three (red, green, and blue) channels and is processed in a Zig-zag direction as shown in Figure 2.14 to obtain intra-channel mixing. On the resulting Zig-zag positions, pixels are XORed with the Third Chaotic Key (z). The block diagram of the technique based on Mixed Transform Logistic Maps is shown in Figure 2.15.

For decryption, the same procedure is carried out in the reverse direction. This process reduces the vulnerability against well-known differential attacks [132]. The algorithm has shown good coherence in various attack analysis including key space analysis, differential analysis, and statistical analysis [133].

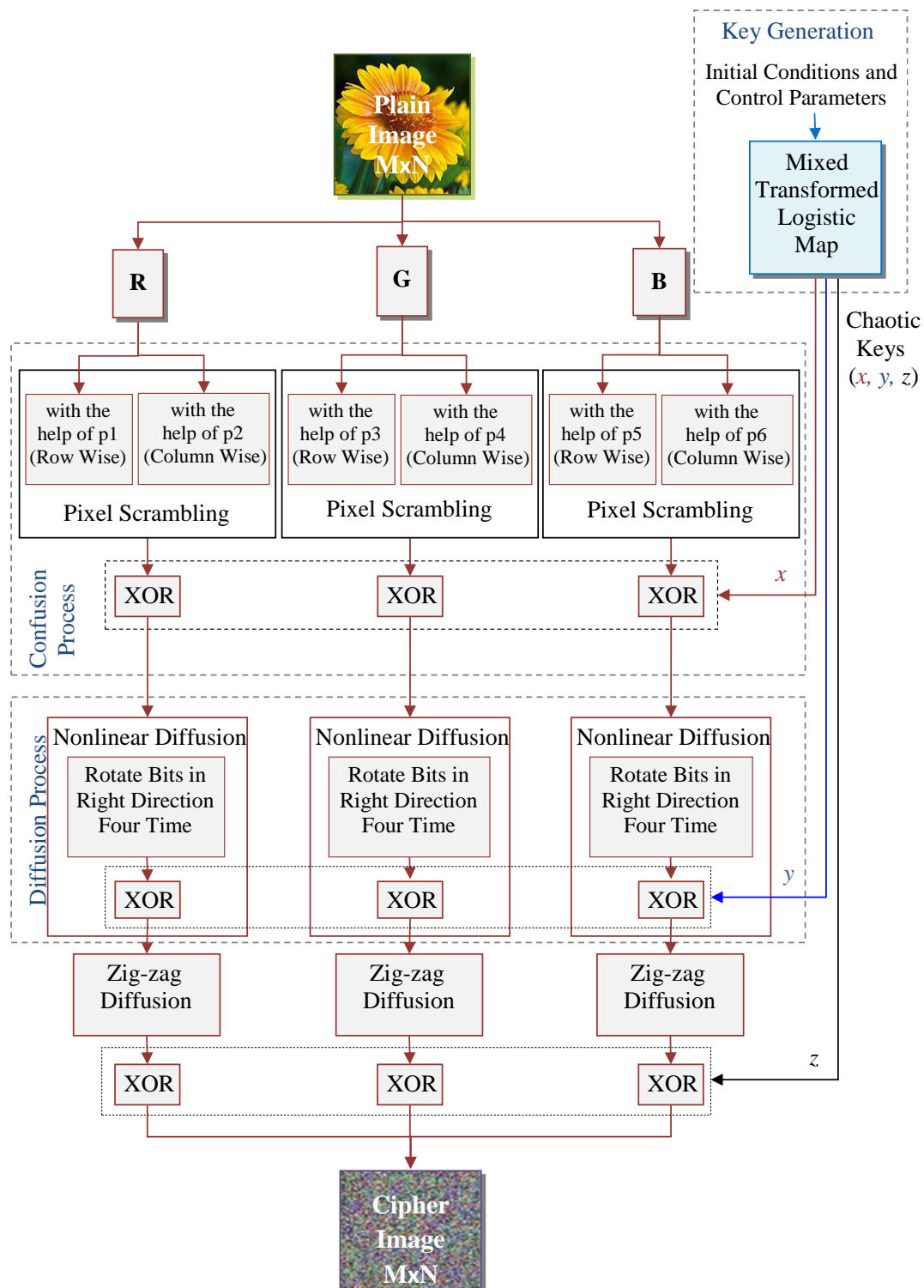


Figure 2.15: Block Diagram of Technique Based on Mixed Transformed Logistic Map

2.5.4 Chaos 4: An Effective Image Encryption Scheme Based on Peter De Jong Chaotic Map and RC4 Stream Cipher

Hanchinamani and Kulkarni [67] proposed a technique based on Peter De Jong chaotic map and RC4 Stream Cipher to generate a highly random cryptosystem. The encryp-

tion process is completed in three major steps i.e. Pixel Permutation, Pixel Rotation, and Diffusion to encrypt an image of size $M \times N$. The algorithm utilizes Peter De Jong Chaotic Map [134] and generates the two sets of keys (x and y) 128 keys each with the help of six secret keys, as initial input condition parameters. As a result, total of 256 key values are obtained. The Key Scheming of round key generation is given in Table 2.4.

Table 2.4: Key Scheming

ROUNDS	KEY VALUES (0:256)	
	Key values (0:127)	Key values (128:255)
1	$x(0), x(1), x(2), \dots, x(127)$	$y(0), y(1), y(2), \dots, y(127)$
2	$x(128), x(129), \dots, x(255)$	$y(128), y(129), \dots, y(255)$
3	$x(256), x(257), \dots, x(383)$	$y(256), y(257), \dots, y(383)$
So on..

The process is iterated two times to attain a high level of security. The resultant values of x and y are placed in PM and PN respectively. The sorted values of PM and PN are placed in PM' and PN' respectively. Now the pixel's positions are permuted row wise and column wise according to the values of PM' and PN' . After this a Pseudorandom Stream is generated with the help of RC4 Stream Cipher Technique, keeping PM' and PN' Values as input. The resulting stream is used for scrambling a pixel's bit position by applying rotation in the left/right and up/down direction. A Pseudo-random Stream is generated again with the help of an RC4 Stream Generator. It is used in the final step which includes a Forward and a Backward Diffusion on the rotated image. The cryptosystem is very effective, and it maintains a high level of security by applying only two rounds of encryption processes. The complete encryption process is shown in Figure 2.16. For decryption, the same process is followed but in reverse order. It is highly resistant against Brute Force, and Differential Attacks.

2.5.5 Chaos 5: An Innovative Image Encryption Scheme Based on Chaotic Map and Vigenère Scheme

In 2016 Bansal et al. [68] introduced a technique based on Chaotic Map and Vigenère Scheme for encryption of a color image. This encryption technique consists of two iterative states i.e. Diffusion and Confusion. The technique employs a very complex method of key generation in which different sets of Chaotic Keys is used at every stage

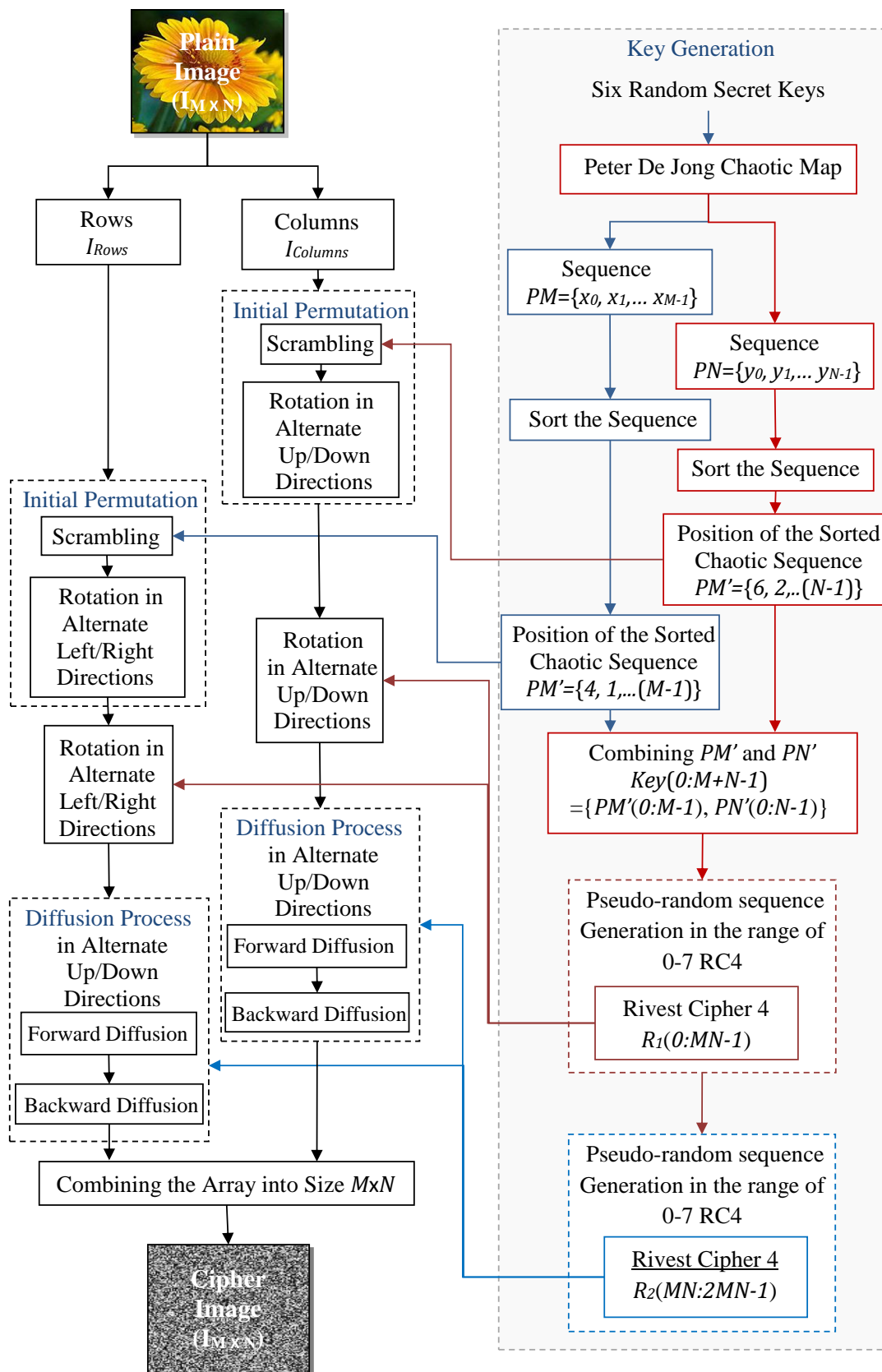


Figure 2.16: Block Diagram of Technique Based on Peter De Jong Chaotic Map and RC4 Stream Cipher

of encryption. Due to this, the cryptography technique is highly robust against Chosen and Plain-text Attacks.

In the Key Generation, predefined seven random secret keys (k_1 – k_7) are used to generate random sequences for encryption as explained in Table 2.5. It is done by two subprocesses, one subprocess utilizes Sine Map [135] and another is a combination of the Logistic Map and Intertwining Chaotic Map [131].

Table 2.5: Details of Key Generation for Encryption Process

Channel	Secret key	Name of Chaotic Map	Resulted sequence	Size	Purpose of sequence Generation
	k_1	Sine Map	Sin_c	1:N	Confusion Process
			Sin_d	1:M	Diffusion Process and Vignère Matrix Creation
x-channel	k_2, k_5	Intertwining Chaotic Map and Logistic Map	$xlog_c$	1:N	Confusion Process
			$xlog_d$	1:M+N	Diffusion Process and Vignère Matrix Creation
y-channel	k_3, k_6	Intertwining Chaotic Map and Logistic Map	$ylog_c$	1:N	Confusion Process
			$ylog_d$	1:M+N	Diffusion Process and Vignère Matrix Creation
z-channel	k_4, k_7	Intertwining Chaotic Map and Logistic Map	$zlog_c$	1:N	Confusion Process
			$zlog_d$	1:M+N	Diffusion Process and Vignère Matrix Creation

The resultant sequences are the key values for encryption of red, green, and blue color planes, which are denoted as x-channel, y-channel, and z-channel respectively. The encryption process consists of two stages i.e. Diffusion and Confusion. The three steps of the Diffusion stage i.e. Pixel Permutation, Forward and Backward Diffusion are done by matching process with the help of Vignère Tables. The Tables are generated according to the sine map and logistic maps. In the Confusion Process, the image is divided into two sequences. One sequence will contain row values and the other sequence contains column values. Then the row and column numbers of a pixel are permuted by sine map and z-channel generated sequences respectively. The same steps are repeated for green and blue components. In the end, the Cipher Image is formed by the concatenation of all the three modified planes. Figure 2.17 shows the complete encryption process. The same process is carried out in a reverse manner to decrypt the image at the receiver side.

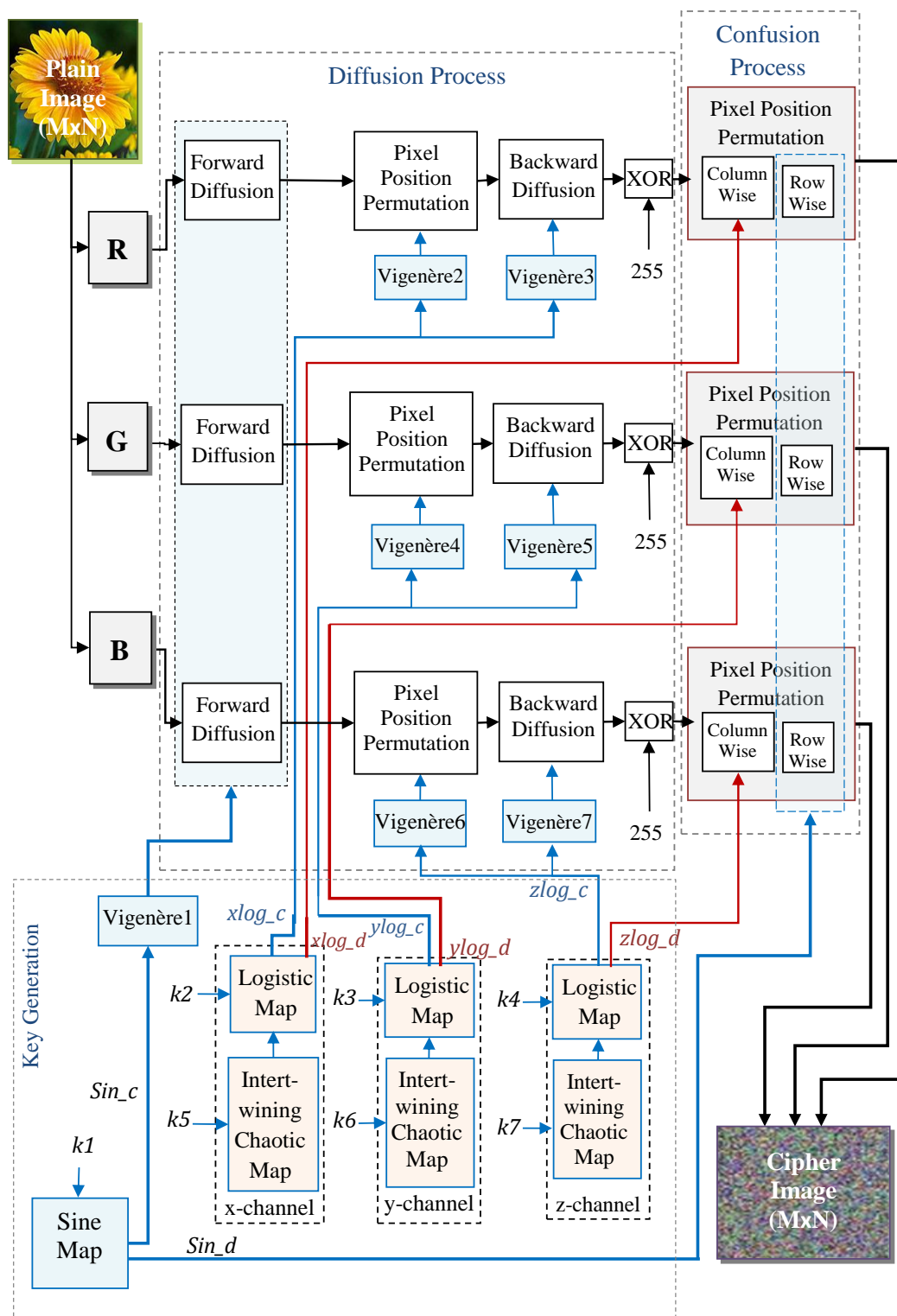


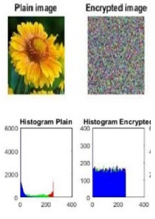
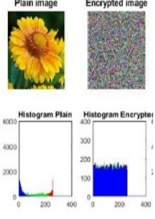
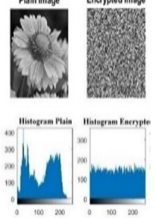
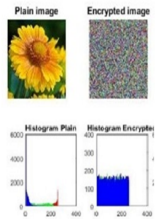
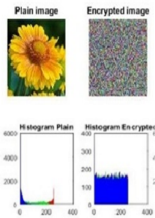
Figure 2.17: Block Diagram of Technique Based on Chaotic Maps and Vigenère Scheme

2.5.6 Comparison of Chaos Cryptography Techniques

The cryptosystem consumes very less time for execution and provides good results of parameters like PSNR and Unified Average Changing Intensity (UACI). Its perfor-

mance is better than its predecessors. Overall comparison of the Chaos-based Encryption Techniques is given in Table 2.6.

Table 2.6: Overall Comparison of Chaos Cryptography Techniques

Cryptography Techniques	Image Perceptual Quality	Key Space	CC	NPCR	UACI	PSNR	Entropy	Execution Time (Sec.)
Chaos 1		2^{216} (H)	-0.0101 (M)	0.9963 (Pass)	0.3344 (Pass)	27.7752 (M)	7.9979 (H)	34.4010 (H)
Chaos 2		2^{126} — 2^{147} (M)	** 0.0015 (VL)	0.9959 (Pass)	0.3341 (Pass)	27.7682 (M)	7.9976 (H)	5.3675 (L)
Chaos 3		2^{192} (M)	0.0059 (L)	0.9962 (Pass)	0.3344 (Pass)	27.7578 (M)	7.9979 (H)	16.8317 (M)
Chaos 4		** 2^{384} (VH)	0.0018 (VL)	0.9965 (Pass)	0.3347 (Pass)	28.0917 (M)	7.9932 (H)	14.5711 (M)
Chaos 5		* 2^{448} (VH)	0.0016 (VL)	0.9961 (Pass)	0.3348 (Pass)	27.7681 (M)	** 7.9985 (H)	0.9051 (L)

The values highlighted in green color indicates the range of satisfactory values of a particular performance parameter as explained previously. Single star(*) indicates best results and double star(**) represents the second-best results based on performance metrics. The results of Traditional cryptography and Chaos-based Cryptography Techniques are compared based on Tables 2.3 and 2.6 respectively. After comparison, it is

shown that Chaos-based Cryptography approaches perform significantly better throughout all categories. The Chaos-based Techniques provide good correlation and entropy. The results of NPCR and UACI tests are in the favorable range which shows that the techniques are highly resistant against differential attacks. Most of the performance metric values in Table 2.6 are either in green color or are star marked (*). Chaos 5 technique is best in its category and is showing satisfactory results for most of the parameters. However, there is a scope of improvement for processing time and Key Space to make the technique fast and attack resistant.

These classical chaotic cryptography systems generated with the help of Logistic Maps are sensitive to initial conditions and generates a highly random encrypted image. But further improvements in entropy, pixel sensitivity, and other parameters like execution time are identified in this survey. In the following sub sections, major Quantum Chaos-based Encryption Techniques are discussed.

2.6 QUANTUM CHAOS CRYPTOGRAPHY TECHNIQUES

In the Quantum Cryptography techniques, Quantum Chaos [31] Based Logistic Maps are used to generate a wide range of random key values to encrypt images. The Quantum Logistic Maps [136] has the tendency to enhance the randomness and processing speed with a large key-space which results in highly pixel scrambled image. These

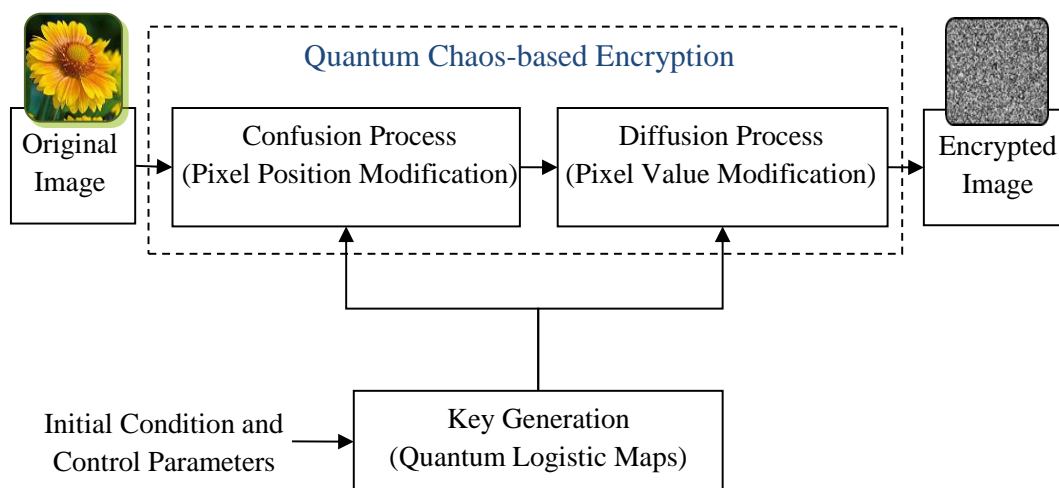


Figure 2.18: Chaos Based Image Encryption Technique

maps are the enhanced form of Logistic Maps which are formed by applying concept of Quantum Mechanics such as Heisenberg Uncertainty Principle on the Chaotic Maps. It is evident in many recent researches that the use of this technique generates a

Hyper-chaotic Cryptography System. The block diagram of encryption process based on Quantum Chaos Technique is shown in Figure 2.18.

2.6.1 Quantum Chaos 1: An Image Encryption Scheme Based on Quantum Logistic Map

Akhshani et al. [70] proposed an image encryption technique based on a Quantum Chaos Logistic Map in 2012. The complete encryption algorithm is shown in Figure 2.19. Initially, the Plain Image $P(M \times N)$ is transformed into a 1-D array $I((M \times N) \times 1)$ in which each entry is filled up by combining four pixel values of the Plain Image. The Quantum Logistic Map [136] is used to iterate one thousand times with the help of Initial Conditions and Control Parameters to remove transient effects. Then the Initial Condition values of x , y , and z are updated after 1001th iteration. Now, the same process of iteration is carried out once again by keeping the updated initial condition values as the input. A modified sequence is generated by applying function E on array I and Chaotic Sequence (x and y) as defined in Eq. (2.1a) and (2.1b). The function E is defined in Eq. (2.1c). The three equations are defined as follows:

$$C(i) = E[x(i), I(i)] \quad (2.1a)$$

$$C(i) = E[y(i), I(i)] \quad (2.1b)$$

$$E[a, b] = \text{floor}((a \times 2^{32}) \bmod 2^{32}) \oplus b \quad (2.1c)$$

Where,

x and y are the Chaotic Sequences.

I is 1-D array of Plain Image.

a and b are the arbitrary variables for function E .

\oplus represents Exclusive-OR Operation.

In every iteration, the value of Control Parameter will be modified with the use of simple mathematical operations on $C(i)$ and $z(i)$. In this way the complete image (I) is transformed into a Cipher Image. K is the iteration control variable, set to be true till all the above defined steps are completed. For decryption, the same process is carried out but in reverse direction.

2.6.2 Quantum Chaos 2: A New Approach to Chaotic Image Encryption Based on Quantum Chaotic System, Exploiting Color Spaces

In 2013, Abd El-Latif et al. [69] introduced an image encryption technique that enhanced the robustness of the test image by exploiting color spaces. In this technique, the pixel values, positions, and color planes are modified. It consists of four steps

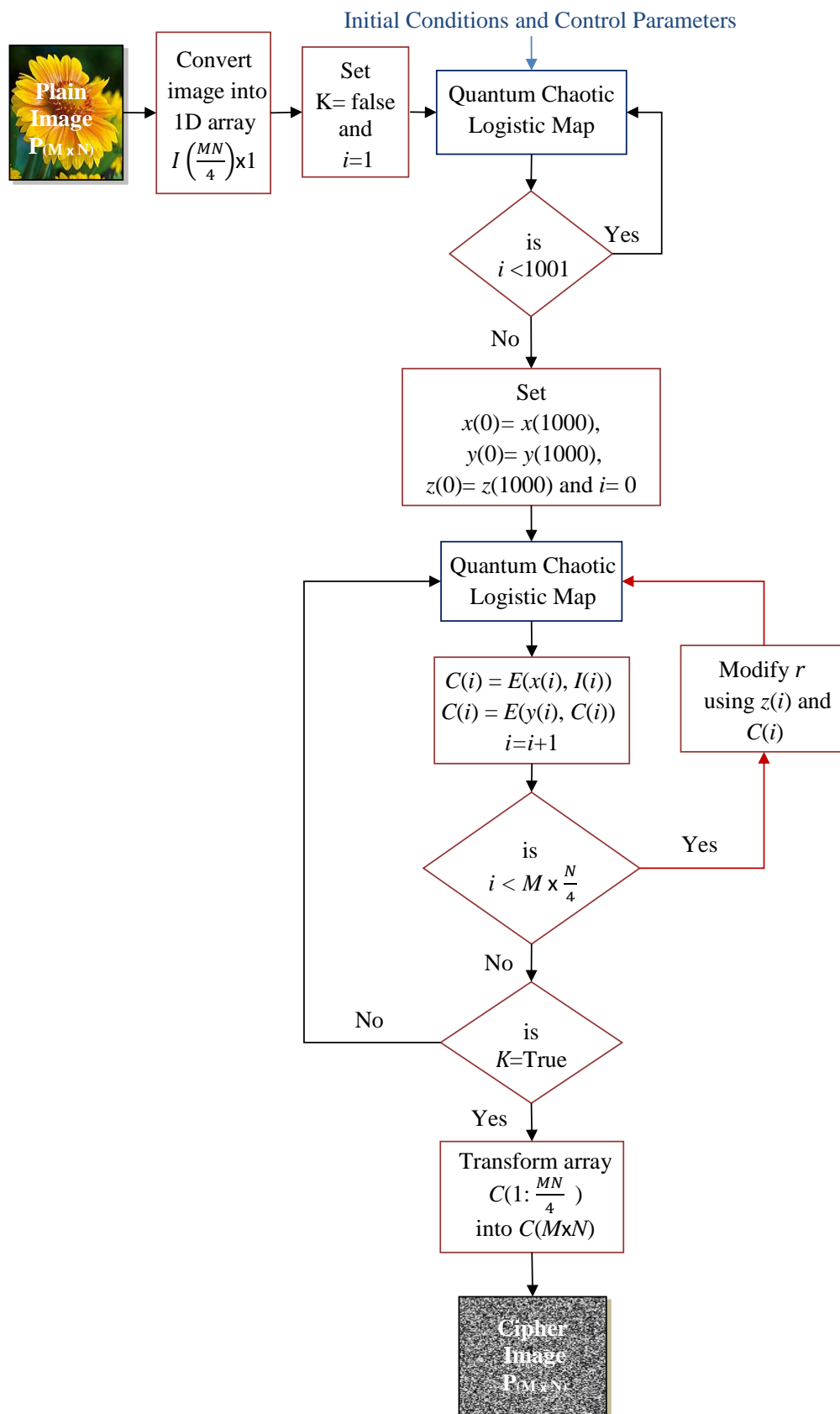


Figure 2.19: Block Diagram of Image Encryption Technique Based on Quantum Logistic Map

i.e. Key Generation, Scrambling the Luminance (Y component of image [137]), Diffusion, and Confusion as shown in Figure 2.20. The Adaptive Quantum Chaotic Logistic

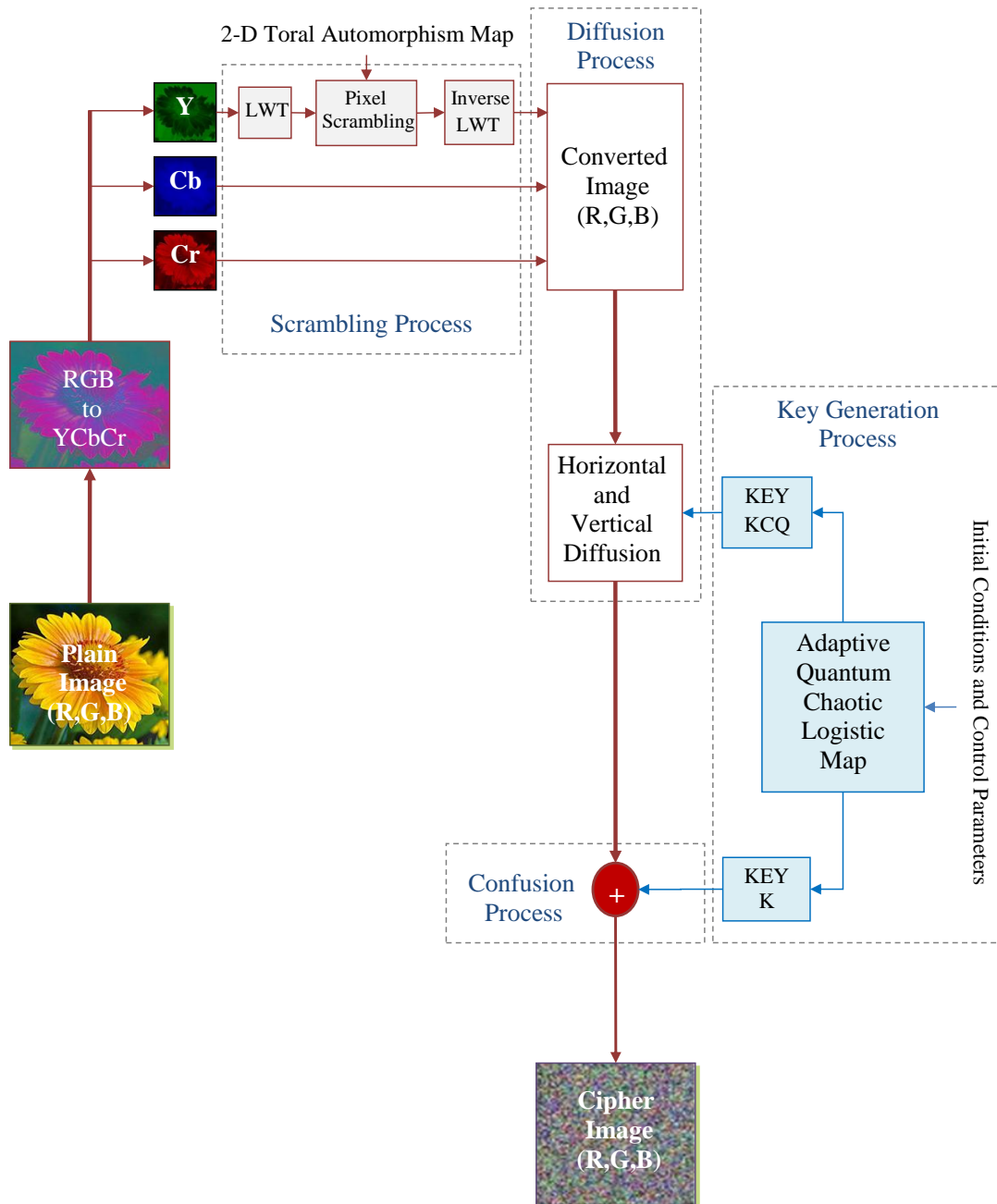


Figure 2.20: Block Diagram of Technique Based on Quantum Chaotic System, Exploiting Color Spaces

Map [121] is used to generate chaotic keys for Diffusion and Confusion Processes, applied on pixels of a Plain Image. The number of iterations equal to the size of the Plain Image are performed to provide a wide range of complexity in the Key Space. Firstly, the color image is transformed into YCbCr color model. The Y component of the image contains maximum frequencies of information. Therefore, only the Y component

is processed with Linear Wavelet Transform(LWT) and the pixel positions are scrambled with the help of 2-D Toral Automorphism Map [138]. To recover the image in the same format, Inverse Linear Wavelet Transform (ILWT) [139] is applied and get transformed into a RGB color model. The color image is diffused in horizontal and vertical directions according to the key sequence KCQ. In the final step, the diffused image is XORed with the second quantum key K. This step is classified as a Confusion Process.

The same process is carried out in a reverse manner to retrieve the original image from the encrypted image at the receiver side. This technique is resistant against brute force search attack due to its large key size. This performs better than Chaos-based Encryption Techniques in terms of randomness. However, the correlation coefficient and processing speed need improvement. The next scheme works upon these limitations.

2.6.3 Quantum Chaos 3: A Novel Color Image Encryption Algorithm Based on Quantum Chaos Sequence

In 2017 H. Liu and C. Jin [71] proposed a color image Quantum Chaos-based Encryption Technique. The technique utilizes a Quantum Logistic Map for the generation of initial conditions, control parameters and an Arnold Map for pixel scrambling. The cryptosystem consists of three major steps: generation of initial conditions & control parameters, permutation, and diffusion, as shown in Figure 2.21.

- i. **Generation of Initial Conditions and Control Parameters:** The process is completed in five steps as defined in Table 2.7. A Control Parameter t_i is generated in each step with the help of pre-defined sixteen secret keys, K_1 to K_{16} . The Two-Dimensional Logistic Map and a Quantum Chaotic Map are coupled together to generate Pseudo-random numbers in the range $[0,1]$. This type of coupling is called Nearest-Neighboring Coupled Map Lattice [140].

Table 2.7: List of Variables for Generation of Initial Conditions and Control Parameters

Steps	Control Parameter (t_i) used in Iteration Process	Initial Conditions and Control Parameters
1	t_1, t_2, t_3, t_4	$\mu_1, \mu_2, \delta_1, \delta_2$
2	t_5, t_6, t_7	a_1, a_2, a_3 and b_1, b_2, b_3
3	t_8, t_9, t_{10}	Ku_1, Ku_2, Ku_3
4	t_{11}, t_{12}, t_{13}	Kv_1, Kv_2, Kv_3
5	t_{14}, t_{15}, t_{16}	x'_0, y'_0, z'_0

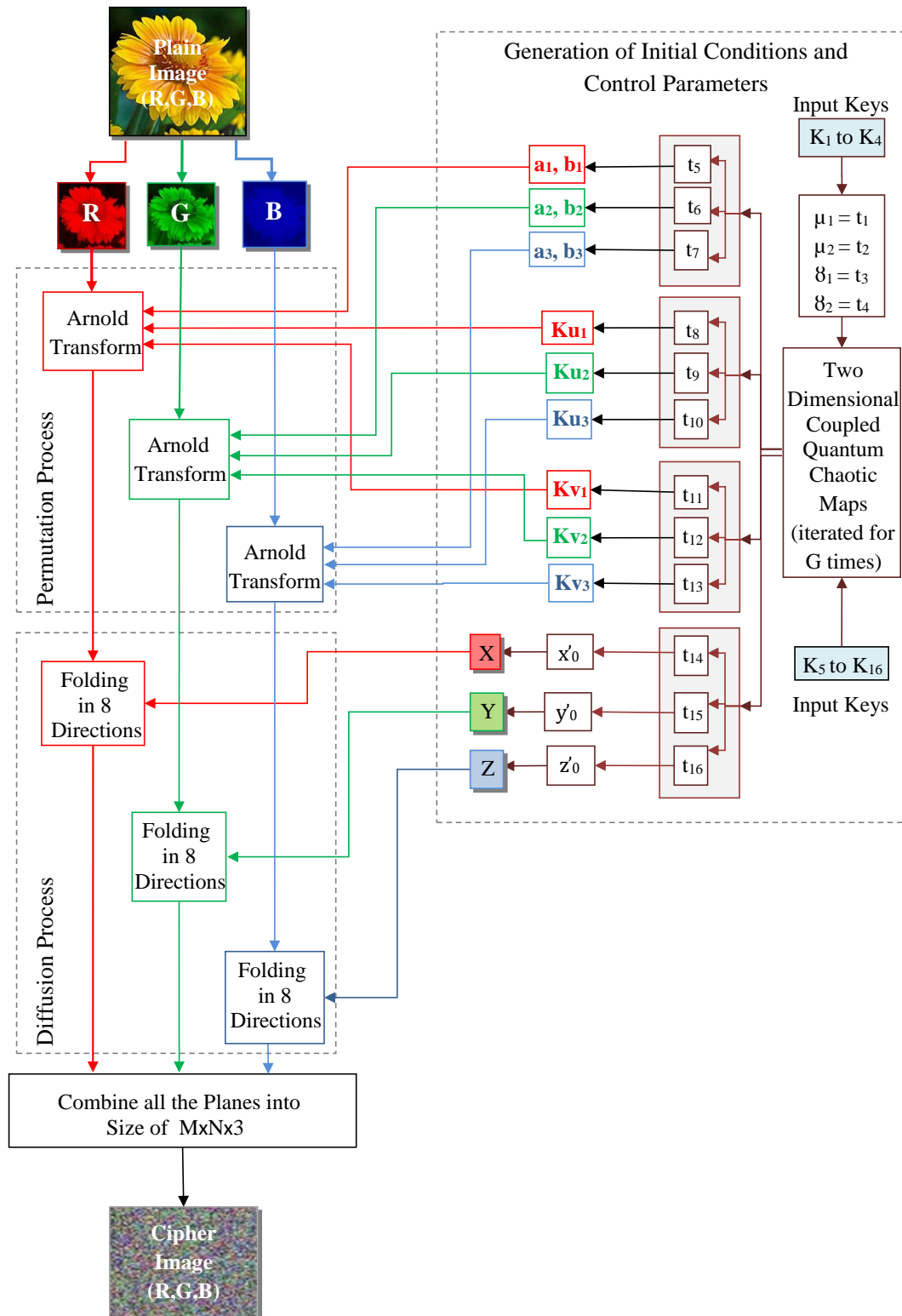
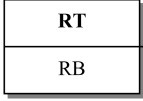
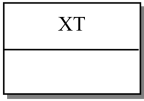

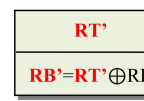
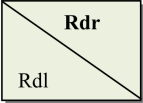
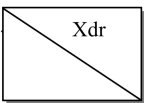
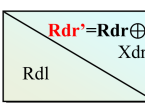
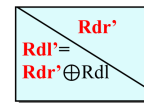
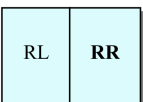
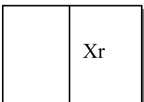
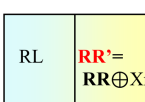
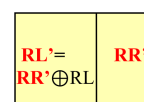
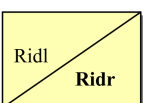
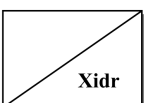

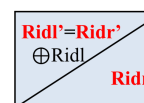
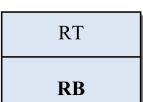
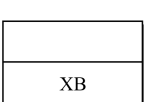
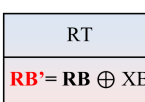

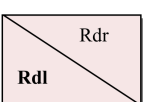
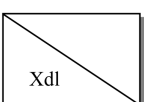
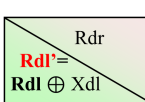
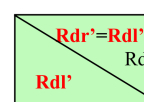
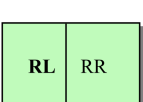
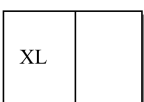
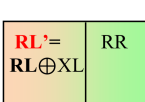







Figure 2.21: Block Diagram of Color Image Encryption Algorithm Based on Quantum Chaos Sequence

Table 2.8: Diffusion Process of R Plane with Eight Direction Folding

Round	Folding Directions	Key Matrix X	Diffusion of Portion 1	Diffusion of Portion 2
1 (Top to Bottom)				
2 (Diagonal Right Top to Left Bottom)				
3 (Right to Left)				
4 (Reverse Diagonal Right Bottom to Left)				
5 (Bottom to Top)				
6 (Diagonal Left Bottom to Right top)				
7 (Left to Right)				
8 (Reverse Diagonal Left Top to Right Bottom)				

- ii. **Permutation Process:** The pixel scrambling is done with the help of general Arnold Transform as described by Eq. (2.2):

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A^n \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} Ku \\ Kv \end{bmatrix} \pmod{256} \quad (2.2)$$

Where,

n is the no. of iterations for matrix A (for best results, n must be set to 6 [71]).

$$\text{Transform Matrix } A = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix}$$

The Arnold Map [71] is a form of chaotic system which produce a sequence of dynamic range of mixed values based on its four input key values i.e. for Red Plane of image a_1, b_1, Ku_1 and Kv_1 . Similarly for Green and Blue Plane corresponding key values a_2, b_2, Ku_2, Kv_2 and a_3, b_3, Ku_3, Kv_3 respectively are used. These key values are also generated with the help of Two Dimensional Coupled Quantum Chaotic Maps. Hence the permuted image is super scrambled due to the use of different chaotic map (Arnold Map) and Quantum Chaotic Maps at multi-levels.

- iii. **Diffusion Process:** In this process, folding of the permuted matrix is applied in eight directions on each plane. The matrix R is divided into two portions as RT (Top of R plane) and RB (Bottom of R plane). The XOR operation is done on RT & RB with the corresponding portion of random matrix X and the remaining part is XORed with the modified portion. Similarly, folding of planes is also done in diagonally right top to left bottom, vertically right to left, reverse diagonally right bottom to left, horizontally bottom to top, diagonally left bottom to right top, vertically left to right and reverse diagonally left top to right bottom direction. The complete rounds of diffusion steps for the R plane are presented in Table 2.8 and the algorithm for the Diffusion Process is also provided. The algorithm for folding process of R plane is defined below:

Algorithm for Folding Process in Eight Directions of R Plane

Round 1 (Top to Bottom Folding)

$$RT' = RT \oplus XT$$

$$RB' = RT' \oplus RB$$

Round 2 (Diagonal Right Top to left Bottom Folding)

$$Rdr' = Rdr \oplus Xdr$$

$$Rdl' = Rdr' \oplus Rdl$$

Round 3 (Right to Left Folding)

$$RR' = RR \oplus Xr$$

$$RL' = RR' \oplus RL$$

Round 4 (Reverse Diagonal Right Bottom to Left Folding)

$$Ridr' = Ridr \oplus Xidr$$

$$Ridl' = Ridr' \oplus Ridl$$

Round 5 (Bottom to Top Folding)

$$RB' = RB \oplus XB$$

$$RT' = RB' \oplus RT$$

Round 6 (Diagonal Left Bottom to Right top Folding)

$$Rdl' = Rdl \oplus Xdl$$

$$Rdr' = Rdl' \oplus Rdr$$

Round 7 (Left to Right Folding)

$$RL' = RL \oplus XL$$

$$RR' = RL' \oplus RR$$

Round 8(Reverse Diagonal Left Top to Right Bottom Folding)

$$Ridl' = Ridl \oplus Xidl$$

$$Ridr' = Ridl' \oplus Ridr$$

The R_f is the folded image obtained in above algorithm. The diffused plane R_d is obtained from R_f by applying XOR operation with random matrix X as follows:

$$R_d = R_f \oplus X$$

The same procedure is applied on G and B planes with random matrix Y and Z respectively, as described below:

$$G_d = G_f \oplus Y$$

$$B_d = B_f \oplus Z$$

The Cipher Image is formed by combining the three modified planes after following the processes of pixel permutation and image diffusion. For decryption, the same procedure is followed but in a reverse direction. This technique performs much better than its predecessors and its overall performance metrics lie in the satisfactory range. However, the key space parameter needs improvement. In the next technique, this parameter is improved.

2.6.4 Quantum Chaos 4: Bit Level Quantum Color Image Encryption Scheme with Quantum Cross-Exchange Operation and Hyper Chaotic System

In 2018, Nanrun Zhou et al. [72] proposed a bit-level quantum color image encryption technique based on a High-definition Hyper-chaotic System. Due to the exis-

tence of quantum color image scrambling using Bit Cross-exchange method and Hyper-chaotic Map, this system becomes highly random and complex. A 5-D Hyper Chaotic Map [141] is used for the generation of key sequences along with a Quantum Cross Exchange of twenty-four qubits. The channel transmission is also performed in between the color planes. The block diagram of the entire process is shown in Figure 2.22. A bit

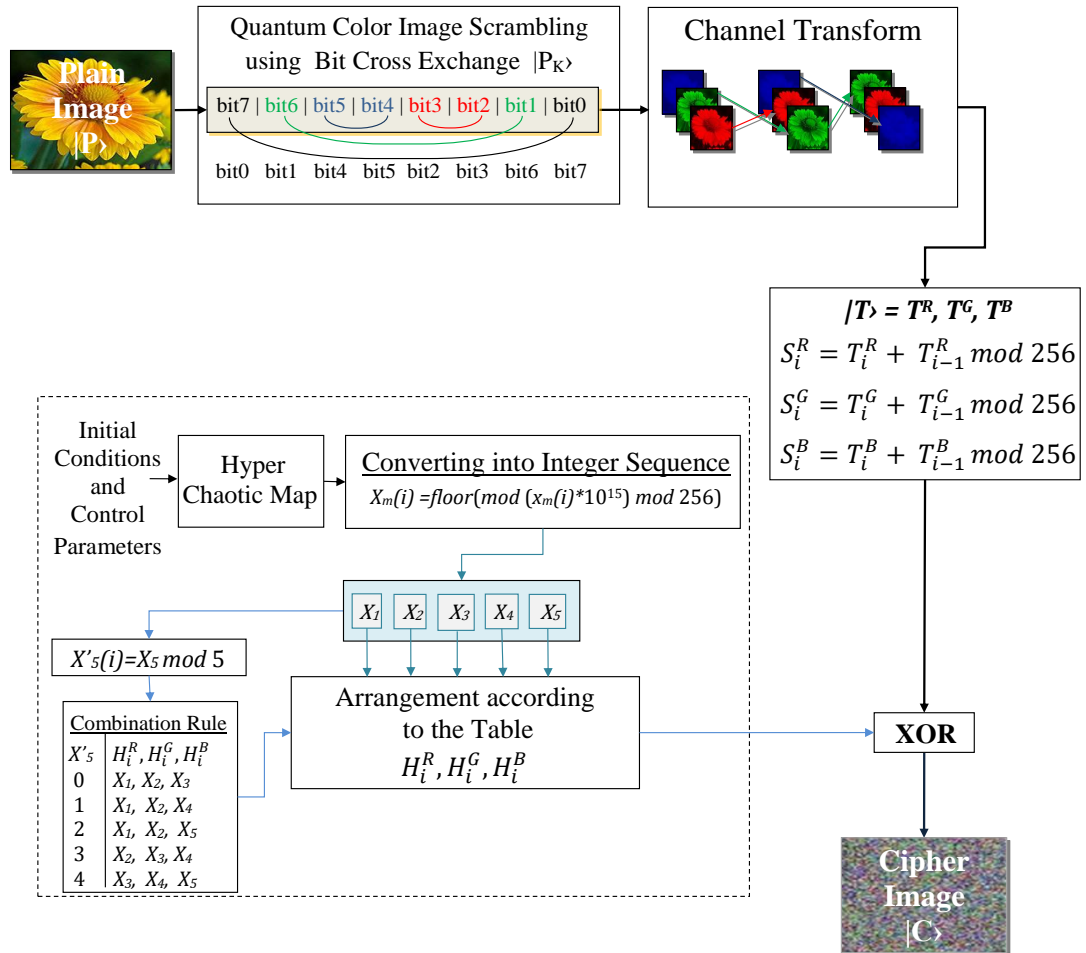


Figure 2.22: Block Diagram of Technique Based on Quantum Cross Exchange Operation and Hyper Chaotic System

planes of the color image, $|P\rangle$ of size $(2^n \times 2^n \times 3)$ is considered for encryption. A new quantum multi-channel representation in the Eq. (2.3) given below for the digital image is described below:

$$|P\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} C_{yx}^{RGB} \otimes |yx\rangle \quad (2.3)$$

Where,

C_{yx}^{RGB} = RGB color image having information of pixel value

$|yx\rangle$ = Information of pixel position

\otimes = Tensor product

After qubit representation of the color image, the bit position scrambling is done with the concept of quantum cross-exchange as given in Table 2.9.

Table 2.9: Quantum Bit Cross-Exchange

Original Bit Position	7	6	5	4	3	2	1	0
Cross Exchanged Bit Position	0	1	4	5	2	3	6	7

The same process of bit cross exchange is also performed for G and B planes. All three encrypted planes are combined to form the crypto image as $|P_K\rangle = |P_R\rangle |P_G\rangle |P_B\rangle$. Next, the quantum color image channel transformation is done in two steps i.e between R and G planes followed by the transformation between G and B planes. With the use of 5D hyper chaotic map, five sets of chaotic sequences X_1 to X_5 are obtained and transformed into integer values in the range $[0, 255]$. Now, to convert these sequences from 1-D array to 3D matrix (size of the original image), a combination rule is applied with the help of the values of X_5 as described in Table 2.10.

Table 2.10: Combination Rule of 5D Hyper-Chaotic Sequence

X'_5	H_i^R, H_i^G, H_i^B
0	X_1, X_2, X_3
1	X_1, X_2, X_4
2	X_1, X_2, X_5
3	X_2, X_3, X_4
4	X_3, X_4, X_5

From this Table, three sets of variables H_i^R, H_i^G, H_i^B is obtained and it is taken as a security key to encrypt the scrambled image.

For decryption, the same procedure is followed but in a reverse direction. This technique performs better than predecessors and gives good key space and correlation value making it highly resistant to brute force and differential attacks.

2.6.5 Quantum Chaos 5: Quantum Image Encryption using Intra and Inter Bit Permuted Based on Logistic Map

In 2019, Xingbin Liu et al. [73] proposed a new encryption technique based on Intra and Inter Bit Permutation on the Qubit Lattice represented color image. In this scheme, a Novel Quantum Image Representation (NEQR) model is designed, which defines the Quantum States. The block diagram of complete encryption process is shown in Figure

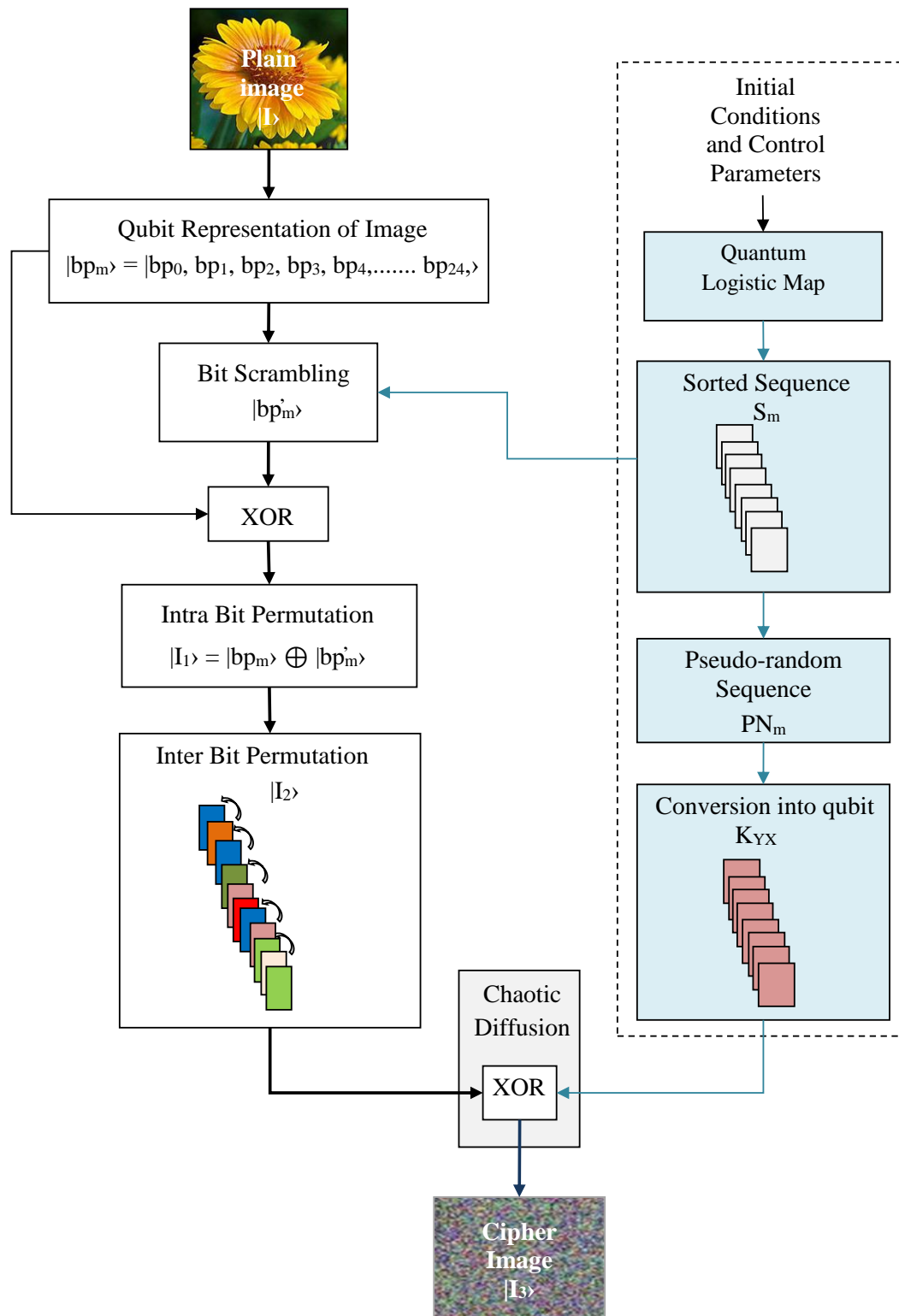


Figure 2.23: Block Diagram of Technique Using Intra and Inter Bit Permutation Based on Logistic Map

2.23. The original image's bit positions are permuted within a pixel as well as pixel positions according to the Chaotic Sequence S_m which is generated with the help of

Quantum Logistic Maps. The computations occur on quantum represented twenty-four qubit planes of the Plain Image. Each plane of the image consists of eight-bit planes for each pixel value. Hence each qubit plane is represented as a bit image which consists only pixel values 0 and 1. The total no. of qubit required in this step is $q+2n$ where $n \times n$ is the size of square image. A Quantum Logistic Map is also used which enhances the randomness during Inter and Intra Bit Permutation and Diffusion Process.

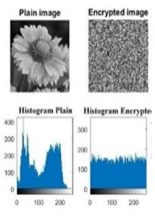
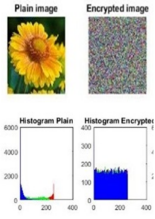
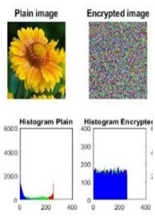
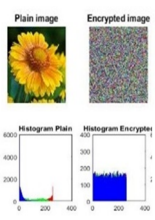
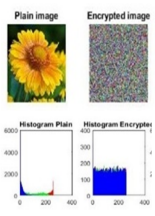
- i. **Intra Bit Permutation:** The image is converted in q qubits binary planes followed by scrambling of bit's positions within a pixel. The scrambling is done with the help of the sequence generated by the Quantum Logistic Map. From this step, out of eight sequences of x_m , the first N_0 values [73] are discarded to reduce the transient effects where N_0 is equal to 10,000. The sequence is arranged in ascending order and the control operation is applied to exchange the bits of original image with respect to corresponding values of S_m . Resulted image $|I_1\rangle$ is obtained.
- ii. **Inter Bit Permutation:** In this step, the bit position is scrambled within its plane only and the XOR operation is applied between inter bit planes according to a pre-defined Operating Sequence set $OS = [0, 2, 4, 6, \dots, q-3, q-1]$. The operator is applied on the intra bit permuted image $|I_1\rangle$ to generate a scrambled image $|I_2\rangle$.
- iii. **Chaotic Diffusion:** This procedure will modify the pixel values of the permuted image. A pseudo-random sequence $P = P_0, P_1, P_2, \dots, P_{2^{2n}-1}$ is generated with the help of quantum logistic map upto $N_0 + 2^{2n}$ times, the first N_0 values are discarded to reduce the transient effects and rest of the 2^{2n} sequences are used as a key for diffusion of pixel values. The Pseudo-random sequence PN is combined to form a qubit matrix of the same size of permuted image and is termed as $|K_{yx}^i\rangle$. The final step involves the XOR operation between $|K_{yx}^i\rangle$ and $|I_2\rangle$.

For decryption, the same procedure is followed but exactly in a reverse order. This is the most complex technique so far, yet it takes very less time for execution and also performs better than its predecessors in terms of all parameters except differential attack analysis.

2.6.6 Comparison of Quantum Chaos Cryptography Techniques

Table 2.11 shows the comparison of results of various Quantum Chaos Cryptography Techniques based on performance metrics. From this analysis, it is observed that these techniques provide optimized results of every performance parameter and ensures good confidentiality. The highlighted values represents the strengths of the corresponding techniques and there is a space for improvement in Correlation Coefficient, Entropy and Execution Time.

Table 2.11: Overall Comparison of Quantum Chaos Cryptography Techniques

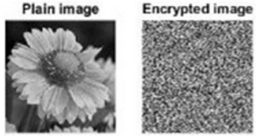


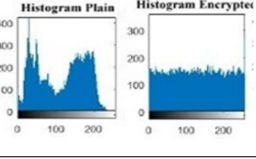
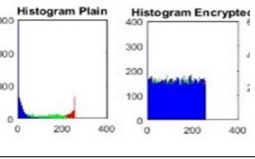
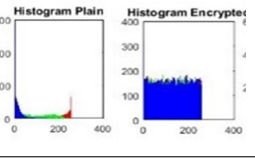
Cryptography Techniques	Image Perceptual Quality	Key Space	CC	NPCR	UACI	PSNR	Entropy	Execution Time (Sec.)
Quantum Chaos 1		2^{224} (H)	0.0462 (M)	0.9961 (Pass)	0.3347 (Pass)	* 23.3799 (L)	7.9285 (H)	10.8278 (M)
Quantum Chaos 2		2^{256} (H)	0.0526 (M)	0.9966 (Pass)	0.3358 (Pass)	** 23.0740 (L)	6.7838 (L)	7.2033 (L)
Quantum Chaos 3		2^{128} (M)	* -0.0005 (VL)	0.9962 (Pass)	0.3361 (Pass)	22.9881 (L)	* 7.9988 (H)	3.4671 (L)
Quantum Chaos 4		2^{240} (M)	-0.0021 (L)	0.5199 (Fail)	0.3352 (Pass)	28.1015 (M)	7.9962 (H)	0.2163 (L)
Quantum Chaos 5		> 2^{100} (M)	0.0018 (VL)	0.5039 (Fail)	0.2515 (Fail)	28.1133 (M)	7.9963 (H)	5.8873 (L)

2.7 OVERALL COMPARISON

The aim of this literature survey was to study various existing cryptography techniques and also to compile the results based on various Performance Metrics available for Cryptanalysis. In this part, ten Traditional, five Chaos, and five Quantum Chaos based encryption techniques are examined. The overall summarized comparison of cryptography techniques are given in Table 2.12 with all the technical details by taking average

of the calculated values of each Performance Metrics.

Table 2.12: Overall Comparisons of Cryptography Techniques

Techniques/ Performance Metrics	Traditional Techniques	Chaos Based Techniques	Quantum Chaos Based Techniques
Image Perceptual Quality (Snapshots)	Pixel Scrambling: Low 	Pixel Scrambling: High 	Pixel Scrambling: High 
Statistical Attack Parameters (Histogram and Correlation Coefficient(CC))	Histogram: Spiked 	Histogram: Uniform 	Histogram: Uniform 
	CC=0.045083 (Moderate)	CC= 0.000132 (Very Low)	CC= 0.001962 (Very Low)
Differential Attack Parameters (NPCR and UACI)	NPCR=0.803032 (Fail)	NPCR= 0.996191 (Pass)	NPCR= 0.992553 (Pass)
	UACI=0.257099 (Fail)	UACI=0.334497 (Pass)	UACI=0.338647 (Pass)
Quantitative Parameters (PSNR and Entropy)	PSNR=28.01196 (High)	PSNR=27.83220 (Low)	PSNR= 25.131360 (Very Low)
	Entropy=7.96181 (High)	Entropy=7.997032 (High)	Entropy=7.740721 (High)
Key Space	2^{132} (Moderate)	2^{277} (High)	$> 2^{200}$ (High)
Execution Time (sec.)	24.993250 (High)	14.415270 (Moderate)	5.520353 (Very Low)

It is clearly evident that most of the techniques are satisfying (highlights with green color) the confidentiality norms other than traditional techniques. Even though, still there is a scope for improvement in the performance. In the next chapter, a Chaos-based Encryption Technique is proposed to achieve the objectives.

CHAPTER 3

A NOVEL IMAGE ENCRYPTION TECHNIQUE BASED ON INTERTWINING CHAOTIC MAPS AND RC4 STREAM CIPHER

3.1 INTRODUCTION

Transmission of digital images (personal and professional) over public data networks has become a necessity in the existing era. The current infrastructure allows us to transmit a huge amount of data due to technological advancements and towering bandwidth support. The data flowing through these channels can be accessed by unauthorized users like ransomware. The annual number of ransomware records (see Figure 3.1) shows that these attacks have grown exponentially from 2004 till 2016 with a projected total 182.76 million attacks for the year 2017 and increased up to 44.3% in 2018 [142]. Due to the enormous growth of these attacks during the last few years, researcher keeps on devising new algorithms with the aim of achieving high data confidentiality. Initially, most of the techniques focused on encrypting small chunks of data via symmetric [48,53,125,143] and asymmetric key algorithms. But, as the network becomes more commercialized and the user base grew up, these traditional encryption techniques become more open to attacks from unauthorized users [84, 129]. These techniques are better suited for textual data and are ineffective for encrypting images [31, 105, 106] since the image has high redundancy and correlation among adjacent pixels.

To overcome this, researchers developed Chaos-based Encryption Algorithms which provide good randomness, low computational time along with good key space. Though, these techniques were good but can further be improved. The first proposal is aimed to

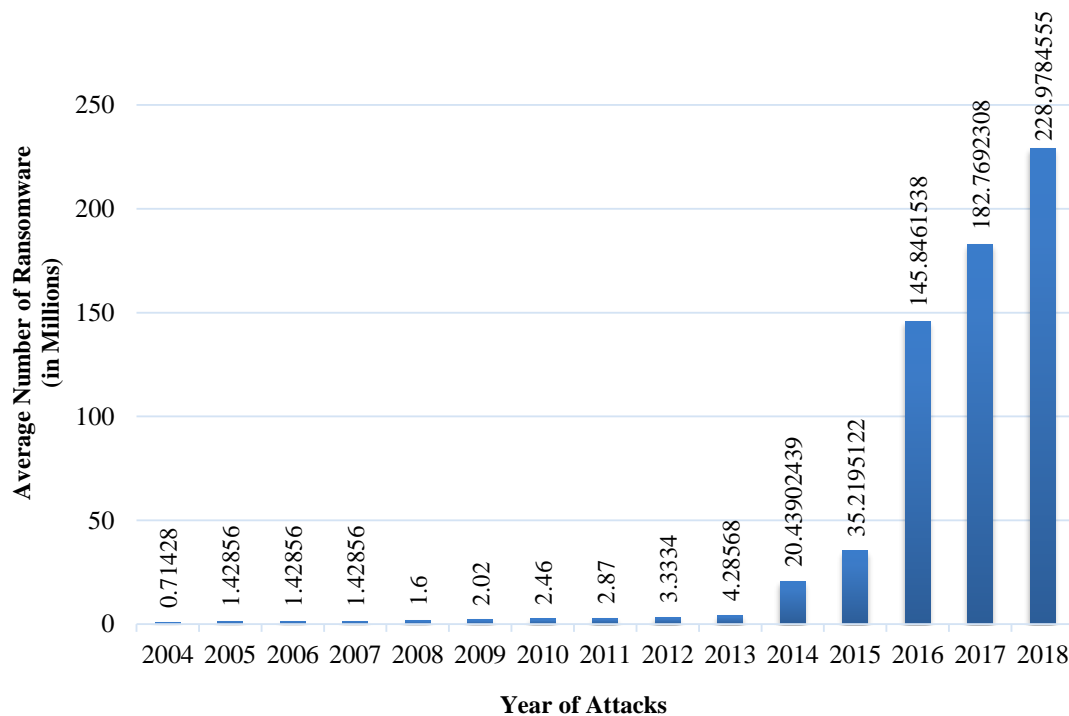


Figure 3.1: Annual Number of Ransomware Families Attacks

provide the following salient features:

- Confidentiality is achieved by visual interpretation of the encrypted image. The resultant image is highly scrambled which ensures that no information about the original image can be extracted from the Cipher Image.
- The security is enhanced by lengthening the key space which makes it resistive against the brute force attack.
- The randomness is increased with the use of highly random intertwining chaotic maps during Confusion and Diffusion Processes which provide a very low correlation value.
- The scheme or technique is highly resistant against the differential attacks because of row-wise and column-wise Forward and Backward Diffusion along with RC4. The technique is resistant to attacks since the value of NPCR and UACI are closed to ideal values. Hence, even a small change in the value will provide a drastic change in the encrypted or decrypted images.
- The time of execution is comparable to the other techniques. Therefore, this technique is also suitable for real time communication.

The next section gives the proposed encryption mechanism.

3.2 PROPOSED ENCRYPTION TECHNIQUE

The proposed technique follows an architecture popular in many of the Chaos-based Cryptography techniques but the novelty is the use of RC4 (one of the Traditional Technique) and Intertwining Chaotic Map (based on Chaos Technique). It contains the following steps:

- (a) Confusion: In this step, the pixel positions are permuted with the aim to confuse the individuals. The intensities of the pixel values do not change but their positions are randomized.
- (b) Diffusion: This step is commonly used to modify the pixel values. The modification can be as simple as XORing that can provide high randomized encrypted images.

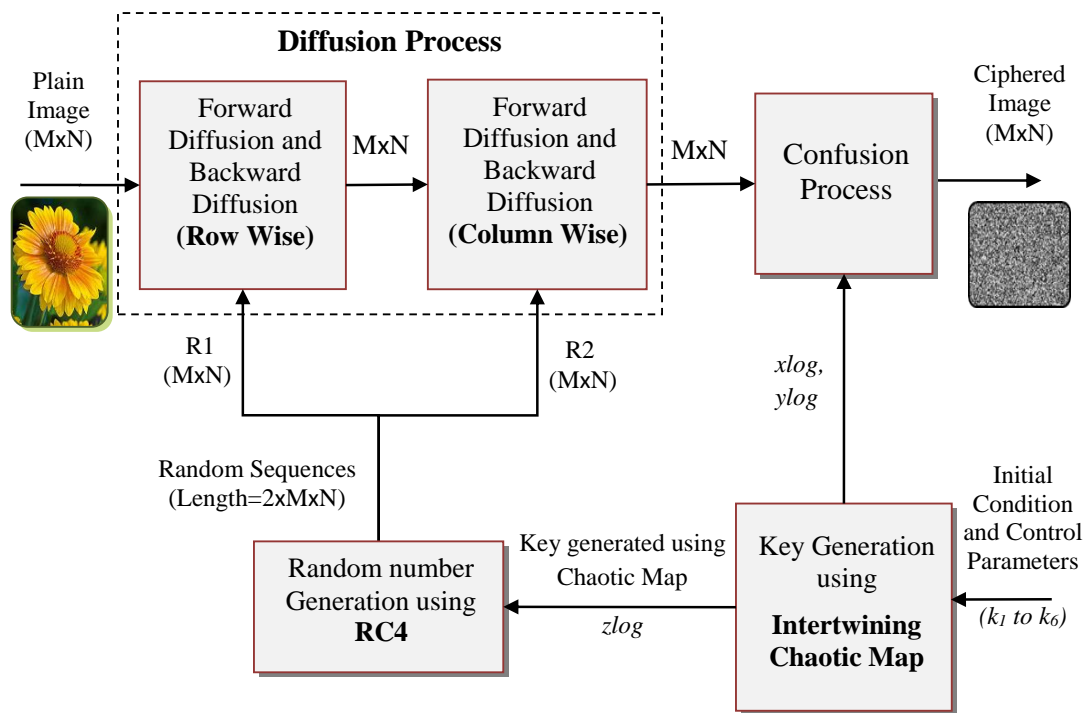


Figure 3.2: Block Diagram of Encryption Process of Proposed Technique

Both the Confusion and Diffusion Processes require key values and random sequences for encrypting images. We have four blocks in our proposed technique as shown below:

- Key Generation using Intertwining Chaotic Map
- Random Sequence Generation using RC4 Stream Cipher
- Confusion Process
- Diffusion Process

Figure 3.2 shows the block diagram of the Encryption Process. As shown, the Keys Generated using the Intertwining Chaotic Maps are used for the Confusion Process and as the input for RC4. The RC4 block uses these keys as input and generates random sequences which are used in the Diffusion Process. The diffusion is done in Row-wise, Column-wise, Forward, and Backward directions. The detailed explanation of all steps of the algorithm is given in the following subsections.

3.2.1 Key Generation using Intertwining Chaotic Map

Chaotic Maps [113] are the mathematical functions which provide a dynamic nature to the system. Logistic maps, also known as Log Maps, are used by researchers to obtain dynamic encryption algorithms. The Logistic Maps provides high randomness, unpredictability and has simple mathematical representation as shown in Eq. (3.1):

$$xlog_{n+1} = \mu \times xlog_n (1 - xlog_n) \quad (3.1)$$

Where;

$xlog$ is the Variable for generated Chaotic Number.

n represents the Number of Sequences (varies from 1 to Length of Key).

$xlog$ at $n=0$ is the Initial Value and $xlog_0 \in (0, 1)$.

μ is Positive Constant and $\mu \in [0, 4]$.

The equation is dependent on the initial conditions and hence provides security greater than the Non-chaotic Techniques (Traditional Techniques). Even after these advantages, the Logistic Maps have an uneven distribution of sequences, stable windows, and a weak key [50], hence is not a practical choice for modern encryption. Modified Logistic Maps, like Intertwining Chaotic Maps, are aimed to make the technique more practical by removing the above-mentioned weakness. Mathematically, Intertwining Logistic Maps [64] are given in Eq. (3.2a), (3.2b) and (3.2c).

$$xlog_{n+1} = \mu \times k_4 \times ylog_n \times (1 - xlog_n) + zlog_n \quad (3.2a)$$

$$ylog_{n+1} = (\mu \times k_5 \times ylog_n) + \left(zlog_n \times \frac{1}{1 + (xlog_n + 1)^2} \right) \quad (3.2b)$$

$$zlog_{n+1} = \mu \times (xlog_n + ylog_n + k_6) \times \sin(zlog_n) \quad (3.2c)$$

Where;

$xlog$, $ylog$ and $zlog$ are the Variables for generated chaotic numbers.

n represents the Number of Sequences (varies from 1 to Length of Key).

$xlog_0$, $ylog_0$ and $zlog_0$ at $n=0$ are the Initial Values and assigned as k_1 , k_2 and k_3 .

μ is the Positive Constant and $\mu \in [0, 4]$.

k_4 , k_5 and k_6 are the Control Parameters. $|k_4| > 33.5$, $|k_5| > 37.9$, $|k_6| > 35.7$

Figure 3.3 shows the key generation scheme. The keys k_1 to k_6 are the defined as input values required for chaotic key generation. k_1, k_2 , and k_3 keys act as initial conditions corresponding to initial values of $xlog_n, ylog_n$, and $zlog_n$ (at $n=0$). These keys were used in three paths, namely X path, Y path, and Z path, to create three different Intertwining Chaotic Maps, namely $xlog, ylog$, and $zlog$. Each path of the chaotic maps used two keys as input parameters and generate sequences which are further used for the next step i.e., Confusion Process and simultaneously given to the RC4 code generator [50] to produce a different chaotic key for the Diffusion Process. All these sequences are 1-dimensional vectors.

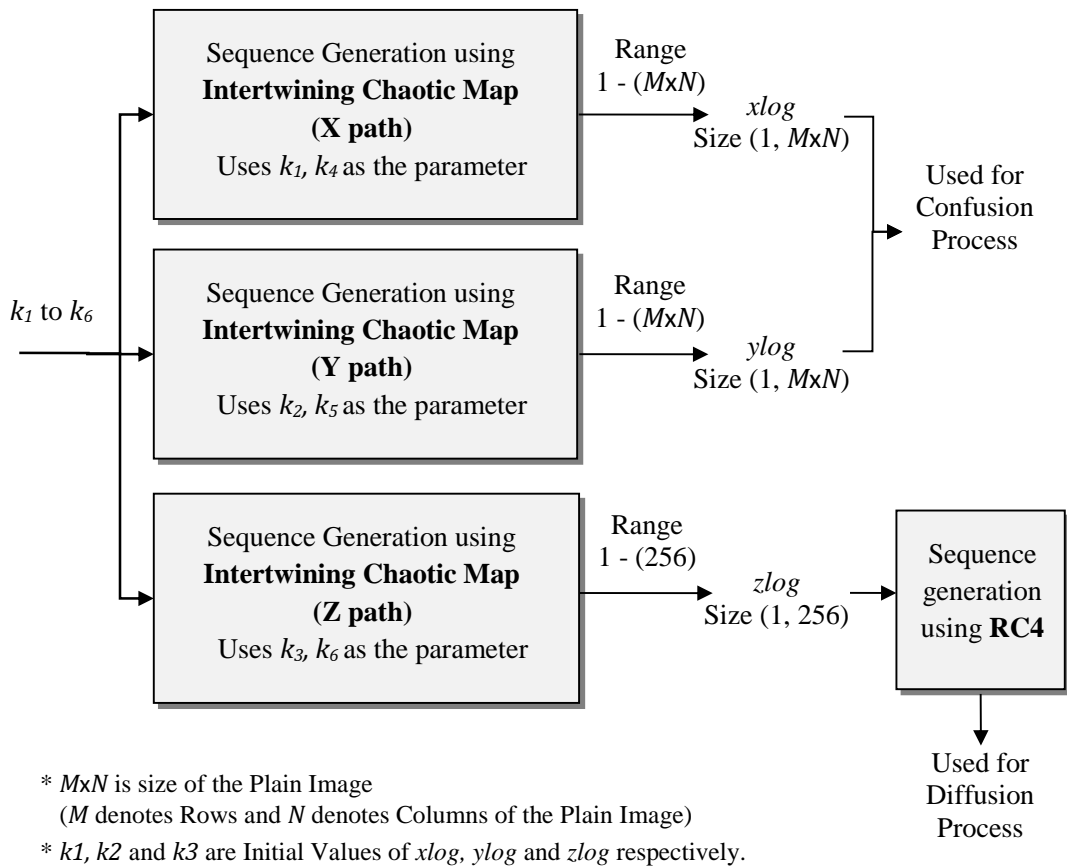


Figure 3.3: Key Generation Using Intertwining Chaotic Map

The sequences generated from the X path and the Y path combined were used for the Confusion stage. The element values in both sequences range from 1 to $M \times N$. Each of the maps has a total $M \times N$ element in it, hence making a successful implementation of the Confusion Process for any image of size $M \times N$. The sequence generated from the Z path was used as the input for RC4 random sequence generation. As the key length required for the RC4 algorithm ranges from 1 to 256 bytes and does not depend on the size of the image, so the sequence generated from the Z path has 256 elements in it, with values ranging from 1 to 256.

3.2.2 Random Sequence Generation using RC4 Stream Cipher

The RC4 [16] is a symmetric key, stream cipher and is known for its speed and simplicity. It was initially developed in 1987 as a trade secret but in 1994 was leaked to public. During the encryption process, the cipher is fed with a key whose length can vary from 1 to 256 bytes. This cipher generates a randomized array which is obtained by feeding the key to a Pseudorandom Byte Generator. The output of the Pseudorandom Generator is known as the Random Sequence. These sequences generated in the proposed algorithm had a length of $2 \times M \times N$ and were fed as the inputs to the Diffusion Process. The decryption process follows a similar step as that of encryption process but in reverse order.

There are numerous variants of the RC4 cipher. These variants provide a better resistance against attacks on RC4 and are modified as per specific application. The current study uses RC4 in which a 256-byte key is passed directly to Pseudorandom Generator which is provided by the Intertwining Chaotic Maps hence eliminating the need of Key Scheduling step. Algorithm for RC4 used is given below:

Algorithm for Pseudorandom Generation (RC4)

```

Function [R1,R2]= RC4Pseudono(zlog,L)                                % L=size of image(M×N)
for
    S(i) = i;
end
j = 0
for i = 1 : 256
    j = ((j + S(i) + zlog(i))mod256);
    if j = 0
        swap S(i) and S(j);
    else
        j = ((j + S(i) + zlog(i))mod256);
        swap S(i) and S(j);
    end
end
i = 0; j = 0;
do;
    i = (i + 1)mod256;
    j = (j + S(i))mod256;
    Swap S(i) and S(j)
    pseudo= S[(S(i) + S(j))mod256];
while(2 × L - 1);
R1 = pseudo(1 : L)
R2 = pseudo((L + 1) : 2 × L)

```

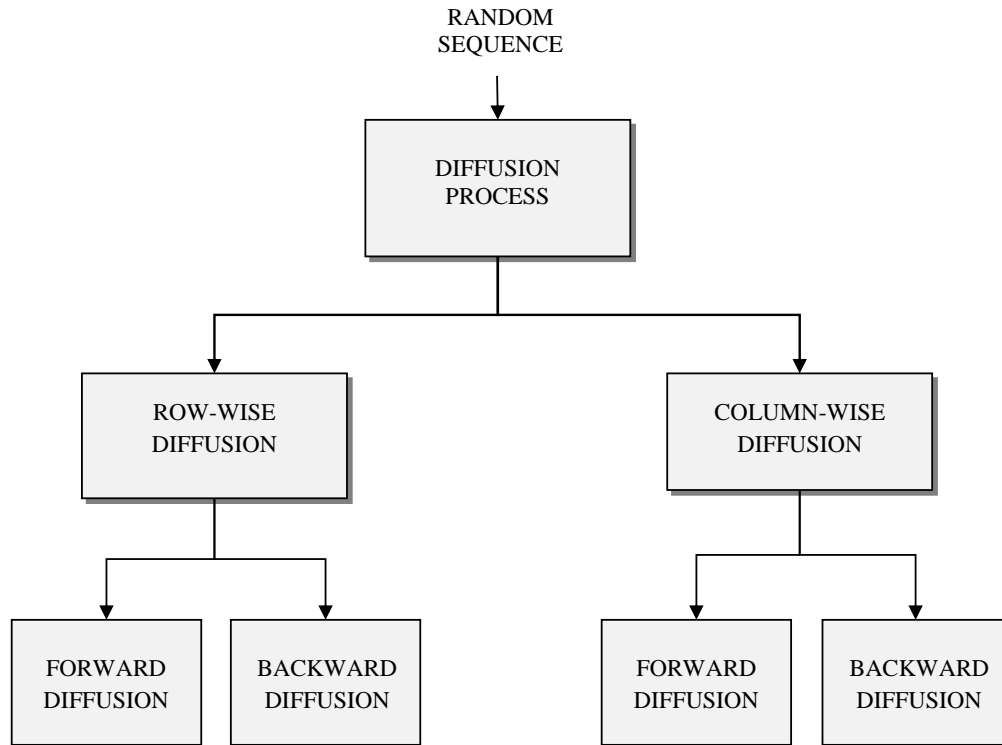



Figure 3.4: Hierarchy of Diffusion Process

3.2.3 Diffusion Process

Diffusion [61] is one of the two important stages of the proposed algorithm and it adds randomness in the pixels of the Plain Image. The diffusion property [29] is responsible for spreading the effect of change in a pixel intensity value throughout the entire image. So, any change in the intensity of one pixel value will change the encrypted image drastically and both the images formed will have no or very low resemblance with each other. As shown in Figure 3.4, the Diffusion step can be branched into row-wise and column-wise diffusion and both diffusion steps are done in forward and backward directions. In row-wise diffusion, the image is scanned row-wise in alternate directions. This scanning is used to turn the $M \times N$ image into an array form before the actual diffusion steps are used. Then the generated array is diffused in forward followed by backward direction. Once the row-wise diffusion is done, the image is turned back into the $M \times N$ form and then it is scanned column-wise to form another similar array followed by similar forward and backward diffusion steps. The algorithms for Diffusion Processes are given below:

Algorithm for Forward Diffusion (Row Wise and Column Wise)

% Input parameters : P=input Row-wise or Column-wise Scanned Array

Function $[E] = \text{forward_diffusion}(P, E2, E1, R1, R2)$

for $i = 1 : 1 : M \times N$

```

if (i - 1 == 0 && i - 2 == -1)
    E2 = 2;
    E1 = 1;
elseif (i - 2 == 0)
    E2 = 1;
    E1 = 0;
else
    E2 = 0;
    E1 = 0;
end
j = P(i) + E2;
a = mod(j, 256);
b = a + E1;
c = mod(b, 256);
d = bitxor(c, R1);           % R1=RC4 Generated Sequence(1 to 256)
e = d + R2;                 % R2=RC4 Generated Sequence(256 to 512)
E(i) = mod(e, 256);        % Obtained Forward Diffusion
end

```

Algorithm for Backward Diffusion (Row Wise and Column Wise)

% Input parameters: E= Output Array of Diffusion Process

Function $[F]$ =backward_diffusion(E, F2, F1, R1, R2)

```

for i = (M × N) : -1 : 1
    if (i + 1 == (M × N) + 1 && i + 2 == (M × N) + 2)           % M = rows of image
        F2 = 2;                                               % N= columns of image
        F1 = 1;
    elseif (i + 2 == (M × N) + 1)
        F2 = 1;
        F1 = 0;
    else
        F2 = 0;
        F1 = 0;
    end
    j = E(i) + F2;
    m = mod(j, 256);
    n = m + F1;
    o = mod(n, 256);
    p = bitxor(o, R1);
    q = p + R2;
    F(i) = mod(q, 256);           % Obtained array from Backward Diffusion
end

```

Finally, the image is again converted back into the $M \times N$ form and passed to the Confusion block.

3.2.4 Confusion Process

This process is the next stage which adds randomness in the pixels of the Plain Image. The confusion [61] used in the proposed algorithm is a permutation of pixel positions of the diffused image. The stage shuffles the position of the pixels present in the image while making no change in the respective pixel intensity values. This stage ensures that no unauthorized user will be able to fetch the plain textual data because the pixels of the image are shuffled in random positions from their original location. Apart from randomness, the permutation of pixel orientation also helps in achieving lower values of correlation coefficients which means that the correlation present in the adjacent pixels in the original image is removed.

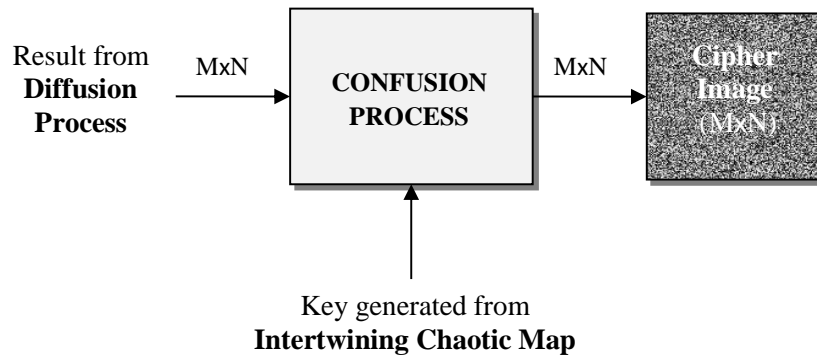


Figure 3.5: Confusion Process of Proposed Technique

Figure 3.5 shows the Confusion Process of the proposed scheme, and its algorithm is given below:

Algorithm for Confusion Process

```

Function [I_out] = confusion(diffused_image,xlog,ylog)
for i = 1 : 1 : M                                % M= No. of Rows of Image
    for j = 1 : 1 : N                              % N = No. of Columns of Image
        temp = diffused_image(i, j);
        I_out(xlog(i),ylog(j)) = temp;
    end
end
  
```

3.3 DECRYPTION

Decryption Process follows steps like the Encryption Process. Here, the encrypted image is taken as input and the steps used by the encryption process are used in reverse order.

3.4 ALGORITHM EXPLANATION

The algorithm was executed in three separate channels. The three channels are denoted here as R, G and B which are used for the red, green, and blue planes of the image. Both, the encryption, and decryption algorithms are executed for all three channels separately keeping the same keys and other Set-up variables. The three channels were merged again before providing the encrypted or decrypted images. The steps used for key generation, encryption, and decryption processes are given below:

Steps for Complete Encryption Process

Step 1: Divide the image into red, green, and blue channels.

➤ **Key generation**

Step 2: Generate $xlog_n$, $ylog_n$, and $zlog_n$ using intertwining chaotic maps by using the respective keys as defined above.

➤ **Encryption Algorithm**

Step 3: For Red channel, generate a random sequence of length $2 \times M \times N$ by using $zlog$, following the process define above in the respective section.

Step 4: Scan the image row-wise to generate a 1-dimensional array and apply Forward Diffusion followed by Backward Diffusion.

Step 5: Convert the array back to $M \times N$ form.

Step 6: Repeat steps 4 and 5 for column-wise diffusion.

Step 7: Apply the Confusion Process.

Step 8: Repeat steps 3 to 7 for green and blue channel.

Step 9: Recombine the three channels together to get the Encrypted Image

➤ **Decryption Algorithm**

Step 1: Divide the encrypted image into the channels.

Step 2: For Red channel, apply the reverse confusion step.

Step 3: Apply the RC4 decryption stage.

Step 4: Scan the image column-wise to perform reverse diffusion, first in backward then in forward directions for the generated array and turn the array back into image.

Step 5: Repeat step 4 for row-wise diffusion.

Step 6: Repeat steps 2 to 5 for green and blue channels.

Step 7: Recombine the three channels to get the Decrypted Image.

3.5 SIMULATION SETUP PARAMETERS

The proposed algorithm, along with the other algorithms used in the study, were implemented on a Personal Computer. Table 3.1 provides the specification of the machine and technical information, test plain-images and initial and modified parameters used for the algorithms in this research work.

Table 3.1: Machine and Image Specifications, Initial and Modified Parameters











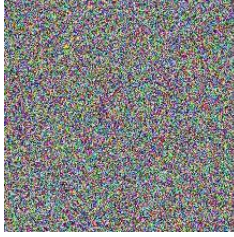





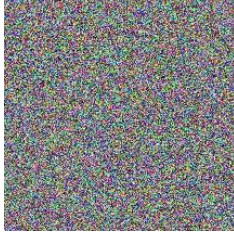

Machine	Specifications of Machine
Processor	1.4GHZ Dual-Core Intel Core I5
Memory	4GB Of 1600 MHz Lpddr3
Simulation Platform	MATLAB Version 2015
Type of data	Specifications of data
Type	Color Images
Size Of Images	256 × 256, 512 × 512
Images Source	USC-SIPI Image Database [79]
Keys Used In	Original values of initial conditions and control parameters as Keys
Proposed Technique [$\mu, k_1, k_2, k_3, k_4, k_5, k_6, pix$]	[3.999, 20.1, 22, 19, 33.5, 37.9, 35.7, 0.1]
Keys used for Key Security and Differential Attack Analysis	Modified values of initial conditions and control parameters as Keys
Proposed Technique [$\mu, k_1, k_2, k_3, k_4, k_5, k_6, pix$]	[3.9991, 20.1, 22, 19, 33.5, 37.9, 35.7, 0.1]

Some of the test images are selected from USC-SIPI Image Database [79] on which the proposed encryption technique is implemented. All the test images are provided in Table 3.2.

Table 3.2: Set of Images for Testing

256 × 256  4.1.01 (Girl)	256 × 256  4.1.02 (Couple)	256 × 256  4.1.05 (House)	256 × 256  4.1.06 (Tree)	256 × 256  4.1.07 (Jellybeans)
512 × 512  4.2.03 (Mandrill)	512 × 512  4.2.04 (Lena)	512 × 512  4.2.05 (Airplane)	512 × 512  4.2.06 (Sailboat)	512 × 512  4.2.07 (Peppers)

Table 3.3: Visual Analysis of Encrypted and Decrypted Images

Image Specifications	Original Image	Encrypted Image	Decrypted Image
4.1.01 (Girl)	256 × 256 	256 × 256 	256 × 256 
4.1.06 (tree)	256 × 256 	256 × 256 	256 × 256 
4.1.07 (Jellybeans)	256 × 256 	256 × 256 	256 × 256 
4.2.03 (Mandrill)	512 × 512 	512 × 512 	512 × 512 
4.2.06 (Sailboat)	512 × 512 	512 × 512 	512 × 512 
4.2.07 (Peppers)	512 × 512 	512 × 512 	512 × 512 

3.6 RESULTS

3.6.1 Visual Analysis

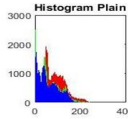
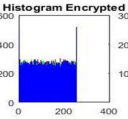
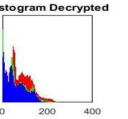
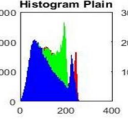
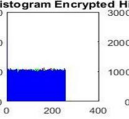
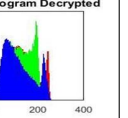
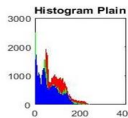
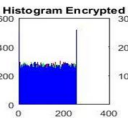
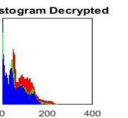
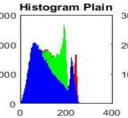
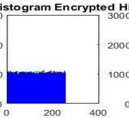
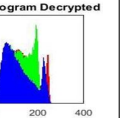
The visual assessment of the encrypted and decrypted images obtained from the proposed scheme can be done from Table 3.3. It shows the visual assessment of four test images. From the figure, it can be clearly seen that all the encrypted images obtained are highly scrambled and there is no visual resemblance between encrypted and the original images. Moreover, it can also be seen that the decrypted images are visually same as the Plain Images, hence ensuring the reliability of data obtained after decryption [49]. Additionally, a visual assessment comparison of proposed and other implemented chaotic techniques is provided in Table 3.4.

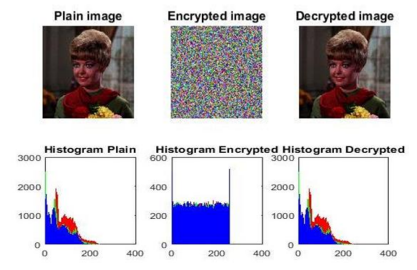
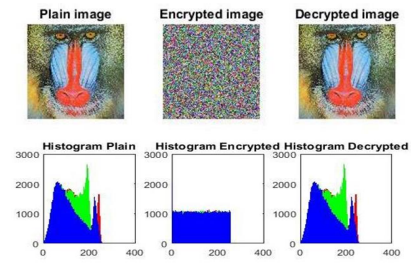
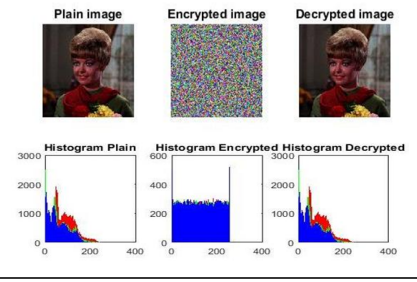
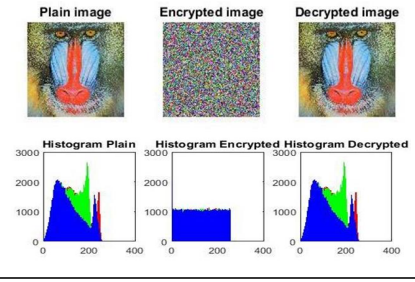
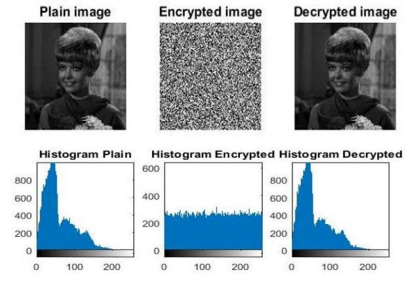
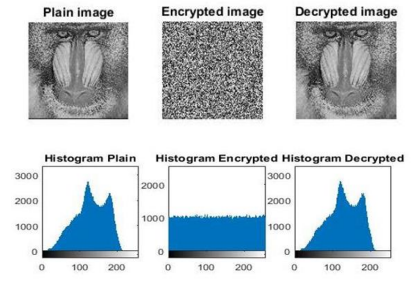
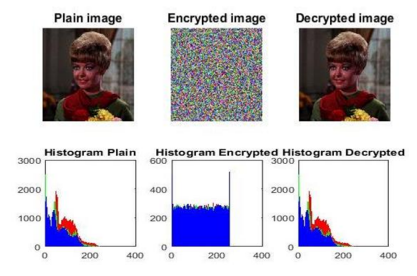
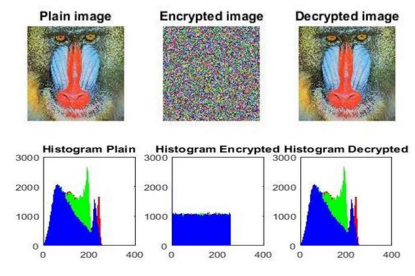
3.6.2 Statistical Attack Analysis

i. Histogram:

The histograms [26] of the original, encrypted, and decrypted images are provided in Table 3.4. From the table, it can be seen that the histograms of encrypted images obtained by the proposed technique are uniformly distributed and have no resemblance with the histograms of the respective original images. So, the proposed algorithm has a strong resistance to the statistical attacks. Moreover, the histograms of the decrypted images are like the histograms of respective original images. Hence there is no measurable data loss during the process.

Table 3.4: Visual Assessment and Histogram of Proposed and Other Techniques

Image/ Technique	4.1.01 (Girl) 256 × 256			4.2.03 (Mandrill) 512 × 512		
Proposed	Plain image	Encrypted image	Decrypted image	Plain image	Encrypted image	Decrypted image
						
Chaos 1	Plain image	Encrypted image	Decrypted image	Plain image	Encrypted image	Decrypted image
						

Image/ Technique	4.1.01 (Girl) 256 × 256	4.2.03 (Mandrill) 512 × 512
Chaos 2		
Chaos 3		
Chaos 4		
Chaos 5		

ii. **Correlation Coefficient:**

Table 3.5 shows the correlation plots of the original and the encrypted images. It shows that the plots obtained from the original images have the elements focused on a central line and doesn't contain a significant number of elements elsewhere in the plots. The plots have a highly non-uniform distribution for all the three orientations. On the other hand, the plots obtained by the encrypted images are uniformly distributed throughout the plot region. Similar characteristics are shown by the proposed. As there is no resemblance between the two correlation graphs, no information leakage is present, and the scheme can withstand the statistical attacks efficiently.

Table 3.5: Correlation Plots of Original and Encrypted Images

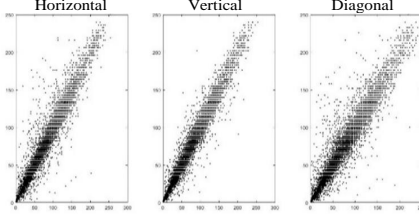
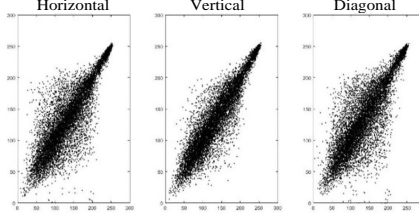
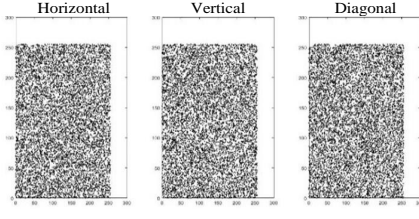
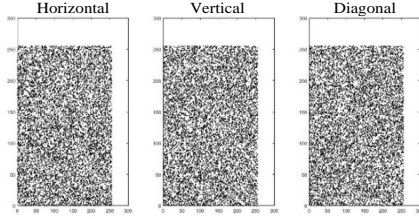
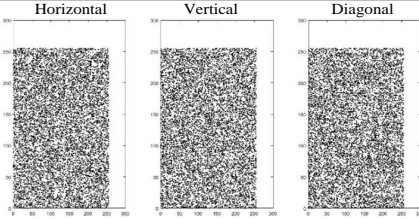
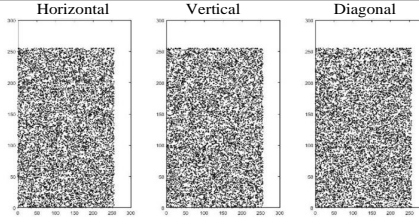
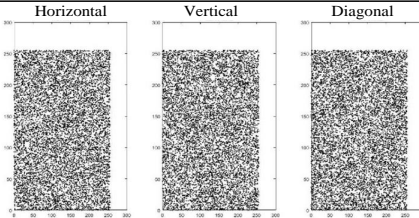
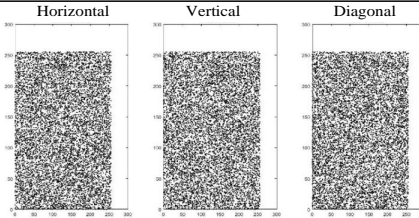
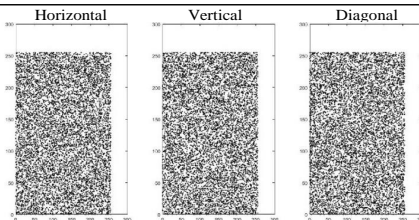
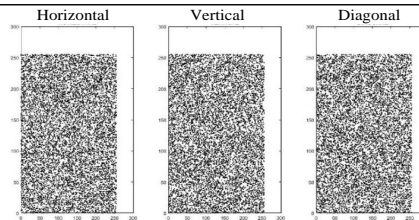
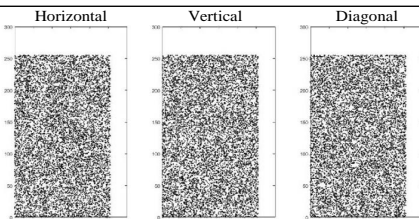
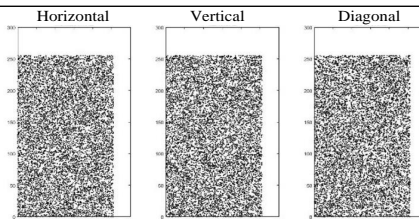
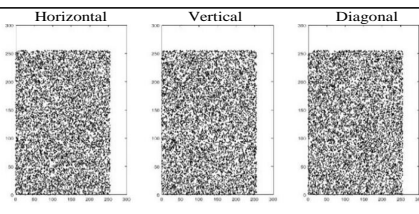
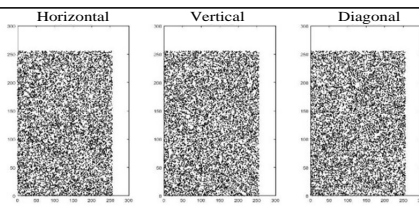
Image/ Technique	4.1.01 (Girl) 256 × 256	4.2.03 (Mandrill) 512 × 512
Original		
Proposed		
Chaos 1		
Chaos 2		
Chaos 3		
Chaos 4		
Chaos 5		

Figure 3.6 provides the horizontal, vertical, and diagonal correlation coefficients between original images and the encrypted images obtained by the proposed algorithm. The correlation coefficient's [120] values are low in all the three orientations.

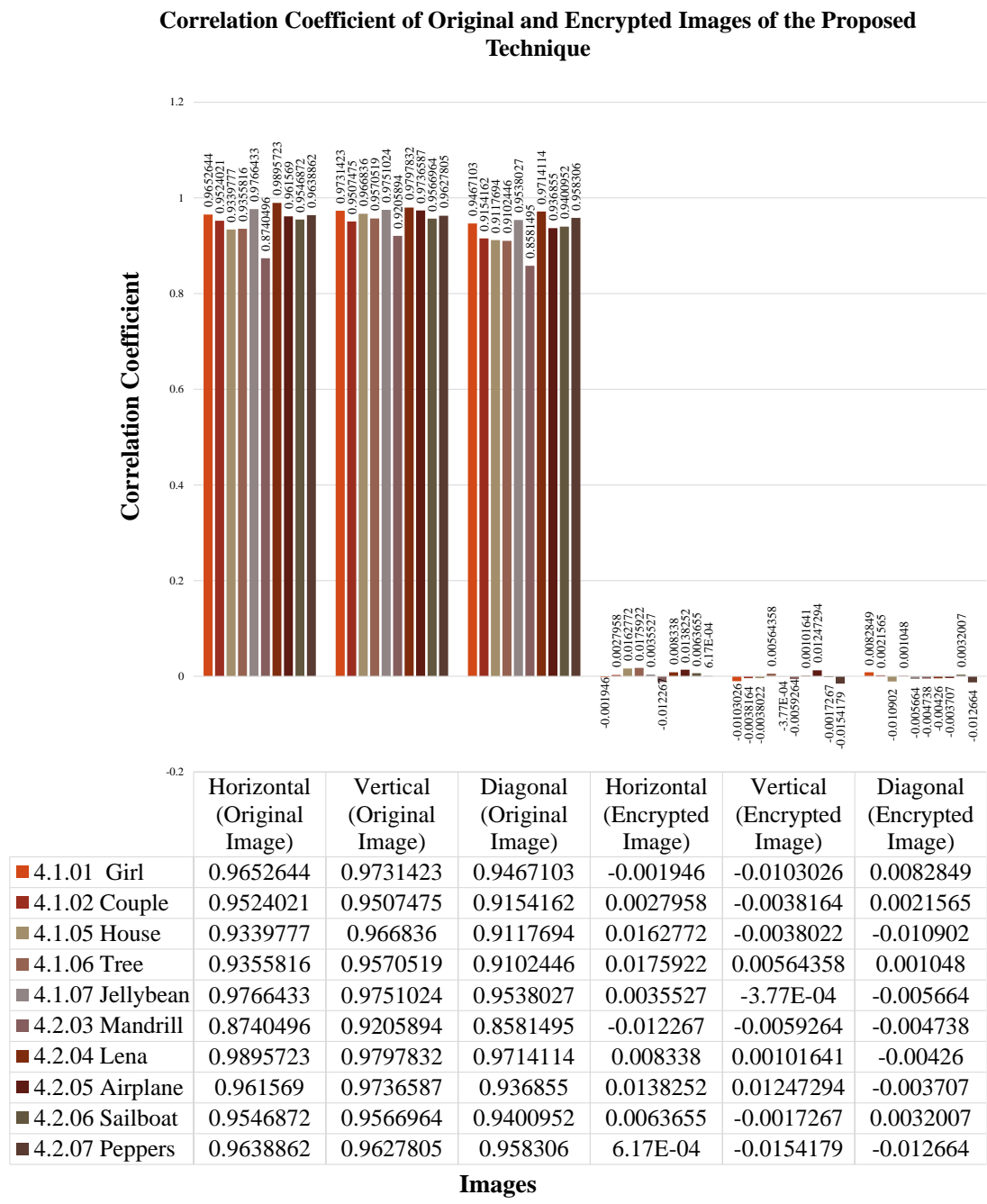


Figure 3.6: Graph of Correlation Coefficient of Original and Encrypted Images of Proposed Technique

Figure 3.7 shows a comparison of correlation coefficients of the proposed algorithm and other implemented algorithms. All the correlation coefficients obtained have very low values.

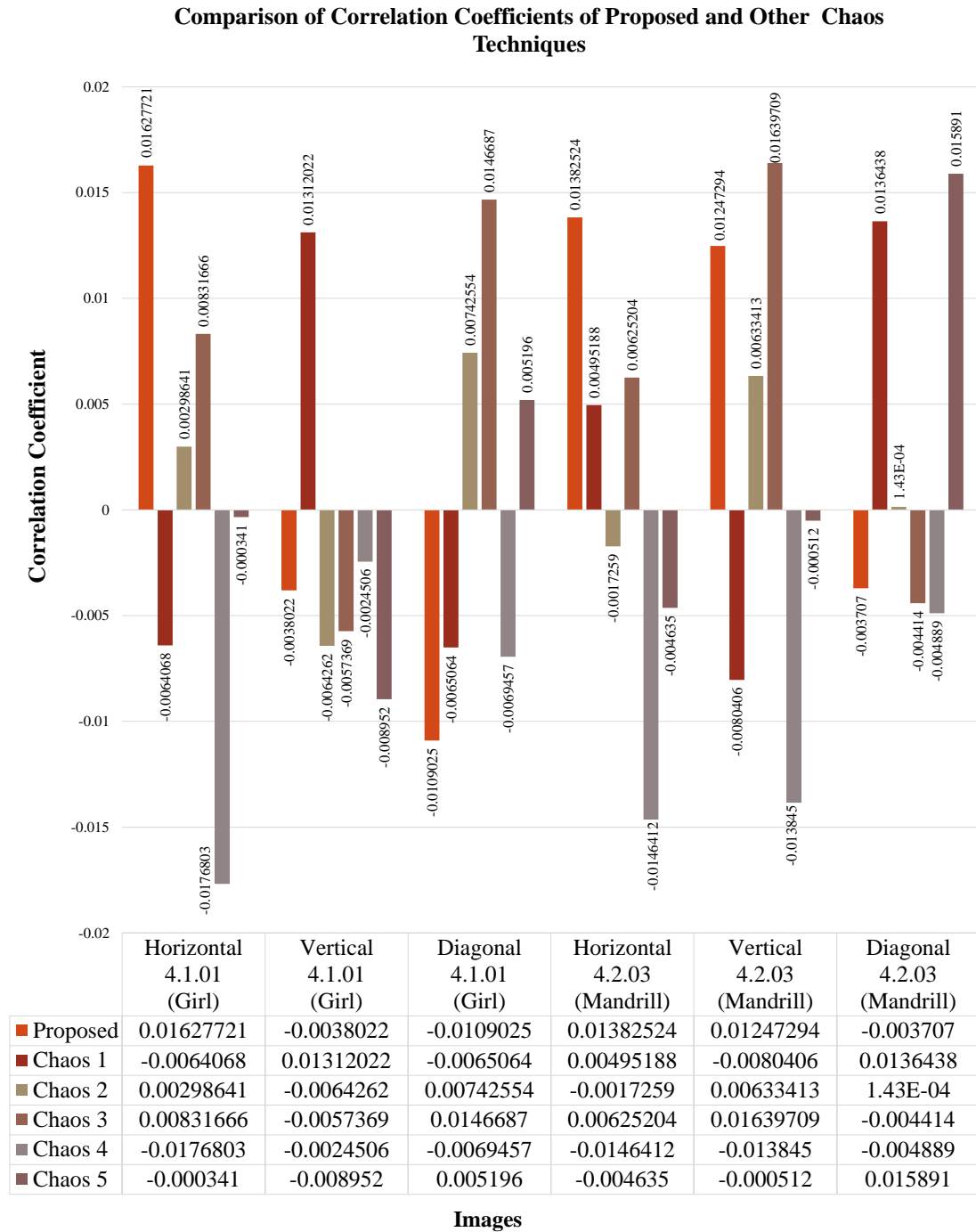


Figure 3.7: Graph of Comparison of Correlation Coefficients of the Proposed and Other Chaos Techniques

3.6.3 Differential Attack Analysis

The effect of one-bit key change is observed based on NPCR and UACI parameters. Table 3.6 shows the NPCR and UACI values obtained for the test images after implementing the proposed and other techniques. For the test images, an average value of 99.60334% is obtained for NPCR and an average value of 31.841% is obtained for

UACI. This shows a high sensitivity of the scheme for even a single bit change in the input parameter. The use of row-wise and column-wise Forward and Backward Diffusion along with RC4 plays a critical role for ensuring the same. Hence, the proposed scheme has a high resistance against the Differential Attacks.

Table 3.6: NPCR and UACI Test for One-Bit Key Change

Technique/ Image		Proposed	Chaos 1	Chaos 2	Chaos 3	Chaos 4	Chaos 5
4.1.01 (Girl)	NPCR	0.9959767	0.9960937	0.9959411	0.9959716	0.9961598	0.9958591
	UACI	0.3536231	0.3344527	0.3335475	0.3330246	0.3342175	0.3351781
4.1.02 (Couple)	NPCR	0.9961090	0.9959869	0.9957122	0.9954477	0.9960479	0.9962570
	UACI	0.3352330	0.3340253	0.3317445	0.3335103	0.3347666	0.3337401
4.1.05 (House)	NPCR	0.9958547	0.9966888	0.9960683	0.9963887	0.9960581	0.9961711
	UACI	0.2957642	0.3342516	0.3348143	0.3345291	0.3345648	0.3355133
4.1.06 (Tree)	NPCR	0.9960531	0.9962921	0.9961700	0.9961293	0.9958750	0.9961151
	UACI	0.3189548	0.3352798	0.3343183	0.3347877	0.3342043	0.3353632
4.1.07 (Jellybeans)	NPCR	0.9959157	0.9956817	0.9961344	0.9969024	0.9960327	0.9959588
	UACI	0.3052330	0.3361388	0.3342727	0.3322330	0.3345485	0.3355255
4.2.03 (Mandrill)	NPCR	0.9959424	0.9961319	0.9961344	0.9962450	0.9961179	0.9964172
	UACI	0.2992334	0.3344746	0.3346924	0.3347134	0.3348335	0.3352412
4.2.04 (Lena)	NPCR	0.9961840	0.9961471	0.9961369	0.9959513	0.9959945	0.9964614
	UACI	0.3047626	0.3357886	0.3343478	0.3333134	0.3347094	0.3350421
4.2.05 (Airplane)	NPCR	0.9960556	0.9961471	0.9961141	0.9963404	0.9961077	0.9960178
	UACI	0.3260339	0.3355736	0.3346573	0.3345290	0.3343801	0.3350141
4.2.06 (Sailboat)	NPCR	0.9960988	0.9959640	0.9959144	0.9961128	0.9959971	0.9959112
	UACI	0.3222411	0.3348957	0.3343166	0.3343759	0.3348410	0.3358877
4.2.07 (Peppers)	NPCR	0.9961446	0.9962272	0.9960098	0.9961751	0.9959983	0.9963163
	UACI	0.3230262	0.3353383	0.3343166	0.3350033	0.3347938	0.3355144

3.6.4 Key Space

Table 3.7 shows the key space produced by the proposed and other techniques used in the study.

Table 3.7: Key Space Analysis of the Proposed and Other Implemented Techniques

Technique	Key Space
Proposed	2^{384}
Chaos 1	2^{216}
Chaos 2	$2^{126} - 2^{147}$
Chaos 3	2^{192}
Chaos 4	2^{384}
Chaos 5	2^{448}

As it can be seen, the proposed technique provides a very large number of possible key solutions. So, it is impractical for an unauthorized user to retrieve the data by guessing the possible key. Hence, the proposed scheme is efficient enough to resist the brute force attacks.

3.6.5 Quantitative Analysis

- i. **Peak Signal-to-Noise Ratio (PSNR):** Figure 3.8 shows the PSNR values for different images encrypted using the proposed and other implemented algorithms. The PSNR values obtained from the proposed scheme are similar to that of other techniques present in the literature. An average PSNR value of 28.186655 is provided by the proposed scheme for the images used in the study.

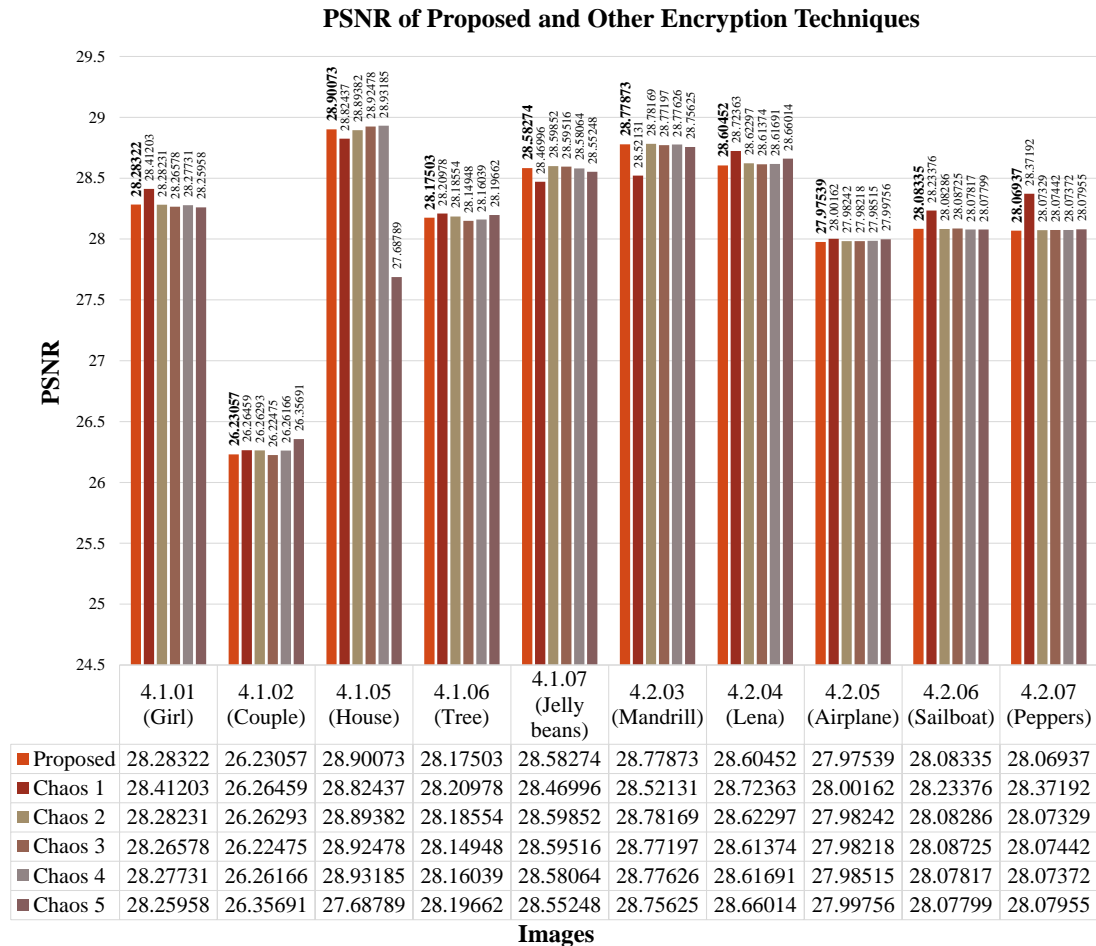


Figure 3.8: Graph of PSNR Values of the Proposed and Other Chaos Techniques

- ii. **Information Entropy:** Figure 3.9 shows the entropy values of the original and encrypted images. It can be seen that, like the other techniques implemented, the entropy values provided by the proposed scheme are approximating the ideal value of 8. The average entropy value obtained was 7.999008.

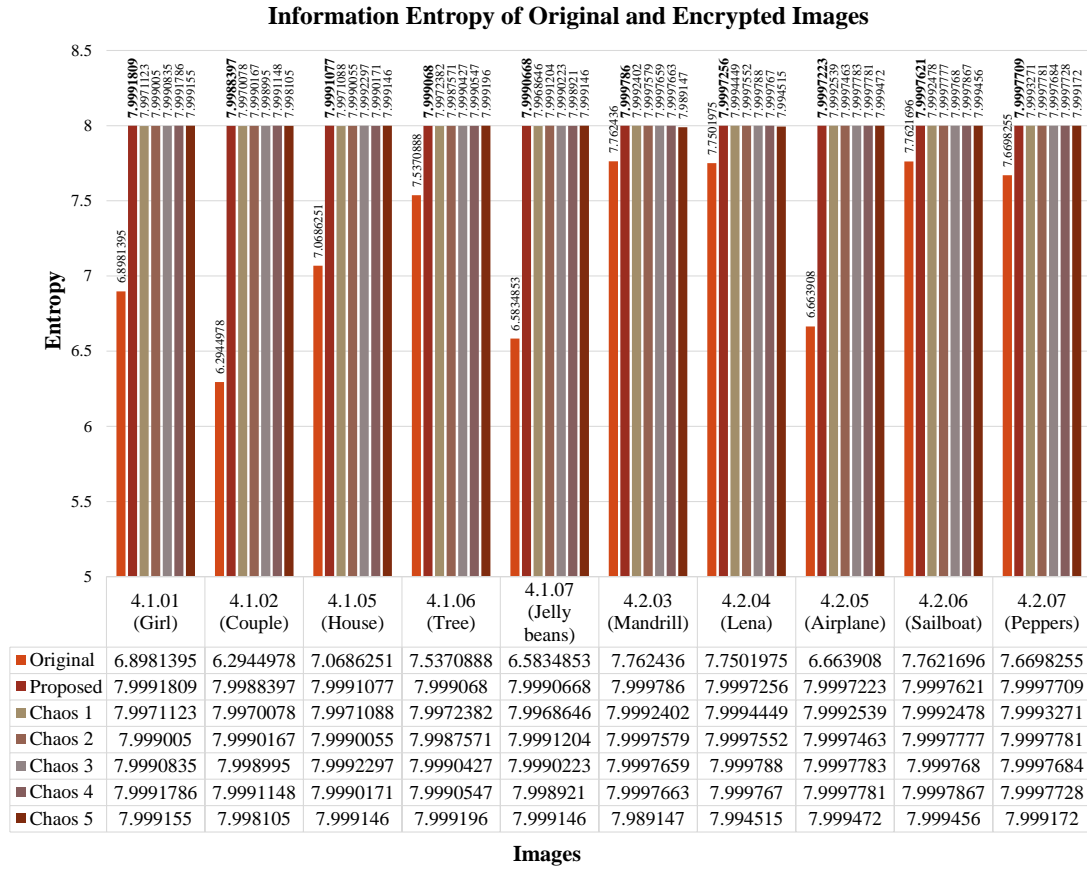


Figure 3.9: Graph of Information Entropy of Original and Encrypted Images

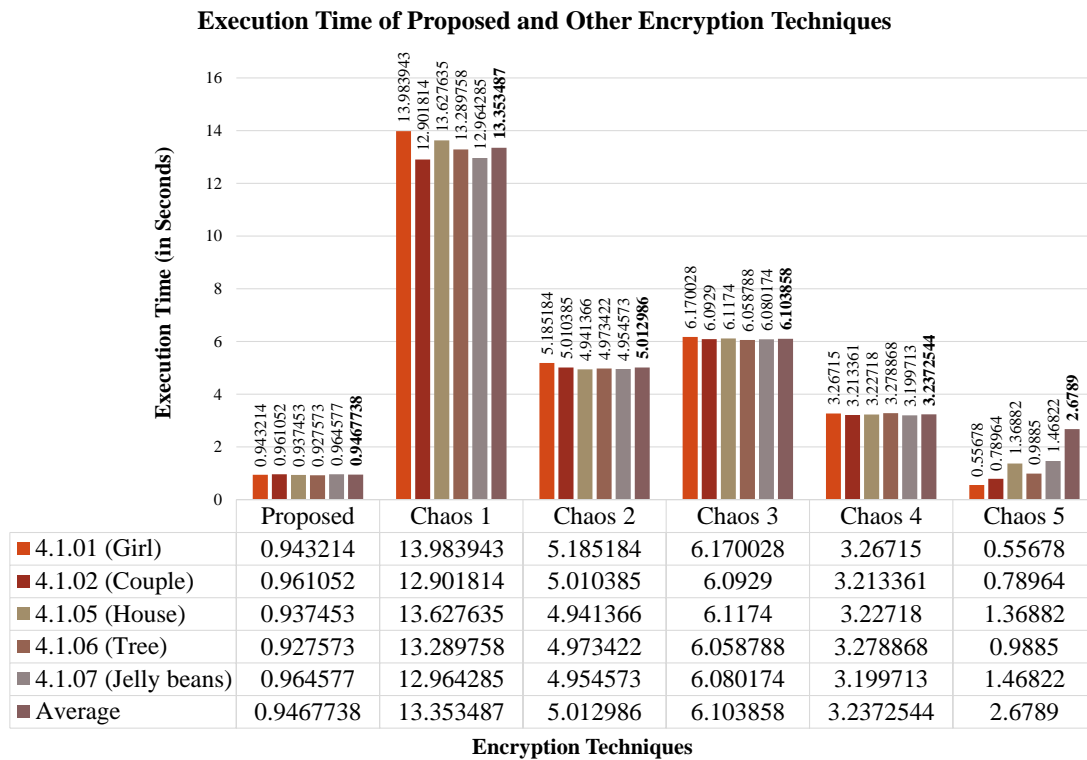


Figure 3.10: Graph of Execution Time of Proposed and Other Techniques

3.6.6 Execution Time

Figure 3.10 shows the time taken for execution by the proposed and other techniques implemented for 256×256 images of the SIPI database. The average time for execution of all the images encrypted by the proposed scheme is 0.946773 seconds which is very less in comparison to other implemented techniques. It can be seen that the proposed scheme is faster than other proposed techniques and hence reflects the efficiency to be used in practical cases.

3.7 CONCLUSION

The research proposes an image encryption technique based on an intertwining map and RC4 stream cipher. The proposed scheme has been evaluated on various performance metrics from which these inferences are drawn:

- The results show that the proposed technique provides highly scrambled encrypted image which have no visual resemblance with the original image. Whereas, the images obtained after decryption were visually alike as of the original images. This ensures no information leakage by a visual inspection and ensures to provide visually reliable decrypted images.
- The technique is very strong resistant against the Statistical Attacks. It is clear from the histograms, which are uniformly distributed and have no resemblance with the histograms of the original images. Also, the encrypted images provide very low values of the correlation coefficients and have uniformly distributed correlation graphs for all three orientations with no resemblance to the original correlation graphs. All this ensures no information leakage and hence ensures security against the statistical attacks.
- The technique is also strong resistant against the Differential Attacks. The NPCR and UACI values obtained are close to the ideal values. An average NPCR of 99.60334% and an average UACI of 31.841% were obtained for a single bit change in the key used.
- The proposed technique has a key space of 2^{384} , which makes it resistant against the Brute Force Attack. The technique provide PSNR values similar to other techniques. Also, the scheme provides an average value of 7.9994 for the information entropy, approximating the ideal value of 8. Finally, the scheme has a faster execution time in comparison to other implemented techniques.

Though the proposed encryption technique has very good Execution Time and Randomness (Entropy) but it failed to pass UACI test. The identified reasons are as follows:

- (a) Diffusion was done in only four directions (row wise and column wise Forward, Backward Diffusion).
- (b) Byte level permutation and substitution was used in Confusion stage.
- (c) Logistics maps were used that are random in nature but for passing UACI test more complex maps are required.

In the next chapter, an advanced Quantum encryption scheme is proposed that tries to achieve all the Performance Metrics.

CHAPTER 4

A SUPERLATIVE IMAGE ENCRYPTION TECHNIQUE BASED ON BIT PLANE USING KEY-BASED ELECTRONIC CODE BOOK

4.1 INTRODUCTION

The world is interconnected by the distinct spectra of technology. Advancements in technology budge into the future of automation which raises reliance on cyber connectivity, resulting in exposure of secret messages, images to the attackers that are always trying to uncover and exploit vulnerabilities [144]. Henceforth necessitates protection of usability for smooth transfusion of data from one port to another. Securing a network is the process of targeting a variety of threats and stopping them from rampaging through the system as just a few minutes of exposure can cause widespread disruption and massive damage to public and private organization's bottom line and reputation; thus, protective measures must always be in place. Confidentiality is the core ingredient that accounts for the plausibility of security services for a message [145]. Mainly providing privacy between the sender and the user is advocated by the phenomena of confidentiality. The authorization over data is held confidential only to the permitted users, attaining garbage values for an unauthorized user. This research works focus upon the principle of preserving confidentiality, particularly for images. Encryption is one of the highly effective techniques to achieve this. Extensive researches are going on in this direction to evolute an infallible encryption mechanism. Literature includes traditional mechanisms followed by Chaos and Quantum Chaos-based Encryption Methods [119]. This evolution is characterized by large key space, high entropy, and low

processing time. Recently, Qubit based techniques [72] are in progress which enhances results in terms of randomness and makes security system more robust.

Previously designed encryption techniques were complicated and were compatible mainly with texts. The techniques possessed low randomness, limited key size, and consumed high processing time to encrypt images, while small key space leads to an easy intruder attack. Chaos-based Techniques [71] were evolved and considered for securing confidentiality for the communication of images over the network. In this technique modified secret keys were used at multiple levels of the encryption process. The Chaos Processes the pixel positions and values are both modified using Confusion and Diffusion respectively. The randomness of encrypted images is much larger due to the nonlinear characteristics of Chaotic Maps used. Furthermore, Quantum Chaos-based Logistic Maps [74] were used to encrypt images, which results in improvement of all the parameters like randomness, entropy, key sensitivity, image perceptual quality, attack analysis, and execution time. Recently proposed Quantum Qubit based techniques [73] lead to a further increase in the extent of randomness and entropy due to the usage of bit instead of byte plane encryption.

This research is an effort to develop a fine quality cryptography technique. The proposed work is a Block Cipher-based Technique that consists of both Confusion and Diffusion Processes. The hallmarks of the proposed scheme are:

- The number of iterations for the Confusion Process is not fixed; it depends on the key which makes the encryption process more secure. As the key changes, the number of iterations also changes resulting in increased randomness.
- The folding procedure used for the Diffusion Process uses different keys for different directions of folding applicable on three channels of the color image independently. This not only increases key space but also increases randomness in the process.
- In the Confusion Process Electronic Code Book (ECB) [93] and IP block [45] are used to secure the data by altering the pixels of an image. These two processes are dependent on keys. With the amendment of key, the values of ECB as well as IP block also changes and hence enhance image imperceptibility.
- The keys generated from the quantum logistic map are not used directly; instead, they are used to generate a random number of iterations for final key generation.
- Both intra and inter bit plane scrambling operations are performed on all the channels collectively instead of scrambling the bit planes of R, G, B channels individually.

4.2 PROPOSED ENCRYPTION SCHEME

A brief description of the Quantum Chaotic Maps [70] is required for better understanding of the proposed encryption scheme.

➤ Quantum Chaotic Maps:

To protect information, various image encryption schemes are proposed. These schemes are designed based on various Chaos and Quantum Chaos Maps. Chaotic systems have various features such as sensitivity to initial conditions and parameters, high efficiency, ergodicity which makes it compatible for securing image encryption schemes. Nowadays, image encryption schemes use Quantum Chaotic Systems to generate pseudo random sequences due to their excellent properties such as randomness, sensitivity to initial conditions, and deterministic nature [146]. Randomness and non-periodicity of the Quantum Chaotic Map are successfully verified by statistical complexity and the normalized Shannon entropy [41]. To study the effects of quantum corrections, $a = \langle a \rangle + \Delta a$ is considered, where Δa is quantum fluctuations about $\langle a \rangle$ [146, 147]. The Quantum Chaotic Map Eq. (4.1a), (4.1b) and (4.1c) with lowest order quantum corrections is followed by the following equations:

$$x(i+1) = r \left(x(i) - (\text{abs}(x(i)))^2 \right) - r \times y(i) \quad (4.1a)$$

$$y(i+1) = \left(-y(i) \times e^{-2\beta} \right) + \left(e^{-\beta} \times r \left(\left(2 - x(i) - \overline{x(i)} \right) y(i) - x(i) \overline{z(i)} - \overline{x(i)} z(i) \right) \right) \quad (4.1b)$$

$$z(i+1) = \left(-z(i) \times e^{-2\beta} \right) + \left(e^{-\beta} \times r \left(2 \left(1 - \overline{x(i)} \right) z(i) - 2x(i)y(i) - x(i) \right) \right) \quad (4.1c)$$

Where,

$x = \langle a \rangle$, $y = \langle \Delta a + \Delta a \rangle$, $z = \langle \Delta a \cdot \Delta a \rangle$ and β are dissipation parameter. In general $x(i)$, $y(i)$ and $z(i)$ are complex numbers. $\overline{x(i)}$, $\overline{z(i)}$ are the complex conjugate of $x(i)$ and $z(i)$ respectively.

If initial conditions are real values, then all successive values will also be real and if the values are complex numbers, then their magnitude is taken into consideration. The random sequences used in subsequent sections are generated with a Quantum Chaotic Map.

The next section gives the complete encryption process of the proposed technique.

4.3 ENCRYPTION PROCESS

Figure 4.1 shows the basic block diagram of the encryption and decryption process of the proposed model. The whole image encryption process includes three stages:

- i. Key Generation
- ii. Confusion
- iii. Diffusion

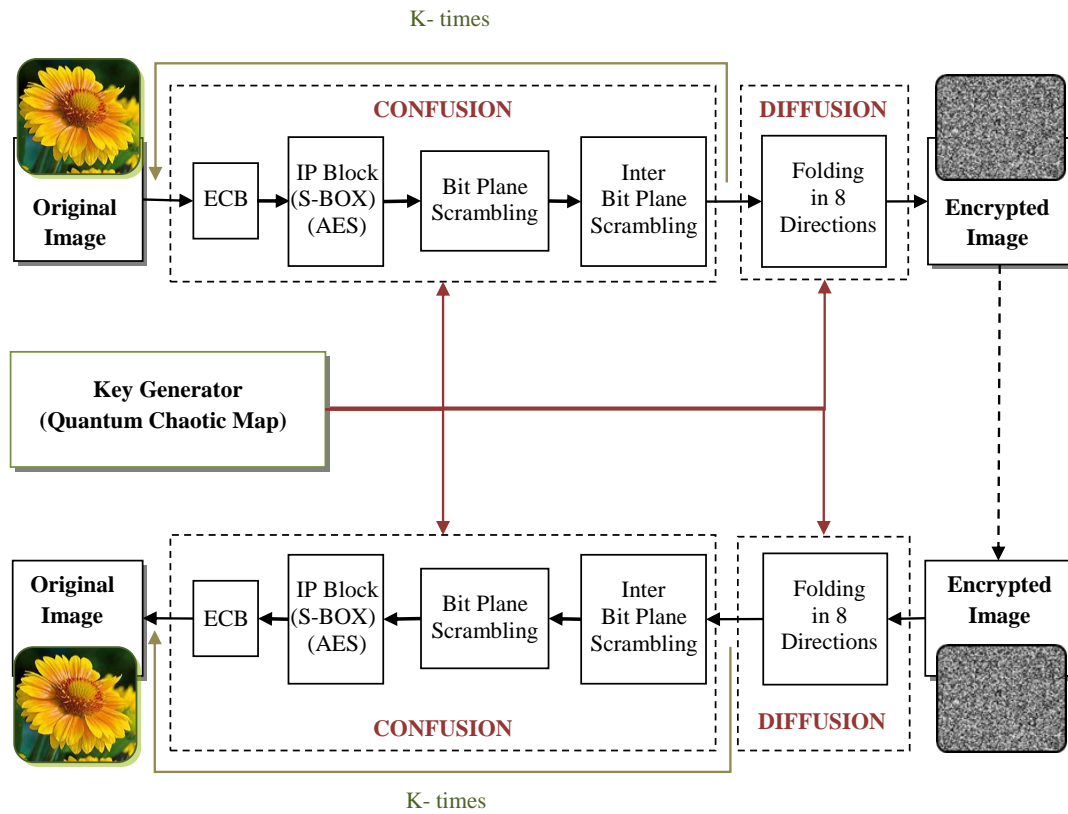


Figure 4.1: Block Diagram of Encryption and Decryption Process of the Proposed Technique

The proposed encryption scheme is elaborated in the subsequent sections:

4.3.1 Key Generation

The keys are generated using the Quantum Chaotic Maps so that Initial Conditions and Control Parameters are highly sensitive to the changes in even a single bit change in the secret key. The steps for the generation of keys are as follows:

- (a) The proposed encryption scheme generates the keys by iterating the Quantum Chaotic Map 1000 times to remove the transient effect.
- (b) The map is iterated using $x = 0.4523444336$, $z = 0.001324523564$, $\bar{x} = 0.002$, $\bar{z} = 0.004$, $y = 0.003453324562$, $r = 3.9$ and $\beta = 4.5$ as initial condition and control parameters.

(c) Now iterate the map 55 times using new initial conditions and then multiplied by 2^{32} . The 55 keys $k_i(k_1, k_2, k_3, \dots, k_{55})$ are generated by taking mod with different values of h as per Table 4.1 and the formula for generation of key k is given in Eq. (4.2).

$$k(i) = (x(i) \times 2^{32}) \bmod h \quad (4.2)$$

Table 4.1 shows the values 'h' for corresponding keys by which mod is taken.

Table 4.1: h Values Corresponding to Different Key Values

Key (k)	h Values
$k_1, k_2, k_{28} - k_{54}$	256
$k_3 - k_{27}$	24
k_{55}	4

Table 4.2 shows the different keys used for the generation of a random sequence of varying sizes and values, corresponding to the encryption block. Different blocks of the proposed scheme use a diverse set of keys for the generation of random sequence which is further used in the process for encryption and decryption of an image.

Table 4.2: Different Keys used for Generation of Random Sequence of Varying Sizes and Values, Corresponding to the Encryption Block

Keys	Used in the Encryption Block	Size of Random Sequences for $m \times n \times 3$ Size Image using Key
k_1	ECB Block in Confusion Process	1×256
k_2	IP Block in Confusion Process	$1 \times (m \times n)$
k_3	Bit Plane Scrambling in Confusion Process	1×24
$k_4 - k_{27}$	Inter Bit Plane Scrambling in Confusion Process	$1 \times (m \times n)$
$k_{28} - k_{54}$	Diffusion Process	1×256
k_{55}	The number of times Confusion Process is done	1×1

The algorithm for the Key Generation and generating random sequence of different size is given as:

**Algorithm for Key Generation and Generating Random Sequences of
Different Size using Key**

Initial Conditions: $x(1) = 0.4523444336; y(1) = 0.003453324562; z(1) = 0.001324523564;$
 $r = 3.9; b = 4.5; x_n = 0.002; z_n = 0.004; keys = [k_1, k_2, k_3, \dots, k_{55}];$

$[mnp] = \text{Size of Image}$

STEP 1: Iterating Quantum Chaotic Map 1000 times to eliminate transient effects

for ($i = 1 : 1 : 1000$)

$$x(i+1) = r \times (x(i) - (\text{abs}(x(i))))^2 - r \times y(i);$$

$$y(i+1) = (-y(i)\exp(-2b)) + (\exp(-b) \times r \times [(2 - x(i) - xn) \times y(i) - x(i) \times zn - xn \times z(i)]);$$

$$z(i+1) = (-y(i) \times \exp(-2b)) + (\exp(-b) \times r \times [(2 - x(i) - xn) \times y(i) - x(i) \times zn - xn \times z(i)]);$$

end;

$$x1(1) = x(1001);$$

$$y1(1) = y(1001);$$

$$z1(1) = z(1001);$$

STEP 2: Iterating the map to get $x1$, $y1$ and $z1$ values needed for keys ($k1 - k55$)

for ($j = 1 : 1 : 55$)

$$x1(j+1) = r \times (x1(j) - (\text{abs}(x1(j))))^2 - r \times y1(j);$$

$$y1(j+1) = (-y1(j) \times \exp(-2 \times b)) + (\exp(-b) \times r \times [(2 - x1(j) - xn) \times y1(j) - x1(j) \times zn - xn \times z1(j)]);$$

$$z1(j+1) = (-z1(j) \times \exp(-2 \times b)) + (\exp(-b) \times r \times [2 \times (1 - xn) \times zn - 2 \times x1(j) \times y1(j) - xn]);$$

end;

STEP 3: Applying round and mod function and multiplication operation to get necessary key values in integer for generating random values of different size.

$$k_{55} = \text{round}(\text{mod}(((z1(55) \times 2^{32})), 4));$$

$$k_1 = \text{round}(\text{mod}(((y1(1) \times 2^{32})), 256));$$

Random sequence sk_1 using key k_1 :

$$\text{rng}(k_1)$$

$$sk_1 = \text{randperm}(256);$$

$$k_2 = \text{round}(\text{mod}(((y1(2) \times 2^{32})), 256));$$

Random sequence sk_2 using key k_2 :

$$\text{rng}(k_2)$$

$$sk_2 = \text{randperm}(m \times n);$$

$$k_3 = \text{round}(\text{mod}(((y1(3) \times 2^{32})), 24));$$

Random sequence sk_3 using key k_3 :

$$\text{rng}(k_3)$$

$$sk_3 = \text{randperm}(24);$$

for ($i = 1 : 1 : 24$)

$$k_{i+3} = \text{round}(\text{mod}(((x1(i+3) \times 2^{32})), 24));$$

Random sequences sk_{i+3} using keys k_{i+3} :

$$\text{rng}(k_{i+3})$$

$$sk_{i+3}(:, :, i) = \text{randperm}(m \times n);$$

end;

for ($i = 1 : 1 : 27$)

$$k_{i+27} = \text{round}(\text{mod}(((x1(i+27) \times 2^{32})), 256));$$

Random sequence $sk(:, :, i)$ using keys k_{i+27} :

$$\text{rng}(k_{i+27})$$

$$sk(:, :, i) = \text{randi}([0, 255], m);$$

end;

4.3.2 Confusion Process

A random key sequence is generated using Key Generation Process which is further applied to different Confusion blocks. The Confusion Process [61] helps in securing the data by making a complicated relationship between the encrypted data and the keys. Thus, it makes harder for the unauthorized users to find the key even if large combinations of original data and encrypted data are tried. The Confusion Process includes ECB (Electronic Code Book [93]), IP block (Initial Permutation [129]), Bit plane scrambling [112], and Inter bit plane scrambling [73]. Figure 4.2 shows the basic block diagram of the Confusion Process with the corresponding keys used in each process. These processes are iterated k times using $k55$ key value whose range varies from 1 to 4 and different values of k makes it more difficult for the unauthorized source to find the number of iterations for decrypting the data.

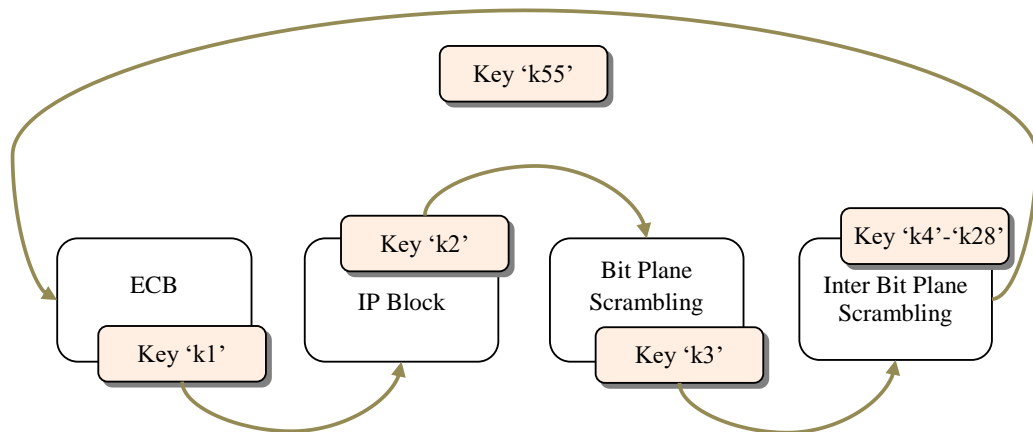


Figure 4.2: Block Diagram of Confusion Process

- i. **Generation of Electronic Code Book (ECB):** Electronic code book [93] is a Block Cipher Algorithm for providing security. In this process, a codebook is generated by using a random sequence with all the values from 0 to 255 corresponding to each pixel value of an image using key $k1$. Now, a codebook is generated which replaces the pixel values of all the 3 planes R, G and B of the color image with the assigned value in the codebook. This process is deterministic as if original data are replaced twice using the same random sequence or key, then the encrypted data is the same as original data. The algorithm for the first stage of the Confusion Process i.e., Electronic Code Book is provided:

Algorithm for Electronic Code Book (ECB) of Confusion Process

Input: $I = RGB$ Image; $[RGB] = R, G, B$ planes of image I ; $[mnp] = size(I)$;

$(i, j) = i^{th}$ row and j^{th} column pixel of image;

$sk_1(i) = \text{value at } i^{\text{th}} \text{ position of random sequence generated using key } k1;$

$I'_{ecb} = \text{out put confused image of ECB process};$

Function $[I'_{ecb}] = ECB(I, sk_1)$
 $sk_1 = sk_1(1 : 256) - 1;$
for $i = 1 : 1 : n$
 for $j = 1 : 1 : n$
 $R'(i, j) = sk_1(R(i, j) + 1);$
 $G'(i, j) = sk_1(G(i, j) + 1);$
 $B'(i, j) = sk_1(B(i, j) + 1);$
 end;
end;
Convert R', G' and B' into matrix of size $m \times n$
 $I'_{ecb} = [R'G'B']$

- ii. **Initial Permutation (IP) Block:** This process is similar to the s-box used in AES [129]. In this process, a random 1-dimensional sequence is generated with the values from 1 to each plane size of an image (i.e. $m \times n$ for the color image of size $m \times n \times 3$) using key $k2$. The values of the sequence correspond to the position where the pixel value needs to be placed and the inverse process also uses the same key and changes the position of the pixel value back to the original position. This process scrambles the pixel values but does not change the value of an image pixel. This process is followed by method for altering bits within pixels. The algorithm for the second stage of the Confusion Process i.e. Initial Permutation (IP) Block is given below:

Algorithm for Initial Permutation (IP) Block of Confusion Process

Input: $I = RGBImage; [RGB] = R, G, B \text{ planes of image } I \text{ in } 1D \text{ array of size } (1, m \times n);$
 $[mnp] = \text{size}(I); (i, j) = i^{\text{th}} \text{ row and } j^{\text{th}} \text{ column pixel of image};$
 $sk_2(i) = \text{value at } i^{\text{th}} \text{ position of random sequence generated using key } k2;$
 $I'_{IP} = \text{out put confused image of IP process}$

Function $[I'_{IP}] = IP_{block}(I'_{ecb}, sk_2);$
for $(i = 1 : m \times n)$
 $R'(sk_2(i)) = R(i);$
 $G'(sk_2(i)) = G(i);$
 $B'(sk_2(i)) = B(i);$
end;
Convert R', G' and B' into matrix of size $m \times n$
 $I'_{IP} = [R'G'B']$

iii. **Bit Plane Scrambling:** A color image is a combination of RGB channels. The pixel values of the color image are changed by the bit plane scrambling process [112]. In this process:

- All the three channels (R, G, B) of the colored images are divided into 8-bit planes each, to get 24-bit planes.
- Using key k_3 a random sequence of values 1 to 24 is created only once.
- Now all the 24-bit planes are scrambled according to the random sequence. For e.g., if in random sequence, the first value is 15, that means now the first-bit plane will be the 15th bit plane of the image. So, all the 24-bit planes are scrambled using this process.
- Reverse bit plane process is exactly the reverse of this process.

The algorithm for the third stage of Confusion Process i.e. Bit Plane Scrambling Process is given below:

Algorithm for Bit Plane Scrambling Confusion Process

Input: $bp = \text{bit planes of RGB Image } (m \times n \times 24)$;

$sk_3(i) = \text{value at } i^{\text{th}} \text{ position of random sequence generated using key } k_3$;

$I'_{bps} = \text{output confused image of IP process}$

Function $[I'_{bps}] = \text{bitplane_scramb}(bp, sk_3)$

for ($i = 1 : 1 : 24$)

$I'_{bps}(:, :, i) = bp(:, :, sk_3(i))$;

end;

iv. **Inter Bit Plane Scrambling:** A random sequence is generated [73] of size $1 \times (m \times n)$ and having values from 1 to $m \times n$ only once.

- The i^{th} bit plane is converted into a 1D array ($1 \times (m \times n)$). The values of the sequence correspond to the position where the bit value needs to be placed and the inverse process also uses the same key and changes the position of the bit value back to the original position.
- Now all the bit planes are combined back to get the image of size $m \times n \times 3$.

The algorithm for the last stage of the Confusion Process i.e. Inter bit plane scrambling process is given below:

Algorithm for Inter Bit Plane Scrambling Confusion Process

Input: $I = \text{RGB Image}$; $[RGB] = R, G, B \text{ planes of image } I \text{ in 1D array of size } (1, m \times n)$;

$[mnp] = \text{size}(I)$; $(i, j) = i^{\text{th}} \text{ row and } j^{\text{th}} \text{ column pixel of image}$;

$sk_{i+3}(:, :, i) = \text{value at } i^{\text{th}} \text{ position of random sequence generated using key } k_2$;

I'_{IP} = output confused image of IP process
Function $[A] = \text{interBitScramb}(I'_{bps}, sk_{i+3})$
 $a = \text{reshape}(I'_{bps}, 1, m \times n)$
for($i = 1 : m \times n$)
 $A(sk_{i+3}(i)) = a(i)$
end;
 $I'_{ibp} = \text{reshape}(A, m, n)$
for($i = 1 : 1 : 24$)
 $I'_{ibp}(:, :, i) = \text{interBitScramb}(I'_{bps}(:, :, i), sk_{i+3}(:, :, i))$
end;

The number of iterations to be performed for the complete encryption process is based on the key $k55$. The value of $k55$ is in the range from 1 to 4. This ensures the security of the encryption process.

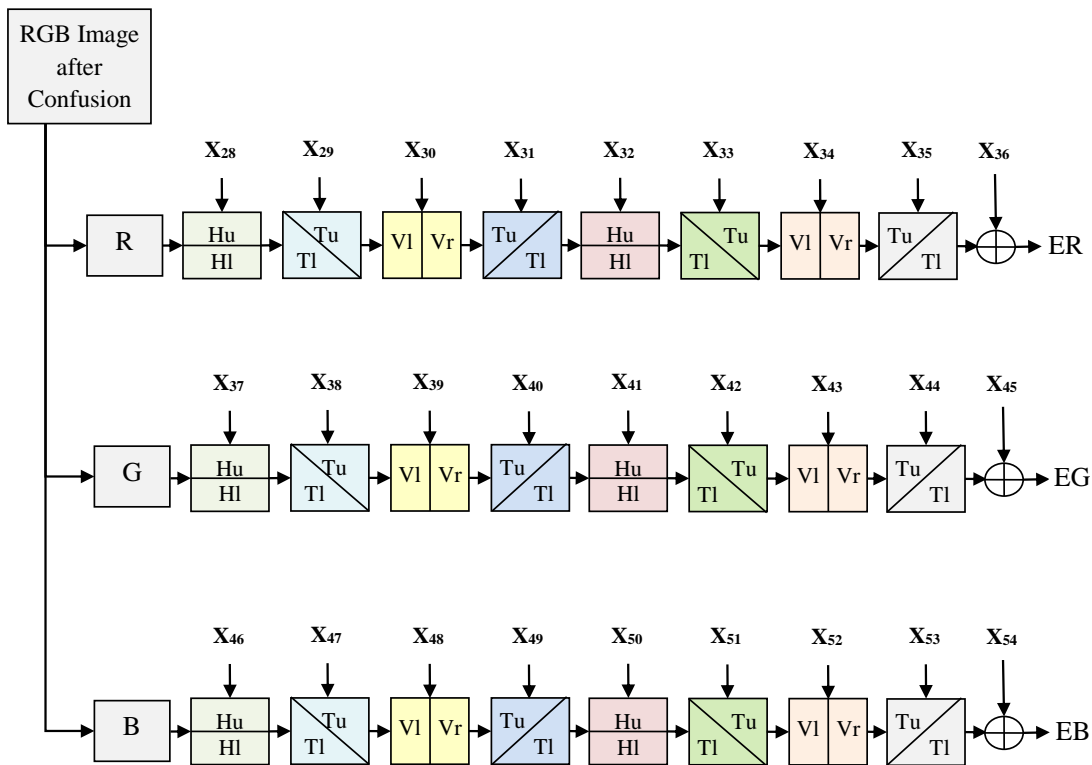


Figure 4.3: Block Diagram of Diffusion Process

4.3.3 Diffusion Process

The process applies a random key sequence generated using keys $K_{R,G,B}$ each in different processes for all the 3 channels (R, G, B). This process helps in increasing redundancy. Even a single bit change in the secret key makes non uniform changes in

the image, which makes it harder for the unauthorized user to detect the data correctly. In this process, a folding technique is used along 8 directions and for each direction different key is used. The block diagram of the Diffusion Process with folding is shown in Figure 4.3. The Diffusion Process is described below:

Using key $k_{28} - k_{54}$, a random matrix of size $m \times n$ is generated having values from 0 to 255. From this, we get 27 matrices say $X_{28}, X_{29}, \dots, X_{54}$.

- For the R channel, the key matrix used is X_{28} to X_{36} . whereas, for G channel, the key matrix used is X_{37} to X_{45} and for B channel, the key matrix used is X_{46} to X_{54} .
- To explain the process, just the R channel is taken into consideration. The R channel matrix is folded from 8 directions for encryption. The algorithm for the Diffusion Process for the Proposed Technique is given below:

Algorithm for Diffusion Process

Step 1 (The matrix R' , is divided into two equal horizontal parts: Hu and HI)

$$Hu'(i, j) = Hu(i, j) \oplus X_{28}(i, j)$$

$$HI'(m-i+1, j) = Hu(m-i+1, j) \oplus Hu'(i, j)$$

where $i = 1, 2, \dots, m/2$ and $j = 1, 2, \dots, n$ and \oplus denotes XOR operation.

Step 2 (The matrix $R1$ obtained after Step 1 is divided into two equal diagonal parts: Tu and TI)

$$Tu'(i, j) = Tu(i, j) \oplus X_{29}(i, j)$$

$$TI'(j, i) = TI(j, i) \oplus Tu'(i, j)$$

where $i = 1, 2, \dots, m$ and $j = i, i+1, \dots, n$.

Step 3 (The matrix $R2$ obtained after Step 2 is divided into two equal vertical parts: Vr and VI)

$$Vr'(i, j) = Vr(i, j) \oplus X_{30}(i, j)$$

$$VI'(i, n-j+1) = VI(i, j) \oplus Vr'(i, n-j+1)$$

where $i = 1, 2, \dots, m$ and $j = n/2+1, n/2+2, \dots, n'$

Step 4 (The matrix $R3$ obtained after Step 3 is divided into two equal diagonal parts: Tu and TI)

$$TI'(i, j) = TI(i, j) \oplus X_{31}(i, j)$$

$$Tu'(i, j) = Tu(i, j) \oplus TI'(i, j)$$

where $i = 1, 2, \dots, m$ and $j = n-i+1, n-i+2, \dots, n$.

Step 5 (The matrix $R4$ obtained after Step 4 is divided into two equal horizontal parts: Hu and HI)

$$HI'(i, j) = HI(i, j) \oplus X_{32}(i, j)$$

$$Hu'(n-i+1, j) = Hu(n-i+1, j) \oplus HI'(i, j)$$

where $i = m/2+1, m/2+2, \dots, m$ and $j = 1, 2, \dots, n$.

Step 6 (The matrix $R5$ obtained after Step 5 is divided into two equal diagonal parts: Tu and TI)

$$TI'(i, j) = TI(i, j) \oplus X_{33}(i, j)$$

$$Tu'(j, i) = Tu(j, i) \oplus TI'(i, j)$$

where $i = 1, 2, \dots, m$ and $j = 1, 2, \dots, i-1$.

Step 7 (The matrix $R6$ obtained after Step 6 is divided into two equal diagonal parts: VI and Vr)

$$VI'(i, j) = VI(i, j) \oplus X_{34}(i, j)$$

$$Vr'(i, n-j+1) = Vr(i, j) \oplus VI'(i, n-j+1)$$

where $i = 1, 2, \dots, m$ and $j = 1, 2, \dots, n/2$.

Step 8 (The matrix $R7$ obtained after Step 7 is divided into two equal diagonal parts: Tu and TI)

$$Tu'(i, j) = Tu(i, j) \oplus X_{35}(i, j)$$

$$Tl'(i, j) = Tl(i, j) \oplus Tu'(i, j)$$

where $i = 1, 2, \dots, m$ and $j = 1, 2, \dots, n - i$.

After round 8, matrix R8 is obtained and XORed with X_{36} , and finally resulted in an encrypted image ER

ER

This is the complete process to encrypt the R channel named as ER. Similarly, G and B channels are encrypted using keys and key matrix corresponding to them, to get EG and EB as shown in Figure 4.3 [71]. The reverse of the Diffusion Process is performed using the same key and the key matrix generated using the key. First, all three channels ER, EG, and EB of the encrypted image are XORed with the key matrix X_{36} , X_{45} , and X_{54} respectively. Then, the process of opening the folded matrix is performed on all the channels. For example, the opening process for round 1 is given in Eq. (4.3a) and (4.3b) is as follows:

$$DHL(m - i + 1, j) = DHL'(m - i + 1, j) \oplus DHu'(i, j) \quad (4.3a)$$

$$DHu(i, j) = DHu'(i, j) \oplus X_{28}(i, j) \quad (4.3b)$$

Where;

$$i = 1, 2, \dots, \frac{m}{2} \text{ and } j = 1, 2, \dots, n.$$

Similarly, the opening process is performed for all the 8 rounds and for all the 3 channels. In the end, all the modified three planes are combined to form a Cipher Image of same size as original or plane image. The decryption process is performed just in the reverse manner of the encryption process.

The next chapter provides simulation set up parameters along with performance metrics used in this work.

CHAPTER 5

SIMULATION SET-UP PARAMETERS AND RESULTS

In the last chapter, the proposed encryption technique based on Quantum Chaos Encryption (Proposed Technique 2) was discussed. Its efficacy is proved in this chapter using several performance metrics. All the techniques along with proposed one is implemented, and efficacy is evaluated in same set up environmental condition. The next section provides the set-up environment parameters followed by performance metrics and results.

5.1 SIMULATION SETUP PARAMETERS

Table 5.1 provides simulation setup parameters used, while evaluating results of other popular encryption techniques along with the Proposed Mechanism.

Table 5.1: Simulation Setup Parameters for Proposed Technique 2

Setup Parameters	Specifications
Processor	1.50GHz Intel Core i3
Operating system	Windows 8
Simulation tool	MATLAB version: R2014a serial update 2
Images Source	USC-SIPI Image Database [79]
Image Type	Color Images (RBG)
Image Format	.jpg, .jpeg
Size Of Images	256 × 256, 512 × 512
Original Key used for Encryption	$x = 0.4523444336$, $y = 0.003453324562$, $z = 0.001324523564$, $\bar{x} = 0.002$, $\bar{z} = 0.004$, $r = 3.9$ and $\beta = 4.5$
Modified Key used for Differential Attack Analysis	$x = 0.4523444336$, $y = 0.003453324562$, $z = 0.001324523564$, $\bar{x} = 0.002$, $\bar{z} = 0.004$, $r = 3.9$ and $\beta = 4.5$

To prove the efficacy of the proposed technique, its performance is evaluated on several performance metrics and corresponding results are analyzed. The next section gives the description of Performance Parameters along with analysis of the results obtained after implementation.

5.2 RESULTS AND DISCUSSIONS

The simulation results of the proposed mechanism are calculated with the help of various Performance Metrics and by taking average of each parameter on ten different images of two sizes i.e. 256×256 and 512×512 .

5.2.1 Visual Analysis

A good image encryption scheme shows no visual information [56] similarity with the original image. Table 5.2 and Table 5.3 shows the visual analysis of images of sizes 256×256 and 512×512 of the proposed technique and different techniques available in the literature. The encrypted image does not show any visual resemblance with the original image.

5.2.2 Statistical Attack Analysis

This attack basically exploits statistical weaknesses in the encryption algorithm to crack it. In our case, Histogram and Correlation analysis are the two parameters used for this purpose [81, 82].

- i. **Histogram:** Histogram of an image is a graphical portrayal of the frequency distribution of the pixel intensity values present in a digital image. Table 5.4 and 5.5 shows the histogram analysis of original, encrypted, and decrypted images for the proposed technique.
- ii. **Correlation Analysis:** In addition to Histogram Analysis, Correlation Analysis [28] is also performed on images. An image, when encoded, ought to have no connection between the corresponding pixels. This analysis can be done horizontally, vertically, and diagonally. For good encryption, the encrypted image must have very little correlation among adjacent pixels in all three directions. Eq. (1.2a), (1.2b), (1.2c) and (1.2d) represents the formula of Correlation Coefficient. Figures 5.1, 5.2 and 5.3 shows the graphical comparison of correlation in all three directions i.e. Horizontal, Vertical, and Diagonal Correlation for different techniques available in the literature.

Table 5.2: Visual Analysis of 256×256 Size Images











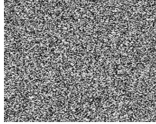


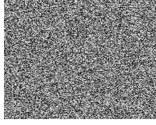





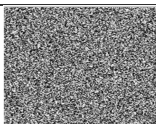


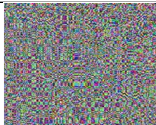


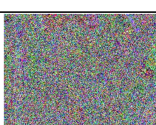


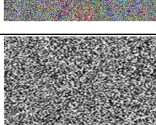

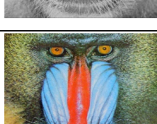
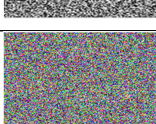
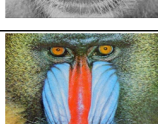
Image/ Technique	Original Image	Encrypted Image	Decrypted Image
Chaos 1			
Chaos 2			
Chaos 3			
Chaos 4			
Chaos 5			
Quantum Chaos 1			
Quantum Chaos 2			
Quantum Chaos 3			
Quantum Chaos 4			
Quantum Chaos 5			
Proposed Technique 2			

Table 5.3: Visual Analysis of 512×512 Size Images











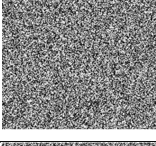




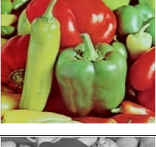
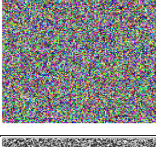
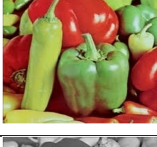







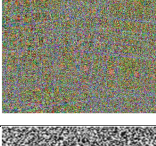


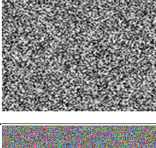

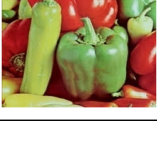
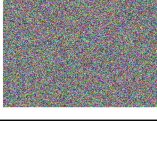
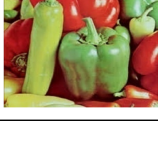
Image/ Technique	Original Image	Encrypted Image	Decrypted Image
Chaos 1			
Chaos 2			
Chaos 3			
Chaos 4			
Chaos 5			
Quantum Chaos 1			
Quantum Chaos 2			
Quantum Chaos 3			
Quantum Chaos 4			
Quantum Chaos 5			
Proposed Technique 2			

Table 5.4: Histogram Analysis of 256×256 Size Images


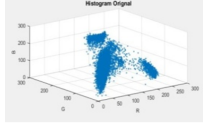
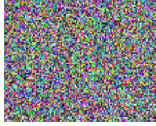
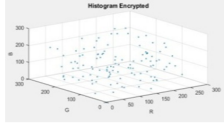

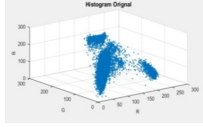



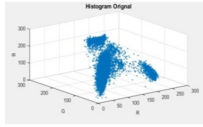

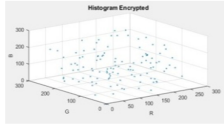

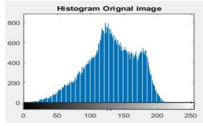
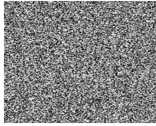
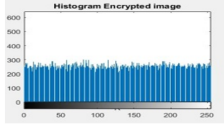
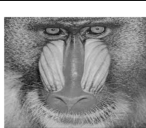
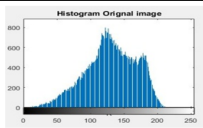
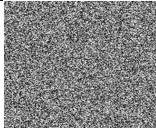
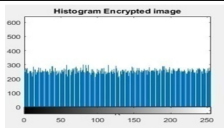

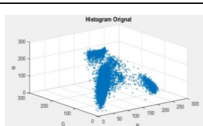

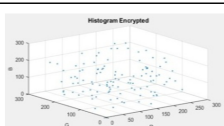
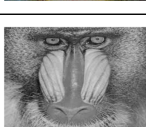
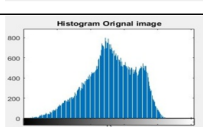

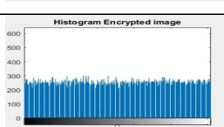
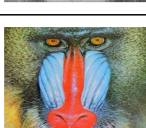
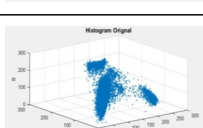

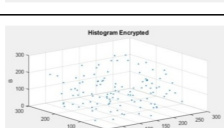

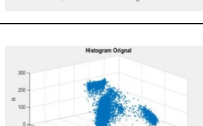

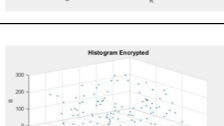
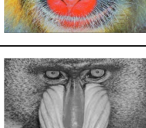
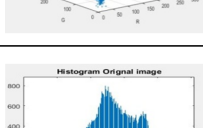
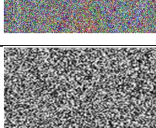
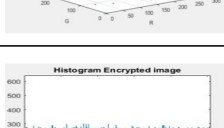

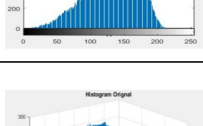
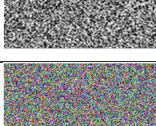
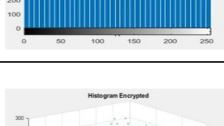

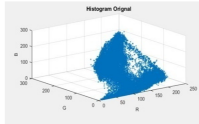

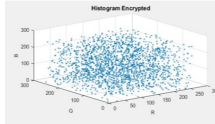

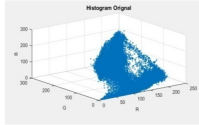

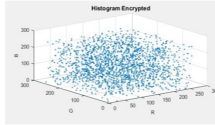

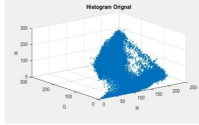

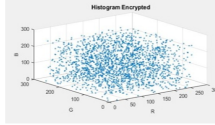

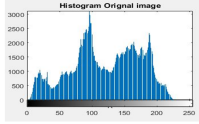
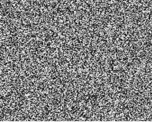
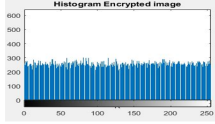

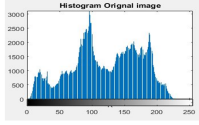
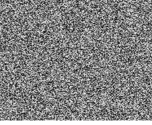
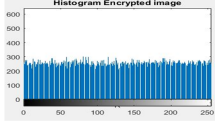

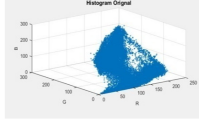

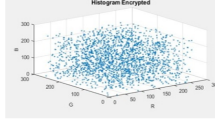

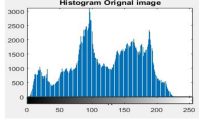
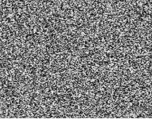
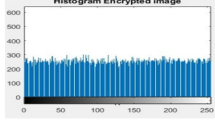

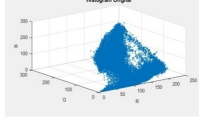

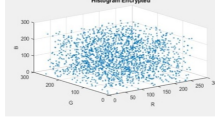

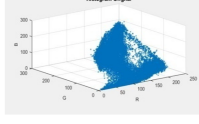

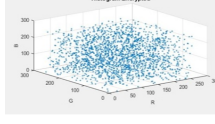

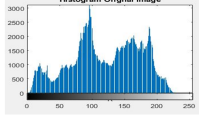
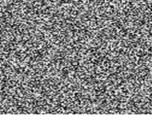
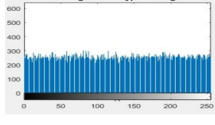

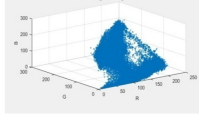

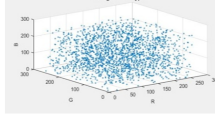
Image/ Technique	Original Image	Histogram (Original Image)	Encrypted Image	Histogram (Encrypted Image)
Chaos 1				
Chaos 2				
Chaos 3				
Chaos 4				
Chaos 5				
Quantum Chaos 1				
Quantum Chaos 2				
Quantum Chaos 3				
Quantum Chaos 4				
Quantum Chaos 5				
Proposed Technique 2				

Table 5.5: Histogram Analysis of 512×512 Size Images

Image/ Technique	Original Image	Histogram (Original Image)	Encrypted Image	Histogram (Encrypted Image)
Chaos 1				
Chaos 2				
Chaos 3				
Chaos 4				
Chaos 5				
Quantum Chaos 1				
Quantum Chaos 2				
Quantum Chaos 3				
Quantum Chaos 4				
Quantum Chaos 5				
Proposed Technique 2				

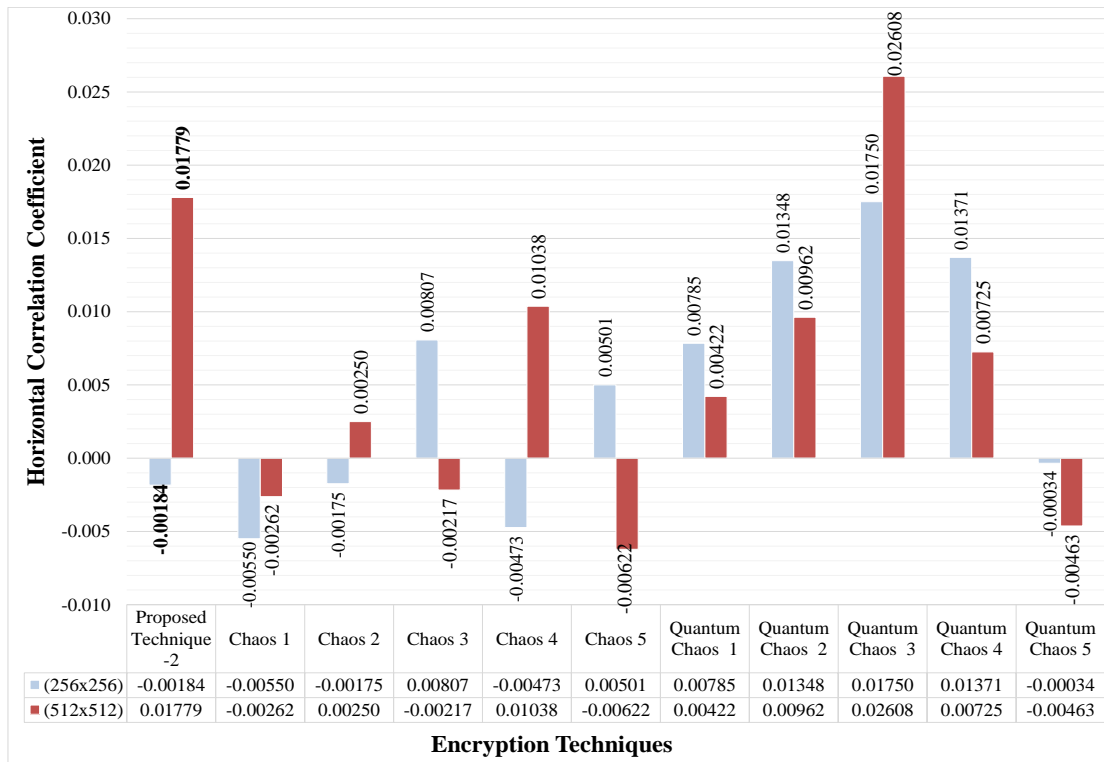


Figure 5.1: Graph Depicting Horizontal Correlation Graphs Respectively Compared with the Chaos and Quantum Chaos Techniques for 256×256 and 512×512 Size Images

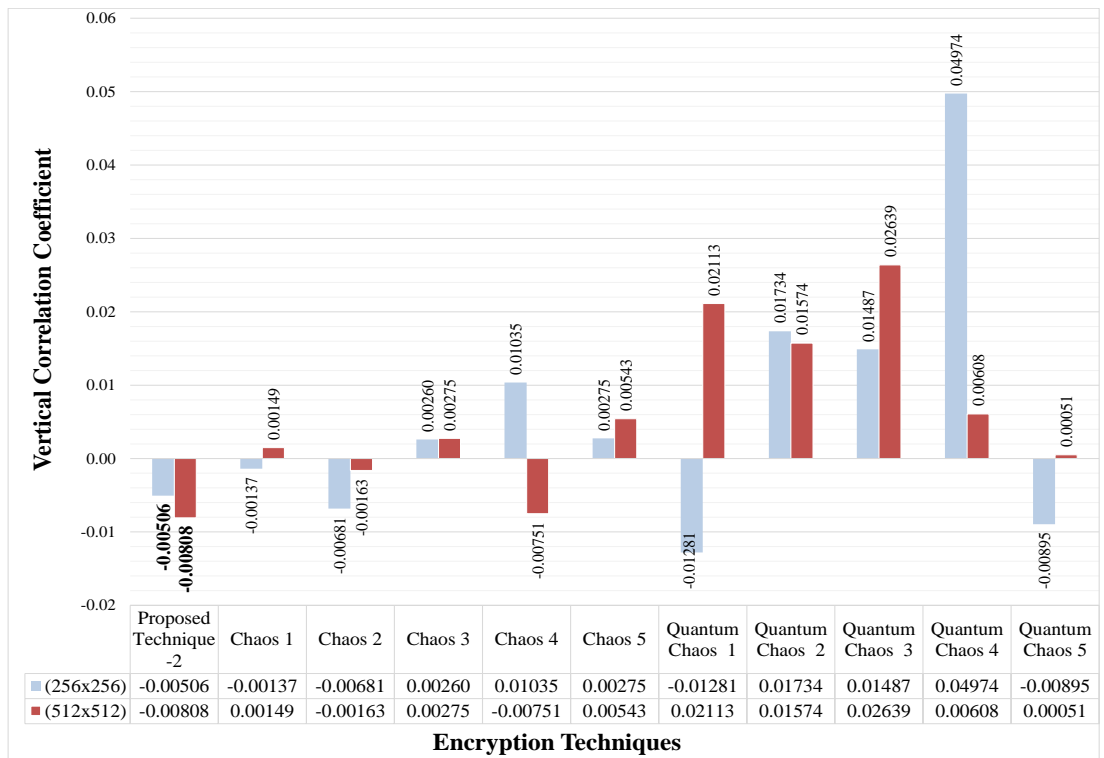


Figure 5.2: Graph Depicting Vertical Correlation Graphs Respectively Compared with the Chaos and Quantum Chaos Techniques for 256×256 and 512×512 Size Images

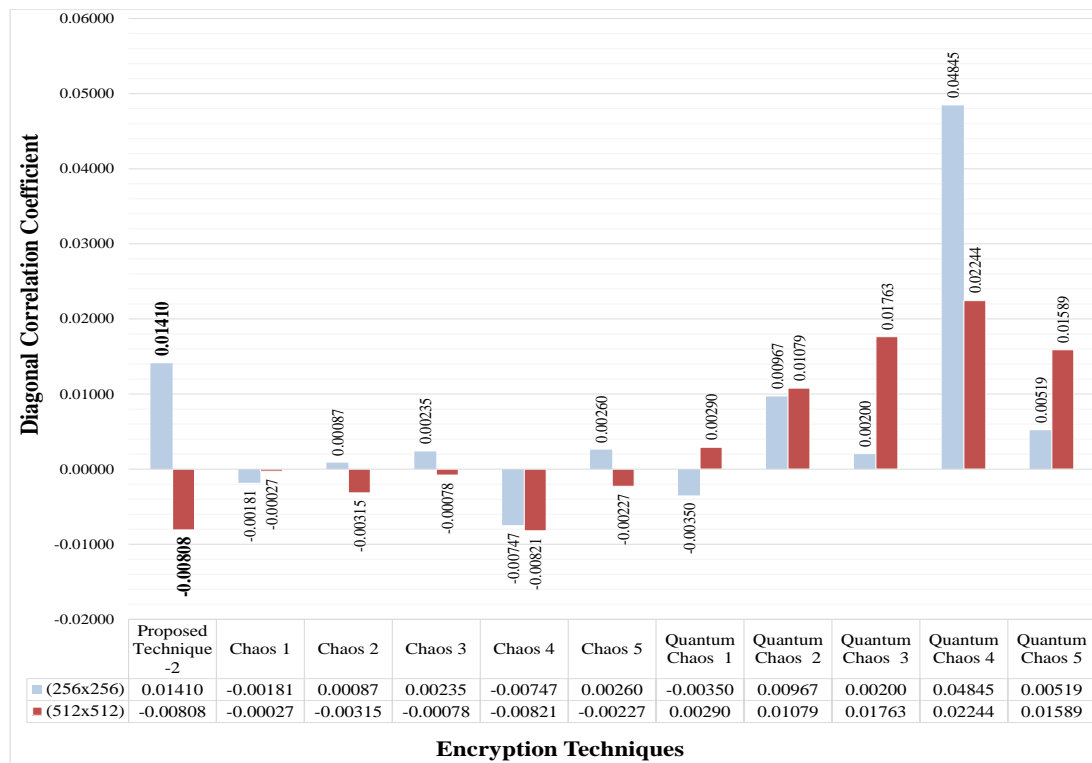


Figure 5.3: Graph Depicting Diagonal Correlation Graphs Respectively Compared with the Chaos and Quantum Chaos Techniques for 256×256 and 512×512 Size Images

5.2.3 Differential Attack Analysis

To do this test, a single bit is modified in data or in Key Value and results are calculated. These changes must be prominent to prove that a security technique is good or not. Two parameters are used for the attack analysis:

- i. **Number of Pixel Change Rate (NPCR) [85]:** It defines the rate of change in the number of pixels in between the two encrypted images formed by the original key and pixel modified (generally a bit only) key or in the Plain Image. The formula for NPCR is provided in Eq. (1.3a) and (1.3b). A slight change in key and original image should result in a completely different encrypted image. The impact of one-pixel change is analyzed by NPCR and UACI [96]. Table 5.6 shows the results of NPCR related to the image size of 256×256 . The results show that the proposed scheme shows better values of NPCR in comparison to theoretical values given in the literature [96]. The techniques Quantum 4 and Quantum 5 do not pass even the NPCR test, which is based on the qubit, whereas the proposed technique which is also based on qubit passes the entire NPCR level tests. This shows that the proposed technique is sensitive to small changes and has great resistance power towards differential attack.

Table 5.6: Number of Pixel Change Rate Test Table

Image 256×256	THEORETICAL NPCR CRITICAL VALUE			
	$N_0^*.05=99.5693\%$ $N_0^*.01=99.5527\%$ $N_0^*.001=99.5341\%$			
Techniques	Reported Values	0.05 level	0.01 level	0.001 level
Chaos 1	99.628194%	Pass	Pass	Pass
Chaos 2	99.568176%	Pass	Pass	Pass
Chaos 3	99.61344%	Pass	Pass	Pass
Chaos 4	99.594416%	Pass	Pass	Pass
Chaos 5	99.624633%	Pass	Pass	Pass
Quantum Chaos 1	99.5513%	Pass	Pass	Pass
Quantum Chaos 2	99.612426%	Pass	Pass	Pass
Quantum Chaos 3	99.59971%	Pass	Pass	Pass
Quantum Chaos 4	51.2329%	Fail	Fail	Fail
Quantum Chaos 5	50.2025%	Fail	Fail	Fail
Proposed Technique 2	99.611218%	Pass	Pass	Pass

- ii. **Unified Average Change in Intensity (UACI):** It defines the average value of differential intensities between the Plain and Encrypted images [85]. Table 5.7 shows the results of UACI related to 256×256 image size. The results show that the Proposed Technique passes the critical values of UACI test. This shows that the proposed technique is sensitive to small changes and has great resistance power towards differential attack.

Table 5.7: Unified Average Change in Intensity Test Table

Image 256×256	THEORETICAL UACI CRITICAL VALUE			
	$U_-^*0.05=33.284\%$ $U_-^*0.01=33.2255\%$ $U_-^*0.001= 33.1594\%$ $U_+^*0.05=33.6447\%$ $U_+^*0.01= 33.7016\%$ $U_+^*0.001= 3.7677\%$			
Techniques	Reported Values	0.05 level	0.01 level	0.001 level
Chaos 1	33.4688%	Pass	Pass	Pass
Chaos 2	33.4713%	Pass	Pass	Pass
Chaos 3	33.4598%	Pass	Pass	Pass
Chaos 4	33.4783%	Pass	Pass	Pass
Chaos 5	33.5468%	Pass	Pass	Pass
Quantum Chaos 1	33.4612%	Pass	Pass	Pass
Quantum Chaos 2	33.5012%	Pass	Pass	Pass
Quantum Chaos 3	33.5638%	Pass	Pass	Pass
Quantum Chaos 4	33.4674%	Pass	Pass	Pass
Quantum Chaos 5	25.0907%	Fail	Fail	Fail
Proposed Technique 2	33.4942%	Pass	Pass	Pass

5.2.4 Key Space Analysis

Key space defines the key length used in the entire process of encryption. Larger the key size lesser will be the feasibility of a brute-force search attack. This is a significant parameter characterizing the possibility of an encryption algorithm to withstand a Brute Force Attack [9, 18]. The key space of different encryption techniques is shown in Table 5.8. The key size used for encryption must be large combination of Key values. Ideally, the Key Space must be greater than 2^{100} for resisting brute force attacks with the current computational ability of computers. The proposed scheme has a large enough key space of 2^{432} which is suitable for secured transmission.

Table 5.8: Key Space Analysis of Various Techniques Available in Literature

Techniques	Key Space
Chaos 1	2^{462}
Chaos 2	2^{192}
Chaos 3	$2^{192} - 2^{216}$
Chaos 4	10^{42}
Chaos 5	2^{384}
Quantum Chaos 1	2^{72}
Quantum Chaos 2	2^{256}
Quantum Chaos 3	2^{128}
Quantum Chaos 4	10^{72}
Quantum Chaos 5	$> 2^{100}$
Proposed Technique 2	2^{432}

5.2.5 Quantitative Analysis

Two parameters are used in this study for quantitative calculation:

- i. **Peak Signal to Noise Ratio (PSNR):** It is the ratio between the maximum signal power components to the noise present in the Ciphred Image [25]. For evaluation of this metric, the Plain Image is considered as the signal and the encrypted image is considered as the noise. A logarithmic decibel scale is utilized to portray PSNR and to scale this on a compact representation of a wide range of the original signal or information available in the encrypted image. Figure 5.4 shows the PSNR for two different sizes of images for different techniques available in the literature. The proposed scheme shows the comparable results in reference to available techniques in the literature.
- ii. **Information Entropy:** It defines the amount of randomness in the given image [87]. More is the entropy of the encrypted image better is its randomness. The

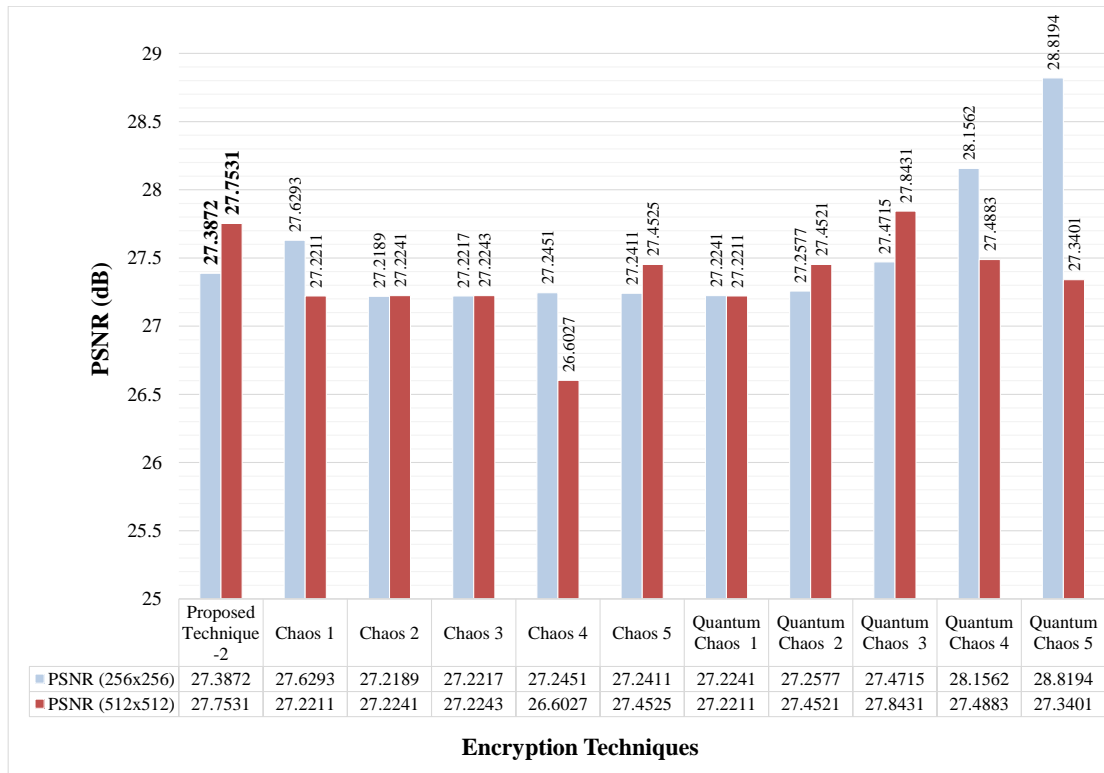


Figure 5.4: Graph Comparing PSNR Values of Proposed Technique with the Chaos and Quantum Chaos Techniques for 256×256 and 512×512 Images

formula of entropy is given in Eq. (1.6). Figure 5.5 shows the graphical and tabular values of entropy for the encrypted and original images of different sizes. If the

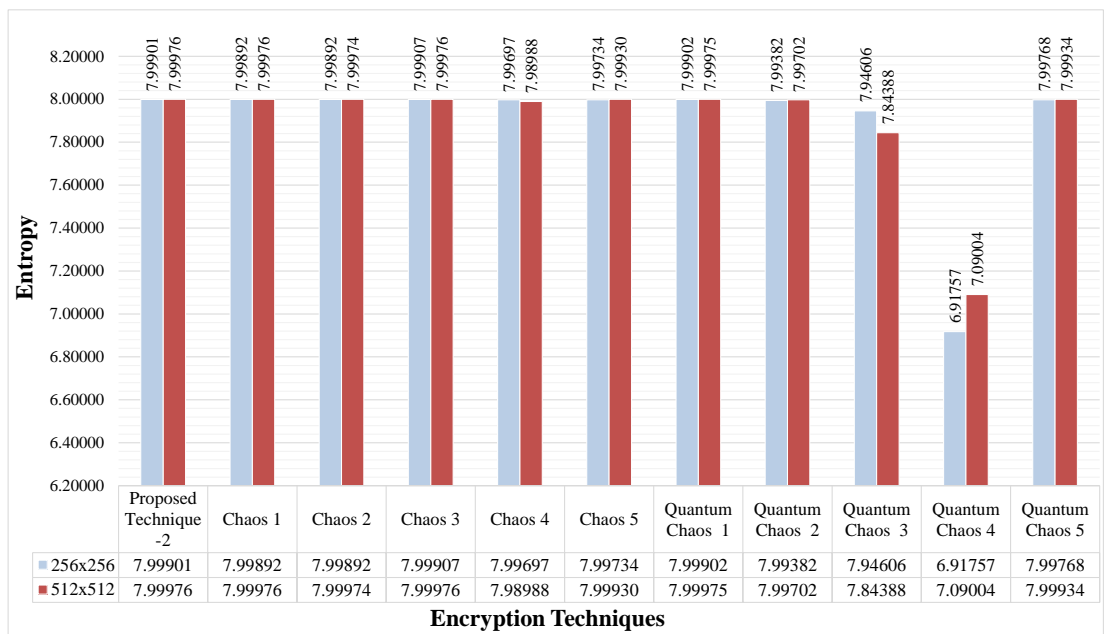


Figure 5.5: Graph Depicting Entropy Values of Proposed and Different Techniques of Different Sizes

image is completely randomized, then the maximum value of entropy comes out to 8 ideally. The proposed scheme shows entropy closed to 8.

5.2.6 Execution Time

The execution time is the amount of time taken for an image to be encrypted. The value of this parameter must be as low as possible. Figure 5.6 shows the time of execution of encryption for two different image sizes. The time of encryption plays a vital role in depicting the practical usability of the cryptography technique. If the execution time is high then it can not be used for practical applications. The table shows that the execution time of the proposed technique is comparable to other popular techniques given in literature.

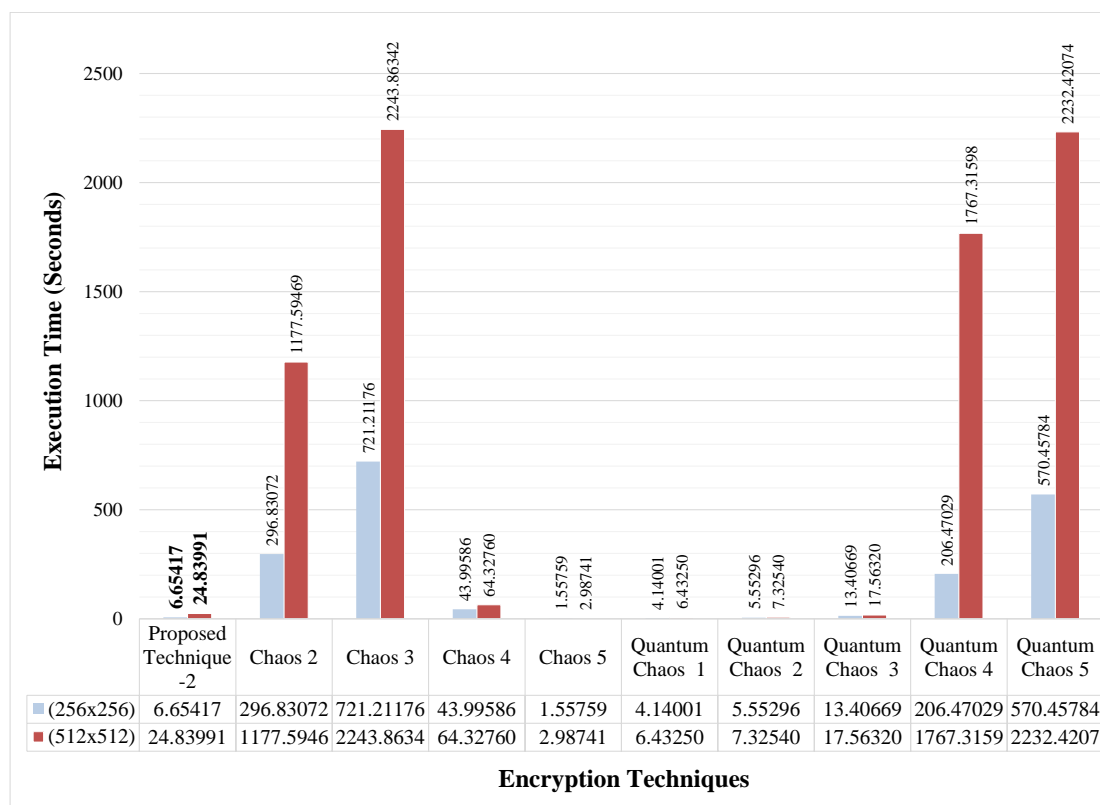


Figure 5.6: Graph Depicting Execution Time of Encryption for Two Different Size Images

5.2.7 Cryptanalysis

The cryptanalysis attack is the most important attack to validate encryption techniques in terms of security. The most well-known cryptanalysis attack is Chosen Plain-text Attack and Known Plain-text Attack. The Chosen Plain-text Attack is the most intimidating attack. It is known that the encryption scheme can resist all other attacks if it can resist the Chosen Plain-text Attack. Like other techniques available in the literature,

our proposed technique has the ability to resist Chosen Plain-text as well as Known Plain-text Attacks.


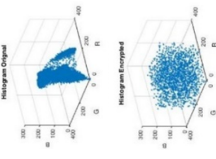
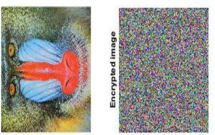
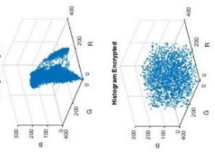
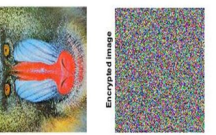
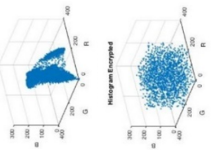
5.3 OVERALL COMPARISON

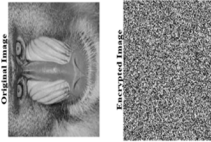
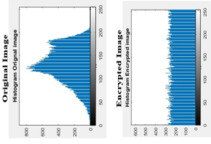
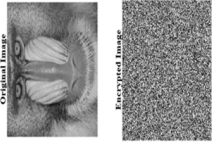
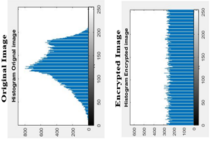
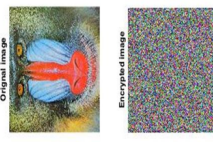
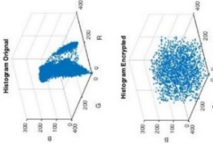
In this chapter, the results of the proposed technique based on Quantum Logistic map are calculated on two different size images. The overall average values of the proposed and studied image encryption techniques are given in Table 5.9.


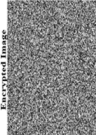

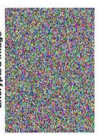
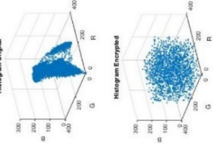

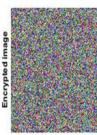
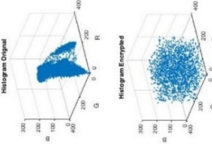
After analyzing the experimental results provided in the Table 5.9, following conclusions are inferred:

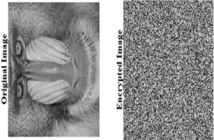
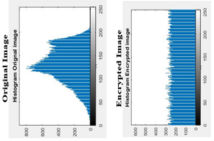
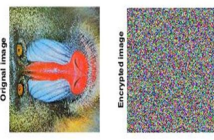
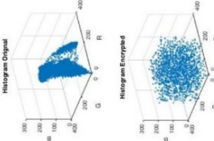

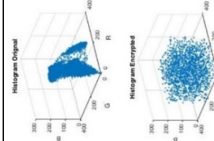
- This technique works on bit planes (24 planes) rather than working on bytes(3 planes) of the colored image, which helps in increasing the amount of randomness of the encrypted image.
- The encryption process is completely dependent on the key values which are generated using the Quantum Chaotic Map with the help of Initial Values and Control Parameters. This implies that our proposed technique can efficiently resist Chosen Plain-text Attack and Known Plaintext Attack.
- The multilevel matching process in the Confusion part consumes less time for execution. Hence, it can be used in wide practical every day applications.
- The multi-directional folding process in the Diffusion part of the proposed technique further enhanced the randomness property of the encrypted image. Also, this is a key dependent Diffusion Process that increases the key space which makes it difficult to retrieve the original information by the unknown receiver.
- The correlation among the pixels of the encrypted image is less than 0 which reflects that there is no continuity available between the adjacent pixels of encrypted image.
- The measured entropy value of the proposed technique is closed to 8. It shows that the encrypted image is highly random.
- The key size of the proposed technique is 2^{432} indicating that it can resist Brute Force Attacks.
- The proposed technique passes all the test levels of NPCR and UACI, because of multilevel matching of Confusion Process applied in bit levels on 24 planes of image.

Table 5.9: Compiled Results of Proposed Technique 2

Performance Metrics/ Techniques	Image Perceptual Quality	Statistical Attack Parameters (Histogram)	Correlation Coefficient (H:Horizontal, V:Vertical, D:Diagonal)	Differential Attack Parameters (NPCR and UACI)	Quantitative Parameters (PSNR and Information Entropy)	Key Space	Execution Time (in Seconds)
Chaos 1			-0.01291(H) -5.24E-03(V) 2.85E-03(D)	NPCR= 99.6280 UACI= 33.4433	PSNR= 27.4251 Entropy= 7.999340	2^{216}	258.688
Chaos 2			-0.00115(H) 4.73E-03(V) 1.98E-03(D)	NPCR= 99.5891 UACI= 33.414	PSNR= 27.2215 Entropy= 7.99933	2^{126} – 2^{147}	737.2129
Chaos 3			-0.00739(H) -4.98E-04(V) 6.92E-03(D)	NPCR= 99.6215 UACI= 33.443	PSNR= 27.2230 Entropy= 7.99941	2^{192}	1482.537

Performance Metrics/ Techniques	Image Perceptual Quality	Statistical Attack Parameters (Histogram)	Correlation Coefficient (H:Horizontal, V:Vertical, D:Diagonal)	Differential Attack Parameters (NPCR and UACI)	Quantitative Parameters (PSNR and Entropy)	Key Space	Execution Time (in Seconds)
Chaos 4			-0.00526(H) -5.42E-03(V) 6.43E-03(D)	NPCR= 99.6462 UACI= 33.466	PSNR= 26.9238 Entropy= 7.99342	2 ³⁸⁴	54.16173
Chaos 5			0.000382(H) 1.38E-03(V) 2.95E-03(D)	NPCR= 99.6092 UACI= 33.4806	PSNR= 27.3468 Entropy= 7.99832	2 ⁴⁴⁸	2.272497
Quantum Chaos 1			0.051004(H) 5.91E-02(V) 2.86E-02(D)	NPCR= 99.6133 UACI= 33.4666	PSNR= 27.2225 Entropy= 7.99938	2 ²²⁴	5.786253

Performance Metrics/ Techniques	Image Perceptual Quality	Statistical Attack Parameters (Histogram)	Correlation Coefficient (H:Horizontal, V:Vertical, D:Diagonal)	Differential Attack Parameters (NPCR and UACI)	Quantitative Parameters (PSNR and Entropy)	Key Space	Execution Time (in Seconds)
Quantum Chaos 2	 		0.042315(H) 7.93E-02(V) 3.63E-02(D)	NPCR= 99.66 UACI= 33.5766	PSNR= 27.3548 Entropy= 7.99541	2^{256}	6.439178
Quantum Chaos 3	 		-0.00598(H) 2.03E-03(V) 2.46E-03(D)	NPCR= 99.6166 UACI= 33.6133	PSNR= 27.6573 Entropy= 7.89497	2^{128}	15.48495
Quantum Chaos 4	 		-0.00031(H) -1.01E-02(V) 3.97E-03(D)	NPCR= 51.99 (Fail) UACI= 33.52	PSNR= 27.8223 Entropy= 7.00380	10^{72}	986.8931

Performance Metrics/ Techniques	Image Perceptual Quality	Statistical Attack Parameters (Histogram)	Correlation Coefficient (H:Horizontal, V:Vertical, D:Diagonal)	Differential Attack Parameters (NPCR and UACI)	Quantitative Parameters (PSNR and Entropy)	Key Space	Execution Time (in seconds)
Quantum Chaos 5			0.009587(H) -1.46E-02(V) 1.05E-02(D)	NPCR= 50.3966 (Fail) UACI= 25.1466	PSNR= 28.0798 Entropy= 7.99851	$> 2^{100}$	1401.439
Proposed Technique 1			-0.00397(H) -2.72E-03(V) -7.95E-03(D)	NPCR= 99.6048 UACI= 30.963 (Fail)	PSNR= 28.2373 Entropy= 7.99940	2^{384}	0.94677
Proposed Technique 2			0.00397(H) -2.72E-03(V) -7.95E-03(D)	NPCR= 99.3633 UACI= 33.1966	PSNR= 27.5701 Entropy= 7.99938	2^{432}	5.24704

- The time of execution of the proposed technique is comparable to almost all the techniques available in the literature. In the proposed technique, the Execution Time is variable as it depends on the key value which is generated with the help of Quantum Chaotic Maps.

All the characteristics of the proposed encryption technique make it useful for preserving image confidentiality on the network, and it is also suitable for real-time applications.

The next chapter provided a conclusion to the research work as well as future directions.

CHAPTER 6

CONCLUSION AND FUTURE SCOPE

6.1 OVERALL CONCLUSION

In the current development, digitization is an indivisible component of each individual entity. Accordingly, it necessitates the safety of relevant electronic data. In addition, information communication should be protected in all aspects. The extensively used solution is cryptography, which is the theme of the study in this research work. The main objectives of the work are the design, development, and testing of the performance of encryption mechanisms to endow with optimal values of vital performance factors like confidentiality, imperceptibility, randomness and speed. Before developing the protection mechanism, available schemes are studied and implemented to understand better the gaps between the ideal and actual performance of the techniques. Consequent to the literature review on existing methods, two protection mechanisms are designed.

In the initial phases of work, the Chaos-based Encryption Techniques were surveyed, and a proposal based on a Chaos Encryption Technique was developed, which outperformed other similar techniques of that period. Afterward, Quantum Chaos-based Cryptography Techniques were developed, and a new encryption scheme was implemented. The overall inferences of the research work are as follows:

- **Image Perceptual Quality:** Both the proposals provides good encrypted image, it is entirely like noise and have no resemblance with original image.
- **Key Space:** The set of all valid, possible, distinct keys of a given crypto-system determines the key space. It must be greater than 2^{100} for resisting brute force attacks with the current computational ability of computers. Both the proposed schemes have a good value of key space (Proposal-1 = 2^{384} and Proposal-2 = 2^{432}) ensuring resistance against brute force search attack.

- **Statistical Attack:** Two parameters are considered for statistical analysis.
 - i. Correlation: The correlation among adjacent pixels of the Encrypted and Plain Image should be as low as possible. In both the proposals, the value is closed to zero ensuring the encrypted image is entirely different from the original one thus ensuring resistance to statistical attacks.
 - ii. Histogram: In both the proposals, the histograms were evenly distributed ensuring that both are not affected by statistical attacks.
- **Time of Execution:** The execution time must be as low as possible for practical usage. The first proposal nearly overpowered all other techniques of its era while the second proposal execution time was good but not the best in comparison to other literature survey techniques.
- **Differential Attacks:** Both of the proposal passed theoretical NPCR test values, but the first proposal failed in passing theoretical UACI value indicating the failure against differential attacks. The second proposal passed both NPCR/ UACI theoretical test values hence was successful against differential attacks.
- **Quantitative Parameters:** In this category, two parameters were taken named as PSNR and Entropy. Both the parameters were found to be fine in comparison to other techniques of literature.

6.2 FUTURE RESEARCH DIRECTIONS

The research work described here revealed the workable techniques enhanced in various features and pointed out numerous probable research guidelines to be investigated in the future. The proposed mechanisms are verified based on numerous performance metrics and validated by comparison with available renowned mechanisms. Both the mechanisms are highly confidential, with complex mathematical computations to make it tedious for anyone to breach the private data. The hardware implementation of methods increases protection standards' swiftness, effectiveness, and consistency. CPLD and FPGA implementations of these software algorithms are proposed for bringing modernism to projected algorithms. In order to use these implemented techniques in working applications, hardware implementation of schemes is recommended for the availability of a readymade electronic hardware tool. Also, in the future, the use of deep learning and machine learning-based techniques can be used to generate random numbers that can not only improve key space but, at the same time, will help in preventing differential attacks.

REFERENCES

- [1] K. Anuradha and P. Naik, “Medical Image Cryptanalysis Using Histogram Matching Bitplane and Adjoin Mapping Algorithms,” *International Journal and Magazine of Engineering, Technology, Management and Research*, vol. 2, pp. 100–105, 2015.
- [2] Z. Hu, S. Petoukhov, I. Dychka, and M. He, *Advances in Computer Science for Engineering and Education II*. Springer International Publishing, 2019, vol. 938.
- [3] L. Alamos, “IEEE Computer Society’s Top 12 Technology Trends for 2020,” [Online]. Available: <https://www.computer.org/press-room/2019-news/ieee-computer-societys-top-12-technology-trends-for-2020>, December 2019, [Accessed: 26-Aug-2021].
- [4] Tanya Editor In Chief, “Latest Technology Trends from 2022 that are Transforming Businesses,” [Online]. Available: <https://www.mobileappdaily.com/future-technology-trends>, July 2019, [Accessed: 02-Jun-2020].
- [5] S. Dhall and S. Gupta, “Multilayered Highly Secure Authentic Watermarking Mechanism for Medical Applications,” *Multimedia Tools and Applications*, vol. 80, no. 12, pp. 18 069–18 105, 2021.
- [6] V. Natoli, “A Decade of Accelerated Computing Augurs Well for GPUs,” [Online]. Available: <https://www.nextplatform.com/2019/07/10/a-decade-of-accelerated-computing-augurs-well-for-gpus/>, Jul 2019, [Accessed: 15-Dec-2019].
- [7] I. Friedberg, M. Wurzenberger, A. Al Balushi, and B. Kang, “From Monitoring, Logging, and Network Analysis to Threat Intelligence Extraction,” in *Collaborative Cyber Threat Intelligence*. Auerbach Publications, 2017, pp. 69–127.
- [8] L. Burita, “Analysis of Reports on Cyber Threats and Attacks Using Text-Analytical Software,” in *ECCWS 2020 20th European Conference on Cyber*

- Warfare and Security*. Academic Conferences and publishing limited, 2020, pp. 50–59.
- [9] Y. G. Zeng, “Identifying Email Threats Using Predictive Analysis,” in *International Conference on Cyber Security And Protection Of Digital Services (Cyber Security)*. IEEE, 2017, pp. 1–2.
- [10] J. Johnson, “Annual Number of Data Compromises and Individuals Impacted in the United States from 2005 to 2022,” [Online]. Available: <https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/>, March 2022, [Accessed: 26-June-2022].
- [11] K. Glamoslja, “Antivirus and Cybersecurity Statistics, Trends & Facts 2023,” [Online]. Available: <https://www.safetydetectives.com/blog/antivirus-statistics/>, Jan 2022, [Accessed: 22-Aug-2022].
- [12] A. Shikder, P. Kumar, and N. K. Nishchal, “Image Encryption by Structured Phase Encoding and Its Effectiveness in Turbulent Medium,” *IEEE Photonics Technology Letters*, vol. 35, no. 3, pp. 128–131, 2023.
- [13] M. Y. Rhee, *Internet Security: Cryptographic Principles, Algorithms and Protocols*. Chichester: Wiley, 2005.
- [14] R. C. Gonzalez, *Digital Image Processing*. 3rd ed. Reading, MA: Addison-Wesley, 2008.
- [15] Y. G. Zeng, “Identifying Email Threats Using Predictive Analysis,” in *2017 International Conference on Cyber Security And Protection Of Digital Services (Cyber Security)*. IEEE, 2017, pp. 1–2.
- [16] P. Jindal and B. Singh, “A Survey on RC4 Stream Cipher,” *International Journal of Computer Network and Information Security*, vol. 7, no. 7, pp. 37–45, 2015.
- [17] A. Lohachab and B. Karambir, “Critical Analysis of DDoS—An Emerging Security Threat over IoT Networks,” *Journal of Communications and Information Networks*, vol. 3, no. 3, pp. 57–78, 2018.
- [18] J. Lopez, R. Roman, and C. Alcaraz, “Analysis of Security Threats, Requirements, Technologies and Standards in Wireless Sensor Networks,” in *Foundations of Security Analysis and Design V Lecture Notes in Computer Science*. Springer, 2009, pp. 289–338.

- [19] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish, and M. M. Fouda, "A New Image Encryption Algorithm for Grey and Color Medical Images," *IEEE Access*, vol. 9, pp. 37 855–37 865, 2021.
- [20] V. Deep, P. Sharma *et al.*, "Analysis and Impact of Cyber Security Threats in India using Mazarbot Case Study," in *International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS)*. IEEE, 2018, pp. 499–503.
- [21] A. Mosenia and N. K. Jha, "A Comprehensive Study of Security of Internet-of-Things," *IEEE Transactions on emerging topics in computing*, vol. 5, no. 4, pp. 586–602, 2016.
- [22] S. Z. Sajal, I. Jahan, and K. E. Nygard, "A Survey on Cyber Security Threats and Challenges in Modern Society," in *2019 IEEE International Conference on Electro Information Technology (EIT)*. IEEE, 2019, pp. 525–528.
- [23] J. Jang-Jaccard and S. Nepal, "A Survey of Emerging Threats in Cybersecurity," *Journal of Computer and System Sciences*, vol. 80, no. 5, pp. 973–993, 2014.
- [24] M. K. Hasan, S. Islam, R. Sulaiman, S. Khan, A.-H. A. Hashim, S. Habib, M. Islam, S. Alyahya, M. M. Ahmed, S. Kamil *et al.*, "Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications," *IEEE Access*, vol. 9, pp. 47 731–47 742, 2021.
- [25] P. Panwar, S. Dhall, and S. Gupta, "A Multilevel Secure Information Communication Model for Healthcare Systems," *Multimedia Tools and Applications*, vol. 80, no. 5, pp. 8039–8062, 2021.
- [26] A. Raheja, R. Chawla, S. Gupta, and A. Vashist, "Controlling Over Enhancement of Images Using Histogram Equalization Technique," in *IOP Conference Series: Materials Science and Engineering*, vol. 804. IOP Publishing, 2020, pp. 1–16.
- [27] S. Ariffi, R. Mahmud, R. Rahmat, and N. A. Idris, "SMS Encryption Using 3D-AES Block Cipher on Android Message Application," in *International Conference on Advanced Computer Science Applications and Technologies*. IEEE, 2013, pp. 310–314.
- [28] D. Braun, "Dissipative Chaotic Quantum Maps: Expectation Values, Correlation Functions and The Invariant State," *The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics*, vol. 11, no. 1, pp. 3–12, 2000.

- [29] G. Ye, K. Jiao, C. Pan, and X. Huang, "An Effective Framework for Chaotic Image Encryption Based on 3D Logistic Map," *Security and Communication Networks*, vol. 2018, pp. 1–11, 2018.
- [30] G. Zhang and Q. Liu, "A Novel Image Encryption Method Based on Total Shuffling Scheme," *Optics communications*, vol. 284, no. 12, pp. 2775–2780, 2011.
- [31] 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.
- [32] M. Chandra and P. Sharma, "Image Encryption Based on Random Scrambling and Chaotic Gauss Iterative Map," *International Journal of Computer Applications*, vol. 157, no. 3, pp. 18–23, 2017.
- [33] A. Malik, S. Jadav, and S. Gupta, "Assessment of Diverse Image Encryption Mechanisms Under Prevalent Invasion," *Multimedia Tools and Applications*, vol. 80, no. 14, pp. 21 521–21 559, 2021.
- [34] N. K. Pareek, V. Patidar, and K. K. Sud, "Image Encryption Using Chaotic Logistic Map," *Image and vision computing*, vol. 24, no. 9, pp. 926–934, 2006.
- [35] A. Malik, S. Dhall, and S. Gupta, "An Improved Bit Plane Image Encryption Technique Using RC4 and Quantum Chaotic Demeanour," *Multimedia Tools and Applications*, vol. 80, no. 5, pp. 7911–7937, 2021.
- [36] A. Joux, "A One Round Protocol for Tripartite Diffie–Hellman," *Journal of Cryptology*, vol. 17, no. 4, pp. 263–276, 2004.
- [37] N. Bourbakis and C. Alexopoulos, "Picture Data Encryption Using Scan Patterns," *Pattern Recognition*, vol. 25, no. 6, pp. 567–581, 1992.
- [38] Q. H. Makki, A. M. Abdalla, and A. A. Tamimi, "A Survey of Image Encryption Algorithms," in *International Conference on Information Technology (ICIT)*. IEEE, 2021, pp. 598–602.
- [39] A. Malik, S. Dhall, and S. Gupta, "An Improved Bit Plane Image Encryption Technique Using RC4 and Quantum Chaotic Demeanour," *Multimedia Tools and Applications*, vol. 80, no. 5, pp. 7911–7937, 2021.
- [40] S. Li, Y. Zhao, B. Qu, and J. Wang, "Image Scrambling Based on Chaotic Sequences and Veginère Cipher," *Multimedia Tools and Applications*, vol. 66, no. 3, pp. 573–588, 2013.

- [41] C.-Y. Lai and K.-M. Chung, “Quantum Encryption and Generalized Shannon Impossibility,” *Designs Codes and Cryptography*, vol. 87, no. 9, pp. 1961–1972, 2019.
- [42] C. Li, S. Li, M. Asim, J. Nunez, G. Alvarez, and G. Chen, “On the Security Defects of an Image Encryption Scheme,” *Image and Vision Computing*, vol. 27, no. 9, pp. 1371–1381, 2009.
- [43] T. Li, B. Du, and X. Liang, “Image Encryption Algorithm Based on Logistic and Two-Dimensional Lorenz,” *IEEE Access*, vol. 8, pp. 13 792–13 805, 2020.
- [44] L. D. Smith, *Cryptography: The science of secret writing*. 1st ed. Reading, New York: Dover Publications, 1955.
- [45] U.S. DEPARTMENT OF COMMERCE/ National Institute of Standards and Technology (NIST), “Data Encryption Standard (DES),” *Federal information processing standards publication 46-3*, pp. 1–22, October 1999.
- [46] M. Thangavel, P. Varalakshmi, M. Murralli, and K. Nithya, “An Enhanced and Secured RSA Key Generation Scheme (ESRKGS),” *Journal of information security and applications*, vol. 20, pp. 3–10, 2015.
- [47] N. Hoffman, “A Simplified IDEA Algorithm,” *Cryptologia*, vol. 31, no. 2, pp. 143–151, 2007.
- [48] B. Schneier, “The Blowfish Encryption Algorithm,” *Dr Dobb’s Journal*, vol. 19, no. 4, pp. 38–40, 1994.
- [49] M. Naor and A. Shamir, “Visual Cryptography,” in *Advances in Cryptology-EUROCRYPT’94 Lecture Notes in Computer Science*, vol. 950. Springer, Berlin, Heidelberg, January 1995, pp. 1–12.
- [50] S. Fluhrer, I. Mantin, and A. Shamir, “Weaknesses in the key scheduling algorithm of RC4,” in *International Workshop on Selected Areas in Cryptography*. Springer, 2001, pp. 1–24.
- [51] R. Rivest, “The RC5 encryption algorithm,” in *International Workshop on Fast Software Encryption*. Springer, 1994, pp. 86–96.
- [52] R. Rivest, M.J.B. Robshaw, R. Sidney2, and Y.L. Yin, “The RC6 Block Cipher,” in *M.I.T. Laboratory for Computer Science, 545 Technology Square, Cambridge, MA 02139, USA*, 1998, pp. 1–21.
- [53] S.S. Keller, “Modes of Operation Validation System for the Triple Data Encryption Algorithm,” *NIST Special Publication 800*, vol. 20, pp. 6–24, 2000.

- [54] U.S. DEPARTMENT OF COMMERCE/ National Institute of Standards and Technology (NIST), “Advanced Encryption Standard (AES),” *Federal information processing standards publication 197*, pp. 5–47, November 2001.
- [55] R. Modugu, Y.-B. Kim, and M. Choi, “Design and Performance Measurement of Efficient IDEA (International Data Encryption Algorithm) Crypto-Hardware Using Novel Modular Arithmetic Components,” in *IEEE Instrumentation & Measurement Technology Conference Proceedings*, 2010, pp. 1222–1227.
- [56] S. Mandal, S. Das, and A. Nath, “Data Hiding and Retrieval Using Visual Cryptography,” *International Journal of Advance Research in Computer Science and Management*, vol. 1, pp. 102–110, 2014.
- [57] D. Singhai and C. Gupta, “An Efficient Image Data Encryption Technique Based on RC4 and Blowfish Algorithm with Random Data Shuffling,” in *Social Networking and Computational Intelligence Lecture Notes in Networks and Systems*. Springer, 2020, vol. 100, pp. 485–494.
- [58] A. H. Koblitz, N. Koblitz, and A. Menezes, “Elliptic Curve Cryptography: The Serpentine Course of a Paradigm Shift,” *Journal of Number Theory*, vol. 131, no. 5, pp. 781–814, 2011.
- [59] S. Chandra, S. Paira, S. S. Alam, and G. Sanyal, “A Comparative Survey of Symmetric and Asymmetric Key Cryptography,” in *International Conference on Electronics, Communication and Computational Engineering (ICECCE)*. IEEE, 2014, pp. 83–93.
- [60] L. Kocarev, “Chaos-Based Cryptography: A Brief Overview,” *IEEE Circuits and Systems Magazine*, vol. 1, no. 3, pp. 6–21, 2001.
- [61] A. Qayyum, J. Ahmad, W. Boulila, S. Rubaiee, F. Masood, F. Khan, and W. J. Buchanan, “Chaos-based Confusion and Diffusion of Image Pixels Using Dynamic Substitution,” *IEEE Access*, vol. 8, pp. 140 876–140 895, 2020.
- [62] G. Veena and M. Ramakrishna, “A Survey on Image Encryption Using Chaos-based Techniques,” *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 1, pp. 379–384, 2021.
- [63] C. Fu, G.-y. Zhang, M. Zhu, Z. Chen, and W.-m. Lei, “A New Chaos-Based Color Image Encryption Scheme With an Efficient Substitution Keystream Generation Strategy,” *Security and Communication Networks*, vol. 2018, pp. 1–13, 2018.

- [64] I. Shatheesh Sam, P. Devaraj, and R. S. Bhuvaneswaran, "An Intertwining Chaotic Maps Based Image Encryption Scheme," *Nonlinear Dynamics*, vol. 69, no. 4, pp. 1995–2007, 2012.
- [65] M. François, T. Grosge, 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.
- [66] I. S. Sam, P. Devaraj, and R. S. Bhuvaneswaran, "A Novel Image Cipher Based on Mixed Transformed Logistic Maps," *Multimedia Tools and Applications*, vol. 56, no. 2, pp. 315–330, 2012.
- [67] 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.
- [68] 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.
- [69] 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.
- [70] 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.
- [71] 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.
- [72] 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.
- [73] X. Liu, D. Xiao, and Y. Xiang, "Quantum Image Encryption Using Intra and Inter Bit Permutation Based on Logistic Map," *IEEE Access*, vol. 7, pp. 6937–6946, 2018.
- [74] G. Ye, K. Jiao, X. Huang, B.-M. Goi, and W.-S. Yap, "An Image Encryption Scheme Based on Public Key Cryptosystem and Quantum Logistic Map," *Scientific Reports*, vol. 10, no. 1, pp. 1–19, 2020.

- [75] 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.
- [76] C. Fu, J.-j. Chen, H. Zou, W.-h. Meng, Y.-f. Zhan, and Y.-w. Yu, "A Chaos-based Digital Image Encryption Scheme With an Improved Diffusion Strategy," *Optics Express*, vol. 20, no. 3, pp. 2363–2378, 2012.
- [77] S. Askar, S. A. Karawia, A, and A. Alshamrani, "Image Encryption Algorithm Based on Chaotic Economic Model," *Mathematical Problems in Engineering*, vol. 2015, pp. 1–10, 2015.
- [78] O. Marques, *Practical Image and Video Processing using MATLAB*. Hoboken, NJ: Wiley-IEEE Press, 2011.
- [79] A. G. Weber, "The USC-SIPI Image Database," [Online]. Available: <http://sipi.usc.edu/database/database.php?volume=misc.>, December 2017, [Accessed: 16-Jan-2018].
- [80] M. Ahmad, M. N. Doja, and M. M. S. Beg, "Security Analysis and Enhancements of an Image Cryptosystem Based on Hyperchaotic System," *Journal of King Saud University-Computer and Information Sciences*, vol. 33, no. 1, pp. 77–85, 2021.
- [81] N. Islam and W. Puech, "Decryption of Noisy Encrypted Images by Statistical Analysis," in *3rd European Workshop on Visual Information Processing*. IEEE, 2011, pp. 192–198.
- [82] K. K. Chennam, L. Muddana, and R. K. Aluvalu, "Performance Analysis of Various Encryption Algorithms for Usage in Multistage Encryption for Securing Data in Cloud," in *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*. IEEE, 2017, pp. 2030–2033.
- [83] B. Ge and H.-B. Luo, "Image Encryption Application of Chaotic Sequences Incorporating Quantum Keys," *International Journal of Automation and Computing*, vol. 17, no. 1, pp. 123–138, 2020.
- [84] E. Biham and A. Shamir, "Introduction to Differential Cryptanalysis," in *Differential Cryptanalysis of the Data Encryption Standard*. Springer, 1993, pp. 11–32.
- [85] F. Özkaynak, "Role of NPCR and UACI Tests in Security Problems of Chaos Based Image Encryption Algorithms and Possible Solution Proposals," in *2017*

- International Conference on Computer Science and Engineering (UBMK)*. IEEE, 2017, pp. 621–624.
- [86] A. Shafique, J. Ahmed, W. Boulila, H. Ghandorh, J. Ahmad, and M. U. Rehman, “Detecting the Security Level of Various Cryptosystems Using Machine Learning Models,” *IEEE Access*, vol. 9, pp. 9383–9393, 2020.
- [87] Y. Wu, J. P. Noonan, and S. Aghaian, “A Novel Information Entropy Based Randomness Test for Image Encryption,” in *IEEE International Conference on Systems, Man, and Cybernetics*. IEEE, 2011, pp. 2676–2680.
- [88] Y. Wu, T. Wang, and J. Li, “Effectiveness Analysis of Encrypted and Unencrypted Bit Sequence Identification Based on Randomness Test,” in *Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC)*. IEEE, 2015, pp. 1588–1591.
- [89] P. Puteaux and W. Puech, “Image Analysis and Processing in the Encrypted Domain,” in *IEEE International Conference on Image Processing (ICIP)*. IEEE, 2019, pp. 3020–3022.
- [90] G. Ye, K. Jiao, X. Huang, B.-M. Goi, and W.-S. Yap, “An Image Encryption Scheme Based on Public Key Cryptosystem and Quantum Logistic Map,” *Scientific Reports*, vol. 10, no. 1, pp. 1–19, 2020.
- [91] V. Kumar, R. Kumar, M. A. Barbhuiya, and M. Saikia, “Multiple Encryption using ECC and its Time Complexity Analysis,” *International Journal of Computer Engineering In Research Trends*, vol. 3, no. 11, pp. 568–572, 2016.
- [92] R. Shelke and S. Metkar, “Image Scrambling Methods for Digital Image Encryption,” in *International Conference on Signal and Information Processing (IconSIP)*. IEEE, 2016, pp. 1–6.
- [93] I. F. Elashry, O. S. F. Allah, A. M. Abbas, and S. El-Rabaie, “A New Diffusion Mechanism for Data Encryption in the ECB Mode,” in *International Conference on Computer Engineering & Systems*. IEEE, 2009, pp. 288–293.
- [94] O. B. Sahoo, D. K. Kole, and H. Rahaman, “An Optimized S-box for Advanced Encryption Standard (AES) Design,” in *International Conference on Advances in Computing and Communications*. IEEE, 2012, pp. 154–157.
- [95] J. S. Teh, M. Alawida, and Y. C. Sii, “Implementation and Practical Problems of Chaos-based Cryptography Revisited,” *Journal of Information Security and Applications*, vol. 50, p. 102421, 2020.

- [96] 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.
- [97] L. Chen, B. Ma, X. Zhao, and S. Wang, “Differential Cryptanalysis of a Novel Image Encryption Algorithm Based on Chaos and Line Map,” *Nonlinear Dynamics*, vol. 87, no. 3, pp. 1797–1807, 2017.
- [98] Buvanewari.V.B, S.Shanthi and M.Pyingkodi, “Big Data Analytics in Map Reduce: Literature Review,” *International Research Journal on Advanced Science Hub*, vol. 3, pp. 38–42, 2021.
- [99] A. Singh and A. Jain, “Study of Cyber Attacks on Cyber Physical System,” in *Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIOTCT)*, 2018.
- [100] S. Al Busafi and B. Kumar, “Review and analysis of cryptography techniques,” in *2020 9th International Conference System Modeling and Advancement in Research Trends (SMART)*. IEEE, 2020, pp. 323–327.
- [101] N. Bourbakis and C. Alexopoulos, “Picture Data Encryption using Scan Patterns,” *Pattern Recognition*, vol. 25, no. 6, pp. 567–581, 1992.
- [102] C. C. Chang, M. S. Hwang, and T. S. Chen, “A New Encryption Algorithm for Image Cryptosystems,” *Journal of Systems and Software*, vol. 58, no. 2, pp. 83–91, 2001.
- [103] Z. Liu, Q. Guo, L. Xu, M. A. Ahmad, and S. Liu, “Double Image Encryption by Using Iterative Random Binary Encoding in Gyration Domains,” *Optics Express*, vol. 18, no. 11, pp. 12 033–12 043, 2010.
- [104] G. Chen, Y. Mao, and C. K. Chui, “A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps,” *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749–761, 2004.
- [105] P. P. Dang and P. M. Chau, “Image Encryption for Secure Internet Multimedia Applications,” *IEEE Transactions on Consumer Electronics*, vol. 46, no. 3, pp. 395–403, 2000.
- [106] Z. Yun Peng, L. Wei, C. Shui Ping, Z. Zheng Jun, N. Xuan, and D. Wei di, “Digital Image Encryption Algorithm based on Chaos and Improved DES,” in *IEEE International Conference on Systems, Man and Cybernetics*. IEEE, 2009, pp. 474–479.

- [107] M. S. Baptista, "Cryptography with Chaos," *Physics letters A*, vol. 240, no. 1-2, pp. 50–54, 1998.
- [108] A. El-Latif, A. Ahmed, L. Li, T. Zhang, N. Wang, X. Song, and X. Niu, "Digital Image Encryption Scheme Based on Multiple Chaotic Systems," *Sensing and Imaging: An International Journal*, vol. 13, no. 2, pp. 67–88, 2012.
- [109] R. Matthews, "On the Derivation of a 'Chaotic' Encryption Algorithm," *Cryptologia*, vol. 13, no. 1, pp. 29–42, 1989.
- [110] G. A. Sathishkumar, K. Bhoopathy bagan, and N. Sriraam, "Image Encryption Based on Diffusion and Multiple Chaotic Maps," *International Journal of Network Security and Its Applications (IJNSA)*, vol. 3, no. 2, pp. 181–194, 2011.
- [111] J. Scharinger, "Fast Encryption of Image Data Using Chaotic Kolmogorov Flows," *Journal of Electronic imaging*, vol. 7, no. 2, pp. 318–325, 1998.
- [112] G. Ye, "Image scrambling encryption algorithm of pixel bit based on chaos map," *Pattern Recognition Letters*, vol. 31, no. 5, pp. 347–354, 2010.
- [113] J. W. Yoon and H. Kim, "An image encryption scheme with a pseudorandom permutation based on chaotic maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 12, pp. 3998–4006, 2010.
- [114] A. Sharif, N. I. Raihana, and A. Samsudin, "Chaos-based Cryptography A Brief Look Into An Alternate Approach to Data Security," *Journal of Physics Conference Series*, vol. 1566, no. 1, pp. 1–4, 2020.
- [115] N. K. Pareek, V. Patidar, and K. Sud, K, "Discrete chaotic cryptography using external key," *Physics Letters A*, vol. 309, no. 1, pp. 75–82, 2003.
- [116] T. Gao and Z. Chen, "A New Image Encryption Algorithm Based on Hyper-Chaos," *Physics letters A*, vol. 372, no. 4, pp. 394–400, 2008.
- [117] E. Solak, C. Cokal, O. T. Yildiz, and T. Biyikoğlu, "Cryptanalysis of Fridrich's Chaotic Image Encryption," *International Journal of Bifurcation and Chaos*, vol. 20, no. 05, pp. 1405–1413, 2010.
- [118] N. Thein, H. A. Nugroho, T. B. Adj, and I. W. Mustika, "Comparative Performance Study on Ordinary and Chaos Image Encryption Schemes," in *international conference on advanced computing and applications (ACOMP)*. IEEE, 2017, pp. 122–126.

- [119] S. Bhandari, "A New Era of Cryptography: Quantum Cryptography," *International Journal on Cryptography and Information Security*, vol. 6, no. 3/4, pp. 31–37, 2016.
- [120] C. Fatima and D. Ali, "New chaotic binary sequences with good correlation property using logistic maps," *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)*, vol. 5, no. 3, pp. 59–64, 2013.
- [121] D. Lambić, "Security Analysis and Improvement of the Pseudo-random Number Generator Based on Quantum Chaotic Map," *Nonlinear Dynamics*, vol. 94, no. 2, pp. 1117–1126, 2018.
- [122] W. H. Al-Hilli and R. A. Kamel, "Some Properties of Chaotic Modified of Bogdanov Map," *Journal of Advances in Mathematics*, vol. 20, no. 1, pp. 135–140, 2021.
- [123] J. Peng, S. Pang, D. Zhang, S. Jin, L. Feng, and Z. Li, "S-boxes Construction Based on Quantum Chaos and PWLCM Chaotic Mapping," in *IEEE 18th International Conference on Cognitive Informatics & Cognitive Computing (ICCI* CC)*. IEEE, 2019, pp. 1–6.
- [124] P. Bonavoglia, "Trithemius, Bellaso, Vigenère-Origins of the Polyalphabetic Ciphers," in *Proceedings of the 3rd International Conference on Historical Cryptology HistoCrypt 2020*, vol. 171. Linköping University Electronic Press, 2020, pp. 46–51.
- [125] A. Shah, "Enhancing Security of Vignere Cipher using Modified RC4," *International Journal of Computer Applications*, vol. 136, no. 5, pp. 38–41, 2016.
- [126] M. Matsui, "The First Experimental Cryptanalysis of the Data Encryption Standard," in *CRYPTO '94: 14th Annual International Cryptology Conference on Advances in Cryptology*, Y. G. Desmedt (Ed.) Springer Berlin Heidelberg, vol. 839. Springer, 1994, pp. 1–11.
- [127] J. Chen, D. Xue, and X. Lai, "An Analysis of International Data Encryption Algorithm (IDEA) Security Against Differential Cryptanalysis," *Wuhan University Journal of Natural Sciences*, vol. 13, no. 6, pp. 697–701, 2008.
- [128] D. E. Standard *et al.*, "Data encryption standard," *Federal Information Processing Standards Publication*, vol. 112, 1999.
- [129] Atikah, M. R. Ashila, D. R. Ignatius Moses Setiadi, E. H. Rachmawanto and C. A. Sari, "AES-RC4 Encryption Technique to Improve File Security," in *2019*

- Fourth International Conference on Informatics and Computing (ICIC)*. IEEE, 2019, pp. 1–5.
- [130] L. Kocarev and G. Jakimoski, “Pseudorandom bits generated by chaotic maps,” *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 50, no. 1, pp. 123–126, 2003.
- [131] L. P. Gagnani and S. Varjani, “Survey of 3D Chaotic Map Techniques for Image Encryption,” *International Journal of Science and Research (IJSR)*, vol. 4, no. 12, pp. 1000–1004, 2015.
- [132] K. Xu and F. MENG, “Value-at-Risk Quantitative Method about Password Chip under Differential Power Analysis Attacks,” *Journal of Computer Applications*, vol. 33, no. 06, pp. 1642–1645, 2013.
- [133] M. Khan and T. Shah, “A Novel Statistical Analysis of Chaotic S-box in Image Encryption,” *3D Research*, vol. 5, no. 3, pp. 1–8, 2014.
- [134] T. T. Wontchui, J. Y. Effa, H. P. E. Fouda, and J. Fouda, “Dynamical Behavior of Peter-De-Jong Map using the Modified 0-1 and 3ST Tests for Chaos,” *Annual Review of Chaos Theory, Bifurcations and Dynamical Systems (ARCTBDS)*, vol. 7, pp. 1–21, 2017.
- [135] H. Zhu, Y. Zhao, and Y. Song, “2D Logistic-Modulated-Sine-Coupling-Logistic Chaotic Map for Image Encryption,” *IEEE Access*, vol. 7, pp. 14 081–14 098, 2019.
- [136] M. Goggin, B. Sundaram, and P. Milonni, “Quantum Logistic Map,” *Physical review A*, vol. 41, no. 10, pp. 5705–5708, 1990.
- [137] A.-W. S. Ibrahim and H. J. Sartep, “Grayscale Image Coloring by using YCbCr and HSV Color Spaces,” *International Journal Modern Trends Engineering and Research (IJMTER)*, vol. 4, no. 4, pp. 130–136, 2017.
- [138] H.-K. Tso, “Meaningful Image Sharing Scheme using Toral Automorphism,” *Nonlinear Dynamics*, vol. 75, no. 1, pp. 1–6, 2014.
- [139] A. Mojahed, L. A. Bergman, and A. F. Vakakis, “New Inverse Wavelet Transform Method with Broad Application in Dynamics,” *Mechanical Systems and Signal Processing*, vol. 156, pp. 107 691–107 699, 2021.
- [140] X.-y. Wang and X.-m. Bao, “A Novel Block Cryptosystem Based on the Coupled Chaotic Map Lattice,” *Nonlinear Dynamics*, vol. 72, no. 4, pp. 707–715, 2013.

- [141] D. Fang and S. Sun, "A New Secure Image Encryption Algorithm Based on a 5D Hyperchaotic Map," *PloS ONE*, vol. 15, no. 11, pp. 1–13, 2020.
- [142] P. Howard, "2018 cyber security predictions vs. reality for Cyber Security Awareness," [Online]. Available: <https://thecybermaniacs.com/cm-blog/2018-cyber-security-predictions-vs.-reality>, May 2018, [Accessed: 17-Feb-2019].
- [143] E. Barker and N. Mouha, "Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher," National Institute of Standards and Technology (NIST), Gaithersburg, MD, Tech. Rep., 2017.
- [144] G. Batey and H. Waine, "Safe internet access for service users: Glenn Batey and Helen Waine explore vulnerable people's access to the internet and social networking sites, and why staff should acquire digital professionalism," *Learning Disability Practice*, vol. 18, no. 3, pp. 16–20, 2015.
- [145] B. Schneier, "Description of a New Variable-length Key, 64-Bit Block Cipher (Blowfish)," in *International Workshop on Fast Software Encryption*, vol. 809. Springer, 1993, pp. 191–204.
- [146] Q. Ran, L. Yuan, and T. Zhao, "Image encryption based on nonseparable fractional fourier transform and chaotic map," *Optics Communications*, vol. 348, pp. 43–49, 2015.
- [147] A. Akhshani, A. Akhavan, A. Mobaraki, S.-C. Lim, and Z. Hassan, "Pseudo Random Number Generator Based on Quantum Chaotic Map," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 1, pp. 101–111, 2014.

BRIEF PROFILE

MANJU KUMARI

Assistant Professor

Department of Electronics Engineering

J.C.Bose University of Science and Technology, YMCA,

Sector-6, Faridabad

✉ manjukumari@jcboseust.ac.in;

manjunimesh88@gmail.com

☎ 9891659175

Area of Interest: Digital Image Processing, Network Security, MATLAB Programming, Digital Signal Processing, Wireless Sensor Networks, Bio-medical Instrumentation

Carrier Background: Currently working in JCBUST, YMCA, Faridabad in department of Electronics Engineering at the post of Assistant Professor since 2012.

Educational Qualification: Received Bachelor of Engineering in Electronics and Communication Engineering in 2009 from Manav Rachana College of Engineering, Faridabad (Affiliated From M.D. University, Rohtak) Haryana and Master of Technology in Electronics and Communication Engineering in 2011 from Deenbandhu Chotu Ram University of Science and Technology, Murthal (Sonipat), Haryana.

Research Work: 07 Publications in SCI/SCIE/SCOPUS/reputed journals and 4 papers presented in conferences.

LIST OF PAPERS PUBLISHED IN INTERNATIONAL JOURNALS

S. No.	Title of the Paper along with Volume, Issue No, Year of Publication	Publisher	Impact Factor	Referred or Non-Referred	Whether you paid any money or not for Publication	Cited By	Remarks
1.	A Survey of Image Encryption Algorithms, Vol.8, 37, November 2017	3D Research, Springer Nature-2017	1.615	Referred	No	87	ESCI/ SCOPUS/ UGC Approved
2.	A Novel Image Encryption Scheme Based on Intertwining Chaotic Maps and RC4 Stream Cipher, Volume 9, 10, March 2018	3D Research, Springer Nature-2018	1.73	Referred	No	21	ESCI/ SCOPUS/ UGC Approved
3.	A Superlative Image Encryption Technique Based on Bit Plane using Key-based Electronic Code Book, Volume 79, 11, August 2020	Multimedia Tools and Applications, Springer Nature 2020	2.917	Referred	No	7	SCIE/ SCI
4.	Performance Comparison Between Chaos and Quantum Chaos Based Image Encryption Techniques, Volume 80, 24, October 2022	Multimedia Tools and Applications, Springer Nature-2021	2.917	Referred	No	6	SCIE/ SCI

LIST OF PAPERS PRESENTED IN INTERNATIONAL CONFERENCES

S. No.	Title of the Paper along with Volume, Issue No, Date of Conference	Presented In	Organized By	Whether you paid any money or not for Conference	Remarks
1.	Comparison of Chaotic and Quantum Chaotic Image Encryption Techniques, 17-19 October, 2019	International Conference on Applied Mathematics and Computational Sciences 2019	Dehradun Institute of Technology, Dehradun(Uttarakhand)	Yes	ICAMCS-2019
2.	Performance Comparison of Quantum Chaos Based Image Encryption Techniques, 29-30 June, 2020	International Conference on Smart Modernistic in Electronics and Communication 2020	St. Martin's Engineering College, Dhulapally, Secunderabad, Telangana, India	Yes	ICSMEC-2020
3.	A Survey of Image Encryption Schemes Based on Chaos Theory, 1-3 March, 2017	11th INDIACom-2017/ 4th International Conference on Computing for Sustainable Global Development 2017	Bharti Vidyapeeth's Institute of Computer Applications and Management, New Delhi	Yes	IEEE Conference ID: 40353