

**SOME STUDIES ON INFORMATION SECURITY
SERVICES AND THEIR MECHANISMS**

A THESIS

SUBMITTED TO THE DELHI TECHNOLOGICAL UNIVERSITY
FOR THE AWARD OF THE DEGREE OF
DOCTOR OF PHILOSOPHY

SUBMITTED BY

ASHISH KUMAR



**DEPARTMENT OF INFORMATION TECHNOLOGY
DELHI TECHNOLOGICAL UNIVERSITY
DELHI, INDIA**

2020

SOME STUDIES ON INFORMATION SECURITY SERVICES AND THEIR MECHANISMS

By

ASHISH KUMAR

(2K14/PHD/IT/06)

Submitted in fulfillment of the requirement of the degree of

DOCTOR OF PHILOSOPHY



Supervisor

Prof. N. S. Raghava

Department of Electronics & Communication Engineering
Delhi Technological University
New Delhi

**DEPARTMENT OF INFORMATION TECHNOLOGY
DELHI TECHNOLOGICAL UNIVERSITY
DELHI, INDIA**

2020

DECLARATION

I hereby declare that the thesis entitled "**Some Studies on Information Security Services and their Mechanisms**" to be submitted in fulfillment of the requirements for the award of the degree of Doctor of Philosophy in the Department of Information Technology of the Delhi Technological University, Delhi is an authentic record of my own work carried out under the supervision of Prof. N. S Raghava. The thesis has not been submitted either in part or whole to any university or institute for the award of any degree or diploma.

Place: **DTU, Delhi**

ASHISH KUMAR

Date:

(2K14/PHD/IT/06)

CERTIFICATE

This is to certify that the thesis entitled "**Some Studies on Information Security Services and their Mechanisms**" being submitted by **Ashish Kumar** to the Department of Information Technology, Delhi Technological University, Delhi, for the award of the degree of Doctor of Philosophy, is a record of bonafide research work carried out by him under my guidance and supervision. In my opinion, the thesis has reached the standards fulfilling the requirements of the regulations relating to the degree.

The results contained in this thesis have not been submitted to any other university or institute for the award of any degree or diploma.

Supervisor

Prof. N. S. RAGHAVA

Professor & HOD

Department of Electronics and Communication Engineering

Delhi Technological University, Delhi

ACKNOWLEDGMENTS

Thank you, God, for giving me the strength to keep going on the right path and for all the people around me who make life more meaningful and happier.

This thesis work has been an exciting and amazing journey and I am indebted to acknowledge a few people who made this journey successful.

First and foremost, it is a great pleasure to express my sincere gratitude and appreciation to my supervisor Prof. N. S. Raghava. It is my honor to work under the supervision of such a kind man of values and great expertise. The completion of my thesis work was an uphill task and without the constant support and suggestions of Prof. N. S. Raghava, this thesis would not have seen the light of the day. He is a professor of wide acclaim and profound knowledge whose valuable guidance and consistent scholarly inputs have helped me to form the basis of this work.

My extended thanks go to Prof. Kapil Sharma (Head of Dept. of IT), Prof. O. P. Verma, faculty and staff of the Department of Information Technology, for their assistance and encouragement during my research work.

In this academic journey, all my friends have been a source of encouragement and I am happy to have friends like Dr. Rahul Bansal, Amit Gautam, Rehaan, Akhilesh Verma. Their unbounded support in my personal and professional life made me complete this work. Thank you for inspiring me and occasionally pushing me to certain deadlines.

I am also thankful to UGC for providing the fellowship for financial support.

To my sisters, Suman Singh and Preeti, brothers Mr. Ravindra Kumar and Mr. Vinod Kumar, Brother-in-Law Mr. Madan Singh and all the children from family, your love and compassion have helped me to sail through the tough times. The fruitful discussions with you have saved me in the darkest hours. I am also thankful to my in-laws Mrs. Savitri, Mr. Ram Swarup, Neeraj and Naveen for their support and compassion.

I am forever indebted to my parents Mrs. Ashrafi Devi and Mr. M Lal, for their unfettered love, invaluable blessings and unwavering belief in me. I dedicate this thesis to my parents. Thank you for teaching me lessons of life with your experiences. This thesis is your dream come true. I owe them everything.

Finally, this is the word of acknowledgment I have saved for my dear wife Jyoti Swarup and my children Ashwika and Anvit. They are the pillars of strength of my life. My heartfelt gratitude for my partner who witnessed this journey with me with deep insight and supported me unconditionally with her love. My children have been the continuous source of energy in my life, whose smile transforms my dull moments instantly. Thank you for being there with me round the clock.

New Delhi, 2020

Ashish Kumar

ABSTRACT

Multimedia is an emerging field that deals with different forms of information such as text, images, audio, sensor data and videos in an integrated manner. The advancement of devices to display multimedia and enabling them to transfer it from one location to another has resulted in increasing danger of their security services. Because of this, the secrecy of information is a critical component while transmitting or storing such information. In a hostile environment, security services are required as per the organizations and individuals need to protect their valuable information and resources. In this context, over the past two decades, dynamic systems and other practices have emerged with cryptography to provide security services like confidentiality, authentication, integrity and non-repudiation. With the advancement of technologies, various attacks are also updated with time. Hence comes the need for revised versions of mechanisms to resist such attacks. Several methodologies are implemented that are usually based upon symmetric and asymmetric key cryptography, which uses different algorithms. Billions of people are getting connected to each other through the Internet and exchange a large amount of personal information over the network. It becomes very important to secure such sensitive information from unauthorized users. This thesis work is primarily based on security services and their proposed mechanisms. This thesis begins with the study and comparative analysis of cryptography and several chaotic systems.

Moreover, this thesis also discusses dynamic systems and other existing techniques. The complete study can be classified as an investigation and identification of several objectives, which are segregated into three major categories of inter-related problems. Every problem is addressed by proposing two different models for the solution. Since digital images are used frequently for communication, the first two problems are identified for digital images to achieve authentication and confidentiality in communication. The third problem is formulated to secure information in IoT networks. Based on these problems, real-time application for the examination system is proposed to preserve integrity in academic institutes, which was implemented during Mid Sem Examinations in DTU in 2018, which is addressed in chapter 6.

Generally, image encryption techniques are based upon symmetric-key cryptography schemes, in which the original image is converted into a cipher image. Image encryption has a significant role in internet communication, multimedia systems, medical imaging, telemedicine, and military communication. Traditional cryptosystems are not suitable for images for

encipherment purposes due to the statistical properties of an image. The objective of this research is to develop mechanisms to obtain security services. We have developed light-weighted cryptosystems for images and bulky-sized data to achieve suitable and excellent results. Digital images hold an important role in multimedia communications in the modern era, where multimedia transfers are done at a rapid pace. With the advent of internet-of-things (IoT) applications, these transfers have become a common practice. However, providing security to sensitive data is an essential and challenging task in case of IoT applications due to the limitations of the sensors in terms of memory and computational efficiency. Therefore, conventional ciphers cannot be applied in the IoT devices. Thus, two different methods have been proposed as follow:

1. Efficient light-weighted image encryption techniques

- (a) **Model 1:** An efficient image encryption scheme using elementary cellular automata with a novel permutation box.
- (b) **Model 2:** An efficient image encryption scheme based on an electromagnetic rotor machine.

The second solution is based on partial or selective image encryption schemes. These algorithms are designed on the amount of encryption involved. So, it deals with the partial image encryption schemes. They are as follow:

2. Selective image encryption schemes

- (a) **Model 1:** DWT based image encryption scheme in frequency domain
- (b) **Model 2:** ROI based image encryption scheme in spatial domain

In the third problem, we have also examined the security issues in the Internet of things (IoT) based devices. IoT devices have limited memory and fewer computational capabilities than other devices. It supports only predefined operations and performs a statistical calculation to identify environmental data, current demand, production cost, faults, etc. Steganography techniques based on frequency transform and chaotic maps are proposed to achieve confidentiality, integrity and authentication. The first solution is designed for smart meters, and the second solution helps to secure information of sensor data in the battlefield.

3. Steganography technique to secure information and integrity preservation of systems in IoT network

- (a) **Model 1** - Chaos-based steganography technique to secure information and integrity preservation of smart grid readings
 - (b) **Model 2**- Internet of Battlefield thing Security: A strategy to secure sensitive information using reversible steganography scheme.
- 4. We have designed algorithms to develop a real-time application that maintains academic integrity and prevents students' fraudulent behavior by the allocation of seats during examinations.

LIST OF PUBLICATIONS

Journals

1. Kumar Ashish, and N. S. Raghava. "Chaos-based steganography technique to secure information and integrity preservation of smart grid readings using wavelet." *International Journal of Computers and Applications*, pp. 1-7. ISSN:1206-212X (Print) 1925-7074, 2019. (Online) <https://doi.org/10.1080/1206212X.2019.1692511>. (Scopus Indexed)
2. Ashish Kumar, and N. S. Raghava. "Selective colour image encryption using Hénon chaotic system with a keyless substitution cipher." *Engineering and Applied Science Research*, 47.1, pp. 66-76, 2020. (Scopus Indexed)
3. Ashish Kumar, N. S. Raghava, " Adaptive Sifting Plan Algorithm Based on Henon Chaotic Map", ISSN(Online):2277-8616, *International Journal Of Scientific & Technology Research*, Volume 8, Issue 07, pp.800-805, July 2019. (Scopus Indexed)
4. Kumar Ashish, and N. S. Raghava, "A Novel Group-Based Cryptosystem Based on Electromagnetic Rotor Machine.", ISSN(Online):2250-0138 ISSN(Print): 0976-2876, *Indian J. Sci. Res* 16.2, pp. 131-136, 2017.

Conferences

1. Ashish Kumar, N S Raghava, " chaos based image encipherment techniques: analysis and comparative review," *International Conference on Innovations in Cyber Physical System (ICICPS-2020)*, Communicated in *Lecture Notes in Electrical Engineering Springer*". HMRITM, New Delhi, India, October 2020. (Scopus Indexed)
2. Ashish Kumar, N S Raghava, "Wavelet based Selective Image Encryption scheme using Tinkerbell Chaotic Map," *2nd International Conference on Communication, Networks and Computing (CNC-2019)*, ITM University, Gwalior, India, December 2020. (Scopus Indexed)
3. Ashish Kumar, N.S. Raghava "A Novel Group-Based Cryptosystem Based on Electromagnetic Rotor Machine," *International Conference on Contemporary issues in*

Science, Engineering & Management (ICCI-SEM- 2K17), pp. 278-282, Feb 2017. (best paper award)

Communicated

Two manuscripts are communicated in international journals

- Ashish Kumar and N S Raghava, An Efficient Image Encryption Scheme Using Elementary Cellular Automata with Novel Permutation Box. (under revision)
- Ashish Kumar and N S Raghava, Internet of Battlefield things Security: A Strategy to Secure Sensitive Information using Reversible Steganography Scheme. (under revision)

LIST OF ABBREVIATIONS

ABBREVIATION	DETAIL
AES	Advanced Encryption Standard
ALU	Arithmetic Logical Unit
BER	Bit Error Ratio
CEB	Contrast Enhancement based Filter
CRN	Cognitive Radio Network
DES	Data Encryption Standard
ECA	Elementary Cellular automata
EEP	Efficient Edge Preserving filter
HEIND	Highly Effective Impulse Noise Detection
IoBT	Internet of Battlefield Things
IoMT	Internet of Military Things
LAN	Local Area Network
MDC	Message Detection Code
MED	Median
MFCCs	Mel Frequency Cepstral Coefficients
MSE	Mean Square Error
NPCR	Number of Changing Pixel Rate

OTP	One Time Pad
P Box	Permutation Box
PDF	Probability Distribution Function
PLP	Perceptual Linear Predication
PRNG	Pseudo Random Number Generator
PSNR	Peak Signal to Noise Ratio
RGB	Red Green Blue
ROI	Region of Interest
S Box	Substitution Box
SDOD	Standard Deviation for obtaining the Optimal Direction
SSIM	Structural Similarity Index Measure
UACI	Unified Averaged Changed Intensity
WSN	Wireless Sensor Network

TABLE OF CONTENTS

ACKNOWLEDGEMENTS.....	iii
ABSTRACT.....	iv
LIST OF PUBLICATIONS.....	viii
LIST OF FIGURES.....	xvii
LIST OF TABLES.....	xxi
CHAPTER 1.....	1
1.1 SECURITY	1
1.1.1 INFORMATION SECURITY	1
1.1.2 NETWORK SECURITY	2
1.1.3 PRINCIPLES OF SECURITY	2
1.2 NETWORK SECURITY MODEL	7
1.3 MULTIMEDIA	8
1.4 CRYPTOGRAPHY	8
1.4.1 CLASSIC CRYPTOGRAPHY	9
1.4.2 TYPES OF CRYPTOGRAPHY	11
1.5 CRYPTANALYSIS ATTACK	17
1.5.1 BRUTE-FORCE ATTACK.....	17
1.5.2 CRYPTANALYSIS.....	17
1.5.3 TYPES OF CRYPTANALYSIS ATTACK	18
1.6 KEY TERMS	19
1.6.1 CRYPTOSYSTEM.....	19

1.6.2	ONE-TIME PAD	19
1.6.3	EAVESDROPPING.....	19
1.6.4	CONFUSION AND DIFFUSION	20
1.7	PROBLEM DEFINITION	21
1.8	RESEARCH QUESTION AND OBJECTIVES.....	22
1.9	CONTRIBUTION AND THESIS OVERVIEW	25
CHAPTER 2		29
2.1	INTRODUCTION OF CHAOS THEORY.....	29
2.1.1	HISTORY OF CHAOS THEORY	30
2.1.2	CHAOTIC SYSTEMS.....	31
2.1.3	ATTRACTOR.....	31
2.2	CHAOTIC MAPS	32
2.2.1	ONE-DIMENSIONAL CHAOTIC MAPS.....	32
2.2.2	TWO-DIMENSIONAL CHAOTIC MAPS.....	33
2.2.3	HENON MAP.....	35
2.2.4	TINKERBELL CHAOTIC MAP	37
2.2.5	ARNOLD CAT MAP	37
2.3	CHAOS BASED CRYPTOGRAPHY	38
2.4	EXPERIMENTAL RESULTS AND OBSERVATIONS.....	41
2.5	TEST CASES FOR PERFORMANCE MEASURES	44
2.5.1	ENTROPY ANALYSIS	45
2.5.2	CORRELATION ANALYSIS.....	45
2.5.3	HISTOGRAM ANALYSIS	46
2.5.4	KEY SENSITIVITY TEST	46
2.5.5	DIFFERENTIAL ATTACK.....	47

2.5.6	KEYSPACE ANALYSIS	48
2.5.7	PERCEPTUAL SECURITY: PEAK SIGNAL-TO-NOISE RATIO (PSNR)...	48
2.5.8	MEAN VALUE ANALYSIS	49
2.6	SUMMARY	49

CHAPTER 3..... 51

3.1	PRELIMINARIES	51
3.2	EFFICIENT IMAGE ENCRYPTION SCHEME USING ELEMENTARY CELLULAR AUTOMATA WITH NOVEL PERMUTATION BOX.....	52
3.2.1	CONCEPT OF ELEMENTARY CELLULAR AUTOMATA	55
3.2.2	PROPOSED ALGORITHM	60
3.2.3	EXPERIMENTAL RESULTS.....	66
3.3	AN EFFICIENT IMAGE ENCRYPTION SCHEME BASED ON ELECTROMAGNETIC ROTOR MACHINE	77
3.3.1	PROPOSED ALGORITHM	79
3.3.2	EXPERIMENTAL RESULTS.....	84
3.4	CONCLUSION AND DISCUSSION	89

CHAPTER 4..... 90

4.1	PREMILIARIES	90
4.2	RELATED WORK	92
4.3	DWT BASED IMAGE ENCRYPTION SCHEME IN FREQUENCY DOMAIN .93	
4.3.1	PRIMARILY BACKGROUND	95
4.3.2	PROPOSED ALGORITHM	96
4.3.3	EXPERIMENTAL RESULTS.....	99
4.4	ROI BASED IMAGE ENCRYPTION SCHEME IN SPATIAL DOMAIN	102
4.4.1	REGION-BASED SELECTIVE ENCRYPTION ALGORITHM	104

4.4.2	EXPERIMENTAL RESULTS.....	109
4.5	COMPARATIVE ANALYSIS WITH THE EXISTING TECHNIQUES	116
4.6	CONCLUSION	118
CHAPTER 5.....		120
5.1	INTRODUCTION.....	120
5.2	STEGANOGRAPHY ALGORITHM TO SECURE INFORMATION AND INTEGRITY PRESERVATION OF SMART GRID READINGS	122
5.2.1	CHARACTERISTICS OF SMART GRID SYSTEM.....	123
5.2.2	SECURITY THREATS TO SMART GRID SYSTEMS	125
5.2.3	HÉNON CHAOTIC MAP	126
5.2.4	WAVELET TRANSFORM.....	126
5.2.5	PROPOSED ALGORITHM	127
5.2.6	EXPERIMENTAL RESULTS.....	130
5.3	INTERNET OF BATTLEFIELD THING SECURITY: A STRATEGY TO SECURE SENSITIVE INFORMATION	137
5.3.1	SECURITY THREATS TO BATTLEFIELD AREA	140
5.3.2	BACKGROUND	141
5.3.3	PROPOSED ALGORITHM	143
5.3.4	EXPERIMENTAL RESULTS.....	147
5.4	CONCLUSION	156
CHAPTER 6.....		157
6.1	BACKGROUND AND AIMS	157
6.2	PROPOSED ALGORITHM	159
6.2.1	ADAPTIVE SITTING ALLOCATION ALGORITHM	160
6.2.2	RANDOM SITTING ALLOCATION USING HENON CHAOTIC MAP	164

6.3	EXPERIMENTAL RESULTS AND DISCUSSION.....	166
6.4	CONCLUSION AND FUTURE WORK.....	166
CHAPTER 7..... 168		
7.1	SUMMARY OF THE WORK.....	168
7.2	CONTRIBUTIONS AND FUTURE WORK.....	171

LIST OF FIGURES

Figure 1.1 Loss of confidentiality	3
Figure 1.2 Absence of authentication	4
Figure 1.3 Loss of integrity.....	4
Figure 1.4 Establishing non-repudiation.....	5
Figure 1.5 Attack on availability	5
Figure 1.6 Network security model	7
Figure 1.7 Block diagram of cryptography.....	11
Figure 1.8 Symmetric-key encryption process	12
Figure 1.9 Stream cipher.....	13
Figure 1.10 Block cipher based on output feedback mode encryption.....	15
Figure 1.11 Asymmetric key cryptography process.	15
Figure 1.12 Thesis overview.....	28
Figure 2.1 Two dimensional representation of Henon Map	36
Figure 2.2 Relationship between chaotic systems and cryptography	39
Figure 2.3 Structural similarity index measures of chaotic maps	42
Figure 2.4 Sequence generation time analysis of chaotic maps.....	43
Figure 3.1 The architecture of the proposed algorithm (Model 1)	53
Figure 3.2 Cellular automata boundary conditions.....	56
Figure 3.3 Flowchart of rule space investigation and extraction for rule tables.....	58
Figure 3.4 Keyed transposition scheme	61
Figure 3.5 Visual representation of encryption algorithm	64
Figure 3.6 Visual illustration of plain images :(a) Leena (b) Baboon (c) Airplane (d) Peppers (e) Barbara; shuffled images in the same order : :(f) Leena (g) Baboon (h) Airplane (i) Peppers (j) Barbara; Encrypted images : :(k) Leena (l) Baboon (m) Airplane (n) Peppers (o) Barbara ; Decrypted images obtained by the proposed algorithm : :(p) Leena (q) Baboon (r) Airplane (s)	

Peppers (t) Barbara	68
Figure 3.7 Visual representation of color image at sender end (a) Input test image :Lena , (b) Shuffled image of Lena after applying P BOX(c) Encrypted image of Lena. Visual representation of color image at receiver end by the proposed scheme: (d) Encrypted image (e) Image after applying CA based cryptosystem (f) Decrypted image	69
Figure 3.8 Correlation plot of two adjacent plain-image pixels of Leena in horizontal direction for the (a) red channel, (b) green channel, and (c) blue channel. Correlation plot of two adjacent pixels of the cipher-image obtained by the proposed scheme: (d) red channel (e) green channel (f) blue channel	72
Figure 3.9 Histogram plot of grayscale Images:(a) Leena (b) Baboon (c) Airplane (d) Peppers (e) Barbara; Histogram of encrypted images by the proposed scheme: (:f) Leena (g) Baboon (h) Airplane (i) Peppers (j) Barbara	73
Figure 3.10 Key Sensitivity analysis (a) Leena (I), (b) cipher image with a wrong encryption key.....	74
Figure 3.11 Proposed architecture of Model 2 based on rotor machine	78
Figure 3.12 (a) War-damaged Enigma rotor A7135 (b) Three rotors on their shaft (c) Original Enigma "D" Reflector number A5221 [206], [207].....	79
Figure 3.13 wire connections within Rotor.....	81
Figure 3.14 Pseudo-random numbers for wire connections within the Rotor	82
Figure 3.15 PLP coefficients of voice sample	84
Figure 3.16 Lena Image: (a) original image (b) cipher image; Cameraman Image (c) Original image (b) Cipher image	85
Figure 3.17 Lena Image: (a) cipher image (b) Decrypted image; Cameraman Image (c) cipher image (b) Decrypted image.....	86
Figure 3.18 Histogram analysis of the proposed algorithm	88
Figure 3.19 Mean value analysis (cameraman)	88
Figure 4.1 Selective image encryption schemes	91
Figure 4.2 Schematic diagram of the proposed architecture.....	94

Figure 4.3 Encryption module of the proposed algorithm	98
Figure 4.4 Cipher image results of the proposed algorithm (a) Original image of Barbara (b) Encrypted image of Barbara (c) Original image of baboon (d) Encrypted image of baboon	100
Figure 4.5 Histogram Analysis (a) Original image of Barbara (b) Encrypted image of Barbara (c) Original image of baboon (d) Encrypted image of Baboon	100
Figure 4.6 Architecture of the proposed algorithm.....	102
Figure 4.7 Flow chart: Adaptive ROI based segmentation.....	104
Figure 4.8 Keyless Bit level substitution algorithm (a) keyless substitution at the sender end, (b) keyless substitution at receiver's end.....	106
Figure 4.9 Diffusion based on Hénon chaotic map.....	108
Figure 4.10 Encoding by system: (a) input image (b) segmented image (c) diffused image using keyless substitution (d) encrypted image	110
Figure 4.11 Decryption by system: (a) encrypted image (b) diffused image after decryption and (c) original image	111
Figure 4.12 Histogram of ROI images (a) original image, (b) segmented image using bit level keyless substitution, (c) encrypted region using MSB based encryption using Hénon chaotic map and (d) decrypted image.....	112
Figure 4.13 Correlation plot of two adjacent plain-image pixels in segmented image in horizontal direction for the (a) green channel, (b) red channel, and (c) blue channel. Correlation plot of two adjacent pixels of the cipher-image obtained by the proposed scheme from the (d) green channel (e) red channel (f) blue channel.....	113
Figure 4.14 Key sensitivity test (a) Image after applying the wrong symmetric key, and (b) intensity range of the corresponding ROI encrypted image	115
Figure 4.15 Mean Value Analysis	115
Figure 5.1 Architecture of the smart grid architecture.....	122
Figure 5.2 Bitwise encryption procedure.....	128
Figure 5.3 Simulation Results on power consumption readings(Watt) A. Original readings B. Stego readings C. Retrieved readings from stego readings	133

Figure 5.4 Gaussian noise Test: a) Original readings b) Stego readings after noise insertion c) Retrieved signal from stego readings.....	135
Figure 5.5 PRD comparison results	136
Figure 5.6 Architecture of the Internet of Battlefield Things	138
Figure 5.7 IEEE 754 Floating-point double precision standard	143
Figure 5.8 Embedding procedure of secret message	145
Figure 5.9 Signal behavior after adding noise	149
Figure 5.10 Simulation Results on Sensor Readings (Watt consumption, Light, humidity) (a). Original readings (b) Stego readings (c) Retrieved readings from stego readings	150
Figure 5.11 PSNR comparison (4 bits, 8bits) embedding capacity	155
Figure 6.1 The proposed architecture of sitting plan algorithm	159
Figure 6.2 Proposed seating plan for examination hall.....	160
Figure 6.3 Pseudorandom numbers generation using Henon chaotic map.....	165

LIST OF TABLES

Table 1.1 Security Services with their Mechanisms	3
Table 1.2. Comparison between Different Traditional Cryptographic Algorithms.....	16
Table 1.3 Taxonomy of Thesis Chapters	26
Table 2.1 Graphical Representation of Different Chaotic Maps.	34
Table 2.2 Recent Chaos-based Image Encryption Algorithms	40
Table 2.3 Chaotic Maps and Performances	43
Table 3.1 Ruleset for Distinct Cell Compositions	57
Table 3.2 ECA based RULETABLE I.....	59
Table 3.3 ECA based RULETABLE II	59
Table 3.4 Entropy Analysis of the Proposed System.....	70
Table 3.5 Correlation Analysis and Comparison of Color Image	71
Table 3.6 Correlation Analysis of Grayscale Images	71
Table 3.7 NPCR and UACI scores of the Test Input Image.....	75
Table 3.8 PSNR Analysis and Comparison	76
Table 3.9 Entropy Analysis.....	87
Table 4.1 NPCR and UACI Scores of the Test Input Images.....	101
Table 4.2 Correlation Analysis of Encrypted ROI.....	114
Table 4.3 Comparative Analysis of Existing Selective Image Encryption Schemes	116
Table 5.1 Taxonomy of Security Attacks in Smart Grids.....	125
Table 5.2 Percentage Residual Difference Test.....	132
Table 5.3 Test Results of Temp. Readings (Embedding capacity 8 Bits/Coff) Model 2	151
Table 5.4 Test Results of Humidity Readings (Embedding capacity 8 Bits/Coff) Model 2	152
Table 5.5 Test Results of Voltage. Readings (Embedding capacity 8 Bits/Coff) Model 2	

.....	152
Table 5.6 Test Results of Light. Readings (Embedding capacity 8 Bits/Coff) Model 2..	153
Table 5.7 Test Results of Temp. Readings (Embedding capacity 4 Bits/Coff) Model 2	153
Table 5.8 Test Results of Humidity Readings (Embedding capacity 4 Bits/Coff) Model 2	
.....	154
Table 5.9 Test Results of Light. Readings (Embedding capacity 4 Bits/Coff) Model 2	154
Table 5.10 Test Results of Voltage. Readings (Embedding capacity 4 Bits/Coff) Model 2	
.....	155
Table 6.1 Attendance Sheet for Classroom A.....	167
Table 6.2 Sitting Plan for Classroom A.....	167

CHAPTER 1

INTRODUCTION

1.1 SECURITY

Security is a continuous process of protecting the resources of the digital system from hackers, attackers and malicious users [1]–[4]. A hacker is a digital criminal who exploits the weaknesses in a computer system or computer network and steals or hack or unauthorized access to its data [5]. Resources that need to be protected can be physical or non-physical. Physical resources comprise computer peripherals and electronic devices, and non-physical resources consist of data and information. In a local area network (LAN), several computers are connected to each other through a network and security is required to protect the transmitted information over the network from unauthorized access. There are two categories of security in computer systems.

- Information security
- Network security

1.1.1 INFORMATION SECURITY

Information security can be described as protecting information or data from unauthorized access, disclosure, and modification irrespective of the form of data. There are two main aspects of information security [6], [7].

- **IT Security:** It is also known as computer security. This security is integrated into technology or some form of the computer system. IT security has a major role in any enterprise due to the use of several old and new technologies. These technologies need to be kept safe and secure from malicious cyber-attacks or any breach of information.

- **Information Assurance:** It is an act of protecting the data which has the potential of being lost when some critical security issues arise. These issues include server malfunction, physical theft. If the data is lost once, it can lead to heavy losses to the organization. When an unauthorized user tries to attack the system, Information assurance is obtained while maintaining the off-site backup of the data.

1.1.2 NETWORK SECURITY

Network security [8]–[11] is a security mechanism via which the administrator can design the network's policies and take necessary action and preventive countermeasures against attacks such as unauthorized access, modification, misuse, and denial of service attack in computer networks in order to protect the available resources in public and private networks. Network security emphasis the security of information in the communication channel of the network. Since a network includes hardware and software technologies, the network administrator provides login details (ID, password) and rights are given to access available resources in the network. Network security covers IoT networks, wireless sensor networks (WSN), cognitive radio networks (CRN), private networks, public networks. It is used in transactions and communications among several areas like E-commerce, national security agencies, and social networking sites [12]. Thus, network security's policy allows only authorized users to the network and monitor all the connected resources to check their strength.

1.1.3 PRINCIPLES OF SECURITY

Telecommunication systems and the development of smart and intelligent networks has opened a wide range of new possibilities. Billions of people are getting connected through the Internet and exchange a large amount of information over the networks. It becomes essential to secure such sensitive information from unauthorized users. There are several standards that are designed to provide security services under ITU-T X.805 to individuals and organizations [13], [14]. For each security service, security mechanisms are also standardized by ITU-T X.805, which are followed by all the countries [15]. Taxonomy of security services with their corresponding mechanisms are listed in Table 1.1.

Table 1.1 Security Services with their Mechanisms

	Confidentiality	Authentication	Integrity	Non-repudiation
Symmetric Key Cryptography	Yes	Yes _{partial}	Yes	
Asymmetric Key Cryptography	Yes	NO	Yes	
Steganography	Yes	Yes		
Data Integrity (MDC)			Yes	
Digital Signature	NO	Yes	Yes	Yes
Notarization				Yes

1.1.3.1 Confidentiality

When communication between multiple users takes place over insecure networks, only the intended recipient should access the contents of a message [16]. The information should not be accessible to any unauthorized recipient. In Fig 1.1, user *A* sends information to the intended user *B*, and the secret message should be delivered to the end-user *B*. However, in this case, confidentiality is manipulated when unauthorized user *C* reads the message.

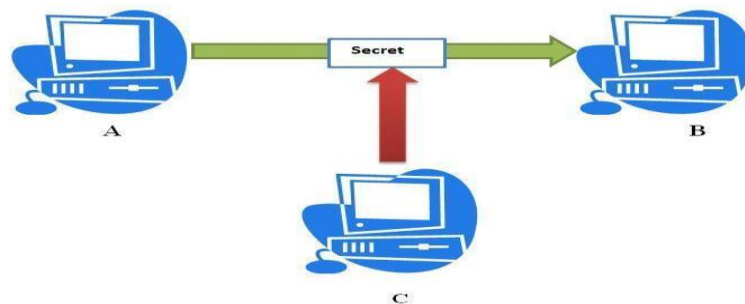


Figure 1.1 Loss of confidentiality

1.1.3.2 Authentication

Authentication mechanisms help to establish proof of the sender and receiver's identities in the communication. It is also known as source authentication; this authentication process ensures that the origin of the message is correctly identified. Figure 1.2 illustrates the authentication process with the help of an example. If a message received by user *B* and it is claimed that it is originated from user *A*, but the message is sent by user *C*, this kind of attack is called the absence of authentication. This type of attack is also called fabrication.

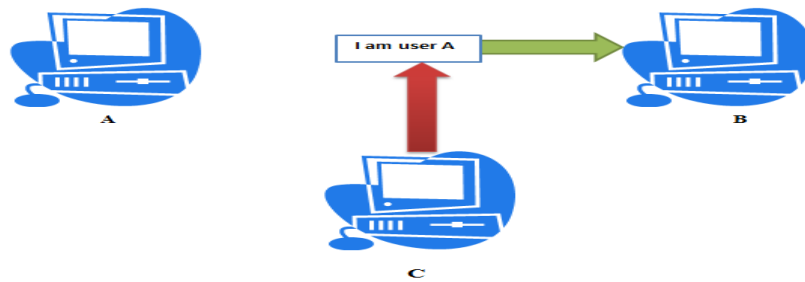


Figure 1.2 Absence of authentication

1.1.3.3 Integrity

The assurance to the receiver that the data is not altered during the transmission and received in the original form as sent by an authorized entity is called integrity. In many cases, information is manipulated and altered due to noise in the channel without any attack. Figure 1.3 shows a way to detect the possibility of a loss of integrity. A message from user *A* should go directly to user *B* without any interruption, but it follows a route via user *C* and the message is altered during the transmission, it is likely that the message has been altered, resulting in loss of integrity.

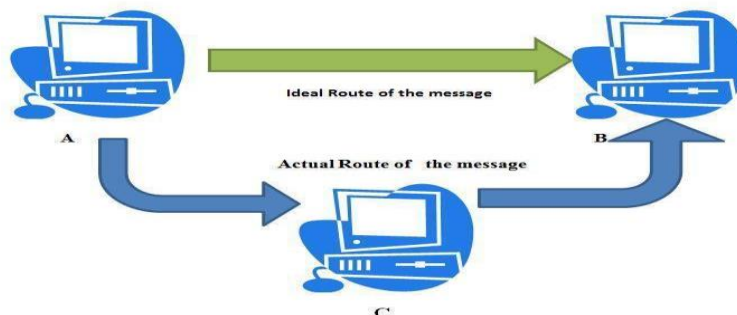


Figure 1.3 Loss of integrity

1.1.3.4 Non-Repudiation

It might happen that a user sends a message and then refuses to be the sender or any user at the receiver's end refuses to have not received the message even if he had read it. To ensure non-repudiation in the systems, a third party is introduced to control the transaction at both ends. Non-repudiation allows rejecting the erroneous claim of not sending that message. Non-repudiation is depicted in Fig 1.4 with the help of an example.

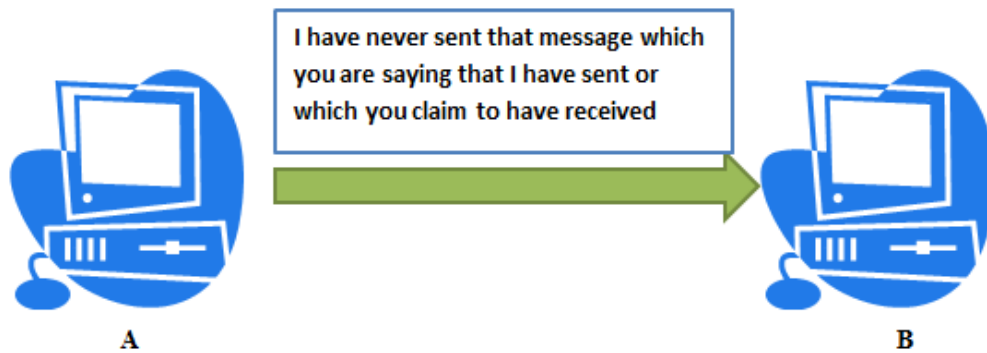


Figure 1.4 Establishing non-repudiation

1.1.3.5 Availability

This attack is referred to as an interruption of an illegitimate user in the network. As shown in Fig. 1.5, user A fails to access user B's resources or fails to contact the server due to the intentional action of unauthorized user C; it is known as an attack on availability.



Figure 1.5 Attack on availability

1.1.3.6 Access Control

Access Control gives users the privilege to access the resources and restrict other users to access it with limited operations. Information needs to be monitor and changed by an authorized entity by allowing access to resources. It prevents unauthorized use of a resource.

1.1.3.7 Security Attacks

An unauthorized user's attempt to gain access to any information by compromising its security is called a security attack [17], [18]. Security attacks can be classified into two categories: active attacks and passive attacks; these attacks might pose a serious threat to the confidentiality and integrity of the system. A typical attack, denial of service attack (DOS), harms computer systems' availability. Either an insider can exploit the network or the network service provider itself. A system should be designed in such a way that it can prevent attacks at the early stages. Also, if an intruder penetrates the system, it should be recovered rapidly. There exist two types of security attacks:

1.1.3.7.1 Passive Attacks

The goal of the attacker is to get the information from the transmitted bitstream in the network. The attacker monitors the traffic [19], [20]. Passive attacks are basically monitoring of communication channels, unethical traffic analysis, unauthorized access of weakly encrypted traffic, eavesdropping, and exposing all the authentic information. Passive attacks are hard to detect as the attacker only sniffs the data without making any modifications in data.

1.1.3.7.2 Active Attacks

Active attacks are the actions that attempt to bypass the secured system [21], [22]. Active attacks are detected easily, although it is challenging to prevent active attacks. It can also be done through viruses, worms, stealth, or Trojan horses. It comprises modification of the bitstream and creation of a false stream to introduce malicious code. The purpose of such attacks is to steal and modify the information to harm the systems. These attacks include masquerading, replay, modification of messages, and denial of service attacks. A masquerading occurs when one illegitimate user impersonates to be a legitimate user. It can further lead to other active attacks. In a replay attack, the attacker tries to get the message; once it is captured, it is used as a fresh copy in retransmission to the same recipient.

1.2 NETWORK SECURITY MODEL

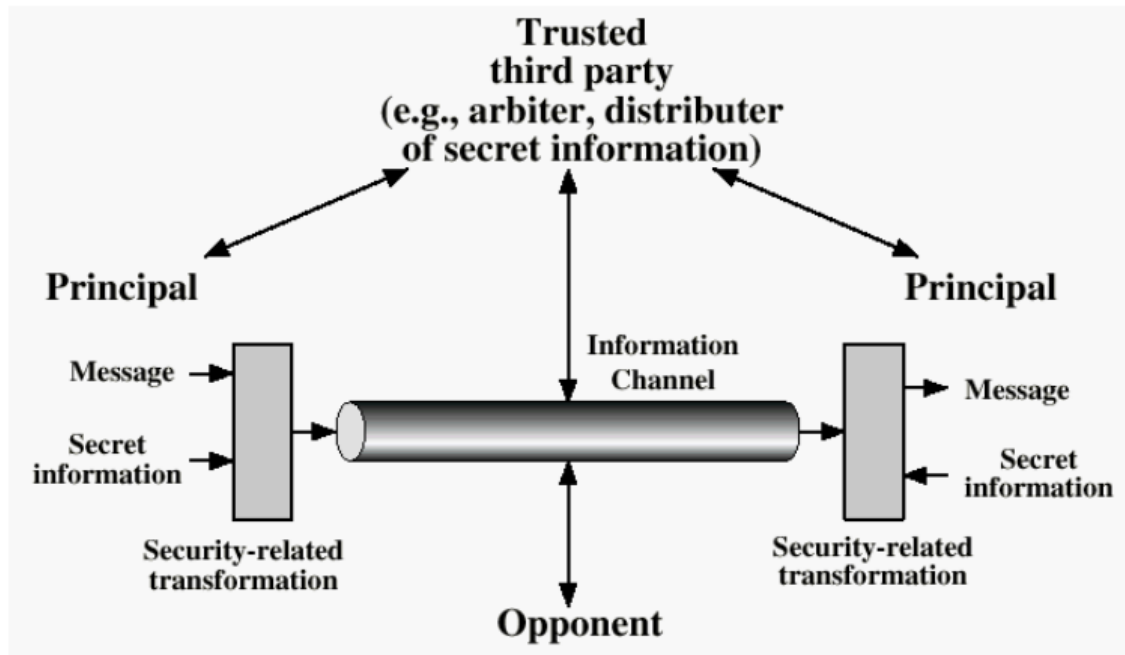


Figure 1.6 Network security model

In the Network security model, as shown in Fig 1.6. [23], the two entities involved in communication tend to send messages via an information channel. A logical channel is implemented for users by setting a route through the Internet from source to the destination. In order to protect the information from intruders, the entities participate in performing some security-related operations on the message. Such activities may involve using a trusted third party to whom some responsibilities, such as distributing secret information or authorization/authentication, are entrusted.

There are four essential tasks involved in designing a security service using this model:

- (a) An algorithm for performing the security-related transformation
- (b) Generate the secret information required by that algorithm
- (c) Method for distribution and sharing of secret information
- (d) A protocol to be used by two entities utilizes the security algorithm and secret information to achieve a particular security service.

1.3 MULTIMEDIA

Multimedia is a piece of digital information that deals with different types of data formats such as text, images, audio, and videos altogether. Multimedia is originated by combining different content formats smartly from the computer systems [24]–[26]. The advancement of devices to display multimedia and enabling them to transfer it from one location to another has resulted in spreading danger over their security services. Information shared over the Internet needs a high level of protection from intruders. Nowadays, digital images are used frequently for communication. Digital information has the advantage that it can be transmitted in different forms by multimedia processing, but due to inadequate security protocols, data can be copied easily on a USB-stick or a hard drive. Also, precisely the same information can be sent over a wireless network or an optical fiber; the transmission of data is efficient, fast and easy. When a sender sends a message, it becomes very important for the receiver to check whether the privacy of the message has been compromised or not. Multimedia security is used to ensure the confidentiality, authenticity and integrity of the message by using standard mechanisms.

1.4 CRYPTOGRAPHY

Cryptography is an art and science of securing information by encoding it to a non-readable form [27]–[29]. Cryptography is synonymous with encryption. This process is systematic and well-structured and related to security services such as confidentiality, integrity, authentication, and non-repudiation. Cryptography is widely used in several applications like banking, financial services, education, satellite communications, defence and security agencies, social networking sites, and E-commerce sectors. Historically, encryption was used by militaries and governments for a long time to facilitate secret communication channels. However, it is widely used in protecting the information of people across the world. In 2007, the computer security institute surveyed many companies based on technologies, and it is found that 71% of companies utilized encryption techniques for securing information during the transmission, and 53% utilized encryption techniques to secure stored files on the digital platforms. Encryption techniques allow users to protect static data, i.e., files on the computers (at rest) and dynamic data (data during the transmission). Usually, in a computer system, files are stored in the secondary memory, and most often, when files have confidential and crucial information; it is

stored in the ciphered format in the storage devices to protect from being visible to the unintended user through loss or theft of such devices and cyber-attacks. When physical security measures fail, encryption of such multimedia-oriented files helps to protect them. Encipherment techniques can prevent unauthorized access or reuse of the copyrighted digital material and software without consent that helps in digital rights management systems. The one who encrypts the message needs to share the decryption technique to regenerate the original information only with intended receivers, thereby prohibiting unwanted people from decrypting the message. Cryptography techniques were used in World War I to communicate the messages secretly. As technology advances with updated hardware and software, enhancement of existing cryptographic algorithms should be carried out. Cryptology is a combination of cryptography and cryptanalysis, which has become the need to build an ideal system design to fight against security attacks.

The foundation of modern cryptographical techniques is based on mathematical concepts and designed around computational hardness assumptions, which makes them practically difficult to break by an attacker. Although it is theoretically possible to break such a system, it is infeasible to do so by any known practical means. Therefore, cryptographic algorithms are termed as computationally secured. A one-time pad (OTP) is an example of information-theoretically secure schemes that probably cannot be fragmented even with unlimited computational power.

1.4.1 CLASSIC CRYPTOGRAPHY

When information is communicated through a nonsecure channel, it is assumed that the information can be intercepted at any point. Therefore, information must be protected, and the cryptography concept arises here, which allows users to encipher the data (convert it into a non-readable format) [30], [31]. Encipherment techniques are classified in two ways: a user can apply either a cryptography scheme or a steganography technique depending upon the security requirements. Since most people could not read the content, the first form of protection is to secure the message which was based on paper and pen analogy. Basic cryptography attracted literate people due to the applications. The main classical cipher types are transposition ciphers and substitution cipher. Transposition cipher rearranges or shuffles

the order of symbols in a message, whereas in substitution ciphers, it replaces symbols or groups of symbols with different symbols or groups of symbols.

Simple versions of cryptography could not provide much confidentiality from opponents. *Caesar cipher* [32] was an early substitution cipher scheme; each letter is replaced by a letter that is located at a specific distance from the alphabet. According to Suetonius, long ago, Julius Caesar used the caesar cipher method to shift letters to distance three to create the ciphertext

The **cryptography scheme** can be described as follow. The input message is given in the form of plaintext denoted by P or plaintext, which is then processed with an encryption system comprising an encryption algorithm and a key generation algorithm. The encrypted message is called ciphertext denoted by C . The encryption procedure is defined as $C = E_{eKey}(P)$, where $eKey$ is the secret key, also known as the encryption key, and $E()$ is the encipherment function. At the receiver end, to get the original information, the decryption module is described as $P = D_{dKey}(C)$, where $dKey$ is the decryption key and $D()$ is the decryption module. An encryption procedure usually needs a key-generation algorithm to produce keys randomly in a large keyspace to ensure end-to-end security

When both the keys, encryption key and decryption keys are same, i.e., $eKey = dKey$, the cipher system is called a symmetric cipher or a private-key cipher. In private key cryptography, encrypted data cannot be decoded unless a user has its secret key. Therefore secret key must be transmitted through the secure channel from sender to the intended receiver.

When an encryption key is different from a decryption key, i.e., $eKey \neq dKey$, is called a public-key cipher based on the usage of key pair. In this scheme, each party has a different pair of keys. The receiver's encryption key $eKey$ is published and distributed to all the parties, while the decryption key $dKey$ of the receiver is kept private. Here, the advantage lies in the fact that there is no need to established a secret channel for the key, i.e., these keys can be distributed through unsecured channels. According to the encryption and decryption function design, ciphers can be classified into two classes: stream ciphers and block ciphers [33]–[36]. In a stream cipher, the plaintext is encrypted with a sequence (called keystream) controlled by the encryption key, whereas in block ciphers, plaintext is encrypted block by block and it is converted into another non-meaningful block of the same length.

1.4.2 TYPES OF CRYPTOGRAPHY

Traditional algorithms of cryptography [28], [37], [38] were designed for text and written according to 26 distinct symbols, whereas these days, information can be communicated through any mode of multimedia such as images, video, audio. Multimedia covers a considerable number of bits that travel across the world very frequently. Hence, to handle such bulky data's intrinsic properties that hold a huge amount of volume and redundant data, we need such systems that can be implemented efficiently on software and hardware. In cryptography, encryption is the process of converting a message into a non-readable format so that eavesdroppers or attackers cannot read it or get any useful information from the cipher message. However, only authorized parties can read the message correctly, passed on with the encryption algorithm's details and the secret key. An eavesdropper having illegitimate access to ciphertext must fail to obtain the original message. A simple procedure of encryption and decryption is illustrated in Fig. 1.7. Based on the key pair, the cryptography scheme can be classified into two categories.

- Symmetric-key cryptography
- Public key Cryptography

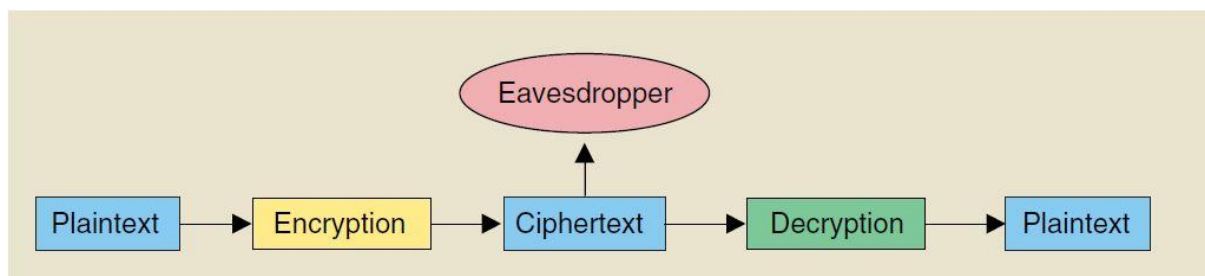


Figure 1.7 Block diagram of cryptography.

1.4.2.1 Symmetric-key Cryptography

In this scheme, a similar key is used for encryption/decryption at both the communication ends to encrypt a message. Thus, the sender and receiver must share the secret key before the communication, as depicted in Fig 1.8. In symmetric-key schemes, the encryption key is transmitted to encrypt messages for interested users to use the encryption algorithm [39], [40], and only authorized persons can decrypt the cipher message. A System is considered vulnerable when the secret key is not changed for the next round and used more than twice. Public-key encryption is a relatively recent invention based on private and public keys. Previously, all encryption schemes were addressed with symmetric keys (private-key) only. Symmetric key cryptography scheme can be designed using either block cipher or stream cipher structure. A block cipher algorithm encrypts input blocks of plaintext instead of individual symbols, the input form used by a stream cipher. In a stream cipher, the plaintext is encrypted by a pseudorandom bit keystream. Stream cipher is also known as state cipher.

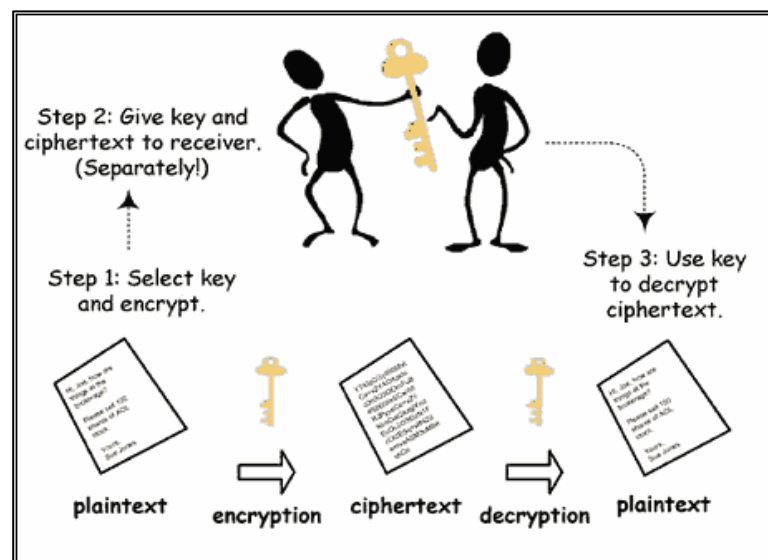


Figure 1.8 Symmetric-key encryption process

AES and DES are two popular modern symmetric key cryptography algorithms used to achieve confidentiality and were designed to modify the text [34], [41]. The emphasis is given to encryption stability instead of giving attention to cryptanalysis attacks and the statistical property of input data. However, cryptanalysis became more critical these days to check the vulnerability of the system. Stream cipher and block cipher are two techniques that are designed under cryptography. DES, AES, 3DES, and International Data Encryption Algorithm (IDEA)

are popular algorithms used in the commercial sector and the mainstream security policies for privacy. Initially, these algorithms were designed for text, which consists of limited input information and different statistical properties than any other multimedia. So, in a few cases, when these traditional algorithms [42]–[44] are applied to images, these techniques do not perform well. Hence, found unsuitable for image encryption. Also, the theoretical values obtained demonstrate that these techniques are ideal for a small amount of information.

1.4.2.2 Symmetric-key Algorithms

It also requires that the sender and receiver have access to the secret key (i.e., keys must be communicated through a secure channel). Since it is assumed that algorithms are public and can be accessed by all users; if an intruder gets access to the key, it can extract information from the cipher data; this is the drawback of symmetric key to public-key encryption.

1.4.2.3 Types of Symmetric-key Algorithms

Usually, symmetric-key encryption algorithms are designed based on **stream ciphers** or **block ciphers**. Message's symbols are encrypted with a series of numbers and processed in a series fashion (one digit at a time). Block ciphers take a number of bits, and blocks of 64 bits have been commonly used and encrypt them as a single unit. Padding the plaintext may be required to ensure that it is a multiple of the block size. NIST approved Advanced Encryption Standard (AES) algorithm, and a 128 bit-sized block was passed as an input in December 2001. A stream cipher [45] based on symmetric-key cryptography is used to encrypt a stream of plaintext, each symbol of the plaintext is combined with a pseudorandom cipher digit stream (keystream) using any mathematical operation between bits as shown in Fig. 1.9. Binary bitstream is encrypted one at a time with the corresponding binary sequence of the keystream, which gives a digit of the ciphertext stream. The encryption of each binary number is dependent on the

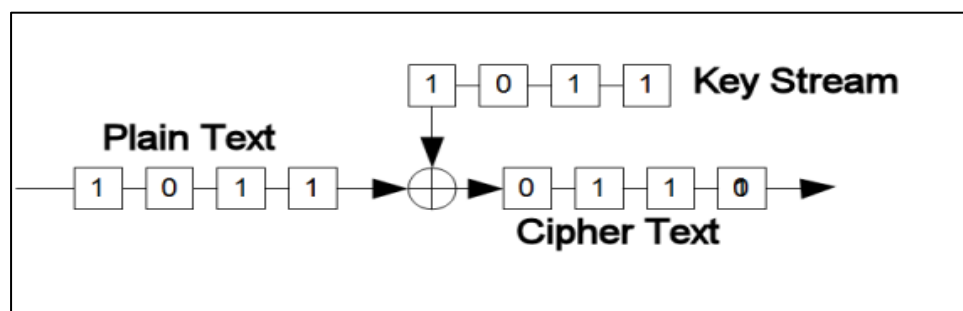


Figure 1.9 Stream cipher

current state, so it is also called a state cipher. In practice, a bit or byte are used as input for the encryption procedure combining logical operations, i.e., XOR, AND, XNOR [46]. RC4 is a commonly used popular stream cipher [47]. The pseudorandom keystream is typically generated by shift registers combining different modules and the keystream is generated in an iterated fashion. The random seed value is treated as the cryptographic key for the cryptosystem. Stream ciphers have a completely different approach from block ciphers. Stream ciphers involve an arbitrarily long stream of a key, combined with the plaintext bit-by-bit or character-by-character, almost similar to the one-time pad.

Block ciphers deal with large blocks of digits with a fixed size and apply a deterministic algorithm to encrypt a group of symbols [48]. Stream ciphers have several advantages when compared to block ciphers. Stream ciphers are faster as they have higher computational speed than block ciphers. Also, block cipher schemes are bound to the hardware that increases the hardware complexity. Therefore, stream cipher has lower hardware complexity. However, if stream cipher is used incorrectly, are prone to serious security problems. Also, block ciphers can be implemented as stream ciphers. To overcome this drawback, the same starting state (seed) must never be used twice. In a stream cipher, the output stream is generated based on a hidden internal state and internal state changes when the cipher operates and the internal state is initially set up using the secret key material. A simple model based on a block cipher, i.e., output feedback mode encryption (OFB), is illustrated in Fig. 1.10; it uses the XOR operation for successive blocks. US government also contributed in cryptography to established some cryptography standards.

The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are designated block cipher designs meeting these standards. DES's designation was finally withdrawn after the adoption of AES. DES is quite popular and is used across the Internet and a wide range of applications, from mail privacy and secure remote access to ATM encryption. Meanwhile, block cipher-based algorithms have been designed and used, with substantial variation in quality.

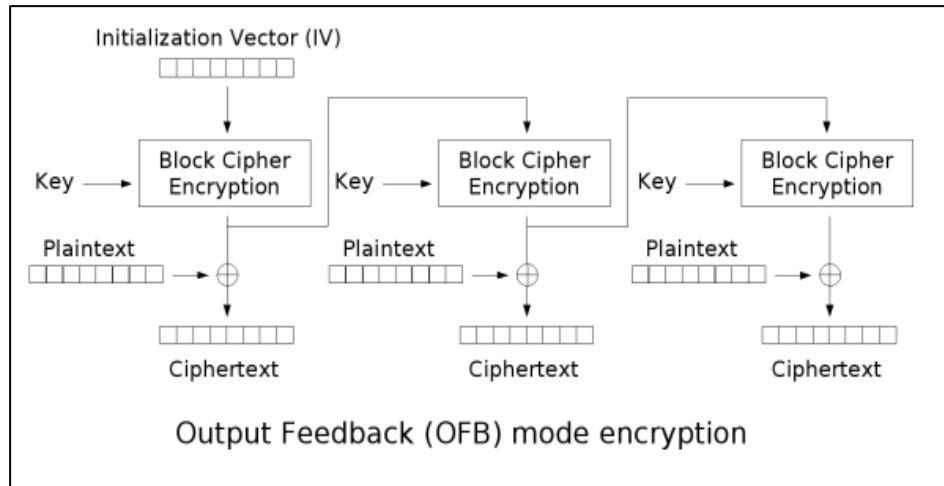


Figure 1.10 Block cipher based on output feedback mode encryption

1.4.2.4 Public-Key Cryptography

In public-key cryptography schemes, A sender encrypts a message by receiver's public key, and it is decrypted by only the private key of the intended receiver [49]. A different key pair is required for each distinct pair of communicating parties, and perhaps each ciphertext is exchanged as well. With the increase in the number of network members, the number of keys required increases. For proper key management, highly secure key management algorithms must maintain privacy in terms of key pair (it increases the complexity of the cryptosystem).

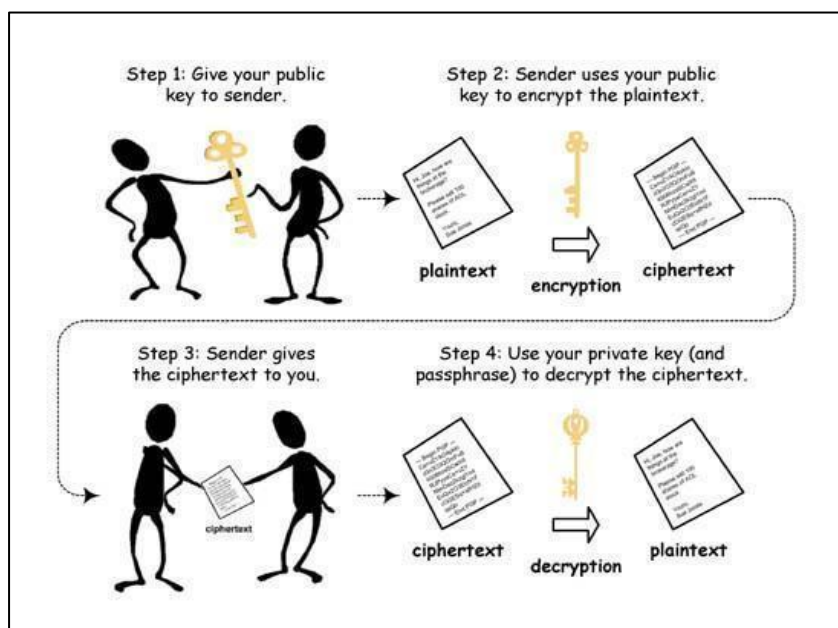


Figure 1.11 Asymmetric key cryptography process.

In public-key cryptosystems as shown in Fig. 1.11., the public key can be distributed freely to all the network parties, whereas the private key is kept secret. In Public-key cryptography schemes, RSA and ECC are popular algorithms for asymmetric key cryptography scheme. Nevertheless, many other algorithms, such as ElGamal, Paillier cryptosystem, are also utilized to fulfill specific service requirements. These techniques are based on a pair of public keys. In [39], [50]–[52], Chaos theory has emerged with these algorithms for the better performance of cryptosystems. Asymmetric key cryptography techniques are based on exhaustive calculations and it takes a good amount of time to compute the keys and the cipher; also, prime importance is given to the key generation phase. Cryptography schemes are listed below in Table 1.2:

Table 1.2. Comparison between Different Traditional Cryptographic Algorithms

	Private key cryptography schemes			Public key cryptography schemes	
Algorithm	DES	3DES	AES	RSA	ECC
Developed	1975	1978	2000	1978	1985
Block round	16	48	10 (128bits key) 12 (192 bits) 14 (256 bits)	01	01
Design	Substitution and permutation	DES is applied three times	Substitution, Shift and bit mixing	Based on Modular arithmetic, Euclidean algorithm and prime numbers.	Point addition and point doubling
Key size	56 bits		128,192, 256 bits	>1024 bits	>160 bits
Input blocks size	64 bits	64	128	Depending upon the input	Very tiny 16 Kb
Encryption Speed	moderate	slow	Faster	Slower	Faster than RSA
Security	Inadequate Secured	More secured than DES	Exceptional secured	Least secured	Secured and can be applied to images
Power Consumption	Low	High	Low	High	Low

Whitfield Diffie and Martin Hellman proposed the notion of *public-key* cryptography or asymmetric key cryptography in 1976. In this, two different but mathematically correlated keys

are used. One is a public key and the other one is a private key. A public-key system is designed so that the private key calculation is computationally infeasible from the public key, even though they are necessarily related. Instead, both the keys are generated secretly, as an interrelated pair. Diffie–Hellman [8] is a key exchange protocol that provides a solution to allow two parties to share encryption keys secretly.

1.5 CRYPTANALYSIS ATTACK

1.5.1 BRUTE-FORCE ATTACK

A **brute-force attack** is an exhaustive search mechanism [53] that is used against the secured system. It is an **exhaustive key search** process for trying every possible combination of keys until the correct key is identified. This method is popularly known as the trial and error method. An attacker guesses all passwords and apply a divide and conquer strategy until the system is accessed to gain unauthorized access. In the worst case, this would result in traversing the entire dictionary. This attack is not possible for data, i.e., encrypted in an information-theoretically secure manner. Such an attack is the only hope for intruders when it is impossible to take advantage of other vulnerabilities in an encryption system that would make the task easier.

1.5.2 CRYPTANALYSIS

Cryptanalysis [37], [54] is the art and science that deals with cracking cryptography techniques to recover information or forge information accepted as authentic. Hidden aspects of security and vulnerability of the system are analyzed by cryptanalyst to break the cryptography-based systems without having knowledge of the security key of the system. Cryptanalysis includes the study of side-channel attacks and the virus injection into the system to steal and corrupt the information, which exploits the weakness in their implementation. The cryptanalysis techniques have evolved over time, ranging from pen-and-paper methods to machines like Bombes and Colossus computers at Bletchley Park in World War II. Present-day methods for cryptanalysis of modern cryptosystems mainly included pure mathematics. Integer factorization is the best-known problem solving scheme.

1.5.3 TYPES OF CRYPTANALYSIS ATTACK

Cryptanalysis attacks are based on the amount of information known to the cryptanalyst. In general, it is assumed that the opponent knows the encryption algorithm. One possible attack is a brute force attack, but it becomes impractical to try all the possible keys if the keyspace is very large. Therefore, attackers have another option that is a mathematical study of the cryptographic algorithm and cipher. A weak algorithm fails to withstand a ciphertext-only attack. An encryption algorithm is designed to withstand a known-plaintext attack. It is not very easy to estimate the amount of effort required to cryptanalyze ciphertext successfully.

In all cryptanalysis attacks, it is assumed that cryptanalyst has access to the encryption algorithm. Here, four types of cryptanalysis attack are described below [37] :

1. **Ciphertext-only:** It is the easiest to defend against as the opponent has no other information except for the ciphertext. It is assumed that intruders have had access only to a set of ciphertexts.
2. **Known-plain text:** The opponent captures one or more plaintext messages and their encryptions, which makes it possible to deduce the key based on how plaintext is transformed.
3. **Chosen-plaintext:** If an analyst can choose the message to be encrypted and gets the source system to insert that message into the system. Cryptanalyst tries to find out the structure of the keys using a cipher message originating from its original plaintext and trying to understand the statistical properties of the key while mapping.
4. **Chosen-cipher text:** The analyst gathers all the relevant information by choosing a ciphertext and obtaining its decryption under an unknown key. He enters one or more chosen ciphertexts into the system and obtains the resulting plaintexts. By combining these pieces of information, he/she tries to reveal the hidden secret key.

1.6 KEY TERMS

1.6.1 CRYPTOSYSTEM

The term is used as a synonym for cryptographic systems [55]. A cryptographic system is any digital device that involves cryptography like a system for secure electronic mail, which includes cryptographic hash functions, key management, methods for digital signatures, and so on. A cryptosystem comprises of three algorithms: key generation algorithm, encryption algorithm and decryption algorithm.

1.6.2 ONE-TIME PAD

In cryptography, the one-time pad [56] belongs to a symmetric key cryptographic scheme, which is highly secure and difficult to break. The ciphertext is obtained by encrypting each bit from the plaintext by a modular or logical operation with a bit from a random secret key (or pad) of the same length as the plaintext. It is difficult to decrypt ciphertext without knowing the correct key. This is possible only when the key is random and it is not reused in whole or in part and kept secret. For easy disguise, the pad was sometimes reduced to a very small size such that it can be used only with the help of a robust magnifying glass. The one-time pad was used to print onto sheets of highly flammable nitrocellulose in order to increase their secrecy. In the early implementation of a one-time pad scheme, a paper pad is used as the key and distributed; after decoding a message, top sheet is destroyed and torn off. Frank Miller first described the one-time pad in 1882, and then it was re-invented in 1917. It was the Vernam cipher, whose name has been named after one of its inventor Gilbert Vernam. Vernam's system is a cipher, which combines message with the key from a punched tape to encrypt a message. Vernam's system's original form was vulnerable to attacks as the key was reused whenever the key tape's loop made a full cycle. Joseph Muborgne identified that if the key tape was totally random, so cryptanalysis would be impossible, leading to the introduction of a one-time pad.

1.6.3 EAVESDROPPING

Eavesdropping is an unethical act of interfering in-between and sneakily listening to a private conversation. It can be considered a passive attack if third parties attempt to observe the flow and gain information. If it attempts to alter the data or affect data flow, eavesdropping is

categorized as an active attack. Eavesdropping can be done by monitoring telephone and Internet conversations by a third party. An intruder can eavesdrop the information over telephone lines (also known as wiretapping), instant messaging, emails, and other communication methods considered private. It is assigned wiretap name because, in older days, the circuit was attached to telephone lines, and a small amount of electric signal carries conversation used as disclosure of information.

1.6.4 CONFUSION AND DIFFUSION

Claude Shannon introduced the two important terms 'confusion' and 'diffusion' in 1949, which are regarded as the crucial aspects of the cryptosystem. Researchers and scientists have applied chaotic maps to images and other multimedia in the last two decades, i.e., usually based on confusion diffusion theory [57]–[59]. In order to achieve the confusion diffusion concept, pseudorandom numbers have been applied to numerous cryptography algorithms based on chaos theory. In some related work, the starting point of the used key or part of the key for decryption can be derived from the frequency distribution of words and letters in plaintext [6]. Therefore, Shannon recommends that the ciphertext should not be dependent on plain text and key used for encryption. Shannon's theory reduces the possibility of deriving the ciphertext based on a statistical analysis of plaintext. Still, some cryptanalyst attacks by using their prior knowledge of statistical analysis of plaintext. Confusion means hiding the relationship between key and the statistics of ciphertext, which made it difficult to derive the key used for encryption and intruder fails to find the relationship between ciphertext and the key. Diffusion means the relation between ciphertext and plain text is hidden as it is observed that a single bit change in plaintext affects the ciphertext generated heavily; more than half of ciphertext bits change. The principle of diffusion prevents the cryptanalyst to derive any relation between ciphertext and plain text. While in the case of confusion, the cryptanalyst is prohibited to find any relation between key and ciphertext. In diffusion, if a single bit is replaced in ciphertext, the cryptanalyst must fail to develop the original input. It refers to make a more complicated relationship between ciphertext and original input. The entire mechanism, also stated in Fridrich architecture (permutation and substitution), is applied to images to enhance security and make it secured against security attacks. A chaotic system based on confusion and diffusion was developed in 1989 [60].

1.7 PROBLEM DEFINITION

In literature, numerous techniques are available to deal with security issues and vulnerability as it can alter, modify, unauthorized access, and delay the true information content of multimedia. This thesis attempts to address some major drawbacks present in existing methods used for privacy and proposes new algorithms for an efficient and reliable system. Images and IoT signals are transmitted very frequently through the unsecured channels; therefore, this thesis contains algorithms to secure images and sensitive information of IoT networks. Image encryption techniques are applied in internet communication, multimedia systems, medical imaging, satellite communication, telemedicine, military communication, etc. Traditional cryptosystems are not suitable for images for the encipherment due to the computational overhead. There are more shortcomings of a conventional cryptosystem apart from the computational cost. The following problems are conferred in this thesis, which are discussed below.

- Images size is practically always much larger than the text. Therefore, the conventional algorithms take longer to encrypt directly to the image data. The second problem is that the decrypted message must be equal to the original message. However, this requirement is not necessary for the image data.
- In the traditional cryptography system, it is challenging to secure a large size of multimedia from intruders or attackers and the calculation of mathematical equations (built-in Encryption technique) is achieved in a high order of complexity. Also, modern encryption algorithms, such as DES, IDEA, AES, were designed for the text. Therefore, these techniques are not suitable for image encryption due to their statistical properties and complexity.
- In literature, compression techniques are applied to reduce the size of input data to decrease the computational cost of the encryption technique. Compressed images contain either lossy or lossless information and a decision can not be made on the lossy or low-resolution images. Sometimes it is also not required to encrypt the entire image (image may contain the object with background details and background information is necessary to encrypt. e.g., Medical images and satellite images)
- Most techniques work efficiently in the spatial domain, but they fail when applied in the frequency domain to preserve the fine details present in an image. The encryption

module modifies the pixel values, but the conversion of an image from the frequency domain to the spatial domain regenerates the image with many side effects on an image, such as blurring, loss of information underflow, and overflow of pixel values. The quality of image data should not be compromised with the encryption.

- In IoT network, sensor nodes and smart devices are connected to the network to transmit information very frequently, and sensor nodes have limited resources in terms of hardware and software. Thus it requires cryptosystems that can be implemented in such environment.
- Lastly, IoT devices have limited memory and fewer computational capabilities than other devices. It supports only predefined operations and performs a statistical calculation to identify current demand, production cost, faults, etc. Thus, the technique must be designed in such a manner that it can hold significant information with a hard time-bound to operate in real-time operations with consistent performance.
- Steganography techniques ensure the confidentiality of secret information in networks. In IoT networks, a stego signal cannot be used directly at the end of the server because when the secret bits are concealed in it, it changes a lot, so a user can not use it directly. The other thing is that only secret information is extracted from the stego object and cover information is discarded at receiver's end. Cover information is also meaningful information, so retrieval is also important. Therefore secret information, as well as original cover information, should be extracted from stego readings.

1.8 RESEARCH QUESTION AND OBJECTIVES

To overcome the above unique challenges, which are discussed in section 1.7. The core objective of the thesis to design algorithms that guarantee to secure information to obtain confidentiality, authentication, integrity and study of nonlinear systems and cryptography schemes. The complete study can be classified as an investigation and identification of several objectives, which are segregated into three major categories of inter-related problems. Every problem is addressed by proposing two different models for the solution. Also, a solution is proposed for real-time application for the examination system to prevent students' unethical behavior during an examination. Furthermore, to achieve the stated objectives, the following

research questions are formed.

Research Question (RQ-1): What is the significance of chaos theory in Cryptography?

Chaos theory contains wide applications in different fields of science. This research question focuses on the study of chaos theory and concludes that chaos has the quality that is used to secure images. Chaos-based schemes follow traditional cryptography schemes' principles to achieve confidentiality, but both work differently in different environments. Based on the question formation, the following objectives are made:

- To study chaos theory and the importance of cryptography techniques.
- There are many chaotic systems available in chaos theory. In order to understand chaos-based cryptography comparative analysis of different chaos-based algorithms and the evaluation of chaotic maps is done which provide a better understanding of nonlinear systems and cryptography.

Research Question (RQ)-2. How can images be secured during the transmission applying the limited operations on the images to preserve confidentiality, authentication in the environment where hardware and software resources are limited?

One of the challenging issues in the IoT network is to protect sensitive information. Encryption and steganography are two mechanisms to achieve confidentiality. In networks, Images are communicated very frequently over the unsecured channel. Therefore algorithms must provide security while achieving confidentiality and source authentication. This must ensure the low computational cost and minimum overheads of encryption/decryption procedure of images. It is also able to provide other security services by system apart from confidentiality. Algorithms must be designed on the simplest operations, such as logic gates and arithmetic operations. The following objectives are enlisted below:

- To propose a lightweight framework to be implemented with minimum hardware requirements (based on simple mathematics). Elementary cellular automata (ECA) and Electromagnetic rotor machine-based algorithms are designed based on simple calculation and mapping procedures.
- To design a permutation box, which is governed by a key, unlike other traditional permutation schemes which are based on the algorithm; here, the key decides the

shuffled location of the original pixel in the proposed algorithm.

- To develop the encryption module based on substitution cipher schemes based on ECA and electromagnetic rotor machine, pixel values are substituted into other values, and it is achieved with a minimum number of computation and mathematical operations.
- To utilize the properties of the electromagnetic rotor machine in image encryption with a novel approach to achieve confidentiality and authentication with high security.

Research Question (RQ)-3. While solving the RQ-2, we have observed that images contain redundant data, and encryption modules are designed for all the pixels that increase the computation cost. How to reduce the size of operations without applying the compression strategy?

Since Compressed images contain lossy and lossless information depending upon the compression algorithms, data management is crucial to handling a huge volume of data, i.e., either stored in a computer system or communicated and other issues discussed in section 1.7 regarding compression. The ideal cryptosystem must be designed so that it can deal with a selective amount of the input information and produce the cipher image. This kind of system must attain a high level of security to resist cryptanalysis attacks.

- To study the selective image encryption techniques and also develop the selective image encryption scheme in the spatial domain using the image processing technique.
- To develop the selective image encryption scheme in the frequency domain

Research Question (RQ)-4. IoT devices are deployed in wireless sensor networks, and it transmits the collected information continuously. Can we use this information stream as a cover object to hide sensitive information to obtain confidentiality and integrity?

Sensor nodes are deployed in many fields to collect information, and this bitstream is used at the end for several purposes depending upon the nature of the signal. To develop the algorithms that can be governed in real-time applications, we need to establish that area and the security challenge in that area and solution must be designed accordingly.

- To design the steganography algorithms in that manner, a stego signal can be used directly at the server end (i.e., stego signal must be similar to like original signal) also

reconstruct the original signal from the stego signal. Therefore secret information, as well as original cover information, is extracted from stego readings.

- While preserving the confidentiality, integrity of the signal is also required; therefore, to design an algorithm that can also preserve the integrity of the signal. If any change is made on the signal, it must be detected through the algorithm.

Research Question (RQ)- 5: After the formulation of the first four research questions, this research question is based on the application of security services to provide integrity in academic institutes. Security policies are enabled in all the communication sector. This problem is formed to secure the education system while preserving integrity preservation. **Can an algorithm be designed to maintain the students' seating allocation list during the examination and prevent malicious actions?**

- To design an algorithm to preserve academic integrity during an examination
- To design an algorithm that reduces the computational overhead of human resources during the examination

The proposed schemes can also be categorized into subcategories, as shown in Table 1.3:

1.9 CONTRIBUTION AND THESIS OVERVIEW

The chapter-wise summary of the thesis is listed with the goals and the outlines and illustrated in Fig 1.12.

Chapter 1 begins with a contextual review of security services. A brief theory of security services and the traditional mechanisms and basic terminologies of cryptography are discussed in all the sections. The last section presents the organization of the thesis.

Chapter 2 presents a brief study of the existing techniques present in the literature used for encipherment techniques. The study of chaos theory and analysis of different chaotic maps are discussed. This chapter presents an in-depth review of traditional cryptography and chaos-based cryptography schemes. This chapter address research question RQ-(1).

Chapter 3 presents the cryptosystems based on the elementary cellular automata (ECA) and the electromagnetic rotor machine. This chapter address research question RQ-(2).

Table 1.3 Taxonomy of Thesis Chapters

	Category	Chapter 3	Chapter 4	Chapter 5	Chapter 6
Spatial Domain	Pixel manipulation	Yes	Yes	No	
	Position manipulation	Yes	Yes	No	Yes (location manipulation)
Frequency Domain	Phase manipulation	No	No	No	
	Frequency manipulation	No	Yes	Yes	
Key dependent	Text key	No	No	No	
	Image key	Yes	No	No	
	Group-based key	Yes	No	No	
Security Services	Confidentiality	Yes	Yes	Yes	No
	Integrity	No	No	Yes	Yes
	Authentication	Yes	No	No	No
Amount of encryption	Full Encryption	Yes	No	yes	
	Partial encryption	No	Yes	No	

- (a) **Model 1** : An Efficient Image Encryption Scheme Using Elementary Cellular Automata with Novel Permutation Box.
- (b) **Model 2** : An Efficient Image Encryption Scheme based on electromagnetic rotor machine.

In this chapter, the chaotic system, biometric features, cellular automata, and confusion-diffusion theory are incorporated, i.e., follows traditional cryptography concepts. Proposed algorithms are tested, and the performance is discussed and compared with other existing methods.

Chapter 4 deals with the implementation of selective image encryption schemes. In Chapter 4, selective image encryption schemes have been studied and analyzed. Two algorithms have been proposed, one in spatial and another in the frequency domain by applying novel modules.

These algorithms are based on a partial encryption scheme, where the amount of encryption is reduced to obtain reduced encryption time. These algorithms are designed on the amount of encryption involved. So, it deals with the partial image encryption schemes. This chapter address research question RQ-(3). They are as follow:

5. Selective image encryption schemes

- (a) **Model 1:** DWT based image encryption scheme in frequency domain
- (b) **Model 2:** ROI based image encryption scheme in spatial domain

Chapter 5 presents a novel steganography technique based on the frequency domain and chaotic map to achieve integrity, confidentiality and authentication. Fresnelet transform and the Haar wavelet is used to generate coefficients for encoding purposes. Sensor data and smart meter readings have been used for the simulation purpose. Periodically collected readings are used as cover objects for hiding the information of users. PRD, MSE, PSNR and BER tests have been performed between stego and original readings as well as the reconstructed readings. The value of the PRD, MSE Tests are observed to be very less than other existing algorithms. This chapter address research question RQ-(4).

Models which are proposed in this chapter as follows:

- (a) **Model 1** - Chaos-based steganography technique to secure information and integrity preservation of smart grid readings
- (b) **Model 2-** Internet of Battlefield thing Security: A Strategy to Secure Sensitive Information using Reversible Steganography Scheme.

Chapter 6 We have designed an algorithm using a pseudorandom sequence for real-time application. This chapter address research question RQ-(5). It uses a chaotic system to allocate sitting arrangements of students during an examination to preserve academic institutes' integrity.

Chapter 7 summarizes the work in this chapter. This chapter concludes the contributions of the work.

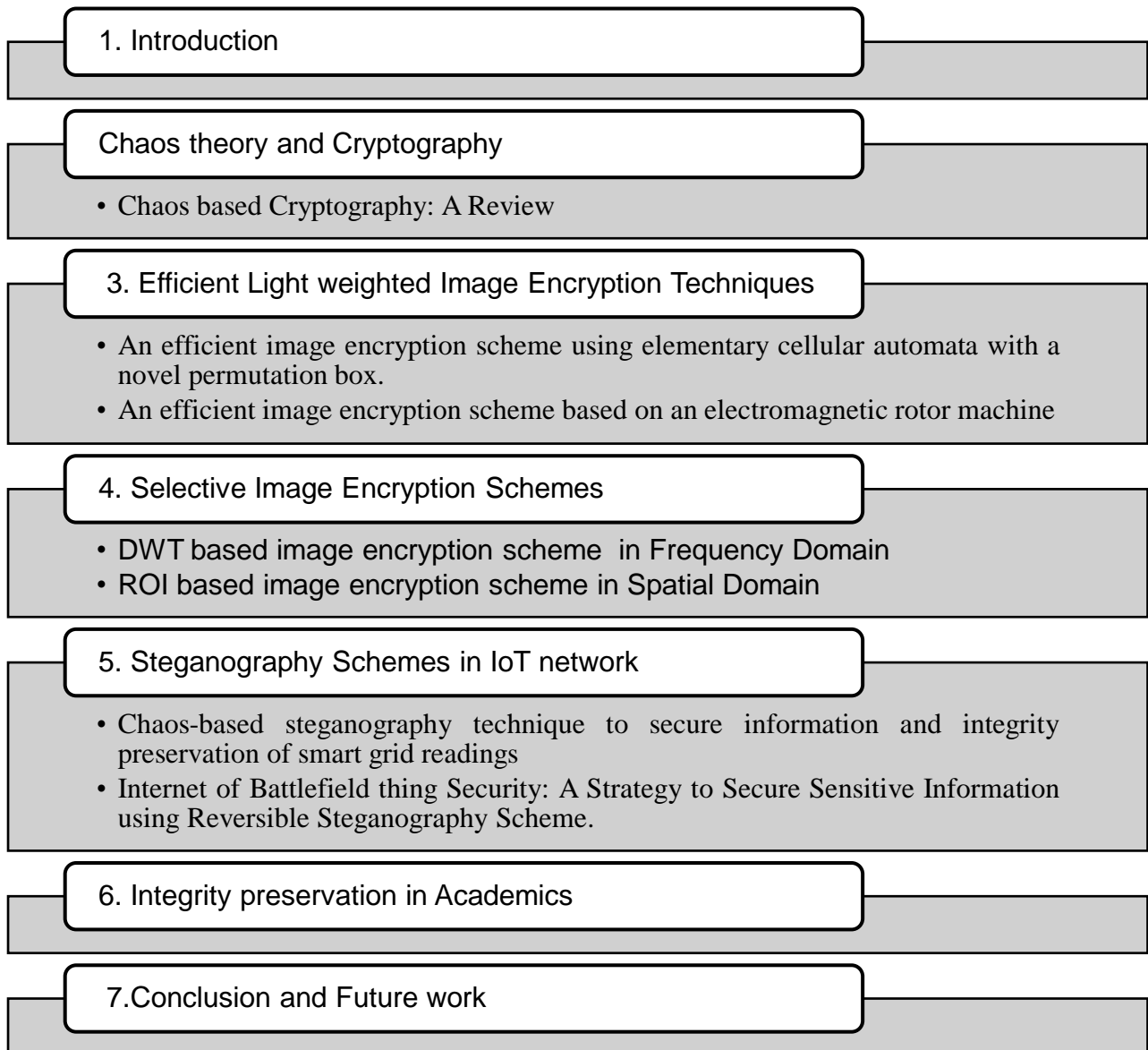


Figure 1.12 Thesis overview

CHAPTER 2

Chaos Theory and Cryptography

2.1 INTRODUCTION OF CHAOS THEORY

Chaos is a Greek word that means unpredictable and is studied under the nonlinear dynamic system. Chaotic systems are popular for their randomness and non-predictable behaviour. Chaos theory defines dynamic systems that are extremely sensitive to their initial parameters. Eventually, every result depends on these initial parameters. In the last few decades, a chaotic signal [61]–[63] is widely used in the cryptography system. Chaos theory is prevalent in recent times, and it is found that many researchers are working in the same direction using various chaotic maps. Chaos theory has emerged in various fields of science and has become useful and attractive due to its properties.

This chapter presents an in-depth review of cryptography schemes and chaos-based cryptography schemes. In the last two decades, security services are achieved by advanced methodologies, which are prominent and reliable, and most of them are based on chaos theory. This chapter investigates the chaos based cryptography schemes and also compares chaotic maps. Chaotic maps and the generated sequence are examined, and their behavior is analyzed on specific parameters to evaluate their performance. The literature review facilitates to find the appropriate system for real-time applications. A general encryption algorithm is applied to obtain PSNR, entropy analysis, SSIM, and time analysis to evaluate different chaotic maps' performance. Thus, experimental results exhibit maps' performance. This study shows that traditional methods are the foundation of the advanced schemes; however, new algorithms are more suitable for bulky sized data. Comparative analysis of different algorithms and evaluation of chaotic maps provides a better understanding of nonlinear systems and cryptography.

Chaos theory is used in several disciplines, including meteorology, engineering, economics, physics, and biology. There exist several kinds of chaotic systems that inherit the property of

chaos theory. Chaotic systems such as Logistic map, Henon map, Tent map, Lorenz attractor, Rossler attractor, and Piecewise linear chaotic map are popular for their property and randomness. The orbit of these map defines the randomness in the attractor field depending upon these initial parameters. Chaos theory is a mathematical physics which has been driven by Edward Lopez. It is stated as follow:

"Chaos: When the present determines the future, but the approximate present does not approximately determine the future."

In this chapter, chaotic maps have been analyzed and the recent approaches for image encryption schemes are studied. This study shows that all the chaotic maps are different from each other in many aspects and capable of generating significant results and contributing to image encryption schemes.

2.1.1 HISTORY OF CHAOS THEORY

In 1960, Lorenz was busy working on the problem of weather prediction, which cannot be solved on its own with a set of twelve equations [64]. A computer program was made to predict the weather theoretically. Once he wanted to see the specific sequence for prediction analysis, he started solving the problem in the middle of the sequence and running the program with slightly changed values. Output sequence evolved to be different. To save the paper, he had a printout of only three decimal places and the pattern deviated from the initial pattern, wildly different from the original in the end position. Eventually, it was found that the computer stores numbers in their memory up to six decimal places. The original sequence had the number equal to 0.506127, and he typed only the first three digits, 0.506. The new output sequence and the driven map were completely different from the previous sequence and a correlation between the sequence was found very low. This effect is known as the butterfly effect. The computed difference in the two curves' starting points is so small that it is comparable to a butterfly flapping its wings. This phenomenon is referred to as chaos theory and it observed that the initial condition decides the behavior of chaos. A slight change in the initial conditions can result in a drastic change in a system's long-term behavior. Such a small difference in a measurement might be considered background noise, experimental noise, or the equipment's inaccuracy.

2.1.2 CHAOTIC SYSTEMS

A system based on chaos theory is called a chaotic system. There are specific parameters to control chaotic maps' behavior and depend on the observations and experiments [64], [65]. The formation of the chaotic map depends on the initial seeds and the parameters; accordingly, the orbit and trajectory of the map are plotted. If a system is based on the sensitivity of initial parameters and topology, it is called a chaotic system. This theory is named so due to the fact that the systems described by this theory are disordered [66], [67], but in reality, chaos theory is all about finding the underlying order in a random sequence. The Chaotic maps are nonlinear systems involved in scientific applications due to their properties, such as ergodicity, dynamicity, randomness, and pseudorandom numbers [68], [69]. Chaotic Maps are dependent on initial conditions and parameters that control the map's chaotic behavior, and it is the primary element to make an ideal cryptosystem.

- 1. Chaotic maps are random in behavior but completely deterministic in nature:** chaotic systems' behavior is purely deterministic but seems to be random. Hence, for the same initial values, the chaotic system produces the same sequence repeatedly. Furthermore, a chaotic dynamical system is defined by the equations that can produce the sequence, and every sequence helps in iteration to produce the next sequence; Thus, the previous state specifies the next state. [39], [70], [71] .
- 2. Highly sensitive to the initial conditions:** A chaotic system is iterated with the initial state (parameters and seeds). A slight change in the initial state plot the different dynamical systems [72]. For example, initial variables are initialized to 0.01 and 0.2 for a chaotic system and then slightly changed to 0.01000001. It does not produce the same sequence as generated by the original initial seed values of the chaotic system.
- 3. Unpredictable:** If any user has the information about the current state, the next state of a chaotic system can not be guessed. It is almost impossible to predict the future states of the chaotic system in the long term, as stated in [73].

2.1.3 ATTRACTOR

Chaotic systems are too complex to visualize through naked eyes. However, certain techniques are available by which we can abbreviate them into a one-point graph. Earlier researchers began

to discover that the complex systems undergo some kind of cycle, even though other parameters are not duplicated or repeated. An attractor is a set of variables that evolves in a discrete dynamical system. This set of variables moves dynamically with time and are closely related to each other. They are represented algebraically with the vector dimension. In short, an attractor is a region in n-dimensional space. The region growth of attractor depends on the dimensional variable set. An attractor [74] can be a curve point and a strange attractor knows a complicated way of fractal structure. The dissimilarity between an Attractor and a Strange Attractor is that an Attractor represents a state to which a system finally settles. In contrast, a Strange attractor represents a trajectory of a system that moves from position to position without settling.

2.2 CHAOTIC MAPS

A chaotic map shows some sort of chaotic behavior in its trajectory. There are two types of chaotic maps (a) discrete-time chaotic maps (2) continuous-chaotic maps. Discrete maps habitually take the form of a module that is iterated recursively. 1-D chaotic maps are applied to data sequence or document. On the other hand, 2-D or higher-dimensional chaotic maps are employed for image encryption. The reason is that the image can be considered a 2D array of pixels. The literature upon chaos consists of standard terms such as a map. A map is nothing but a function whose value is uniquely determined by one or more input variables.

2.2.1 ONE-DIMENSIONAL CHAOTIC MAPS

A one-dimensional map deals with only one physical quantity. It is a rule relating that feature's value at one time to its value at another time. Graphical representations of these data are common in nature. Traditionally, the input or older value is across the horizontal axis and the corresponding output value or function is represented on the vertical axis. A list of some of the one-dimensional chaotic maps is given below:

Complex Squaring Map

- Complex Quadratic Map
- Duffing Equation
- Gauss Map

- Interval Exchange Map
- Logistic Map
- Tent Map
- Van Der Pol Oscillator

2.2.2 TWO-DIMENSIONAL CHAOTIC MAPS

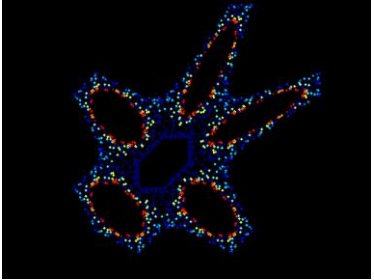
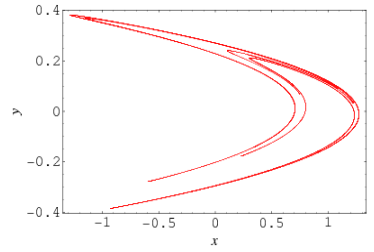
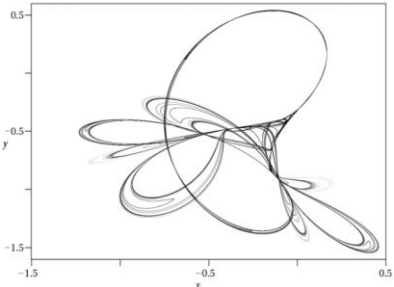
A two-dimensional map deals with more than one variable quantity. Two-dimensional chaotic maps exist as objects in a three-dimensional space, where x and y – *axis*s indicate the ruling equation of the chaotic map, and the z -axis is the temporal axis. A list of some of the two-dimensional chaotic Maps is given below :

- Arnold's Cat Map
- Baker's Map
- Duffing Map
- Exponential Map
- Henon Map
- Horseshoe Map
- Ikeda Map
- Kaplan-Yorke Map
- Tinkerbell Map

Chaotic maps are listed in Table 2.1. with the graphical representation:

Table 2.1 Graphical Representation of Different Chaotic Maps.

CHAOTIC MAP	EQUATION FOR MAP	PLOT
<p>Logistic Map</p>	$x_{n+1} = rx_n(1 - x_n)$	
<p>Rickers' Map</p>	$x_{n+1} = R(x_n)$ <p>Where, $R(x) = xe^{p-x}$ on $[0, \infty]$</p>	
<p>Sin Map</p>	$x_{n+1} = \sin(\pi x_n)$	
<p>Cubic Map</p>	$x_{n+1} = 3x_n(1 - x_n)^2$	

<p>Gingerbread Map</p>	$\begin{cases} x_{n+1} = 1 - y_n + x_n \\ y_{n+1} = x_n \end{cases}$	
<p>Henon Map</p>	$\begin{cases} x_{n+1} = 1 + y_n - ax^2 \\ y_{n+1} = bx_n \end{cases}$	
<p>Tinkerbell Map</p>	$\begin{cases} x_{n+1} = x_n^2 - y_n^2 + ax_n + by_n \\ y_{n+1} = 2x_ny_n + cx_n + dy_n \end{cases}$	

2.2.3 HENON MAP

Edward Lopez derived a Chaos theory, which is a part of mathematical physics. Chaotic systems are highly sensitive nonlinear, deterministic, and easy to reconstruct after filling in the image. Hénon chaotic map is one of the chaotic maps discovered in 1978 [1], [75], often used to generate pseudorandom sequences required for different mechanisms to provide security services in recent research. Hénon chaotic map is a two-dimensional discrete-time non-linear dynamic system and is used to generate a pseudorandom sequence; that is, it is required in different mechanisms to provide viable security services. It is used as a symmetric key cryptographic system in recent researches. Hénon chaotic map produces sequence using (2.1) and (2.2) that is described below:

$$X_{n+1} = 1 + Y_n - a \times X_n^2 \tag{2.1}$$

$$Y_{n+1} = bX_n \quad n = 0,1,2 \dots \quad (2.2)$$

Initial seeds X_1 and Y_1 works as a key for the following equations Eq. (2.1) and Eq.(2.2) of the chaotic map to produce pseudo-random numbers, and used for encryption in most of the research literature. Initial seeds X_1 and Y_1 [75] work as a key for the chaotic map.

The dynamic behaviour of the system depends on a and b values. The system cannot be chaotic unless the value of a and b are 1.4 and 0.3, respectively, as shown in (2.3) and (2.4)

$$X_{n+1} = 1 + Y_n - 1.4 \times X_n^2 \quad (2.3)$$

$$Y_{n+1} = 0.3X_n \quad n = 0,1,2 \dots \quad (2.4)$$

Henon map is defined in the discrete-time domain and in most common cases, they are described by iterated functions. Since Hénon map is deterministic, so decryption of the cipher produces original information at the receiver's end with the same initial seeds X_1 and Y_1 . Thus, the sensitivity of a key and encryption algorithm contributes to avoiding different types of cryptanalysis attacks.

These seeds are of major importance in private key cryptography and are used in encryption and decryption algorithms for privacy. Therefore, a key must be transmitted through a secure channel. Representation of the Henon map is illustrated in Fig. 2.1.

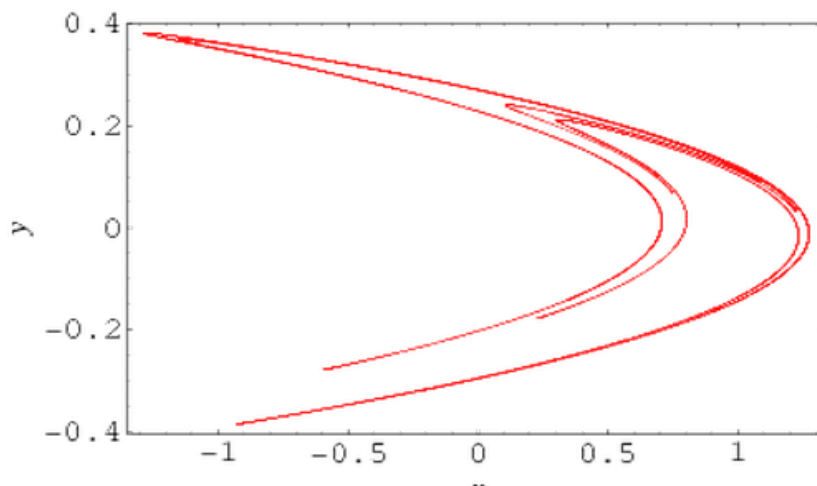


Figure 2.1 Two dimensional representation of Henon Map

2.2.4 TINKERBELL CHAOTIC MAP

Tinkerbell chaotic map, a discrete-time dynamic system, is defined as a two-dimensional chaotic map [76]. It is assumed that the Tinkerbell map derives its name from the famous Cinderella story. The Tinkerbell map exhibits vibrant dynamics, including chaotic behavior and a range of periodic states. It is mostly used to produce chaotic sequences that are deterministic and preserve pseudo randomness property.

$$x_{n+1} = x_n^2 - y_n^2 + ax^n + by^n \quad (2.5)$$

$$y_{n+1} = 2x^n y^n + cx^n + dy^n \quad (2.6)$$

The chaotic behavior of the system depends upon the variables a, b, c, d. n defines the discrete number of iterations that are used to produce the sequence. x_0 and y_0 together work as a key for the proposed cryptosystem, the initial seed of the iteration is used to generate a pseudorandom number sequence.

2.2.5 ARNOLD CAT MAP

Russian mathematician Vladimir I. Arnold developed a system based upon chaos theory to shuffle an image known as Arnold cat map. It is a two-dimensional invertible chaotic map, which is used as a scrambling algorithm in cryptography schemes, also known as cat face transform [77]. Any square size image of size $N \times N$ is used as an input to produce a shuffled image, and a scrambled image is obtained by applying Eq. (2.7) as shown below:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \text{ mod}(N) \quad (2.7)$$

Here, the dimension of an image is denoted by $N \times N$, and coordinates of the pixels within an original image are denoted by x, y , and x', y' , which are new positioned coordinates of an original image [78]. Reconstruction of the original image from a scrambled image is done by using Eq. (2.8).

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} \begin{bmatrix} x' \\ y' \end{bmatrix} \text{ mod}(N) \quad (2.8)$$

2.3 CHAOS BASED CRYPTOGRAPHY

In the past few decades, chaotic systems are used in cryptography to secure multimedia over insecure networks. A chaotic system based on confusion and diffusion was developed in 1989 [66]. Although it was already being used for the cryptographic system but there was no theorem to prove the authenticity of the chaotic map. Chaotic systems have attracted cryptography due to the characteristics such as sensitivity, nonlinear, unpredictability, and random-look nature, deterministic and easy to reconstruct after filling in the multimedia [64].

The traditional cryptographic system was based on the integer number system, whereas chaotic systems used floating-point numbers for encryption transformation. The initial parameter is a meaningful term associated with the encryption key or decryption key in cryptography algorithms. The correlation between modern cryptography and chaos-based cryptography algorithms is illustrated in Fig. 2.2. chaotic systems have all the required properties to make an ideal cryptosystem. The chaos theory is applied to various security primitives like block cipher, hash function, and pseudorandom number generator [56], [79].

- **Block Cipher Based on Chaotic Systems:** A block cipher is a transformation function used to map the units of plaintext bits to ciphertext bits consisting of the same unit size. Several Chaos-based algorithms use block cipher schemes to develop cryptosystems, in which permutation and substitution of blocks are considered.
- **Hash Function Based on Chaotic Systems:** SHA-1 is an extensively used hash function that has importance in several security applications and protocols. Since 2005, when SHA-1 was attacked, It has been an attraction for several researchers to designed a novel secure hash function using chaos theory.
- **Random Number Generators Based on Chaotic Maps:** Researchers worldwide started working in chaotic systems to design pseudorandom number generators. Several stream cipher algorithms are based on pseudorandom number generators (PRNGs) and usually the keystream of generator XORed with plaintext to generate the correspondence ciphertext using mathematical operations. Moreover, it is crucial to

generate the secret keys and initialization variables by PRNGs. In literature, it is found that chaotic systems are used in many applications to produce the PRNG.

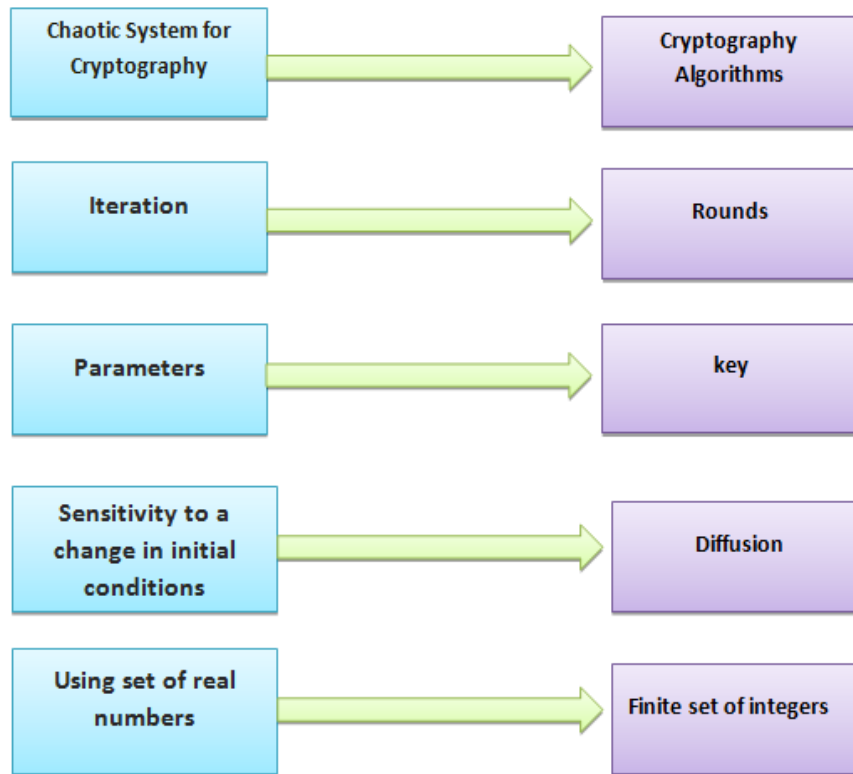


Figure 2.2 Relationship between chaotic systems and cryptography

In [61], [80], [81], chaotic systems have collaborated with other existing fields like DNA and wavelet transforms to provide a more realistic and reliable approach to advancing security protocols. Chaotic systems are used to generate the pseudorandom sequence. These sequences are treated as a keystream to obtain a cipher image.

Since image encryption techniques are based on Shannon's confusion diffusion strategy, they are more sustainable against statistical attacks. Table 2.2. Exhibits the chaotic map-based cryptography schemes, where several researchers have proposed algorithms based on confusion diffusion.

Table 2.2 Recent Chaos-based Image Encryption Algorithms

Scheme	Parameter for the encryption process	Purpose	Confusion Module	Diffusion Module	Test performed	Remark
[82]	Keystream cipher	Confidentiality	2D rectangular transform	Tent map with pseudorandom numbers [0 255]	Keyspace, key sensitivity, histogram, correlation analysis, entropy, NPCR, UACI, robustness, speed test	It is based on an enhanced version of 2D rectangular transform by adding some variable values.
[83]	Bit level and column level indexing and shuffling (between pixels)	Confidentiality	Henon chaotic map Lorenz map Chua attractor Rossler attractor	-	Keyspace , correlation analysis FIPS PUB test (monobit test, poker test, runs test, long-run test) NPCR, UACI	Sequences are used to arrange pixels and bits among pixels using chaotic maps.
[63]	Blocks pixels	To secure Bulky images, i.e., satellite images	nil	Henon map, Chebyshev, cubic, sine, Tent map	Maximum deviation, information entropy, Histogram analysis, Keyspace analysis, key sensitivity analysis, performance analysis	Average encryption time is less than 0.31 second
[73]	One-time pad scheme	confidentiality	Arnold cat map	Modifies Logistic map	Entropy analysis, Histogram analysis	The maximum Lyapunov exponent is used to check the chaotic behavior of a new chaotic map
[58]	Block based cipher	Confidentiality with compression	Chebyshev map	6 D chaotic map	Entropy, Histogram, Correlation, NPCR, UACI, Time complexity Chosen plaintext and ciphertext attack analysis	Compressive sensing is applied using gauss matrix based on a chaotic map.
[84]	2 Round of S Box using cyclically shifted	Confidentiality	Enhanced Rectangular transform, S Box	Double Dependent substitution based on logistic map	Chi-square statistics, Correlation analysis, information entropy, Histogram analysis, NPCR, UACI, Keyspace analysis, speed analysis, robustness against cropping attacks	Rectangular transform scramble nonsquare images, and S box is applied during the confusion phase on each pixel.

[85]	One-time pad (XOR)	Confidentiality	Arnold cat map, logistic tent map, logistic sine map	Tent + sine map,	Keys space, Histogram, Correlation, entropy, NPCR, UACI, PSNR	A discrete fractional random transform is used after the diffusion process.
[51]	All pixels of an image	Confidentiality	5-D multiwing hyper-chaotic system is used to shuffle pixel and bits	5-D multiwing hyper-chaotic system	Keys space, Histogram, Correlation, Key sensitivity, entropy, NPCR, UACI	keystream is strongly related to plain-image
[86]	Chained block scheme	Compression, integrity and encryption	Chaos-based encryption and Huffman coding	arbitrarily	PSNR, Entropy, Correlation analysis	MAC is used to provide integrity
[1]	One time pad scheme	Confidentiality	Bit level permutation	Hénon chaotic map with Key-value transformation	Entropy, correlation analysis, mean value analysis, histogram analysis, key sensitivity test	To secure object-oriented images and size is not fixed of the region. It is adaptive as per the region
[87]	Multiplication and addition operations	Confidentiality	Logistic map with optimised sequences	Logistic map with optimized sequences	Decryption error, secret key size analysis, key sensitivity, histogram, correlation, differential, chosen/known plain attack, entropy, time analysis	Image characteristics is added to the key resist known plain image attack.

2.4 EXPERIMENTAL RESULTS AND OBSERVATIONS

In this section, chaotic maps are analyzed and initiated with initial seed value to generate sequences for the encryption scheme as per Algorithm 2.1. The MATLAB R2015a software has been used for the simulation purpose. The proposed framework has been applied similarly to all the chaotic maps described in Table 2.3. The standard image of 'lena.jpg' of size 204×204 is taken as input for the encryption process. Comparative performance matrices are listed in Table 2.3. Structural similarity index (SSIM) [88], (peak signal to noise ratio) PSNR, entropy and sequence generation time analysis is done to evaluate the performance. In addition, range and Cut-off point are also determined that can be used to generate binary sequence on the basis of the threshold value. SSIM is used to quantifies the degradation quality of an image after encryption. For the ideal cryptosystem, the SSIM and entropy value must be near zero and eight, respectively. Figure 2.3 illustrates that all the chaotic maps obtain SSIM values that are

near to zero. Sequence generation, time analysis graph is illustrated in Fig. 2.4.; it shows that all the chaotic maps are fast enough to generate the sequence. Here PSNR values are calculated between original and encrypted images, thus low PSNR value indicated an ideal cryptosystem as shown in Table 2.3.

Algorithm 2.1: The encryption algorithm

1. Start
2. initiate seed and control parameters
3. Read an image with size [m, n]
4. generate sequence [X] of size m×n using a chaotic map
5. Keystream= (X ×10⁷) mod 255
6. Encipher all the pixels of an image using the generated keystream. The procedure applies to all the pixels in a bitwise manner.
7. End

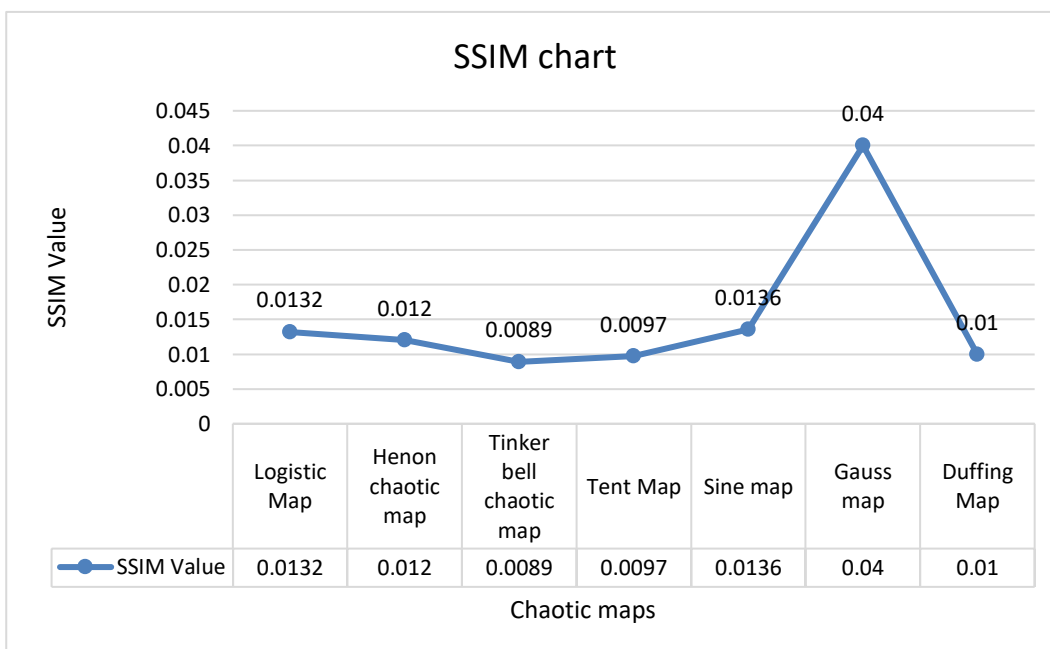


Figure 2.3 Structural similarity index measures of chaotic maps

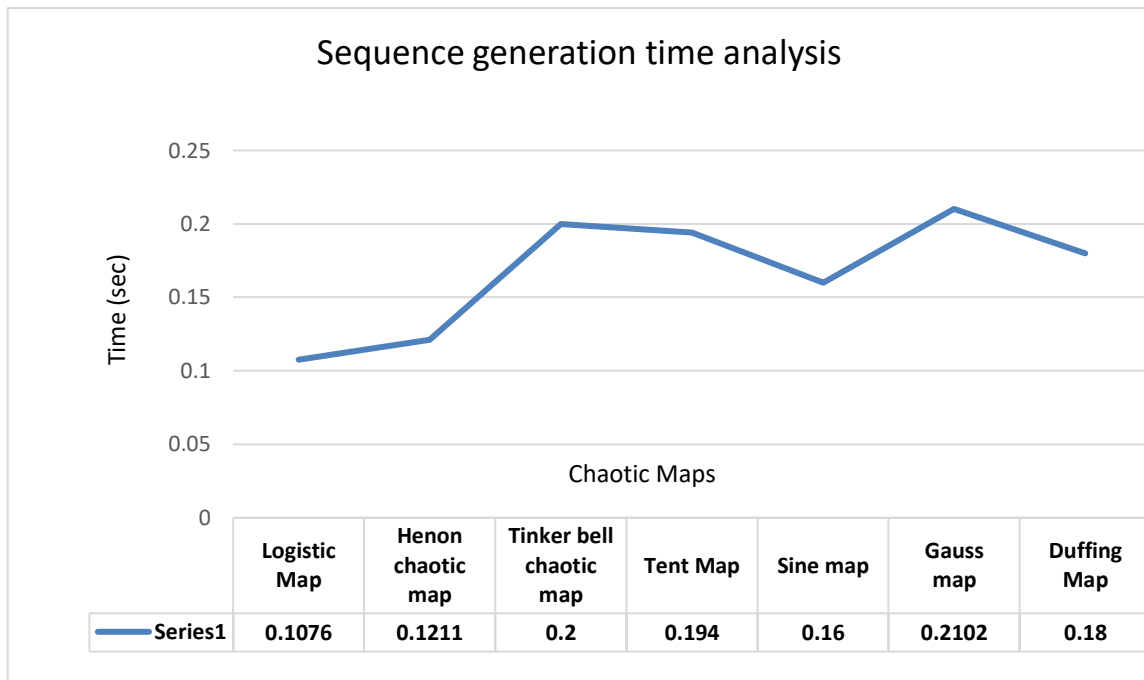


Figure 2.4 Sequence generation time analysis of chaotic maps

Table 2.3 Chaotic Maps and Performances

	Equation	Parameters	Range	Cut-off point	PSNR	entropy
Logistic Map	$x_{n+1} = rx_n(1 - x_n)$	$3.57 \leq r \leq 4$	[0.00001 0.99]	0.551	27.57	7.99
Henon chaotic map	$x_{n+1} = 1 + y_n - ax_n^2$ $y_{n+1} = bx_n$	a=1.4 b=0.3	[-1.2846 1.2730]	0.4142	27.58	7.99
Tinker bell chaotic	$x_{n+1} = x_n^2 - y_n^2 + ax_n + by_n$ $y_{n+1} = 2x_ny_n + cx_n + dy_n$	a=0.9 b= -0.6013 c=2, d=0.5000	[-1.231 0.4600]	- 0.1128	27.55	7.99

map						
Tent Map	$x_{n+1} = \begin{cases} \mu x_n & \text{for } x < 0.5 \\ \mu(1 - x_n) & \text{for } x > 0.5 \end{cases}$	$\mu=1.99$	[0.00014, 0.999]	0.49	27.54	7.99
Sine map	$x_{n+1} = \lambda \sin(\pi x_n)$	$\lambda = 0.99$	[0.0001, 0.99]	0.522	27.59	7.99
Gauss map	$x_{n+1} = \exp(-\alpha x_n^2) + \beta$	$\alpha = 4.9,$ $\beta = 0.5$	[-0.1434, 0.4000]	0.035	27.20	7.81
Duffing Map	$x_{n+1} = y_n$ $y_{n+1} = -bx_n + ay_n - y_n^3$	a=2.75 b=0.2	[-1.7095, 1.7095]	0.1938	27.59	7.9954

2.5 TEST CASES FOR PERFORMANCE MEASURES

To assess the performance of cryptosystems, many metrics are available in research. The performance measures used in our work for the evaluation of the proposed algorithms using several test cases. In the thesis, test cases are identified to examine the proposed work after a literature review and also implemented to evaluate security performance. The number of test cases is used in the thesis to check the vulnerability and the performance of the cryptosystems are:

- Encryption Illustration
- Differential Attack
 - NPCR
 - UACI
- Statistical attack
 - Histogram analysis
 - Correlation analysis
- Security key analysis
- PSNR
- Mean values analysis
- Information entropy analysis
- Speed performance
- PRD (Percentage residual difference test)

- Bit Error Ratio

These test cases are discussed below in brief:

2.5.1 ENTROPY ANALYSIS

In 1949, Shannon proposed a mathematical equation to calculate the uncertainty and randomness of the information source. Shannon entropy is also used as a primitive measure to check uncertainty within an image [89]. If Shannon entropy is calculated near to eight, it indicates that the encrypted image has uniformly distributed pixels with a high order of randomness and the texture of an image is so complex and unreadable; it is the ideal case of encryption. In a permutation cipher, the entropy of a cipher image always remains the same as an original image because in cipher, usually pixels are shifted to other coordinates within the image and the information could be accessible in cipher images; Therefore, the entropy of encrypted image decides the ability of cryptosystem. Therefore, confusion is not the complete solution to encrypt an image; a combination of confusion and diffusion makes it more effective. Shannon entropy formula can be seen in equation (2.9)

$$H(X) = -\sum_{i=0}^{N-1} P_i \log_2 P_i \quad (2.9)$$

2.5.2 CORRELATION ANALYSIS

It is a statistical measure to find the closeness of two variables or datasets. Correlation is also calculated to determine the pixel strength within an image; based on it, texture can be classified. When the correlation of plain image is calculated, it is either positive or negative, whereas the correlation of encrypted image must be near $\cong 0$. When correlation is found near to ideal value, it is considered that the encryption scheme is an effective scheme. Correlation analysis is conducted within an image on pixels with respect to their neighborhood pixels [1] [39]. In the literature, for the simulation of correlation analysis, random pixels along with their neighbor pixel in horizontal, vertical, and diagonal directions of original as well as encrypted images are considered. The formula of correlation analysis is given in the following equations.

$$D(r) = \frac{1}{N} \sum_{i=1}^N [r_i - E(r)]^2 \quad (2.10)$$

$$Cov(r, s) = \frac{1}{N} \sum_{i=1}^N [r_i - E(r)][S_i - E(s)] \quad (2.11)$$

$$r_{r,s} = \frac{Cov(r, s)}{\sqrt{D(r)}\sqrt{D(s)}} \quad (2.12)$$

where r_i and s_i are 8-bit values of two contiguous pixels. N represents the total number of pixel pairs.

2.5.3 HISTOGRAM ANALYSIS

Histogram of an image is a visual representation of pixel intensity values. It is not the measurement to challenge any type of statistical attack [90]. However, obtaining authorized information from an encrypted image for an intruder is not easy, whose histogram is evenly distributed. The intensities of pixels are plotted on the scale of intensity level versus a count of pixel intensity. In a gray image, there are 256 different intensities plotted with the help of a histogram.

2.5.4 KEY SENSITIVITY TEST

In order to attain an efficient system, the initial seed (keyspace) must be large over the range of 2^{100} , i.e., the key size must be of at least 100 bits to resist brute force attack, where an attacker tries to find the actual key; it is fulfilled in chaos-based cryptosystems due to the large precision of seeds. Thus, it is highly sensitive to the initial key conditions and deterministic. It is assumed that systems are made for public access, and it is open for all the users, now security relies upon the key. A system should be sensitive to its keys; a slight change in the key generates a different result than applying the original key pair. It is observed that the generated image at the receiver

end with the wrong key is entirely different from the original image (that was supposed to generate with the original key values).

2.5.5 DIFFERENTIAL ATTACK

1)NPCR 2) UACI

The differential attack is an important way to crack the encryption algorithm. Intruders typically make little changes to the plain image (e.g., alter only one pixel or slight changes in a key) to observe the working technique of the encryption algorithm. By comparing the differences, the cryptanalyst can detect the subtle relationship between the plain image and the resulting cipher image. The number of changing pixel rate (NPCR) and unified average changed intensity (UACI) tests are performed on two encrypted images [91]. Encrypted C image originates from the original image and the other Encrypted image C' is found by changing one pixel in the original image to determine the strength against differential attack. Theoretical ideal values of NPCR and UACI scores are 1 and 0.33, respectively.

$$NPCR = \frac{\sum_{(i,j)} D(i,j)}{m \times n} \times 100\% \quad (2.13)$$

$$\text{where } D(i,j) \begin{cases} 1 & \text{if } (C(i,j) \neq C'(i,j)) \\ 0 & \text{if } (C(i,j) = C'(i,j)) \end{cases}$$

$$UACI = \frac{1}{m \times n} \left(\sum_{i,j} \frac{|C(i,j) - C'(i,j)|}{255} \right) \times 100\% \quad (2.14)$$

2.5.6 KEYSPACE ANALYSIS

The reliability of the cryptosystem is based on the keyspace. A keyspace is called as the total number of different keys entirely to be used in the algorithm. Keys, which are used in encryption algorithm, is carried forward to the receiver through the secure channel. The computational precision for 64-bit double-precision numbers is 10^{-15} ; it is based on the IEEE floating-point standard format [59]. Thus, in a two-dimensional chaos-based cryptosystem, a user can configure 64×64 bit keyspace. To resist the cryptanalysis attacks, keyspace must be in the range of large numbers (integer, binary, and real numbers).

2.5.7 PERCEPTUAL SECURITY: PEAK SIGNAL-TO-NOISE RATIO (PSNR)

PSNR usually applies to signal to check the distortion level and the quality after retrieval at the other end. In cryptography, PSNR measures the perceptual security of the proposed algorithm, and it is calculated between the original image and its cipher image. Researchers suggest that the lower values of PSNR indicate that a proposed system encrypt the multimedia efficiently. MSE values must be high in the cryptosystem (i.e., cipher image must be entirely different from its original image, so MSE values must be on the higher side of the scale).MSE and PSNR are inversely proportional (High MSE indicates lower values of PSNR). PSNR (in dB) is calculated by the following Equation:

$$MSE = \frac{1}{m \times n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [(I(i, j) - \Omega (i, j))^2] \quad (2.15)$$

$$PSNR = 10 \log_{10} \left(\frac{255^2}{MSE} \right) \quad (2.16)$$

Where $I(i, j)$ and $\Omega (i, j)$ represents the original image and cipher image, respectively.

2.5.8 MEAN VALUE ANALYSIS

Mean value analysis is an important measure to check the correctness and level of secrecy of a cipher image. It is a calculation of the vertical distribution of mean pixel values of an image until the width of an image is reached [92]. The mean value of input plain image varies along the width of the image. On the other side, a cipher image in mean value visual representation that remains consistent along with the width of the image. It can also be seen that the mean distribution of the cipher image is very close to each other and is uniform in the distribution graph of mean values.

The mean is calculated using equation (2.17), where A is an image having N scalar observations. Mean value analysis gives the average intensity distribution of pixels in any direction of an image. Usually, it is calculated in a horizontal direction across the image. On the contrary, encrypted images are assumed to have a balanced amount of chaotic information with no significant meaning. In mean value analysis, the plot of such encrypted images remains constant, which is the ideal case of an encryption algorithm.

$$\mu = \frac{1}{N} \sum_{i=1}^N A_i \quad (2.17)$$

2.6 SUMMARY

In this chapter, chaotic maps are examined and studied, and it is found that chaotic maps are rich in features and can perform cryptographic operations in an insignificant amount of time. These chaotic maps are based on a simple calculation and can be implemented in limited resources. It is also analyzed that all these chaotic maps performed well with images; it is evident through entropy, SSIM and PSNR tests. In this study, different chaotic maps are studied and it is observed that different parameters are available to evaluate the performance of the cryptosystem.

However, the prime goal is only to achieve confidentiality in chaos-based schemes using stream cipher techniques. Pseudorandom sequences are useful in all the fields of science, and thus, sequence generation time can improve the speed of systems based on chaotic maps.

Therefore, this chapter emphasizes chaos-based schemes and experimental results show that it can be used in real-time applications. Evaluation of chaotic maps and Comparative analysis of different algorithms provides a better understanding of nonlinear systems and cryptography.

CHAPTER 3

Efficient Light-Weighted Image Encryption Techniques

3.1 PRELIMINARIES

In this chapter, we first introduce the preliminaries to understand the concept of image encipherment schemes and then walk through two proposed schemes. With the deployment of network-based technologies, the web world is more concerned about the privacy of multimedia-based information over the Internet [93]. In recent years, many devices such as mobile, TV, smart meter, sensor node, and military surveillance devices, etc., can receive and transmit information over the Internet; humans or inbuilt functions usually operate such devices. Military data transfer and personal conversation between two people have equal importance and need to be confidential. When information is transmitted, ethically, it should reach its destination without any interference of others, which is taken care of by cryptography. Multimedia is an emerging field that deals with different forms of information such as text, images, audio, sensor data and videos in an integrated manner. With the advancement of devices to display multimedia and enabling them to transfer it from one location to another has resulted in increasing danger of their security issues. Because of this, the secrecy of information is an essential critical component while transmitting or storing such information [94]. In a hostile environment, security services are required as per the organizations and individuals need to protect their valuable information and resources. In this context, over the past two decades, dynamic systems and other practices have emerged with cryptography to provide security services like confidentiality, authentication, integrity and non-repudiation [95].

There are several standards that are designed to provide security services under ITU-T X.805 to individuals and organizations [13]. For security services; security mechanisms are also standardized by ITU-T X.805, which are followed by all the countries. With the advancement of technologies, various attacks are also updated with time. Hence comes the need for revised versions of mechanisms to resist such attacks. Several methodologies are implemented that are usually based upon symmetric and asymmetric key cryptography, which uses different algorithms. Billions of people are getting connected to each other through the Internet and exchange a large amount of personal information over the network. It becomes very important to secure such sensitive information from unauthorized users and chaotic maps are used for that purpose, i.e., based on confusion diffusion. Each multimedia element holds particular types of characteristics, which define the behavior of the multimedia unit. For example, in the English language, 26 alphabets with some grammar rules are used to form the statement, and 'E' and 'T' are the most frequently used letters in the English language. So, when text is encrypted by any scheme, letters of the text are enciphered into different letters [27], [29]. In the hill cipher scheme, statistical attacks are not possible, whereas in Vigenère cipher, there are some properties of the language that remain unchanged in the ciphertext. Therefore, a crypt-analyst can use this statistical information to break a cryptographic algorithm.

As issues and objectives are explained above, two algorithms have been proposed in this chapter. This chapter has two Models, and the algorithms are listed below:

- (a) **Model 1** : An Efficient Image Encryption Scheme Using Elementary Cellular Automata with Novel Permutation Box.
- (b) **Model 2** : An Efficient Image Encryption Scheme based on electromagnetic rotor machine. IoT Friendly Image Encryption Schemes

The algorithm and their analysis have been described in the next sections.

3.2 EFFICIENT IMAGE ENCRYPTION SCHEME USING ELEMENTARY CELLULAR AUTOMATA WITH NOVEL PERMUTATION BOX

As explained in chapter 2, chaotic maps are widely used in all aspects of cryptography to provide privacy and authentication. A significant extension policy of cellular automata systems in cryptography and its properties has also been added to a series of dynamic systems.

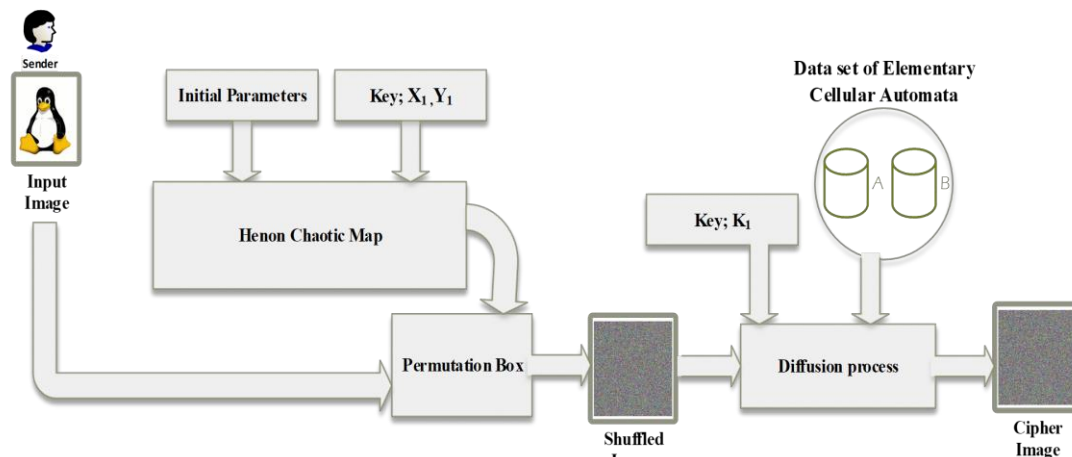


Figure 3.1 The architecture of the proposed algorithm (Model 1)

Randomness, unpredictability, chaotic and dynamic behavior are some of its fundamental properties. J. Von Neumann and Stan Ulam gave self-producing automata theory in the year 1950. Besides, Stephen Wolfram extended the concept by adding generation and local transition rules concepts, i.e., cellular automata (CA) theory; also, Wolfram was the first person to implement cellular automata-based stream cipher [96]. Meanwhile, various cellular automata properties have been investigated, and attention was given to its use in the privacy and other security models. The proposed work is based upon the confusion and diffusion theory. The algorithm is designed, taking into account all the above statements and the architecture of the proposed algorithm is exhibited in Fig. 3.1., where the permutation box and the encryption module operate as confusion and diffusion, respectively.

A.A. Abdo et al. [55] proposed an algorithm on elementary cellular automata; in this algorithm, a special kind of periodic boundary cellular automata with unity attractors is used. From the viewpoint of security, the number of cellular automata attractor states are changed with respect to the encrypted image, and different key streams are used to encrypt different plain images. The cellular neural network with chaotic properties is used as the generator of a pseudorandom keystream. Jun Jin [97] proposed a new image encryption/decryption scheme. The behavior of a number of elementary cellular automata (ECA) of length 8 with periodic boundary conditions is investigated of rule 42. It is also found in the state-transition diagram that some ECA rules result in state attractors satisfies the basic requirement of the encryption/decryption scheme that can perform encrypting function to substitute the pixel values. Simulation results on some grayscale and color images show that the proposed image encryption method satisfies the

properties of confusion and diffusion. In [98], cellular automata (CAs) are used to design a symmetric key cryptography system based on Vernam cipher. CAs are applied to generate a pseudorandom number sequence (PNS) which is used during the encryption process. In [99], Wolfram introduced a cellular automata-based cryptographic scheme for symmetric encryption protocol using one-dimensional cellular automata. Rey [100] presented a secure protocol for message communication using finite cellular automata as a hash function, which results in different hash digest for different messages. Azza A.A. et al. [101] proposed a novel technique using cellular automata called Multi-Secret image sharing scheme with steganography in which unary attractors are used to share the secret images. In 2020, Babaei et al.[102] proposed cellular automata and DNA sequence based image encryption technique, though having high computational cost and large memory space. Enayatifar et al.[103] also proposed an algorithm on the same concept using CA along with DNA. Authors have worked on indexed based technique that requires heavy computation due to DNA sequence. Thus, the technique is not found suitable for those applications in which limited resources and memory spaces are limited. In [104] Roy proposed a programmable cellular automata (PCA) based block cipher which utilizes the characteristics of programable cellular automata to encrypt the image by using the rule table of 8×256 values as a data structure.

In this work, state **attractors/transitions** are analyzed under elementary cellular automata (ECA) rule space, which is introduced as a lookup table for the cryptosystem. The objectives of this work are as follow:

- (a) To develop a novel cryptosystem using cellular automata to achieve confidentiality while sending images over the public networks and IoT networks.
- (b) To propose a lightweight framework to be implemented with minimum hardware requirements (based on simple mathematics). Rules are analyzed, and generations are found from the rule space to identify the specific property of the cryptography. For eight-bit values, several rules are tested and the generations are stored in a tabular form to operate the encryption/decryption module.
- (c) To design a permutation box, i.e., is governed by a key, unlike other traditional permutation schemes which are based on the algorithm; here, the key decides the shuffled location of the original pixel. Since the permutation box is solely dependent on the key, it can also be called a keyed transposition scheme. For the purpose, the Henon chaotic map is used, which is initiated by the initial key pair, which is used as a

key for the cryptosystem.

- (d) To develop the encryption module based on substitution cipher schemes, in which pixel values are substituted into other values and it is achieved with a minimum number of computation and mathematical operations.

3.2.1 CONCEPT OF ELEMENTARY CELLULAR AUTOMATA

Elementary cellular automaton is widely used for various applications of science due to its properties. We have identified and developed generations or transition of states by applying cellular automata rules based upon periodic boundary conditions, which can be used to secure any multimedia information. To design a permutation box (P Box), Hénon chaotic map is associated with the proposed work to produce pseudorandom numbers. Overall properties of Henon chaotic map and ECA play a major role in leading the algorithm, which is discussed in this section and also, it is also explained how these rule tables are extracted from the rule space of ECA. Henon map is described in chapter 2, and it is used in model 1 to designing the P Box.

3.2.1.1 Elementary cellular automata

Cellular automata (CAs) is a dynamical, physical, discrete-time computational model widely used in various fields of science and technology [105], [106]. Pseudorandom number generation, pattern recognition, and developing games (Conway's Game of Life is a top-rated game based on cellular automata) are a few of the applications of CA [107]. CA evolves on an array of cells or lattice of neighboring sites. CA is classified into two categories based on the lattice structure of identical sites (cells). When CA is deployed over a one-dimensional grid, it is known as one-dimensional cellular automata or elementary cellular automata. In two-dimensional cellular automata, CA spreads over a 2-D grid structure with several neighborhood configurations of cells. In 2-D cellular automata, Von-Neumann, Moore, Cole and smith model are popular in several applications of image processing and cryptography.

Elementary cellular automata (ECA) is a one-dimensional mathematical model based on discrete number of input and output [108], [109]. Automata based systems are constructed depending upon certain criteria, i.e., number of cells, state of a cell (0 or 1), participation of neighboring cells and choice of local rules. State values are binary values, either zero or one. Each cell is surrounded by its adjacent cells on both sides; if a cell integrates itself with its neighbors, this whole cell sequence can be called 3 neighborhoods and the selection of

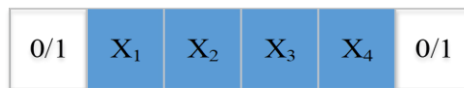
neighbors for the boundary cells can be decided by different conditions as shown in Fig. 3.2.

Three-neighborhood cells with radius one and every cell having two states are also known as ECA, and in each iteration, a cell has two possible values, either 0 or 1, and accordingly, distinct neighborhood configurations will be: $2 \times 2 \times 2 = 8$.

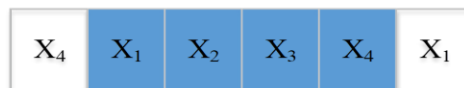
In equation (3.1), Let t, i represent time and index of a cell, respectively. New state of a cell (x_i^{t+1}) depends upon the current state of its neighboring cells i.e. x_{i-1}^t and x_{i+1}^t .

$$x_i^{t+1} = f(x_{i-1}^t, x_i^t, x_{i+1}^t) \tag{3.1}$$

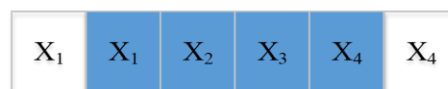
Since $f()$ is a Boolean function of combinational logic, it produces a binary value depending upon the local rule of elementary cellular automata. Therefore, $x_i^{t+1} \in \{0,1\}$. At every discrete time step (clock cycle), Boolean cellular automata sites update their state by using some rules (combination function or rule). Table 3.1. exhibits the nature of local transition rules of ECA. Assume, S_0 represents $(000)_2$ binary block format, S_1 represents $(001)_2, \dots, S_7$ maps to $(111)_2$ binary block configuration. Now, these eight different binary block configurations can be



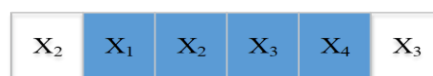
(a) Fixed boundary condition



(b) Periodic boundary condition



(c) Adiabatic boundary condition



(d) Reflexive boundary condition

Figure 3.2 Cellular automata boundary conditions

evolved with discrete-time in 2^8 different possible ways. Therefore, the rule table of cellular automata has 256 distinct rules from rule 0 to rule 255. Each rule has its characteristics and pattern in elementary cellular automata, which influences the state of cells.

Table 3.1 Ruleset for Distinct Cell Compositions

S ₇	S ₆	S ₅	S ₄	S ₃	S ₂	S ₁	S ₀	RULE NUMBER
0	0	0	0	0	0	0	0	RULE 0
0	0	0	0	1	1	1	1	RULE 15
1	1	1	1	1	1	1	1	RULE 255

In setup, we have identified elementary rules which support stream cipher property. If the same rules are applied to entire cells of lattice, then it is called uniform cellular automata; otherwise, it is called hybrid cellular automata. Here, we have applied the same rule to the entire grid of cells. Among four boundary conditions, the periodic boundary condition is selected to generate the state attractor. In every iteration, when a rule is applied at time t and at time $t + 1$, state of a cell gets updated and this transition is known as an attractor.

To investigate the chaotic behavior of cellular automata rules, Periodic boundary condition is applied with all the 8-bit grayscale possible values, i.e., D here, and numerous rules are tested [110]. It is found that rule 15 has the ability to perform some cryptographic functions. Corresponding combination logic rule of 15 can be written as:

$$S_i^{t+1} = \overline{S_{i-1}^t}$$

Periodic boundary condition works as a ring for 8-bit value to determine the next state of the current state and we have recursively applied the same rules to the previous output at time $\{t + i \mid 0 \leq i \leq 7\}$. and this output has 256 distinct global states. We have tested up to nine generations for each and every $0 \leq D \leq 255$. Generations are further tested to accumulate the progress of the rules in such a way to be characterized by XOR and XNOR. We have determined and extracted two different tables, Table 3.2 and Table 3.3. In which, TABLE 3.2 is based on XOR property and Table 3.3 is based on XNOR property.

$$Ruletable I = \begin{cases} D \oplus generation_1 \oplus generation_2 \dots \oplus generation_6 \oplus generation_7 = 0 \\ D \oplus generation_1 \oplus generation_2 \oplus generation_3 = 0 \end{cases} \quad (3.2)$$

$$Ruletable II = \begin{cases} D \oplus generation_1 \oplus generation_2 \dots \oplus generation_6 \oplus generation_7 = 255 \\ D \oplus generation_1 \oplus generation_2 \oplus generation_3 = 255 \end{cases} \quad (3.3)$$

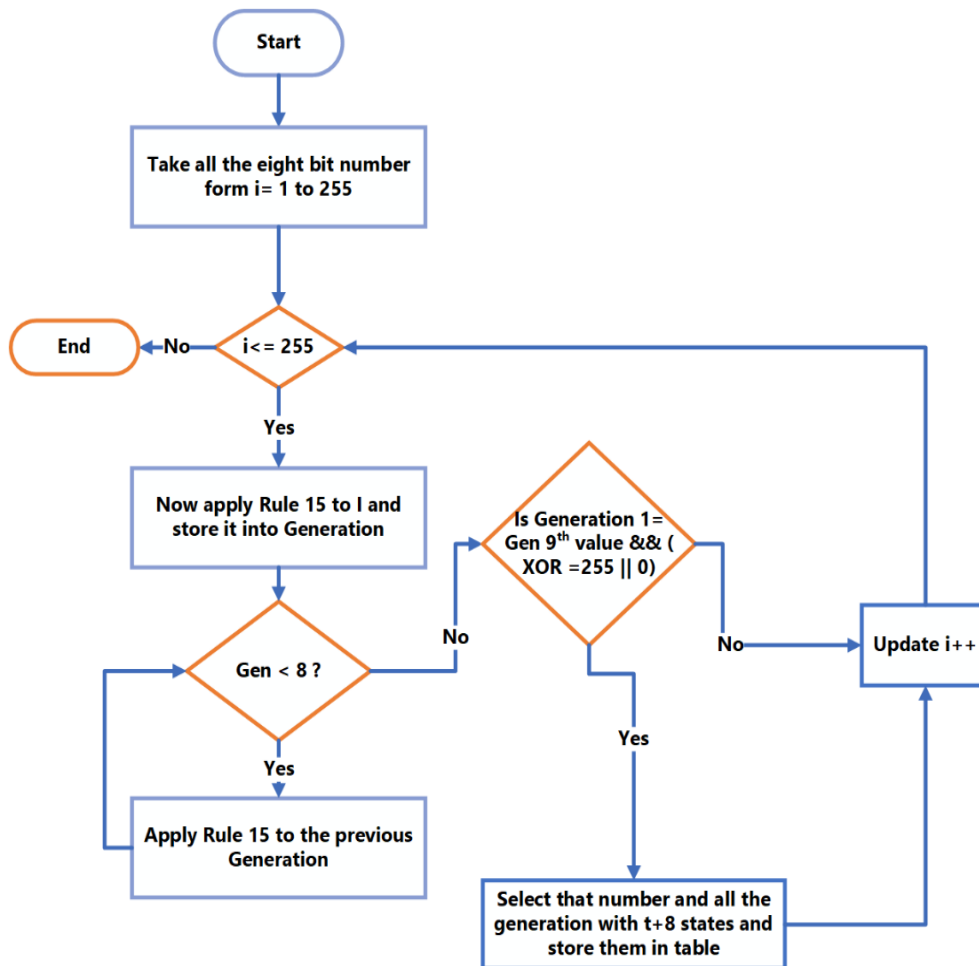


Figure 3.3 Flowchart of rule space investigation and extraction for rule tables

In the following attractors, it is investigated further that attractors are updated in each iteration and XOR operation is applied between iterated values after applying rule 15 with ECA. It yields either 255 or 0 as shown in equations (3.2) and (3.3). In the proposed cryptosystem, state attractors tables have been extracted using the property of XOR XNOR logic operations generated by ECA; out of 33, 31 attractors are chosen with eight states. In Fig. 3.3, The flowchart of the procedure is given with all the necessary steps.

Table 3.2 ECA based RULETABLE I

Row	Column								
	1	2	3	4	5	6	7	8	
1	0	0	0	0	0	0	0	0	0
2	3	126	192	159	48	231	12	249	0
3	5	125	65	95	80	215	20	245	0
4	6	252	129	63	96	207	24	243	0
5	9	123	66	222	144	183	36	237	0
6	10	250	130	190	160	175	40	235	0
7	15	120	195	30	240	135	60	225	0
8	18	246	132	189	33	111	72	219	0
9	23	116	197	29	113	71	92	209	0
10	27	114	198	156	177	39	108	201	0
11	43	106	202	154	178	166	172	169	0
12	45	105	75	90	210	150	180	165	0
13	46	232	139	58	226	142	184	163	0
14	51	102	204	153	0	0	0	0	0
15	53	101	77	89	83	86	212	149	0
16	54	228	141	57	99	78	216	147	0

Table 3.3 ECA based RULETABLE II

Row	Column								
	1	2	3	4	5	6	7	8	
1	1	127	64	223	16	247	4	253	255
2	2	254	128	191	32	239	8	251	255
3	7	124	193	31	112	199	28	241	255
4	11	122	194	158	176	167	44	233	255
5	13	121	67	94	208	151	52	229	255
6	14	248	131	62	224	143	56	227	255
7	19	118	196	157	49	103	76	217	255
8	21	117	69	93	81	87	84	213	255
9	22	244	133	61	97	79	88	211	255
10	25	115	70	220	145	55	100	205	255
11	26	242	134	188	161	47	104	203	255
12	35	110	200	155	50	230	140	185	255
13	37	109	73	91	82	214	148	181	255
14	38	236	137	59	98	206	152	179	255
15	41	107	74	218	146	182	164	173	255
16	42	234	138	186	162	174	168	171	255

3.2.2 PROPOSED ALGORITHM

The proposed algorithm is designed in the context of sensitive information of digital color and gray images. The algorithm is performed in two iterative stages. In the first phase, confusion is performed, and after that diffusion process takes place. Shuffled image is obtained by the shuffling procedure (section 3.2.2.1), which is based on the property of keyed based transposition method. ECA is a vital core part of the second phase of the algorithm. A shuffled image is used as an input for the second phase of the encryption module. Let us consider a digital color image I with dimension $m \times n \times 3$. (i.e., m rows and n columns) and its grayscale image is represented by $I_{m \times n}$. A digital color image is decomposed into 2D channels, which are $Red_{m \times n}$, $Green_{m \times n}$, $Blue_{m \times n}$. Since the proposed algorithm is designed for two-dimensional images, thus the dimension of 2D image is $I_{m \times n}$. Each channel supports [0 255] decimal values represented in the 8-bit binary format of the computer system. The following subsections discuss the procedure for gray images, which can be performed on color images as well.

3.2.2.1 Keyed Transposition Method

Input: plain image I

Output: shuffled image I'

The correlation between pixels of the same area within an image is very high due to the same texture in the region, whereas an ideal cipher image should follow a negligible correlation among pixels. Therefore, shuffling is useful to disturb the relationship between adjacent pixels. In traditional cryptography, the majority of P boxes are designed for text information, but they are found not suitable for images and videos. In the spatial domain, pixel location of an image is represented by mathematical function $f(x, y)$, where x represents horizontal axis, and y represents vertical axis of an image. In the first phase, the shuffling process is done using Hénon chaotic map, which is based on keyed transposition property. Hénon chaotic map is a two-dimensional map where X_1 and Y_1 are used as a key to generate pseudorandom numbers. Using these numbers, a new pixel location $f(x', y')$ is generated for every pixel $f(x, y)$ of an original image, and as a result, a pixel is shifted to a newly updated location. Therefore, it is really hard to visualize the shuffled image to get sensitive information from it. Here, confusion is achieved by the shuffling method, whereas to achieve diffusion, a shuffled image is used as an input for

the diffusion process. Fig. 3.4 demonstrates the working procedure of the method, where random integers 1 to n is generated as per the following steps :

Step 1. Henon map is initialized with initial parameters a and b , and specific constant values of these parameters develop chaotic behaviors of Henon map.

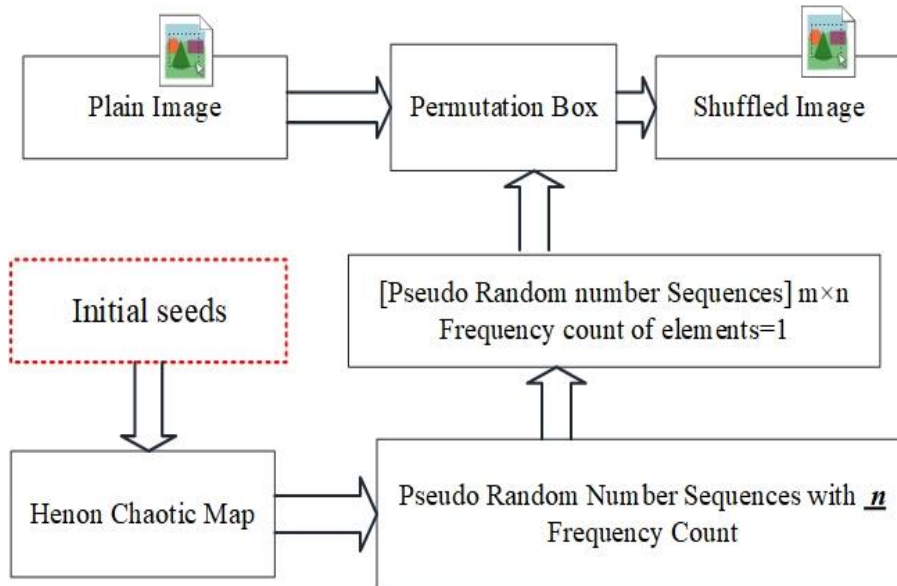


Figure 3.4 Keyed transposition scheme

Step 2. X_1 and Y_1 referred to as a secret symmetric key for the shuffling procedure and chosen by the sender; these initial seeds are kept private by the user for privacy purposes.

Step 3. In the next step, Henon chaotic system is used as a keystream generator for the proposed cryptosystem. The size of sequence depends upon the size of an image. If the input image size is $m \times n$, then the number of the sequence is produced of size $m \times n$. Thus, Sequence values are obtained by using Eq. (2.1) and Eq. (2.2), i.e., is iterated as per the size of an input image.

Step 4. Sequence values are obtained in signed float number format; $X \in \{-I, +I\}$.

Step 5. For all float numbers of X , the modular arithmetic concept is used to change the values of X under the range of $[1 m \times n]$.

$$New_X = [(m \times n) \times X_{m \times n}]$$

$$New_matrix = (New_X \bmod N) + 1$$

It follows that $[New_matrix] \in [1,2,3 \dots \dots \dots m \times n]$,

Frequency count of elements in $New_matrix \geq 1$

Step 6. Subsequently, New_matrix stores duplicate values and for all the numerical values of New_matrix , frequency count of all the elements (bin) and store it into $Frequency_count$.

1. Initialize $i = 1$.
2. while $i \leq m \times n$
3. Count frequency of i in New_matrix and it is represented by $Frequency_count$;
4. $Frequency_matrix[i] = Frequency_count$;
5. $i = i + 1$;
6. while end

Step 7. Now the next step after calculating $Frequency_count$ of the matrix is to remove all the duplicate numbers and create a matrix with a single frequency count. A detailed procedure is explained in Algorithm 1.

After applying step 7. of the shuffling procedure, $[New_matrix]_{m \times n} \in [1 m \times n]$, where the frequency count of each element is one

Step 8. Covert image into a one-dimensional image and coordinate (x, y) of an image $I_{(x,y)}$ is shuffled and shifted to a new location $F(x', y')$ using New_matrix . Thus, the **shuffled image I' is produced.**

1. Initialize $i \leftarrow 1$
2. **While** $i \leq N$
3. Shuffled image ($New_matrix(i)$) = image(i);
4. $i \leftarrow i + 1$
5. **While-end**

Furthermore, a one-dimensional shuffled image is converted into a two-dimensional image I' in a row ordered fashion of 2D array. The detailed procedure of the modules is explained in algorithm 3.1.

Algorithm 3.1. Permutation Box Generation Algorithm

1. initialize $i \leftarrow 1$
2. while i to $m \times n$ do
3. If $\text{Frequency_matrix}(i) == 0$ then
4. $\text{ptr} = i + 1$ until we find $\text{Frequency_matrix}(i) > 0$
5. $\text{Frequency_matrix}(\text{ptr}) = \text{Frequency_matrix}(\text{ptr}) - 1$;
6. search ptr value in New_matrix ; where it is found out in New_matrix , that value is replaced by i and $\text{Frequency_matrix}(i)$ is updated and it is increased by 1.
7. else if $\text{Frequency_matrix}(i) > 1$ Then
8. $\text{ptr} = i + 1$ until we Find $\text{Frequency_matrix}(i) == 0$
9. update $\text{Frequency_matrix}(\text{ptr}) = \text{Frequency_matrix}(\text{ptr}) + 1$
10. Search i in New_matrix , wherever it is found in New_matrix , on that location value of ptr is copied.
11. $\text{Frequency_matrix}(i) = \text{Frequency_matrix}(i) - 1$;
12. Repeat this process until $\text{Frequency_matrix}(i) == 1$
13. else $\text{Frequency_matrix}(i) == 1$ then
14. Do nothing in this situation.
15. endif
16. Increment i
17. while-end

3.2.2.2 Encryption Algorithm based on Elementary Cellular Automata

Input: shuffled image I'

Output: cipher Image Ω

In the second phase, elementary cellular automata become a significant component of the

proposed cryptosystem as shown in Fig. 3.5. Elementary cellular automata (ECA) operates on the shuffled image, where each pixel acts as a key for the next neighbor pixels, but for the first pixel of an image, a key **KEY1** is selected by a user. **Rule table I** and **Rule table II** are used for the encryption module. Each table has sixteen distinct transition state attractors with a length of eight states and four states. These state attractors are based on the property of the XOR and XNOR scheme. Traditionally, encipherment techniques are based on pseudorandom numbers. However, CA has emerged with cryptographic techniques. Rule tables are divided into different parts on the basis of XOR and XNOR properties, which are discussed in section 3.2. One more attractor is added in this list, where 0 decimal value is assigned to all eight states. Now, these state attractors are divided into two tables. Algorithm 3.2 includes all the steps of the encryption module in the form of an algorithm for better understanding.

Step 1. First, we choose a key **KEY1** for the first pixel of an image, and any 8-bit binary number is chosen as key **KEY1**. Then for the second pixel, the first pixel of the shuffled image behaves as a key and for the third pixel, the second pixel works as a key. The process is executed in a linear fashion to cover all the pixels of an image. Furthermore, this process is being continued for the remaining pixel until the last pixel of an image is encrypted with the second last pixel of the shuffled image.

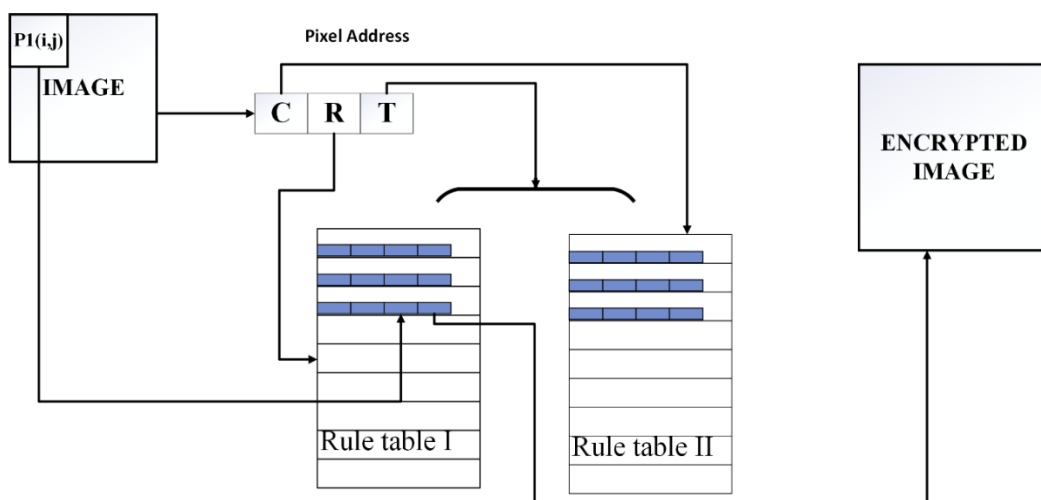


Figure 3.5 Visual representation of encryption algorithm

Algorithm 3.2 Encryption Algorithm

```

Encryption module (C, R, PTR)

8. while PTR ≠ 0 do
9.   Out = RULETABLE(R,C)XOR Out
10. C=C+1 in a modular fashion.
11. PTR=PTR-1
12. end
13. Encryption Algorithm (I', KEY1)
14. for i = 1 .....m do
15.   for j = 1 .....n do
16.     out= I' (i, j)
17.     convert Key1 in binary value with eight-bit
        representation.
18.     T = LSB(Key1)
19.     R = key1(Key1(7)to key1(4) )
20.     C = key1(Key1(3)to key1(1) )
21.     PTR =
        sum (i, j), summation in a modular airthmatic fashion with mod 8i,
22.   If T == 1
23.     Ruletable ← Ruletable I
24.     Call Encryption module (C, R, PTR)
25.   else T== 0 then
26.     Ruletable ← Ruletable II
27.     Call Encryption module (C, R, PTR)
28.   endif
29.   Ω(i,j) ← out
30.   Key1 = I' (i,j)
31. end for
32. end for

```

Step2. Pixel plays an essential role as a key to encrypt an image. Pixel is broken into fixed-size blocks with a specific width to execute the encryption process. LSB bit of a key, **Table number (T)** is used to reach the tables, **Row number (R)** and **column number (C)** are represented here by **R** and **C** respectively to trace the row and column index of the

selected rule table. Pixel index (i, j) determines the length of EXOR and EXNOR operations. A detailed procedure of the encryption module has been discussed below in Algorithm 2.:

3.2.2.3 Decryption Algorithm

Step 1. At the receiver's end, *KEY1* and the initial seed of Henon chaotic map are transmitted through a secure channel. The decryption algorithm is presented in Algorithm 3.3.

Step 2. It is assumed that these rule tables are public and anyone who is connected to the network can access it. Therefore, security relies upon the key *KEY1* and the P Box's initial seeds. A detailed procedure of the decryption process is explained in Algorithm 3. Which operates it first on the encrypted image Ω to obtain the I' . (that is still a shuffled image)

Step 3. The second phase of the decryption algorithm is based on the keyed transposition algorithm. Since the chaotic system behavior is deterministic, so the reconstruction of an image using the same keys X_1 and Y_1 at the receiver's end gives the decrypted image. At the receiver end, pseudorandom numbers are generated with secret keys and henon map, which are further used to get back pixel values at their original positions. This shuffled image I' is further arranged in order exactly opposite of the way done for encryption. Further shuffling of pixels in the shuffled image in reverse direction produces the original image (I).

3.2.3 EXPERIMENTAL RESULTS

In this section, the experimental results of the proposed image encryption algorithm are explained and discuss the efficiency and performance of the proposed algorithm. MATLAB R2015a software has been used for simulation and implementing the proposed algorithm. Standard input grayscale images and color images of size 256×256 are shown in Fig.3.6 and Fig. 3.7., respectively. The secret symmetric key for encryption is $X_1 = 0.1231, Y_1 = 0.1231$ is selected for Eq. (2.1) and Eq.(2.2) to initiate the P Box. Extracted State attractors tables, which are discussed in section 3.2, are used and the initial key $KEY1 = 15$ for the encryption algorithm is selected for the simulation process. The proposed algorithm is also applied to color images as well; here, standard leena.jpeg is selected for that purpose. Similar mechanisms are applied to all three channels of a color image separately. Several tests are performed to judge the efficiency of the proposed cryptosystem that is discussed in this section.

Algorithm 3.3 Decryption Algorithm

Decryption Algorithm (I', KEY1)

1. for $i = 1 \dots m$ do
2. for $j = 1 \dots n$ do
3. convert **Key1** in binary value with eight-bit representation.
4. $T = LSB(Key1)$
5. $R = key1(Key1(7) \text{ to } key1(4))$
6. $C = key1(Key1(3) \text{ to } key1(1))$
7. $PTR =$
sum (i, j), summation in a modular arithmetic fashion with mod eig
8. $Temp \leftarrow \Omega(i, j)$
9. **If** $T == 1$
10. **Ruletable** \leftarrow **Ruletable I**
11. Call Decryption module (C, R, PTR)
12. **else** $T == 0$ **then**
13. **Ruletable** \leftarrow **Ruletable II**
14. Call Decryption module (C, R, PTR)
15. $temp = 255 - temp$
16. **endif**
17. $Key1 = Decrypted_image(i, j) = temp$
18. **end for**
19. **end for**
- 20.
21. Decryption module (C, R, PTR)
22. $col = ((col + PTR - 1) \% 8) + 1$
23. $PTR = 8 - PTR$
24. **while** $PTR \neq 0$ **do**
25. $temp = RULETABLE(R, C) XOR (temp)$
26. $C = C + 1$ in a modular fashion.
27. $PTR = PTR - 1$
28. **End**

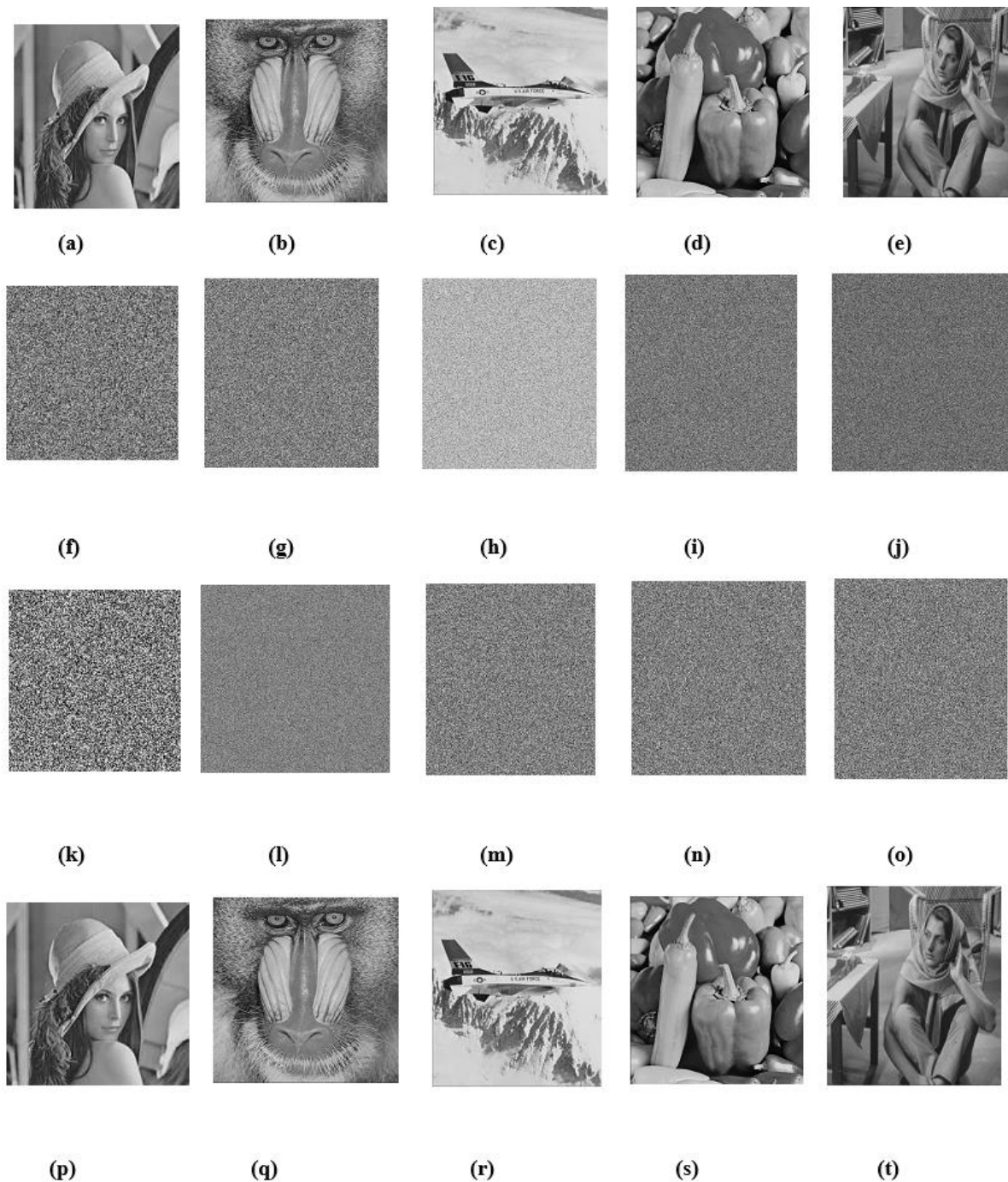


Figure 3.6 Visual illustration of plain images :(a) Leena (b) Baboon (c) Airplane (d) Peppers (e) Barbara; shuffled images in the same order : :(f) Leena (g) Baboon (h) Airplane (i) Peppers (j) Barbara; Encrypted images : :(k) Leena (l) Baboon (m) Airplane (n) Peppers (o) Barbara ; Decrypted images obtained by the proposed algorithm : :(p) Leena (q) Baboon (r) Airplane (s) Peppers (t) Barbara

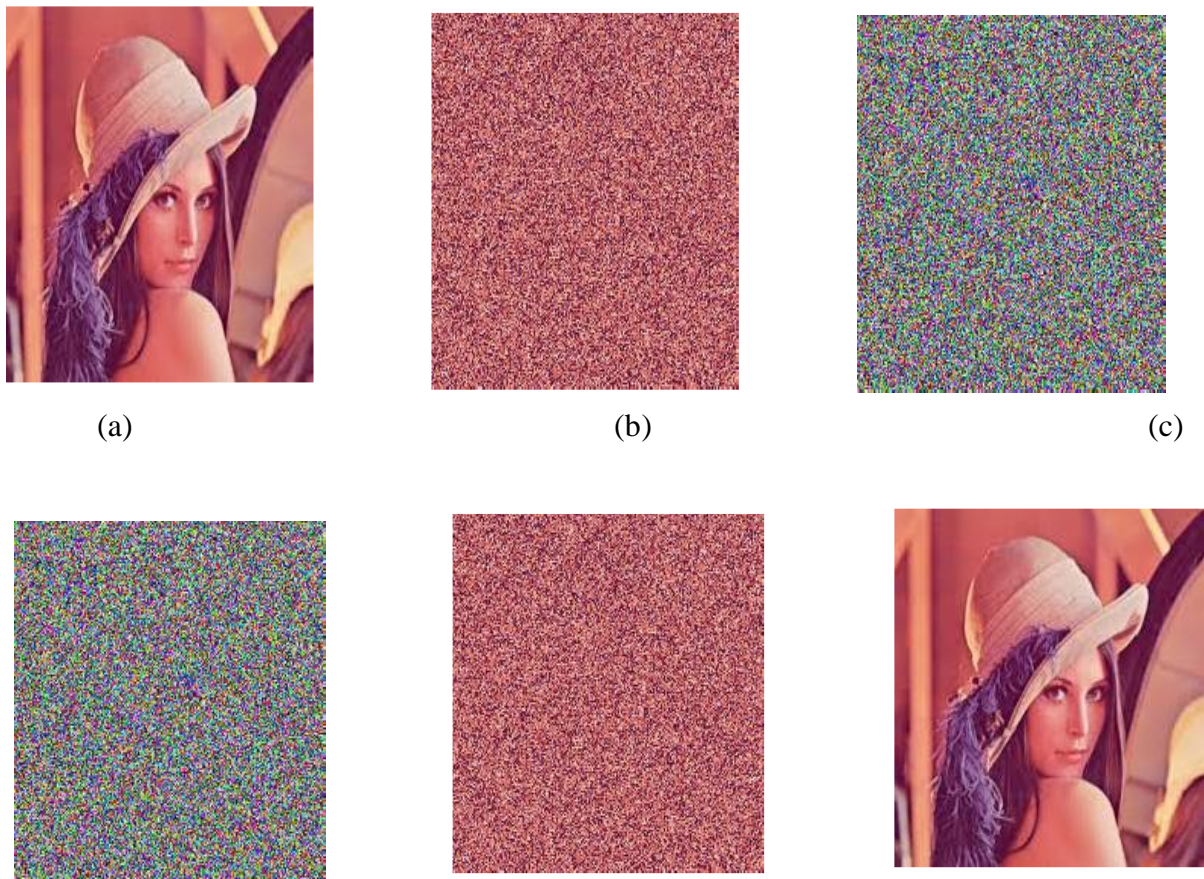


Figure 3.7 Visual representation of color image at sender end (a) Input test image :Lena , (b) Shuffled image of lena after applying P BOX(c) Encrypted image of lena. Visual representation of color image at receiver end by the proposed scheme: (d) Encrypted image (e) Image after applying CA based cryptosystem (f) Decrypted image

3.2.3.1 Entropy Analysis

Entropy analysis is done to calculate the uncertainty in the image cryptosystem. Shannon entropy is calculated using Eq. (2.9), and the obtained values are listed in Table 3.4 of different input images and cryptosystem produce good results in terms of entropy that is evident through the entropy Comparison of different existing models as shown in Table 3.4.

Table 3.4 Entropy Analysis of the Proposed System

Test images	Entropy (original image)	Entropy (encrypted image) Proposed	Ref.[111]	Ref. [97]	Ref. [104]	Ref.[51]
Leena	7.4318	7.9922	7.9909	7.9927	7.9646	7.8232
Baboon	7.2283	7.9934	7.9912	7.9934	7.9823	7.4069
Airplane	6.8114	7.9830	-	7.9837	-	7.0227
Peppers	7.5807	7.9937	-	7.9961	-	7.5378
Barbara	7.3986	7.9922	-	7.9942	-	7.3056

3.2.3.2 Correlation Analysis

It is a statistical measure to find the closeness of two variables or datasets. Correlation is also calculated to determine the pixel strength within an image; based on it, texture can be classified. For the simulation of correlation analysis, we have selected 2000 random pixels along with their neighbor pixel in horizontal, vertical, and diagonal directions of original as well as encrypted images.

The formula of correlation analysis is given in the equations Eq.(2.10). Eq. (2.11) and Eq. (2.12). Correlation analysis of different schemes and the proposed algorithm are shown in Table 3.5 and Table 3.6. correlation visual representation is illustrated in Fig. 3.8.

Table 3.5 Correlation Analysis and Comparison of Color Image

Color Image	Orientation	Red Channel	Green Channel	Blue Channel
Plain Image (Leena)	Horizontal	0.962	0.9683	0.985
	Vertical	0.9015	0.9466	0.9621
	Diagonal	0.87	0.91	0.9402
Cipher (proposed)	Horizontal	0.0141	0.0304	-0.00278
	Vertical	-0.0094	0.0034	-0.0083
	Diagonal	0.0159	-0.00170	0.0014
Ref. [111]	Horizontal	-0.0463	0.04359	0.01369
	Vertical	-0.05877	-0.0682	-0.0688
	Diagonal	-0.0200	-0.0052	0.0127

Table 3.6 Correlation Analysis of Grayscale Images

Color Image	Orientation	Test input image	Proposed algorithm
Leena	Horizontal	0.9457	0.0006
	Vertical	0.9751	-0.0227
	Diagonal	0.9102	0.0247
Baboon	Horizontal	0.8723	0.0135
	Vertical	0.8321	-0.0041
	Diagonal	0.7821	0.0107
Airplane	Horizontal	0.9301	0.0051
	Vertical	0.9632	-0.0150
	Diagonal	0.9.20	0.0185
Peppers	Horizontal	0.9615	-0.0164
	Vertical	0.9670	0.0297
	Diagonal	0.9408	-0.0146
Barbara	Horizontal	0.9393	0.0053
	Vertical	0.9515	-0.0035
	Diagonal	0.9061	-0.0111

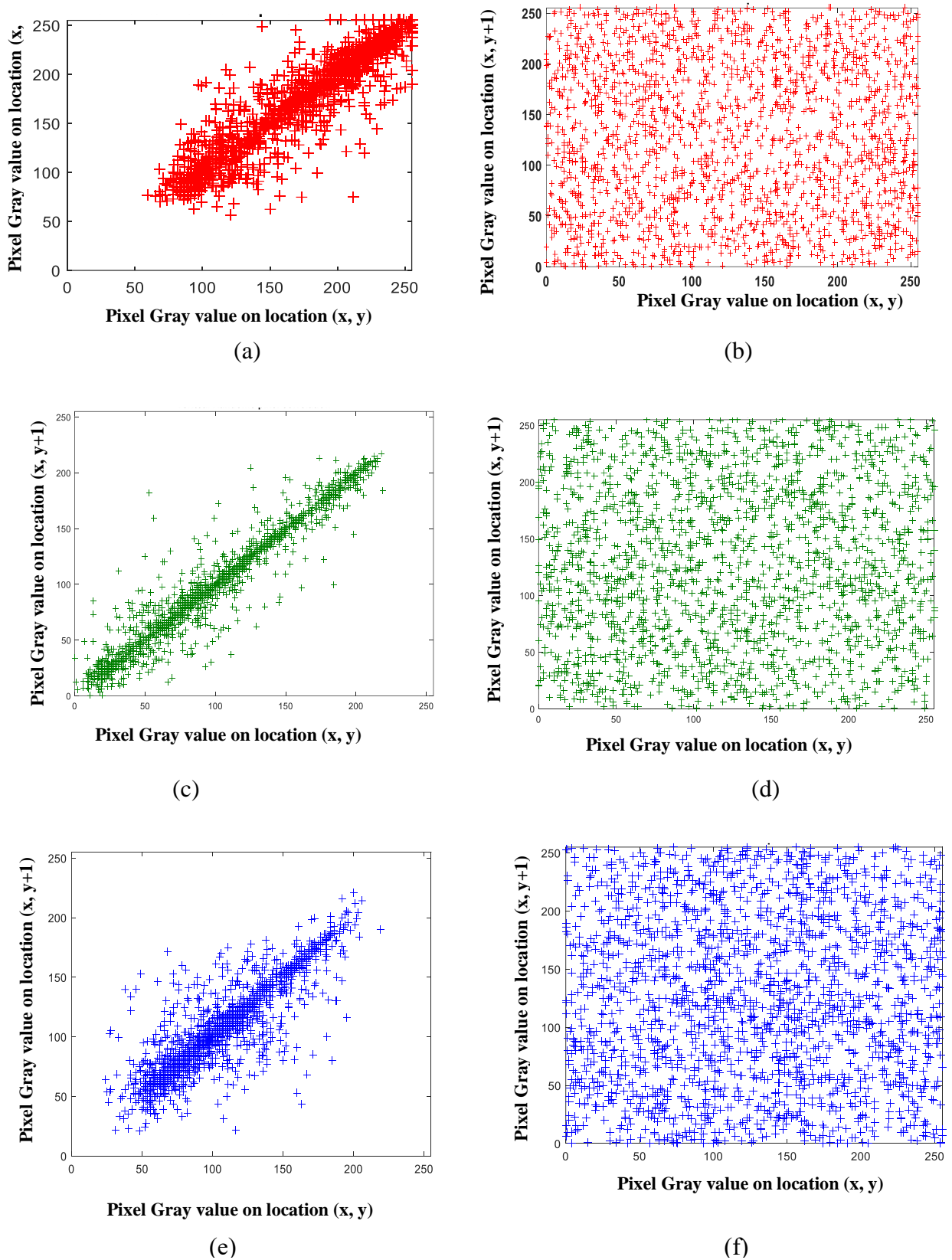


Figure 3.8 Correlation plot of two adjacent plain-image pixels of Leena in horizontal direction for the (a) red channel, (b) green channel, and (c) blue channel. Correlation plot of two adjacent pixels of the cipher-image obtained by the proposed scheme: (d) red channel (e) green channel (f) blue channel

3.2.3.3 Histogram Analysis

A histogram of an image is a visual representation of pixel intensity values. Figure 3.9 shows uniform distribution of grayscale pixel values in cipher image, and significantly different from the histogram of the original image, which proves that encrypted image does not help intruders employ a statistical attack on encryption procedure.

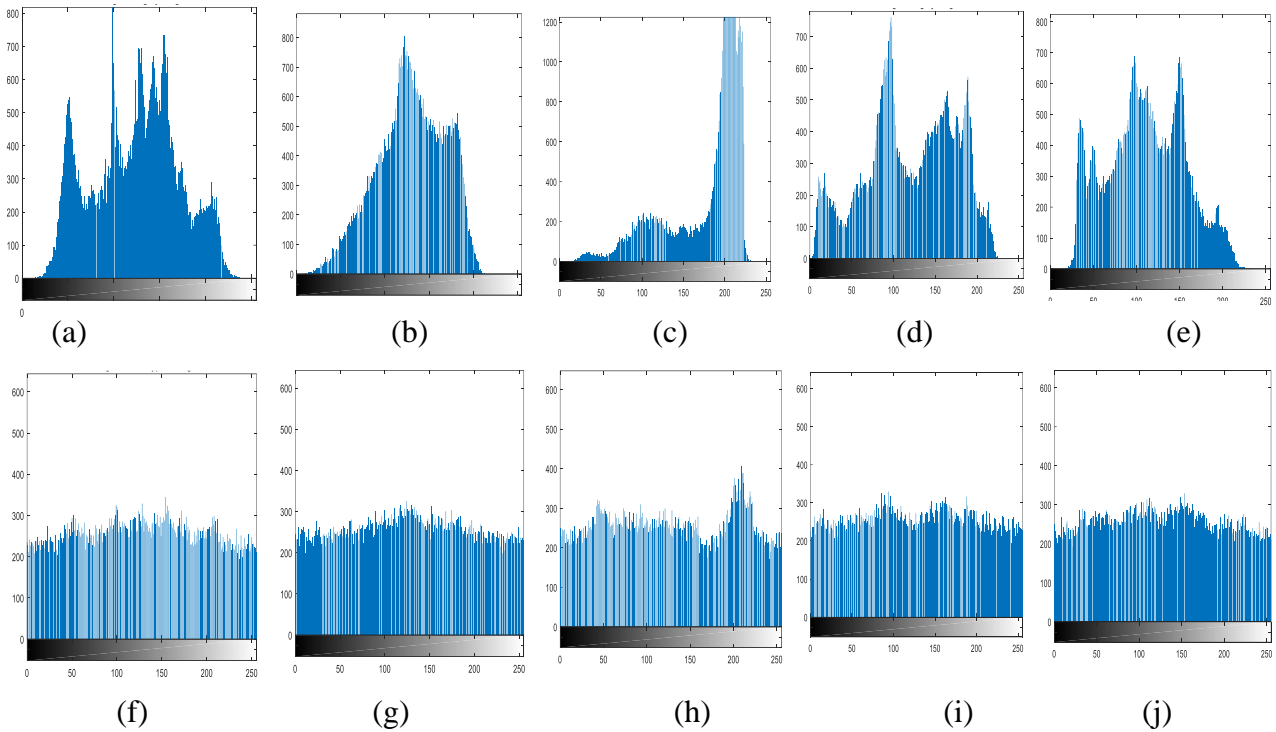


Figure 3.9 Histogram plot of grayscale Images:(a) Leena (b) Baboon (c) Airplane (d) Peppers (e) Barbara; Histogram of encrypted images by the proposed scheme: (f) Leena (g) Baboon (h) Airplane (i) Peppers (j) Barbara

3.2.3.4 Key sensitivity Test

It is assumed that the proposed system is public, and it is open for all the users; now, security relies upon the key. The proposed system is sensitive to its keys. A slight change in the key generates a different result than applying the original key pair. We have replaced the key values from $X_1 = 0.1231, Y_1 = 0.1231$ to $X_1' = 0.12310001, Y_1' = 0.1231000021$, and the obtained image is shown in Fig. 3.10. It can be observed that the generated image at the receiver end is entirely different from the original image (that was supposed to generate with the original key values).

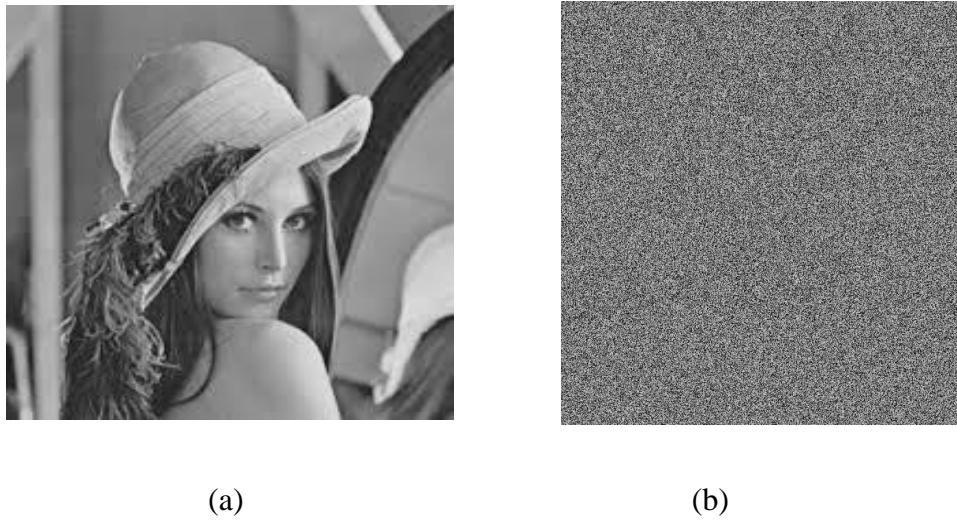


Figure 3.10 Key Sensitivity analysis (a) Leena (I), (b) cipher image with a wrong encryption key

3.2.3.5 Differential Attack Analysis

3.2.3.5.1 NPCR 2) UACI

The differential attack is an important way to crack the encryption algorithm. Intruders typically make little changes to the plain image (e.g., alter only one pixel or slight changes in a key) to observe the working technique of the encryption algorithm. Theoretical ideal values of NPCR and UACI scores are 1 and 0.33, respectively.

To calculate the NPCR and UACI values, Eq.(2.13) and Eq. (2.14) are used (described in chapter 2.), and Table 3.7 shows the NPCR and UACI results. It can be observed that the obtained values are found suitable that are ideal for the cryptosystem.

Table 3.7 NPCR and UACI scores of the Test Input Image

position	Image	Original value	Modified Value	NPCR	UACI
(174,50)	Leena	234	235	0.992	0.334
(174,47)	Baboon	172	171	0.996	0.339
(200,200)	Airplane	79	80	0.993	0.331
(1,1)	Peppers	61	62	0.994	0.332
(187,245)	Barbara	237	238	0.998	0.331

3.2.3.6 Keyspace analysis

The reliability of the cryptosystem is based on the keyspace. A keyspace is called as the total number of different keys entirely to be used in the algorithm. The keys X_1, Y_1 are used in this algorithm to carry forward the conformation originated from the Henon map according to the initial conditions. Which contributes to the confusion as well as the decryption process. The computational precision for 64-bit double-precision numbers is 10^{-15} ; it is based on the IEEE floating-point standard format [59]. Thus, for henon chaotic map, the user can configure 64×64 bit keyspace. In addition, Key *KEY1* is also used to initiate the encryption algorithm, and it needs an 8-bit space in memory. Therefore, the keyspace for the proposed algorithm reaches $64 \times 64 \times 8$. Interestingly for every pixel, a new key is selected; thus, it is also based on the size of an image; Thus, key length $\cong 64 \times 64 \times 8 \times m \times n$.

3.2.3.7 Perceptual security: Peak signal-to-noise ratio (PSNR)

PSNR usually applies to signal to check the distortion level and the quality after retrieval at the other end. In cryptography, PSNR measures the perceptual security of the proposed algorithm, and it is calculated between the original image and its cipher image. Researchers suggest that lower values of PSNR indicate that a proposed system efficiently encrypt the multimedia. Before calculating PSNR, the Mean square error (MSE) value is also calculated, and it must be on the higher side of the scale. PSNR (in dB) is calculated by the Equations, Eq. (2.15) and Eq. (2.16) are discussed in chapter 2.

Table 3.8 PSNR Analysis and Comparison

Test images	Proposed Scheme	Ref. [97]	Ref. [104]	Ref. [51]
Leena	27.60	28.50	65.12	28.46
Baboon	27.38	29.46	42.56	28.56
Airplane	25.9198	28.01	-	25.59
Peppers	27.7218	28.38	-	28.40
Barbara	28.1030	29.12	-	29.07

3.3 AN EFFICIENT IMAGE ENCRYPTION SCHEME BASED ON ELECTROMAGNETIC ROTOR MACHINE

With the recent growth of multimedia, the Web world is now being focused on multimedia-based information over the Internet; this security is an important key concern while transmitting or storing information [28]. There are two types of cryptography method which is used to secure information. One of them is symmetric-key cryptography[39], [112] and another one is asymmetric key cryptography. In asymmetric key cryptography schemes, both sender and receiver use different keys. In the traditional cryptography system, it was difficult to secure a large size of multimedia from intruders or attackers and calculation of mathematical equation (built-in Encryption technique) was not so easy; therefore, many researchers worked upon the security of bulky information. In this series, the Chaotic system, biometric features, confusion, and diffusion are materialized in cryptography, followed by traditional cryptography concepts. Rotor cipher was effectively used in the past; the enigma machine is an example of a Rotor Machine. The Enigma machines were developed as a chain of electro-mechanical rotor cipher machines used in the era of the mid-twentieth century to protect confidential information and diplomatic and military communication. Arthur Scherbius Enigma invented the enigma machine at the end of World War II [113], [114]. Enigma machine has a set of independent wheels through which the electric pulse can flow to other wheels. Each cylinder or wheel has a fixed amount of input pins and output pins. Each input pin is connected to a unique output pin of the cylinder. So there is a unique path between input pins and output pins.

If a machine has three cylinders or wheels, then it is categorized into a fast rotor, medium rotor and slow rotor. Whenever any input is given, the fast rotor is shifted circularly in a clockwise direction and according to prior connections of wires, internal connections between pins are also shifted towards the rotor movement. A rotor with n number of labels completes its one rotation after n number of inputs. When fast rotor completes one cycle then the middle rotor rotates in a clockwise direction by unit position. Slow rotor shifts one position to right after one complete cycle of middle rotor. This movement makes the system dynamic in nature.

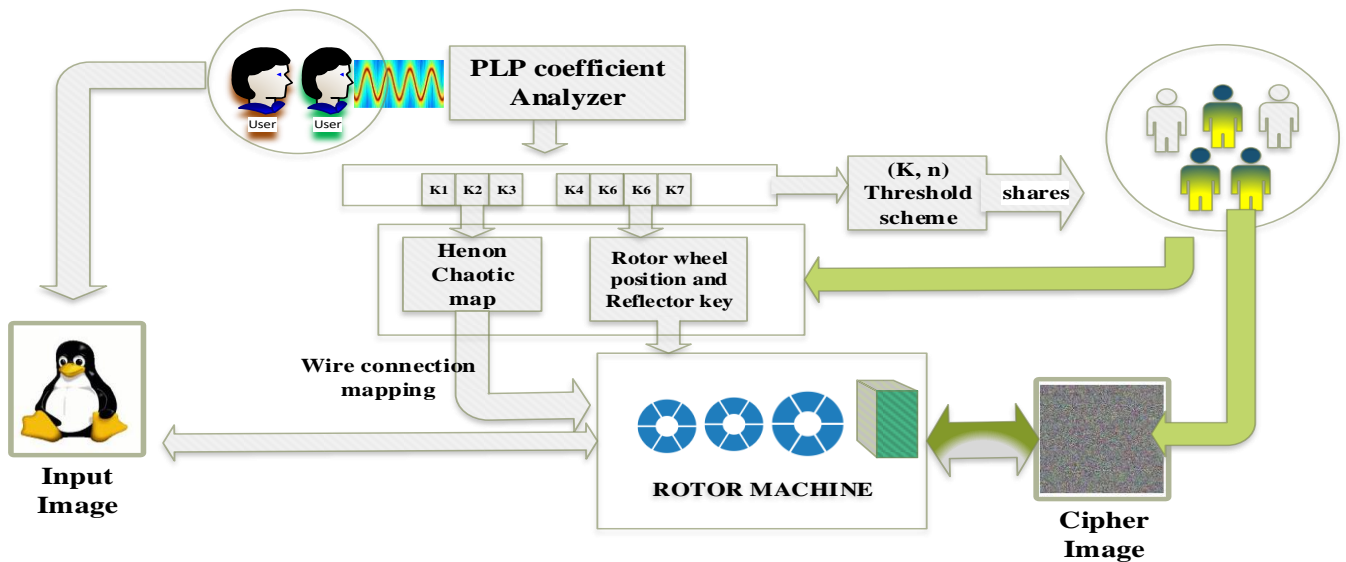


Figure 3.11 Proposed architecture of Model 2 based on rotor machine

Every person has their own way of speaking a language. This voice sample is preprocessed and further synthesized for various applications, such as authentication. When any person speaks, the sound is perceived by the human ear or machine. MFCCs (Mel Frequency Cepstral Coefficients) and PLP (perceptual linear predication) coefficients of Voice are unique biometric feature which can be used to provide security services according to security requirements [115], [116]. In PLP, the perceptual property of the human ear is captured. The power spectrum of the speech signal in the bark scale is equivalent to the human's perceptual model. MFCC coefficients are found out under the Mel scale filters, which are triangular filters, whereas PLP coefficients are found out under Bark scale filters, which are trapezoidal in shape. In cryptography, speech processing is being used with other biometrics at the vast level for reliable security systems.

Zhi-liang ZHU et al. proposed an encryption method based on the nonlinear mechanism of the enigma machine and chaos controlling the encryption process[117]. In [35], Elkamchouchi and Elshafee proposed a rotor enhanced block cipher method to obtain permutation and substitution operations in which rotor generates the round key to achieve cipher text key dependency. In[118], the author proposed a cryptographic system with unbalanced rotor to achieve goals of permutation and substitution. In [39], Chen et al. presented a symmetric image encryption scheme based on 3D chaotic cat maps. Wang et al.[40], introduced a 3D Cat map

3.3.1.1 PLP (Perceptual Linear Prediction) Feature through Voice Segment

Step 1: choose the speech acquisition tool to capture the voice segment and take 256 samples from this wave file.

Step 2: calculate FFT and calculate the power spectrum using squared magnitude of signal.

Step 3: covert frequency bin point to the corresponding bark and bark scale is divided into equal 14 filters.

Step 4: calculate the cube root of the power spectrum for each bark scale values.

Step 5: Bark scale is divided equally spaced triangular filters, width of filters equal to 5 bark scales with 50% overlap.

Step 6: Calculate IFFT of each triangular filter; these 14 values are known as PLP coefficients.

Step 7: out of 14 coefficients, 7 coefficients are chosen by the person to generate a keystream [122], [123] and following steps which are given below:

1. $keystream \leftarrow K[7]$
2. $|K[7]| \leftarrow K[7] \times 256$
3. $K[7] \leftarrow MOD(K[7], 256)$
4. $Keystream \leftarrow K[7]$

3.3.1.2 Digital Electromagnetic Rotor Machine

Electromagnetic machines used in World War II to send secret information, where each rotor's pins were labeled with 26 characters and mapping wires within the rotor, was static. So basically, it was based on the initial position of the rotor and the wired mapping of the reflector. Here we have designed a cryptosystem that is truly based on the electromagnetic machine concept. It is a digital model of electromagnetic machine to encrypt information with more number of combinations and dynamic wired mapping between pins, so it is hard to eavesdropper to deduce the original content from cipher. Here we have designed rotor with 256 input pins and each pin is connected with their corresponding output pins. Labels of output pins are generated using Hénon chaotic map and according to that, input pins are connected to output pins with their corresponding number. For example, a rotor has 4 pins. Initial rotor position starts from $K1 = 4$ and $K4$ be some number as initial seeds for Hénon chaotic map which

generates a sequence, say, [3 2 1 4].

Figure 3.13 illustrates the wiring connections between rotors and reflector; an example to understand the rotor machine. The initial input at the fourth pin gives output at the third pin. Output pins label of rotor one is generated using Hénon chaotic map, and according to that, input pins are connected to output pins with their corresponding number. The blue path shows the flow of current within the model with respect to the input.

3.3.1.3 Encryption Module

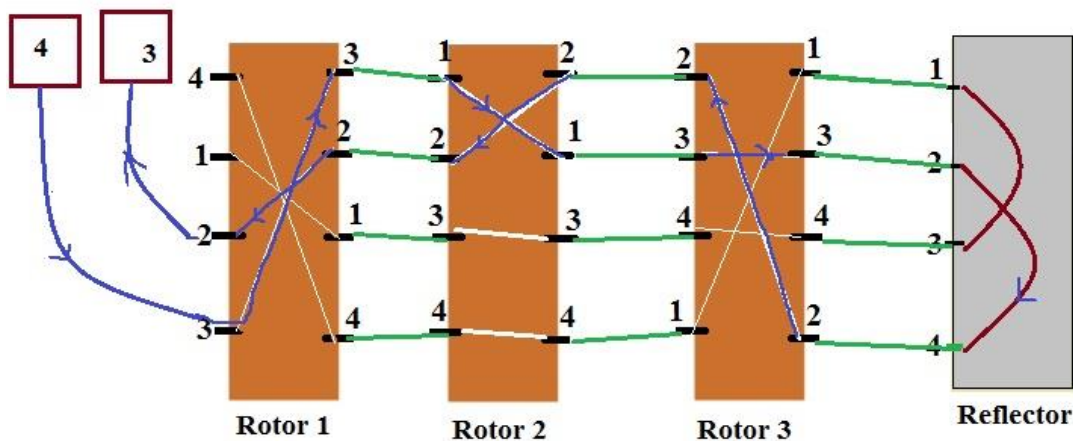


Figure 3.13 wire connections within Rotor

Step 1: K_1, K_2, K_3 are the initial seeds for Hénon chaotic map using (1), which generates the sequence for Rotor1 Rotor2 and Rotor3, respectively, as shown in fig. 2.

Step 2: keystream K_4, K_5, K_6 are used to initialize the positions of all rotors in the machine. K_7 is used to connect pins within the reflector. In every rotation, Rotor 1 moves into a clockwise direction by unit interval.

Step 3: Hénon chaotic map [75] discovered in 1978 is used as a pseudo-random number generator in security systems. Two dimensional discrete-time nonlinear dynamical Hénon chaotic map generates pseudorandom binary sequence using eq. (2.1) and eq. (2.2); In equations, the parameters a and b are of prime importance as the system's dynamic behavior depends on these values. The system cannot be chaotic unless the value of a and b is 1.4 and 0.3.

Step 4: This sequence is converted into [1256] range using modular arithmetic.

$X \in \{-I, +I\}$; Where I is integer

$New_X \leftarrow floor\{(256 \times X_{256})\}$

$New_X \leftarrow MOD(New_X, 256)$

Step 5: remove duplicate numbers from the sequence and replace those numbers with 0 frequency count in the sequence list as shown in Fig. 3.14.

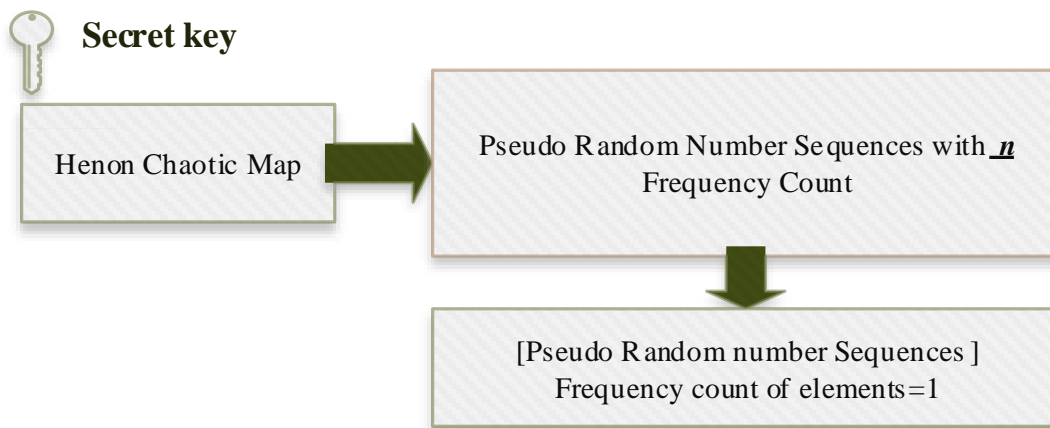


Figure 3.14 Pseudo-random numbers for wire connections within the Rotor

Step 7: Using the pseudo random sequence, labeling of output pins are done and wire are mapped with their corresponding label. This wiring of the model remains the same until the next setup.

Step 8: Grayscale image is used as an input, where each pixel intensity is responsible for fast rotor movement. Every pixel goes as input one by one into the system and gives output calculated by the below-mentioned pseudo-code for encryption of image.

Pseudo code for the encryption process (step 8)

```

1. For I ← 1:M
2. For J ← 1: N
3. Ptr ← I (I, j) +1
4.     For Rotor=1:3
5.     Number ← rotor (input pin, ptr)
6.     search (number1, rotor1) in output pin
7.     return index where number is found
8.     end
9.     Ref_indx ← mod(index[rotor3]+K7), 256)
10. For Rotor ← 3:1
11. search (number1, rotor) in input pin
12. return index where number is found
13. end
14. end
15. end

```

3.3.1.4 Key Generation for Group B members

The secret sharing scheme[124] basically splits the secret into shares and these shares are further distributed to the concerned group. Secret can be constructed only when group members participate to generate a secret key. Here Shamir's secret sharing (k, n) threshold scheme is used to split secret n members of the group. Therefore, parameters are taken as $n=5, K=3$ and $P=17$.

An equation is created with a degree $(K-1)$, and the coefficients (a_1, a_2) of the equation are chosen by group A members. The keystream is processed in a secret sharing scheme and n shares of keystream's size are distributed to the concern group where secret keystream is written in place of a_0 .

$$f(x) = a_0 + a_1x + a_2x^2 \tag{3.4}$$

3.3.1.5 Decryption Procedure

Group members can reconstruct a secret key using the LaGrange interpolation method, which is given below:

$$p(x) = \sum_{j=1}^n P_j(x)$$

$$\text{Where, } P_j(x) = Y_j \prod_{\substack{k=1 \\ k \neq j}}^n \frac{x - x_k}{x_j - x_k} \tag{3.5}$$

At the decryption end, users can generate a keystream using (3.5) to reconstruct the original image using the rotor machine.

3.3.2 EXPERIMENTAL RESULTS

In this section, the experimental results of the proposed image encryption algorithm are given to appreciate the efficiency of the proposed security system. MATLAB 7.9 software is used for the implementation of the proposed algorithm. Figure 3.15 shows the PLP coefficients of the voice sample (.wav format) used to generate the keystream. The encryption results of the proposed system are shown in Fig.3.16. and decryption results of the proposed system are depicted in Fig. 3.17.

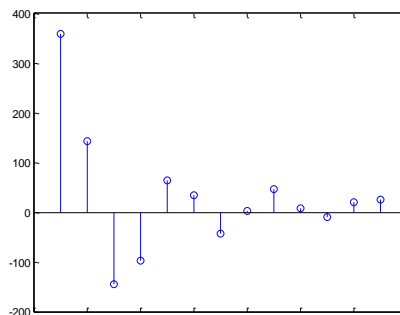
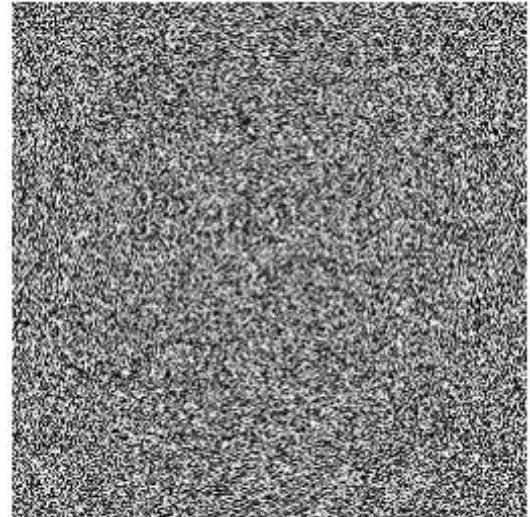


Figure 3.15 PLP coefficients of voice sample

3.3.2.1 Encryption Process



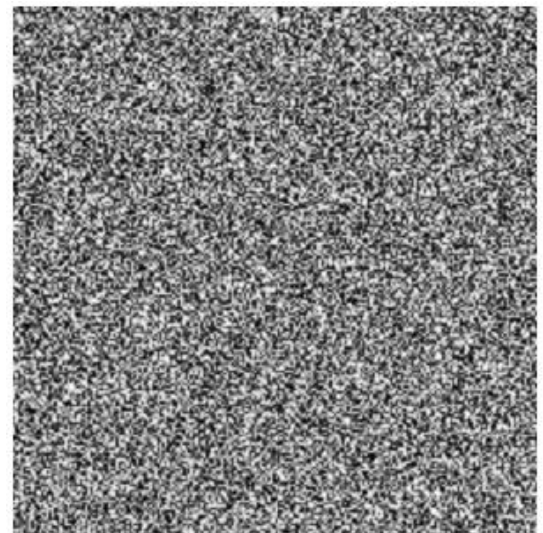
(a)



(b)



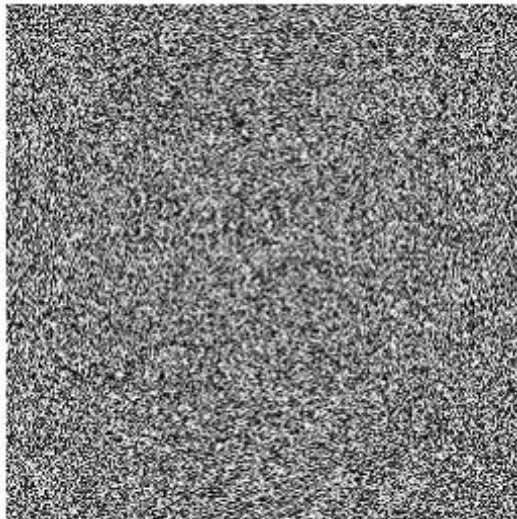
(c)



(d)

Figure 3.16 Lena Image: (a) original image (b) cipher image; Cameraman Image (c) Original image (b) Cipher image

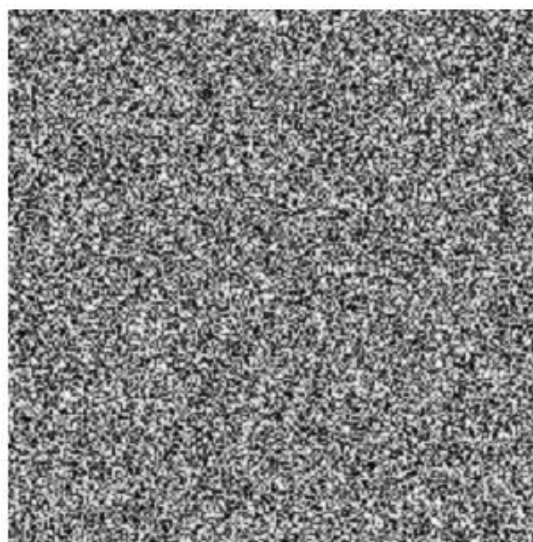
3.3.2.2 Decryption Process



(a)



(b)



(c)



(d)

Figure 3.17 Lena Image: (a) cipher image (b) Decrypted image; Cameraman Image (c) cipher image (b) Decrypted image

3.3.2.3 Entropy analysis of results

Entropy of encrypted image decides the ability of a cryptosystem, which makes it difficult for an eavesdropper to deduce information from cipher images. The ideal entropy of a cryptosystem is $\cong 8$ which means uniform distribution of pixel values.

Table 3.9 Entropy Analysis

Image name	Entropy of original image	Entropy of encrypted image
Cameraman.jpeg	7.086010767836325	7.996133299611271
Lena.jpg	7.466871535624320	7.997155374413349

3.3.2.4 Histogram

Figure 3.18 shows uniform distribution of grayscale pixel values in cipher image, and significantly different from the histogram of the original image, which proves that the encrypted image does not help intruders employ a statistical attack on encryption procedure.

3.3.2.5 Mean Value Analysis

Mean value analysis gives the average intensity of pixels in the horizontal direction across the image. The mean value of the cipher image in Fig. 3.19 is shown by green color, which is consistent throughout. This indicates the uniform distribution of gray levels, whereas the decrypted image and original image are shown by red and blue colors, respectively. Both the lines overlap each other, which means the original image is obtained by the group after decryption.

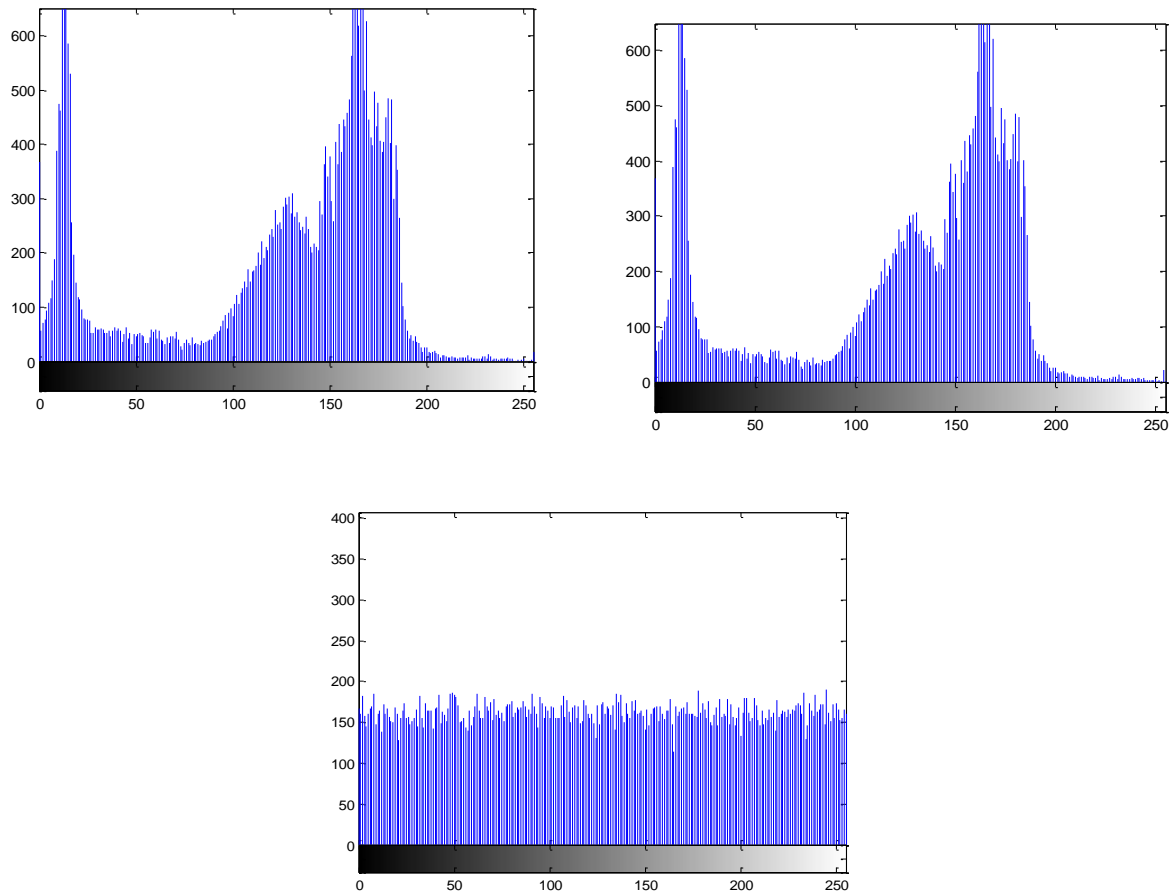


Figure 3.18 Histogram analysis of the proposed algorithm

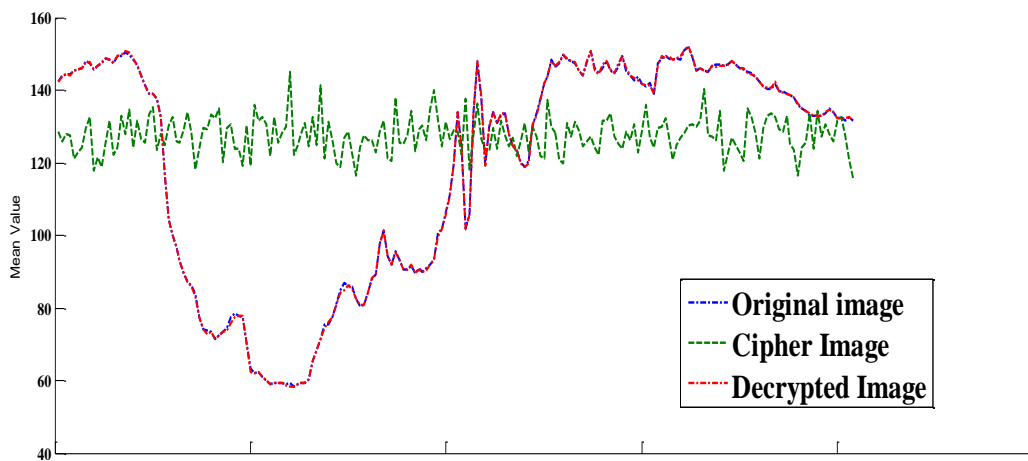


Figure 3.19 Mean value analysis (cameraman)

3.4 CONCLUSION AND DISCUSSION

The proposed algorithms have been applied to color and grayscale images, and it can be observed that the proposed algorithms are resistant to all types of statistical attacks. For the measurement purpose, various tests are applied to the test images to demonstrate the efficiency of the proposed cryptosystems. The proposed algorithms are lightweight in nature; thus, it can also save device power consumption of electronic devices. The proposed algorithms are based on the simple mapping procedure, i.e., it takes a minimum number of operations to obtain a cipher image. **Model-1** is based on a keyed transposition algorithm is designed for images to disturb the correlation among pixels with an excellent amount of keyspace. Elementary cellular automata are being used in all the scientific applications; in this work, dynamic properties are achieved and analyzed to obtain the rule tables. Since the computational power of many devices is usually limited, these rule tables can be used as relevant algorithms that are with low computational complexity in real-time computing systems. ECA is popular due to its implementation process, i.e., it takes minimum time to implement either on software or hardware platforms. In the proposed work, rule tables are used as a lookup table for each pixel of an image, and the lightweight operations are performed on a pixel to generate a cipher pixel. In this work, a simple rule is imposed by applying simple calculations. It is also evident that the proposed algorithm can resist all types of statistical attacks, which is possible on the public communication channel.

In the second **Model-2**, the properties of the electromagnetic machine are used with a novel approach to achieve confidentiality and authentication with high security. Speech is used for the authentication process and substitution cipher is achieved by the electromagnetic machine based on the keystream and Hénon chaotic map. A system with three rotors will have 256^3 different combinations and the same is followed in the mapping of wires within rotor. Since chaos systems are very sensitive to initial conditions, so a slight change in the initial key gives a different result and makes it impossible for an intruder to break the cipher image. The proposed cryptosystem is applied on several test images and results show a high level of security given by the system. For a few test images, the decrypted images were found to have insignificant noise. Here, the security of the system also relies on a speech signal along with the electromagnetic machine.

CHAPTER 4

Selective Image Encryption Schemes

4.1 PREMILIARIES

In the previous chapter, discussions were confined to algorithms based upon the mapping encryption schemes to gain efficiency and low computation cost of the cryptosystem. This chapter addresses the research question RQ-(3) that is discussed in section 1.8., Two algorithms are designed on the principle that is considering the selective amount of information for the encryption process. Security is a continuous process via which information is secured from several active and passive attacks. Several security mechanisms are used to ensure integrity, authentication, and confidentiality of the information [125], [126]. Cryptography is one of the primitive ways to secure information across unreliable communication networks. Cryptography schemes are of two types: (1) symmetric-key cryptography (2) asymmetric key cryptography. Since digital images communicate very frequently, thus users' privacy must be protected on untrusted communication channels. In the traditional cryptography system, it is difficult to secure a large size of multimedia from intruders or attackers, and the calculation of mathematical equations (built-in Encryption technique) increases overhead. Traditional algorithms are ideal for small amount of information, but images are having an excessive amount of information and bulky in size. When traditional algorithms are applied to images such as satellite images and medical images, it takes so much time to encrypt the image and increases the computational cost [36]. In the last few decades, Chaotic systems have been used in the cryptography system due to the characteristics such as sensitivity, ergodicity, non-linear, unpredictability, and random-look nature, deterministic and easy to reconstruct after filling in

multimedia data [62]. Several researches have been done on traditional cryptography schemes such as AES DES, RSA. Recently, chaos-based algorithms are designed on the basic principle of Shannon's theory of confusion and diffusion using pseudo-random numbers.

A lightweight encryption scheme is achieved by a selective image encryption technique, where only a significant part of the original image is encrypted. Detection of significant part in the spatial domain as well as in frequency domain is calculated by various image processing techniques and wavelet functions, respectively [127]. When a significant part of an image is encrypted instead of full image, it reduces the computational cost and time complexity. There are more shortcomings of a conventional full image encryption scheme apart from the computational cost. It is discussed below: (1) Pseudo-random numbers are generated as per the size of an image. Therefore, the number of iterations is increased to produce the key sequence as compared to the selective image encryption scheme. (2) Encryption and decryption speeds are increased due to the bulky size of data [67]. The selective image encryption scheme can be categorized as Fig. 4.1.

In addition, both schemes are based on the amount of input data. However, in the spatial

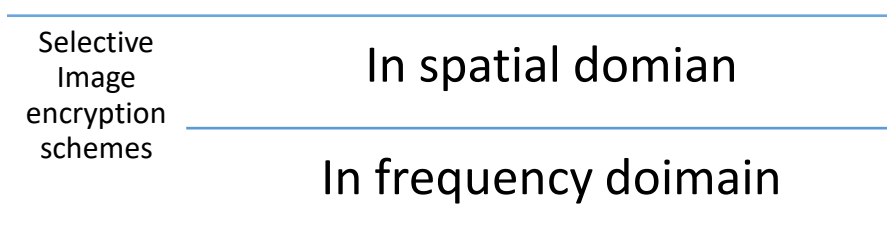


Figure 4.1 Selective image encryption schemes

domain, input data is based upon the pixels and it is achieved by selecting only significant pixels from an image to reduce the computation cost. It is also indicated by the cipher image, where ciphered pixels and original pixels can be distinguished. Thus spatial domain encryption schemes are based on the region of interest. Whereas in the frequency domain, significant coefficients of an image can reconstruct the original image with little distortion. So, when any algorithm encrypts such coefficients, it is enciphered the entire image.

Digital images are a significant source of information among all multimedia applications in terms of storage, as well as in transmission [128], [129]. When a sender or any host is connected to a subnet and sends multimedia to any other host, the secrecy of information over the

communicated channel is a significant concern. Information is passed from various layers of TCP/IP when it comes to the network layer. Routers play an essential role in directing packets to the intended user [130]. The sensor nodes have limited computation, communication and storage capabilities. As a result, it requires high security in the transmission medium because eavesdroppers can monitor the traffic with mal-intentions and can easily eavesdrop to gain useful information. In such cases, the information should be in a non-readable format and it should be difficult for the cryptanalyst to generate original information from the cipher image. In this chapter, two image encryption schemes are proposed as follows:

(a) **Model 1:** DWT based image encryption scheme in Frequency Domain

(b) **Model 2:** ROI based image encryption scheme in Spatial Domain

The chapter is organized as follows; Section 4.2 discusses related work. Section 4.3 introduces the DWT based image encryption scheme in the frequency domain. In section 4.4, ROI based image encryption scheme in the spatial domain is discussed. Section 4.3 and section 4.4 include all the required experimental results, and comparisons of all the existing algorithms with the proposed algorithm are presented in Section 4.5. Section 4.6 provides conclusions and a summary of the chapter.

4.2 RELATED WORK

Numerous researchers are continuously working on segmentation techniques as well as in cryptography. A variety of techniques and algorithms have been developed to build fast and secure image transmission systems. Mahmood and Dony [131] proposed a technique that applied segmentation-based encryption to medical images achieving faster processing time. Liu [132] proposed a method of selective image encryption. He has proposed an efficient selective encryption scheme to protect the privacy of an image and achieve access control of a JPEG 2000 code stream. A secret key, along with a mapping function, is used to generate a table to encrypt the selected DWT code in the entropy coding stage of the JPEG 2000 coding standard.

Ravishankar and Venkateshmurthy proposed an architecture where sensitive regions are not detected automatically since such regions are marked by the user [133]. The proposed selective region-based image encryption technique also has a further advantage. After completing the permutation and segmentation processes, the regions are encrypted individually. Spatially

localized and boundary finding approaches are found in the segmentation domain [134], where monochromatic images are tested using discontinuity measures. Susan et al. proposed an algorithm for segmenting out the region of interest by integrating the edge information to decrease the imperfections of the seeded region growing technique [135]. Younis et al. proposed a scheme where 6.25–25% of the plaintext data is encrypted to decrease the encryption and decryption time [136]. Taneja et al. proposed a method to secure a large size of data using Fresnelet transform, where only signed bits of coefficients are used for encryption [137]. In [138], a selective image encryption scheme was implemented based on the permutation and encryption module using 2D DWT. In [139], the Authors proposed three schemes using the same image encryption algorithm applied at different steps of JPEG compression; also, they have maintained the range of coefficients after encryption. Selective image encryption algorithms are designed on the basis of selective pixels or coefficients of the **images** [26], [140]. Xiang proposed a selective image encryption system, and an encryption algorithm selectively encrypts 50% of the whole image. They have used skew chaotic tent map to produce keystream to encrypt the significant component of an image [141]. Prajwalasimha proposed pseudo-hadamard transform (PHT)-based image encryption scheme based on confusion and diffusion using S-box [142]. In [143], An object detection algorithm is applied to detect objects within the image using Harr – cascade classification technique to increase the computation speed of encryption, and the detected object is encrypted with the help of the residue number system. In the year 2020, confusion and diffusion-based selective image encryption algorithm using dual hyperchaos map and DNA was proposed to secure medical images. DNA encoding and decoding rules are embedded in the selected pixel to implement the algorithm using chaotic sequences [144].

4.3 DWT BASED IMAGE ENCRYPTION SCHEME IN FREQUENCY DOMAIN

In this era of information technology, the exchange of information is taking place globally. In order to facilitate it, special attention is being given to network policies as well as security. The digital images contain a significant amount of information; therefore, an encryption module should be fast and processed in minimum time without facing any complexity in a shared network environment. This section includes a novel symmetric image encryption algorithm in

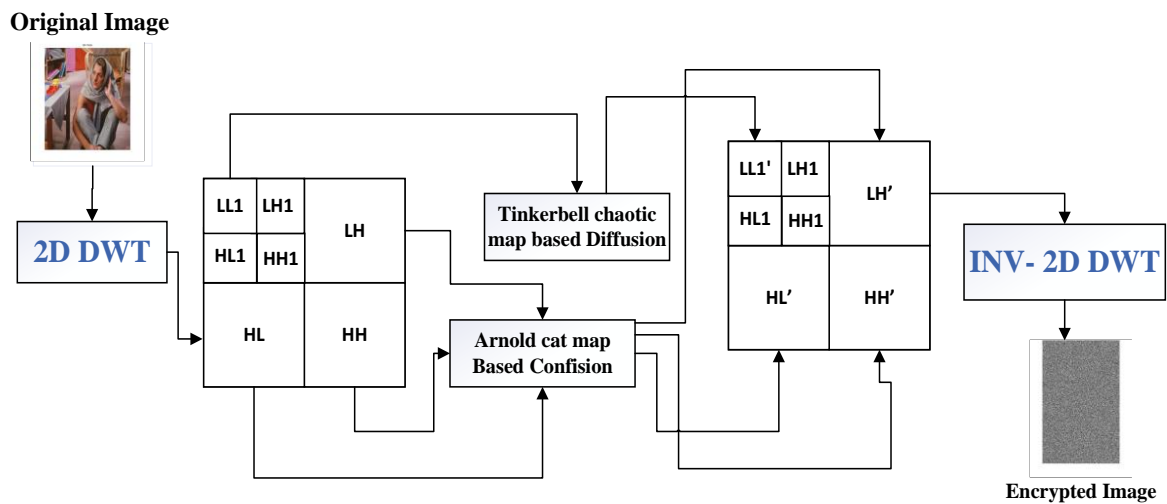


Figure 4.2 Schematic diagram of the proposed architecture

the wavelet transform domain based upon the properties of the Tinkerbell chaotic system along with Arnold's cat map to support confusion and diffusion. Two-Dimensional Discrete wavelet transform (2D-DWT) is used to decompose an image into its wavelet transform domain. The shuffling module is applied to the least significant coefficients using Arnold's cat map, whereas the encryption module deals with the most significant part of the image using Tinkerbell chaotic map based on the stream cipher. All the suitable parameters measure the algorithm's overall performance, and it is evident through results that it can be used for satellite and medical images to provide confidentiality. Fig. 4.2. Illustrate the schematic diagram of the proposed algorithm.

In the proposed algorithm, the given input grayscale image is disintegrated into four sub-bands (LL, LH, HL, HH) by applying 2D DWT. These sub-bands contain the approximations and details coefficients of the image. LH, HL, and HH belong to multiresolution representation (MRR); these sub-bands preserve higher frequency information such as texture and edges of an image. **LL** belongs to multiresolution approximation (MAR), which represents the lower frequency information. Lower frequency part or approximation coefficients of the image preserve characteristics of the image while higher frequency contains the details of the image. LL band is the approximation of the entire image, i.e., high significant information is allocated to the LL band. Therefore, a chaotic system deals only with the LL band [140], [145]. Many researchers have shown their interest in the spatial domain cryptosystem instead of frequency

domain due to loss of information. Efficient retrieval of images with minimal loss of information at the receiver end is one of the objectives of the proposed algorithm.

4.3.1 PRIMARILY BACKGROUND

Digital images are being used as a source of information in digital imaging applications, such as surveillance, telecardiology, satellite communication. Therefore, to protect such information from the attackers or intruders on the untrusted network is the necessity of an ideal communication system. Chaotic maps are widely used for symmetric key encryption scheme to protect bulky information. Here, we have used Tinkerbell chaotic map along with wavelet transform to accomplish the aim of the proposed algorithm.

4.3.1.1 Tinkerbell Chaotic Map

The explanation of Tinkerbell's chaotic map is briefly explained in chapter 2. In the proposed work, it is used to produce chaotic sequences that are deterministic and preserve pseudo randomness property.

$$x_{n+1} = x_n^2 - y_n^2 + ax^n + by^n \quad (4.1)$$

$$y_{n+1} = 2x^ny^n + cx^n + dy^n \quad (4.2)$$

Chaotic behavior of the system depends upon the variables a, b, c, d . n defines the discrete number of iterations that are used to produce the sequence. x_0 and y_0 together work as a key for the proposed cryptosystem, the initial seed of the iteration is used to generate a pseudo-random number sequence. The proposed model also utilized the Arnold cat map (chapter 2) to shuffle the image.

4.3.1.2 Discrete Wavelet Transform

The wavelet-based transforms are broadly used in image processing techniques for compression and watermarking schemes because the time-frequency representation of a signal is possible by wavelet transforms. JPEG-2000 coding standard is one of the perfect applications of DCT Transform. Wavelets are functions that derive from a single function called mother

wavelet. In 2D DWT, low pass and high pass filters are applied to input function or an image [146] in the horizontal direction and vertical directions and then it is downsampled by a factor of 2 to obtain approximation coefficients matrix and detail coefficients matrices; 1D DWT is applied to the image in both the directions to construct 2D DWT. The detail subbands include horizontal (HL), vertical (LH), and diagonal (HH) sub-bands of the image.

The resultant values of the low pass filter represent the most significant coefficients or a low-resolution version of the original image, which is called the approximation coefficient (LL). For the subsequent level of decomposition, the approximation coefficients matrix of the previous level is decomposed into its sub-band coefficients. One level-DWT [147] and inverse discrete wavelet transform are defined by the following equation (4.3) and (4.4):

$$D(a,b) = \sum_a \sum_b S(a) \Phi_{ab}(n) \quad (4.3)$$

$$S = \sum_a \sum_b D(a,b) \Phi_{ab}(n) \quad (4.4)$$

$D(a,b)$ describes the coefficient of DWT. Shift parameters and scale transform are denoted by a and b , respectively. $\phi_{ab}(n)$ represents the base time wavelet of the function. A bottom-up approach is used to reconstruct the original signal S by applying Inverse-DWT.

4.3.2 PROPOSED ALGORITHM

In this chapter, we have proposed and implemented an algorithm based on the selective image encryption scheme. The proposed algorithm consists of the DWT, Arnold cat map and the chaotic map. In order to obtain the Frequency component, 2D-DWT up to two levels is applied to input grayscale image $I_{(x,y)}$. $LL1$ sub-band becomes an input for the encryption module and bands (LH, HL, HH) are shuffled as using the Arnold cat map. Modified bands are combined and passed to IDWT to generate the encrypted image and the decryption module is performed in the reverse order of the encryption module to obtain the decrypted image.

4.3.2.1 DWT based Coefficients Generation

DWT is recursively applied to the image to obtain frequency coefficients, and for each call, the LL band behaves as input for the DWT. In this chapter, 2D DWT is applied up to two-level. Since 2D DWT works upon the square matrix, therefore, an input image $I_{(x,y)}$ has been taken in the size of $2^m \times 2^m$.

Step (1): Implement equation (2) upon the input image $I_{(x,y)}$ to produce sub-band coefficient matrices LL, LH, HL, HH at level one with the size of $2^{m/2} \times 2^{m/2}$.

Step (2): In the next level of decomposition, 2D DWT (2) is applied to LL , and the produced coefficient matrices of LL , are LL_1, LH_1, HL_1, HH_1 with the size $2^{m/4} \times 2^{m/4}$.

Step (3): Generated coefficients are used further for the confusion and diffusion process of the cryptosystem. LH, HL, HH coefficient matrices are used as input for section 3.2 to shuffled the location of coefficients.

Step (4): It is observed that coefficient values are float values by applying 2D DWT. LL_1 coefficients matrix values are decomposed into two parts: (a) Integer value segment $Int(LL_1)$ (b) Fractional value $Fra(LL_1)$, and encryption is performed upon the $Int(LL_1)$ of the float numbers and later encrypted integer matrix $Enc_{int}(LL_1)$ is combined with Fractional value matrix $Fra(LL_1)$.

4.3.2.2 Shuffling Module

Arnold's cat map is performed on LH, HL, HH bands separately using Eq. (4). Arnold's cat map achieves the shuffling of coefficient locations. In this chapter, twenty-five number of iterations are performed upon the coefficient matrix LH, HL, HH , and $N = 2^{m/2}$.

$$\text{Input: } \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$$

$$HL' = S(HL)_{25} ; HH' = S(HH)_{25} ; LH' = S(LH)_{25}.$$

Where $S()$ is, Arnold cat map function and subscript denotes the number of iterations.

4.3.2.3 Encryption Module

Step (1): Tinkerbell chaotic map works as a keystream generator to produce sequences X and

Y for the cryptosystem. It depends upon initial seeds X_0 and Y_0 , parameters a, b, c, d and n iterations. The size of a sequence depends upon iterations, which is defined by the size of LL_1 . Thus, $2^{m/4} \times 2^{m/4}$ sequences are necessary, which are produced by applying equation (1).

Step (2): Experimental analysis of coefficients bands concludes that the values of the coefficients in $Int(LL_1)$ need minimum of 16 bits to preserve the entire information. Two Dimensional Tinkerbell chaotic map generates sequences and stores them as a single array by applying element multiplication between X and Y matrix. These sequences are normalized and decimal values are then converted into 10 bits [0 1024] using equation (4.5).

$$S = \text{mod}(|(X \times Y)| \times 10^6, 1024) \tag{4.5}$$

Step (3): Now, reshape the sequence S as per the size of $Int(LL_1)$ and keystream of sequence S is XORed with the LSB bits of $Int(LL_1)$ in a bitwise fashion until all the coefficients of $Int(LL_1)$ are XORed with sequence S . Fig. 4.3. illustrate the encryption procedure of the

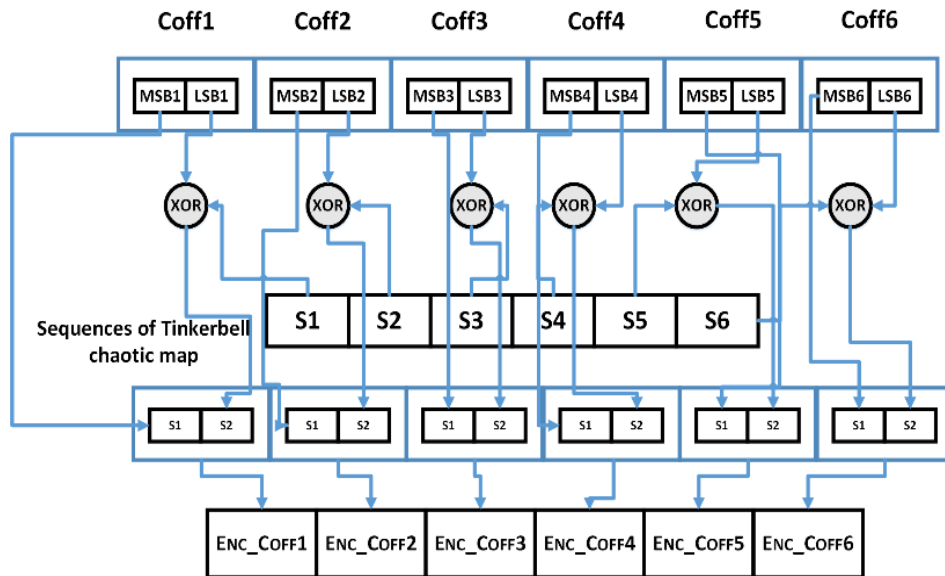


Figure 4.3 Encryption module of the proposed algorithm

proposed algorithm. matrix $Enc_{int}(LL_1)$ save all the encrypted coefficient values into it after XOR operation.

Step (4): Later, $Enc_{int}(LL_1)$ are combined with their own decimal values of $Fra(LL_1)$ of the LL_1 band as per the below equation :

$$LL'_1 = Enc_{int}(LL_1) + Fra(LL_1).$$

Step (6): Inverse-2D DWT is used to reconstruct the LL' . Which is passed further to reconstruct the encrypted image Enc_I as shown below:

$$Enc_I = IDWT(IDWT(LL'_1, LH_1, HL_1, HH_1) LH', HL'HH')$$

Step (7): To preserve all the information in Enc_I , encrypted image is saved in the tagged image file format (TIFF) due to the property, i.e., it can save values in 16-bit format and we have formatted decrypted values using half-precision standard format.

4.3.2.4 Decryption Module

This chapter presents a mechanism to protect confidential information within an image over the public networks. Thus, the reconstruction of a decrypted image from an encrypted image is equally important as the encryption process. Since chaotic maps are very sensitive to initial conditions, therefore using the same key pair of seeds generates the same key that is used to decrypt an encrypted image at the receiver's end. Since the chaotic system behavior is deterministic, so the reconstruction of an image using the same key pair at the decryption end gives the decrypted image.

Step (1): Encrypted image Enc_I is received at the receiver end, then applying the 2D-DWT with two levels gives the coefficients of the encrypted image as per section 4.3.2.3..

Step (2): Arnold map generates the original location of coefficients of HH , HL , and LH band after performing the same number of iterations.

Step (3): Now, the LL_1 band is extracted from the encrypted image, and the same procedure is applied in reverse order of the encryption module. Thus, a decrypted image is generated with a minimum loss of information.

4.3.3 EXPERIMENTAL RESULTS

The MATLAB R2015a software has been used to implement the proposed algorithm, the test input images, Barbara and Baboon of size 256×256 , as shown in Fig. 4.4.(a) and (c), respectively. The initial parameters for the Tinkerbell map are chosen as $a = 0.9, b = -0.6013, c = 2.0, d = 0.50$ to make the system chaotic. The secret symmetric key for

encryption is $X_0 = 0.1231$ and $Y_0 = 0.009231$

4.3.3.1 Cipher Image Illustration

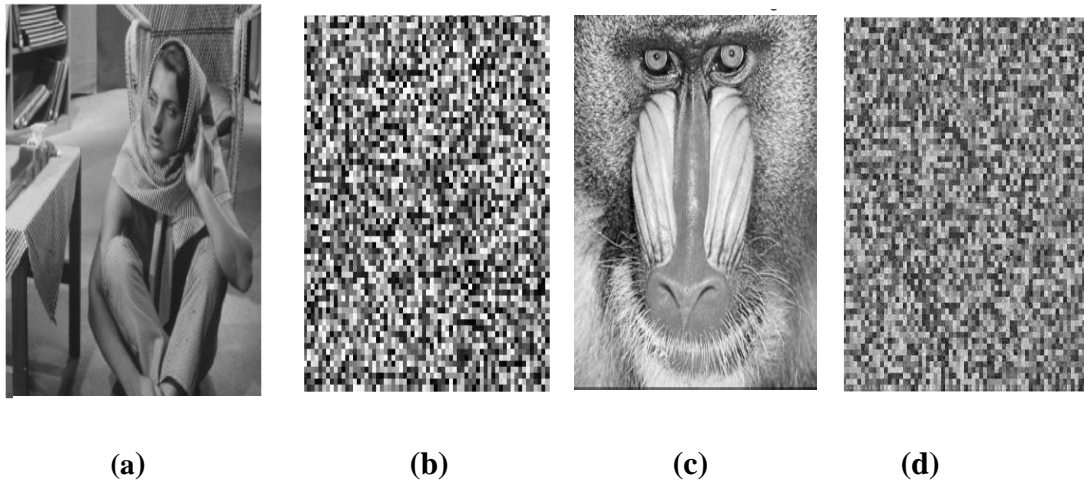


Figure 4.4 Cipher image results of the proposed algorithm (a) Original image of Barbara (b) Encrypted image of Barbara (c) Original image of baboon (d) Encrypted image of baboon

4.3.3.2 Histogram Analysis

Histogram analysis demonstrates the pictorial representation of the frequency count of all the available pixel intensity values within an image. Histogram analysis has been performed to the input images and visual representation of histogram shown in Fig.4.5 (a), (b), (c) and (d). the

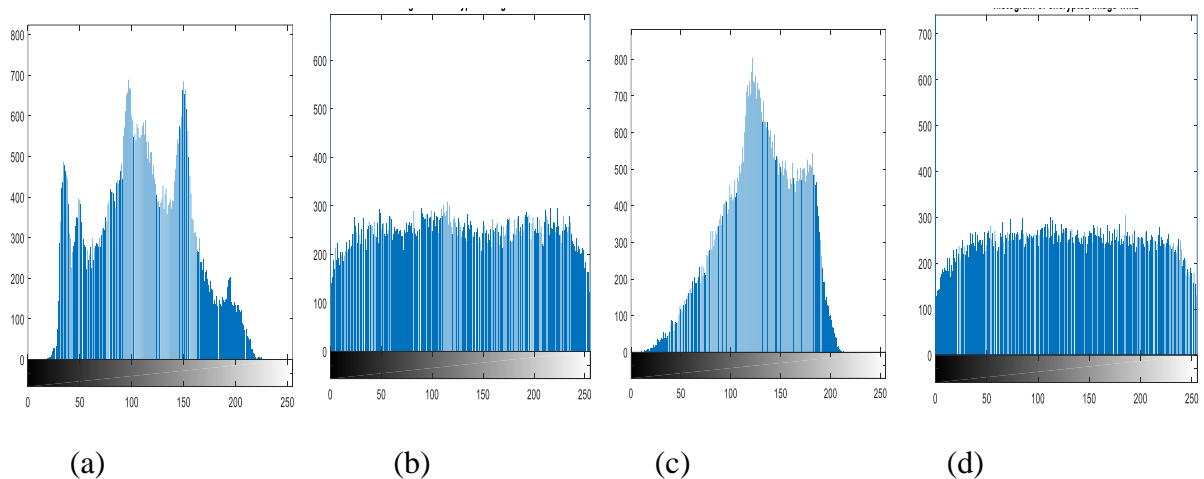


Figure 4.5 Histogram Analysis (a) Original image of Barbara (b) Encrypted image of Barbara (c) Original image of baboon (d) Encrypted image of Baboon

x-axis defines the intensity values and the y-axis defines the count of intensity values. Uniform distribution of pixel intensity in histogram representation in Fig.4. (b) and Fig. 4. (d) shows that all the pixels within an image have a similar count, and images are well encrypted.

4.3.3.3 NPCR and UACI Analysis

The number of changing pixel rate (NPCR) and unified average changed intensity (UACI) tests are performed on two encrypted images. Encrypted C image originates from the original image and the other encrypted image C' is found by changing one pixel in the original image to determine the strength against differential attack. Theoretical ideal scores of NPCR and UACI are $\cong 1$ and $\cong 0.33$. Table 4.1. shows obtained values for the input images and NPCR and UACI are calculated by the following equations.

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

$$\text{where } D(i,j) \begin{cases} 1 & \text{if } (C(i,j) \neq C'(i,j)) \\ 0 & \text{if } (C(i,j) = C'(i,j)) \end{cases}$$

$$UACI = \frac{1}{m \times n} \left(\sum_{i,j} \frac{|C(i,j) - C'(i,j)|}{255} \right) \times 100\%$$

Table 4.1 NPCR and UACI Scores of the Test Input Images

position	Image	Original value	Modified Value	NPCR	UACI
(174,50)	Barbara	70	71	0.96	0.334
(174,47)	Baboon	172	171	0.97	0.339

4.4 ROI BASED IMAGE ENCRYPTION SCHEME IN SPATIAL DOMAIN

In images, the secrecy of unnecessary information within an image is not required for all the legitimate users. Therefore, it is possible to encrypt only the foreground details. This technique is called Region-based encryption. Image segmentation is an emerging field of image processing, which is very helpful in determining non-overlapping homogenous regions of an image. Many researchers are participating in image processing and usually focus upon certain portions of an image called the foreground (the remainder is called the background) having a unique and specific nature. Object segmentation is particularly important in computer vision applications, such as medical image analysis, video surveillance, content-based image retrieval, and information security, among other applications. It is defined by segmentation and encryption simultaneously. Considering the limitations of over-segmentation and under-segmentation of the classical region-based object segmentation, object segmentation is done by an automatic edge constrained seeded region growing method. In this proposed algorithm,

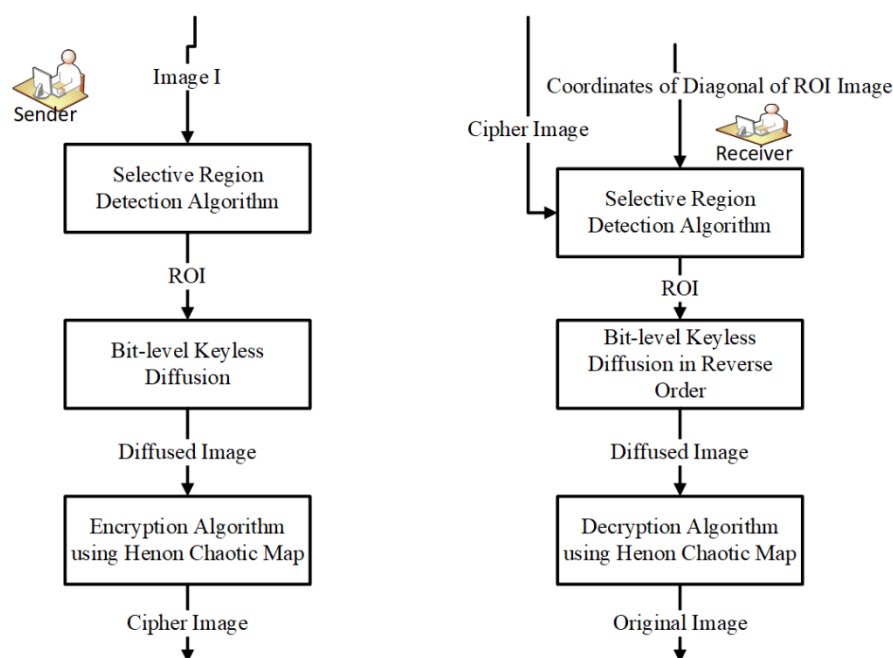


Figure 4.6 Architecture of the proposed algorithm

nearest edge pixels are used to solve the problem of over-segmentation and under-segmentation, where a center window containing some part of the object and threshold value with a seed selection is calculated on the basis of an input image [135]. The architecture of the proposed model is illustrated in Fig. 4.6.

Medical images are used to diagnose the health of a patient before treatment. Compressed and low-resolution images may be the origin of some incorrect diagnosis, so this is a constraint since diagnosis and treatment of the patient should be based on high quality and lossless compressed images, which hold important data than lossy or compressed images [148]. When a medical report or information of a patient is exchanged between medical personnel for further diagnosis, they do not want to reveal their patient's sensitive information. In this particular case, the medical technician will only send relevant information that is encapsulated with hidden information of the patient by region based selective image encryption. Region-based selective image encryption methodology is also required for the military and defense sectors of any country so that sensitive information within an image can be sent in encrypted or cipher mode. In this chapter, the presented algorithm is suitable for digital colour images. In the first phase, a sensitive region of an image is segmented and then the region of interest (ROI) of an image is introduced in a bit level keyless substitution method, where each pixel value is substituted. After that, a diffused image is passed to the next module of the proposed algorithm, where it is encrypted using Hénon chaotic system with a symmetric key cryptographic approach. In the complete process, sensitive details of image, i.e., the ROI is encrypted, while the remaining section of the image, region of background (ROB), remains in its original form.

Advantages of the proposed algorithm include that:

- A minimum number of bits are required for encryption. Hence, the computational cost of encryption is decreased.
- The proposed architecture ensures that various users from different spaces can only view a certain portion of an image.
- This algorithm can be used in two ways depending upon the user's requirements, whether sender wants to send an encrypted ROI image along with foreground details or choose to send only the ROI encrypted part of an image.

4.4.1 REGION-BASED SELECTIVE ENCRYPTION ALGORITHM

The proposed algorithm acts at two levels to achieve better processing times than previous methods. In the proposed method, first, a region of interest is found using the extended segmentation approach. Then, this sensitive information is encrypted with the help of a Hénon chaotic system. To understand the procedure, flow chart of the adaptive segmentation of an image is illustrated in Fig. 4.7.

4.4.1.1 Image Segmentation Module

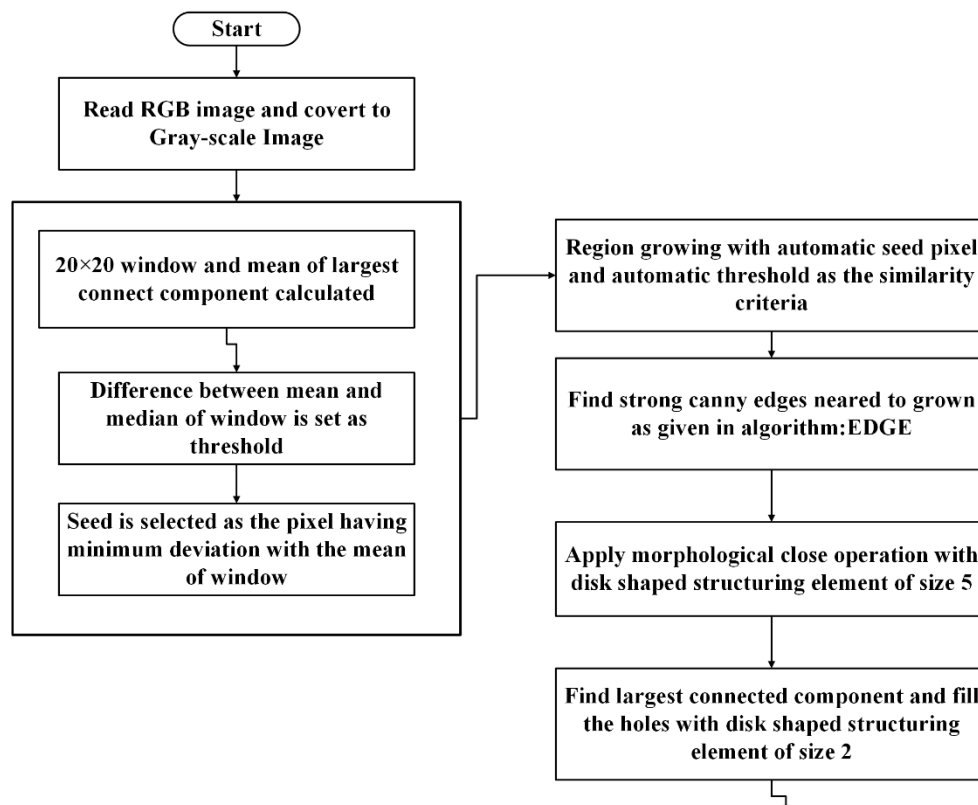


Figure 4.7 Flow chart: Adaptive ROI based segmentation

4.4.1.1.1 Calculate the automatic threshold and initial seed

- (a) A 20×20 window W is chosen across the center pixel to start the automatic phase of the method.
- (b) Threshold determination is done from the window W .

- (c) Find the largest connected component of this window and the mean of the grey pixels in the largest connected component. Absolute distance between the mean of window and median of all the window pixels gives the threshold to decide whether a neighbour pixel is included in a region or not.

$$\text{Threshold, } T = |Mean_w - Meadian_w| \quad (4.6)$$

- (d) Automatic initial seed selection from the window and calculate deviation of pixel values in the window from the mean,

$$Dev = |W_{(x,y)} - Mean_w| \quad (4.7)$$

Find the coordinates (x, y) in the window where deviation is minimum and embed this window back into the actual image to obtain the initial seed coordinates.

4.4.1.2 Seeded Region Growing Process

The initial seed is the deciding factor for the overall segmentation by region growing technique. It decides the region of interest or object within the image [149]. The initial seed obtained above is labeled as the grown region. All eight neighboring pixels are checked for similarity criteria to determine whether or not to include them in this region. The similarity criterion is whether the Euclidean distance of seed and the pixel in question is less than the threshold of the image (as obtained by the above process). The pixel is labelled as a region that then grows based on a similarity measure.

Euclidean distance is:

$$ED = \sqrt{(seed - n_p)^2} \quad (4.8)$$

where, ED= Euclidean Distance, n_p = neighbor of the seed, $p=1,2, 3, \dots, 8$

If $ED \leq \text{threshold}$, label the unlabeled pixel and push it onto the stack.

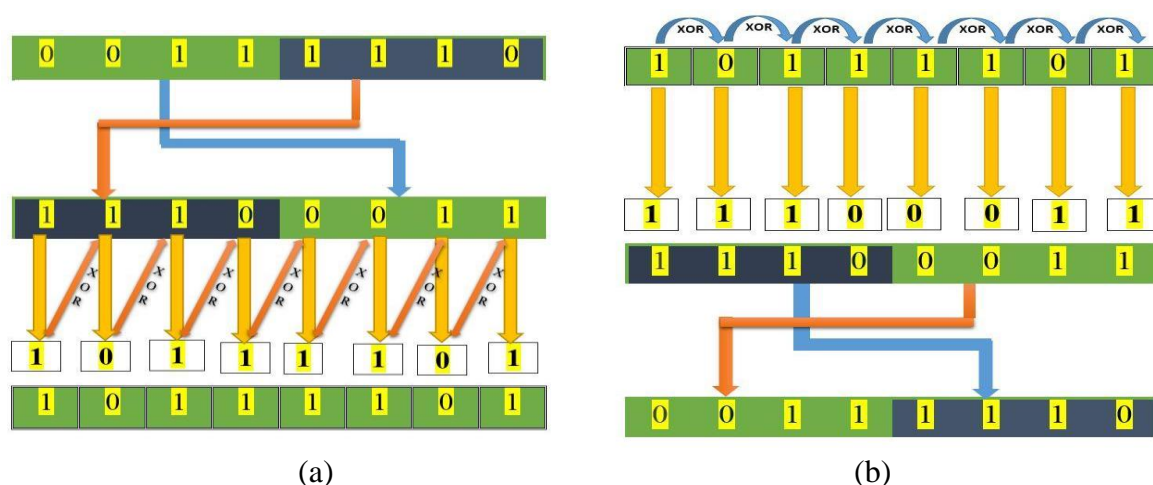


Figure 4.8 Keyless Bit level substitution algorithm (a) keyless substitution at the sender end, (b) keyless substitution at receiver's end

The grown region first calculates its distance with canny edge pixels of the image and then marks the minimum distance as the nearest strong edge pixel. Some discontinuities and holes may be present in the object. These defects are overcome by applying certain morphological operations onto the segmented image.

4.4.1.3 Perform Morphological Operations to Refine The Segmentation

Results

- For a morphologically close image, perform a dilation followed by erosion on a binary image using the same structuring element.
- Trace region boundaries in a binary image to identify the exterior boundaries of objects in the image to produce the largest connected component. This function returns the position of border pixels in the image.
- Structure elements of size five and size two are used for morphological closing and filling, respectively. This gives the single largest connected component in the image. The size of the morphological tools is determined through experimentation to determine the best results. The single largest connected component is the region of interest, which is further worked upon for efficient encryption.

Identify the target object and extract only the segmented area with two coordinates of diagonal.

Then, further processing is applied to the segmented region. The ROI based segmentation is applied to 100 images of the 'CAR' category of the PASCAL VOC 2005 dataset [150]. It is observed that more than 95% of the images achieve accurate precision.

4.4.1.4 Bit-level keyless Substitution Cipher

In gray images, each pixel is represented in an 8-bit format and they have different values to form a meaningful image. Here, a novel approach has been introduced that is based on the XORed property of gray code conversion. The first bit of a pixel will remain the same and the second bit will be generated using an XOR between the first and second bits. The complete process is repeated until all the bits of pixels are covered. Later, these eight bits are divided into two halves and the vales interchanged as shown in pseudocode 4.4.1.4.

```

Pseudocode 4.4.1.4. : Keyless Substitution
Pixel Pi = B1B2B3B4B5B6B7B8,
    for (i=1 to 8)
    {
    if (i=1)
    Ci = Bi
    else
    Ci = XOR (Bi , Bi-1)
    }
    
```

Let one Pixel, P_i, have a bit value in 8-bit format, B₁, B₂, B₃, B₄, B₅, B₆, B₇, and B₈. Keyless substitution of a pixel will be obtained by the algorithm given below.

When pixel value is converted into bit format using a given algorithm, it is found that it is converted into other decimal values, as shown in Fig. 4.8.

4.4.1.5 Encryption of Segmented Image

When any data is converted into a non-readable format and a procedure returns this original data, then this complete procedure is known as cryptography. Readable data, when converted into a non-readable form, is called encryption. In a stream cipher categorized under private key

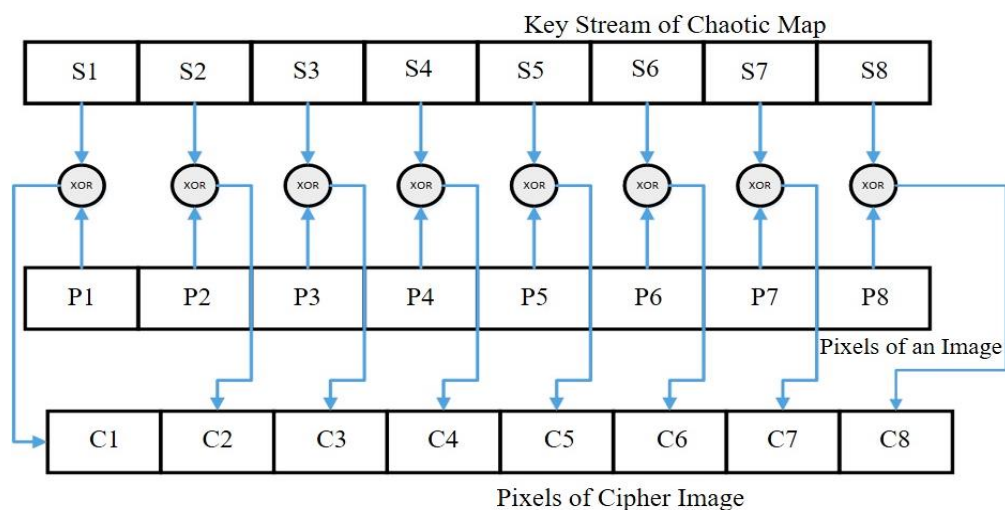


Figure 4.9 Diffusion based on Hénon chaotic map

cryptography, every bit of a message is encrypted with the corresponding key, which is generated with the help of a pseudo-random key generator. Pseudo-random numbers are used for the encryption in a stream cipher. Here, chaos theory has emerged due to its properties.

The Hénon map is a non-linear dynamic system which is generally used for generating the pseudo-random sequence in various disciplines of science [151]. A two-dimensional discrete-time non-linear dynamic Hénon chaotic map generates a pseudo-random binary sequence (described in chapter 2.2.3) using Eq (2.3) and (2.4) :

- **Step 1:** Choose the initial values (X_1, Y_1) for the Hénon map. These seeds act as an initial secret symmetric key for the Hénon map. For every initial seed, a Hénon map generates different pseudo-random numbers.
- **Step 2:** Hénon map works as a keystream generator for the cryptosystem. The size of the sequence depends on the size of a selective image. If the selective image size is $M \times N$, then the Hénon sequence will be a size $2 \times M \times N$, obtained by Eq.(2.1) and Eq.(2.2).
- **Step 3:** Experimental analysis concludes that the obtained sequence is not normalized and does not come under the image intensity values. A two-dimensional Hénon chaotic map generates sequences and stores them as a single array by applying element multiplication between X and Y matrices. These sequences are normalized, and decimal values are then converted into $[0, 255]$ values using equation (4.9).

$$G = |(X \times Y)| \times 10^6$$

$$G = \text{mod}(G, 255) \quad (4.9)$$

- **Step 4:** The Hénon sequence is then reduced by combining each sequence value into one byte-oriented value. This pair of bits of the keystream is XORed with a pixel in bitwise fashion and the next key value of the keystream is XORed with next pixel of an image. The procedure goes on until all the pixels of an image are XORed with the keystream of the Hénon Chaotic system [56]. Figure 4 illustrates the working procedure of the Hénon chaotic map.
- **Step 5:** Encryption is done by a bitwise Exclusive-OR (XOR) operation between pixels and the sequence generated in step 4. An obtained *ROI* encrypted image is combined with the foreground to make a complete image with selective encryption.

4.4.1.6 Decoding Algorithm at Receiver's end

At the receiver's end, the cipher image is further processed for decryption and the secret key is transmitted through a secure channel that applies the Hénon chaotic system to generate the deterministic sequence. These sequences are applied to the cipher image in the process to obtain the original image. An ROI selective encrypted segment is attached with foreground details of an image and sent to the receiver along with the diagonal coordinates of the ROI image. Since the chaotic system behavior is deterministic, reconstruction of the image using the same key (X_1, Y_1) at the decryption end gives a diffuse image. Later, this diffused image is passed using a bit-level keyless substitution to rearrange it in a manner exactly reverse of the way done for encryption, as discussed in Section 4.4.1.4. Finally, the original digital colour image is reconstructed at the receiver's end.

4.4.2 EXPERIMENTAL RESULTS

The proposed framework has been applied to several colour images. Excellent results demonstrate the effectiveness and efficiency of the proposed cryptosystem. MATLAB 7.9 software was used for implementing the proposed algorithm. Here, an input image of size 156×507 is shown in Figure 4.10 (a). The dynamic behavior of the system depends on the

values of a and b . These sets of values are of key significance to create the chaotic behavior of Hénon system. In experiments, the initial parameters for Hénon map are best chosen as $a=1.4$ and $b=0.3$ to make the system chaotic [151]. In the implementation of the process, a secret symmetric key for encryption is a combination of $X_1=0.01$ and $Y_1=0.02$ that is assigned here. Figure 5(b-c) illustrates the growing region of the input image and diffused image after keyless substitution, respectively. The image is shown in Figure 4.10 (c) is used as the input for the next module and an encrypted image is obtained by applying the methodology of Section 4.4.1.5. The image is transmitted to receiver's end and the main aim is to decrypt the received image using the secret key and known algorithm. Experimental results of the decryption process are shown in Fig. 4.11. This is the original decrypted image at the receiver's end.

4.4.2.1 Encryption at sender end

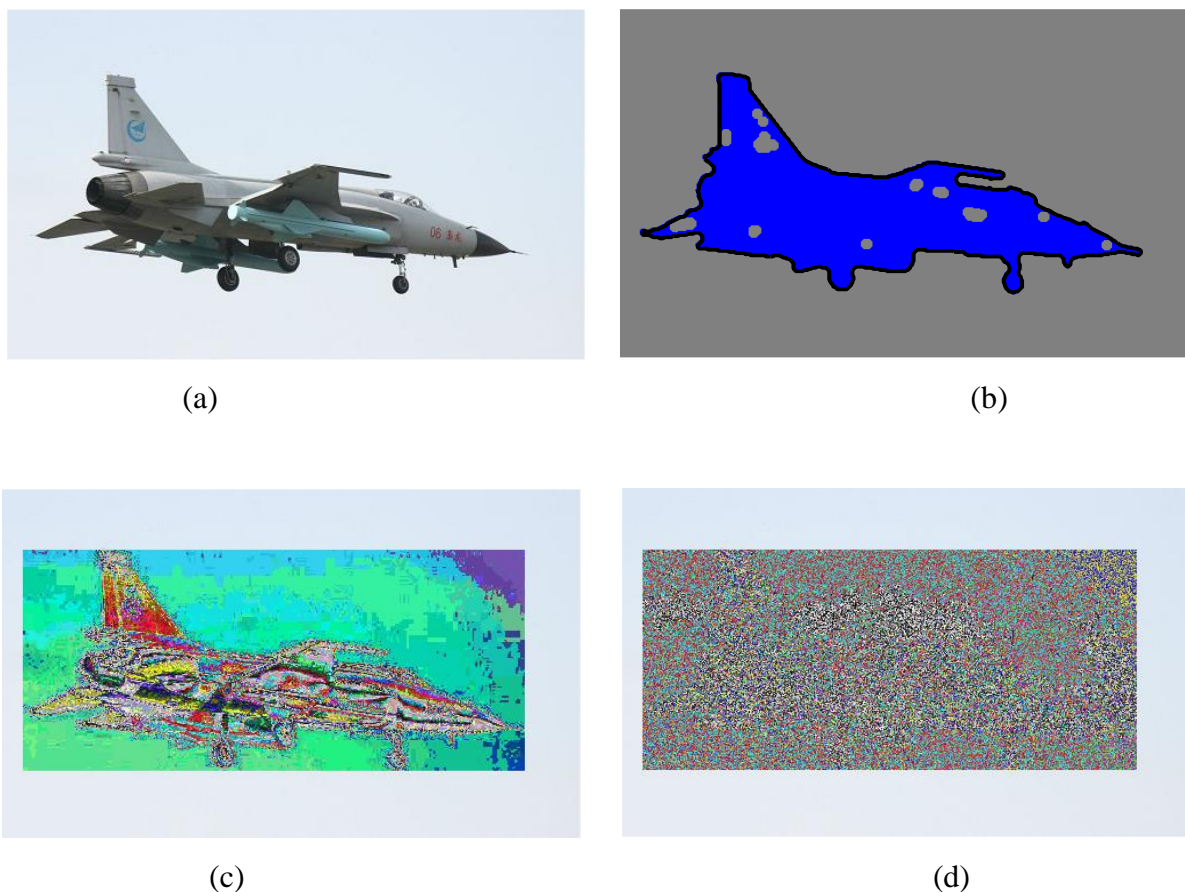


Figure 4.10 Encoding by system: (a) input image (b) segmented image (c) diffused image using keyless substitution (d) encrypted image

4.4.2.2 Decryption at receiver end

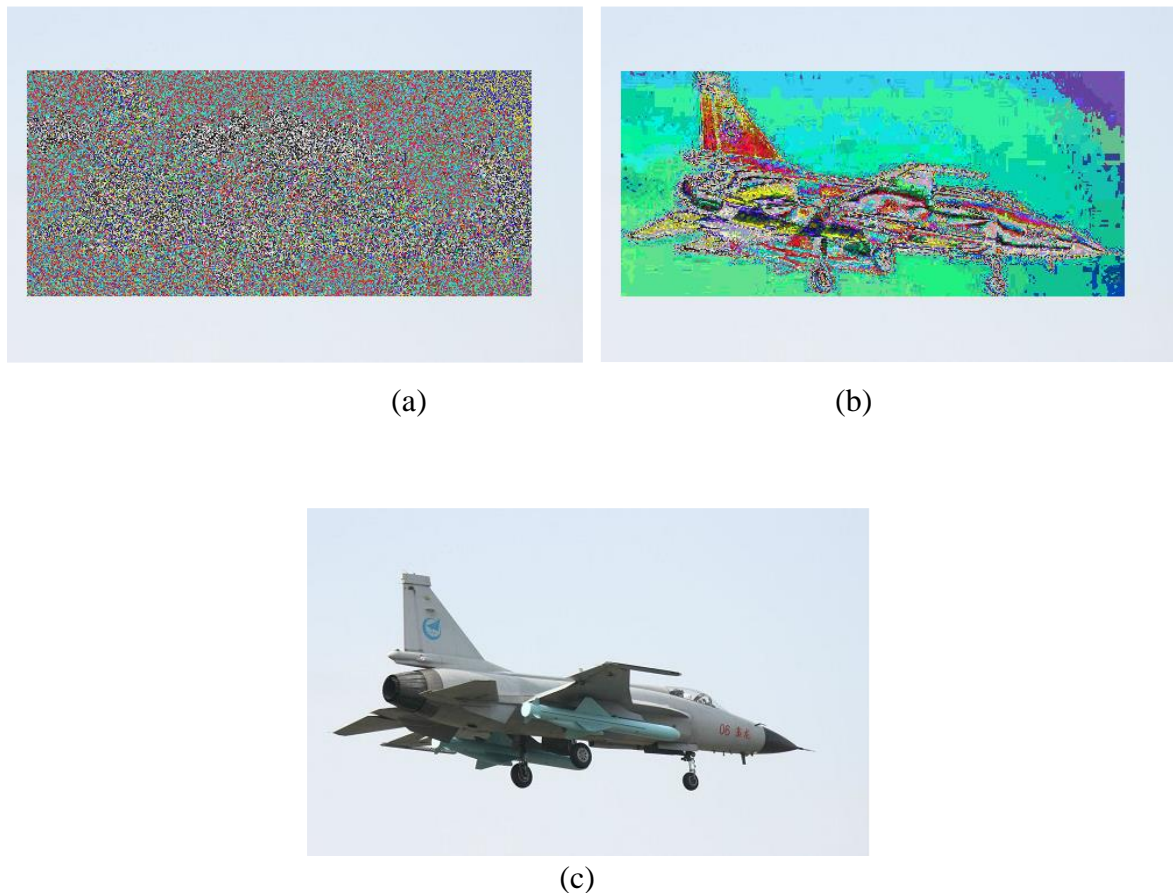


Figure 4.11 Decryption by system: (a) encrypted image (b) diffused image after decryption and (c) original image

4.4.2.3 Histogram Analysis

A histogram can be used as a graphical representation of pixel intensity values. There are 256 different possible intensities for a grey image or a single color channel. So the graphical representation of the histogram will display 256 intensities and the distribution of pixels amongst those intensity values. Based on the histogram, it can be concluded that cipher image is well encrypted and has more variation than original color image histogram. Visual representation of the histogram of original image, as well as diffused image, encrypted image, and decrypted image, are given in Figure 4.12.

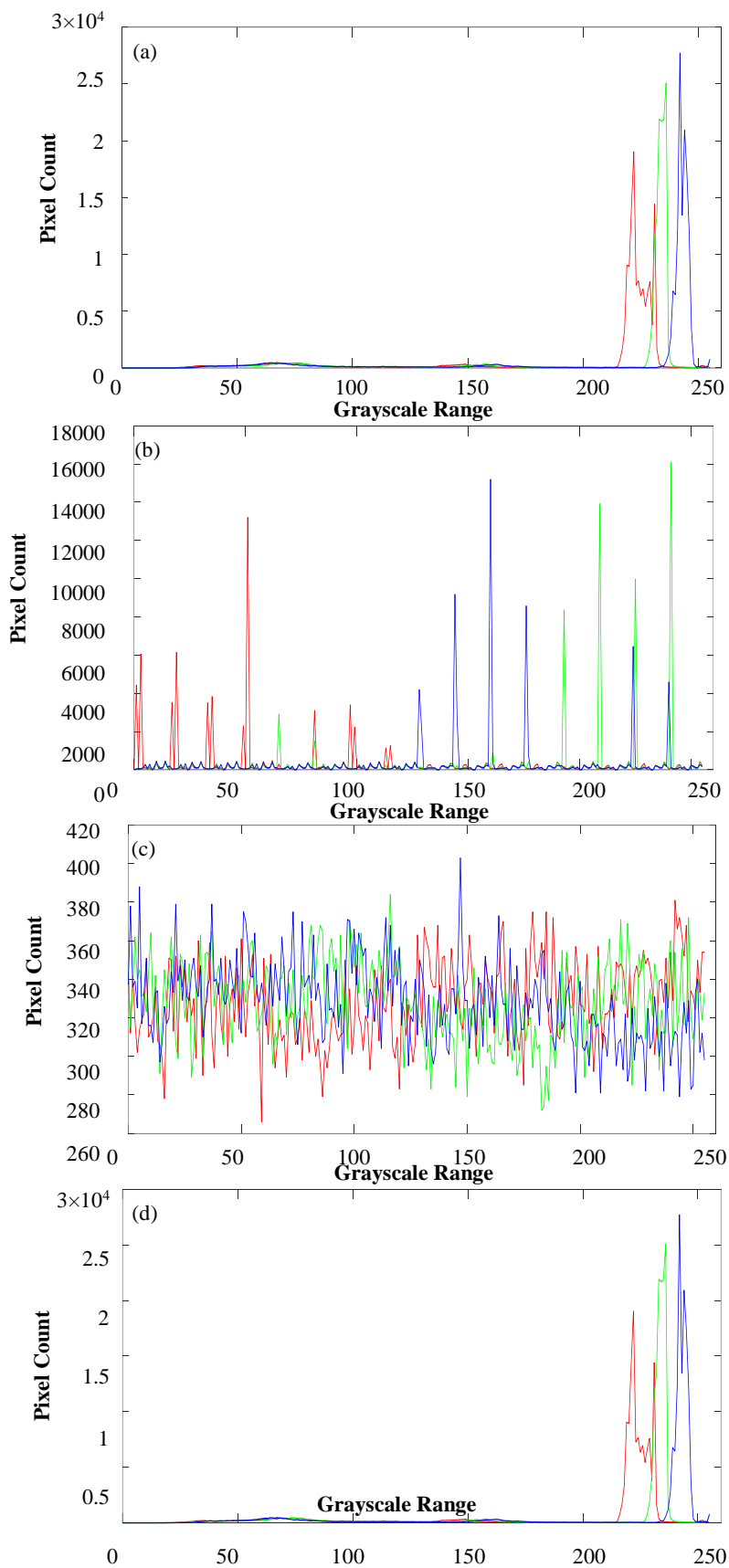


Figure 4.12 Histogram of ROI images (a) original image, (b) segmented image using bit level keyless substitution, (c) encrypted region using MSB based encryption using Hénon chaotic map and (d) decrypted image

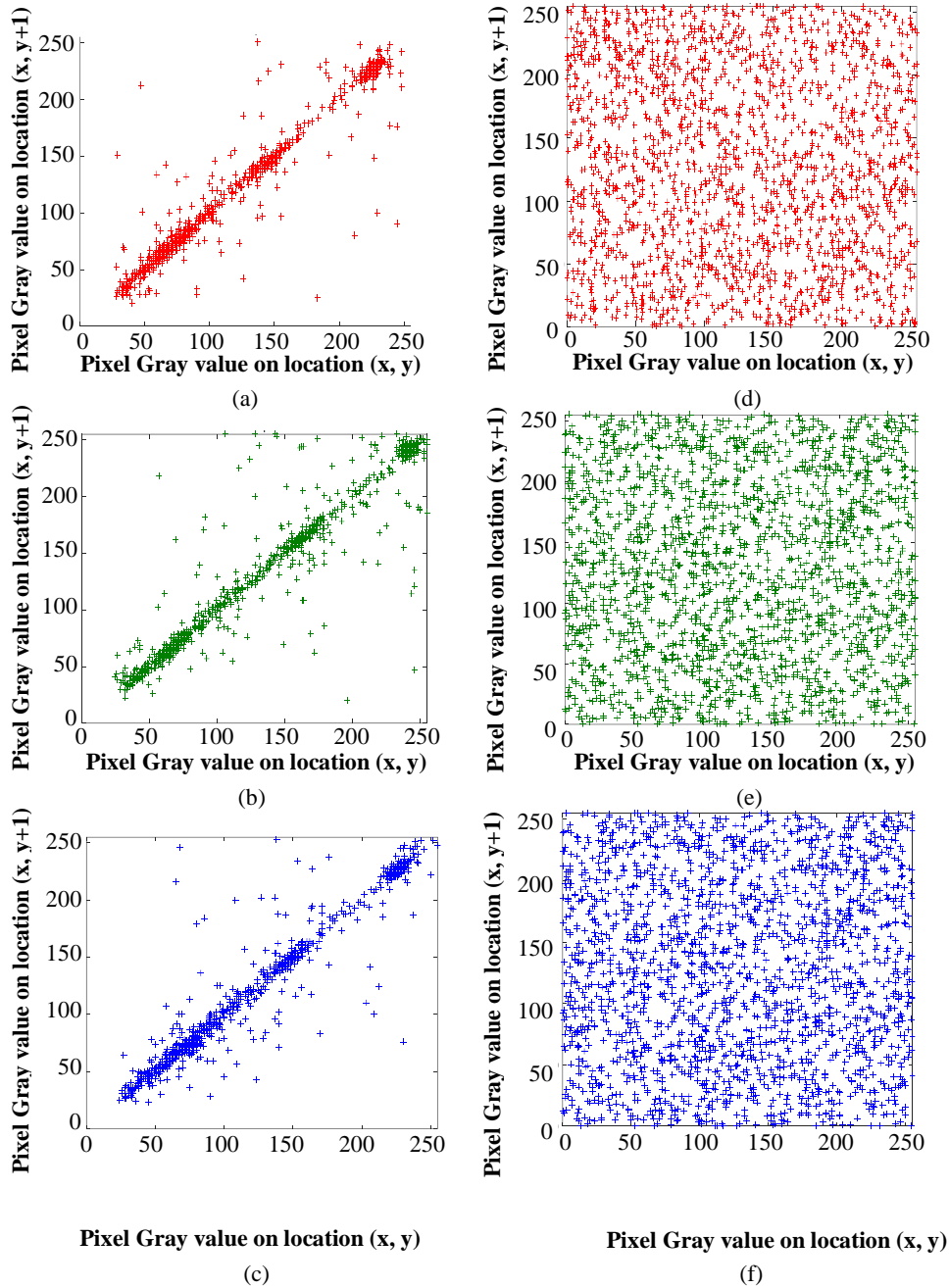


Figure 4.13 Correlation plot of two adjacent plain-image pixels in segmented image in horizontal direction for the (a) green channel, (b) red channel, and (c) blue channel. Correlation plot of two adjacent pixels of the cipher-image obtained by the proposed scheme from the (d) green channel (e) red channel (f) blue channel

4.4.2.4 Correlation Analysis

Correlation is used to find the relationship between two variables or two different datasets. In image processing, the correlation between every two adjacent pixel pairs of an image is usually very high, which indicates that pixels are strongly connected with their neighboring pixels within an image [152]. In this work, correlation analysis represents horizontal correlation in all the channels of original color image and it is also calculated in the cipher image, as well as shown in Fig. 4.13. Correlation between pixel values is calculated using the equations, Eq.(2.10) Eq.(2.11) Eq.(2.12) .

Table 4.2 shows a correlation of 2000 randomly selected pairs of adjacent pixels. It can be observed that correlation of cipher image is approximately equal to 0 while the correlation of plain image is nearly 1. This shows that the proposed algorithm is secure against all types of statistical attacks.

Table 4.2 Correlation Analysis of Encrypted ROI

Image	Orientation	Red Channel	Green Channel	Blue Channel
Plain Image	Horizontal	0.962	0.9683	0.985
	Vertical	0.9015	0.9466	0.9621
	Diagonal	0.87	0.91	0.9402
Cipher Image	Horizontal	0.0141	0.0304	-0.00278
	Vertical	-0.0094	0.0034	-0.0083
	Diagonal	0.0159	-0.00170	0.0014

4.4.2.5 Key Sensitivity test

For secure encryption, the key should be sensitive to a large keyspace and resist all kinds of brute force attacks. To test the sensitivity of the key involved, a tiny variation is done in the original secret key by changing it from $x(1)=0.01$ and $y(1)=0.02$ to $x'(1)=0.010001$ and $y'(1)=0.020001$. As a result, it was not possible to obtain the original image at the receiver's end without knowing the secret key, as shown in Figure 9. A failed decryption image is shown in

Figure 4.14 (a) with its corresponding intensity range in Figure 4.14 (b). Comparing these results with the correct decrypted image and its intensity range, it is clear that the decrypted image with the wrong key is completely different, and its intensity range is still balanced.

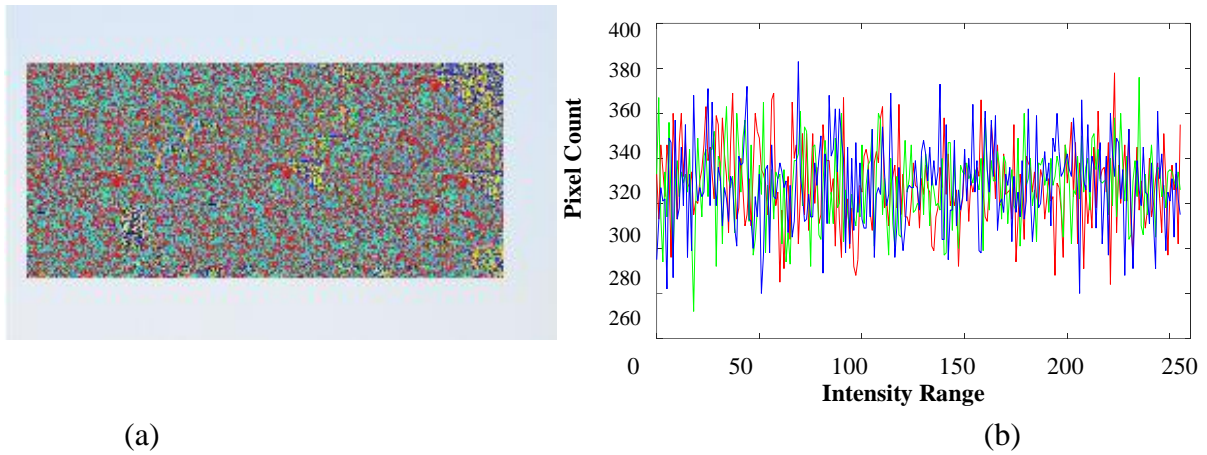


Figure 4.14 Key sensitivity test (a) Image after applying the wrong symmetric key, and (b) intensity range of the corresponding ROI encrypted image

4.4.2.6 Mean Value Analysis

The mean value of input plain image varies along the width of the image. On the other side, a cipher image in mean value visual representation remains consistent along with the width of the image as shown in Figure 4.15. It can also be seen that the mean distribution of the cipher image is very close to each other and is uniform in the distribution graph of mean values. The mean is calculated using equation (2.17),



Figure 4.15 Mean Value Analysis

4.5 COMPARATIVE ANALYSIS WITH THE EXISTING TECHNIQUES

Several selective image encryption techniques are usually classified into two domains, i.e., spatial and transformed domain enlisted in Table 4.3.

Table 4.3 Comparative Analysis of Existing Selective Image Encryption Schemes

	Parameter for the encryption process	Domain	Purpose	Scheme	Module for ROI	Image Type	Test performed	Remark
[153]	JPEG2000 Code stream	Wavelet domain	To secure medical images.	AES with CFB mode	Precincts Selection	Grayscale images	PSNR	Less than 10% of the data is encrypted.
[133]	Pixels of ROI	Spatial Domain	Speeds up the encryption process and enhances confidentiality	Permutation and value transformation	Manual selection as per the user, i.e., fixed-size block	Grayscale images	Encryption time	Regions are encrypted independently
[154]	Blocks of ROI	Spatial Domain	To secure biometric images i.e., iris images	Logistic Map and Arnold map	Edge-based detection	Grayscale images	Computational time analysis	Encryption time is less than 1 second
[152]	DWT coefficients	Transform Domain	Confidentiality	AES S BOX, Cat map, and Logistic map	cAP band	Grayscale images	Time, Entropy, key space, Histogram, speed analysis, correlation, NPCR and UACI	Two-layer security and the complete image is ciphered

	Parameter for the encryption process	Domain	Purpose	Scheme	Module for ROI	Image Type	Test performed	Remark
[155]	Blocks of an image	Spatial domain	Confidentiality	Arnold Map, PRN and AES	Entropy-based sensitive block selection	Grayscale and color images	Entropy, Histogram, ID, Correlation, NPCR,UACI analysis, Encryption time	Two layer security and the complete image is ciphered
[148]	Coefficients, JPEG2000 Code stream	Transform domain	Confidentiality for medical images	Invert MSB, AES	Decomposition of image using wavelet	Grayscale Images	PSNR	Two schemes are designed
[156]	Pixel of ROI	Spatial domain	Confidentiality	Blowfish symmetric cipher	Edge detected using the Prewitt detector	Color Images	Encryption time and ROI ratio	Based on Edge based and face detection
[86]	All pixels of an image	Spatial domain	Confidentiality	Lorenz and sine map	Sobel edge detection operator	Grayscale Images	Differential attack, Histogram, key sensitive analysis, PSNR	Entire image is encrypted based on importance
[157]	Pixels of ROI	Spatial domain	Compression, integrity and encryption	Chaos-based encryption and Huffman coding	arbitrarily	Grayscale Image	PSNR, Entropy, Correlation analysis	MAC is used to provide integrity

	Parameter for the encryption process	Domain	Purpose	Scheme	Module for ROI	Image Type	Test performed	Remark
ROI based scheme (Proposed)	Pixels of ROI	Spatial domain	To secure object-oriented images	Hénon chaotic map with Key-value transformation	Automatically by the proposed algorithm	Color images	Entropy, correlation analysis, mean value analysis, histogram analysis, a key sensitivity test	Size is not fixed of the region. It is adaptive as per the region
DWT scheme (proposed)	Coefficients	Frequency domain	To secure any bulky sized image	DWT with the chaotic map system	High significant coefficients		NPCR, UACI, Histogram, visual representation	Retrieval of the image at receiver image without alternation

In the spatial domain, an image is treated as a collection of pixels and ROI is identified by image processing techniques. In the transform domain, highly significant coefficients are incorporated in the encryption technique. Thus, ROI techniques [86], [133], [148], [152]–[157] are different in several aspects, which is presented in Table 2. A brief comparison of the proposed algorithm with existing techniques is done and it achieves a balanced amount of security and robustness. The proposed work is applied to medical and standard images. Information entropy is always obtained near eight, which shows that ROI based algorithm is adaptive and efficient to object based images.

4.6 CONCLUSION

Model 1: In DWT based encryption scheme, chaotic system is used, and it is very sensitive to the initial condition means a slight change in the initial key gives a different result, and that is why intruders cannot break the cipher image. Image Reconstruction of an image at the receiver's end with a negligible difference has been achieved through the proposed algorithm with the help of TIFF image format. Only 6.3% of coefficients are encrypted to enhance the

speed of the encryption also initial parameters increase the key size. The proposed algorithm is useful, and it has real-time applications to encrypt a large size of data in order to fulfill all the aspects of security. Various tests are also performed to evaluate the efficiency of the proposed algorithm, and the results of tests show that the proposed algorithm has an ample amount of substantial-quality to protect the information in a reliable manner and can resist all types of brute force attacks. Future work can also be done on different color models as well as different wavelet transforms.

In **Model 2**, ROI based encryption scheme is discussed. The proposed algorithm is applied to several images in MATLAB and tests were performed to find its correctness. It is estimated that the proposed algorithms give appropriate results to get higher levels of security for images and is more space-efficient and secure than previous algorithms and techniques. Statistical analysis was done on the test images, which yielded better results in all dimensions. A key sensitivity test demonstrates a small change in the symmetric key; it gives a different decrypted image which is not even near to original image. It makes system more reliable and robust against harmful activities. Sometimes, the foreground of image is an important source of information and it has to be kept secret for both communications ends. The proposed architecture ensures that various users from different spaces can only view a certain portion of an image. Experimental results show that the proposed algorithm has all the merits of an ideal cryptosystem. It is more secure and is a fast encryption module for large-sized images.

CHAPTER 5

Steganography Techniques to Secure Information and Integrity Preservation of Systems in IoT Network

5.1 INTRODUCTION

In chapters 3 and 4, we emphasized the algorithms based on symmetric key cryptographic schemes. In this chapter, the proposed models are based on steganography and wavelet transforms to protect sensitive information in IoT networks using sensor readings. Information was processed and stored in computer systems during the late 20th century. However, in the early 21st century, the digital revolution took place and technology evolved with several computational devices. Also, telecommunications have been integrated into digital devices to provide ethernet services in all the important sectors. Today, more than ever before, the Internet is reached to every individual and all the areas wherever it is required to digitize the structure. In recent years, sensor nodes have attracted much attention due to their digital properties. The sensors capture environmental data every second, and such data or readings are transmitted through cognitive networks at a specific frequency. Sensor nodes play a vital role in transmitting the collected readings and other sensitive information through public networks. Therefore confidentiality of information and integrity protection of periodically collected readings are required for better assessment. This chapter presents two novel steganography techniques based on the wavelet transforms and chaotic maps to achieve integrity and authentication of sensitive information in smart grid systems and the Internet of battlefield things. This chapter includes novel approaches to secure sensitive information of different

sectors based on IoT. The algorithms have been designed to be implemented practically in the real-time world for the enhancement of existing security mechanisms. To understand the importance of sensor and IoT devices, smart grid systems and Internet of battlefield things have been studied and accordingly, by using different concepts, two algorithms are proposed as follows:

(a) **Model 1** - Chaos-based steganography technique to secure information and integrity preservation of smart grid readings

(b) **Model 2**- Internet of Battlefield thing Security: A Strategy to Secure Sensitive Information using Reversible Steganography Scheme.

Sensors transmit the collected information and this information is meant to the intended person only. It is not required to convert readings into a nonreadable format in many cases, but it needs to be in original format at both ends; it is achieved by steganography. Steganography is a part of cryptography, which ensures that transmitted data is secure and confidential [158]. Steganography has three parts- secret information, cover object, and a key. Secret information is embedded in the cover object in such a way that an unauthorized person cannot retrieve information from the stego object [19]. Integrity is also an essential aspect of security for end-to-end users, whether received data is original or altered by noise or intruder during transmission. Usually, for integrity protection, Message Detection Code (MDC) is attached with original data and the receiver verifies it by obtaining the same MDC from the received data.

The algorithms are based on reversible steganography because readings are constructed with negligible distortion in original readings after concealing bits into a cover object applying a double-precision floating-point format. For simulation, the sensor's data is stored in the form of readings. Periodically collected readings are used as a cover object to hide the sensitive information of IoT devices. The percentage residual difference test (PRD) test has been performed between stego and original readings as well as the reconstructed readings. The value of the PRD test is observed in both algorithms found to be very less than other existing algorithms. Experimental results illustrate that the proposed algorithms are reliable, robust and highly sensitive to its initial key and retrieval of information at the receiver's end is not labyrinthine. In section 5.2, the steganography technique is applied to the smart meter readings.

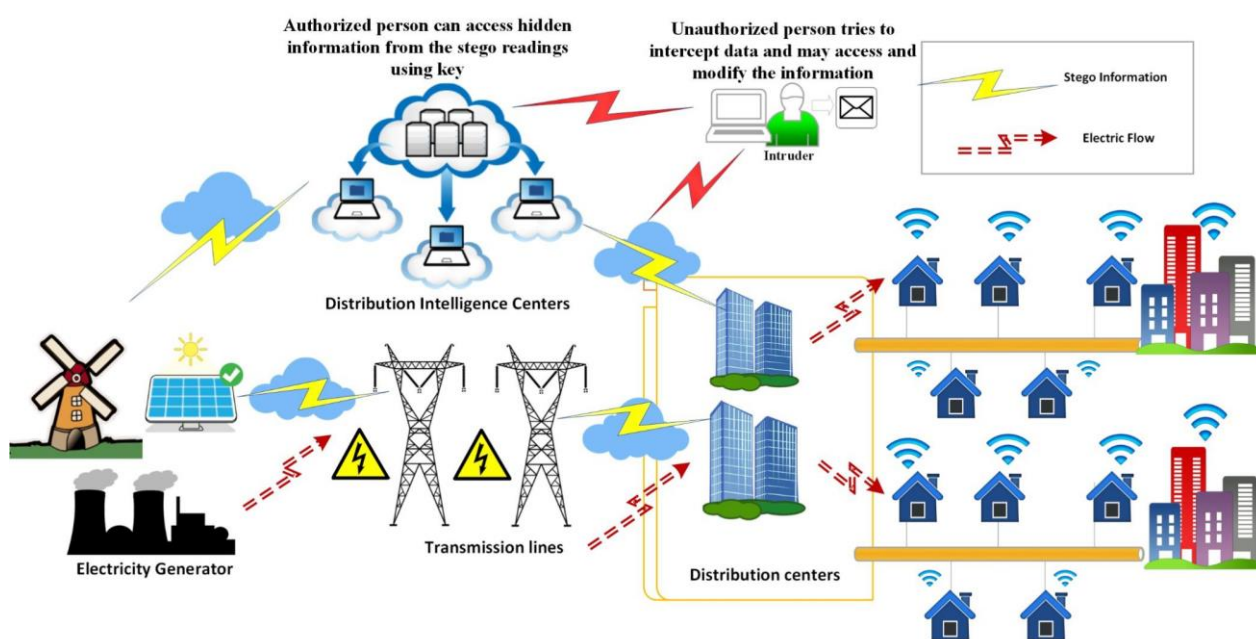


Figure 5.1 Architecture of the smart grid architecture

5.2 STEGANOGRAPHY ALGORITHM TO SECURE INFORMATION AND INTEGRITY PRESERVATION OF SMART GRID READINGS

A smart grid is an electrical grid containing several operations and energy measures, including smart meters, smart appliances, renewable energy sources, and energy-efficient resources [159]–[163]. In other words, it is an electricity supply network that uses bi-directional digital communication technology to detect and react to local changes in usage and deal with dynamic outage management and renewable energy. Real-time data of electricity consumption helps entities in the complete process of transmission for the efficient power system; due to this, load forecasting is also possible. The traditional grid system is unidirectional, and electricity flows from one point to another, whereas smart grids are bidirectional; one channel transmits electricity and the second channel transmits digital information [164], [165]. Fig. 5.1 illustrates the architecture of the proposed algorithm, including all the entities. The smart grid has many advantages over the traditional grid system:

- (a) It brings together all the entities involved in transmission systems to create an effective mechanism to be strong economically.

- (b) Generally, in a traditional grid system, faults or flaws cannot be gauged easily in power lines, whereas diagnosis can be made quickly on power lines, which are based on smart grid.
- (c) There are many features of a smart grid that help in the production of electricity. It is similar to the request-response model, where the production of electricity depends on the current needs of customers based on real-time data. Sudden changes in the system lead to an outage; the smart grid distribution intelligence system reroutes the path and restores electricity in the outage area. It is only possible with the cooperation of customers and distributors of electricity.

A smart meter has the potential to collect readings of every second or a minute (energy consumption readings and environmental features of the premises). Smart grid devices have limited memory and fewer computational capabilities than other smart devices [166]. It supports only predefined operations and performs a statistical calculation to identify current demand, production cost, faults, etc. Experiment is performed on periodically collected readings; readings are used as a cover object for hiding information of smart meter and consumer. The discrete wavelet transform is used to decompose readings into sub-band coefficients and used as cover object. Sensitive information is converted into cipher using Hénon chaotic map. Stego readings are constructed with negligible distortion in original readings after concealing bits into a cover object applying a double precision floating-point format.

5.2.1 CHARACTERISTICS OF SMART GRID SYSTEM

Smart grid system is recognized as a new trend of the power system in the 21st century due to its principal characteristics [159], [167], [168].

- 1. Consumer Participation:** Consumer participation is a major part of the complete system. The actual consumption of electricity is dependent on the real-time smart meter readings [169]. Demand side management can take many steps based on adequate real-time data. Since the meter readings are subject to daily fluctuations, electricity production is flexible enough to facilitate consumers and service providers economically. In some developed countries, price signals are sent by the energy

distributors to customers to manage their energy costs. It also helps production plants to avoid energy crises [170].

2. **Real-Time Pricing algorithm:** Tariffed Retail charges are calculated for the consumed electric energy. Monthly retail charges are based on an hour to hour meter readings which is not constant [171]. Every second, meter readings are significantly changed due to the usage of home appliances. Small changes in meter readings can affect domestic charges. Electricity providers rebate and surcharge the final amount, i.e., based on peak and off-peak hours.
3. **Resilience Network:** Many countries have envisioned smart grid architecture and are deploying smart meters along with sensors to monitor various kinds of readings and external parameters which influence the power supply. Ostensibly, climate changes also influence the consumption charges; due to this, the resultant payable amount is also affected [172]. Also, load forecasting and load shedding are based on the off-shore operations on the cloud data. Peak demand is fulfilled without using expensive electricity generation plants. Hence, the smart grid is sustainable.
4. **Distributed Generation:** To produce electricity dynamically, incorporating renewable energy resources into the grid helps the distributor fulfill large scale production of electricity [173]. On-site near transmission line or at distributor's end, renewable energy resources and small power plants are being established to help consumers and enterprises in applying dynamic pricing algorithm [170].
5. **Dependability:** Fault detection and self-healing are two significant features of a smart grid. It has many routers and multiple connections. Supply, as a result, is uninterrupted and smooth.
6. **Efficient:** Demand side management can improve the infrastructure of energy transmission and reduce greenhouse gas emissions in smart grid systems [174]. When load is increased at distribution's end, smart grids alert those channels consuming maximum energy, which is an indication to switch to a backup generator and operate on the local base station using stored energy.

Table 5.1 Taxonomy of Security Attacks in Smart Grids

	Customer's Information	Price Information	Smart Meter Information, Grid ID, Geometric Location, Total watts	Commands
Confidentiality	Eavesdropping of sensitive information	Price information and behaviour of electricity consumption leak.	Affect the resilience network	Disclosure identity and frequency
Integrity	Damage the entire system	Incorrect billing amount	Affect dynamic pricing and utilization of distributed energy	Malicious command activation (terrorist attack)

5.2.2 SECURITY THREATS TO SMART GRID SYSTEMS

In a hostile environment, sensitive information of a customer, smart meter readings and detailed data of power consumption recorded every second or minute along with different parameters are transmitted through public networks. Therefore, many security threats are possible in smart grid systems, such as false meter readings, denial of service, malware spreading and unauthorized access of the network [175], [176]; it is the result of passive (traffic analysis and snooping) and active attacks. Table 5.1 lists malicious actions that an adversary can perform to violate security services (confidentiality and integrity), affecting various parameters like price and meter readings.

Since sensitive data should be protected from illegitimate users and should reach only intended recipients, this entire mechanism is known as confidentiality. Payable or billing amount is completely based on energy consumption. If any change is made in recorded readings (watt consumption), the cost is different from the actual due amount. Integrity preservation ensures all the communicating parties that the data is completely accurate and it is derived from the actual route [81]. In order to attain these security services with minimum computation, steganography has been implemented for a resilient smart grid communication network.

In the last few years, many researchers have investigated the smart grid system to have an optimal solution for the security aspect using different cryptographic techniques [177]–[179]. In this work, sensitive information is converted into cipher using Hénon chaotic map based on one-time pad stream cipher scheme. Consequently, smart meter readings are used as a cover object and cipher is concealed in readings in such a way that there is almost negligible distortion in original readings after hiding the secret information.

Most often, only secret information is retrieved from the stego object at the receiver's end, but in this model, along with the secret information, original readings are also reproduced by stego readings [180].

5.2.3 HÉNON CHAOTIC MAP

In the proposed model, Henon chaotic map is used to secure the sensitive information of users. Henon chaotic map is discussed in section 2.2.3. and Equations. Eq.(2.1)-Eq. (2.4) are used in this work to encrypt the sensitive information of smart meter and user.

5.2.4 WAVELET TRANSFORM

Wavelets are the functions that originate from a single function called the mother wavelet. Wavelets are most likely used in image and signal processing to convert signal or image from spatial domain to frequency domain for obtaining various details. Discrete wavelet transform (DWT) and the continuous wavelet transform are two ways to analyse the signal [181]. In the last few decades, DWT is primarily used to analyse the signal due to its property, i.e., sub-band coefficients are discrete numbers rather than continuous functions.

When a signal S is processed with DWT, detail coefficients and approximation coefficients are obtained from the high pass filter and low pass filter respectively [182]. Discrete wavelet transform and inverse discrete wavelet transform are defined by the equations Eq.(4.3) and Eq.(4.4).

5.2.5 PROPOSED ALGORITHM

This section presents a novel technique to secure information of customers and smart meters using the steganographic technique. Secret information is embedded in meter readings in such a way that eavesdropper cannot extract the secret information. In literature, only secret information is extracted from the stego object and cover information is discarded at the receiver's end. However, in this model, secret information, as well as original meter readings, are extracted from stego readings. Recovered readings have practically insignificant differences with actual meter readings. N numbers of readings and $L = 5$ levels for the Haar wavelet (i.e., *db1*) are used to obtain the sub-band coefficients. Readings are the prime attribute of size 1×2^n , where n must be an integer number.

5.2.5.1 Information Encoding

Name, address, contact number, grid id, and geometric location are the prime attributes of a customer to define his identity. In first phase, secret information is converted into a binary format. Then this 8-bit value is divided into two halves containing 4 bits each. Each chunk value lies between 0 to 15. m and n (size of hidden data) are calculated based on the level of reading and Wavelet Transform, where, $m = 2^{L-1}$ and $n = \frac{N}{2^L}$. Secret information is stored in matrix M of certain size. Thus, the resultant matrix M , of order $m \times n$ is obtained.

5.2.5.2 Secret Data Generator using Hénon Chaotic Map

Matrix M is encrypted through the pseudorandom numbers which are generated by the initial seeds or pair of keys. Thus security relies on the keys. Equations (2.1) and Eq. (2.2) are used to generate the sequence, which is converted into bit values by applying (5.3). One set of four bits is combined to generate a decimal value and stored in the matrix of order $m \times n$. Cipher matrix M' is generated by applying the detailed procedure of the encryption algorithm.

Step 1: Hénon map acts as a keystream generator for the cryptosystem. The size of the sequence depends on the size of secret data created after dividing byte information into a 4-bit format (i.e., matrix M). If the size of secret data is $m \times n$, then $4 \times m \times n$ sequence is produced by applying Eq.(2.3), Eq. (2.4)

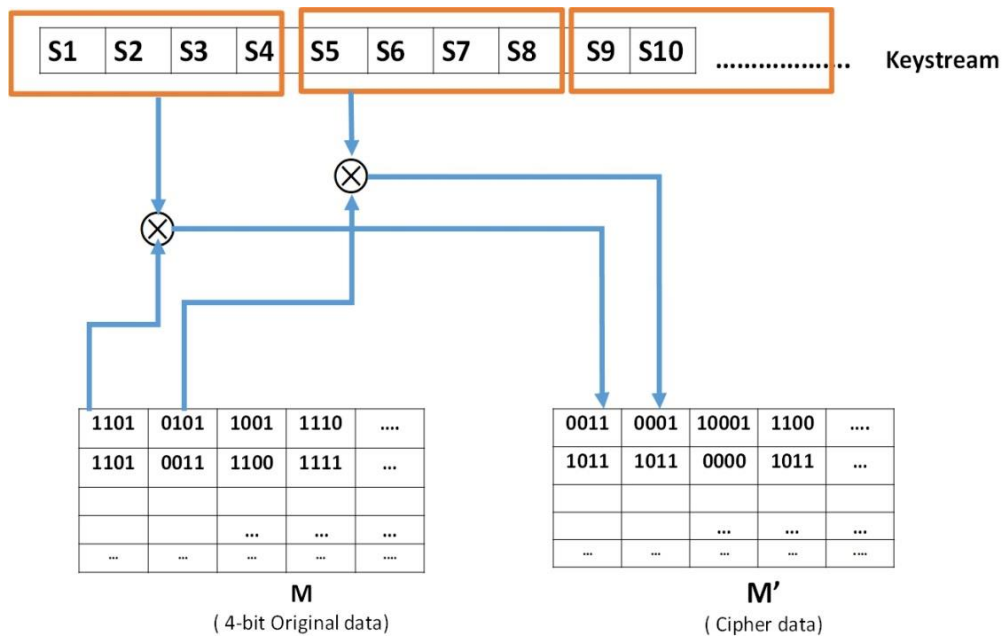


Figure 5.2 Bitwise encryption procedure

Step 2: Experimental analysis concludes that if the cut-off point is 0.3992, then the sequence is balanced, as shown in equation (5.1). Values are then converted into binary values depending upon the threshold value Z , where,

$$Z_i = \begin{cases} 0, & \text{if } X_i \leq 0.3992 \\ 1, & \text{if } X_i \geq 0.3992 \end{cases} \quad (5.1)$$

Step 3: Hénon sequence is then reduced by combining each consecutive four bits into one pair of bitstream. This pair of bits are XORed with data at first index position of M in bit-wise fashion, and next four bits of keystream is XORed with next value of M and the procedure goes on until all the elements of M are XORed with keystream of Hénon chaotic system as shown in Fig. 5.2.

5.2.5.3 Generation of Coefficients

One-Dimensional DWT with Haar wavelet is used to decompose smart grid meter readings

into least significant (detailed coefficients) and approximation coefficients. Smart meter readings are stored in the tree structure at root node (Level 0) and also consider that detailed coefficients are always stored as right child. Haar wavelet is applied to obtain these coefficients up to 5 levels. All leaf nodes (sub-band coefficients) of the right subtree of the root node are used as a cover object to hide the sensitive information. DWT has the property to reconstruct the signal using approximation coefficients. Therefore, detailed sub-band coefficients are utilized as a cover object for the secret data. For N numbers of meter readings, DWT is only applied to detailed coefficients of the meter readings to obtain the subband coefficients. These subband coefficients at level five are stored in 2D matrix Z ; after that, these coefficients are normalized. It has been observed after examining the coefficients that value up to 12 precision can produce better results. For clarification, if 1024 readings have been recorded and the Haar wavelet is applied up to five levels, size of matrix Z is 16×32 .

5.2.5.4 Bit Insertion into a Cover Object

The goal of the proposed algorithm is to hide the secret data efficiently to gain minimum

Algorithm 5.1: Bit Insertion into a Cover Object

1. Initialize ptr←21;
2. for i ←1: to m
3. for j ←1 to n
4. temp ← Z(i,j);
5. convert the value of temp into IEEE-754 64-bit double precision.
6. Take fraction part F of temp
7. Stego ← (F(ptr: ptr+3)&(0000))
8. stego'← (stego | M(i, j)).
9. F'←(F(1: ptr-1),stego', F(ptr:end-4))
10. Generate a floating point number from the new F' and saved as Z'.
11. end

distortion in original readings. After conducting many experiments, it is observed that a double-precision floating-point number system (IEEE 754) has the potential to conceal data inside the subband coefficients to achieve the goal of the proposed algorithm. Resultant high-frequency coefficients are used as cover object to embed the resultant matrix M' . The fractional part F is used for hiding secret bits into coefficients. Stego coefficients Z' are used to construct the stego meter readings applying the inverse discrete wavelet transform IDWT. The secret information is incorporated in such a manner that without losing a single bit, information and readings from stego are recoverable. Statistical results are obtained using the stego and retrieved readings (after the removal of hidden information). The pseudocode of the bit insertion is discussed in Algorithm 5.1.

5.2.5.5 Retrieval Process at Receiver's end

Stego meter readings are received on the other side of the communication channel. DWT is applied to stego meter readings to obtain the coefficients at the receiver's side. Resultant coefficient matrix is generated. Now information is extracted from the coefficients and bits are arranged into a decoded array and converted into 8-bit values. Since Hénon chaotic map is deterministic, therefore using the same key pair (keys are transmitted through a secure channel) secret data is retrieved using the same mechanism for encryption but in reverse order. Now reconstruct the original coefficient from the stego coefficients, original meter readings attained by applying the inverse discrete wavelet transform. It has been observed that retrieved readings have almost negligible difference from original meter readings sent from the customer's end. The retrieval process is briefly explained in the proposed Algorithm 5.2.

5.2.6 EXPERIMENTAL RESULTS

The Proposed algorithm is implemented on several different types of smart meter readings along with sensitive information of a customer and smart meter. Matlab (2015) with the 64-bit machine, is used for numerical simulation. The laboratory for advanced software systems calculated the consumption of power and its affecting factors (inside/outside temperature, wind-chill and heat index) of every minute and every second of several months with the support of smart meters in many homes and buildings under "Smart Project" in their database [183], [184]. Database readings are temporal because they are collected every second from different houses by equipping smart meters with different sensors. For numerical simulation, smart

Algorithm 5.2: Retrieval Process

```
1. Initialize: ptr←21
2. for i←1: to m
3. for j ←1 to n
4. temp ← Z'(i,j);
5. convert the float value of temp into IEEE-754 64-bit
   double precision and stored into a temp
6. Take fraction part F of temp
7. Secret_info← F(ptr);
8. M(i,j) ← secret_info
9. Now rearrange the rest of the bits into F'. Now
   formation of bit starts from:
10. F' = (F (1: k-1), F(k+4:end),0000)
11. Generate a floating-point number from the new F', which
    is stored into coeff matrix.
12. end
13. end
```

meter readings are taken as a cover object for the steganography with the support of smart meters in many homes and buildings under "Smart Project" in their database. The experimental results of three different readings can be observed in Fig. 5.3. Plots of smart meter readings and its stego readings are similar in watt consumption versus time (X-axis). Also, the plots of smart meter readings and extracted meter readings are similar and there exists a strong relationship between these readings; both graphs are similar.

5.2.6.1 Key strength Analysis

Hénon chaotic map is used to generate pseudorandom numbers using initial seeds X_1 and Y_1 ; the key is elected in floating-point number and double precision is represented by the 64-bit system [185], [186]. Since two values X_1 and Y_1 are considered for the key, in this case, the key size is 2^{128} . It means the key is very sensitive to the initial condition and can resist brute force attack; a small change in a key gives almost different results while deciphering the encrypted data.

5.2.6.2 Percentage Residual Difference Test

To evaluate the performance of the proposed algorithm, the percentage residual difference test (PRD) is performed on smart meter readings. This test is used to find the difference between actual readings and stego readings or retrieved readings (i.e., resultant distortion in original readings) at the recipient's side.

$$PRD = \sqrt{\frac{\sum_{i=1}^N (R_i - R_i')}{\sum_{i=1}^N (R_i^2)}} \times 100 \quad (5.2)$$

Here R_i is original meter reading and R_i' denotes either stego reading or reconstructed meter reading (i.e., removing all the sensitive information from the stego reading). PRD test is calculated between stego and original readings, and also between retrieved readings and original readings. Table 5.2 shows the PRD outcomes of several smart meter readings using Eq. (5.2).

Table 5.2 Percentage Residual Difference Test

No.	PRD (Original Readings, Stego Readings)	PRD (Original Readings, Retrieved Readings)
1	0.00010600	0.00000019
2	0.00007206	0.00000010
3	0.00081278	0.00000162
4	0.00007230	0.00000018
5	0.00089600	0.00000065
6	0.00006990	0.00000015
7	0.00009320	0.00000065
8	0.00006320	0.00000078
9	0.00003320	0.00000003
10	0.00011265	0.00000017

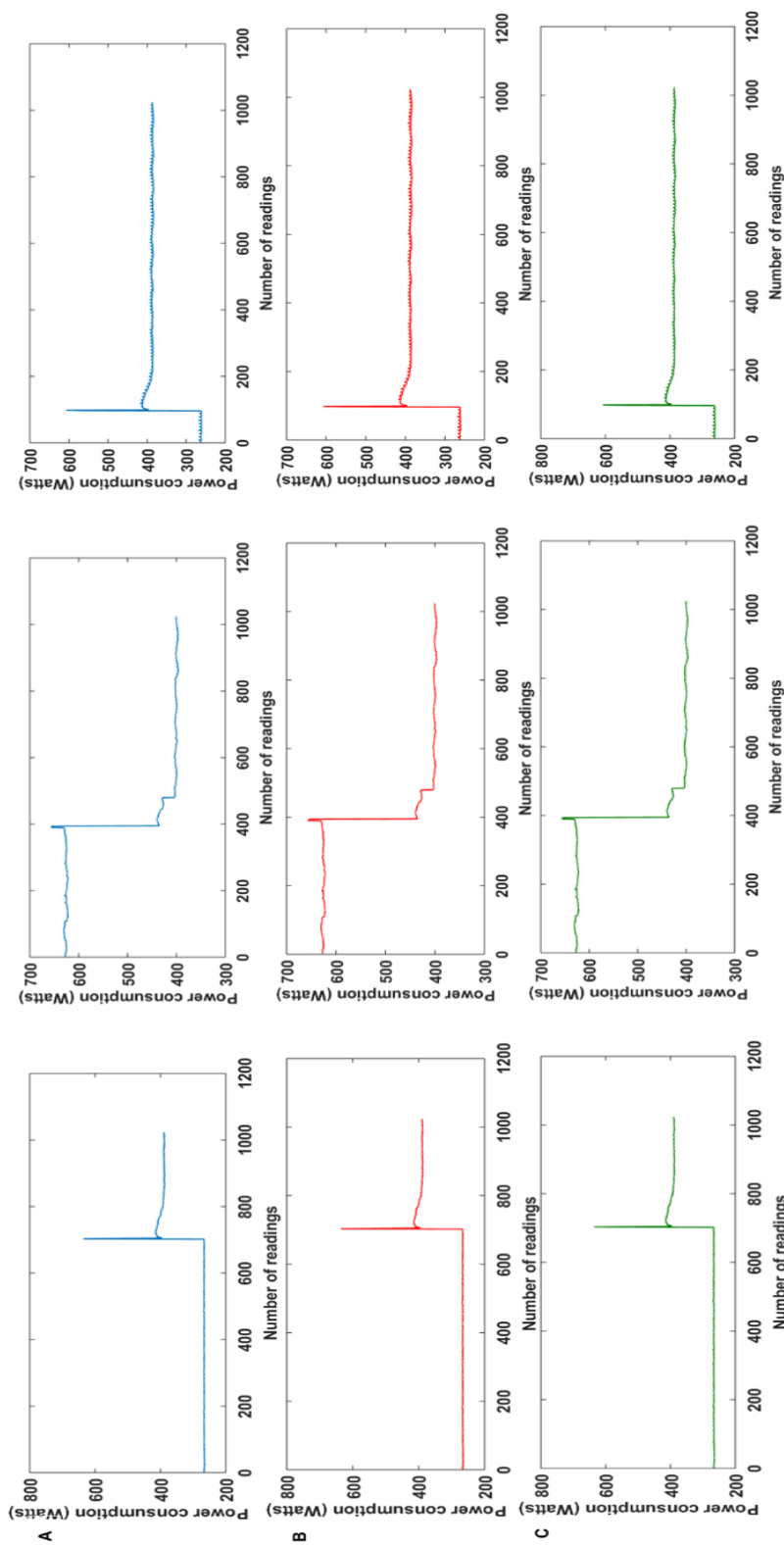


Figure 5.3 Simulation Results on power consumption readings(Watt) A. Original readings B. Stego readings C. Retrieved readings from stego readings

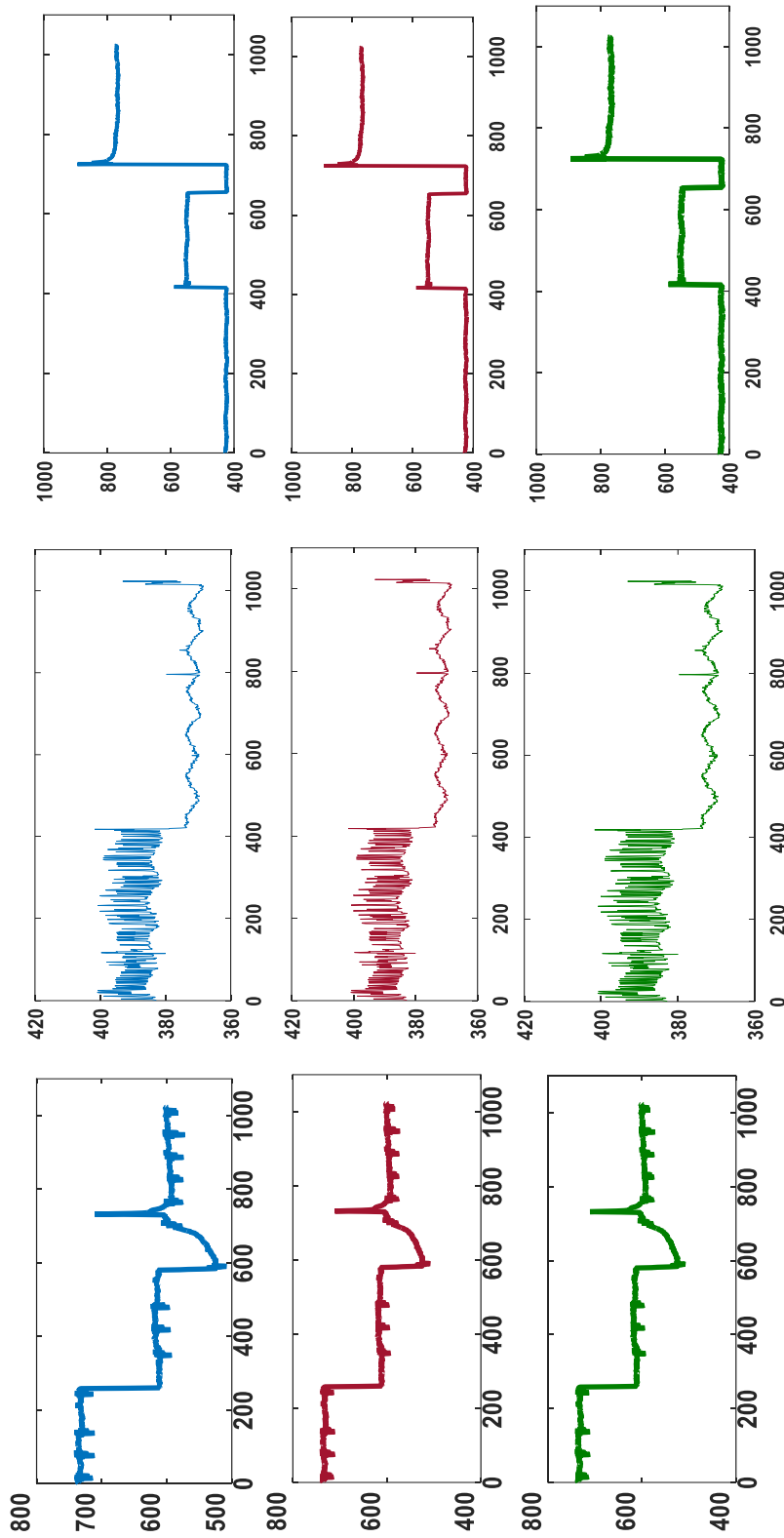


Figure 5.3 (Second Simulation Results on power consumption readings(Watt) A. Original readings B. Stego readings C. Retrieved readings from stego readings

5.2.6.3 Integrity Preservation

A signal is transmitted through public networks and it is the challenge for a smart grid system to verify that readings are accurate and not altered during the transmission. There are two main reasons of integrity loss: (1) In digital transmission, bits are transmitted through the communication channel in which bits are corrupted or altered due to noise, distortion and interference. (2) To harm the system, channel is continuously monitored and analyzed for the wrong purposes. Data is altered and modified data is injected into the place of original data. To verify the integrity of the proposed system, Bit Error Ratio (BER) is carried to the smart meter reading, which is capable of detecting data loss even if a single bit changes. If it is any non-zero value, this means that the data has lost its authenticity. For numerical simulation, unity matrix is initialized to '0000,' i.e., 4-bits, concealed instead of secret information in the original signal (based on the parity bits concepts). Later, Gaussian noise is added to the stego readings. Figure 5.4 depicts the impact of noise after adding it to the signal and BER is calculated for

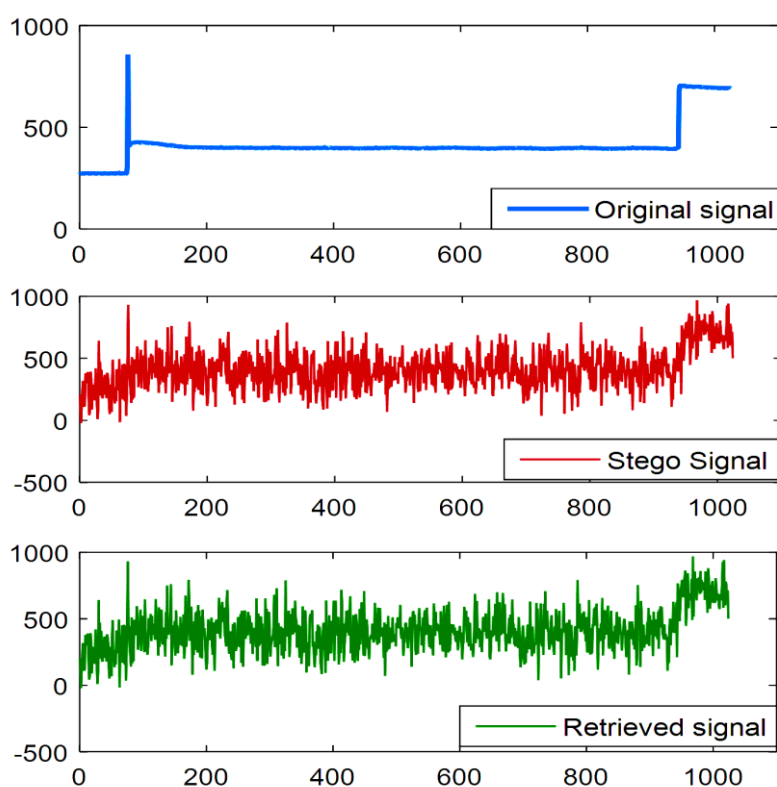


Figure 5.4 Gaussian noise Test: a) Original readings b) Stego readings after noise insertion c) Retrieved signal from stego readings.

the above scenario and it is obtained to be 51%, and without noise, it has been observed 0% using equation (5.3).

$$BER = \frac{B_{\text{erroneous bits}}}{B_{\text{total bits}}} \times 100 \quad (5.3)$$

5.2.6.4 Comparison with other Models

Various research has been undertaken to design a system to secure customer information and protect smart meter readings. The billing amount is based on electricity consumption. If unit

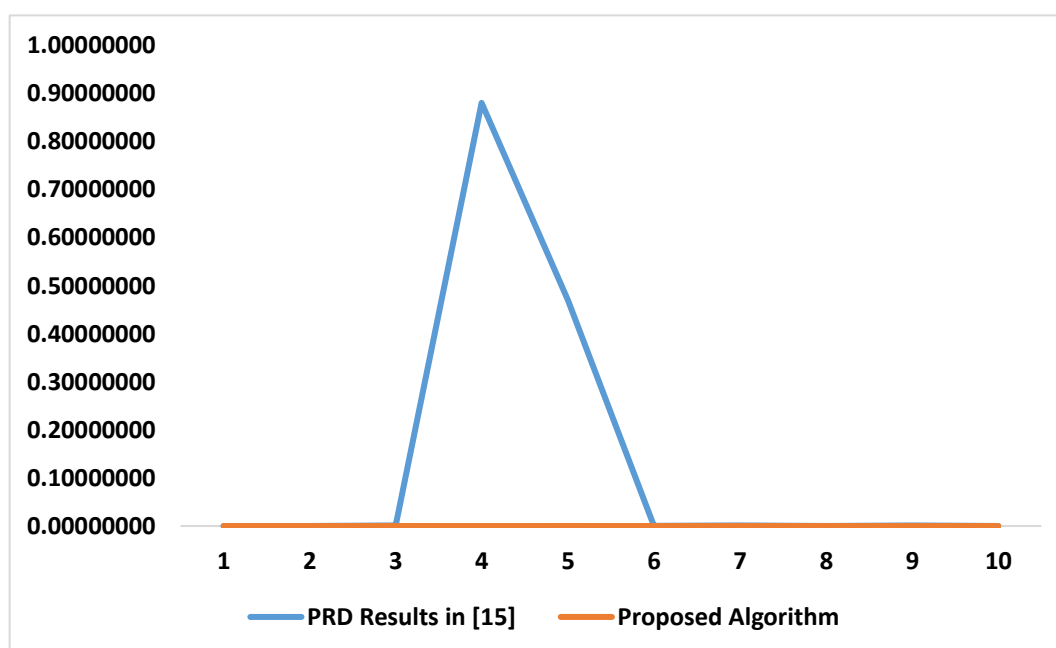


Figure 5.5 PRD comparison results

cost is high, then a small reading error may give an inaccurate bill to the customer. Simulation results are compared to [181], and it is found that the proposed algorithms give less distortion than their work (i.e., percentage residual difference), as shown in Fig.5.5. In order to obtain negligible distortion, research has been conducted on IEEE 754 double-precision floating-point number system along with Hénon chaotic map.

5.3 INTERNET OF BATTLEFIELD THING SECURITY: A STRATEGY TO SECURE SENSITIVE INFORMATION

The proposed model also aims for similar objectives, as we have discussed in section 5.2. Furthermore, we have taken sensor readings and sensitive information of the battlefield instead of a smart grid. The battlefield is emerging with the advancement of new technologies in wireless sensor networks. This work presents a novel approach to secure sensitive information such as geometric coordinates, weapon information, military equipment, defence logistics and soldier's sensitive information in the surveillance area of the battlefield by using steganography. Digital sensing devices are installed on their combat suits, helmets, shoes, weapons and equipped with smart devices to transmit and acquiring the war strategical information and environmental data. The proposed algorithm is based on the reversible data hiding technique, where sensor's readings are taken as cover object to hide sensitive information. Secret information is extracted and readings (cover object) can be reconstructed at the receiver's end with almost negligible distortion. Also, stego readings can be used directly at the recipient end without applying any mathematical operation. In order to achieve the low complexity and minimum computation of the proposed algorithm, the Fresnelet transform is used to decompose the sensor's data into its subband coefficients along with the adaptive model of the elementary cellular automata to protect the sensitive information. The least significant coefficients are used as a cover object to hide sensitive information. The sensitive information can be embedded in each coefficient in the form of either 4 bits/coefficient and 8 bits/coefficient. The percentage residual difference test (PRD), MSE (mean square error), PSNR tests have been performed between stego and original readings as well as with reconstructed readings. The obtained value of the PRD test has much significantly lower compared to other existing algorithms. Other experimental results show that the proposed algorithm is reliable, robust, and highly secure for the devices in the Internet of battlefield things (IoBT) because information retrieval at the receiver end is trivial and also preserves the integrity of the sensor's data. Battlefields are exploiting the IoT driven technologies for their advancement with the best possible technologies. IoT in military establish the communication channel that enhances the throughput by developing trust and authentication in the system. The modern battlefield management systems can monitor and analyze the warfare area and perform

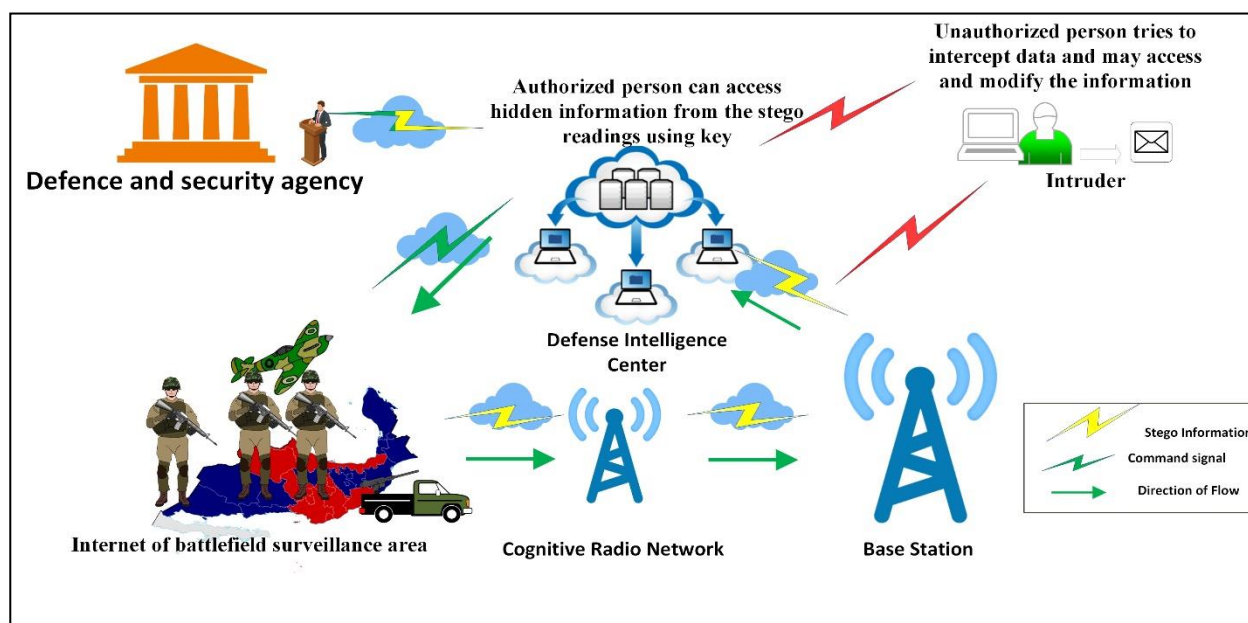


Figure 5.6 Architecture of the Internet of Battlefield Things

multiple measurements according to the war zone situation.

Sensory information is collected through the sensors and it is transmitted through the cognitive radio networks. When a spectrum is consumed by many users (primary and secondary users) in the region, it is difficult to manage all the available resources; Cognitive radio helps in such a scenario that all the interconnected devices of IoBT can access the channel [165]. Since wireless sensor networks are those networks that operate on a specific frequency band, and for the availability of the channel, security agencies and satellite channels are using TV bands due to their capability to transmit data efficiently. Tracing and monitoring are two major applications of the sensor network.

In a battlefield environment, situational awareness is very much required to reciprocate the enemies. The Internet of Battlefield Things is equipped with the best possible smart military devices and networks to conduct their operations efficiently. Usually, signals are transmitted through public networks, but national security agencies transmit the data at a specific frequency [187]–[189]. Many countries and organizations have prepared a roadmap for implementing cognitive radio networks (CRN) for war-level strategic communication, i.e., tactical communication. In contrast, a tactical cognitive radio is also based on the same cognitive radio policy, but here it uses the existing radio sensor networks [190], [191]. As per the news reports

of the year 2020, it can be believed that all developed countries are deploying software-defined radios (SDR) due to a variety of features. Reducing the number of hardware components results in reduced equipment weight significantly. Besides, the computation power of equipment or devices is becoming limited. SDR helps soldiers on the battlefield speed up by removing the blockage caused by overhead. The proposed model is based on a simple calculation that needs minimum storage as well as the computation efficiency of systems. Fig. 5.6 illustrates the architecture of the proposed work (Model 2); it is based on IoBT.

IoT has very strong applications in the military and battlefield. IoBT is also referred to as IoMT, an abbreviation as the Internet of Military Things finds applications such as connected military infrastructure like Radar station, operational bases, command and control center etc. and connected military equipment like battleships, submarines, fighter and cargo planes, drones etc. IoBT is realized in a network that connects the infrastructure equipment and helps reduce the response time and increase situational awareness. Risk and damage assessment is also a part, and it can be achieved using IoBT. Connecting a soldier to the Internet can revolutionize the idea of modern warfare. Soldiers wear sensors and cameras connected to the network and provide real-time feed so that the commanders at the command and control centers can assess and monitor the situation that allows them to make timely decisions. Sensors also communicate information between soldiers so that different groups of soldiers are well aware of other sections' position and status, be them friendlies or enemies. It includes their GPS coordinates, their weapon status and casualty status. It helps the on-ground commander to take quick actions and execute the operation and planning correctly. Decisions are made based on knowledge and awareness of the environment and such information is collected through the rules, sensor node, and network topology. From the past experience, CR can take necessary actions quickly. Power management of sensor nodes is done by consumption states such as sleep, deep sleep, and hibernate. Sensor nodes have minimal computation capacity, along with limited memory. Dynamic Spectrum Access (DSA) is the real-time adjustment technique that ensures that all the secondary participants can share the available resources until the primary users demand it for their utility access [71]. The interconnection of military equipment with networks and physical infrastructure lead to modern combat war. Keeping the main points of the specific effects of signals led to the signal corps formation, a group that held a special place in military communications strategy. The signal core evolved into a specific task, where the

signalliner became a highly technical task to deal with all modes of communication ranging from simple to available. Many digital components from the civilian area can be weaponized to help out military tasks. Geographical information is stored and transmitted through a geographical information system via spatial coordinates. An application is a geographical information system (GIS) that supports many features such as collecting data, monitoring analysis, and changes in a map. It is very important to be aware of the exact situation of guns in the military and war zones. It is necessary that the soldiers fighting the warfare should give accurate details of their health-related information, location, and distance of the enemy in their headquarters for a fixed time interval. The proposed work is designed in such a way that sensor information can be transmitted without any alternation. In addition, sensitive information can be concealed in the readings. In the future, the battlefield will be converted into a digital war zone, where soldiers' involvement will be reduced due to embedded systems and machine intelligence. The Internet of things has also been introduced to military and security agencies of many countries. Traditional management is being equipped with the Internet of battlefield things. With the advancement of digital technology, signals are being transmitted through channels. In the last few years, researchers and government agencies are interested in securing battlefield information. The battlefield is usually connected with the wireless sensor network to transmit crucial information to their agency and the server room to take necessary actions. Several researchers have identified the research gap in this area and proposed many algorithms to overcome such issues.

5.3.1 SECURITY THREATS TO BATTLEFIELD AREA

In a hostile environment, A better decision can be made on the basis of a reliable decision. IoBT includes many components like sensors, devices, weapons, radio networks and IoT devices. Now soldiers are connected directly with headquarter and can collect real-time information. Soldiers can transmit and receive valuable information to make decisions. Digital devices are also upgrading with time to increase the robustness with high tech development. The opponent also governs other battles to harm the system by attacking the network, blocking the signal, large exposure amounts of information, and altering the true information without giving any clue. In a hard real-time world, accessibility of communication channels is becoming an issue and trust is created when users assure them that channels are functional and

on-demand; communication can be established without any delay. Receiving and transmitting information, images, voice, and images is done through several sources such as radar, image acquisition tools, and sensors. The flow of signal needs to be barrier-free without any interruption for the smooth functioning of all the equipment and devices. The following objectives are designed to ensure the privacy and integrity of the proposed model.

1. Signals are usually transmitted through the unsecured channel, i.e., Cognitive sensor node, without applying any security protocols. Therefore, it is required to protect information that could be a game-changer in the war zone. With the help of steganography, information cannot be read by unauthorized persons (secret data must be encrypted before embedding procedure). Only the intended person can decrypt or fetch the actual information which is embedded in the original signal or sensor data.
2. Periodically collected readings are received at the receiver end and it is claimed that it has been sent by the genuine source. Now defense server can find a solution for such a situation by using watermark extraction. The proposed algorithm also supports verifying the source authentication by embedding a watermark.
3. The proposed algorithm can also be used for integrity preservation if any noise due to the physical medium or signal is altered by the unauthorized person. At the receiver end, it can find out that the received signal is altered or modified. MDC (message detection code) can be hidden in the signal for such a process. Checksum bits are concealed with the signal; if alterations are made on the signal, that can be easily detected.
4. Since the stego signal contains a significant amount of information of readings, and one of the advantages of the proposed model is that stego signal can be used and processed at the receiver's end without any further operations.

5.3.2 BACKGROUND

The proposed work defines the capability to handle sensitive information securely to achieve confidentiality and integrity. The proposed algorithm is based on steganography and consists of Fresnel transform, ECA and P Box to achieve confidentiality and integrity. Steganography technique is applied to hide the sensitive information in such way that eavesdroppers cannot retrieve or access sensitive information by applying all possible cryptanalysis attacks.

5.3.2.1 Fresnelet Transform

Linear integral transforms are widely used in several fields of science and optics due to its properties, such as a complex problem that can be converted into another domain with its normalized equation, and the solution can be reverting back to the original domain using inverse transform. Duality property plays a vital role in reconstruction in the transformed domain. FT also has the advantage of rapid reconstruction of high-resolution Fresnel holograms [192]. Many researchers are experimenting with watermarking and steganography using linear integral transforms. Fresnelet Transform is selected for the proposed algorithm because a signal can be reconstructed using only five percentage high energy coefficients; therefore, High energy coefficients are not utilized, and operations are performed on least significant coefficients. Many transforms have inherited the properties of the generalized Fresnelet transform. Functions of FT are shift-invariant on a level-by-level compression. FT has multiresolution properties when it is applied to wavelet bases. The general formula of the two-dimensional Fresnelet transform [193] and its kernel K_{τ}^{\approx} is given in Equations. (5.4) and (5.5):

$$F_{\tau}^{\approx}(x, y) = (F \times K_{\tau})(x, y) \quad (5.4)$$

$$K_{\tau}^{\approx}(x, y) = \frac{1}{\tau^2} e^{i\pi(\|x, y\|/\tau)^2} \quad (5.5)$$

5.3.2.2 IEEE 754 Standard

Digital devices are equipped with arithmetic logical units (ALU) to handle the real-time applications and are designed according to the pre-processing capability. IEEE Floating-point numbers are data type standard that follows the representation format to store float values. Real numbers are extensively used in cryptography. The Institute of Electrical and Electronics Engineers represented a binary floating-point number in 1985 and augmented it in the year 2008 to represent floating-point numbers and process them [194]. It depends on the computer hardware that how numbers are stored and processed for required operations. IEEE has designed many standards of floating-point numbers. Unlike integer data types, floating-point numbers are used for real-time scientific computation operations along with sharper precision. Integers are generally used for counting, but fractional numbers are used in advanced

technology, where every part of the numerical value is important to get adequate results. In the proposed algorithm, the IEEE 754 standard of double-precision, as shown in Fig. 5.7, has been used to store the values of the coefficients. In this standard, Three components are required to represent a binary floating-point number: $(sign) \times mantissa \times 2^{\pm exponent}$

Where the sign is one bit, the mantissa is a binary fraction with a non-zero leading bit, and the exponent is a binary integer.

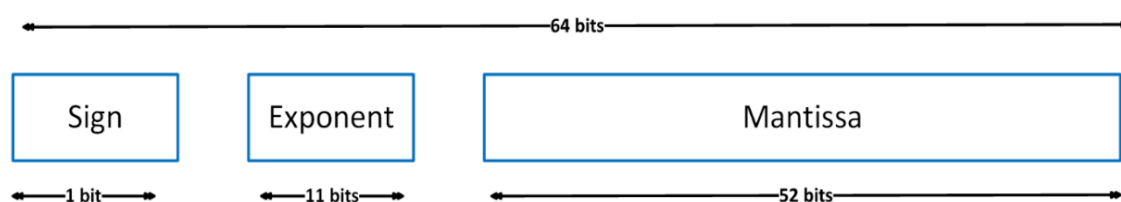


Figure 5.7 IEEE 754 Floating-point double precision standard

5.3.3 PROPOSED ALGORITHM

In this study, we have taken Fresnelet Transform, and it operates on signal differently than DWT; also, generated coefficients by Fresnelet transform are obtained in complex numbers wherein DWT coefficients are collected in a real number system. Secret data is embedded into the readings after applying the encryption module (chapter 3: Model 1) is applied to sensitive information. These coefficients play a vital role in steganography. Since stego readings contain the same information as the original signal, so the cloud and head of the server room can use it directly without any decoding mechanisms. The proposed algorithm can also be utilized as a mechanism to give the assurance of integrity preservation by using checksum bit insertion; it verifies that the readings are not altered by eavesdropper or noise. Readings S is used as an input for the first phase of the proposed algorithm, where Fresnelet transform operates on the readings. Later, sensitive information is embedded in the least significant coefficients and stego coefficients are generated. The inverse of Fresnelet Transform is applied to stego coefficients for the formation of the stego signal.

5.3.3.1 Information Encoding and Secret Information Generation

In the warzone, every detail of crops and the enemy is important. Sensitive information on the

war field plays a critical role in taking necessary actions; therefore, such information must be protected. Here, the secret information size is completely based on the signal size and the amount of least significant coefficients.

- In the experiment, it has been found that the signal can be reconstructed with 5% of high energy coefficients using the Fresnelet transform. Thus the least significant coefficients can be used up to 95% to hide the secret information. Therefore, secret information also relies upon the sample size of the signal. In each coefficient, four or eight bits of the secret message is embedded to obtain minimum distortion in the signal. Let signal size is N and the least significant coefficients are obtained in *percentage*.

Bit capacity of secret data = (length of the signal \times percentage \times (4,8)bits)

- To ensure data privacy, sensitive information of the battlefield is encrypted with Model 1 (ECA, P Box), i.e., is presented in chapter 3, section 3.2. after the encryption process, Confidential data M' is converted into the encrypted secret message M . Since security of the encryption algorithm relies upon the key so the message can not be decrypted unless one has the correct key of the cryptosystem.
- Now, secret information is preserved in M , and these bits are concealed in the cover object. The entire process is highly secured and based on the key (i.e., is kept as a secret)

5.3.3.2 Coefficient Generation and Bit insertion Algorithm

- (a) Sensor readings are transmitted through the sensor node, and it is assumed that it is transmitted through an unreliable medium. Sometimes confidentiality of signal is not required in a communication network; in such cases, it can be used as a cover object to hide the sensitive information. These readings can be treated as a signal for the proposed model.
- (b) Input signal S is one-dimensional and it is reshaped to a two-dimensional signal. In this work, we have taken 1024 samples of the signal. If the size of the signal is N , then the updated signal S' will be the size of $[m, n] = 2^{\left(\frac{\log_2 N}{2}\right)} \times 2^{\left(\frac{\log_2 N}{2}\right)}$
- (c) Fresnelet transform is applied to the signal up to the five levels to decompose the signal S' . Coefficients are the sum of least and most significant coefficients. A signal can be

reconstructed easily, only applying high energy coefficients. Low energy coefficients can be avoided in the retrieval process. Fresnel transform requires a set of parameters such as wavelength, sampling distance between values of S' and based on these set of values, τ (tau) is calculated. Obtained coefficients are stored in the 2 D matrix $coeff_S'$. The working procedure of embedding is illustrated in Fig. 5.8.

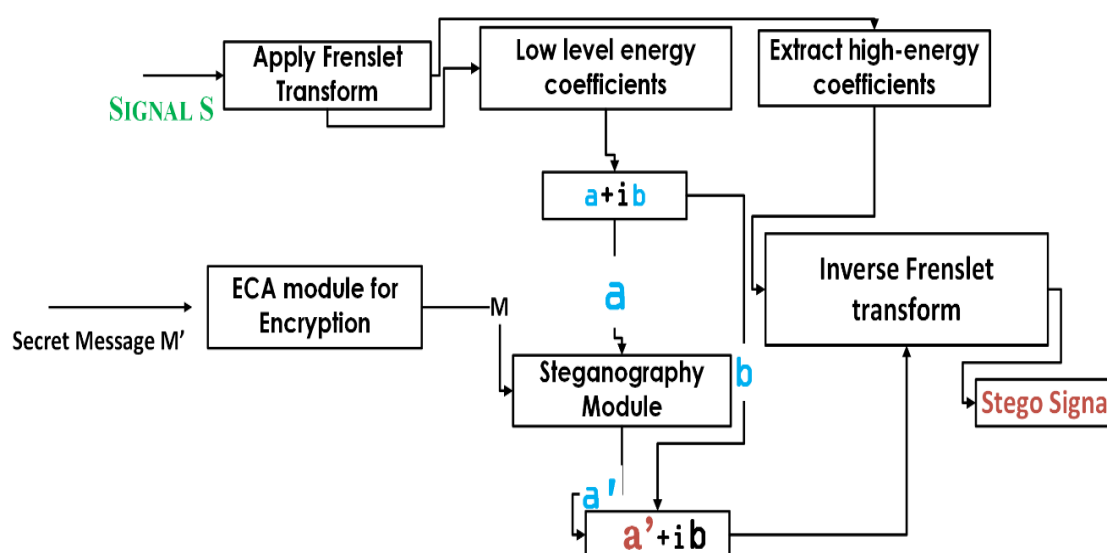


Figure 5.8 Embedding procedure of secret message

Algorithm 5.3: Bits concealed into signal/readings

1. Initialize ptr (ptr=29:8bits/coff ptr=21 4bits/coff)
2. Bits per Coefficients $\leftarrow n$
3. Read the $coeff_S'$ coefficients matrix.
4. for $i \leftarrow 1$: to Row
5. for $j \leftarrow 1$ to Col
6. if FLAG==zero
7. $coeff_S' = (Real(coeff_S') + \text{imaginary part } Img(coeff_S'))$
8. $temp = Real(coeff_S')$
9. Convert the value of $temp$ into IEEE-754 64-bit double

```

precision.
10. Stego ← (temp(ptr: ptr+(n-1))&&(0̄)n)
11. stego' ← (stego || M(i, j)).
12. temp' ← (temp(1: ptr-1), stego', temp(ptr:end-n))
13. Generate a floating-point number from the new temp'.
14. assigned values to StegoReal(Coffs').
15. Stego_coff = StegoReal(Coffs') + Img(coffS')
16. else
17. Stego_coff = coffS' // No change in the coefficients.
18. end
19. end
20. end
21. Reconstruct the Stego signal StegoS' using the Stego_coff
    by applying inverse Fresnelet transform.

```

- (d) Now, **coff_{S'}** values are associated with flag values (0,1) based on the energy threshold. It is observed in the experiment that Fresnelet transform can be reconstructed using 5% high energy coefficients along with stego coefficients. Thus, 95% of the lower band's coefficients can be utilized as a cover object (i.e., the least significant coefficients are used as cover object to hide the secret information). **Flag 1** is linked with higher energy coefficients, and **Flag 0** is linked with the least significant coefficients.
- (e) The least significant coefficients are used to hide secret information. Secret information is concealed into the coefficients in such a way that if a signal is reconstructed, it has a minimum or almost negligible distortion in the original signal.
- (f) It is observed that coefficient values are complex numbers ($a + bi$) by applying Fresnelet transform. **coff_{S'}** coefficients matrix values are decomposed into two parts: (i) Real value segment **Real(coff_{S'})** (ii) imaginary value part **Img(coff_{S'})**, and steganography is performed upon the **Real(coff_{S'})** of the least significant coefficients (Coefficients in **coff_{S'}**, where flag values are associated with zero). Later stego real value matrix **Stego_{Real}(Coff_{s'})** is combined with imaginary

value matrix $Img(\mathit{coeff_S'})$. Algorithm 5.3 discusses the embedding procedure of the proposed work.

5.3.3.3 Bit extraction and Reconstruct of Original Signal

Stego signal or stego readings are collected at the receiver end. These sensor readings can be directly used without applying operations as original readings because stego readings have as minimum distortion as possible in the original sensors readings. At the receiver's end stego signal works as an input and to get the secret message and cover information, steps are followed as per Algorithm 5.4.

5.3.4 EXPERIMENTAL RESULTS

The Proposed algorithm is tested on several readings of the cognitive radio network. A similar setup of software and hardware is used for the simulation, as described in section 5.2. Database readings are temporal because they are collected every second from different sensor networks by equipping smart devices. Intel Berkeley research lab collected data of sensor nodes that are used for numerical simulation [195]; they have collected 2.3 million readings through multiple sensors and collected different readings (Temperature, humidity, light, voltage). Sensor node readings are taken as a cover object for the steganography. The experimental results of three different readings can be observed in Fig. 5.10. Plots of sensor readings and their stego readings are similar versus time (X-axis). Also, the plots of readings and extracted meter readings are similar, and there exists a strong relationship between these readings; both graphs are similar. Sensor data readings are continually transmitted through the cognitive radio network; Hence security is required to ensure the authenticity of the signal. Embedding capacity 8 bits/coefficient and 4 bits/coefficient are used of secret data, and the proposed model works efficiently in both cases. To ensure the integrity of the designed model, we have applied the BER test case to the readings after the insertion of noise. The values of $\lambda = 632.8e^{-9}$; and distance among readings $d = 0.01\%$ (meters) are considered for the Fresnelet Transform to generate the coefficients [193].

ALGORITHM 5.4: RETRIEVAL PROCESS

1. Initialize: ptr
2. Read the stego signal Stego_S'.
3. Repeat all the required steps of section 5.3.3.2 to generate the coefficients.
4. Fresnelet transform is applied on Stego_S' to obtain **Stego_coff** (coefficients which are linked with FLAG 0).
5. Traverse the entire matrix of **Stego_coff**
6. convert the **Stego_coff** into two components ($a + ib$).
7. Convert it into IEEE-754 64-bit double precision values.
8. **Secret_info** \leftarrow **Binary_value(ptr:ptr + n)**
9. Encrypted secret information \leftarrow secret_info
10. Now rearrange the rest of the bits. Now the formation of bit in stego signal to get the signal
11. **Binary value** \leftarrow ($F(1:ptr - 1), F(ptr + n: end)(\bar{0})n$)
12. Generate a floating-point number from the new Binary value, which is stored in **coeff matrix**.
13. Reconstruct the signal using **coeff matrix**.
14. Decipher the Encrypted secret information using section 3.2.2.3
15. end
16. end

5.3.4.1 Key strength Analysis

The key size should be large enough to prevent cryptanalysis attacks. If the key is known to the intruder, then the algorithm cannot protect confidentiality and authentication. In this work, the key size is also based on the IEEE 745 standard. The minimum value can be represented in 64 bit is 1.2222×10^{-10} , and it is the minimal requirement of the key of a large keyspace. ECA and 2 D chaotic maps are used, so the key is elected in floating-point number, and double

precision is represented by the 64-bit system [33] [34]. Since two values X_1 and Y_1 are considered for the key. In this case, the key size is 2^{128} . It means the key is very sensitive to the initial condition and can resist brute force attack; a small change in a key gives almost different results while deciphering the encrypted data.

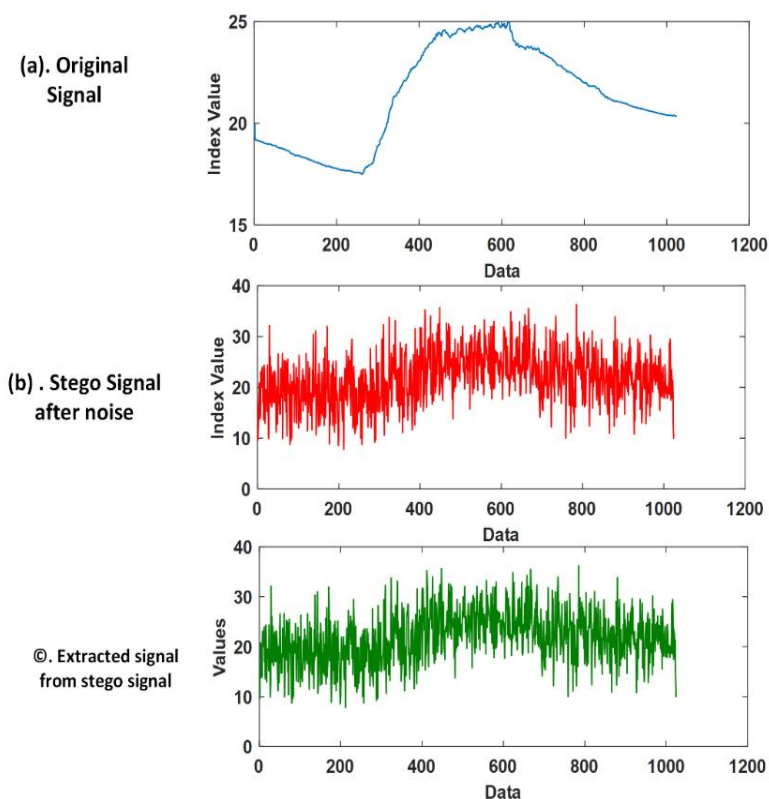


Figure 5.9 Signal behavior after adding noise

5.3.4.2 Bit Error Ratio

As we have already discussed the bit error ratio test in section 5.2.6.3, BER is used to monitor the performance in terms of integrity preservation capability of the designed system. In a battlefield environment, the opponent can alter bits for their benefit, or there is a possibility that transmitted data is altered due to noise or other environmental parameters. We have calculated BER by the proposed algorithm. BER is calculated for the mentioned scenario in section 5.2.6.3, and it is obtained to be 56%, and without noise, it has been observed 0% using equation (5.3). Therefore results indicate that the proposed system can be used to verify the integrity of the sent signal.

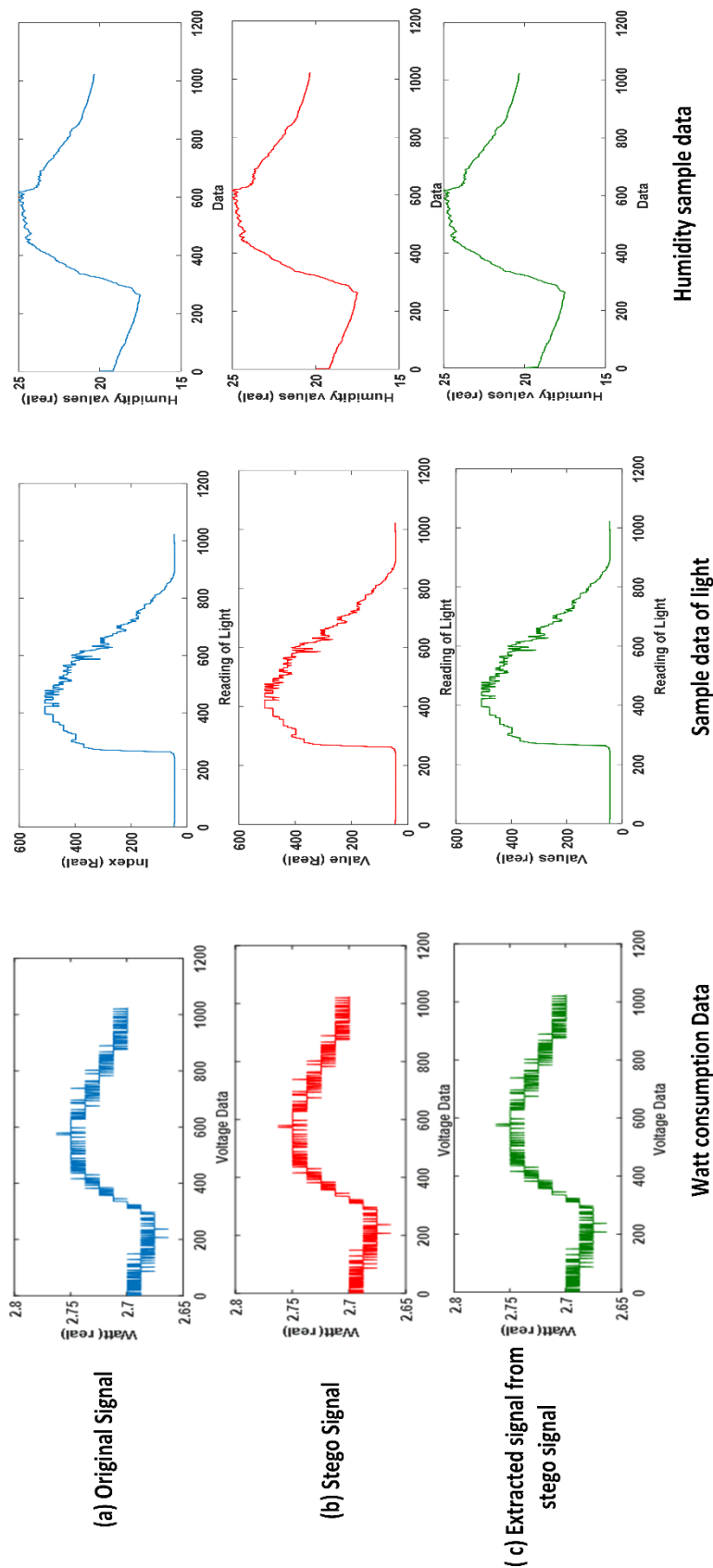


Figure 5.10 Simulation Results on Sensor Readings (Watt consumption, Light, humidity) (a). Original readings (b) Stego readings (c) Retrieved readings from stego readings

5.3.4.3 PRD Test Results

PRD test is discussed in section 5.2.6.2, and PRD test is calculated using Eq. (5.2). For the simulation, sensitive information is embedded in each coefficient in the form of either 4 bits/coefficient and 8 bits/coefficient. In both cases, the PRD, MSE, PSNR test is performed and the results of 8 bits/ coefficients are enlisted in Table 5.3, Table 5.4, Table 5.5, Table 5.6 for Temperature, humidity, light, voltage, respectively [195]. Similarly, for 4 bits/coefficient, results of PRD and MSE on different readings are enlisted in Table 5.7, Table 5.8, Table 5.9, Table 5.10 for Temperature, humidity, light, voltage, respectively PSNR values and comparison is illustrated in Fig. 5.11. It can be observed that the PRD and MSE values of different signals are obtained below zero. It is evident through the obtained values of the PRD test that the stego signal can be used directly at the server end.

Table 5.3 Test Results of Temp. Readings (Embedding capacity 8 Bits/Coff) Model 2

Temperature sample	PRD (Original Readings, Stego Readings)	PRD (Original Readings, Retrieved Readings)	MSE(Original Readings, Stego Readings)	MSE (Original Readings, Retrieved Readings)
1	0.0029	0.0001	2.23E-13	1.21E-19
2	0.0054	0.0001	3.07E-12	4.20E-19
3	0.0025	0.0000	1.32E-13	1.69E-20
4	0.0042	0.0001	1.31E-12	1.86E-19
5	0.0033	0.0001	5.09E-13	3.87E-20
6	0.0148	0.0003	4.34E-09	6.30E-16
7	0.0041	0.0001	8.72E-13	1.07E-19
8	0.0026	0.0000	1.16E-13	1.11E-20
9	0.0031	0.0003	4.42E-09	6.19E-16
10	0.0022	0.0001	5.75E-14	1.74E-20

Table 5.4 Test Results of Humidity Readings (Embedding capacity 8 Bits/Coff) Model 2

Humidity Reading	PRD (Original Readings, Stego Readings)	PRD (Original Readings, Retrieved Readings)	MSE (Original Readings, Stego Readings)	MSE (Original Readings, Retrieved Readings)
1	0.00217905	0.00004424	5.45E-13	9.31E-20
2	0.00325936	0.00011152	7.89E-12	1.28E-17
3	0.00184394	0.00004666	6.59E-13	2.90E-19
4	0.00416296	0.00007505	1.83E-11	1.98E-18
5	0.00307462	0.00004668	2.55E-12	1.29E-19
6	0.0059133	0.00044239	2.40E-13	2.40E-19
7	0.00303765	0.00005574	2.83E-12	3.18E-19
8	0.00128074	0.00004099	1.93E-13	2.24E-19
9	0.0011686	0.00002758	1.10E-13	1.10E-18
10	0.00133432	0.00003043	1.64E-13	4.25E-20

Table 5.5 Test Results of Voltage. Readings (Embedding capacity 8 Bits/Coff) Model 2

Voltage reading No sample	PRD (Original Readings, Stego Readings)	PRD (Original Readings, Retrieved Readings)	MSE (Original Readings, Stego Readings)	MSE (Original Readings, Retrieved Readings)
1	0.0035	0.0001	1.26E-16	2.23E-23
2	0.0155	0.0003	3.82E-14	6.09E-21
3	0.0029	0.0001	3.83E-17	5.39E-24
4	0.0161	0.0003	4.08E-14	4.56E-21
5	0.0038	0.0001	1.63E-16	1.36E-23
6	0.0187	0.0004	5.69E-14	7.97E-21
7	0.0035	0.0001	1.31E-16	1.71E-23
8	0.0053	0.0001	6.00E-16	9.31E-23
9	0.0213	0.0004	1.14E-13	1.15E-20
10	0.0032	0.0001	5.26E-17	2.25E-23

Table 5.6 Test Results of Light. Readings (Embedding capacity 8 Bits/Coff) Model 2

Light Reading	PRD (Original Readings, Stego Readings)	PRD (Original Readings, Retrieved Readings)	MSE (Original Readings, Stego Readings)	MSE (Original Readings, Retrieved Readings)
1	0.0025	0.0001	3.80E-09	1.74E-15
2	0.0053	0.0001	6.62E-08	8.84E-15
3	0.0028	0.0000	2.47E-09	2.40E-16
4	0.0061	0.0001	7.18E-08	8.25E-15
5	0.0046	0.0001	1.93E-09	1.43E-16
6	0.0042	0.0001	5.53E-07	8.71E-14
7	0.0017	0.0000	9.96E-08	6.11E-15
8	0.0022	0.0000	3.98E-08	3.11E-15
9	0.0052	0.0001	2.32E-08	3.86E-15
10	0.0052	0.0001	4.11E-09	3.33E-16

Table 5.7 Test Results of Temp. Readings (Embedding capacity 4 Bits/Coff) Model 2

Temperature sample	PRD (Original Readings, Stego Readings)	PRD (Original Readings, Retrieved Readings)	MSE (Original Readings, Stego Readings)	MSE (Original Readings, Retrieved Readings)
1	0.001319	0.000023	1.03E-14	9.50E-22
2	0.002708	0.000027	1.97E-13	1.90E-21
3	0.001241	0.000014	8.75E-15	1.32E-22
4	0.002028	0.000021	7.37E-14	8.45E-22
5	0.001708	0.000018	3.47E-14	3.25E-22
6	0.007197	0.000075	2.36E-10	2.87E-18
7	0.001937	0.000024	4.64E-14	1.06E-21
8	0.001213	0.000014	5.70E-15	9.09E-23
9	0.006283	0.000065	2.38E-10	2.82E-18
10	0.001106	0.000015	3.64E-15	1.12E-22

Table 5.8 Test Results of Humidity Readings (Embedding capacity 4 Bits/Coff) Model 2

Humidity Readings	PRD (Original Readings, Stego Readings)	PRD (Original Readings, Retrieved Readings)	MSE (Original Readings, Stego Readings)	MSE (Original Readings, Retrieved Readings)
1	0.00106970	0.00001581	3.20E-14	1.27E-21
2	0.00160791	0.00001665	4.67E-13	5.63E-21
3	0.00094526	0.00000921	4.65E-14	4.18E-22
4	0.00200496	0.00001953	9.85E-13	9.04E-21
5	0.00143627	0.00001411	1.23E-13	1.04E-21
6	0.00522174	0.00001810	2.23E-13	1.59 E-21
7	0.00141482	0.00001739	1.32E-13	2.93E-21
8	0.00063410	0.00000728	1.22E-14	2.04E-22
9	0.00203610	0.00002232	4.37E-13	5.96E-21
10	0.00061710	0.00000870	7.65E-15	2.78E-22

Table 5.9 Test Results of Light. Readings (Embedding capacity 4 Bits/Coff) Model 2

Light Readings	PRD (Original Readings, Stego Readings)	PRD (Original Readings, Retrieved Readings)	MSE (Original Readings, Stego Readings)	MSE (Original Readings, Retrieved Readings)
1	0.00120	0.00002	1.94E-10	8.99E-18
2	0.00263	0.00003	3.91E-09	4.10E-17
3	0.00149	0.00002	1.93E-10	2.78E-18
4	0.00295	0.00003	4.11E-09	4.08E-17
5	0.00221	0.00002	1.08E-10	1.04E-18
6	0.00204	0.00002	3.12E-08	3.92E-16
7	0.00080	0.00001	5.08E-09	6.54E-17
8	0.00110	0.00001	2.31E-09	2.82E-17
9	0.00253	0.00003	1.32E-09	1.78E-17
10	0.00133	0.00002	1.80E-11	2.12E-18

Table 5.10 Test Results of Voltage. Readings (Embedding capacity 4 Bits/Coeff) Model 2

Voltage Reading	PRD (Original Readings, Stego Readings)	PRD (Original Readings, Retrieved Readings)	MSE (Original Readings, Stego Readings)	MSE (Original Readings, Retrieved Readings)
1	0.00084	0.00004	4.37E-19	3.70E-24
2	0.00378	0.00008	1.35E-16	2.76E-23
3	0.00067	0.00002	1.12E-19	3.53E-26
4	0.00385	0.00037	1.34E-16	1.37E-20
5	0.00094	0.00002	6.11E-19	8.40E-26
6	0.00467	0.00011	2.17E-16	8.72E-23
7	0.00086	0.00002	4.67E-19	1.30E-25
8	0.00126	0.00002	1.83E-18	3.44E-25
9	0.00503	0.00010	3.43E-16	5.11E-23
10	0.00078	0.00007	1.90E-19	1.35E-23

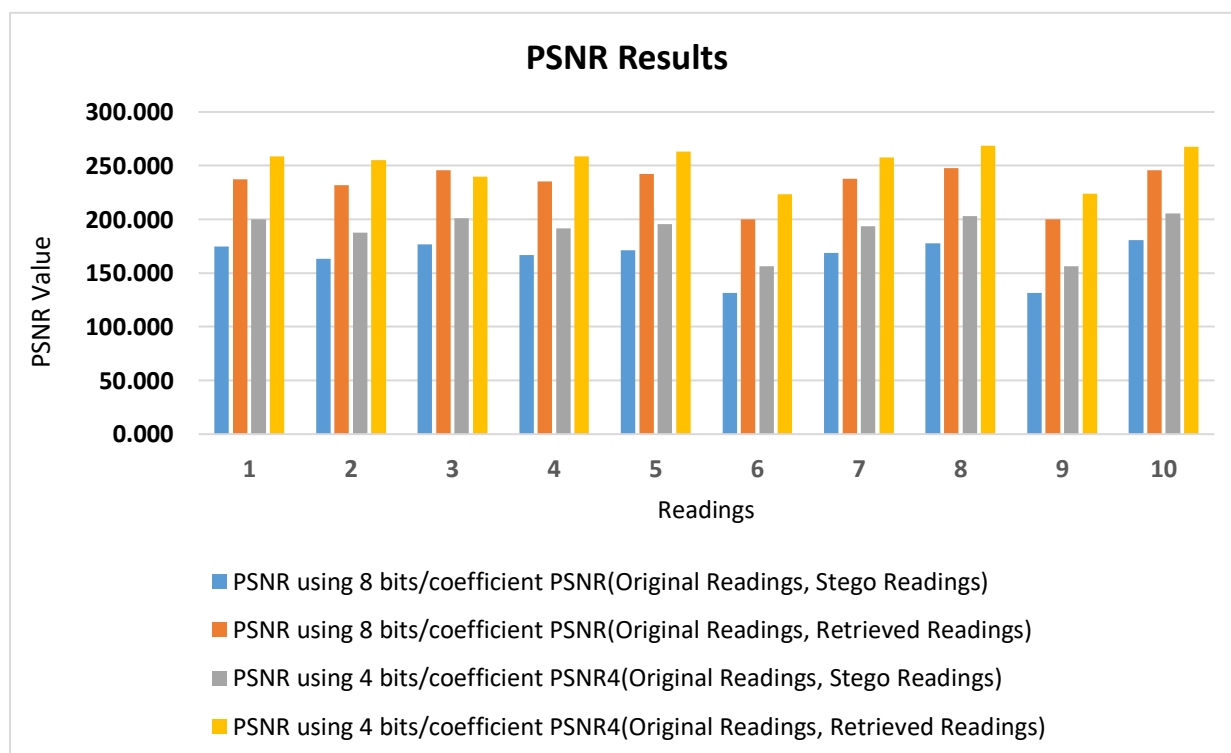


Figure 5.11 PSNR comparison (4 bits, 8bits) embedding capacity

5.4 CONCLUSION

A set of wavelet transforms are used in steganography and watermarking schemes and that is made from scratch. Wavelet transforms specially designed for the study of signal in the frequency domain. In this work, two models are implemented based on these transform to serve security services. **Model 1** discuss the issues and solutions in the smart grid system, the proposed algorithm has been implemented on different collected readings through smart meters, and it is observed that normal readings and stego readings are closely similar with a negligible difference. Retrieval of confidential information is linear and secure. The proposed algorithm also obtains integrity preservation of smart meter readings. Therefore, manipulation of sensor and meter readings is not possible for an intruder. Hence, stego readings can be used directly by the operational center because the PRD value is almost negligible.

Model 2 discuss the IoMT issues, and it is addressed by another promising approach using the Fresnelet transform and ECA. The battlefield is being digitalized with the advancement of technology. The security organization of many countries is establishing new rules and policies for the war zone. Having said that, Communication networks are deploying in the war zone along with the heavy vehicles and arm forces. In the proposed algorithm (Model 2), readings, which are collected by the cognitive radio networks, are used as a cover object and we have concealed eight and four bits into the coefficients and MSE, PSNR, and PRD tests are performed to evaluate the performance of the system. It is also treated in a different manner as it could be game-changing information. This work (Model 1 and Model 2) evaluates PRD between original readings and retrieved readings and PRD between original readings and stego readings. PRD values thus obtained for the signals are less than 0.00000001% (when four bits are embedded). It means that the retrieved signal and stego signal contains all the details of the original signal. Experimental results demonstrate that the proposed algorithm is suitable and reliable for the real-time environment.

CHAPTER 6

Integrity Preservation in Academics

6.1 BACKGROUND AND AIMS

Exams are the crucial phase in every academic institute, and it also takes place in a competitive exam where many candidates enroll themselves to get a job or admission [196]–[199], and it is conducted at an immense scale. In this chapter, we have designed two algorithms. The first algorithm generates an automatic sitting arrangement plan for examination halls to prevent mismanagement, prohibited material, and cheating during examinations. The second algorithm deals with Henon chaotic map to rescheduled the sitting plan. It is based on the sitting allocation methodology to generate random allocation in classrooms for every exam to prevent cheating from their surrounding locations. To preserve academic integrity, it is essential to decrease the possibility of cheating in the examination hall. The maximum utilization of classrooms and less human resources are the main objectives of the proposed algorithms. Proposed work has been applied to university, and it gives a better environment during examination with less human resource in a less executable time rather than a manual sitting plan allocation method.

Examinations are an essential part of colleges, universities and academic institutes, where students go through many stages of evaluation schemes for better assessment. An exam hall's organized structure with a proper sitting arrangement of students leads the implementation process of examination. In order to write exams in the given time frame, it is necessary to adjust the students in the classroom along with efficient management. To conduct an examination, the exam controller takes in charge of all the responsibilities related to exams [200]. Arrangements of desks in a classroom most often are fixed, and they cannot be transferred from

the place, which leads to an administrator or exam controller for the students have to take concrete steps to the seating arrangement of seats in each classroom. Before the examination, the sitting plan of every classroom is generated and is also shared with students. When the student finds the right place for his sitting according to the sitting plan, then for each exam, the student has to sit in the same place that was already designated during the examination. Invigilators are sent by the authority in classrooms to monitor students and also for conducting exams successfully. In a classroom, during the examination, its corresponding attendance sheet is also essential to calculate the total number of present students and absentees to maintain students' records. Exam sheets are collected in the end and it also verified with the attendance sheet as shown in Fig. 6.1.

Exam seating allocation algorithm is required to accommodate students in such a way that all the students of different disciplines can write their exams efficiently without any interruptions[201], [202]. Many institutes do not use algorithms or techniques to generate a seating allocation plan; it is based on some basic rules, number of students, size of classrooms, number of disciplines in the institute, time-slots and types of examinations. A cooperative seating arrangement can trouble the invigilators, and there are more chances for students to copy content from their neighbor's exam sheet. Generally, in many institutes, Seats are allocated to students in a traditional approach with some facile rules, which increases the cost and time to get a feasible solution. Fraudulent behavior such as cheating in examinations can hamper the efforts of many students; it is the Machiavellian behavior of students, which is being increased with technology and the rapid growth of the Internet.

There are possibilities of error in manual approach which are like, few seats are left empty, overlapping of seats between students, no seat is allocated to students, and there is also the fear that two adjacent students are writing the same paper. Having said that, question papers are distributed to students and increases the sore difficulties of invigilators and make a complex system. Positive academic behavior is developed with a proper sitting plan during the examination and even in classrooms during theory lectures to maintain discipline [203]. This chapter has designed two algorithms to preserve academic integrity; the first algorithm generates an automatic sitting arrangement plan for examination halls to prevent prohibited material and cheating during examinations. The second algorithm deals with Henon chaotic map; It is associated with the sitting plan to generate random allocation in classrooms for every exam to prevent cheating from their surrounding locations. To conduct the examination in the

institute, sitting plan, along with its corresponding attendance for better monitoring, is required. Cheating is a common phenomenon in human nature, which is also replicated in academics because of a few students. Cheating can be done in various ways, which are mentioned below:

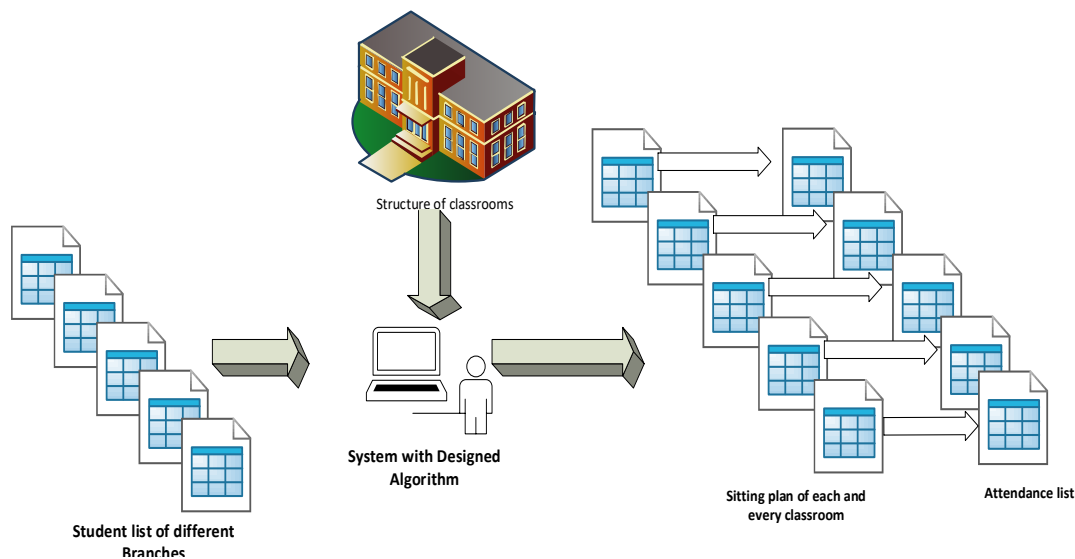


Figure 6.1 The proposed architecture of sitting plan algorithm

- To answer the exam questions, copying content from the adjacent student's answer sheet from the same discipline in the examination hall.
- Cheating is also done through state-of-the-art technology.
- Once a student knows his sitting position in the examination hall, then there is a possibility that a student may write answers or text on the desk for the next upcoming exam and may hide exams related materials.

6.2 PROPOSED ALGORITHM

In many institutes, a sitting allocation plan is designed by members of exam cell or by the exam controller, and it is required to have a large number of human resources to create an environment to generate a proper sitting plan. Many meetings of faculties with board members are placed before the examination to facilitate students for a proper atmosphere to write their exams. In order to reduce the enormous load, this chapter introduces two algorithms. The student database is considered as input for the proposed algorithms. The first algorithm deals

with the allocation of seats in classrooms with a detailed attendance sheet of students of every classroom, whereas the second algorithm is designed to generate a random sitting plan to prevent unethical things during the examination. Fig. 6.2 demonstrates the proposed algorithm, where different discipline participates in the examination process.

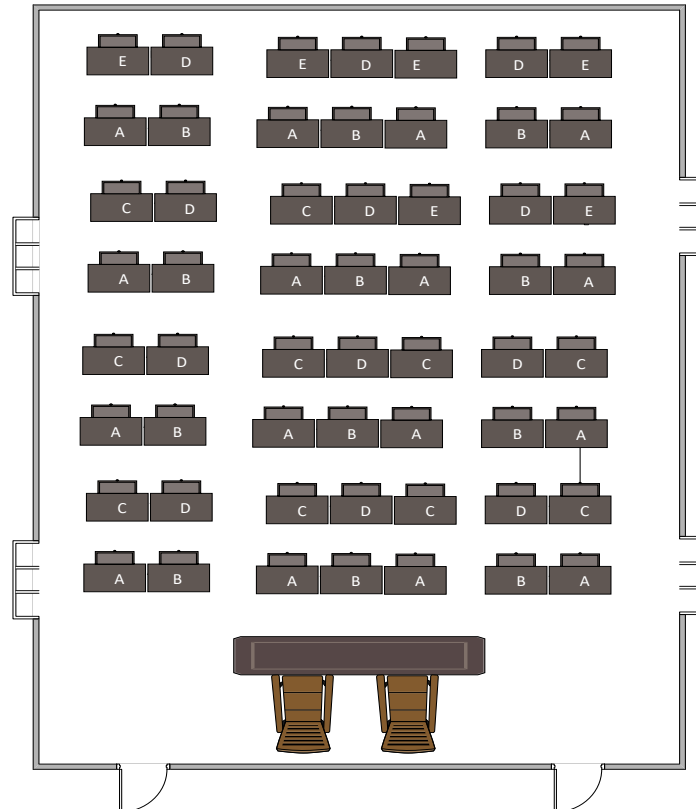


Figure 6.2 Proposed seating plan for examination hall.

6.2.1 ADAPTIVE SITTING ALLOCATION ALGORITHM

The education system also has an essential contribution to any country's economic growth and the education system helps students to gain knowledge. Examination is required for better assessment of students; through this, the foundation of the students' future is laid. Various disciplines of institute participate in the examination process simultaneously. At the initial stage, several registered students who will appear in the exam are identified and count number of students in each discipline. The second input for this algorithm is based on classrooms, where two parameters are taken: the size of classrooms and number of classrooms. The size of the examination hall defines how many students can be accommodated for the examination.

Generally, examination halls consist of tables which are arranged in a row-column fashion. The maximum utilization of examination halls is one of the primary objectives of the proposed algorithm.

6.2.1.1

Initially, a student list is prepared by the system and roll numbers are extracted and are stored in an array. It is also dependent on the number of disciplines n . It is also found by the system administrator in which column roll numbers of students are written in the file. The number of students in every discipline may be the same or may not be the same, so column size is taken maximum into account for the driven approach.

Pseudocode of step 6.2.1.1
<ol style="list-style-type: none"> 1. for $i \leftarrow 1$ to n do 2. filename \leftarrow file(i).xlsx 3. [num, text(i)] \leftarrow xlsread (filename, size) 4. extracted only roll numbers from the list by specified that column 5. $m(i) \leftarrow$ size(text(i)); 6. end for

6.2.1.2

Roll numbers of each branch are stored in a separate list, and the number of students of different disciplines is counted. For maximum utilization of classrooms or examination halls, student data lists are equally divided into four parts. An administrator finalizes four different lists with the manual and automatic approaches. Therefore, the creation of these four lists entirely depends upon the examination controller. In two ways, allotment can proceed further. The total number of students is counted by using the following equation.

$$M = \sum_{i=1}^n m_{(i)} \tag{6.1}$$

Where M represents the total number of students in the institute.

6.2.1.2.1 Automatically System Generated List

In this approach, the system works itself to divide the total number of students list into four equal parts, and processed lists are further used as input for step 3.

Pseudocode of step 6.2.1.2.1

```

1. total = 0
2. text = emptylist
3. for i = 1: n do
4. text ← text + text(i)
5. total ← total + m(i)
6. end for
7. d ← total/4;
8. rem ← total%4
9. list1 = text(1 : d)
10. list2 = text(d + 1 : 2d)
11. list3 = text(2d + 1 : 3d)
12. list4 = text(3d + 1 : 4d + rem)

```

6.2.1.2.2 Manual Approach to Generate a List

In this approach, lists are prepared by a member of the examination cell. Manually, we have taken four lists to allocate students in examination halls. Various disciplines enrolled and wrote their exams. So, it is considered that students of the same discipline can be found at a nearby location. For example, A, B, C, D, E, F, G are different disciplines, and the lists are created in such a way that there is not much difference in the size of the list or, ideally, the number of students in the list should be equal.

$$list1 = A + G$$

$$list2 = B + H$$

$$list3 = C + E$$

$$list4 = D$$

Pseudocode for step 6.2.1.3.

```

Initialize: ptr1=1, ptr2=1, ptr3=1, ptr4=1
for i ← 1: total number of rows
  for j ← 1: N
    if (i and j both variables are not divisible by 2)
      if (ptr1 ≤ size of list1)
        c (i, j) ← list1(ptr1,1)
        ptr1=ptr1+1;
      else
        c (i, j) ← seat is empty
      end

    else if (i is not divisible by 2 and j is divisible by 2)
      if (ptr2 ≤ size of list2)
        c (i, j) ← list2(ptr2,1)
        ptr2=ptr2+1;
      else
        c (i, j) ← seat is empty
      end

    else if (i is divisible by 2 and j is not divisible 2)
      if (ptr3 ≤ size of list1)
        c (i, j) ← list3(ptr3,1)
        ptr1=ptr3+1;
      else
        c (i, j) ← seat is empty
      end

    else (i and j are divisible by 2)
      if (ptr4 ≤ size of list4)
        c (i, j) ← list4(ptr4,1)
        ptr4=ptr4+1;
      else
        c (i, j) ← seat is empty
      end
    end
  end
end
end
end

```

6.2.1.3

Classroom's structure is constructed in a row, column fashion. In which the position of desks is fixed, and it is assumed that a table or desk will not be moved from one classroom to another classroom. The classroom is taken as a matrix, and it is also found that how many classes have the same number of columns, those classes are put together in which the number of columns are the same and treated as a single classroom. Let us consider, the class1 dimension is $M1 \times N$ and class2 dimension is $M2 \times N$, then these two classrooms can be merge and can be treated as a single classroom having the strength to accommodate student will be $(M1 \times M2) \times N$. similar mechanism is followed with other classrooms.

6.2.1.4

In this section, 6.2.1.3. is repeated until all the classrooms of the institute are covered. A sitting plan which is generated by step 6.2.1.3. is divided into a separate and individual sitting plan for every classroom. Attendance lists of classrooms are also generated itself by the proposed algorithm on the basis of the sitting plan.

6.2.2 RANDOM SITTING ALLOCATION USING HENON CHAOTIC MAP

Henon chaotic map is introduced in sitting allocation methodology to provide a random sitting allocation for every examination hall. Sometimes students write the relevant content of the next exam on a desk or table and enclosure walls; it helps them to copy content from the table or desk to their answer sheets. One more way that once a student knows his location as per the sitting plan, a student may hide notes or books near to their surrounding location. Subsequently, for a legitimate reason, students come out from the examination hall. Meanwhile, the student receives answers from the hidden material. Chaotic maps are widely used in various fields of science; therefore, different chaotic maps are also associated with chaos theory. Chaotic maps are mainly used to generate pseudorandom numbers and can be used as per research requirements [204].

- (a) Henon chaotic map described in chapter 2.2.3 is used to generate the pseudo-random numbers using equations (2.2), (2.4)
- (b) In the adaptive sitting allocation algorithm, four lists were generated in two ways. Here, the size of each list is taken for further approach. This sequence is converted into

$[1, size(list)]$ using modular arithmetic, as shown in Fig. 6.3.

- (c) Now, the Random sequence is used to shuffle the roll numbers of a student's list; the pseudorandom sequence is used to rearrange the list by its indexing position with a new index position using the $Newx []$ matrix. Later this shuffled list is utilized to regenerate the new sitting plan. The detailed procedure to generate the pseudo-random numbers (frequency count of numbers in list = 1)

Pseudocode for 6.2.2

1. **while until all the list are covered do**
2. $X \in \{-I, I\}$ Where I is an integer
3. $Newx \leftarrow floorsizeoflist(i) \times X$
4. $Newx \leftarrow mod(Newx, size\ of\ list(i))$
5. Remove all duplicate numbers from and replaced by those numbers which are having zero frequency.
6. Remove duplicate numbers from the sequence $Newx[]$ and replace those numbers with 0 frequency count in the sequence list, as shown in Fig. 4.
7. **end while**

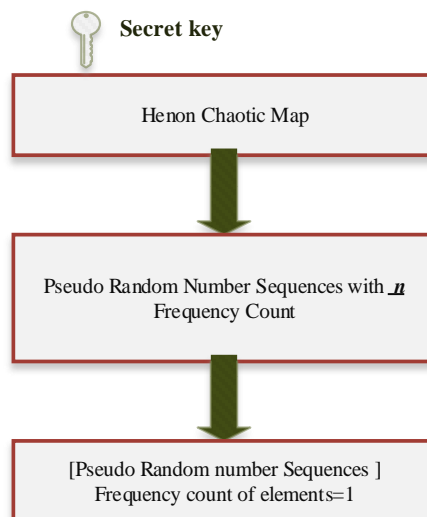


Figure 6.3 Pseudorandom numbers generation using Henon chaotic map

6.3 EXPERIMENTAL RESULTS AND DISCUSSION

The sitting plan is prepared by locating the number of students in the examination hall. Generally, when the individuals of the institutes do this work, it takes a lot of time and resources. In order to reduce the complexity of the system and prevent unethical practices, this paper helps in many ways. The proposed algorithm gives impressive results, and when the algorithm is implemented and tested, the drawbacks that were found in the traditional approaches seem to be removed away through this proposed algorithm. In this section, the experimental results of the proposed algorithm are given to appreciate the efficiency of the proposed security system. MATLAB 7.9 software with 8 GB RAM is used to implement the proposed algorithm along with the use of a Microsoft Excel worksheet for reading and writing operations. The proposed algorithm generates Table 6.1 and Table 6.2, and it shows that the proposed algorithm works appropriately without any overlapping or underlapping problem and also reduces the cost of the prior implemented system. Henon chaotic map plays an important role in generating a new sitting plan for every exam, which helps the institute to prevent cheating and misconduct of students.

6.4 CONCLUSION AND FUTURE WORK

Cheating is a common practice among students, and their human behavior brings it. Academic institutes cannot stop the trend of imitating the students completely, but by creating an improved environment, an ideal education system can be prepared. The sitting plan gives proper management for conducting the examination process. A system with MATLAB and Microsoft excel worksheet is enough to generate a sitting plan; it takes a few seconds instead of taking several weeks. The education system is the backbone of any country, and many academic institutions are working to make it strong in this direction. If an institute governs a healthy examination process, then by the results obtained, many steps can be taken to improve the education system, and this is only possible by the cooperation of teachers and students. Institute for upcoming exams can train those students who could not get a good result in an examination. The Henon chaotic map has been used to generate a random sittings plan to prevent cheating during the examination; it helps invigilators and also students for better assessment. It is possible that this input could be taken automatically by the system itself for the maximum utilization of examination halls.

Table 6.1 Attendance Sheet for Classroom A

ATTENDANCE SHEET											
ROOM NO: HALL-01											
CO	BOOK LET NO.	SIGN ATUR E	ME	BOO K. NO.	SIG NAT URE	EE	BOO K. NO.	SIGNA TURE	EC	BOOKL ET NO.	SIGNAT URE
CO/01			ME/01			EE/01			EC/01		
CO/02			ME/02			EE/02			EC/02		
CO/03			ME/03			EE/03			EC/03		
CO/04			ME/04			EE/04			EC/04		
CO/05			ME/05			EE/05			EC/05		
CO/06			ME/06			EE/06			EC/06		
CO/07			ME/07			EE/07			EC/07		
CO/08			ME/08			EE/08			EC/08		
CO/09			ME/09			EE/09			EC/09		
CO/10			ME/10								
CO/11			ME/11								
CO/12			ME/12								

Table 6.2 Sitting Plan for Classroom A

ROOM NO. HALL -01											
CO/01	EE/01		CO/02	EE/02		CO/03	EE/03		CO/04		
ME/01	EC/01		ME/02	EC/02		ME/03	EC/03		ME/04		
CO/05	EE/04		CO/06	EE/05		CO/07	EE/06		CO/08		
ME/05	EC/04		ME/06	EC/05		ME/07	EC/06		ME/08		
CO/09	EE/07		CO/10	EE/08		CO/11	EE/09		CO/12		
ME/09	EC/07		ME/11	EC/08		ME/11	EC/09		ME/12		
CO/01- CO/12 =12						ME/01-ME/12=12					
EE/01 -EE/09= 09						EC/01- EC/09=09					
TOTAL= 42											

CHAPTER 7

Conclusion and Future Work

This thesis work has a prime focus on security services and their mechanisms. Schemes for privacy and protection of information are devised for more enhanced results and optimum performance in the field of cryptography. The formulation of algorithms presented in this thesis contributes to better research of images and sensors that are used in multiple fields like satellite imaging, medical analysis, biometrics, astronomy, military surveillance, and many more. These techniques are also compared with the state of art algorithms. Before constructing the thesis, we have studied and investigated the available existing methods and then developed algorithms to serve many purposes, and all the algorithms present in this work performed well. Simulation results show that algorithms are efficient and robust and these algorithms can be applied in real-time applications to solve security issues.

7.1 SUMMARY OF THE WORK

Based on all the chapters included in this thesis, it can be said that security is not related to one specific area, but security has an essential role in all digital areas, and securing the smooth operation of information is an important and challenging task for each sector. To achieve security primitives, we have studied traditional cryptosystems and proposed mechanisms for digital communication systems, wireless sensor networks, and academic institutes to ensure a variety of security services. We recapitulate the features of this investigation and the results obtained by proposed encipherment techniques in the following points: -

1. To hybridize the existing encryption techniques with dynamic systems to obtain a

better encryption technique, we have designed algorithms using electromagnetic rotor machine and cellular automata theory along with chaos theory. These algorithms can be implemented with the minimum support of hardware and software requirements. Besides, speech is also merged with cryptography to provide authentication to the communication system.

- (a) One dimensional elementary cellular automaton (ECA) has been combined with a chaotic map to produce unprecedented results in the field of cryptography. A novel approach of keyed transposition cipher is applied to digital images to produce a shuffled image with the help of the Hénon chaotic map; then, the shuffled image becomes the input for the diffusion process. State attractors for rule space are also investigated and analyzed for the lookup encryption scheme. Since ECA is popular due to its implementation process, i.e., it takes minimum time to implement either on software or hardware platforms and also it can save device power consumption.
 - (b) A novel group-based cryptosystem based on an electromagnetic rotor machine is implemented for the digital images. The algorithm is aimed to make a cryptosystem for gray-level images based on voice features, secret sharing scheme and electromagnetic rotor machine. Here, Shamir's secret sharing (k, n) threshold scheme is used to secure a key along with the voice features of $(n - k)$ users. The proposed cryptosystem is highly secure and fast. In this section, the enigma machine is designed for images using a chaotic system.
2. We derived the solutions for image confidentiality based on the amount of input data within an image. Proposed algorithms are tested on gray and color images as well. These algorithms are listed below:
- (a) Model 1 : Selective color image encryption using Henon chaotic system with a keyless substitution cipher (spatial domain).
 - (b) Model 2: DWT based selective image encryption scheme (frequency domain).

A selective image encryption technique achieves a lightweight encryption scheme. In the proposed work, only a significant part of the original image is encrypted. Detection of a significant part in the spatial domain as well as in the frequency domain is calculated by an

object segmentation image processing technique and wavelet function, respectively. When a significant part of an image is encrypted instead of the full image, it reduces the computational cost and can be operated in limited memory space. There are advantages of the proposed image encryption schemes, which are discussed below:

- In a chaos-based cryptosystem, pseudorandom numbers are generated as per the size of an image. Therefore, the number of iterations increases to produce the key sequence as compared to the proposed selective image encryption schemes. A minimum number of bits are required for encryption. Hence, the computational cost of encryption is decreased.
 - Model 2(a) can be used in two ways depending upon the user's requirements, whether the sender wants to send an encrypted ROI image along with foreground details or choose to send only the ROI encrypted part of an image.
 - The proposed algorithms are useful, and it has real-time applications to encrypt a large size of data in order to fulfill all the aspects of security. Various tests are also performed to evaluate the efficiency of the proposed algorithms, and the results of tests show that the proposed algorithms have an ample amount of substantial-quality to protect the information in a reliable manner and can resist all types of brute force attacks.
3. Internet of things (IoT) devices plays an important role in transmitting collected data of devices and sensitive information of the users through the public network. Therefore, the confidentiality of information and integrity protection of periodically collected data is required for better assessment. Chapter 5 presents novel steganography techniques based on the transforms and chaotic map to achieve integrity and authentication. Periodically collected readings and sensor data are used as a cover object for hiding information. Stego readings are constructed with negligible distortion in original readings. We developed the algorithms with a simple structure and intuitive nature, which are more practical for real-time applications. Proposed algorithms are designed for smart devices as per the need of the organizations and possible threats in such environment. Two models are discussed in chapter 5, which are as follows :
1. Steganography technique to secure information and integrity preservation of smart grid readings using wavelet.

2. Internet of Battlefield things Security: A Strategy to Secure Sensitive Information using Reversible Steganography Scheme.

Chapter 6 address the issues of academic institutes and discuss the fraudulent behavior of students during examination. We have developed a system based on the proposed algorithms. The system is found reliable, robust, and efficient in terms of security aspects. The proposed work can be applied to institutes to reduce human resources, and it is able to generate a sitting plan in a quick manner.

7.2 CONTRIBUTIONS AND FUTURE WORK

Images and sensor data are vital sources of information, which are communicated through the public network. Image encryption techniques and privacy protection of IoT are among the dominant class of modern cryptography. The contributions made by this thesis work are:

The thesis addresses the fundamental component of cryptography to understand the terminology of cryptography. It gives the idea of chaos theory in cryptography, and comparative analysis and study of chaos theory help to understand the usage of chaos theory in cryptography.

1. We devised the algorithms for privacy protection with potent encryption schemes. These schemes are utilitarian in the digital channels. Since the algorithms are based on a simple structure and intuitive nature that are more practical for real-time applications, therefore, the implementation of algorithms can be served to gain ideal results. Besides, the proposed algorithms can be modified according to security requirements.
2. The proposed algorithms are robust in nature and capable of handling even the maximum amount of information as input and can deal with it by preserving the basic structure of the input.
3. We have designed algorithms using dynamic systems, which aids in low computational complexity and is easy to implement in hardware and software.

Since algorithms are developed in this work for images and sensor data using dynamic systems to obtain confidentiality, it can be expanded for other security services along with the cryptanalysis study. The work has explored the utility of chaos theory for ideal cryptosystems, but in the future other effective alternatives can be explored for cryptosystems. The extensive approaches of the proposed algorithms can also be tested in different environments on different kinds of multimedia. A detailed study can be done on chaos theory and cellular automata to extract more properties that can be applied to image processing and encryption schemes. Key generation, digital signature with chaos theory can be investigated. At last, security is the continuous process to make systems resistible against attacks, so mechanisms can be designed according to the situation and updated. Steganalysis can be done on the existing techniques and can develop novel algorithms according to the study. Several chaotic maps are available in a dynamic system. We can also exploit chaotic maps in the field of cryptography. Proposed algorithms are applied to color and gray images; other color models can be used to input the proposed algorithms.

The proposed encryption techniques can improve various aspects of cryptosystems, such as increasing efficiency, computational complexity, and security.

- Future research can be conducted to exploit the proposed pseudo-random number generator in security systems and applications to increase randomness and provide high-level security.
- Since prime numbers are used at a wide scale in public-key cryptography scheme, so based on the study of algorithms, prime number generator can be designed in the future.
- In this thesis, the proposed work is based on symmetric-key cryptography. This work can be extended further for asymmetric key cryptography.
- Henon chaotic system is not the only chaotic system that is dynamic. Other chaotic systems are also available, which could be used in cryptography.
- To understand the complex behavior of chaotic maps, the Lyapunov exponent can be calculated that can help to establish the novel chaotic systems.

REFERENCES

- [1] A. Kumar and N. S. Raghava, “Selective colour image encryption using Hénon chaotic system with a keyless substitution cipher,” *Eng. Appl. Sci. Res.*, vol. 47, no. 1, pp. 66–76, 2020.
- [2] C. P. Pfleeger, *Security in computing*. Pearson Education India, 2009.
- [3] J. H. P. Eloff and M. M. Eloff, “Information security architecture,” *Comput. Fraud Secur.*, vol. 2005, no. 11, pp. 10–16, 2005.
- [4] A. J. A. Wang, “Information security models and metrics,” in *Proceedings of the 43rd annual Southeast regional conference-Volume 2*, 2005, pp. 178–184.
- [5] P. Himanen, *The hacker ethic*. Random House, 2010.
- [6] W. V. Maconachy, C. D. Schou, D. Ragsdale, and D. Welch, “A model for information assurance: An integrated approach,” in *Proceedings of the 2001 IEEE workshop on information assurance and security*, 2001, vol. 310, pp. 5–6.
- [7] B. Cambou, P. G. Flikkema, J. Palmer, D. Telesca, and C. Philabaum, “Can ternary computing improve information assurance?,” *Cryptography*, vol. 2, no. 1, p. 6, 2018.
- [8] M. E. Whitman and H. J. Mattord, *Principles of information security*. Cengage Learning, 2011.
- [9] O. Mozhaev, H. Kuchuk, N. Kuchuk, M. Mozhaev, and M. Lohvynenko, “Multiservice network security metric,” in *2017 2nd International Conference on Advanced Information and Communication Technologies (AICT)*, 2017, pp. 133–136.
- [10] H. Lin, Z. Yan, Y. Chen, and L. Zhang, “A survey on network security-related data collection technologies,” *IEEE Access*, vol. 6, pp. 18345–18365, 2018.
- [11] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, “An evaluation framework for network security visualizations,” *Comput. Secur.*, vol. 84, pp. 70–92, 2019.
- [12] B. Padrtova, “Frozen narratives: How media present security in the Arctic,” *Polar Sci.*, vol. 21, pp. 37–46, 2019.

-
- [13] A. R. McGee, U. Chandrashekhar, and S. H. Richman, "Using ITU-T X.805 for comprehensive network security assessment and planning," *11th International Telecommunications Network Strategy and Planning Symposium. NETWORKS 2004*, IEEE, 2004.
- [14] M. A. S. Santos, A. Ranjbar, G. Biczók, B. Martini, and F. Paolucci, "Security requirements for multi-operator virtualized network and service orchestration for 5G," in *Guide to Security in SDN and NFV*, Springer, 2017, pp. 253–272.
- [15] S. Abidin, V. R. Vadi, and A. Rana, "On Confidentiality, Integrity, Authenticity, and Freshness (CIAF) in WSN," in *Advances in Computer, Communication and Computational Sciences*, Springer, 2020, pp. 87–97.
- [16] O. Ur-Rehman and N. Zivic, *Security in Autonomous Driving*. Walter de Gruyter GmbH & Co KG, 2020.
- [17] T. Roosta, S. Shieh, and S. Sastry, "Taxonomy of security attacks in sensor networks and countermeasures," in *The first IEEE international conference on system integration and reliability improvements*, 2006, vol. 25, p. 94.
- [18] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, 2017, pp. 32–37.
- [19] N. S. Raghava, A. Kumar, A. Deep, and A. Chahal, "Improved LSB method for Image Steganography using Hénon Chaotic Map," *Open J. Inf. Secur. Appl.*, vol. 2014, no. 1, pp. 34–42, 2014.
- [20] J. Ning, J. Xu, K. Liang, F. Zhang, and E.-C. Chang, "Passive attacks against searchable encryption," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 3, pp. 789–802, 2018.
- [21] M. E. Aminanto and K. Kim, "Detecting active attacks in Wi-Fi network by semi-supervised deep learning," in *Conference on Information Security and Cryptography 2017 Winter*, 2016.
- [22] F. Shahzad, M. Pasha, and A. Ahmad, "A survey of active attacks on wireless sensor networks and their countermeasures," *arXiv Prepr. arXiv1702.07136*, 2017.
- [23] S. Alabady, "Design and Implementation of a Network Security Model for Cooperative

- Network.,” *Int. Arab. J. e Technol.*, vol. 1, no. 2, pp. 26–36, 2009.
- [24] A. Shifa, M. N. Asghar, and M. Fleury, “Multimedia security perspectives in IoT,” in *2016 Sixth International Conference on Innovative Computing Technology (INTECH)*, 2016, pp. 550–555.
- [25] F. Y. Shih, *Multimedia security: watermarking, steganography, and forensics*. CRC Press, 2017.
- [26] X. Liu and A. M. Eskicioglu, “Selective encryption of multimedia content in distribution networks: Challenges and new directions,” *IASTED Commun. Internet Inf. Technol. (CIIT), USA*, 2003.
- [27] A. McAndrew, “Introduction to Cryptography with Open-Source Software.” CRC Press, 2016.
- [28] W. Diffie and M. Hellman, “New directions in cryptography,” *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, 1976.
- [29] J. F. Dooley, “Cipher Mysteries,” *History of Cryptography and Cryptanalysis*. Springer International Publishing, pp. 263–292, 2018.
- [30] D. V. V. Deepthi, B. H. Benny, and K. Sreenu, “Various Ciphers in Classical Cryptography,” in *Journal of Physics: Conference Series*, 2019, vol. 1228, no. 1, p. 12014.
- [31] J. Y. AbuEl-Reesh and S. S. Abu-Naser, “An Intelligent Tutoring System for Learning Classical Cryptography Algorithms (CCAITS),” 2018.
- [32] K. Goyal and S. Kinger, “Modified caesar cipher for better security enhancement,” *Int. J. Comput. Appl.*, vol. 73, no. 3, pp. 975–8887, 2013.
- [33] L. Krikor, S. Baba, T. Arif, and Z. Shaaban, “Image encryption using DCT and stream cipher,” *Eur. J. Sci. Res.*, vol. 32, no. 1, pp. 47–57, 2009.
- [34] C. Sanchez-Avila and R. Sanchez-Reillo, “The Rijndael block cipher (AES proposal) : a comparison with DES,” *Proceedings IEEE 35th Annual 2001 International Carnahan Conference on Security Technology (Cat. No.01CH37186)*. IEEE, 2001.
- [35] H. Elkamchouchi and A. M. Elshafee, “REBC2, Rotor Enhanced Block Cipher 2,” *2007 National Radio Science Conference*. IEEE, 2007.

-
- [36] D. Puthal, S. Nepal, R. Ranjan, and J. Chen, "A dynamic prime number based efficient security mechanism for big sensing data streams," *J. Comput. Syst. Sci.*, vol. 83, no. 1, pp. 22–42, 2017.
- [37] D. Boneh and G. Durfee, "Cryptanalysis of RSA with private key d less than $N^{\sup 0.292}$," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1339–1349, 2000.
- [38] A. Faquih, P. Kadam, and Z. Saquib, "Cryptographic techniques for wireless sensor networks: A survey," in *2015 IEEE bombay section symposium (IBSS)*, 2015, pp. 1–6.
- [39] 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.
- [40] K. Wang, Pei, L. Zou, A. Song, and Z. He, "On the security of 3D Cat map based symmetric image encryption scheme," *Phys. Lett. A*, vol. 343, no. 6, pp. 432–439, 2005.
- [41] S. D. Rihan, A. Khalid, and S. E. F. Osman, "A performance comparison of encryption algorithms AES and DES," *Int. J. Eng. Res. Technol.*, vol. 4, no. 12, pp. 151–154, 2015.
- [42] Y. Zhang, "Test and Verification of AES Used for Image Encryption," *3D Res.*, vol. 9, no. 1, 2018.
- [43] C. Chen, T. Wang, Y. Kou, X. Chen, and X. Li, "Improvement of trace-driven I-Cache timing attack on the RSA algorithm," *J. Syst. Softw.*, vol. 86, no. 1, pp. 100–107, 2013.
- [44] D. Coppersmith, "The Data Encryption Standard (DES) and its strength against attacks," *IBM J. Res. Dev.*, vol. 38, no. 3, pp. 243–250, 1994.
- [45] N. K. Sreelaja and G. A. V. Pai, "Stream cipher for binary image encryption using Ant Colony Optimization based key generation," *Appl. Soft Comput.*, vol. 12, no. 9, pp. 2879–2895, 2012.
- [46] M. J. Aqel, Z. A. Alqadi, and I. M. El Emary, "Analysis of stream cipher security algorithm," *J. Inf. Comput. Sci.*, vol. 2, no. 4, pp. 288–298, 2007.
- [47] "An Efficient Image Encryption Technique using Chaotic Logistic Map and RC4 Stream Cipher," *Int. J. Mod. Trends Eng. Res.*, vol. 3, no. 9, pp. 213–218, 2016.
- [48] H. Feistel, "Block cipher cryptographic system." Google Patents, 19-Mar-1974.
- [49] S. M. Matyas *et al.*, "Public key cryptosystem key management based on control
-

- vectors.” Google Patents, 06-Apr-1993.
- [50] L. Kocarev, “Chaos-based cryptography: a brief overview,” *IEEE Circuits Syst. Mag.*, vol. 1, no. 3, pp. 6–21, 2001.
- [51] Y. Li, C. Wang, and H. Chen, “A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation,” *Opt. Lasers Eng.*, vol. 90, pp. 238–246, 2017.
- [52] J. De Dieu Nkapkop, J. Y. Effa, A. Toma, F. Cociota, and M. Borda, “Chaos-based image encryption using the RSA keys management for an efficient web communication,” *2016 12th IEEE International Symposium on Electronics and Telecommunications (ISETC)*. IEEE, 2016.
- [53] D. Wang, J. Ming, T. Chen, X. Zhang, and C. Wang, “Cracking IoT device user account via brute-force attack to SMS authentication code,” in *Proceedings of the First Workshop on Radical and Experiential Security*, 2018, pp. 57–60.
- [54] E. Biham and A. Shamir, “Differential cryptanalysis of DES-like cryptosystems,” *J. Cryptol.*, vol. 4, no. 1, pp. 3–72, 1991.
- [55] A. A. Abdo, S. Lian, I. A. Ismail, M. Amin, and H. Diab, “A cryptosystem based on elementary cellular automata,” *Commun. Nonlinear Sci. Numer. Simul.*, vol. 18, no. 1, pp. 136–147, 2013.
- [56] C. Jeyamala, S. GopiGanesh, and G. S. Raman, “An image encryption scheme based on one time pads — A chaotic approach,” *2010 Second International conference on Computing, Communication and Networking Technologies*. IEEE, 2010.
- [57] M. Essaid, I. Akharraz, A. Saaidi, and A. Mouhib, “A New Image Encryption Scheme Based on Confusion-Diffusion Using an Enhanced Skew Tent Map,” *Procedia Comput. Sci.*, vol. 127, pp. 539–548, 2018.
- [58] S. Zhu, C. Zhu, Y. Fu, W. Zhang, and X. Wu, “A secure image encryption scheme with compression-confusion-diffusion structure,” *Multimed. Tools Appl.*, vol. 79, no. 43–44, pp. 31957–31980, 2020.
- [59] B. Murugan and A. G. Nanjappa Gounder, “Image encryption scheme based on block-based confusion and multiple levels of diffusion,” *IET Comput. Vis.*, vol. 10, no. 6, pp.

- 593–602, 2016.
- [60] X. Chai, “An image encryption algorithm based on bit level Brownian motion and new chaotic systems,” *Multimed. Tools Appl.*, vol. 76, no. 1, pp. 1159–1175, 2015.
- [61] A. ur Rehman, X. Liao, R. Ashraf, S. Ullah, and H. Wang, “A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2,” *Optik (Stuttg.)*, vol. 159, pp. 348–367, 2018.
- [62] O. Jallouli, “Chaos-based security under real-time and energy constraints for the Internet of Things.” 2017.
- [63] M. Usama, M. K. Khan, K. Alghathbar, and C. Lee, “Chaos-based secure satellite imagery cryptosystem,” *Comput. Math. with Appl.*, vol. 60, no. 2, pp. 326–337, 2010.
- [64] D. Ruelle, “Early chaos theory,” *Phys. Today*, vol. 67, no. 3, pp. 9–10, 2014.
- [65] R. Matthews, “ON THE DERIVATION OF A ‘CHAOTIC’ ENCRYPTION ALGORITHM,” *Cryptologia*, vol. 13, no. 1, pp. 29–42, 1989.
- [66] G. Jakimoski and L. Kocarev, “Analysis of some recently proposed chaos-based encryption algorithms,” *Phys. Lett. A*, vol. 291, no. 6, pp. 381–384, 2001.
- [67] M. Kumar, A. Saxena, and S. S. Vuppala, “A Survey on Chaos Based Image Encryption Techniques,” *Multimedia Security Using Chaotic Maps: Principles and Methodologies*. Springer International Publishing, pp. 1–26, 2020.
- [68] N. Nesa, T. Ghosh, and I. Banerjee, “Design of a chaos-based encryption scheme for sensor data using a novel logarithmic chaotic map,” *J. Inf. Secur. Appl.*, vol. 47, pp. 320–328, 2019.
- [69] J. Ahmad and S. O. Hwang, “A secure image encryption scheme based on chaotic maps and affine transformation,” *Multimed. Tools Appl.*, vol. 75, no. 21, pp. 13951–13976, 2015.
- [70] P. N. Ruane, “Nonlinearity, chaos and complexity: The dynamics of natural and social systems, by Cristoforo Sergio Bertuglia and Franco Vaio. Pp. 387. £85 (hbk). 2005. ISBN 9780198567905 (Oxford University Press).,” *Math. Gaz.*, vol. 91, no. 520, pp. 181–182, 2007.
- [71] “IEEE Standard for Definitions and Concepts for Dynamic Spectrum Access:

- Terminology Relating to Emerging Wireless Networks, System Functionality, and Spectrum Management.” IEEE.
- [72] T. S. Parker and L. O. Chua, “Practical Numerical Algorithms for Chaotic Systems.” Springer New York, 1989.
- [73] X. Zhang and Y. Cao, “A novel chaotic map and an improved chaos-based image encryption scheme,” *ScientificWorldJournal.*, vol. 2014, p. 713541, 2014.
- [74] K. Aihara and L. Chen, “Strange attractors in chaotic neural networks,” *IEEE Trans. Circuits Syst. I Fundam. Theory Appl.*, vol. 47, no. 10, pp. 1455–1468, 2000.
- [75] N. S. Raghava and A. Kumar, “Image encryption using henon chaotic map with byte sequence,” *Int. J. Comput. Sci. Eng. Inf. Technol. Res.*, vol. 3, no. 5, pp. 11–18, 2013.
- [76] A. Ouannas, A.-A. Khennaoui, S. Bendoukha, T. Vo, V.-T. Pham, and V. Huynh, “The Fractional Form of the Tinkerbell Map Is Chaotic,” *Appl. Sci.*, vol. 8, no. 12, p. 2640, 2018.
- [77] L. Agilandeeswari and K. Ganesan, “RST invariant robust video watermarking algorithm using quaternion curvelet transform,” *Multimed. Tools Appl.*, vol. 77, no. 19, pp. 25431–25474, 2018.
- [78] H. Elkamchouchi, W. M. Salama, and Y. Abouelseoud, “ArMTFr: a new permutation-based image encryption scheme,” *Int. J. Electron. Secur. Digit. Forensics*, vol. 11, no. 1, p. 1, 2019.
- [79] X. Zeng, R. A. Pielke, and R. Eykholt, “Chaos Theory and Its Applications to the Atmosphere,” *Bull. Am. Meteorol. Soc.*, vol. 74, no. 4, pp. 631–644, 1993.
- [80] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, “A color image cryptosystem based on dynamic DNA encryption and chaos,” *Signal Processing*, vol. 155, pp. 44–62, 2019.
- [81] X. Chai, Y. Chen, and L. Broyde, “A novel chaos-based image encryption algorithm using DNA sequence operations,” *Opt. Lasers Eng.*, vol. 88, pp. 197–213, 2017.
- [82] xiaolin wu, B. Zhu, Y. Hu, and Y. Ran, “A novel colour image encryption scheme using rectangular transform-enhanced chaotic tent maps,” *IEEE Access*, p. 1, 2017.
- [83] C. K. Huang and H. H. Nien, “Multi chaotic systems based pixel shuffle for image encryption,” *Opt. Commun.*, vol. 282, no. 11, pp. 2123–2127, 2009.

-
- [84] X. Zhang, X. Fan, J. Wang, and Z. Zhao, "A chaos-based image encryption scheme using 2D rectangular transform and dependent substitution," *Multimed. Tools Appl.*, vol. 75, no. 4, pp. 1745–1763, 2014.
- [85] A. Bisht, M. Dua, and S. Dua, "A novel approach to encrypt multiple images using multiple chaotic maps and chaotic discrete fractional random transform," *J. Ambient Intell. Humaniz. Comput.*, vol. 10, no. 9, pp. 3519–3531, 2018.
- [86] V. Sankaradass, P. Murali, and M. Tholkapiyan, "Region of Interest (ROI) Based Image Encryption with Sine Map and Lorenz System," *Proceedings of the International Conference on ISMAC in Computational Vision and Bio-Engineering 2018 (ISMAC-CVB)*. Springer International Publishing, pp. 493–502, 2019.
- [87] M. A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R. M. López-Gutiérrez, and O. R. Acosta Del Campo, "A RGB image encryption algorithm based on total plain image characteristics and chaos," *Signal Processing*, vol. 109, pp. 119–131, 2015.
- [88] S. Anwar and S. Meghana, "A pixel permutation based image encryption technique using chaotic map," *Multimed. Tools Appl.*, vol. 78, no. 19, pp. 27569–27590, 2019.
- [89] N. Flores-Gallegos, "A new approach of Shannon's entropy in atoms," *Chem. Phys. Lett.*, vol. 650, pp. 57–59, 2016.
- [90] D. Ravichandran, S. Malayappan, R. Manavalan, P. Madhuri, and R. Amirtharajan, "A 3D Key for Encrypting 2D Images - A DNA Melded Chaotic Approach," *2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN)*. IEEE, 2019.
- [91] J. Ahmad, M. A. Khan, F. Ahmed, and J. S. Khan, "A novel image encryption scheme based on orthogonal matrix, skew tent map, and XOR operation," *Neural Comput. Appl.*, vol. 30, no. 12, pp. 3847–3857, 2017.
- [92] S. Somaraj and M. A. Hussain, "Performance and Security Analysis for Image Encryption using Key Image," *Indian J. Sci. Technol.*, vol. 8, no. 35, 2015.
- [93] S. Hussain and S. A. Chaudhry, "Comments on 'Biometrics-Based Privacy-Preserving User Authentication Scheme for Cloud-Based Industrial Internet of Things Deployment,'" *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10936–10940, 2019.
-

-
- [94] R. Jadhav and V. V., “Security Issues and Solutions in Wireless Sensor Networks,” *Int. J. Comput. Appl.*, vol. 162, no. 2, pp. 14–19, 2017.
- [95] A. Riahi Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, “A roadmap for security challenges in the Internet of Things,” *Digit. Commun. Networks*, vol. 4, no. 2, pp. 118–137, 2018.
- [96] “MSB based Cellular Automata for Edge Detection,” *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 9, pp. 1354–1358, 2019.
- [97] J. Jin, “An image encryption based on elementary cellular automata,” *Opt. Lasers Eng.*, vol. 50, no. 12, pp. 1836–1843, 2012.
- [98] F. Serebinski, P. Bouvry, and A. Y. Zomaya, “Cellular automata computations and secret key cryptography,” *Parallel Comput.*, vol. 30, no. 5–6, pp. 753–766, 2004.
- [99] S. Wolfram, “Cryptography with Cellular Automata,” *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, pp. 429–432.
- [100] A. M. Rey, “Message Authentication Protocol Based on Cellular Automata,” *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, pp. 52–60.
- [101] A. A.A. and S. Lian, “Multi-secret image sharing based on elementary cellular automata with steganography,” *Multimed. Tools Appl.*, vol. 79, no. 29–30, pp. 21241–21264, 2020.
- [102] A. Babaei, H. Motameni, and R. Enayatifar, “A new permutation-diffusion-based image encryption technique using cellular automata and DNA sequence,” *Optik (Stuttg.)*, vol. 203, p. 164000, 2020.
- [103] R. Enayatifar, F. G. Guimarães, and P. Siarry, “Index-based permutation-diffusion in multiple-image encryption using DNA sequence,” *Opt. Lasers Eng.*, vol. 115, pp. 131–140, 2019.
- [104] S. Roy, U. Rawat, H. A. Sareen, and S. K. Nayak, “IECA: an efficient IoT friendly image encryption technique using programmable cellular automata,” *J. Ambient Intell. Humaniz. Comput.*, 2020.
- [105] J. G. Kemeny, “Theory of Self-Reproducing Automata. John von Neumann. Edited by Arthur W. Burks. University of Illinois Press, Urbana, 1966. 408 pp., illus. \$10,” *Science*
-

- (80-), vol. 157, no. 3785, p. 180, 1967.
- [106] K. Bhattacharjee, N. Naskar, S. Roy, and S. Das, “A survey of cellular automata: types, dynamics, non-uniformity and applications,” *Nat. Comput.*, vol. 19, no. 2, pp. 433–461, 2018.
- [107] M. Gardner, “Mathematical Games,” *Sci. Am.*, vol. 223, no. 4, pp. 120–123, 1970.
- [108] E. Borriello and S. Imari Walker, “An Information-Based Classification of Elementary Cellular Automata,” *Complexity*, vol. 2017, pp. 1–8, 2017.
- [109] A. Moran, C. F. Frasser, M. Roca, and J. L. Rossello, “Energy-Efficient Pattern Recognition Hardware With Elementary Cellular Automata,” *IEEE Trans. Comput.*, vol. 69, no. 3, pp. 392–401, 2020.
- [110] S. Kamilya and S. Das, “A Study of Chaos in Cellular Automata,” *Int. J. Bifurc. Chaos*, vol. 28, no. 03, p. 1830008, 2018.
- [111] C. Li, G. Luo, K. Qin, and C. Li, “An image encryption scheme based on chaotic tent map,” *Nonlinear Dyn.*, vol. 87, no. 1, pp. 127–133, 2016.
- [112] S. Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi, and A. Akhavan, “A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps,” *Phys. Lett. A*, vol. 366, no. 4–5, pp. 391–396, 2007.
- [113] K. Gaj and A. Orłowski, “Facts and Myths of Enigma: Breaking Stereotypes,” *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, pp. 106–122, 2003.
- [114] L. Kruh and C. Deavours, “THE COMMERCIAL ENIGMA: BEGINNINGS OF MACHINE CRYPTOGRAPHY,” *Cryptologia*, vol. 26, no. 1, pp. 1–16, 2002.
- [115] A. Fazel and S. Chakrabarty, “An Overview of Statistical Pattern Recognition Techniques for Speaker Verification,” *IEEE Circuits Syst. Mag.*, vol. 11, no. 2, pp. 62–81, 2011.
- [116] T. Kinnunen and H. Li, “An overview of text-independent speaker recognition: From features to supervectors,” *Speech Commun.*, vol. 52, no. 1, pp. 12–40, 2010.
- [117] Z. Zhu, C. Bu, H. Li, and H. Yu, “A New Chaotic Encryption Scheme Based on Enigma Machine,” *2011 Fourth International Workshop on Chaos-Fractals Theories and Applications*. IEEE, 2011.

-
- [118] H. ElKamchouchi and A. ElShafee, "URESC, Unbalanced Rotor Enhanced Symmetric Cipher," *MELECON 2008 - The 14th IEEE Mediterranean Electrotechnical Conference*. IEEE, 2008.
- [119] S.-M. Chang, M.-C. Li, and W.-W. Lin, "Asymptotic synchronization of modified logistic hyper-chaotic systems and its applications," *Nonlinear Anal. Real World Appl.*, vol. 10, no. 2, pp. 869–880, 2009.
- [120] L.-X. Hong, C.-M. Li, and M.-X. Lu, "Combined image encryption algorithm based on diffusion mapped disorder and hyperchaotic systems.," *Jisuanji Yingyong/ J. Comput. Appl.*, vol. 27, no. 8, pp. 1891–1894, 2007.
- [121] . W., W. Astuti, and S. Mohamed, "Intelligent Voice-Based Door Access Control System Using Adaptive-Network-based Fuzzy Inference Systems (ANFIS) for Building Security," *J. Comput. Sci.*, vol. 3, no. 5, pp. 274–280, 2007.
- [122] F. Monrose, M. K. Reiter, Q. Li, and S. Wetzel, "Cryptographic key generation from voice," *Proceedings 2001 IEEE Symposium on Security and Privacy. S&P 2001*. IEEE Comput. Soc.
- [123] D. Shaila and D. Apte, "Speech and audio Processing." Wiley India Publication, 2012.
- [124] C.-C. Thien and J.-C. Lin, "Secret image sharing," *Comput. Graph.*, vol. 26, no. 5, pp. 765–770, 2002.
- [125] S. K. Shivakumar and S. Sethii, "DXP Security," in *Building Digital Experience Platforms*, Springer, 2019, pp. 183–200.
- [126] J. M. Kizza, "Computer Network Security Fundamentals," *Guide to Computer Network Security*. Springer International Publishing, pp. 41–57, 2017.
- [127] S. Som, A. Mitra, S. Palit, and B. B. Chaudhuri, "A selective bitplane image encryption scheme using chaotic maps," *Multimed. Tools Appl.*, vol. 78, no. 8, pp. 10373–10400, 2018.
- [128] D. Le Gall, "MPEG," *Commun. ACM*, vol. 34, no. 4, pp. 46–58, 1991.
- [129] F. A. P. Petitcolas, "Introduction to information hiding," *Katzenbeisser, S Petitcolas, FAP*, pp. 275–290, 2000.
- [130] M. Vardhana, N. Arunkumar, E. Abdulhay, and P. V Vishnuprasad, "Iot based real time
-

- traffic control using cloud computing,” *Cluster Comput.*, vol. 22, no. S1, pp. 2495–2504, 2018.
- [131] A. B. Mahmood and R. D. Dony, “Segmentation based encryption method for medical images,” in *2011 International Conference for Internet Technology and Secured Transactions*, 2011, pp. 596–601.
- [132] J.-L. Liu, “Efficient selective encryption for JPEG 2000 images using private initial table,” *Pattern Recognit.*, vol. 39, no. 8, pp. 1509–1517, 2006.
- [133] K. C. Ravishankar and M. G. Venkateshmurthy, “Region based selective image encryption,” *2006 International Conference on Computing & Informatics*. IEEE, 2006.
- [134] J. Kittler, “A locally sensitive method for cluster analysis,” *Pattern Recognit.*, vol. 8, no. 1, pp. 23–33, 1976.
- [135] S. Susan, O. P. Verma, and J. Swarup, “Object Segmentation by an Automatic Edge Constrained Region Growing Technique,” *2012 Fourth International Conference on Computational Intelligence and Communication Networks*. IEEE, 2012.
- [136] H. A. Younis, T. Y. Abdalla, and A. Y. Abdalla, “Vector Quantization Techniques For Partial Encryption of Wavelet-based Compressed Digital Images,” *Iraqi J. Electr. Electron. Eng.*, vol. 5, no. 1, pp. 74–89, 2009.
- [137] N. Taneja, B. Raman, and I. Gupta, “Selective image encryption in fractional wavelet domain,” *AEU - Int. J. Electron. Commun.*, vol. 65, no. 4, pp. 338–344, 2011.
- [138] L. Oteko Tresor and M. Sumbwanyambe, “A Selective Image Encryption Scheme Based on 2D DWT, Henon Map and 4D Qi Hyper-Chaos,” *IEEE Access*, vol. 7, pp. 103463–103472, 2019.
- [139] K. He, C. Bidan, G. Le Guelvouit, and C. Feron, “Robust and Secure Image Encryption Schemes During JPEG Compression Process,” *Electron. Imaging*, vol. 2016, no. 11, pp. 1–7, 2016.
- [140] N. Hazarika, S. Borah, and M. Saikia, “A wavelet based partial image encryption using chaotic logistic map,” *2014 IEEE International Conference on Advanced Communications, Control and Computing Technologies*. IEEE, 2014.
- [141] T. Xiang, K. Wong, and X. Liao, “Selective image encryption using a spatiotemporal

- chaotic system,” *Chaos An Interdiscip. J. Nonlinear Sci.*, vol. 17, no. 2, p. 23115, 2007.
- [142] S. N. Prajwalasimha, “Pseudo-Hadamard Transformation-Based Image Encryption Scheme,” *Integrated Intelligent Computing, Communication and Security*. Springer Singapore, pp. 575–583, 2018.
- [143] S. Kelur, R. Kumar H S, and R. K., “Selective Area Encryption using Machine Learning Technique,” *2019 Innovations in Power and Advanced Computing Technologies (i-PACT)*. IEEE, 2019.
- [144] P. T. Akkasaligar and S. Biradar, “Selective medical image encryption using DNA cryptography,” *Inf. Secur. J. A Glob. Perspect.*, vol. 29, no. 2, pp. 91–101, 2020.
- [145] S. Lahmiri, “A Wavelet-Wavelet Based Processing Approach for Microcalcifications Detection in Mammograms,” *J. Adv. Inf. Technol.*, vol. 3, no. 3, 2012.
- [146] A. Ahmad, A. Muharam, and A. Amira, “GPU-based implementation of CABAC for 3-Dimensional Medical Image Compression,” *J. Telecommun. Electron. Comput. Eng.*, vol. 9, no. 3–8, pp. 45–50, 2017.
- [147] A. Kumar and N. S. Raghava, “Chaos-based steganography technique to secure information and integrity preservation of smart grid readings using wavelet,” *Int. J. Comput. Appl.*, pp. 1–7, 2019.
- [148] Y. Ou, C. Sur, and K. H. Rhee, “Region-Based Selective Encryption for Medical Imaging,” *Frontiers in Algorithmics*. Springer Berlin Heidelberg, pp. 62–73.
- [149] O. P. Verma, M. Hanmandlu, S. Susan, M. Kulkarni, and P. K. Jain, “A Simple Single Seeded Region Growing Algorithm for Color Image Segmentation using Adaptive Thresholding,” *2011 International Conference on Communication Systems and Network Technologies*. IEEE, 2011.
- [150] S. Agarwal, A. Awan, and D. Roth, “UIUC image database for car detection,” *Retrieved March*, vol. 1, p. 2007, 2002.
- [151] A. Kumar and N. S. Raghava, “A NOVEL GROUP-BASED CRYPTOSYSTEM BASED ON ELECTROMAGNETIC ROTOR MACHINE.,” *Indian J. Sci. Res.*, pp. 131–137, 2017.
- [152] A. Belazi, A. A. Abd El-Latif, R. Rhouma, and S. Belghith, “Selective image encryption

- scheme based on DWT, AES S-box and chaotic permutation,” *2015 International Wireless Communications and Mobile Computing Conference (IWCMC)*. IEEE, 2015.
- [153] Z. Brahim, H. Bessalah, A. Tarabet, and M. K. Kholadi, “A new selective encryption technique of JPEG2000 codestream for medical images transmission,” *2008 5th International Multi-Conference on Systems, Signals and Devices*. IEEE, 2008.
- [154] G. Mehta, M. K. Dutta, C. M. Travieso-Gonzalez, and P. S. Kim, “Edge based selective encryption scheme for biometric data using chaotic theory,” *2014 International Conference on Contemporary Computing and Informatics (IC3I)*. IEEE, 2014.
- [155] A. M. Ayoub, A. H. Hussein, and M. A. A. Attia, “Efficient selective image encryption,” *Multimed. Tools Appl.*, vol. 75, no. 24, pp. 17171–17186, 2015.
- [156] O. A. Khashan, A. M. Zin, and E. A. Sundararajan, “Performance study of selective encryption in comparison to full encryption for still visual images,” *J. Zhejiang Univ. Sci. C*, vol. 15, no. 6, pp. 435–444, 2014.
- [157] D. Xiao, Q. Fu, T. Xiang, and Y. Zhang, “Chaotic Image Encryption of Regions of Interest,” *Int. J. Bifurc. Chaos*, vol. 26, no. 11, p. 1650193, 2016.
- [158] H. Kaur and A. Kakkar, “Comparison of different image formats using LSB Steganography,” *2017 4th International Conference on Signal Processing, Computing and Control (ISPCC)*. IEEE, 2017.
- [159] V. C. Gungor *et al.*, “Smart Grid Technologies: Communication Technologies and Standards,” *IEEE Trans. Ind. Informatics*, vol. 7, no. 4, pp. 529–539, 2011.
- [160] A. R. Devidas, M. V. Ramesh, and V. P. Rangan, “High performance communication architecture for smart distribution power grid in developing nations,” *Wirel. Networks*, vol. 24, no. 5, pp. 1621–1638, 2016.
- [161] J. Aghaei and M.-I. Alizadeh, “Demand response in smart electricity grids equipped with renewable energy sources: A review,” *Renew. Sustain. Energy Rev.*, vol. 18, pp. 64–72, 2013.
- [162] F. Yu, P. Zhang, W. Xiao, and P. Choudhury, “Communication systems for grid integration of renewable energy resources,” *IEEE Netw.*, vol. 25, no. 5, pp. 22–29, 2011.
- [163] M. M. Eissa, “First time real time incentive demand response program in smart grid with

- 'i-Energy' management system with different resources," *Appl. Energy*, vol. 212, pp. 607–621, 2018.
- [164] D. Kumar, F. Zare, and A. Ghosh, "DC Microgrid Technology: System Architectures, AC Grid Interfaces, Grounding Schemes, Power Quality, Communication Networks, Applications, and Standardizations Aspects," *IEEE Access*, vol. 5, pp. 12230–12256, 2017.
- [165] A. A. Khan, M. H. Rehmani, and M. Reisslein, "Cognitive Radio for Smart Grids: Survey of Architectures, Spectrum Sensing Mechanisms, and Networking Protocols," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 1, pp. 860–898, 2016.
- [166] D. Alahakoon and X. Yu, "Smart Electricity Meter Data Intelligence for Future Energy Systems: A Survey," *IEEE Trans. Ind. Informatics*, vol. 12, no. 1, pp. 425–436, 2016.
- [167] I. Ilieva, B. Bremdal, S. Ødegaard Ottesen, J. Rajasekharan, and P. Olivella-Rosell, "Design characteristics of a smart grid dominated local market," *CIGRE Workshop 2016*. Institution of Engineering and Technology, 2016.
- [168] Z. Cao, J. Lin, C. Wan, Y. Song, Y. Zhang, and X. Wang, "Optimal Cloud Computing Resource Allocation for Demand Side Management," *IEEE Trans. Smart Grid*, pp. 1–13, 2016.
- [169] S. Darby, "Smart metering: what potential for householder engagement?," *Build. Res. Inf.*, vol. 38, no. 5, pp. 442–457, 2010.
- [170] Y. Mo *et al.*, "Cyber-Physical Security of a Smart Grid Infrastructure," *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, 2012.
- [171] D. S. Kirschen and G. Strbac, *Fundamentals of power system economics*. John Wiley & Sons, 2018.
- [172] Y. Arafat, "On possibilities of using smart meters for compulsory load shedding supported by load forecasting." Chalmers Tekniska Hogskola (Sweden), 2018.
- [173] S. Kakran and S. Chanana, "Smart operations of smart grids integrated with distributed generation: A review," *Renew. Sustain. Energy Rev.*, vol. 81, pp. 524–535, 2018.
- [174] V. Potdar, A. Chandan, S. Batool, and N. Patel, "Big Energy Data Management for Smart Grids—Issues, Challenges and Recent Developments," *Smart Cities*. Springer

- International Publishing, pp. 177–205, 2018.
- [175] A. Ghosal and M. Conti, “Key Management Systems for Smart Grid Advanced Metering Infrastructure: A Survey,” *IEEE Commun. Surv. Tutorials*, vol. 21, no. 3, pp. 2831–2848, 2019.
- [176] C.-C. Sun, A. Hahn, and C.-C. Liu, “Cyber security of a power grid: State-of-the-art,” *Int. J. Electr. Power Energy Syst.*, vol. 99, pp. 45–56, 2018.
- [177] A. Hamlyn, H. Cheung, T. Mander, L. Wang, C. Yang, and R. Cheung, “Computer network security management and authentication of smart grids operations,” *2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*. IEEE, 2008.
- [178] Y.-J. Kim, V. Kolesnikov, H. Kim, and M. Thottan, “SSTP: A scalable and secure transport protocol for smart grid data collection,” *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2011.
- [179] K. Wang, M. Du, S. Maharjan, and Y. Sun, “Strategic honeypot game model for distributed denial of service attacks in the smart grid,” *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2474–2482, 2017.
- [180] R. Amirtharaj, P. Praveenkum, K. Thenmozhi, and J. Bosco Bala, “Inbuilt Image Encryption and Steganography Security Solutions for Wireless Systems: A Survey,” *Res. J. Inf. Technol.*, vol. 9, no. 2, pp. 46–63, 2017.
- [181] A. Abuadbbba and I. Khalil, “Walsh–Hadamard-Based 3-D Steganography for Protecting Sensitive Information in Point-of-Care,” *IEEE Trans. Biomed. Eng.*, vol. 64, no. 9, pp. 2186–2195, 2017.
- [182] D. Engel and G. Eibl, “Wavelet-Based Multiresolution Smart Meter Privacy,” *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1710–1721, 2017.
- [183] J. A. S. Barker, A. Mishra, D. Irwin, E. Cecchet, P. Shenoy, “Smart project,” 2012. [Online]. Available: <http://traces.cs.umass.edu/index.php/Smart?smart>.
- [184] S. Barker, A. Mishra, D. Irwin, E. Cecchet, P. Shenoy, and J. Albrecht, “Smart*: An open data set and tools for enabling research in sustainable homes,” *SustKDD, August*, vol. 111, no. 112, p. 108, 2012.

-
- [185] B. Pradhan and S. Sengupta, "Chaotic-cipher based memory efficient symmetric key cryptosystem," *2018 Emerging Trends in Electronic Devices and Computational Techniques (EDCT)*. IEEE, 2018.
- [186] S. J. Sheela, K. V Suresh, and D. Tandur, "Image encryption based on modified Henon map using hybrid chaotic shift transform," *Multimed. Tools Appl.*, vol. 77, no. 19, pp. 25223–25251, 2018.
- [187] D. K. Tosh, S. Shetty, P. Foytik, L. Njilla, and C. A. Kamhoua, "Blockchain-empowered secure internet-of-battlefield things (iobt) architecture," in *MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM)*, 2018, pp. 593–598.
- [188] N. B. Gaikwad, H. Ugale, A. Keskar, and N. C. Shivaprakash, "The Internet of Battlefield Things (IoBT) based Enemy Localization using Soldiers Location and Gunshot Direction," *IEEE Internet Things J.*, 2020.
- [189] Y. Feng, M. Li, C. Zeng, and H. Liu, "Robustness of Internet of Battlefield Things (IoBT): A Directed Network Perspective," *Entropy*, vol. 22, no. 10, p. 1166, 2020.
- [190] E. Onem, S. Eryigit, T. Tugcu, and A. Akurgal, "QoS-enabled spectrum-aware routing for disaster relief and tactical operations over cognitive radio ad hoc networks," in *MILCOM 2013-2013 IEEE Military Communications Conference*, 2013, pp. 1109–1115.
- [191] S. Couturier *et al.*, "End-to-end optimization for tactical cognitive radio networks," in *2018 International Conference on Military Communications and Information Systems (ICMCIS)*, 2018, pp. 1–8.
- [192] S. Uma Maheswari and D. Jude Hemanth, "Frequency domain QR code based image steganography using Fresnelet transform," *AEU - Int. J. Electron. Commun.*, vol. 69, no. 2, pp. 539–544, 2015.
- [193] M. Liebling, T. Blu, and M. Unser, "Fresnelets: new multiresolution wavelet bases for digital holography," *IEEE Trans. Image Process.*, vol. 12, no. 1, pp. 29–43, 2003.
- [194] V. Rajaraman, "IEEE standard for floating point numbers," *Resonance*, vol. 21, no. 1, pp. 11–30, 2016.
- [195] P. Bodik, W. Hong, C. Guestrin, S. Madden, M. Paskin, and R. Thibaux, "Intel berkeley

- research lab data,” URL <http://db.csail.mit.edu/labdata/labdata.html>, 2004.
- [196] B. R. Clark, *The higher education system: Academic organization in cross-national perspective*. Univ of California Press, 1986.
- [197] J. Nishchal, S. Reddy, and P. N. Navya, “Automated Cheating Detection in Exams using Posture and Emotion Analysis,” in *2020 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*, 2020, pp. 1–6.
- [198] X. Li and Y. Meng, “How to Prevent College Students from Cheating in Exams?—Based on Game Theory,” *Int. J. Res. Stud. Sci. Eng. Technol.*, vol. 3, no. 9, pp. 39–42, 2016.
- [199] M. S. Mizruchi, “Who Controls Whom? An Examination of the Relation Between Management and Boards of Directors in Large American Corporations,” *Acad. Manag. Rev.*, vol. 8, no. 3, pp. 426–435, 1983.
- [200] W. R. Klemm, “Use and Mis-Use of Technology for Online, Asynchronous, Collaborative Learning,” *Computer-Supported Collaborative Learning in Higher Education*. IGI Global, pp. 172–200, 2005.
- [201] E. K. Burke, D. G. Elliman, and R. Weare, “A University Timetabling System Based on Graph Colouring and Constraint Manipulation,” *J. Res. Comput. Educ.*, vol. 27, no. 1, pp. 1–18, 1994.
- [202] K. T. Hill and A. Wigfield, “Test Anxiety: A Major Educational Problem and What Can Be Done about It,” *Elem. Sch. J.*, vol. 85, no. 1, pp. 105–126, 1984.
- [203] J. Biggs, “What the student does: teaching for enhanced learning,” *High. Educ. Res. Dev.*, vol. 31, no. 1, pp. 39–55, 2012.
- [204] E. Petrisor, “Entry and exit sets in the dynamics of area preserving Hénon map,” *Chaos, Solitons & Fractals*, vol. 17, no. 4, pp. 651–658, 2003.
- [205] “Enigmas and other cipher machines for sale.” <https://w1tp.com/4sale/>
- [206] “Cipher machines and cryptology.” <http://users.telenet.be/d.rijmenants/pics>