

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

# Elliptic Curve Computation and Their Applications in Data Security



**Muhammad Imran Haider**

**Department of Mathematics  
Quaid-i-Azam University  
Islamabad, Pakistan  
2023**

# Elliptic Curve Computation and Their Applications in Data Security



**Muhammad Imran Haider**

Supervised by

**Dr. Asif Ali**

**Department of Mathematics  
Quaid-i-Azam University  
Islamabad, Pakistan  
2023**

# Elliptic Curve Computation and Their Applications in Data Security



A Thesis Submitted to the Department of Mathematics, Quaid-i-Azam University, Islamabad, in the partial fulfillment of the requirement for the degree of

**Doctor of Philosophy**

in

**Mathematics**

By

**Muhammad Imran Haider**

Supervised by

**Dr. Asif Ali**

**Department of Mathematics**

**Quaid-i-Azam University**

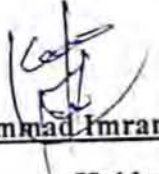
**Islamabad, Pakistan**

**2023**

## Author's Declaration

I, Muhammad Imran Haider, hereby state that my PhD thesis titled entitled Elliptic Curve Computation and Their Applications in Data Security is my own work and has not been submitted previously by me for taking any degree from the Quaid-I-Azam University Islamabad, Pakistan or anywhere else in the country/world.

At any time if my statement is found to be incorrect even after my graduate the university has the right to withdraw my PhD degree.

Name of Student:   
Muhammad Imran  
Haider


Date: 31-Aug-2023

## Plagiarism Undertaking

I solemnly declare that research work presented in the thesis titled "Elliptic Curve Computation and Their Applications in Data Security" is solely my research work with no significant contribution from any other person. Small contribution/help wherever taken has been duly acknowledged and that complete thesis has been written by me.

I understand the zero tolerance policy of the HEC and Quaid-i-Azam University towards plagiarism. Therefore, I as an Author of the above titled thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred/cited.

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even afterward of PhD degree, the University reserves the rights to withdraw/revoke my PhD degree and that HEC and the University has the right to publish my name on the HEC/University Website on which names of students are placed who submitted plagiarized thesis.


  
Student/Author Signature

Name: Muhammad Imran  
Haider

## Certificate of Approval

This is to certify that the research work presented in this thesis entitled Elliptic Curve Computation and Their Applications in Data Security was conducted by Muhammad Imran Haider under the kind supervision of Prof. Dr. Asif Ali. No part of this thesis has been submitted anywhere else for any other degree. This thesis is submitted to the Department of Mathematics, Quaid-i-Azam University, Islamabad in partial fulfillment of the requirements for the degree of Doctor of Philosophy in field of Mathematics from Department of Mathematics, Quaid-i-Azam University Islamabad, Pakistan.

Student Name: Muhammad Imran Haider

Signature: 

External committee:

a) External Examiner 1:

Name: **Dr. Akbar Azam**

Designation: Professor

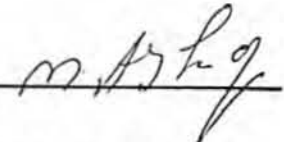
Office Address: Department of Mathematics, COMSATS University, Park Road, Chak Shahzad, Islamabad.

Signature: 

b) External Examiner 2:

Name: **Brig. Dr. Muhammad Ashiq**

Office Address: National University of Technology NUTECH, Islamabad.

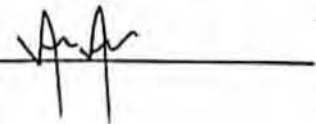
Signature: 

c) Internal Examiner

Name: **Prof. Dr. Asif Ali**

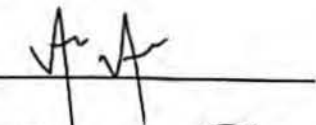
Designation: Professor

Office Address: Department of Mathematics, QAU Islamabad.

Signature: 

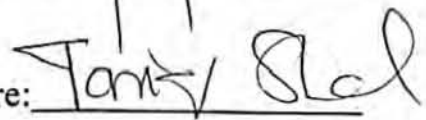
Supervisor Name:

Prof. Dr. Asif Ali

Signature: 

Name of Dean/ HOD

Prof. Dr. Tariq Shah

Signature: 

# Elliptic Curve Computation and Their Applications in Data Security

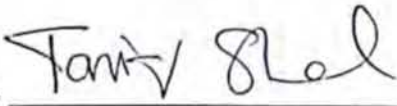
By

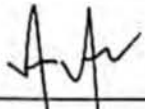
**Muhammad Imran Haider**

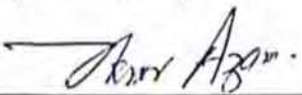
CERTIFICATE

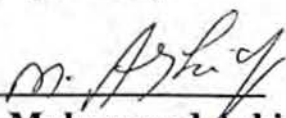
A THESIS SUBMITTED IN THE PARTIAL FULFILLMENT OF THE  
REQUIREMENTS FOR THE DEGREE OF THE  
DOCTOR OF PHILOSOPHY IN MATHEMATICS

We accept this thesis as conforming to the required standard

1.   
Prof. Dr. Tariq Shah  
(Chairman)

2.   
Prof. Dr. Asif Ali  
(Supervisor)

3.   
Prof. Dr. Akbar Azam  
(External Examiner)

4.   
Brig. Dr. Muhammad Ashiq  
(External Examiner)

Department of Mathematics, COMSATS  
University, Park Road, Chak Shahzad,  
Islamabad.

National University of Technology NUTECH,  
Islamabad.

**Department of Mathematics**  
**Quaid-I-Azam University**  
**Islamabad, Pakistan**  
**2023**



Dedicate to

**My Parents, Wife, and children**

## Acknowledgement

All praise for almighty Allah, the creator and the Merciful Lord, who guides me in darkness, helps me in difficulties and enables me to reach the ultimate stage with courage. All of my reverence and devotion goes to our beloved Prophet Muhammad, peace be upon him, the source of humanity, kindness and guidance for the whole creatures, who declared it an obligatory duty of every Muslim to seek and acquire knowledge.

Special appreciation goes to my honorable supervisor **Dr. Asif Ali** and Co-supervisor **Dr. Tariq Shah**, Chairman Department of Mathematics for their supervision, advice, and crucial contribution, which made a backbone of this research and so to this thesis. I would like to thank all the faculty members of **Mathematics Department**, Quaid-i-Azam University Islamabad Pakistan for their help, support and encouragement throughout my Doctoral study.

I would like to thank my parents, whose love and guidance are with me in whatever I pursue. They are the ultimate role models. My Father, Mr. Haider Khan, in the first place who put the fundamentals for my learning character, showing me the joy of intellectual pursuit ever since I was a child. My Mother is the one who sincerely raised me with her caring and gentle love. My brothers, sisters and all my family members, thanks for being supportive and caring.

I would like to express my sincere thanks to Assistant Professor Dr. Saif Ur Rehman (INS, Gomal Univeesity, DIKhan), Dr. Ijaz Khalid and Dr. Sami Ullah Kahn (Director, INS Gomal Univeesity, DIKhan) for their generous assistance and invaluable comments throughout the entire PhD program. I am also indebted to my dear friends Mr. Mashal Khan, Dr. Aftab Marwat (Homeopathic specialist), Dr. Khurshid (Homeopathic specialist), and Dr. Ashfaq Awan (Homeopathic specialist), not only for all their useful suggestions but also for being there to listen when I needed an ear. Without the help of those who participated in this study, this study would have not been possible.

Finally, I would like to say thanks to everybody who was important to the successful realization of this thesis, as well as expressing my apology to all that I couldn't mention personally one by one.

**Muhammad Imran Haider**

**February, 2023**

## Preface

In the recent era, the security of sensitive information has gained widespread attention. The multimedia data is one of the key sources of information, which can be agreements, photographs, medical reports, contracts, or other types of scanned papers, with the highest rank of sensitivity. The privacy of digital information is of utmost importance while communicated among authorized parties. To deal the security and privacy of multimedia data gave rise to the various efficient encryption algorithms. These algorithms are further based on two different ideas: symmetric and asymmetric key-algorithm. Various efficient algorithms are developed to generate substitution boxes (S-boxes) and pseudo-random number sequences. S-boxes have two major categories: Static and dynamic S-box. A static S-box depends on fixed operating as well as generating modes while a dynamic S-box has both variable modes of operations. As a result, dynamic S-boxes algorithms are preferred mostly to increase the computational cost for cryptanalysts.

Recently, Razaq et al. [108], developed a novel algorithm with the help of group structure for secure S-box in terms of high nonlinearity. Toughi et al. [13], proposed an image encryption algorithm with core modules PRNG and advanced encryption standard AES. The authors in [14], used the chaotic model to design image encryption scheme with enough pseudo creation capability. Due to multiple advantages such as non-periodicity, high sensitivity to input parameters, ergodicity, key sensitivity, chaotic systems, and ECs are extensively adopted for S-box and pseudo-random number generation in image encryption algorithms. The authors in [19], designed a secure algorithm that can be suitable in either digital and optical environments. Wang et al. [20], suggested a cryptosystem based on multi-group techniques such as chaotic map, Fisher-Yates Shuffling, and DNA sequence encoding. The authors of this research study claimed to have high accuracy with fast convergence as an advantage of the encryption algorithm. In light of computational precision, chaotic maps can have the possibility to generate a random sequence with a short period. Reyad et al. [22], developed an idea based on ECs to get pseudo-random numbers that work efficiently in image cryptography. El-Latif et al. [23], utilized both cyclic ECs and hybrid-chaotic systems for developing an efficient image encryption scheme.

The less computational effort with strong security, Elliptic curve based cryptographic architectures are more reliable as compared to the existing cryptographic methods. We introduced an efficient cryptosystem based on elliptic curves for digital image encryption. The designed scheme is consisting of three steps. Initially, the system uses the special type of

the isomorphic elliptic curves over a prime field and scrambles the pixel position of the plain image. Consequently, it disperses the intra-correlation among the pixels of the original image, and capable the scheme to be secure against statistical attacks. In the third step, the scheme generates multiple S-boxes with good cryptographic features by using isomorphic elliptic curves. The generated S-boxes are then used to substitute the scrambled data that produce optimum confusion in the ciphered data. Eventually, the encryption procedure generates PRNs through the arithmetic operation of the elliptic curves instead of elliptic curve group law; the operation used in the scheme creates high randomness as a result our proposed scheme shows high security against classical attacks. The simulation results and performance analysis divulge that the proposed scheme has excellent encryption performance with less computational effort, which indicates that the scheme has effective potential in real-time image encryption application.

Secondly, we discuss the security strength of the elliptic curve cryptosystems (ECC) is due to its core operations-based group law. This aspect of the elliptic curve provides key service to ensure security against modern cryptanalysis. However, the excess use of group law in EC based algorithms make it computationally hard for real time applications. In this context, we presented a smart-like algorithm based on subgroup co-set operations. The suggested scheme uses all co-sets that generates multiple sequences that can smoothly be adopted in most promising communication architectures of the future such as internet of things (IoT). Besides, the subgroup structure on a small prime with possible embedding is managed to construct efficient S-box. Whereas, the performance of the proposed S-box is examined via standardized tests thus found significant for multimedia data security applications. Moreover, a small prime based EC subgroup coset model is designed, that generates a set of experimentally verified independent pseudo random streams. The atypical mathematical model for its application to image data encryption is established, by combining the S-box module (SM) and subgroup coset module (ECS-PRNSM). Several statistical tests revealed that the proposed technique is suitable for various cryptographic applications.

Thirdly, in this dissertation, we discuss the Efficient multiple PRNS and S-boxes are one of the most significant building blocks, which are jointly adopted normally for secure data encryption. Multiple aspects pave the way to handle large-scale multimedia data. However, the computational work on multiple constructions may certainly lead to limits the required ciphering through-put. Therefore, reducing the computational time of multiple PRNS and S-boxes is the main requirement for an efficient cryptosystem. For this achievement, we exploited the indexing technique over elliptic curves with small prime fields and introduce a

computationally efficient mechanism for multiple PRNS and S-boxes. Statistical results of multiple S-boxes show that the proposed S-box mechanism is the most effective method that generates strong multiple S-boxes on minimum prime fields. Likewise, the PRNS's assessment indicates that the proposed mechanism is the highly productive model for generating multiple verified patterns on small prime fields in a single round. Consequently, it might be smoothly formalized to diffused large-scaled image data. Subsequently, the experimental results and analysis show that the proposed algorithm provides desired keyspace, better statistical properties of encrypted data, and less computational effort.

## Research profile

- 1).** Haider, M. I., Ali, A., Shah, D., & Shah, T. (2021). Block cipher's nonlinear component design by elliptic curves: an image encryption application. *Multimedia Tools and Applications*, 80, 4693-4718. <https://doi.org/10.1007/s11042-020-09892-5>.
- 2).** Haider, M. I., Shah, T., Ali, A., Shah, D., & Khalid, I. (2022). Pseudo random sequences based on elliptic curve subgroups and mathematical model for its application to digital image security. *Multimedia Tools and Applications*, 81(17), 23709-23734. <https://doi.org/10.1007/s11042-022-12358-5>.
- 3).** Haider, M. I., Shah, T., Ali, A., Shah, D., & Khalid, I. (2023). An Innovative approach towards image encryption by using novel PRNs and S-boxes Modeling techniques. *Mathematics and Computers in Simulation* <https://doi.org/10.1016/j.matcom.2023.01.036>.

# Table of Contents

<b>1. Introduction and Preliminaries .....</b>	<b>7</b>
1.1 Introduction.....	7
1.2 Elliptic Curve.....	7
1.2.1 Elliptic Curve Points Arithmetic.....	8
1.2.2 Elliptic Curves and Finite Fields.....	9
1.2.3 Some Definitions and Results .....	11
1.3 Elliptic Curves and Its Cryptographic Applications .....	13
1.3.1 RSA.....	14
1.3.2 El Gamal Public Key Encryption.....	15
1.4 Substitution Boxes .....	16
1.5 Objectives .....	18
1.5.1 Elliptic Curve Diffie Hellman Key Exchange .....	18
1.6 Own Work.....	19
<b>2. A Novel Approach Towards S-box and PRNs over Elliptic Curve .....</b>	<b>21</b>
2.1 Motivation.....	21
2.2 Proposed S-boxes Based on IECS .....	22
2.3 Performance Analyses of the Generated S-box .....	24
2.3.1 Nonlinearity (NL) .....	25
2.3.2 Linear Approximation Probability (LP).....	26
2.3.3 Strict Avalanche Criterion (SAC).....	26
2.3.4 Bit Independence Criterion (BIC).....	26
2.3.5 Differential Approximation Probability (DP) .....	27
2.4 Construction of Pseudo Random Numbers.....	27
2.4.1 Key Space Analysis .....	29
<b>3. Squared and Non-Squared PRN and their Application to Color Image Encryption .....</b>	<b>30</b>
3.1 Motivation.....	30
3.2 Proposed Encryption Scheme .....	31
3.3 Experimental Results and Comparison .....	33
3.3.1 Histogram Analysis.....	34
3.3.2 Entropy Analysis.....	35
3.3.3 Contrast.....	35
3.3.4 Energy.....	35
3.3.5 Homogeneity.....	36
3.3.6 Correlation .....	37
3.3.7 Differential attack .....	39

3.4	Robustness Analyses.....	40
3.4.1	Noise Analyses.....	41
3.4.2	Occluded Attack.....	42
3.4.1	Peak Signal to Noise Ratio (PSNR).....	42
3.5	Algorithm Complexity .....	44
<b>4.</b>	<b>Efficient Random Numbers Generation and S-box Construction Scheme.....</b>	<b>46</b>
4.1	Motivation.....	46
4.2	Basic Concepts.....	48
4.2.1	Elliptic Curve Group Operations .....	49
4.2.2	Point Addition Formula .....	49
4.2.3	Point Doubling Formula.....	49
4.3	Mechanism for S-box (MS) .....	50
4.3.1	Measurements and Results of the Proposed S-box .....	51
4.4	EC Subgroup PRNS Module (ECS-PRNSM).....	53
4.5	NIST (800-22 test suit) .....	56
4.5.1	Frequency (monobit) Test (FM. T):.....	56
4.5.2	Frequency Test within Block (BF. T).....	56
4.5.3	Longest of Runs of Ones in a Block Test (LR. T) .....	56
4.5.4	Run Test (R. T) .....	56
4.5.5	Binary Matrix Rank Test (BMR. T).....	56
4.5.6	Cumulative Sums Test (CS. T) .....	57
4.5.7	Approximation Entropy Test (AE. T).....	57
4.5.8	Non overlapping Template Matching Test (NTM. T) .....	57
4.5.9	Overlapping Template Matching Test (OTM. T) .....	57
4.5.10	Maurer’s Universal Statistical Test (MUS. T).....	57
4.5.11	Random Excursions Test (RE. T) .....	57
4.5.12	Random Excursions Variant Test (REV. T) .....	57
4.5.13	Linear Complexity (LC. T) .....	57
4.5.14	Discrete Fourier Transform Test (DFT. T): .....	57
4.5.15	Serial Test (S. T).....	58
4.6	NIST Analysis and Comparison .....	58
<b>5.</b>	<b>Mathematical Model Based on PRN with Image Encryption Applications .....</b>	<b>61</b>
5.1	Motivation.....	61
5.2	Mathematical Modeling for Image Encryption.....	63
5.3	Performance Analyses of the Proposed Encryption Scheme .....	65
5.3.1	Keyspace Analysis .....	66



5.3.2	Key Sensitivity Analysis.....	68
5.3.3	Three-Dimensional Histogram.....	68
5.3.4	Differential Analysis.....	69
5.3.5	Information Entropy.....	70
5.3.1	Correlation.....	70
<b>6.</b>	<b>Image Encryption by using Novel PRNs and S-boxes Modeling Techniques.....</b>	<b>75</b>
6.1	Motivation.....	75
6.2	Basic Concept.....	77
6.3	Proposed Methodology for S-boxes and Pseudorandom Numbers Streams.....	78
6.3.1	SCM.....	78
6.3.2	PRNGM.....	80
6.4	Performance Analysis of SCM and PRNGM.....	84
6.4.1	SCM Analysis.....	84
6.4.2	PRNGM Analysis.....	84
6.4.3	National Institute of Standard and Technology (NIST).....	84
6.5	Proposed Scheme in Image Encryption.....	85
6.6	Performance Analysis of Image Encryption.....	86
6.6.1	Histogram Analysis.....	86
6.6.2	Correlation Analysis.....	86
6.6.3	Information Entropy.....	87
6.6.4	Differential Attack.....	87
6.6.5	Key Sensitivity Analysis.....	87
6.7	Comparison and Discussion.....	91
<b>7.</b>	<b>Conclusion and Future Work.....</b>	<b>93</b>
7.1	Conclusion of Thesis.....	93
7.2	Perspective of Future Directions.....	96

## List of Figures

Figure 1. Point Doubling.....	8
Figure 2. Graphical interpretation of E1,217(F17) .....	10
Figure 3. Flowchart of the proposed encryption scheme .....	31
Figure 4. Original and Ciphered images: (a) The original color images of Lena, Baboon, Pepper, and Deblur; (b) The Permuted images; (c) The Substituted images; (d) The Ciphered images. ....	33
Figure 5. Histograms of original color images and ciphered images: (a). The original color images: Lena, Swat image and Nature image; (b). The histograms of the original images; (c) The ciphered images; (d). The histograms of the ciphered images.....	34
Figure 6. Correlation plots of two adjacent pixels of R, G, and B channels of the original color image <i>Lena</i> from the first to third column illustrates: the vertical, diagonal, and horizontal adjacent pixels of each channel respectively. ....	38
Figure 7. Correlation plots of two adjacent pixels of R, G, and B channels of the ciphered <i>Lena</i> image: from the first to third column illustrates the vertical, diagonal, and horizontal adjacent pixels of each channel, respectively. ....	39
Figure 8. Slat and Peppers analysis of Deblur image: first row (a-d) Deblur ciphered image with salt and peper variance 0.0005, 0.005, 0.05 and 0.5; second row (e-h) corresponding deciphered images	41
Figure 9. Gaussian analysis of Deblur Image: first row (a-d) Deblur ciphered image with salt and peper variance 0.0004, 0.0003, 0.0002 and 0.0001; second row (e-h) corresponding deciphered images .....	42
Figure 10. Occlusion attack: first two rows (a-e) Occluded ciphered images; last two rows (i-p) Deciphered images corresponding to occluded ciphered images.....	43
Figure 11. Chapter description (Flowchart).....	48
Figure 12. (a)-(b) show the clear picture of pointwise dissimilarity between consecutive rows and columns. (a) first 1360 random stream of consecutive rows (b) Representatives of each IPRNS on consecutive indexes. ....	55

## List of Tables

Table 1. Points on elliptic curve over finite field $F_{17}$ .....	10
Table 2. Points on elliptic curve over finite field $F_{13}$ .....	12
Table 3 The S-box $S_{0,2,25785,49}$ based on the proposed method.....	25
Table 4. Non-linearity of some existing and proposed S-boxes .....	25
Table 5. Comparison of experimental results of the proposed S-boxes with standard S-boxes .....	27
Table 6. Comparison for the entropy results of the ciphered images.....	35
Table 7. Statistical analysis of the proposed scheme with some existing techniques .....	36
Table 8. Comparison of correlation coefficient results of the proposed scheme with some existing techniques in three layers .....	37
Table 9. Comparison of NPCR and UACI analysis results of the proposed scheme with some existing techniques .....	40
Table 10. UACI, NPCR, MSE and PSNR scores of proposed schemes .....	44
Table 11: The proposed S-box $S_{(460,74)0,91,521}$ .....	52
Table 12. Results and comparisons with existing Substitution Boxes (S-boxes) .....	52
Table 13. NIST (800-22 test suit) results for ES-PRNS subgroup-based pseudo random number sequences .....	58
Table 14. NPCR and UACI numerical values and their comparison.....	70
Table 15. Entropy numerical values and their comparison.....	71
Table 16. Comparison of correlation coefficient results of the proposed scheme with some existing techniques in three layers .....	72
Table 17. Sample S-boxes.....	78
Table 18. Security analysis of the proposed S-boxes.....	80
Table 19. Graphical representation of indexing technique (IT) .....	80
Table 20. Simulation results of PRNM by the NIST testing suit.....	82
Table 21. Time comparison of proposed technique with existing techniques w.r.to point generation. 83	
Table 22. Entropy, NPCR and UACI results of All-White and All-Black images .....	89
Table 23. Entropies, Correlations Coefficients, NPCR and UACI values .....	90
Table 24. Comparison table for second order statistics and entropy with that of recent schemes .....	90

## List of Abbreviations

ECC	Elliptic curve cryptography
PRNG	Pseudo random number generator
PRNs	Pseudo random numbers
S-box	Substitution box
SM	S-box Module
PRNS	Pseudo random number sequences
ECS-PRNSM	Elliptic curve subgroup PRNS module
IECS	Isomorphic elliptic curves
MS	Mechanism for S-box
SCM	S-box construction mechanism
PRNGM	PRN generation mechanism
GWE	Generalized Weiestrass-equation
IPRNS	Independent pseudo random number sequences
MM	Mathematical model
EC-PG	Elliptic curve point group
GL-OT	Group law operating tool
RA	Recursive approach
IT	Indexing technique

# Chapter 1

## Introduction and Preliminaries

### 1.1 Introduction

This chapter is mainly devoted to the major concepts, namely elliptic curve (EC) and cryptography. The fundamental elements of both EC and cryptography are thoroughly presented separately. In addition, we will discuss some EC based cryptographic algorithms to validate the importance of EC structure in cryptography.

This introductory chapter consists of five sections. In section 1.2, we discuss the detail of elliptic curve and related results while section 1.3, presents the importance of EC in cryptography and discuss some well-known symmetric and asymmetric algorithms. In section 1.4, the theory of substitution box is briefly discussed. The next section 1.5, of this chapter consists of our main objectives while in section 1.6, we demonstrate our own contribution to this dissertation.

### 1.2 Elliptic Curve

An elliptic curve  $E_{a_1, a_2, a_3, a_4, a_5}$  defined over a prime field  $L$ , is an algebraic expression of the form

$$y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_5 \quad (1)$$

Where  $a_1, a_2, a_3, a_4, a_5, x, y \in L$ . The set of all solutions  $(x, y)$  to the equation (1) are the points of the ring  $L \times L$ . Apart from that, a point at infinity " $O$ " is added to the set of solutions and refer this elliptic curve as  $E_{a_1, a_2, a_3, a_4, a_5}^{|L|}$ . Generally, this elliptic curve is known as Generalized Weiestrass-equation (GWE). Furthermore, it is preferable to consider GWE while working with the fields having characteristics 2 or 3. Considering a field of characteristic other than  $\text{char} \neq 2, 3$ , the equation (1) can be transformed initially to the form  $y'^2 = x^3 + a'_1x^2 + a'_2x + a'_3$  by making substitutions  $y' = y + \frac{a_1x + a_2}{2}$ ,  $a'_1 = a_3 + \frac{a_1^2}{4}$ ,  $a'_2 = a_4 + \frac{a_1a_2}{2}$  and  $a'_3 = a_5 + \frac{a_2^2}{4}$ . Finally, we get  $y'^2 = x'^3 + Ax' + B$  by using  $x' = x + \frac{a'_1}{3}$ . This equation  $y'^2 = x'^3 + Ax' + B$  is named as Weiestrass-equation (WE). Besides, for WE to get the representation of an elliptic curve, the expression on the right hand of WE must

have distinct roots. This means that the cubic  $x'^3 + Ax' + B$  has non-zero discriminant (that is:  $4A^3 + 27B^2 \neq 0$ ).

### 1.2.1 Elliptic Curve Points Arithmetic

Here we may develop the intrinsic model of EC structure with the help of utmost two points lying on EC and generate another point [1]. The description of this process is examined in more detail.

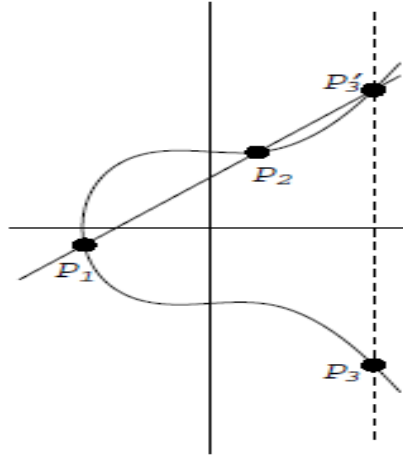


Figure 1. Point Doubling

For any two points  $P_1 = (x_1, y_1)$ ,  $P_2 = (x_2, y_2)$  on EC represented by the equation  $y^2 = x^3 + ax + b$ . Then the sum  $P_1 + P_2 = P_3 = (x_3, y_3)$  is also an element on EC by drawing a line  $l$  through  $P_1$  and  $P_2$ . It could be observed that  $l$  passes through third point  $P_3'$  on EC. Finally, the reflection of  $P_3'$  along  $x$ -coordinate generates  $P_3$  which is the sum of  $P_1$  and  $P_2$  as shown in Figure 1. Since the sum is not a usual addition of pairs. Therefore, it might be suitable to denote this sum by  $P_1 \oplus P_2$ . Initially we assume that  $P_1 \neq P_2$  with  $P_1$  or  $P_2 \neq \infty$ . Draw a line  $l$  that passes through both points  $P_1$  and  $P_2$ . The slope of  $l$  is

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

Now, we obtain the sum  $P_1 \oplus P_2$  by the following expression

$$P_3 = (\lambda^2 - x_1 - x_2, \quad \lambda(x_1 - x_3) - y_1)$$

If  $P_1 = P_2 = (x_1, y_1)$  and  $y_1 \neq 0$ , then the sum  $P_1 \oplus P_2$  is obtained as

$$(\lambda^2 - 2x_1, \lambda(x_1 - x) - y_1)$$

Whereas  $\lambda$  is the slope at  $P$ . The mathematical expression for  $\lambda$  is given below

$$\lambda = \frac{3x_1^2 + a}{2y_1}$$

If  $P_1 = P_2 = (x_1, y_1)$  and  $y_1 = 0$ , then the sum  $P_1 \oplus P_2$  is considered as  $\infty$ .

Furthermore, define

$$P \oplus \infty = P, \text{ for all } P \in E_{a,b}^{|L|}.$$

This sum of points looks a little bit unnatural. But we might show that it satisfies some nice properties. The following steps describe the main properties.

1. For any  $P_1, P_2 \in E_{a,b}^{|L|}$  implies that  $P_1 \oplus P_2 \in E_{a,b}^{|L|}$  (closed under “ $\oplus$ ”).
2. For any  $P \in E_{a,b}^{|L|}$ ,  $P \oplus \infty = P$  (existence of identity).
3. Given  $P$  on  $E_{a,b}^{|L|}$ , there exists a unique point  $P'$  on  $E_{a,b}^{|L|}$  such that  $P \oplus P' = \infty$ . The point  $P'$  is normally denoted  $-P$  (existence of inverses).
4. For all  $P_1, P_2, P_3 \in E_{a,b}^{|L|}$ ,  $(P_1 \oplus P_2) \oplus P_3 = P_1 \oplus (P_2 \oplus P_3)$  (associativity).
5. For all  $P_1, P_2 \in E_{a,b}^{|L|}$ ,  $P_1 \oplus P_2 = P_2 \oplus P_1$  (commutativity).

In short, the set of all points on  $E_{a,b}^{|L|}$  form an abelian group under “ $\oplus$ ” with identity element  $\infty$ .

### 1.2.2 Elliptic Curves and Finite Fields

In the above discussion, we have been defined an elliptic curve over arbitrary fields, but the field of finite size is the principal component for area of cryptography and its applications. Assume the elliptic curve  $E_{a,b}^p$  over some finite field of size  $p$ ,  $F_p$ . As the size of  $F_p$  is finite, so the resulting group  $E_{a,b}^p(F_p)$  also contains finite number of points.

One procedure of finding  $E_{a,b}^p(F_p)$  is through brute force. First, we generate a set of quadratic residues (square element) in the field  $F_p$ , denoted by  $\mathbb{Q}(F_p)$ . It is pertinent to mention that there are exactly half of the square elements in any finite field of characteristic greater than 2, as discussed in [2]. This deduces from the fact  $\mathbb{Q}: F_p \rightarrow F_p$  defined by  $\mathbb{Q}(x) = x^2$ . Particularly, the mapping  $\mathbb{Q}$  is a group homomorphism with kernel  $\{-1, 1\}$ .

After getting the list of square elements, we proceed towards computing  $f(x') = x'^3 + Ax' + B$  for each  $x' \in F_p$ . Each value  $f(x') \in \mathbb{Q}$  then produce  $\pm y$  satisfying  $y^2 = f(x')$ .

**Example 1.1:** Let  $E_{1,2}^{17}$  be an elliptic curve with  $y'^2 = x'^3 + x' + 2$ . We first construct a list of quadratic residues of  $F_{17}$  denoted by  $\mathbb{Q}(F_{17})$  with minor calculations as under.

$$\mathbb{Q}(F_{17}) = \{1, 2, 4, 8, 9, 13, 15, 16\}$$

We write values of  $x$ , solving  $x^3 + x + 2 \pmod{17}$  for  $x$  selecting only the ones which gives values from  $\mathbb{Q}(F_{17})$ .

Table 1. Points on elliptic curve over finite field  $F_{17}$

$x'^3 + x' + 2 \text{ mod } 17$	$y^2 \text{ mod } 17$
2	0
4	1
12	4
15	9
2	16
13	8
3	2
12	15
12	13
9	13
9	15
1	2
8	8
2	16
6	9
9	4
0	1

The above Table 1, gives us 24 different points including point at infinity ' $\infty$ '. We then say that size of  $E_{1,2}^{17}(F_{17})$  is 24.

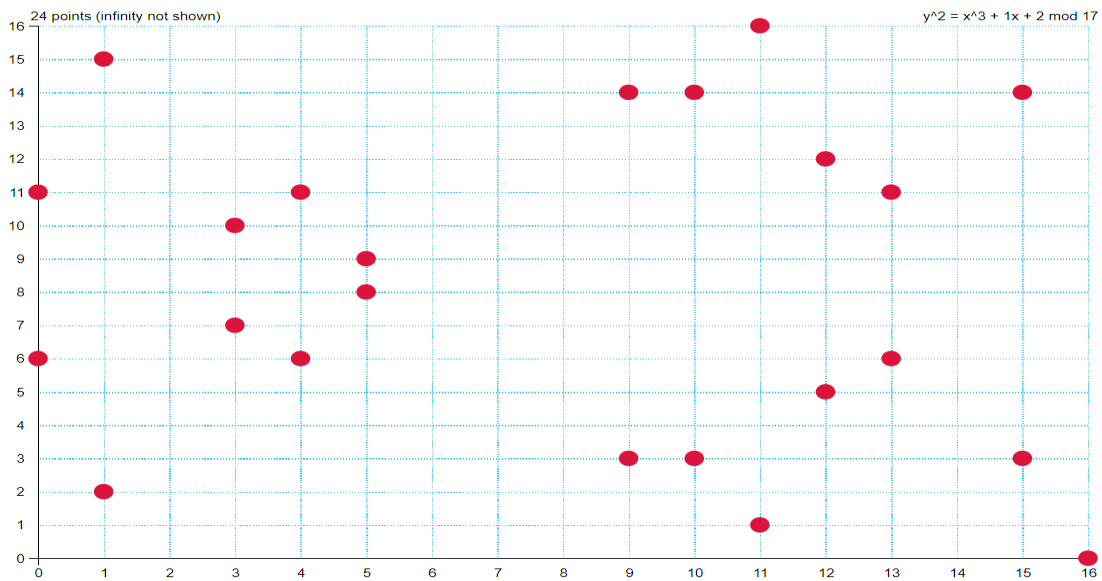


Figure 2. Graphical interpretation of  $E_{1,2}^{17}(F_{17})$



Since the characteristic of field  $F_{17}$  is neither 2 nor 3, the points of  $E_{1,2}^{17}(F_{17})$  can be easily added using formula given in section 1.2. All arithmetic in addition should be made within the given field.

### 1.2.3 Some Definitions and Results

The main results that are useful for determining the total number of points on elliptic curve over finite field.

**Theorem 1.1.** [[1], Theorem 4.1] Let  $E_{a,b}^q$  be an elliptic curve, defined on the field  $F_q$  with finite size  $q$ . Then either  $E_{a,b}^q(F_q) \cong Z_n$  or  $E_{a,b}^q(F_q) \cong Z_{n_1} \oplus Z_{n_2}$  for some positive integer  $n$ , or for some integers  $n_1, n_2 \geq 1$  with  $n_1$  dividing  $n_2$ .

**Theorem 1.2.** [[1], Hasse's Theorem] Let  $E_{a,b}^q$  be an elliptic curve the field  $F_q$  of finite size  $q$ . Then the order of  $E_{a,b}^q(F_q)$  satisfies the following relation  $|q + 1 - \#E_{a,b}^q(F_q)| \leq 2\sqrt{q}$ .

**Lemma 1.1.** [[1], Lemma 4.33] An elliptic curve  $E_{0,b}^p$  over a prime field  $F_p$  with  $p - 2 \equiv 0 \pmod{3}$  has exactly  $p + 1$  distinct points, where each integer in the field  $F_p$  appear once as  $y$ -coordinates.

**Theorem 1.3.** [[3], Example 9.5.2] Let  $p > 2$  be any prime integer and  $E_{a,b}^p : y'^2 = x'^3 + ax' + b$  is an elliptic curve over  $F_p$ . Then  $E_{a,b}^p$  is not isomorphic to  $E_{a',b}^p$ , with  $a' = t^2a$  and  $b' = t^3b$ ; for any  $t \in F_p^*$  if and only if  $t$  is non-square in  $F_p^*$ .

**Proposition 1.1.** [[4], page 230] If  $r/\text{ord}(G)$ , where  $G$  is a finite Abelian group, then there exists a subgroup of order  $r$  in  $G$ .

**Example 1.2:** Let's add the points (1,2) and (4,6). Before addition, we need to calculate  $\lambda$ , which can be computed as.

$$\lambda = \frac{6 - 2}{4 - 1} \equiv \frac{4}{3} \equiv 4 \times 6 \equiv 24 \pmod{17} \equiv 7$$

Now we may calculate the sum of (1,2) and (4,6)

$$x'_3 = 7^2 - 4 - 1 \equiv 49 - 4 - 1 \equiv 44 \pmod{17} \equiv 10$$

$$y'_3 = 7(1 - 10) - 2 \equiv 7 \times -9 - 2 \equiv -65 \pmod{17} \equiv 3$$

Hence, the sum  $(1,2) \oplus (4,6) = (10,3)$ .

Similarly, the point (5,8) is one of the generators of  $E_{1,2}^{17}(F_{17})$ :

$$\begin{aligned}
 P &= (5,8), 2P = (3,10), 3P = (10,14), 4P = (15,14), 5P = (13,11) \\
 6P &= (1,11), 7P = (9,3), 8P = (12,5), 9P = (4,11), 10P = (0,11) \\
 11P &= (11,16), 12P = (16,0), 13P = (11,1), 14P = (0,6), 15P = (4,6) \\
 16P &= (12,12), 17P = (9,14), 18P = (1,15), 19P = (13,6), 20P = (15,3) \\
 21P &= (10,3), 22P = (3,7), 23P = (5,9), 24P = \infty
 \end{aligned}$$

Thus, it is revealed that  $E_{1,2}^{17}(F_{17})$  is cyclic group generated by (5,8) whose order is 24. It is worth noting that not every elliptic curve over finite fields generates cyclic groups, as we show in the following example:

**Example 1.3:** Consider the elliptic curve  $E_{0,10}^{13} y'^2 = x'^3 + 10$  over finite field  $F_{13}$ . Clearly,  $\mathbb{Q}(F_{13}) = \{1,4,9,3,12,10\}$ , then from Table 2.

$$E_{0,10}^{13}(F_{13}) = \{\infty, (0,6), (0,7), (4,3), (4,10), (10,3), (10,10), (12,3), (12,10)\}$$

Since the number of points in  $E_{0,10}^{13}(F_{13})$  are 9. It is evident that either  $E_{0,10}^{13}(F_{13}) \cong \mathbb{Z}_9$  or  $E_{0,10}^{13}(F_{13}) \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3$ . After computation we conclude that:

Table 2. Points on elliptic curve over finite field  $F_{13}$

$x'^3 + 10 \text{ mod } 13$	$y'^2 \text{ mod } 13$
0. 10	0. 0
1. 11	1. 1
2. 5	2. 4
3. 11	3. 9
4. 9	4. 3
5. 5	5. 12
6. 5	6. 10
7. 2	7. 10
8. 2	8. 12
9. 11	9. 3
10. 9	10. 9
11. 2	11. 4
12. 9	12. 1

$$\begin{aligned}
1(0,6) &= (0,6), & 2(0,6) &= (0,7), & 3(0,6) &= \infty \\
1(4,3) &= (4,3), & 2(4,3) &= (4,10), & 3(4,3) &= \infty \\
1(10,3) &= (10,3), & 2(10,3) &= (10,10), & 3(10,3) &= \infty \\
1(12,3) &= (12,3), & 2(12,3) &= (12,10), & 3(12,3) &= \infty
\end{aligned}$$

Furthermore, the calculations show that all elements without identity have order 3, as a result  $E_{0,2}^{13}(F_{13}) \cong Z_9$  (as  $Z_9$  is cyclic group). Consequently,  $E_{0,2}^{13}(F_{13}) \cong Z_3 \oplus Z_3$ .

**Definition 1.1:** [[3], page 144] Let  $(E_{a_1, b_1}^p, \infty_{E_1})$  and  $(E_{a_2, b_2}^p, \infty_{E_2})$  be elliptic curves over prime field  $F_p$ . An isomorphism of elliptic curves

$$\theta: E_{a_1, b_1}^p \rightarrow E_{a_2, b_2}^p$$

The mapping  $\theta$  is an isomorphism over  $\overline{F_p}$  of algebraic varieties such that  $\theta(O_{E_1}) = O_{E_2}$ . If there is an isomorphism between  $E_{a_1, b_1}^p$  and  $E_{a_2, b_2}^p$ , then we write  $E_{a_1, b_1}^p \cong E_{a_2, b_2}^p$ .

**Definition 1.2:** [[3], page 144] Let  $E_{a_1, b_1}^q$  be an elliptic curve over  $F_q$ . An elliptic curve  $E_{a_2, b_2}^p$  over  $F_q$  is called a twist of  $E_{a_1, b_1}^q$ , if there is an isomorphism  $\theta: E_{a_1, b_1}^q \rightarrow E_{a_2, b_2}^p$  over  $\overline{F_q}$  of pointed curves, such that  $\theta(\infty_{E_1}) = \infty_{E_2}$ . If there is an isomorphism between elliptic curves  $E_{a_1, b_1}^q$  and  $E_{a_2, b_2}^q$  over  $F_q$ , then  $E_{a_1, b_1}^p$  and  $E_{a_2, b_2}^p$  of  $E_{a, b}^p$  are called equivalent twists.

**Definition 1.3:** [[3], page 140] Let  $E_{a, b}^p$  be an elliptic curve over finite field  $F_p$  and let for any  $Q \in E_{a, b}^p(F_p)$ . We define

$$\begin{aligned}
\tau_Q: E_{a, b}^p &\rightarrow E_{a, b}^p \\
\tau_Q(P) &= P + Q; \forall P \in E_{a, b}^p
\end{aligned}$$

Clearly the map  $\tau_Q$  is bijective.

**Theorem 1.4.** [[3], page 144] Let  $p > 2$  be any prime integer and  $E_{a, b}^p: y'^2 = x'^3 + ax' + b$  is any elliptic curve over  $F_p$ , such that  $t \in F_p^*$ . Then the twist  $E_{t, a, b}^p \cong E_{a, b}^p$  if and only if  $t$  is non-square in  $F_p^*$ . Furthermore, if  $t_1$  and  $t_2$  are non-squares in  $F_p^*$ , then  $E_{t_1, a, b}^p \cong E_{t_2, a, b}^p$  over  $F_p$ .

### 1.3 Elliptic Curves and Its Cryptographic Applications

In recent decades, data security gets more and more attention due to rapid advancement in the fields of communication technology and computer vision. The tools used to protect the contents of the data from the access of adversaries during transmission is cryptography. The

security aspect of the secret data entirely depends on the designing procedure of the cryptographic scheme. To design efficient cryptographic scheme, many researchers prefer to construct crypto algorithms rely on mathematical structures. Due to their highly sensitive and random natures, the non-linear dynamical systems are the best choices for the researchers [5]–[8]. These systems have wide range of applications in multimedia data security. In some systems such as chaotic systems, the security risk and computational efforts are depended to some extent on their dimensions. High dimensional chaotic systems are considered secure as compared to low dimensional chaotic system. However, in respect to computational complexity, these require more calculation time in the designing of cryptosystems. Besides, low dimensional chaotic systems are apparently more at risk against cryptanalysis attacks due to small key space [9].

On the other hand, elliptic curve EC structures are found better to resolve the above issues in respect of randomness [10]. With the help of the EC core structure, the level of randomness and uncertainty in the output data can be increased for security insurance in either of the asymmetric or symmetric encryption algorithms. The most well-known EC based asymmetric or public key algorithms are RSA, El Gamal Public Key Encryption, Elliptic curve Diffie Hellman key exchange, Elliptic curve Digital Signature Algorithm. Some of them are discussed as following:

### 1.3.1 RSA

In cryptography we often consider two imaginary people, Alice, and Bob. They both communicate over open channel for sharing secret information. In this connection, Alice needs to forward secret information to Bob. Before this, Bob secretly selects two prime numbers  $p, q$  and from their product we obtain  $n = pq$ . Furthermore, Bob also selects an integer  $e \in Z_m$  such that there exists  $d \in Z_m$  with  $ed \equiv 1(\text{mod } m)$  where  $m = (p - 1)(q - 1)$ . He then makes  $e, n$  public and holds  $d$  secret. Alice's wants to send a secret message  $M$  (A number)( $\text{mod } n$ ). She calculates  $t \equiv M^e(\text{mod } n)$  and forwards  $t$  to Bob. After receiving the message  $t$  Bob calculates  $M \equiv t^d(\text{mod } n)$ . If Eve could trace  $p$  and  $q$ , then she could easily find  $d$  such that  $ed \equiv 1(\text{mod } (p - 1)(q - 1))$ . The security of this algorithm is mainly concerned to the factorization of  $n$ . This analogue can also be used using elliptic curve. In this connection Koyama-Maurer-Okamoto- Vanstone present one such algorithm which is not normally used in practice.

Alice needs to send a secret message to Bob. They adopted the following procedure:

- i. First, Bob selects two distinct large prime numbers  $p_1, p_2$  with the condition  $p_1 \equiv p_2 \equiv 2 \pmod{3}$  and calculates  $n = pq, m = (p + 1)(q + 1)$
- ii. Bob picks an integer  $e$  such that  $es \equiv 1 \pmod{\text{lcm}(p + 1, q + 1)}$ ; for some integer  $s$ .
- iii. Bob publishes  $e$  and  $n$  publicly and keeps  $(s, p, q)$  private.
- iv. Alice considers her secret message as a pair of integers  $(M_1, M_2) \pmod{n}$ . She considers  $(M_1, M_2)$  as a point  $M$  lying on the elliptic curve  $E_{0,b}^n$  defined by  $y'^2 = x'^3 + b$   
Where  $b = M_2^2 - M_1^2 \pmod{n}$ .
- v. Alice adds  $M$   $e$  times with the formulas for elliptic curve group law on  $E_{0,b}^n$  to get  $T = (t_1, t_2) = eM$ . She forwards  $T$  to Bob.
- vi. Bob calculates  $M = sT$  on  $E_{0,b}^n$  to get  $M$ .

In case eavesdropper factors  $n$  as  $pq$ , then she computes  $(p + 1)(q + 1)$  without any hurdle, therefore, she could easily find  $s$  which satisfies  $es \equiv 1 \pmod{(p + 1)(q + 1)}$ . Hence, she could decrypt the encrypted Alice's message.

### 1.3.2 El Gamal Public Key Encryption

Alice wants to forward a secret data to Bob. First, Bob generates his public encryption key by the following procedure:

He selects an elliptic curve  $E_{a,b}^p$  over a finite field  $F_p$  such that the DLP (Discrete log problem) is hard for  $E_{a,b}^p(F_p)$ . He picks a point  $Q$  on  $E_{a,b}^p$  of large prime. He also picks a secret integer  $r$  and calculates  $B = rQ$ . Bob publishes the elliptic curve  $E_{a,b}^p$ , the field  $F_p$ , and the points  $Q, B$  a public encryption key, which are used by Alice. Bob keeps the integer  $r$  secret.

Alice adopts the following steps while sending a message to Bob.

- i. Downloads Bob's public encryption key.
- ii. Arrange her secret message as a point  $M \in E_{a,b}^p(F_p)$ .
- iii. Select a private random integer  $d$  and calculate  $m_1 = dQ$ .
- iv. Computes  $m_2 = dB + M$ .
- v. Forwards  $m_1, m_2$  to Bob.

Bob decrypts the encrypted message by computing

$$M = m_2 - rm_1$$

This decryption process is meaningful because

$$m_2 - rm_1 = (dB + M) - r(dQ) = M + d(rQ) - d(rQ) = M$$

The Eve knows Bob's public encryption key and the points  $m_1, m_2$ . If Alice can compute discrete logarithm, she is able to find  $r$  using  $Q, B$ , which she can then easily manage to decrypt the cipher message as  $m_2 - rm_1$ . Moreover, she can also find  $d$  by using  $Q$  and  $m_1$ . As a result, she can compute  $M = m_2 - dB$ . If Alice cannot compute discrete logarithm, it will seem infeasible for her to compute  $M$ .

It is notable for Alice to choose distinct random integers  $d$  each time while sending a secret message to Bob. Otherwise, Eve can recognize the message because then  $m_1 = m_1'$ . She then calculates  $m_2' - m_2 = M' - M$ .

#### 1.4 Substitution Boxes

In cryptography, S-boxes are normally the main non-linear component in various cryptographic encryption schemes. Particularly these play an important role in ensuring the security strength of scheme. It is known that practically efficient S-box need to have some Cryptographic properties. Cryptographic properties and designing of S-box can be made possible by using vector Boolean functions. An S-box, or cryptographic S-box, is a function that takes an input (string) of length  $s$  and outputs (string) of length  $t$ . In other words, an S-box is a mapping  $S(x)$  from  $GF(2^s)$  to  $GF(2^t)$ . For this sake, an S-box can also be referred as  $(s, t)$ -Boolean function. More precisely, we may use S-boxes and  $(s, t)$ -Boolean functions interchangeably. It is noted that an  $(s, t)$ -Boolean function could always be represented as the  $t$ -Boolean functions, and we can write

$$S(x) = [s_1(x), s_2(x), \dots, s_t(x)]$$

Where each  $s_j$ , is a Boolean function in  $s$  variables. These  $s_j$  are the coordinate functions of  $S(x)$ . Security strength of an S-box is usually expected to possess the property that any part of its output provides no meaningful pattern about the other part (bits) of the output. Specifically, the  $(s, t)$ -Boolean function that describes an S-box has the characteristic that the  $t$  outcome functions  $s_1(x), s_2(x), \dots, s_t(x)$ , are statistically mutually independent. If an S-box is bijective that is one-to-one and onto. That means every input uniquely mapped to the possible outcome in S-box. In symmetric key cryptosystems the bijective S-boxes play significant role regarding security aspect.

For the evaluation of cryptographic properties of an S-box, we use some standardized statistical analysis such as nonlinearity (NL), bit independent criteria (BIC), linear approximation probability (LAP), strict avalanche criteria (SAC), and differential approximation probability (DAP)

which examine the efficiency and strength of S-box. In the next chapter, all the above-mentioned tests are discussed in detail.

Likewise, Fathi et al. [6] proposed PRNs generated scheme rely on ECC for image encryption. They discussed the applications in the back-door problems efficiently. Elliptic curve-based cryptography was first introduced in 1985 by Koblitz [11] and Miller [10]. Reyad et al. [14] encrypted the original image through Koblitz encoding algorithm and Chaos-Driven elliptic curve PRNGs (C-D ECPRNG). In [11], the author made a connection between the discrete logarithm problem (DLP) and EC. Since then, many researchers made their efforts to employ ECC using various encryption techniques to enhance its performance. Later on, Amara et al. [15] showed that the ECC based cryptosystem provide better security than RSA. In [6], a technique for an image encryption is established that utilizes a combination of Elliptic Curve Based Random Number Generator (EC-B-RNG) and AES (Advanced Encryption System). Accordingly, the scheme gets better results for image encryption. In this method, the PRNs are computed followed by public shared key and the base point of the elliptic curve group. Then, AES algorithm is performed to complete the encryption. In this algorithm, one party can send a key to an authorized party few days in advance. Then, whenever they send secret information through encryption algorithm, they both could read using that key. Although it is not applicable in each situation. Similarly, the asymmetric algorithm or public key encryption, both parties are not bound to have contact in advance. In this case, one party communicates publicly the public encryption key, which the other authorized party uses. He also must have a private key for decryption which is organized in advance to decrypt encrypted message. Though, the encryption key is known to everyone, but it is not feasible to detect the decryption key. In this connection many researchers used various mathematical structures such as chaotic systems [16]–[25] and encryption using the elliptic curve (EC) [6], [26]–[31]. Elliptic curve-based algorithms are most used to provide more security to the information. Here, we shall focus our attention on elliptic curve cryptography (ECC) using different techniques suggested by many researchers. The first proposed scheme to employ the elliptic curve as a public key cryptosystem was designed in 1985 by Miller [12] and independently by Koblitz [11]. Later on, the significant advantages of (ECC) on which researchers are being attracted, where power consumption or bandwidth and storage is of prime objective [32]. These aspects enhance our attention to use the elliptic curve as a foundation for image encryption.

In general, public key or asymmetric algorithms are slower as compared to efficient symmetric algorithms. Therefore, a public key algorithm is normally used to generate a key

which is then managed to use in a symmetric algorithm. The speed of algorithm is much important when large amounts of data is being transmitted. With this in mind, we now turn our attention to what we hope to accomplish in this dissertation.

## **1.5 Objectives**

The main objectives are listed below:

- a) In this study, we will be present an innovative use of the Elliptic curve over prime field for the construction of various cryptographic schemes and will be improve the security of the existing cryptographic algorithm.
- b) Elliptic curve over prime field will be solved and apply some suitable mathematical operations or structures on the points of the given elliptic curve for the construction of efficient nonlinear component of block cipher.
- c) Analyze the proposed substitution box through various standard security performance tests.
- d) Show the strength of the newly generated S-boxes based on the experimental tests when compared to S-boxes generated using various mathematical structures.
- e) The pseudo random numbers are generated to create diffusion using elliptic curve over another prime field.
- f) Both confusion and diffusion phases depend on various parameters preferably distinct.
- g) Application of above-mentioned points in (image/audio/video encryption) cryptography, steganography, and digital watermarking.
- h) Some standard performance evaluation metrics are performed on encrypted data to conclude the efficiency of the proposed scheme.

### **1.5.1 Elliptic Curve Diffie Hellman Key Exchange**

Alice and Bob both agree on a fixed key that they can utilize for sharing secret data through a symmetric encryption algorithm such as AES or DES. Assume that Alice and Bob are considered as banks that want to share secret financial information. It is unfeasible to share a secret key through courier service. It is further assumed that Alice and Bob have not prior contact and they only communicate through public channels. In this way the secret key can be established by the following procedure, due to Diffie-Hellman (The process is based on the set of non-zero elements of finite field).



- 1) Both Alice and Bob agree on choosing an elliptic curve over a finite field  $F_{p^s}$  such that the discrete logs problem is hard to compute in  $E_{a,b}^{p^s}(F_{p^s})$ . They also agree on a point  $Q$  in  $E_{a,b}^{p^s}(F_{p^s})$  whose order is large prime.
- 2) Alice selects a secret random integer  $a$ , calculates  $Q_a = aQ$ , and sends  $Q_a$  to Bob.
- 3) Bob selects a secret random integer  $b$ , calculates  $Q_b = bQ$ , and sends  $Q_b$  to Alice.
- 4) Alice calculates  $aQ_b = abQ$ .
- 5) Bob calculates  $bQ_a = baQ$ .
- 6) Alice and Bob agree on procedure which is used to extract encryption/decryption key from  $abQ$ . For instance, they could either extract the last 256 bits from  $x$ -coordinate of  $abQ$  as the key or by using a hash function at the  $x$ -coordinate.

The only public information that the eavesdropper Eve could see, is the elliptic curve  $E_{a,b}^{p^s}$ , the finite field  $F_{p^s}$ , and the point  $Q$ ,  $aQ$ , and  $bQ$ . She must need to compute  $abQ$ .

While in symmetric algorithm, the key is same for both encryption and decryption process. One of the most Popular EC based symmetric algorithms are the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES, normally referred as Rijndael algorithm). Both DES and AES depend on the S-box. S-boxes are widely used in modern cryptographic algorithms. It plays important role in furnishing the non-linearity of the cryptosystem. Consequently, the chance of any attack is reduced as well as meaningful patterns in the ciphered data. Therefore, the construction of efficient S-boxes is prime feature for successful cryptographic application. The core idea behind S-box is the Boolean function's structure which comprises of Boolean operations (XOR and OR). In the following we present a brief introduction of Boolean function and its application in S-box theory.

**Definition 1.4:** Let  $GF(2^s)$  be an  $s$ -dimensional vector space over the binary field  $F_2$ . A Boolean function  $\beta$  is mapping:

$$\beta: GF(2^s) \mapsto GF(2)$$

$GF(2^s)$  stands for the Galois field with  $2^s$  points of the form  $b = (b_1, \dots, b_s)$ . Since the total number of points in the domain  $GF(2^s)$  and codomain  $GF(2)$  are  $2^s$  and 2 respectively. So, the total number of distinct ( $s$ -variable) Boolean functions is  $2^{2^s}$ .

## 1.6 Own Work

This thesis is divided into the following chapters.

1. In the second chapter, we propose an efficient technique for strong S-box based on squared and non-squared elements using isomorphic elliptic curves over finite fields

and present their security performance by evaluating some metrics. Moreover, the PRNs are generated over non isomorphic ECs using translation map.

2. Chapter 3 consists of the application of S-box and PRNS in the image data security. For this purpose, we shall make use of EC permutations to permute substituted images. Moreover, the security analyses results and computer simulation outputs of the proposed encryption algorithm are examined. In addition, we discuss the comparison and some conclusive remarks on image encryption algorithm.
3. In Chapter 4, we establish a technique based on EC core operations that effectively generates dynamic S-boxes and PRNS. The mechanism of both S-box and PRNS are separately operated over EC subgroup coset model with distinct technique. The efficiency of subgroup coset model is verified through statistical analysis of S-box and PRNS. As both S-box and PRNS algorithms generates verified PRNS and S-boxes.
4. Chapter 5 deals with the atypical well-defined mathematical model for its application to image data encryption. We jointly manage both S-box and subgroup coset modules to formalize diffusion. Consequently, it will be the main source of the proposed scheme for diffusing all kind of multimedia data having any dimension. Generally, multiple sequences and S-boxes are mainly generated to cipher multiple data files simultaneously. Several statistical tests revealed that the proposed technique is suitable for various cryptographic applications.
5. In Chapter 6, the efficient multiple pseudo-random numbers and S-boxes are established which are significant building blocks jointly adopted for image data security. Multiple aspects pave the way to handle large-scale multimedia data. For this achievement, we exploited an indexing technique over elliptic curves to introduce a computationally efficient mechanism for multiple PRNS and S-boxes. The statistical results will also show that the proposed S-box mechanism is the most effective method for generating strong multiple S-boxes on minimum prime fields. Furthermore, the experimental results will show that the proposed algorithm provides desired key-space and less computational effort.
6. This dissertation closed with Chapter 7, which consists of the conclusion of this dissertation with future directions.

## Chapter 2

# A Novel Approach Towards S-box and PRNs over Elliptic Curve

In this chapter, we have suggested an improved scheme using S-box, pseudo-random numbers generator (PRNG), and action of permutation over different prime fields. The proposed S-box depends only on  $y$ -coordinates by applying modulo operation of all isomorphic elliptic curves (IECS) to any fixed elliptic curve over one of the prime fields. The proposed work is novel in the sense that it gives us a guarantee to generate a dynamic S-box. Meanwhile, simple arithmetic operations are utilized in the generation of pseudo-random numbers (PRNs). In our proposed scheme, we use an elliptic curve which yields a permutation on the field, on which it is defined.

### 2.1 Motivation

Data transmission through any communication channel is a sensitive task securely. Before transmission, various techniques including S-box, chaotic maps in all three dimensions, and many more are being established to encrypt the digital data securely. The main source of secure information is lying under the scope of cryptography, steganography, and watermarking. The theme behind cryptography, steganography, and watermarking is to hide information from casual readers. In recent years, rapid development has been increasingly taken place in the field of digital information technology and multimedia data. With these advances, security has a key factor in sharing secret information which is not accessible for unauthorized persons. One of the reliable channels for this purpose is an image as a base, using standard-based cryptosystems. Images itself are very important, sending them in routine or unusual activity regarding personal, institutional, military circles, medical history, and so on.

The application of chaos theory played a significant role in the development of crypto algorithms using S-boxes, PRNs, and permutation maps to enhance diffusion and confusion [21]–[24], [33]–[35]. Belazi et al. [36], proposed a technique for the construction of an S-box via a chaotic sin map. The stated technique generates static S-box with minimum nonlinearity score 103 and maximum nonlinearity not greater than 108. Nonlinear dynamical systems are extensively used for multimedia data security [37]. These systems are further divided into two categories: one dimensional chaotic systems and high dimensional chaotic systems. Since

one-dimensional systems consist of less number of parameters and initial conditions. Therefore, the cryptanalyst can easily figure out the initial values and parameters used for encryption and decryption. Accordingly, the encryption schemes based on one-dimensional chaotic maps are considered insecure. Besides, the high dimensional chaotic based cryptosystems have large keyspace, exceeding dynamical behavior and ergodicity [21], [38], [39]. Thus, the encryption schemes based on high dimensional are considered more secure than the scheme based on a low dimensional scheme. However, due to the high computational complexity of the high dimensional, chaotic system makes their implementation on hardware-software costly.

On the other hand, elliptic curves group structures are much sensitive to input parameters similar to chaos-based structures, but it ensures more security by comparison with chaos. In [40], the author designed a hybrid cryptosystem based on AES and elliptic curve cryptography (ECC). The pseudo-random numbers are generated via EC points whereas encryption keys are achieved by the implementation of AES to pseudo-random numbers. The stated scheme provides more security but pseudo-random numbers are based on elliptic curve group law, which increases the computational cost of the encryption algorithm. The combination of a chaotic map and cyclic EC are used to design an encryption algorithm in [41]. In this scheme, the author overcomes the problem of small keyspace but is insecure against chosen-plaintext/known-plaintext attacks [40]. Similarly, an image encryption scheme in reference [28], generates pseudo-random numbers and S-box using EC, where the generation of S-box is not possible for each input EC, which is time-consuming.

## 2.2 Proposed S-boxes Based on IECS

In this study, we show the worth of isomorphic elliptic curves to any fixed EC in the construction of S-box. In [28], S-boxes are designed using total order relation and y-coordinates of any isomorphic elliptic curve corresponds to a fixed elliptic curve and showed that at most  $\frac{p-1}{2}$  S-boxes can be constructed. But we utilize all trivial twists of an elliptic curve over  $F_p$  to increase the quantity of efficient, cryptographically strong S-boxes up to  $(\frac{p-1}{2})^2$ .

**Definition 2.1:** Let  $E^{(a,b,p)}$ :  $y^2 = x^3 + ax + b$  be an elliptic curve over a finite field  $F_p$ . Suppose for any  $(x, y) \in E^{(a,b,p)}$ . Define a set

$$S^y = \{y_k: y_k = t_k^3 y; \forall t_k \in (F_p^*)^2, k = 1, 2, \dots, \frac{p-1}{2}\}$$

Then obviously for each  $y_k \in S^y$  there exists an isomorphic elliptic curve  $E^{(a,b,p)}$  to  $E^{(a',b',p)}$  such that  $(x_k, y_k) \in E^{(a',b',p)}$ ; with  $a' = t^2 a$  and  $b' = t^3 b$ ; for some  $t_k \in (F_p^*)^2$ . Also, for any  $(x_1, y_1), (x_2, y_2) \in E^{(a,b,p)}$  with  $y_1$  is squared and  $y_2$  is square free, which is given below.

$$S^{y_1} \cap S^{y_2} = \emptyset \text{ and } S^{y_1} \cup S^{y_2} = F_p^*$$

**Proposition 2.1:** Let  $E^{(a,b,p)}: y^2 = x^3 + ax + b$  be an elliptic curve over a finite field  $F_p$ . Then for any  $(x_1, y_1), (x_2, y_2) \in E^{(a,b,p)}$  with  $y_1$  is squared and  $y_2$  is square free,  $S^{y_1} \cap S^{y_2} = \emptyset$ .

*Proof:* Suppose  $S^{y_1} \cap S^{y_2} \neq \emptyset$ . Then there exist  $u \in S^{y_1} \cap S^{y_2}$ . such that  $u \in S^{y_1}$  and  $u \in S^{y_2}$ . So, by definition 2.1,  $u = t_1^3 y_1$  and  $u = t_2^3 y_2$ ; for some  $t_1, t_2 \in (F_p^*)^2$ . This means,  $t_1^3 y_1 = t_2^3 y_2$ . A contradiction as L.H.S is squared while R.H.S is square free. Hence  $S^{y_1} \cap S^{y_2} = \emptyset$ .

Furthermore, each element of  $S^y$  is lying on one of the elliptic curves, which are isomorphic to  $E^{(a,b,p)}$ .

**Proposition 2.2:** For any elliptic curve  $E^{(a,b,p)}: y^2 = x^3 + ax + b$  over a finite field  $F_p$  with odd prime  $p$ . Let  $(x_1, y_1), (x_2, y_2) \in E^{(a,b,p)}$  with  $x_1, y_1$  are squared and  $x_2, y_2$  are non-squared. If  $t_i^2 x_1 \neq t_j^2 x_2$  and  $t_i^3 y_1 \neq t_j^3 y_2$ . Then  $(t_i^2 x_1, t_i^3 y_1) \neq (t_j^2 x_2, t_j^3 y_2)$  for all  $t_i, t_j \in (F_p^*)^2$ .

**Proof:** Suppose

$$t_{j_1}^{-3} t_{i_1}^3 y_1 = y_2 \quad (1)$$

Implies

$$(t_{j_1}^{-1} t_{i_1})^2 x_1 = x_2 \quad (2)$$

And

$$(t_{j_1}^{-1} t_{i_1})^3 y_1 = y_2 \quad (3)$$

Which is not possible as L.H.S of equation (1) is multiple of squares while R.H.S is non-square. Similarly, in equation (2),  $t_{i_1}, t_{j_1}^{-1}$  are squares. (As inverse, product, any power of square element is square infinite field). So, L.H.S of equation (2) is squared, whereas R.H.S is non-squared. Hence  $t_i^2 x_1 \neq t_j^2 x_2$  and  $t_i^3 y_1 \neq t_j^3 y_2$ ;  $\forall t_i, t_j \in (F_p^*)^2$ .

**Corollary 2.1:** Let  $E^{(a,b,p)}: y^2 = x^3 + ax + b$  be an elliptic curve over a finite field  $F_p$ , where  $p > 257$  and  $(x_1, y_1), (x_2, y_2) \in E^{(a,b,p)}$  such that  $y_1$  is squared and  $y_2$  is non-squared in  $F_p^*$ . Then there is a substitution box  $S_{a,b,p}^{y_1, y_2}$  such that  $S_{a,b,p}^{y_1, y_2} = S^{y_1} \cup S^{y_2}$ .

**Proof:** Followed by Propositions 2.1 and 2.2.

Let  $E^{(0,b,p)}: y^2 = x^3 + b$  be an elliptic curve over the prime field  $F_p$ , where  $p \equiv 2 \pmod{3}$  and  $p > 3$ . The number of points on  $E^{(0,b,p)}$  are  $p + 1$  including  $O_E$  and no repetition occurs in  $y$ -coordinate (such that for each  $y_i \in F_p$ , there exists unique  $x_i \in F_p$  such that  $(x_i, y_i) \in E^{(0,b,p)}$ ). Let  $I = \{E^{(0,b',p)}: b' = t_k^3 b; \forall t_k \in (F_p^*)^2, k = 1, 2, \dots, \frac{p-1}{2}\}$  be the set of all elliptic curves which are isomorphic to  $E^{(0,b,p)}$  [1]. Then for any two  $(x_1, y_1), (x_2, y_2) \in E^{(a,b,p)}$  with  $y_1$  is squared and  $y_2$  is square-free in the field  $F_p$ . Then by Corollary 2.1, there exist two disjoint sets  $S^{y_1}$  and  $S^{y_2}$  which generate S-box  $S_{0,b,p}^{y_1, y_2}$  for instance  $S_{0,b,p}^{y_1, y_2} = S^{y_1} \cup S^{y_2}$ . Also, we note that the square element generates sets  $S^{y_1}$ , containing only squared elements while square free points generate sets  $S^{y_2}$  having square free elements. Besides, the same number of sets contains squared and square-free elements. Since all points of the field  $F_p$  appear only once on the  $y$ -coordinate of the elliptic curve  $E^{(0,b,p)}$ . One can obtain  $p$  number of such sets by the proposed technique. In this collection, half of the sets contain squared elements only and the remaining half contain square free elements. It follows that either two sets are disjoint or equal in the collection. To generate the proposed S-box, we can choose any two disjoint sets in the collection. It is observed that for each set  $S^{y_1}$  having squared entries there are  $\frac{p-1}{2}$  sets, containing square free elements in each set. Thus, the total numbers of S-boxes are  $(\frac{p-1}{2})^2$ . For instance, the S-box  $S_{0,b,p}^{y_1, y_2}$  constructed by the proposed scheme is shown in standard form  $16 \times 16$  look up Table 3.

### 2.3 Performance Analyses of the Generated S-box

In this section, we discuss the experimental results of randomly generated S-boxes based on the proposed technique. One can examine that the S-boxes generated by the proposed scheme are very efficient to use for secure communication. Here, we consider some S-boxes generated by the proposed technique and compare them with some existing S-boxes, presented in [6], [28], [42].

Table 3 The S-box  $S_{0,2,257}^{85,49}$  based on the proposed method

85	171	138	147	191	40	180	148	49	153	137	118	225	144	134	173
43	37	150	108	94	209	156	175	52	236	26	29	30	187	99	116
28	188	80	14	131	151	115	65	255	60	31	0	9	81	157	234
182	45	55	39	91	93	230	186	244	162	198	89	122	232	57	207
206	203	130	33	181	103	161	5	22	114	211	16	189	11	117	18
250	10	210	245	237	102	125	216	129	36	242	111	185	213	193	58
38	63	6	24	254	167	201	19	34	124	73	35	92	190	4	17
83	112	53	152	179	97	183	87	196	249	88	136	79	195	42	159
109	82	192	71	252	41	238	170	84	141	23	50	239	199	240	98
77	101	142	27	96	132	56	74	123	158	100	200	140	64	253	215
217	48	106	164	154	155	90	160	113	70	176	25	246	44	67	62
66	163	126	166	76	20	3	78	32	227	248	135	68	72	165	178
110	149	243	218	224	12	233	105	139	228	1	168	241	146	222	121
119	107	177	202	127	47	251	204	120	231	226	59	46	15	184	169
86	220	69	212	54	247	194	145	104	21	197	95	143	221	133	8
172	214	229	75	51	7	219	174	208	205	2	13	235	128	223	61

### 2.3.1 Nonlinearity (NL)

The key role of an S-box is to create confusion in the data up to the required level to keep safe from unauthorized people. The non-linearity security test is a metric which calculates the confusion ability of an S-box over  $GF(2^n)$ , which is defined as below.

$$N(S) = \min_{\xi, \zeta, \eta} \{ \alpha \in GF(2^n) \mid \xi \cdot S(\alpha) \neq \zeta \cdot \alpha \oplus \eta \}$$

Where  $\xi \in GF(2^n)$ ,  $\eta \in GF(2)$ ,  $\zeta \in GF(2^n) \setminus \{0\}$  and “ $\cdot$ ” is the dot product over  $GF(2)$ .

The upper bound for non-linearity (NL) score of an S-box is 120. It is observed that an S-box S with the maximum score of non-linearity (that is 120) may not satisfy the required criteria of other cryptographic security tests [43]. In Table 4, the nonlinearity (NL) criteria of newly design S-boxes by the proposed method and some existing S-Boxes are given comparatively. It can be seen easily that the newly constructed S-boxes have greater non-linearity when compared to the elliptic curve-based S-boxes in [26], [28]. The newly constructed S-boxes have much capability of resistance against linear attack.

Table 4. Non-linearity of some existing and proposed S-boxes

S-boxes	$S_{0,3,461}^{313,229}$	$S_{0,49,599}^{122,179}$	$S_{0,49,599}^{440,270}$	$S_{0,2,353}^{114,1}$	Ref. [28]	Ref. [26]	Ref. [42]	Ref. [34]	Ref. [36]	Ref. [44]
Nonlinearity	107	107	107	107	106	106	103.25	107	105.5	106.25

### 2.3.2 Linear Approximation Probability (LP)

The concept of linear approximation probability test of an S-box is used to calculate the highest value  $LP(S)$  of coincident masked input bits with masked output bits [45]. The mathematical form of LP test is given in the following

$$LP(S) = \frac{1}{2^n} \left\{ \max_{\alpha, \beta} \{ |\#\{x \in GF(2^n): \alpha \cdot x = \beta \cdot S(x)\} - 2^{n-1}| \} \right\}$$

Where  $\alpha \in GF(2^n)$  and  $\beta \in GF(2^n) \setminus \{0\}$ . A cryptographically strong S-box has the property that it attains a low score of LP. In Table 5, some of the newly constructed S-boxes by the proposed technique and their corresponding LP values are listed, which shows that the S-boxes based on the proposed scheme is suitable for secure communication against linear approximation attacks.

### 2.3.3 Strict Avalanche Criterion (SAC)

Webster et al. [45], [46], introduced the concept of strict avalanche criterion. The primary objective of his test is used to analyze the diffusion creation capability of an S-box in the data. The strict avalanche criterion indicates the likelihood of change in all yield bits by applying a single change at an info bit. The mathematical description of SAC of an S-box is given as follows

$$m(i, j) = \left\{ \frac{1}{2^n} [w(S_i(x + \alpha_j) + S_i(x))] \mid \alpha_j \in GF(2^n), w(\alpha_j) = 1 \text{ and } 1 \leq i, j \leq n \right\}$$

Clearly,  $m(i, j)$  are entries of the dependency matrix. If all the entries of the SAC matrix are lying in the small neighborhood of 0.5, then one can say that the SAC criterion is fulfilled. The proposed S-boxes  $S_{0,b,p}^{y_1, y_2}$  and their corresponding SAC scores are shown in Table 5. These results show a clear sign to have enough diffusion capability of the newly constructed S-boxes. Furthermore, the SAC results indicate the effectiveness of the proposed S-boxes in comparison with some existing S-boxes.

### 2.3.4 Bit Independence Criterion (BIC)

This criterion is also introduced by Webster et al. [45], [46] to examine the inversion of the plain-text bit  $p$  effects the cipher bit  $r$  without dependence on each other. This test is investigated by means of the correlation coefficient. The BIC test of standard S-box is a square matrix of dimension  $16 \times 16$ . If the entries of the BIC matrix of an S-box are close to 0.5 then the S-box is said to satisfy the BIC criteria. The BIC test is applied to the various proposed and existing S-boxes. Our designed S-boxes  $S_{0,b,p}^{y_1, y_2}$  and BIC test scores are given in



Table 5. The average scores of the BIC matrices corresponding to some newly constructed S-boxes are given in Table 5. The scores of the BIC test ensure the resistance of the proposed S-boxes against common attacks.

### 2.3.5 Differential Approximation Probability (DP)

The differential approximation probability (DP) of S-box is used to calculate the differential uniformity and is defined as:

$$DP (\Delta a \rightarrow \Delta b) = \frac{|\{a \in X | S(a) \oplus S(a \oplus \Delta a) = \Delta b\}|}{2^m}$$

This implies that for each an input differential  $\Delta a_i$ , there exists a unique output differential  $\Delta b_i$ , thus ensuring a uniform mapping probability for each  $i$ . The average value of differential approximation probability of some proposed S-boxes is listed in Table 5. We conclude that the results of the DP test of the proposed box are comparable with S-boxes in [21], [23], [24], [47] based on the chaotic map.

Table 5. Comparison of experimental results of the proposed S-boxes with standard S-boxes

S-box	SAC	BIC	LP	DP
$S_{0,3,461}^{313,229}$	0.499023	0.50635	0.1250000	0.0390620
$S_{0,49,599}^{122,179}$	0.493408	0.50628	0.1328125	0.0468750
$S_{0,49,599}^{440,270}$	0.495117	0.50691	0.1328125	0.0390620
$S_{0,2,353}^{114,1}$	0.499023	0.49665	0.1328125	0.0390620
$S_{0,9,653}^{397,606}$	0.504639	0.50216	0.1484375	0.0468750
Ref. [48]	0.506836	0.5017	0.140625	0.03906
Ref. [42]	0.5151	0.4864	0.15625	0.171875
Ref. [21]	0.5095	0.5092	0.1250	---
Ref. [34]	0.4973	0.5052	0.1172	0.0391
Ref. [23]	0.4960	0.4994	0.1094	0.0313
Ref. [24]	0.5001	0.498	0.102	0.0313

## 2.4 Construction of Pseudo Random Numbers

There are three classes of random numbers of generators, pseudo-random number generators (PRNGs), true random number generators (TRNGs), and hybrid random number generators (PRNGs). In cryptography, many security applications like encryption, protocols make use of Pseudo-random number generators (PRNGs). Besides, Pseudo-random number generators

(PRNGs) are used to create high diffusion in the pixels of the plain image. Various PRNGs using the elliptic curve have been established [6], [49]. Most of them have very complex computations due to the elliptic curve group law operation. In this section, we generate PRNs through fixed EC using square free elements of finite field  $F_{\mathcal{P}}$ . Let  $E^{(0,d,\mathcal{P})} \setminus \{0\}$  be an elliptic curve over a finite field  $F_{\mathcal{P}}$ . Then, for each square free element  $t' (> 0) \in F_{\mathcal{P}}$  that is  $t' \neq r^2 \pmod{\mathcal{P}}; \forall r \in F_{\mathcal{P}}^*$ . There is a non-isomorphic elliptic curve  $E^{(0,\ell,\mathcal{P})}$  to  $E^{(0,d,\mathcal{P})}$ . Thus, one may have  $\frac{\mathcal{P}-1}{2}$  number of non-isomorphic elliptic curves to given EC  $E^{(0,d,\mathcal{P})}$ . On each curve, the y-coordinates play a vital role to generate the proposed PRNs. The following algorithm is used to calculate the PRNs.

1. Select a prime number  $\mathcal{P}$  with  $\mathcal{P} \equiv 2 \pmod{3}$ , greater than the length  $M$  and width  $N$  of the color image  $I$ .
2. Generate an elliptic curve  $E^{(0,d,\mathcal{P})}$ , (where  $d < \mathcal{P} - 1$  is a non-negative integer) over a finite field  $F_{\mathcal{P}}$ .
3. Pick y-coordinates of the EC  $E^{(0,d,\mathcal{P})}$  and leaving x-coordinates to reduce the time complexity of the proposed algorithm for further consideration.
4. Generate a set  $S^y$  for each value of EC  $E^{(0,d,\mathcal{P})} \setminus \{0\}$  by using square free elements in the field  $F_{\mathcal{P}}$ . each such set  $S^y$  consisting of elements as y-component lying on the non-isomorphic elliptic curve.
5. Select a prime  $p' > \mathcal{P}$  and  $t$  with the conditions;  $p' \equiv 2 \pmod{3}$  and  $t \in F_{p'}^*$ .
6. Generate EC  $E^{(0,b,p')}$  over prime field  $F_{p'}$ . Choose a non-identity element  $Q \in E^{(0,b,p')}$  and define a translation map

$$\tau_Q: E^{(0,b,p')} \rightarrow E^{(0,b,p')}$$

Defined by

$$\tau_Q(P) = P + Q; \forall P \in E^{(0,b,p')}$$

Clearly, the map  $\tau_Q$  is bijective. The ordering of points is a matter of concern. Pick only y-coordinates of the imaging set of  $\tau_Q$ . Place each set  $S^y$ , where its first entry lying in the sequence consisting of y coordinates obtained via translation map. Form a rectangular box  $S_{\mathcal{P} \times (\mathcal{P}-1)/2}$  of height  $(\mathcal{P} - 1)/2$  and width  $\mathcal{P}$ .

### 2.4.1 Key Space Analysis

One of the main components of a secure cryptosystem is a large key space. An encryption algorithm is said to be much secure against brute-force attack or commonly known as exhaustive key search whenever the set of keys involved in the algorithm has sufficiently large cardinality. In this proposed scheme, the order, the base fields for elliptic curves, coefficients of the elliptic curve and translation map are used as secret keys. We analyze key space by calculating all keys in each step of the proposed scheme. The detailed description is given in the following

- a. The permutation operation of the proposed scheme uses six parameters  $\{b_1, b_2, b_3, p_1, p_2, p_3\}$  of length at least 9-bits. Thus, the total precision turns out to be  $2^{54}$ .
- b. The substitution box acquires six parameters  $\{t, s, b_4, p_4, y_1, y_2\}$ . Each having length not less than 10-bits. So, the total precision turns into  $2^{60}$ .
- c. The PRNs phase requires four secret keys  $\{l, r, b_5, b_6, p_5, p_6, Q\}$ . The minimum length of each key is 10-bits. The precision of  $l, r, b_5, b_6, p_5, p_6$  is  $2^{60}$  and  $Q$  has a precision of  $2^{20}$ . The total precision is  $2^{80}$ .

The total key space is  $2^{54} \times 2^{60} \times 2^{80} = 2^{194}$ , which describes that the keyspace of the proposed technique is much greater than  $2^{128}$ . Therefore, it is evident that the proposed cryptosystem is much secure against all kinds of brute force attacks.

In the next chapter, we shall discuss the image encryption applications based on S-boxes, PRN, and various permutations operations depending on the dimension of the original color images by using different finite fields.

## Chapter 3

# Squared and Non-Squared PRN and their Application to Color Image Encryption

Image encryption is the process to convert the original image in such a way that unauthorized source cannot access to understand without having secret keys. The digital image is a matrix of numerical values. These values are denoted as pixels. With the development of information technologies, digital images are a source of information, such as medical images, color images. To protect this information is a big challenge.

### 3.1 Motivation

To consider the characteristic of the digital image, various image encryption schemes have been designed on the basis of different mathematical structures, including SCAN-CA [50], circular random grids [51], Ordered elliptic curve [26],  $(n, k, p)$ -Gray code for image [52], Self-adaptive wave transmission [53], vector quantization and index compression [50], fractional wavelet transform [24], chaotic theory [37], [54], [55], vector quantization and index compression [50], fractional wavelet transform [56], [57] and DNA sequences [18], [19], [58]. The Security performance of the encryption algorithm can be measured based on three parameters such as Low (L), Medium (M), and High (H). The security of a cryptographic scheme is assessed below if it is insecure against cryptanalysis attacks. If the cryptographic scheme is unbreakable through some of the cryptanalysis attacks, then its security is labeled as moderate, and finally, whenever it is secure against all kinds of cryptanalysis attacks, then the scheme is evaluated to be highly secure. Some of the existing cryptographic schemes and their security performance have been discussed in [59].

In this chapter, we introduce a new color image encryption algorithm. This chapter is organized as follows: in section 3.2, we present an image encryption scheme by using EC permutations, S-boxes, and PRN respectively. While in sections 3.3 & 3.4, we perform some known statistical analysis to validate the performance of the proposed scheme. Finally, in section 3.5, we present the time complexity of the proposed algorithm.

### 3.2 Proposed Encryption Scheme

Let the color image  $I_{M \times N}$  of dimension  $M \times N \times 3$ , where  $M$  and  $N$  indicate the width of the image and height  $N$  of the image respectively. In this work, we denote the color components Red, Green, and Blue of the image by  $R$ ,  $G$ , and  $B$  of  $M \times N$ . Also, in the encryption process all three channels  $R$ ,  $G$ , and  $B$  considered as a gray image, each component will be encrypted independently. The flowchart of the proposed scheme is provided in Figure 3 while the detail description is given after the flowchart.

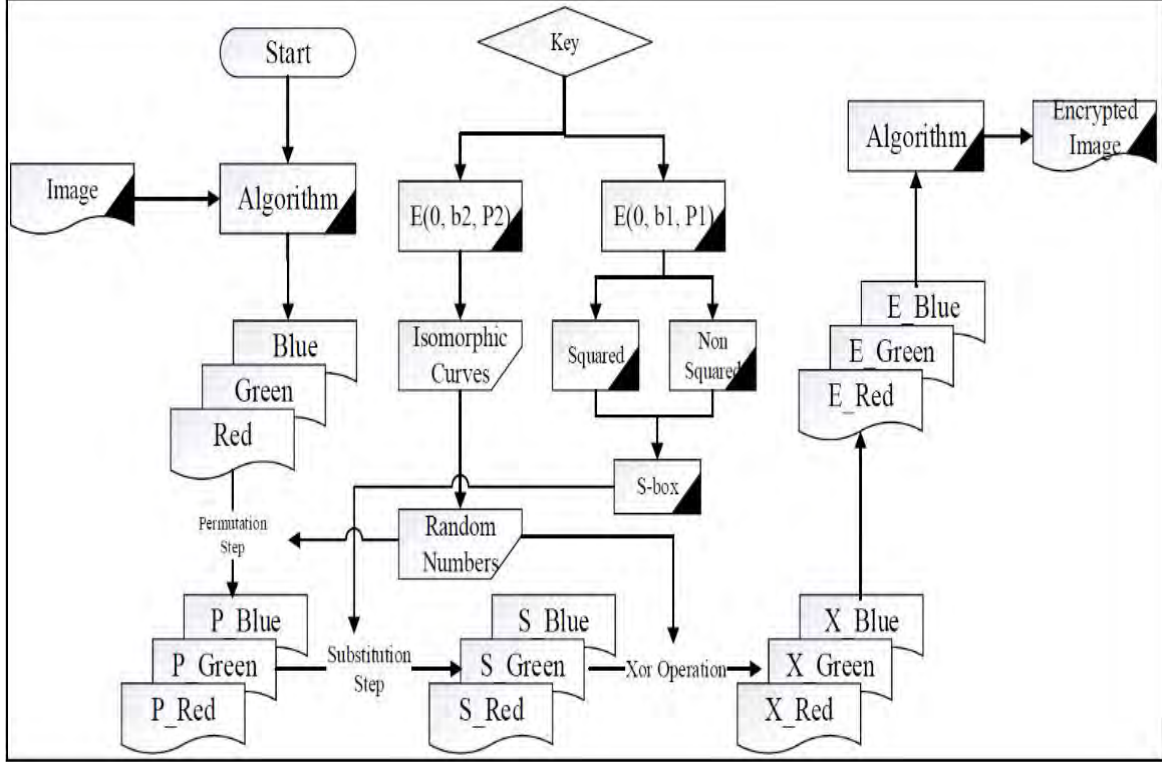


Figure 3. Flowchart of the proposed encryption scheme

**Step 1:** Let  $I$  be the true color image of dimensions  $M$  rows and  $N$  columns, with size  $M \times N \times 3$  pixels. Here, 3 represents the intensities of red, green, blue layers. We work separately on red, green, blue channels. We choose two primes  $p_1, p_2$  with  $p_1 > M$  and  $p_2 > N$  and  $p_1, p_2 \equiv 2 \pmod{3}$ . For each  $i = 1, 2, \dots, M$  and  $j = 1, 2, \dots, N$ , the pair  $(i, j)$  denotes the coordinate of a pixel location in the image. One can observe the one-one correspondence between all the pixel positions and ring  $Z_M \times Z_N$ , where  $Z_M$  and  $Z_N$  are finite rings modulo  $M$  and  $N$  respectively. Therefore, we refer to the locations of all pixels in an image  $I_{M \times N}$  by simply a ring  $(Z_M \times Z_N)$ . Now it is easy to see that  $y$ -coordinates of both elliptic curves  $E(0, \alpha, p_1)$  and  $E(0, \beta, p_2)$  act as permutations on the set  $Z_M \times Z_N$ . Define a set

$$A = \{(E(0, \alpha_i, p_1), E(0, \beta_i, p_2)); \text{ with } \alpha_i = t^3 \alpha \text{ and } \beta_i = s^3 \beta, \text{ for some } t \in (F_{p_1}^*)^2, s \in (F_{p_2}^*)^2\}$$

Where left component of  $A$  is an elliptic curve isomorphic to  $E^{(0,\alpha,p_1)}$  and right component corresponds  $E^{(0,\beta,p_2)}$  over finite fields  $F_{p_1}$  and  $F_{p_2}$  respectively.

So, we introduce some simple notations, we denote  $Z_M \times Z_N = Z_{M \times N}$ ,  $S_p$  is symmetric group of all permutations over a finite field  $F_p$ ; y-coordinates of both elliptic curves  $E^{(0,\alpha,p_1)}, E^{(0,\beta,p_2)}$  by  $e_{b,y}^{p_1}$  and  $e_{b',y}^{p_2}$ , respectively. Let  $B = \{(e_{b,y}^{p_1}, e_{b',y}^{p_2}) \text{ with } b \in F_{p_1}^*, b' \in F_{p_2}^*\}$ . Then clearly  $e_{b,y}^{p_1} \in S_{p_1}$  and  $e_{b',y}^{p_2} \in S_{p_2}$ .

We now define maps

$$\mu_1: S_{p_1} \times Z_{M \times N} \rightarrow Z_{M \times N} \text{ and } \mu_2: S_{p_2} \times Z_{M \times N} \rightarrow Z_{M \times N}$$

Defined by

$$\mu_1(e_{b,y}^{p_1}(z_m, z_n)) = (e_{b,y}^{p_1}(z_m), z_n) \quad (2.1)$$

$$\mu_2(e_{b',y}^{p_2}(z_m, z_n)) = (z_m, e_{b',y}^{p_2}(z_n)) \quad (2.2)$$

$$e_{b,y}^{p_1}(z_m, z_n) = z_{m+l} \text{ if } z_m < z_{m+l} \text{ and } z_{m+l} \in e_{b,y}^{p_1} \cap Z_M$$

$$e_{b',y}^{p_2}(z_m, z_n) = z_{n+l} \text{ if } z_n < z_{n+l} \text{ and } z_{n+l} \in e_{b',y}^{p_2} \cap Z_N$$

The above action of permutation is applied to each color component of the image to scramble the position of the pixels of the image. Consequently, one can get new components  $P_R$ ,  $P_G$  and  $P_B$ . The scrambled image after the action of permutation is shown in Figure 4(b).

**Step 2:** In any cryptographic algorithm, the substitution step is an essential part, which boosts the security strength of the scheme against the chosen plain text attack. In the proposed scheme, the S-box generated scheme (which we have discussed in section 2.2) is deployed, which generates good quality S-box having good cryptographic features. Subsequently, the obtained S-boxes are then used to substitute the scrambled components  $P_R$ ,  $P_G$  and  $P_B$  of the image (the procedure is the same as AES substitution). As a result, one can get the substituted components  $S_R$ ,  $S_G$  and  $S_B$ . The ciphered image after substitution is shown in Figure 4(c).

$$E_{R,G,B}(i, j) = S_{R,G,B}(i, j) + r_{p'}(d, \mathcal{P})_{i \times j} = S_{R,G,B}(i, j) + t_j^3 y_i \text{ mod } 256; \text{ for some } t_j \in F_{\mathcal{P}} \setminus (F_{\mathcal{P}}^*)^2$$

Where  $S_{R,G,B}(i, j)$  and  $r(d, \mathcal{P})_{i \times j}$  are  $(i \times j)$ th element of the substituted component  $S_{R,G,B}$ . Consequently, one can get the new components  $E_R$ ,  $E_G$  and  $E_B$ , then combine the new components and get the ciphered image, shown in Figure 4(d).

### 3.3 Experimental Results and Comparison

An encryption algorithm is said to be good enough for implementation purpose if it is thoroughly tested through various security performance tests and satisfies the corresponding criteria.

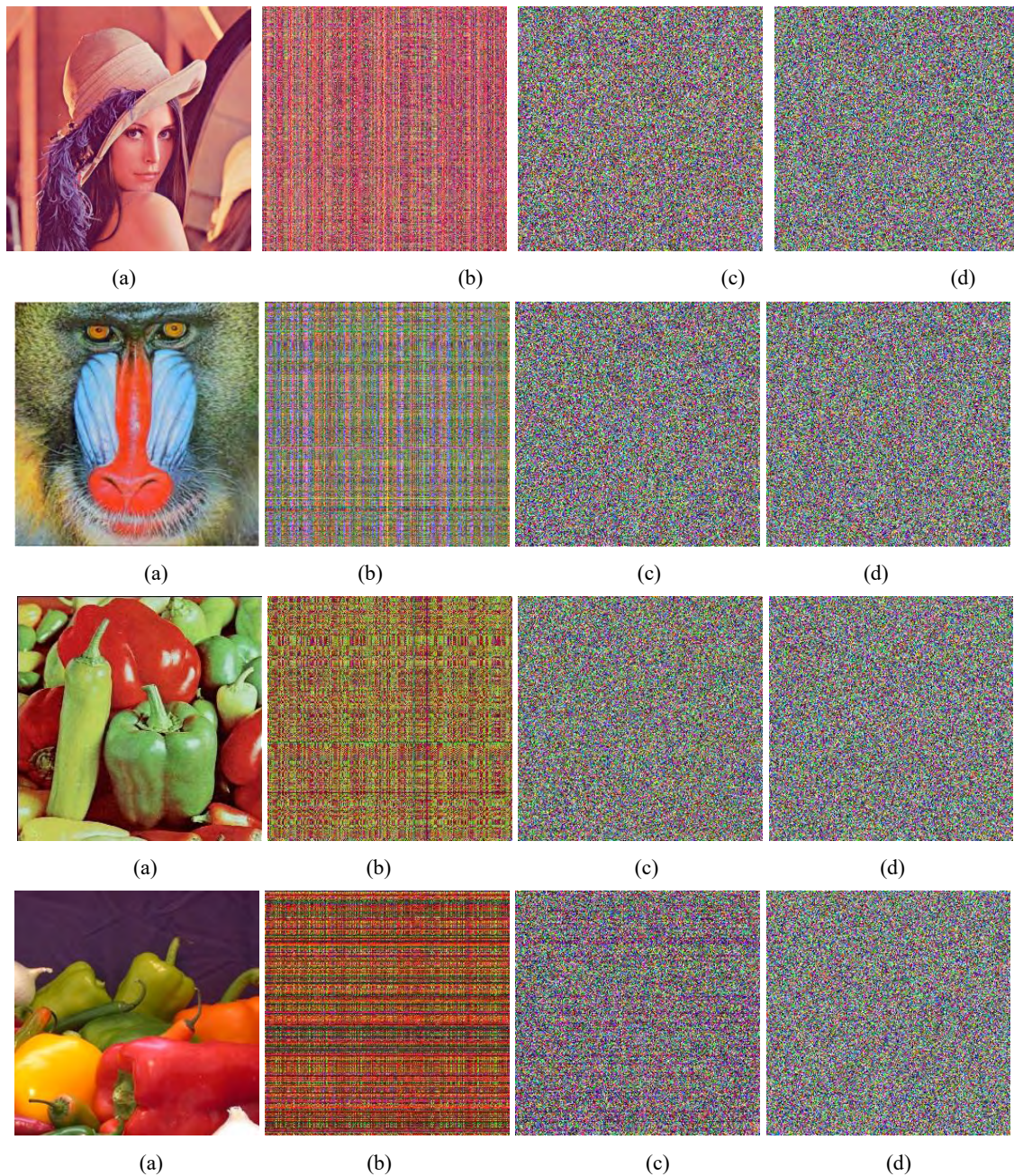


Figure 4. Original and Ciphred images: (a) The original color images of Lena, Baboon, Pepper, and Deblur; (b) The Permuted images; (c) The Substituted images; (d) The Ciphred images.

To examine the security performance against various attacks, in this study we used the color images of Lena, Baboon, Peppers, Deblur, with each and encrypt these images by the

proposed cryptosystem, shown in Figure 4. The encrypted images are then analyzed through various performance tests, which we discuss in upcoming subsection.

### 3.3.1 Histogram Analysis

A histogram is an important tool that measures the total number of pixels having the same intensity value in the image. A well-designed encryption algorithm can create uniform-ness in the distribution of the pixels of a ciphered image and is completely different than the histogram of the original color image.

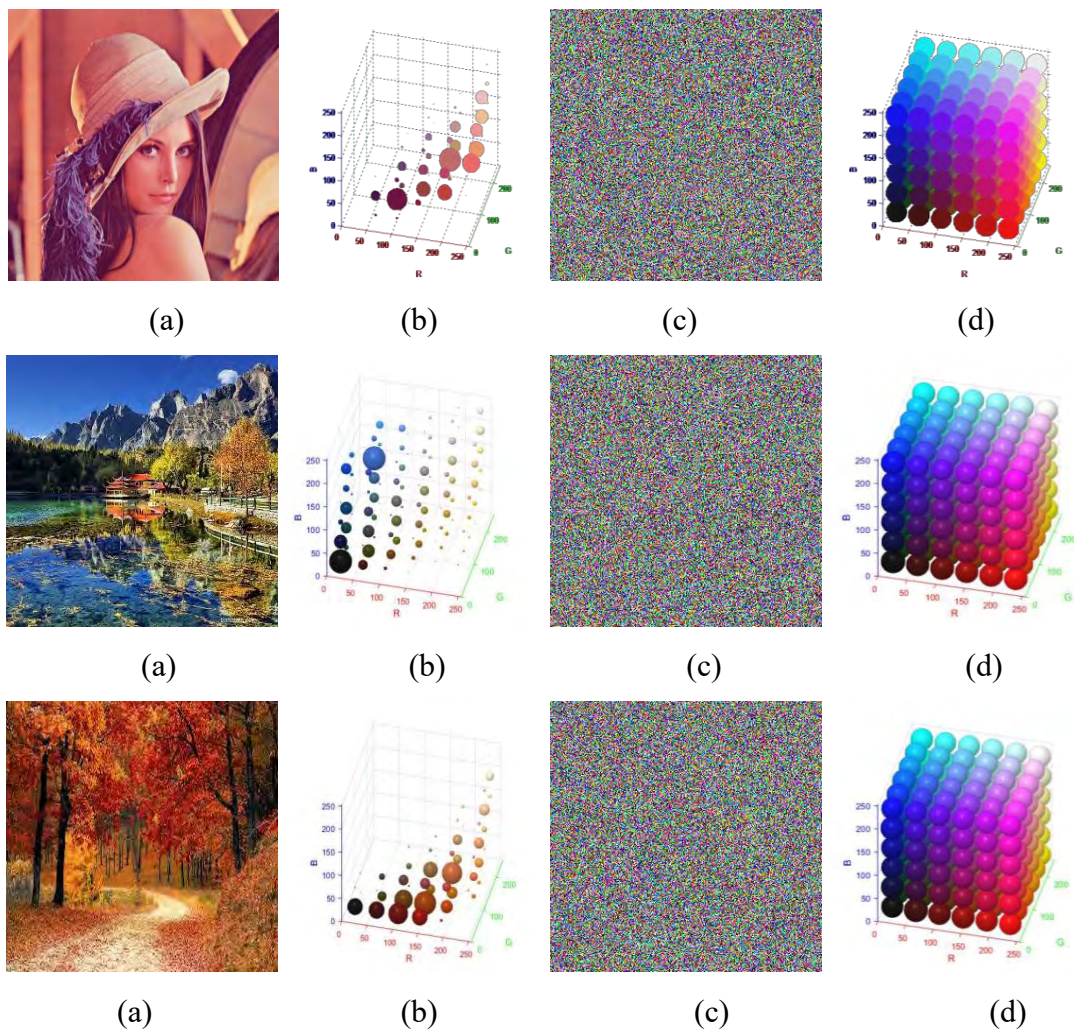


Figure 5. Histograms of original color images and ciphered images: (a). The original color images: Lena, Swat image and Nature image; (b). The histograms of the original images; (c) The ciphered images; (d). The histograms of the ciphered images.

To observe the resistance of the proposed encryption technique against statistical attacks, we investigate the histograms of ciphered images. Figure 4 shows the histograms of the original color images and corresponding ciphered images of ‘Lena’, ‘Swat’, and ‘Nature’. The histograms of the ciphered images have almost uniform distribution and significantly



dissimilar from those of the corresponding original images. Thus, it is revealed that the proposed scheme is highly resistive against the statistical attacks.

### 3.3.2 Entropy Analysis

The entropy test is used to measure the probability of occurrence and randomness in the ciphered image. The maximum value of the entropy analysis test for the encrypted image is 8. The ciphered image  $I'$  of the original color image,  $I$  is considered to have efficient encryption if its entropy test gets a high score that is 8. Besides the high entropy, its encryption strength is resistant to common attacks. The following mathematical description is used to compute the entropy

$$EA(I') = \sum_{x=0}^{255} [p(x) \times \log_2(\frac{1}{p(x)})]$$

$p(x)$ , represents the probability of the happening of the pixel  $x$ .

Table 6. Comparison for the entropy results of the ciphered images

Schemes	Proposed			Ref.[19]	Ref.[60]	Ref. [54]	Ref. [46]	Ref. [61]
Images	Lena	Pepper	Baboon	Lena				
Entropy	7.9993	7.9993	7.9993	7.9927	7.9952	7.9878	7.9971	7.9974

The entropy results of the proposed scheme and some of the existing are given in Table 6. In Table 6, the results of the proposed scheme are approximately equal to 8, which is comparatively better than the result of the existing scheme. So, the scheme can efficiently resist the statistical analysis.

### 3.3.3 Contrast

One of the main aspects of the picture quality is the contrast ratio, enabling the viewer to identify the object in the picture. Contrast analysis (CA) is used to measure the intensity level of contrast about pixels in the whole image. If the contrast ratio is high in the ciphered image, the encryption scheme is said to satisfy the contrast test. The mathematical representation of the contrast coefficient is given the following

$$C = \sum_{i,j} \frac{p(i,j)}{1+|i-j|}$$

Where  $p(i, j)$  denotes the number of gray level co-occurrence matrices of the image.

### 3.3.4 Energy

The energy analysis (AE) of an image is dependent on the gray-levels co-occurrence matrices of the encrypted image. The energy test measures the uniformity in pixel intensities by calculating the square root of the angular second moment. The following mathematical equation is used to calculate energy

$$E = \sum_{i,j} p(i,j)^2$$

Whereas  $p(i,j)$  represents Gray-level co-occurrence matrices (GLCM).

### 3.3.5 Homogeneity

Images have naturally distributed contents when captured. This analysis is used to measure the closeness of distributed elements of Gray Level Co-occurrence Matrix (GLCM) to GLCM diagonal. It is also documented as a gray tone spatial dependency matrix. Mathematically, the look for homogeneity analyses is represented by the equation:

$$H^* = \sum_i \sum_j \frac{f(i,j)}{1 - |i - j|}$$

The value of contrast is zero for the constant image.

Table 7. Statistical analysis of the proposed scheme with some existing techniques

Schemes	Image	Metric	Original color Image			Ciphered Image		
			R	G	B	R	G	B
Our scheme	Deblur	Contrast	0.1193	0.1210	0.1051	10.4439	10.5109	10.4721
		Energy	0.1749	0.2139	0.2606	0.0156	0.0156	0.0156
		Homogeneity	0.9484	0.9482	0.9532	0.3905	0.3906	0.3913
	Lena	Contrast	0.3672	0.3946	0.3405	10.4758	10.4449	10.4788
		Energy	0.1391	0.0988	0.1755	0.0156	0.0156	0.0156
		Homogeneity	0.8720	0.8706	0.8784	0.3894	0.3894	0.3897
	Pepper	Contrast	0.4370	0.4520	0.3849	10.5370	10.6502	10.4483
		Energy	0.1160	0.1054	0.1425	0.0156	0.0156	0.0156
		Homogeneity	0.8576	0.8704	0.8661	0.3891	0.3882	0.3890
	Baboon	Contrast	0.4116	0.4297	0.4530	10.5565	10.3775	10.4869
		Energy	0.0881	0.1021	0.0862	0.0156	0.0156	0.0156
		Homogeneity	0.8397	0.8332	0.8265	0.3890	0.3902	0.3895

The texture results of the different color images of Deblur, Lena, Pepper and Baboon via proposed scheme are given in Table 7. The contrast score of each channel of the original color image Lena is in between 0.3405 and 0.3946, whereas corresponding scores of an ciphered image is approximately 10.45, which clearly shows the occurrence of high change in the intensity of a pixel and its neighbor of the entire ciphered image. The homogeneity score for ciphered image of Lena is very low. Consequently, it indicates that GLCM difference is

higher. Energy score of Lena original and ciphered images illustrate the low quantity of recurring pairs, which describes the worth of the proposed encryption scheme.

### 3.3.6 Correlation

In the color image, the correlation between the adjacent pixels is high due to their pixel values are close to each other. The correlation coefficient measures the linearity among the value of the adjacent pixel in the neighborhood. The main objective of the encryption scheme is to distort the pixels to get the least correlation among the adjacent pixels along with horizontal, diagonal, and vertical directions in the image.

Table 8. Comparison of correlation coefficient results of the proposed scheme with some existing techniques in three layers.

Schemes	Images	Metrics	Original color Image			Ciphered Image		
			R	G	B	R	G	B
Proposed scheme	Deblur	Vertical	0.9942	0.9912	0.9829	0.0000082	0.0000089	0.0000052
		Diagonal	0.9902	0.9831	0.9701	-0.000035	-0.000022	0.0000950
		Horizontal	0.9967	0.9946	0.9875	0.0000094	0.0000065	-0.000071
	Lena	Vertical	0.9802	0.9819	0.9625	-0.000035	0.0000092	0.0000110
		Diagonal	0.9344	0.9320	0.9018	0.0000140	0.0000620	-0.000037
		Horizontal	0.9604	0.9619	0.9303	0.0000052	0.0000043	0.0000058
	Pepper	Vertical	0.9532	0.9743	0.9527	0.0000300	0.0000220	0.0000860
		Diagonal	0.9225	0.9550	0.9053	0.0000230	0.0000640	0.0000340
		Horizontal	0.9510	0.9783	0.9509	-0.000060	0.0000940	0.0000230
	Baboon	Vertical	0.9570	0.9303	0.9608	0.0000250	0.0000340	0.0000430
		Diagonal	0.9299	0.8758	0.9317	0.0000075	0.0000190	0.0000830
		Horizontal	0.9600	0.9402	0.9641	-0.000052	0.0000084	0.0000074
Vertical		0.9803	0.9594	0.9294	0.0203	-0.0025	0.0006	
Ref.[58]	Lena	Diagonal	0.9668	0.9433	0.9099	-0.0073	-0.0131	0.0111
		Horizontal	0.9813	0.9691	0.9455	0.0092	0.0002	0.0076
		Vertical	0.9682	0.9755	0.9642	0.0031000	0.0001000	0.0022000
Ref. [60]	Lena	Diagonal	0.9377	0.9474	0.9271	0.0007000	0.0017000	0.0007000
		Horizontal	0.9651	0.7202	0.9572	0.0049000	0.0054000	0.0053000
		Vertical	0.9508	0.9370	0.9171	-0.001300	-0.005100	-0.007800
Ref. [19]	Lena	Diagonal	0.9259	0.9111	0.8867	-0.002500	-0.010300	0.0099000
		Horizontal	0.9777	0.9670	0.9496	0.0090000	-0.002700	-0.015500
		Vertical	0.9635	0.9648	0.9280	-0.0141	-0.0134	-0.0486
Ref. [24]	Lena	Diagonal	0.8993	0.9075	0.8449	-0.0464	-0.0189	-0.0501
		Horizontal	0.9278	0.9278	0.8867	-0.0362	-0.0089	-0.0105
		Vertical	0.9642	0.9757	0.9742	0.0032000	0.0003000	0.0021000

An image encryption scheme is robust and healthy enough for security applications if the correlation coefficient of the ciphered image is near to zero. The correlation coefficient of two adjacent pixels  $u$  and  $v$  are represented by the following equation.

$$r_{uv} = \frac{cov(u, v)}{\sqrt{D_u D_v}}$$

Whereas

$$cov(u, v) = \frac{1}{M \times N} \sum_{i=1}^{M \times N} (u_i - E(u))(v_i - E(v))$$

$$E(u) = \frac{1}{M \times N} \sum_{i=1}^{M \times N} u_i$$

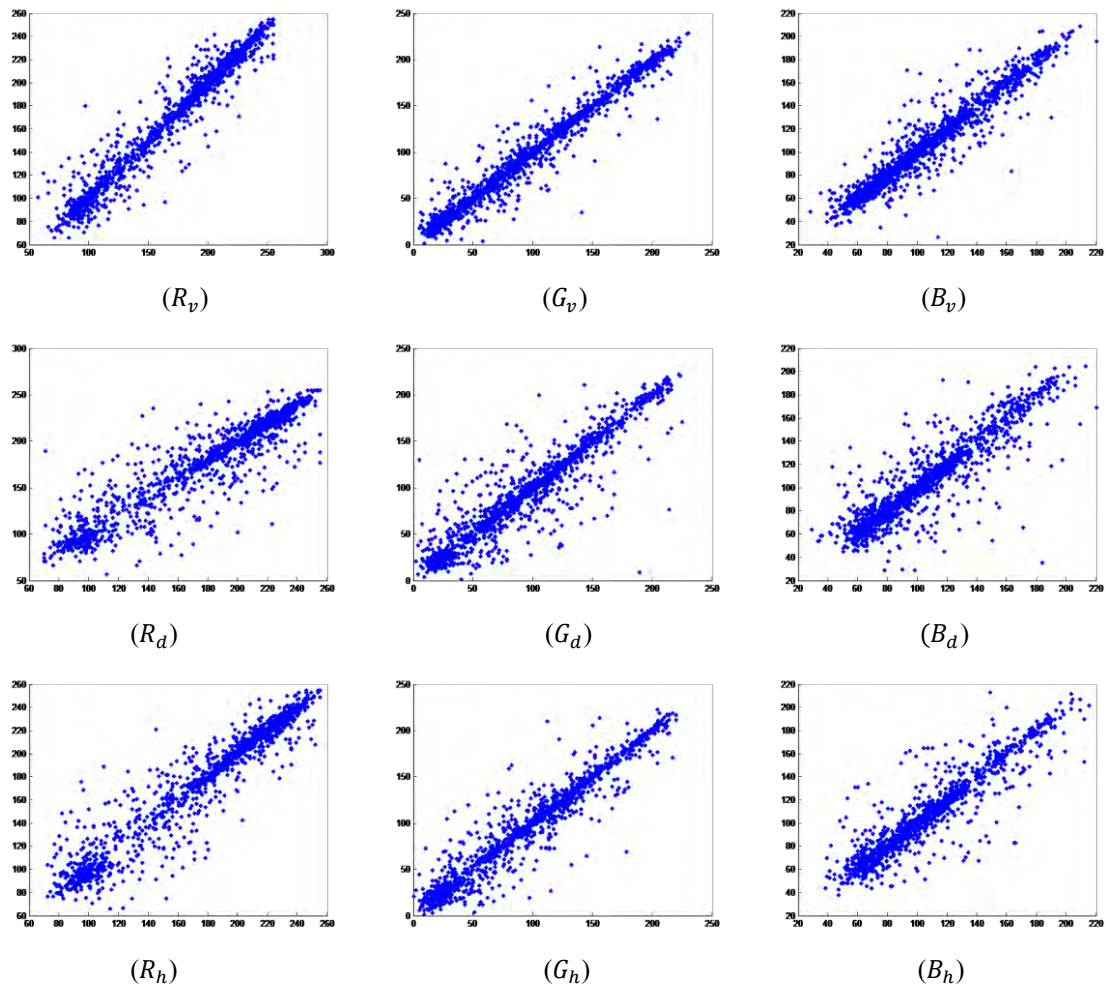


Figure 6. Correlation plots of two adjacent pixels of R, G, and B channels of the original color image *Lena* from the first to third column illustrates: the vertical, diagonal, and horizontal adjacent pixels of each channel respectively.

The experimental results of the correlation test of various plain and ciphered images along each channel are shown in Table 8. In this paper, it is easy to observe that the correlation of two adjacent pixels of plain images along vertical, horizontal, and diagonal directions are almost equal to 1. While the correlation coefficient scores along all three directions of two adjacent pixels in the ciphered images by the proposed scheme are nearly 0. Furthermore, the results of the correlation coefficient show that the proposed encryption scheme is much efficient and resistant against statistical attacks in comparison to some existing relevant literature.

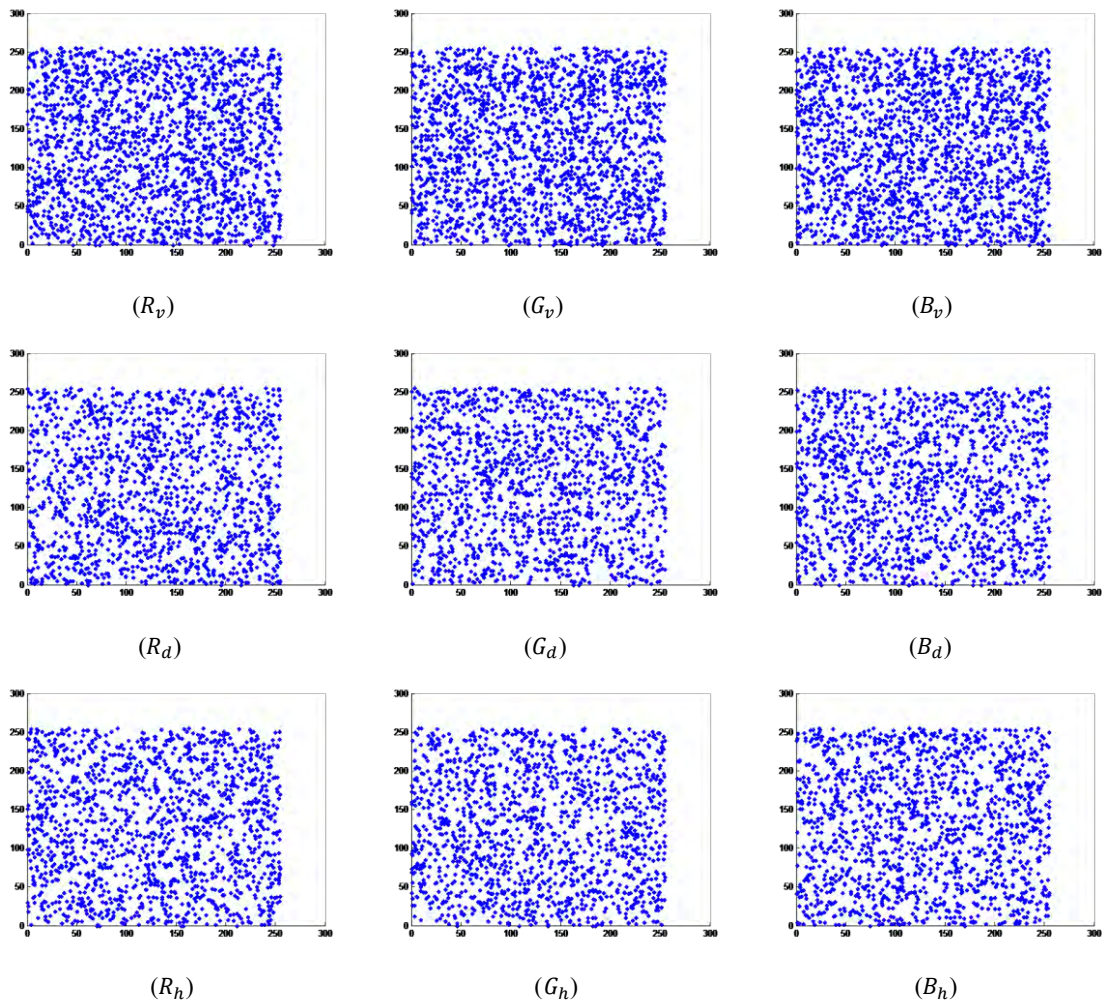


Figure 7. Correlation plots of two adjacent pixels of R, G, and B channels of the ciphered Lena image: from the first to third column illustrates the vertical, diagonal, and horizontal adjacent pixels of each channel, respectively.

### 3.3.7 Differential attack

The NPCR (Number of pixels change rate) analysis measure the number of pixels change rate when one byte is adjusted of the plain image. The NPCR value of a sensitive cryptosystem when changing original data is close to 100%. UACI mean average intensity of difference

between original color image and cipher image. The increase of UACI analysis implies the resistance of the cryptosystem against differential attacks increase. The NPCR and UACI analysis mathematically represented as:

$$NPCR = \frac{\sum_{\zeta_1, \zeta_2} B(\zeta_1, \zeta_2)}{M \times N} \times 100\%$$

Where

$$B(\zeta_1, \zeta_2) = \begin{cases} 1 & \text{if } C_1(\zeta_1, \zeta_2) = C_2(\zeta_1, \zeta_2) \\ 0 & \text{if } C_1(\zeta_1, \zeta_2) \neq C_2(\zeta_1, \zeta_2) \end{cases}$$

$$UACI = \frac{1}{M \times N} \sum_{\zeta_1, \zeta_2} \left[ \frac{|C_1(\zeta_1, \zeta_2) - C_2(\zeta_1, \zeta_2)|}{255} \right] \times 100\%$$

Where  $C_1(\zeta_1, \zeta_2)$  and  $C_2(\zeta_1, \zeta_2)$  represent the original image and one-pixel change image.

Table 9. Comparison of NPCR and UACI analysis results of the proposed scheme with some existing techniques

Schemes	Image	NPCR%			UACI%			Average
		R	G	B	R	G	B	
	Deblur	99.980	99.976	99.983	36.9809	30.0386	33.7423	33.5872
Our scheme	Lena	99.979	99.985	99.982	33.4044	33.7832	35.6901	34.2925
	Pepper	99.981	99.982	99.977	33.7500	32.4338	33.1319	33.1052
	Baboon	99.970	99.979	99.974	34.4991	35.0323	34.3105	34.6140
Ref. [58]	Lena	99.653	99.652	99.651	33.4572	33.4715	33.4715	33.4384
Ref. [62]	Lena	99.650	99.644	99.662	33.4462	33.4131	33.4399	33.4330
Ref. [19]	Lena	99.630	99.602	99.601	33.60	33.30	33.40	---
Ref. [28]	99.5964 (Gray Image)			33.4762 (Gray Image)			---	

Table 9 shows the result of NPCR and UACI analysis of the proposed and previous cryptosystems. From Table 9, we can see that the proposed algorithm illustrates good performance that would resist differential attacks.

### 3.4 Robustness Analyses

In this section, we investigate the performance of the encryption-decryption algorithm with noises. During transmission, some sort of noises creates distortion/errors in multimedia data via the communication channel. Therefore, to send the ciphered image through the communication channel, some noises are added to examine the efficiency of the decryption of the proposed scheme, which are briefly discussed as under.

### 3.4.1 Noise Analyses

Impulsive or fat-tail distribution is usually known as salt and Pepper noise. An image with salt and Pepper noise degrades the dark and bright regions by sudden and sharp disturbances. Consequently, it is scattered randomly over the image in the form of dark and white pixels. This noise is occurred due to bit errors in transmission or during the conversion of the analog signal to a digital signal. Many techniques/algorithms like non-local means, block-matching 3D filtering (BM3D), dark frame subtraction and interpolation are applied to remove such noise. In this study, we added the salt and peppers and Gaussian noise to the ciphered color image of Deblur and subsequently decipher the noisy image ciphered images as shown in Figure 8 and Figure 9. In Figure 8(a-d) and Figure 9(a-d) depicts the noisy cipher images and Figure 8(e-h) and Figure 9(e-h) display the decrypted images of the corresponding noisy images. It can be observed easily from the figures that deciphered images are still recognizable, even after the existence of noises in the ciphered images. Besides, the UACI, NPCR, MSE and PSNR scores are measured among the noiseless decrypted images and the noisy deciphered images, the results are listed in Table 10.

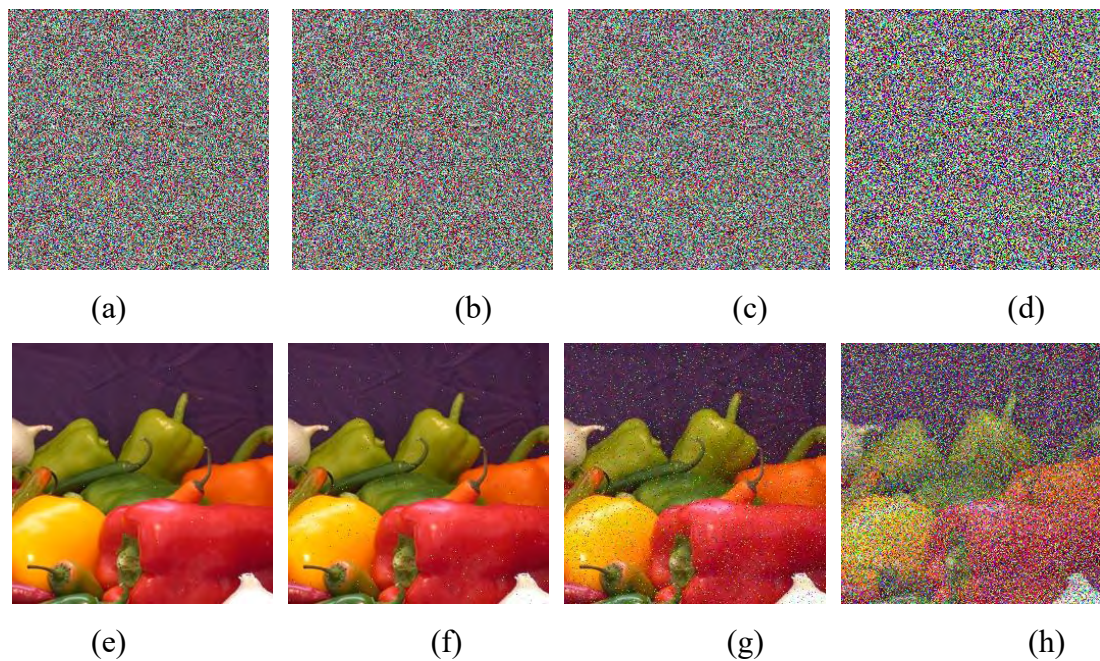


Figure 8. Salt and Peppers analysis of Deblur image: first row (a-d) Deblur ciphered image with salt and pepper variance 0.0005, 0.005, 0.05 and 0.5; second row (e-h) corresponding deciphered images

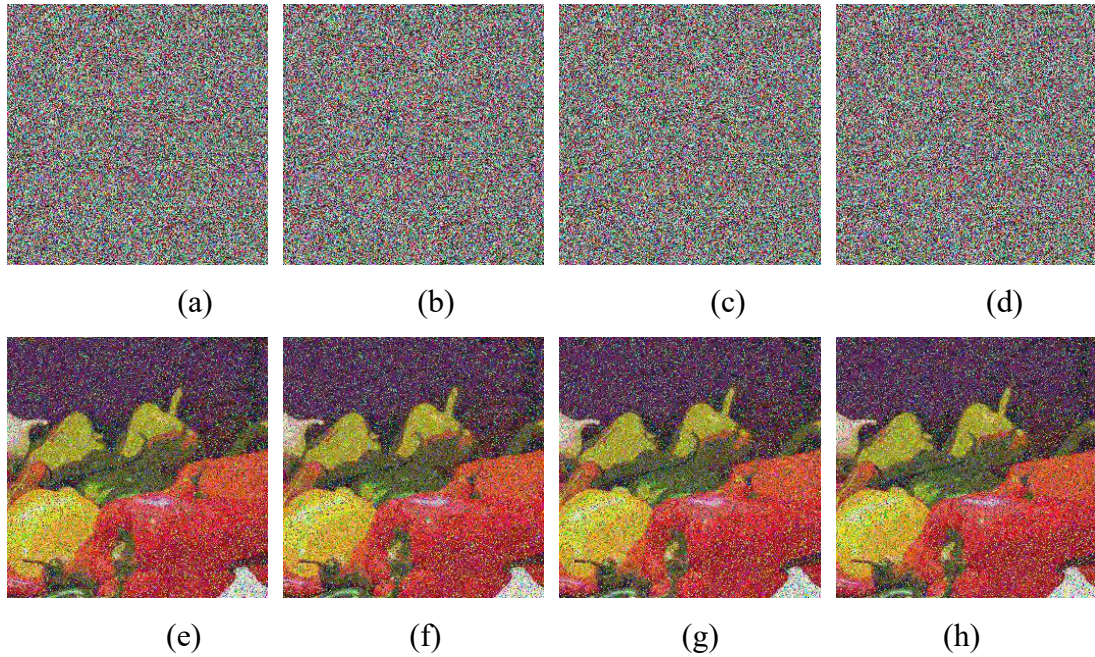


Figure 9. Gaussian analysis of Deblur Image: first row (a-d) Deblur ciphered image with salt and peper variance 0.0004, 0.0003, 0.0002 and 0.0001; second row (e-h) corresponding deciphered images

### 3.4.2 Ocluded Attack

Due to congestion in the source of communication, some amount of image data may be occluded during transmission. The efficient cryptosystem should be capable to decrypt the recognizable image, whenever some portion of the corresponding ciphered image is lost during the communication. To examine the proposed encryption scheme against the occluded attack, we remove various parts from the ciphered images and then decipher these images as shown in Figure 10. Figure 10(a-e) shows the occluded ciphered images, and the corresponding deciphered images are shown in Figure 10(i-p). The resultant deciphered images demonstrate that the proposed encryption scheme is capable to preserve the information of the images, whenever  $\frac{1}{2}$  portion of the ciphered image is lost during communications.

### 3.4.1 Peak Signal to Noise Ratio (PSNR)

The quality of signal representation is affected by corrupted noise. Peak signal to noise ratio (PSNR) is a metric that measures the ratio between the actual power of a signal and the power of a noisy signal and expressed in decibel unite. Furthermore, it is one of the tools that assess the quality of the image encryption scheme. We have used a digital image as an actual signal, and the distortion produced by encryption is termed as the noise in our study. The higher score of PSNR usually indicates that a negligible amount of data is lost in the deciphered image and specifies the higher strength of the encryption algorithm.



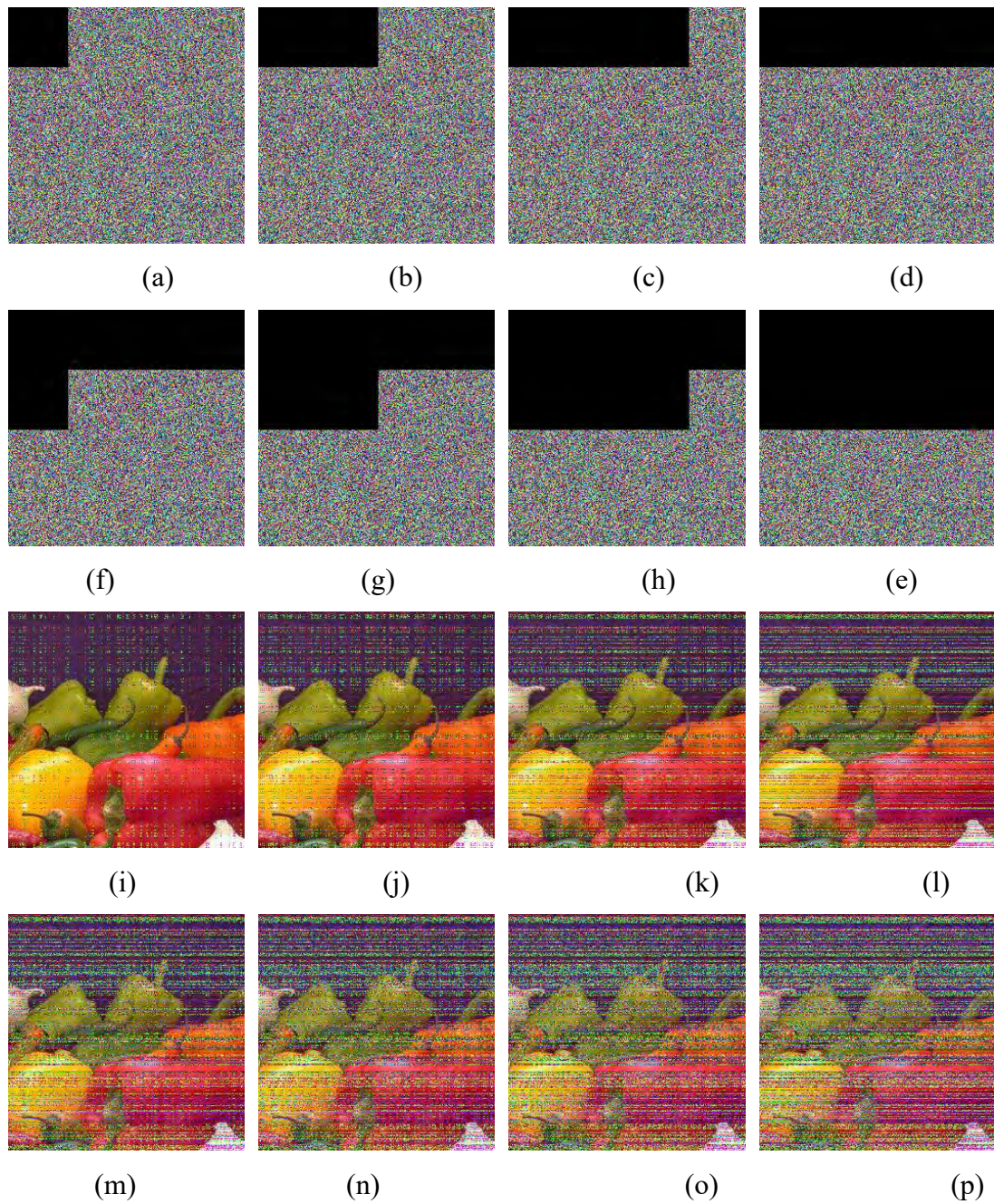


Figure 10. Occlusion attack: first two rows (a-e) Occluded ciphered images; last two rows (i-p) Deciphered images corresponding to occluded ciphered images.

The mathematical formula for computing PSNR is given by:

$$PSNR = 20 \cdot \log_{10} \left( \frac{255}{\sqrt{MSE}} \right)$$

where  $MSE$  (mean square error) is defined as:

$$\text{MSE} = \frac{1}{M \times N} \sum_{i=0}^M \sum_{j=1}^N [I(i,j) - I'(i,j)]^2$$

where  $I(i, j)$ ,  $I'(i, j)$  are the pixel values of the original and ciphered image respectively.

Table 10. UACI, NPCR, MSE and PSNR scores of proposed schemes

Noise Attack	Parameters	Proposed Encryption Scheme			
		PSNR	MSE	NPCR	UACI
Salt &peppers	0.0005	30.690	71.68	10.61	3.92
	0.005	28.965	103.12	15.62	5.61
	0.05	25.732	314.22	30.59	9.77
	0.5	20.126	587.76	49.98	16.3
Gaussian	0.0004	23.856	409.92	46.21.	12.54.
	0.0003	22.687	413.57	46.74	12.87
	0.0002	22.976	429.92	47.23	13.654
	0.0001	21.562	465.98	48.67	14.021
Occluded Attack	1/16	36.765	20.654	9.761	01.36
	1/8	34.932	32.453	15.54	03.15
	3/16	32.167	43.654	21.65	06.25
	1/4	29.765	55.176	25.76	07.75
	5/16	28.564	62.453	30.43	10.43
	3/8	26.876	76.987	37.65	13.65
	7/16	23.564	88.433	43.87	15.86
	1/2	20.543	120.76	49.54	21.76

### 3.5 Algorithm Complexity

Some of the factors such as Structure of CPU, memory size, image dimension plays a vital role in the execution of an encryption algorithm. Furthermore, the measurement of an algorithm is a very important part of computer science. An encryption algorithm is most efficient in terms of time complexity if completion of task requires the smallest number of operations. The standard way of expressing the time complexity of an algorithm using Big O notation. Therefore, the time complexity of our proposed encryption algorithm is discussed in the following steps.

**Step 1:** ( $p^2$ ) number of operations are expected to find all solutions of an elliptic curve.

**Step 2:** ( $M \times N$ ) number of operations are expected to permute each channel of the image.

**Step 3:** ( $p$ ) number of operations are expected to construct S-box.

**Step 4:** ( $p^2$ ) number of operations are expected to generate PRNGs.

**Step 5:**  $(M \times N)$  number of operations are expected in the final step.

Thus, our proposed encryption algorithm requires  $\mathcal{O}\{\max(p^2, M \times N)\}$  bits operations.

In the next chapter, we shall apply the core arithmetic operations of EC to generate efficient dynamic S-boxes and will also try to verify PRN sequences by using NIST analysis. Furthermore, we shall show the better passing performance of the proposed of PRN sequences as compared to some of the existing scheme.

## Chapter 4

# Efficient Random Numbers Generation and S-box Construction Scheme

In this Chapter, we present a smart-like algorithm based on subgroup co-set operations. The suggested scheme uses all co-sets that generates multiple sequences that can smoothly be adopted in most promising communication architectures of the future such as internet of things (IoT). Besides, the subgroup structure on a small prime with possible embedding is managed to construct efficient S-box. Whereas the performance of the proposed S-box will be examined via standardized tests thus found significant for multimedia data security applications. Moreover, a small prime based EC subgroup coset model will design, that generates a set of experimentally verified independent pseudo random streams.

This chapter introduces two different methods of PRNGs. In both methods EC operations will be used, which produces quality random numbers. However, the first method will use for the construction of S-box while the second method generates PRNGs. The graphical representation of complete chapter is shown in Figure 11.

### 4.1 Motivation

In recent decades, data security gets more and more attention due to rapid advancement in the fields of communication technology and computer vision [63]–[68]. The tools used to protect the contents of the data from the access of adversaries during transmission is cryptography. The security aspect of the secrete data entirely depends on the designing procedure of the cryptographic scheme. To design efficient cryptographic scheme, many researchers prefer to construct crypto algorithms rely on mathematical structures. Typically, the mathematical structures are used to generate PRNs, that play significant role in cryptographic schemes. In [13], [69], [70], chaotic based PRNs are constructed. The scheme in [5], utilized Bernoulli map for the construction of PRNs. The author also observed that our random numbers generator is more useful then Mersenne Twister MT19937. Payingat et al. [71], generated elliptic curve-based PRNs. Moreover, the author claimed that the proposed PRNs are much suitable for data encryption. Another interesting non-periodic PRNs are generated by Gaston E. Barberis in [72] using logistic maps. To increase the performance ability of the cryptosystem, researchers make use of pseudo random numbers generators (PRNGs) based

on algebraic structures. The PRNGs with sufficient size and randomization are widely used in the cryptographic systems, that strengthen its security characteristic. In addition, it plays central role in electronic games, simulation and cryptography. To examine the predictability feature, the NIST testing tool affirms whether the PRNGs are random or not. The internet source that is worldwide used to shared media files such as text, image, and video. On the other hand, transmission security is prominent against eavesdroppers. For instance, some digital images having bio-signal of irises, fingerprints. Various cryptographic algorithms including image encryption schemes are being established using PRNGs. Ramesh et al. [73], presented two phase image encryption scheme using combination of two pseudo random generators, which is fast to implement for image encryption. Fathi et al. [6], proposed PRNs generated scheme rely on ECC for image encryption. Furthermore, they discussed the applications in the back-door problems efficiently. Elliptic curve-based cryptography was first introduced in 1985 by Koblitz [11] and Miller [10]. Reyad et al. [14], encrypted the original image through Koblitz encoding algorithm and Chaos-Driven elliptic curve PRNGs (C-D ECPRNG). In [11], the author made a connection between the discrete logarithm problem (DLP) and EC. Since then, many researchers made their efforts to employ ECC using various encryption techniques to enhance its performance. Later on, Amara et al. [15], showed that the ECC based cryptosystem provide better security than RSA. In [6], a technique for an image encryption is established that utilizes a combination of Elliptic Curve Based Random Number Generator (EC-B-RNG) and AES (Advanced Encryption System). Accordingly, the scheme gets better results for image encryption. In this method, the PRNs are computed followed by public shared key and the base point of the elliptic curve group. Then, AES algorithm is performed to complete the encryption. In symmetric key algorithm such as AES, the S-box is the main non-linear component. This module is capable of being creating confusion between the key and cipher data as discussed in [74] by Claude Shannon. In recent years, various algorithms have been appeared in the literature for the construction of S-box [75]–[77]. Authors [72], adopt cubic polynomial map for the construction of S-box. This technique is considered useful because of its simple implementation. Due to the their highly sensitive and random natures, the chaotic and EC structures are the best choices for the researchers for generating random numbers and S-boxes. Therefore, these are widely adopted in image data encryption and hardware security schemes [5]–[8], [78]. The public key based cryptosystem is introduced to encrypt image data via two phase (EC and AES (Advanced Encryption Standard)) [6]. The former phase EC is deployed to generate effective random

sequence while the latter one is used traditionally. Farwa el al.[5] described an efficient encryption algorithm, which utilized Fresnelet transform and EC over Galois field.

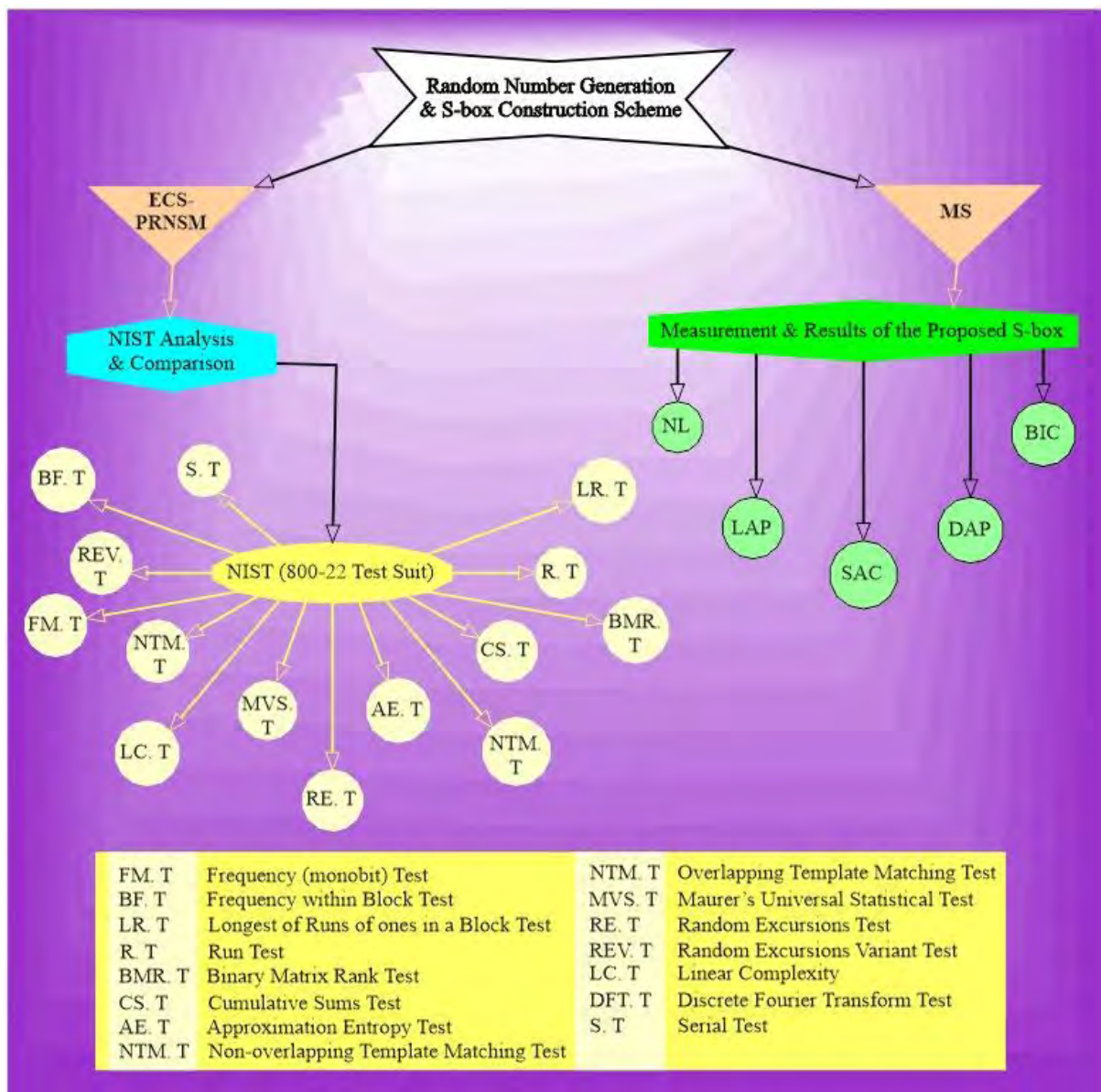


Figure 11. Chapter description (Flowchart)

## 4.2 Basic Concepts

An elliptic curve  $E_{a,b}^p$  defined over a prime field  $F_p$ , is an algebraic expression of the form

$$y^2 = (x^3 + ax + b) \text{mod } p \quad (1)$$

where  $a, b \in F_p$  and  $p > 3$  with the condition

$$(27b^2 + 4a^3) \neq 0(\text{mod } p).$$

The set of all solutions  $(x, y)$  to the equation (1) are the points of the ring  $F_p \times F_p$ . Apart from that, a point at infinity "O" is added to the set of solutions as an identity element. These points form an abelian group under the elliptic curve addition operation given in [1] and

denoted as  $E_{a,b}^p(F_p)$ . In this manuscript, we refer to an elliptic curve rather than an elliptic curve over a prime field, otherwise stated.

#### 4.2.1 Elliptic Curve Group Operations

The primary operations for the elliptic curve points group (EC-PG) are the main concern in this section. The scalar multiple of an element of EC-PG is much harder task as compared to do in other group structures. The core idea behind the scalar multiplication depends on the point addition and point doubling.

$$P + O = P, \text{ for all } P \in E^{(a,b,p)}$$

#### 4.2.2 Point Addition Formula

For any  $P_1 = (x_1, y_1)$ ,  $P_2 = (x_2, y_2) \in E_{a,b}^p(F_p)$  with  $P_1 \neq P_2$ . Then the sum  $P_1 \oplus P_2 = R = (x_3, y_3)$  is also an element of  $E_{a,b}^p(F_p)$  using the method given as follows

$$R = (x_3, y_3) = (\lambda^2 - x_1 - x_2 \text{ mod } p, \lambda(x_1 - x_3) - y_1 \text{ mod } p),$$

Where  $\lambda$  represents the slope of the line between  $P_1$  and  $P_2$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \text{ mod } p$$

#### 4.2.3 Point Doubling Formula

For any  $P = (x_0, y_0) \in E_{a,b}^p(F_p)$ . Then  $Q = P + P = (x, y)$  is calculated as

$$Q = (x, y) = (\mu^2 - 2x_0 \text{ mod } p, \mu(x_0 - x) - y_0 \text{ mod } p)$$

Whereas  $\mu$  is the derivative of  $E_{a,b}^p$  at  $P$ . The mathematical expression for  $\mu$  is given below

$$\mu = \frac{3x_0^2 + a}{2y_0}$$

The other properties of the group such as unique inverses and associativity are easily verified using sections 4.2.2 & 4.2.3. Aside from that, the doubling formula is applied one time while obtaining  $k$ -length sequence using single point of EC. On the other hand, the formula in 4.2.2, is promising in generating the terms of the sequence up to the required length. We recall some results:

**Theorem 4.1.** [[1], Hasse's Theorem] Let  $E_{a,b}^p$  be an elliptic curve over the finite field  $F_p$ . Then the order of  $E_{a,b}^p(F_p)$  satisfies

$$|q + 1 - \#E_{a,b}^p(F_p)| \leq 2\sqrt{q}.$$

**Lemma 4.1.** [[1], Lemma 4.33] An elliptic curve  $E_{0,b}^p$  over a prime field  $F_p$  with  $p - 2 \equiv 0 \pmod{3}$  has exactly  $p + 1$  distinct points and each integer in the field  $F_p$  appear once as  $y$ -coordinates.

**Proposition 4.1.** [[4], page 230] If  $r/\text{ord}(G)$ , where  $G$  a finite Abelian group  $G$ , then there exists a subgroup of order  $r$  in  $G$ .

### 4.3 Mechanism for S-box (MS)

In this section, we discuss the idea of S-box. The construction of S-boxes is one of the main fulcrums to validate the security of symmetric cryptographic algorithms [79] and it is a prime module of non-linear mappings. It was proposed in 1949 by Claude Shannon [74]. The central objective of an S-box is to make the relation confused between the ciphered data and the keys used in ciphering. Therefore, generating efficient S-boxes through secure techniques are the utmost requirement of modern cryptographic schemes. For this purpose, the security of an elliptic curve structure enhanced our attention for designing S-boxes via its core operations. In this connection a simple and fast algorithm is introduced in this section. Initially, select a prime  $\rho$  and a point  $P = (x, y)$  with  $\rho \equiv 2 \pmod{3}$  and  $\rho > 257$ . Then generate a subgroup  $\aleph = \langle P \rangle$  of order  $k_1$ . Then collect all points  $G_{i=1}^{\rho+1} \in \aleph \cup \{E_{0,t}^\rho(F_\rho) \cap \aleph^c\}$  and sort the points  $G_{i=1}^{k_1} \in \aleph$  and  $G_{i=k_1+1}^{\rho+1} \in E_{0,t}^\rho(F_\rho) \cap \aleph^c$  to construct Substitution box S-box using  $y$ -coordinates of  $S_P^{0,t,\rho} = G_{i=1}^{k_1} \cup G_{i=k_1+1}^{\rho+1}$ . By Lemma 4.1 prime field and given elliptic curve have some special relation [1]. Therefore, it is possible to use only subgroup generated by base elements of EC. However, it may be time consuming to look for the base points of EC. So, without loss of generality, we simply pick any single point on EC, and then form a subgroup preferably a proper subgroup. As it is also required to reduce the time complexity by using a proper subgroup. The construction process is clearly shown in Algorithm 1, while its outcome for  $\rho = 521, t = 91, P = (460, 74)$  is shown in Table 11. Similarly, Table 12 provides results of some common tests and their comparison with that of some existing S-boxes.



**Algorithm 1:** Construction of proposed  $8 \times 8$  S-box

**Input:** A subgroup  $\mathfrak{K} = \langle P \rangle$ , a minimum order of 257 generated by some point  $P = (x, y)$  lying on elliptic curve  $E_{0,t}^\rho$  with prime  $\rho \equiv 2 \pmod{3}$ .

**Output:** Substitution box  $S_p^{0,t,\rho}$  ( $8 \times 8$  S-box)

1.  $P := (x, y)$ ;
2.  $1 \leftarrow i$  do
3.  $R = P \oplus P$ ;
- While**  $R \neq \infty$
- $S_i = P \oplus R$
- $i + 1 \leftarrow i$  do
4. **end while**
5.  $h_1 = \{X(i)\} \cup \{x\}$
6.  $h_2 = \{Y(i)\} \cup \{y\}$
7.  $\mathfrak{K} = [h_1, h_2]$
8.  $K = E_{0,t}^\rho(F_\rho) \cap \mathfrak{K}^c$
9.  $K = [s_1, s_2]$
10.  $S_p^{0,t,\rho} = \{s_2\}$

The security analysis of the proposed S-box is to verify the cryptographic strength of the proposed S-box algorithm, we carried out several standard measurements (Tests). The briefly discussion is given below.

#### 4.3.1 Measurements and Results of the Proposed S-box

A substitution box S-box with good cryptographic properties (CP), affirms high security of the encryption scheme against cryptanalyst. To check the strength of CP of an S-box, some commonly used measurements (Tests) such as nonlinearity (NL), bit independent criterion (BIC), linear approximation probability (LAP), differential approximation probability (DAP) and strict avalanche criterion (SAC) play vital role. The concept of NL is essential component among those cryptographic measurements on the Boolean functions which is thoroughly presented in [80]. Now and in the foreseeable future, it has undoubtedly been affirmed its importance in cryptosystems against various linear assaults [81].

Table 11: The proposed S-box  $S_{(460,74)}^{0,91,521}$

13	54	140	102	23	246	9	84	31	147	109	110	85	123	225	209
130	60	180	120	192	94	142	35	144	30	152	135	59	64	219	185
243	105	98	227	77	45	46	199	153	247	146	66	67	183	127	237
201	61	95	15	92	69	251	56	89	6	220	14	252	76	10	20
3	249	191	43	149	1	26	138	112	151	148	53	104	228	179	12
107	197	236	38	165	167	91	238	47	215	216	71	33	204	8	226
162	141	211	212	83	145	99	250	156	189	22	126	196	68	136	203
132	75	16	39	96	161	48	134	174	154	214	87	111	52	44	158
70	253	232	160	113	157	240	166	2	57	241	4	150	223	177	106
80	198	90	7	88	122	21	229	217	235	50	190	173	184	143	222
248	11	205	159	81	168	51	118	101	63	195	116	97	234	73	210
186	5	114	170	125	193	213	41	255	49	65	218	194	163	124	29
121	19	128	139	221	42	164	32	58	18	175	182	242	181	233	133
245	129	208	115	202	0	17	207	231	206	25	224	176	108	187	137
28	55	78	37	86	40	254	155	188	178	239	119	27	230	171	74
62	131	172	93	79	117	24	34	100	82	72	200	36	244	169	103

The optimal score of non-linearity of an S-box is 120. The average value of nonlinearity of our designed S-box  $S_{(460,74)}^{0,91,521}$  is 107. BIC is a significant property in the measurements of an S-box, introduced by Webster and Tavares in [82]. This criterion is depending on the correlation between the output vector correspond to slightly change in input bits vector. The BIC score lies in the interval [0,1]. LAP [22], is an important feature in the measurements of strength of an S-box. It measures the highest probability value of an event with same parity of bits masked of input and output for different combinations of bits. DAP is the study of differential uniformity in an S-box. The minimum the DAP score of an S-box, the more it efficient against differential assaults. Webster and Tavares in [82], presented another criterion, called strict avalanche criterion (SAC). SAC of an S-box is an attractive property that examines the half bits change in the output by flipping a single bit of the input. The above Table 12, indicates that the average nonlinearity of the proposed S-box is better than the existing S-boxes in [39], [83], [84], while minimum value of NL is greater than the S-boxes generated in [39], [71], [83], [84], which clearly shows that proposed technique has the

capability of generating efficient S-boxes to transform the input data of the image to cipher output data.

Table 12. Results and comparisons with existing S-boxes

S-box	NL			BIC		LAP	DAP	SAC		
	Min	Avg	Max	Min	Avg			Min	Avg	Max
Proposed	106	107	108	0.46289	0.50223	0.125	0.039062	0.40625	0.49829	0.578125
Ref.[71]	104	--	--	0.4667968	0.5022	0.13290	0.0234375	0.40625	0.497558	0.6250
Ref.[12]	106	--	--	0.4707031	0.5013	0.14060	0.0234375	0.390625	0.49415	0.6094
Ref.[39]	104	105.8	108	--	0.5032	0.12500	0.0390625	--	0.4976	--
Ref.[84]	100	104.7	108	--	0.4942	0.14063	0.0390625	--	0.4982	--
Ref.[26]	104	106	110	--	0.5058	0.14063	0.0390625	--	0.5039	--
Ref.[27]	104	--	--	0.4667969	0.4989	0.05470	0.0391000	0.4018	0.4946	0.5781
Ref.[85]		106		0.5023		0.12500	0.0313000	0.4958		

Furthermore, the average scores for the BIC and SAC of  $\mathcal{S}_{(460,74)}^{0,91,521}$  are slightly more close to optimal score as compare to the S-boxes in [39], [83], [84], and the minimum score of the SAC of  $\mathcal{S}_{(460,74)}^{0,91,521}$  is greater than or equal to the SAC scores of S-boxes constructed in [71], [84], [86]. Similarly, the SAC maximum score of  $\mathcal{S}_{(460,74)}^{0,91,521}$  is far better than that of [15], [71], and approximately equal to the S-box in [86]. Thus, it is clearly revealed that our designed S-box is more capable of creating confusion in the cipher data than that of S-boxes designed in [39], [83], [84]. Additionally, the DAP score of our proposed S-box  $\mathcal{S}_{(460,74)}^{0,91,521}$  is comparable with all S-boxes [39], [83], [84], which is enough to resist against differential attacks. Moreover, the LAP score of our suggested S-box  $\mathcal{S}_{(460,74)}^{0,91,521}$  is not so bad to resist against linear attacks.

#### 4.4 EC Subgroup PRNS Module (ECS-PRNSM)

In this section, we introduced a new efficient algorithm in order to generate ECS-PRNSM (EC subgroup PRN sequences module) using points on EC. The multi set of sequences arise a question, whether the proposed algorithm allows us to generate independent sequences using single seed. The answer to this is follows from the Lemma 4.1. In which we tried to prove that the sequences obtained, are independent. A non-trivial and proper cyclic subgroup of  $E_{0,a}^p(F_p)$  is the key requirement for the generation of ECS-PRNSM. The process description of the proposed scheme is given as under. For any prime number  $p > 2$  and  $a \in F_p$  satisfying Lemma 4.1. There exists an elliptic curve  $E_{0,a}^p$  over a field  $F_p$  with  $E_{0,a}^p(F_p)$  as a group. Since  $E_{0,a}^p(F_p)$  is abelian group, then every divisor of  $\text{Ord}(E_{0,a}^p(F_p))$  produces a subgroup of that order. Let a point  $P_0$  is chosen at a random lying on EC  $E_{0,a}^p$  such that

$$\text{Ord}(P_0) \ll \text{Ord}(E_{0,a}^p(F_p)).$$

Furthermore, we need to introduce some notations and basics of proposed ECS-PRNSM scheme. The term  $\text{Ord}$  represents the order of an element. Let  $|\mathcal{H}| = |P_0 \setminus \{\infty\}| = n$ , that is,  $n + 1$  is number of elements in the cyclic group  $\langle P_0 \rangle$  generated by  $P_0$ ,  $K = E_{0,a}^p(F_p) \setminus \{\infty\}$  and  $M = K \cap \mathcal{H}^c$  with  $\mathcal{H}^c = E_{0,a}^p(F_p) - \mathcal{H}$ , cardinality of  $M$  is  $r$ . The set  $W = \prod_{i=1}^r M$  is cartesian product of  $M$ . Consider the set

$$G \subset W \text{ and } G = \{(g_1, g_2, \dots, g_r) : g_i \neq g_j \text{ for all } i \neq j\}$$

Moreover, for any  $g \in G$ , we define a set

$$g + \mathcal{H} = \{g + Q : g + Q = (g_i \oplus Q) ; \forall Q \in \mathcal{H}\}$$

Define a map

$$\begin{aligned} \omega_y : g + \mathcal{H} &\rightarrow (F_p)^r \\ \omega_y((g_i \oplus Q)) &= (y_i^{Q_i}) \end{aligned}$$

Where  $y_i^{Q_i}$  is the  $y$ -coordinate of  $g_i \oplus Q$ .

**Proposition 4.2:** The mapping  $\omega_y$  is one-one.

**Proof.** First, we show that the mapping above is well defined. Let for any  $g + Q_1, g + Q_2 \in g + \mathcal{H}$  with  $Q_1 \neq Q_2$ . Let  $g + Q_1 = g + Q_2$ . Implies that  $(g_i \oplus Q_1) = (g_i \oplus Q_2)$  for all  $i$ . On contrary, suppose  $\omega_y(g + Q_1) \neq \omega_y(g + Q_2)$  implies that  $(y_i^{Q_1}) \neq (y_i^{Q_2})$ , which implies  $y_i^{Q_1} \neq y_i^{Q_2}$ , for some  $i \leq r$ . Then there exists some  $g_i \in g$  such that  $g_i \oplus Q_1 \neq g_i \oplus Q_2$ , for some  $i$ . Which is contradiction to the fact  $g + Q_1 = g + Q_2$ . So,  $\omega_y(g + Q_1) = \omega_y(g + Q_2)$ . Therefore,  $\omega_y$  is well defined.

To show that the map  $\omega_y$  one-one. Let  $g + Q_1, g + Q_2 \in g + \mathcal{H}$  with  $Q_1 \neq Q_2$ ,  $\omega_y(g + Q_1) = \omega_y(g + Q_2)$  implies that  $(y_i^{Q_1}) = (y_i^{Q_2})$ . On contrary, suppose that

$g + Q_1 \neq g + Q_2$ , then  $g_i \oplus Q_1 \neq g_i \oplus Q_2$ , for some  $i$ . Thus,  $y_i^{Q_1} \neq y_i^{Q_2}$  or  $x_i^{Q_1} \neq x_i^{Q_2}$  for some  $i$ . This implies that if  $y_i^{Q_1} \neq y_i^{Q_2}$  for some  $i$ , then it clearly contradicts the fact in equation (3). So,  $y_i^{Q_1} = y_i^{Q_2}$ , for all  $i$ . On the other hand, if  $x_i^{Q_1} \neq x_i^{Q_2}$  for some  $i$ . Which is again a contradiction to the fact in Lemma 4.1. Thus  $x_i^{Q_1} = x_i^{Q_2}$ , for all  $i$ . Consequently  $g + Q_1 \neq g + Q_2$ , and the mapping  $\omega_y$  is one-one.

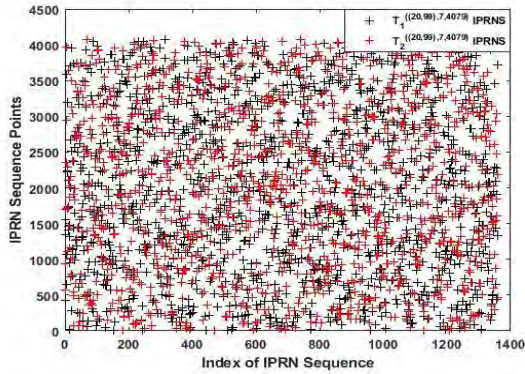
Obviously, Propositions 4.1 and 4.2, facilitate to generate with confirmation a set  $A = \{T_n^{P_0, c, p}\}$  of dimension  $n \times r$  consisting of multi-independent pseudo random sequences and the point  $P_0$  of order  $n + 1$ . Figure 12, shows the mutual dissimilarity pattern among these

**Algorithm 2.** Generation of ECS-PRNSM

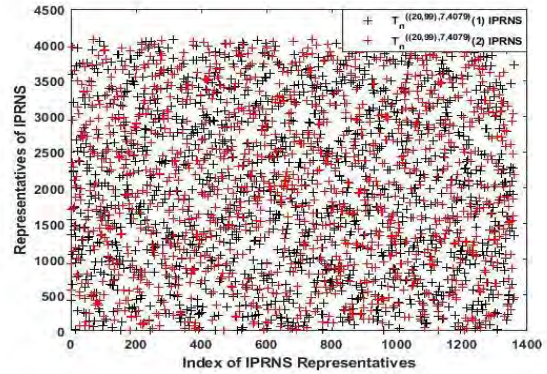
**Input** A subgroup  $\mathcal{H} = \langle Q \rangle$ , generated by some point  $Q = (x, y)$  lying on elliptic curve  $E_{b,a}^p$  with number of points  $E_{b,a}^p(F_p)$  and prime  $p = 2(\text{mod}3)$ .

**Output** Random number sequences  $S_{i=1}^n$

1. Start
2.  $\mathcal{T} := \emptyset$
3.  $\mathcal{H} = \langle Q \rangle$ , %Algorithm 1
4.  $X_1 := \mathcal{H}(:, 1)$
5.  $Y_1 := \mathcal{H}(:, 2)$
6.  $\mathcal{B} := \mathcal{H}^c \cap E_{b,a}^p(F_p)$
7.  $\mathcal{B} := \text{sortrow}(\mathcal{B}, 2)$
8.  $[r_1, r_2] := \text{size}(\mathcal{H})$
9.  $[s_1, s_2] := \text{size}(\mathcal{B})$
10.  $\mathcal{C} := []$
11.  $[r + 1, r + 1] := \text{size}(\mathcal{C})$
12.  $[s + 2, s + 2] := \text{size}(\mathcal{D})$
13.  $i = 1$  and  $j = 1$
14. **while**  $i \leq s$  **do**
15. **while**  $j \leq r$  **do**
16.  $R := \mathcal{B}_i \oplus \mathcal{H}_j$
17.  $i = i + 1$
18. **end while**  $i$
19.  $j = j + 1$
20. **end while**  $j$
21. **return**  $\mathcal{C}(R(:, 2))$
22. **end for**
23.  $\mathcal{C}$
24.  $\mathcal{T} := [\mathcal{C}, Y_1]$



(a)



(b)

Figure 12. (a)-(b) show the clear picture of pointwise dissimilarity between consecutive rows and columns. (a) first 1360 random stream of consecutive rows (b) Representatives of each ECS-PRNSM on consecutive indexes.

sequences. Furthermore, the dimension of  $A$  is directly proportional to the choice of a prime  $p$  and order of the point  $P_0$ .

**Proposition 4.3:** Let  $I_{u \times v}$  be an image data and a prime number  $P$  such that  $\max\{u, v\} < P < u \times v$  with  $p = 2(\text{mod}3)$ . Then there exists a subgroup  $\mathcal{H} \leq E_{0,b}^P(F_p)$  such that encryption scheme is possible.

**Proof.** Proof followed by propositions 4.1 and 4.2.

#### 4.5 NIST (800-22 test suit)

Numerous statistical tests are performed to determine the randomness quality of the ECS-PRNSM. In this reason, NIST test suite is the standard tool for evaluation of the sequence. The test suite consists of fifteen tests of different natures for computing and evaluation of the randomness of cryptographic generated ECS-PRNSM [73]. These tests are briefly discussed in the following.

##### 4.5.1 Frequency (monobit) Test (FM. T):

The frequency test is focus on the proportion of zero's and one's on the whole sequence. A bit's sequence is passing the frequency monobit test if its test score attains minimum value of 0.01. All these tests depend on being successful of this test.

##### 4.5.2 Frequency Test within Block (BF. T)

The prime idea of this test is to examine the percentage of ones in M-bits blocks. If the frequency of ones in each M-bit block is close to  $\frac{M}{2}$  of a sequence, the sequence is said to satisfy BF test criteria.

##### 4.5.3 Longest of Runs of Ones in a Block Test (LR. T)

LR. T calculates the probable value of longest runs of ones in a sequence.

##### 4.5.4 Run Test (R. T)

An R. T determines the expected value of number of runs of zeros and ones of different lengths in a sequence.

##### 4.5.5 Binary Matrix Rank Test (BMR. T)

The main motive behind BMR. T is to inspect whether the substrings of a constant length of the original sequence have linear dependence among them.

#### **4.5.6 Cumulative Sums Test (CS. T)**

CS. T is used to examine the cumulative sum in the tested sequence of partial sequences occurred, relative to the expected behavior of that cumulative sum for random sequences.

#### **4.5.7 Approximation Entropy Test (AE. T)**

For the comparison of overlapping blocks' frequency of two consecutive lengths ( $n$  and  $n+1$ ) with the probable outcome for any random sequence. The length might be taken to be 10 bits of each block.

#### **4.5.8 Non overlapping Template Matching Test (NTM. T)**

The rejection of a sequences based on too many occurrences of a given non periodic pattern is made by this test.

#### **4.5.9 Overlapping Template Matching Test (OTM. T)**

The rejection of a sequences based on deviations from the expected number of runs of ones of a given length is made using this test.

#### **4.5.10 Maurer's Universal Statistical Test (MUS. T)**

MUS. T is used to compress a sequence without losing information.

#### **4.5.11 Random Excursions Test (RE. T)**

The purpose of this test is to determine if the number of times a particular state is visited within a cycle deviate from expected value for a random sequence.

#### **4.5.12 Random Excursions Variant Test (REV. T)**

The key role of this test is the detection of deviations of various stats from the expected number of visits in the random walk.

#### **4.5.13 Linear Complexity (LC. T)**

This test determines whether the structure of the sequence is complex enough to be considered random.

#### **4.5.14 Discrete Fourier Transform Test (DFT. T):**

The core phenomenon of DFT. T is to detect the repetitive patterns in the tested sequence that would exhibit a deviation from the assumption of randomness.

#### 4.5.15 Serial Test (S. T)

To determine the similarity between the number of occurrences of the  $2^m$   $m$ -bit overlapping patterns and expected for a random sequence is judged using this test.

### 4.6 NIST Analysis and Comparison

In this section, we present the NIST statistical Testing tool to evaluate the bits sequence for randomness. The package comprises fifteen different tests. A sequence is assessed through each test separately. The sequence that passes all the tests would call random otherwise insufficient. The passing score for each test is the numerical value  $P$ , which is greater or equal to pre-defined threshold  $\beta$ . The sequence that satisfies the test criteria relative to  $\beta$  is random with confidence of  $1 - \beta$ .

Our ECS-PRNSM are evaluated by setting  $\beta = 0.01$ , which imply that a sequence is accepted as random with confidence 0.99 unless it's  $P$  value is greater than 0.01. 1359 sequences are generated by the proposed mechanism, each of length 32652 bits. Then, employed each test to compute  $P$  values for their respective sequence. The test results in terms of  $P$  values of the proposed sequences are shown in table 1. Likewise, the ratio of the passing sequences to the total number of sequences are computed too. The single most remarkable fact to emerge from the Table. 13 is that the tests  $FM. T$ ,  $CS. T$ ,  $R. T$ ,  $S. T$  and  $AE. T$  are easily verified by each sequence, whereas for the remaining tests except  $MUS.T$ , the average value of the proportions is 99.1%. These facts indicate that our proposed scheme gives great confidence in generating maximum number of bitstreams then the scheme in [87]. The drawback of the pseudo random sequences generated by the scheme in [87] is that, some of the sequences fail to satisfy each test. Moreover, the ignorance of its application aspect also arises a question mark on its efficiency. In [88], the authors developed a novel TRNG scheme using stochastic diffusive memristor. In this technique, 76 sequences are generated and assessed using NIST 800-22 test suite. Furthermore, the scheme hardly generates the random sequences with proportion value 0.95, which is in fact much less than the proportion value produced by our scheme. This fact is revealing that our proposed technique is far better as compare to the scheme in [88].

In the next Chapter, we shall present the practical application of ECS-PRNSM and MS in multimedia data security along with S-box and PRN mechanisms. Besides a well-defined



mathematical model (MM) will introduce for practical implications regarding smooth diffusion that will make it easy to stretch via slight change in one of its secret keys.

Table 13. NIST (800-22 test suit) results for ECS-PRNSM subgroup-based pseudo random number sequences

<i>S.No</i>	<i>Test name</i>	<i>Number of sequences with <math>p \geq 0.01</math>(Passed)</i>	<i>Number of sequences with <math>p \leq 0.01</math>(Failed)</i>	<i>Passing Rate</i>
1	<i>FM. T</i>	1359	0	1
2	<i>CS. T(Forward)</i>	1359	0	1
	<i>CS.T(Backward)</i>	1359	0	1
3	<i>LC. T</i>	1334	15	0.9816
4	<i>BF. T</i>	1350	9	0.9934
5	<i>LR. T</i>	1344	15	0.9889
6	<i>R. T</i>	1359	0	1
7	<i>BMR. T</i>	1337	22	0.9838
8	<i>NTM. T</i>	1349	10	0.9926
9	<i>OTM.T</i>	1357	2	0.9985
10	<i>S. T Test 1</i>	1359	0	1
	<i>Test2</i>	1359	0	1
11	<i>MUS.T</i>	<i>Not applicable</i>	-----	-----
12	<i>DFT. T</i>	1343	16	0.9882
13	<i>AE. T</i>	1359	0	1
<i>14 RE. T (Sample=1300)</i>				
1)	<i>x=-4</i>	1281	19	0.9853
2)	<i>x=-3</i>	1285	15	0.9885
3)	<i>x=-2</i>	1292	8	0.9938
4)	<i>x=-1</i>	1290	10	0.9923
5)	<i>x=1</i>	1293	7	0.9946
6)	<i>x=2</i>	1294	6	0.9954
7)	<i>x=3</i>	1291	9	0.9930
8)	<i>x=4</i>	1292	8	0.9938
<i>15) REV.T(Sample=1300)</i>				
1)	<i>x=-9</i>	1291	9	0.9930
2)	<i>x=-8</i>	1290	10	0.9923

3)	$x=-7$	1290	10	0.9923
4)	$x=-6$	1287	13	0.9900
5)	$x=-5$	1291	9	0.9930
6)	$x=-4$	1287	13	0.9900
7)	$x=-3$	1292	8	0.9938
8)	$x=-2$	1292	8	0.9938
9)	$x=-1$	1288	12	0.9907
10)	$x=1$	1287	13	0.9900
11)	$x=2$	1289	11	0.9915
12)	$x=3$	1293	7	0.9946
13)	$x=4$	1293	7	0.9946
14)	$x=5$	1292	8	0.9938
15)	$x=6$	1291	9	0.9930
16)	$x=7$	1292	8	0.9938
17)	$x=8$	1289	11	0.9915
18)	$x=9$	1291	9	0.9930

## Chapter 5

# Mathematical Model Based on PRN with Image Encryption Applications

It is very hard to design a cryptosystem that could be implemented to secure all types of multimedia data regardless of its dimension. Since a single seed may not cover to manage all dimensions simultaneously. To achieve this goal, we proposed an image encryption system with large key space, quality encryption and smooth decryption process that probably works to encrypt image data of any size. The whole description of this chapter is shown in Figure 13.

### 5.1 Motivation

Nonlinear dynamical systems have wide range of applications in multimedia data security. In some systems such as chaotic systems, the security risk and computational efforts are depended to some extent on their dimensions. High dimensional chaotic systems are considered secure as compared to low dimensional chaotic system. However, in respect to computational complexity, these require more calculation time in the designing of cryptosystems. Besides, low dimensional chaotic systems are apparently more at risk against cryptanalysis attacks due to small key space [9].

On the other hand, elliptic curve EC structures are found better to overcome these issues while generating random numbers [10]. Toughi et al. [6], developed an image encryption technique adopts pseudo random architecture using an EC with finite field as a domain. Haider et al. [78], investigated a scheme with an image application based on PRNs, permutation-substitution modules. In [6], [89], pseudo random numbers schemes are stacked to create better diffusion impact in the image data. Although, in these schemes, the authors effectively made use of core operations of EC, but at least two core operations are required to obtain each random number [6]. Consequently, it is more costly and higher computational complexity during its real time implementation. Similarly, pseudo random numbers are generated to design an efficient image encryption schemes [78], [90], but their efficiency is not verified through one of the standardized tests suits such as NIST 800-22 or DIEHARD.

To address these problems more efficiently and reduce the time complexity, we design a smart-like cryptosystem for image data encryption based on EC core structure. With the help of the EC core structure, the level of randomness in the output data is increased, so that it passes almost all standardized tests. As a result, the original content is almost impossible for adversary to recover once masked with the data generated using proposed structure. In this way, one may consider the core operations of EC as a striking feature of the proposed work. Besides EC core operations, a well-known group technique is performed to develop S-box and PRN construction mechanisms. Along with S-box and PRN mechanisms, a well-defined mathematical model (MM) is introduced for practical implications regarding smooth diffusion. The reason behind the smooth diffusion is that it can be easy to stretch via slight change in one of its secret keys. Consequently, it is the main source of the proposed scheme for diffusing all kind of multimedia data having any dimension. In other words, our scheme is not limited to generate a single PRN sequence and S-box, but rather multiple independent PRN sequences (IPRNS) and S-boxes in a single round. Generally, multiple sequences and S-boxes are mainly generated to cipher multiple data files simultaneously. As far as the time complexity is concerned, there exactly two operations are attached to obtain each pseudo random number. To the best of author knowledge, this algebraic aspect of EC is not addressed for the purpose to generate random sequences in the recent past. The main intention behind the proposed scheme is to enlighten the strength and efficiency of the purely algebraic EC-group structure. The generation of IPRNS in the ECS-PRNSM are obtained through group theoretic coset operation on EC over a small prime. Likewise, S-box generation technique is developed using embedded sample of elements to the subgroup of elliptic curve point group (EC-PG). These jointly generate an efficient and smart cryptosystem for practical implications.

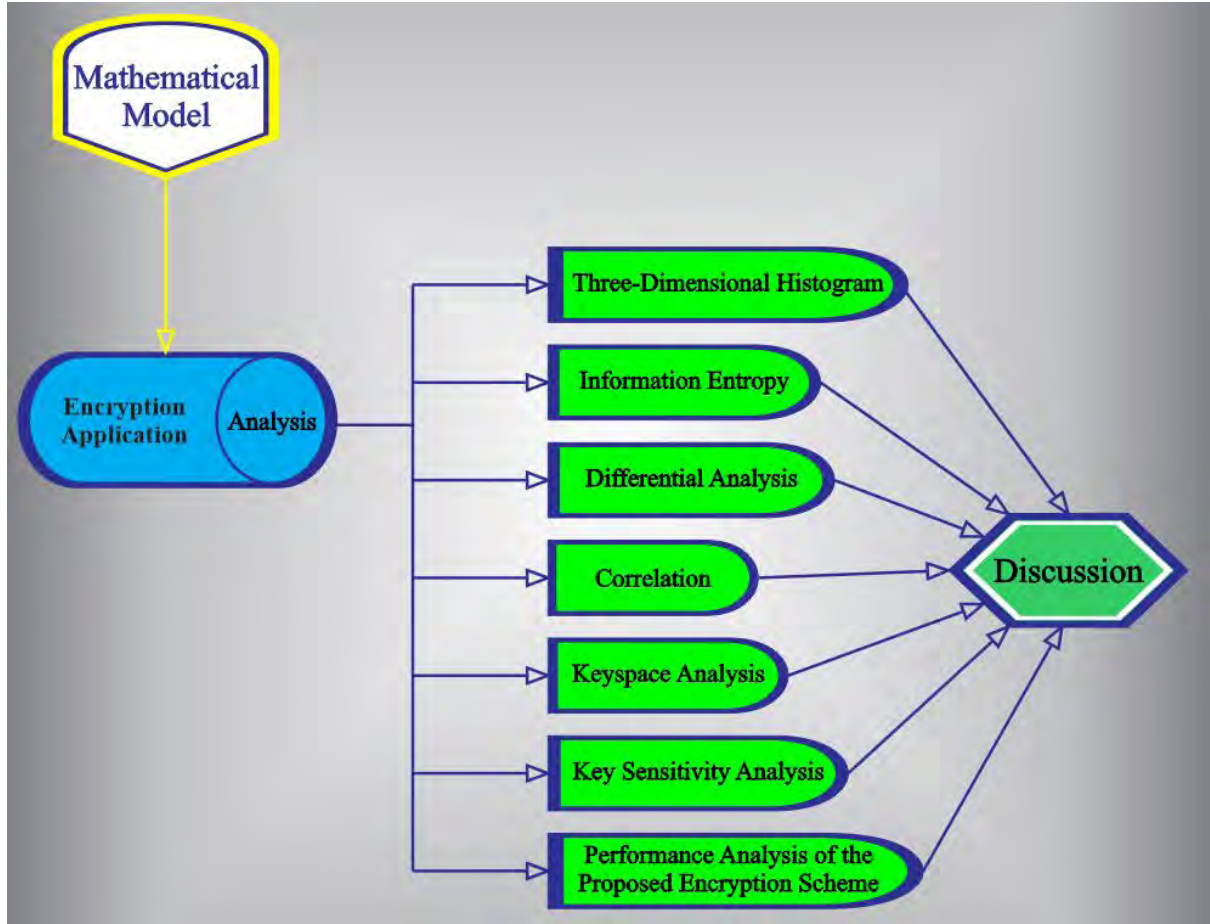


Figure 13. Chapter description (Flowchart)

## 5.2 Mathematical Modeling for Image Encryption

In this section, the plain image data  $I_{u \times v}$  is chosen to encrypt through proposed cryptosystem. This encryption process consists of two modules 4.3 & 4.4, the implementation output is shown in Figures 14, 15 & 16. The detailed description of our proposed scheme is given by the following steps

**Step.1.** Without loss of generality, we assume the sequences set  $W$  sized  $n \times r$ , and a prime  $p$  is

chosen with  $n + r < p < u \times v$ , satisfying proposition 4.2. Select some  $i \leq n$  and  $j \leq r$ , there exists a triplet  $\mathcal{M} = (\mathcal{H}, T_i^{P_0, c, p}, g_j + \mathcal{H})$  with y-coordinates express as  $(\mathcal{H}, T_i^{P_0, c, p}, g_j + \mathcal{H})_y = F_p^\times$ . Meanwhile, elliptic curve  $E_{0, b}^p$  with y-coordinates  $e_{b, y}^p$  except zero entry is adopted to act on the triplet  $(\mathcal{H}, T_i^{P_0, c, p}, g_j + \mathcal{H})$  as permutation. The generalized mathematical model is defined below

$$\mu: e_{b, y}^p \times \mathcal{M} \rightarrow F_p$$

$$\{\text{if } e_{(m+l)} \leq \text{ord}(\mathcal{M}), \text{ for some } l \in F_p^\times \text{ and } m = 1, 2, \dots, n\}$$

$$\mu(e_{b,y}^p, m) = \mu(e_m, m) = m_{e_{(m+l)}}$$

**Step.2.** Collect non-repeated random streams of length  $r$ , which refer as  $\mathcal{M}_n$ . On the other hand, pick out

an arbitrary  $\alpha \in \mathcal{M}_n$  and sort a set  $\mathcal{M}_n$  as

$$\mathcal{M}_\alpha = \{\mathcal{M}_n(k) \preceq \mathcal{M}_n(l) ; \forall \mathcal{M}_n(k) \geq n - \alpha ; \text{where } k, l \in \{1, 2, \dots, n\}\}$$

Then defined a mapping

$$\gamma_\alpha : \mathcal{M}_\alpha \times A \rightarrow F_p^r$$

$$\gamma_\alpha(\mathcal{M}_\alpha, T_n^{P_0, c, p}) = \begin{cases} T_n^{P_0, c, p}; & n = 1, 2, \dots, \alpha - 1 \\ T_{\mathcal{M}_\alpha(k)}^{P_0, c, p}; & k = \alpha, \alpha + 2, \dots, n \end{cases}$$

Then clearly  $\gamma_\alpha$  is one-one, and generate a  $A'$  by embedding a new sample set of sequences  $\Delta = \{\gamma_\alpha(T_n^{P_0, c, p}) : \forall n \geq \alpha\}$  in the set  $A$ .

**Step.3.** Diffusion: Select a channel  $C$  of the image data  $I_{u \times v}$  with  $1 < l_1, l_2 < n$  such that  $l_1 < l_2$  and  $l_2 - l_1 = u$  Then, there exists a subset given as follows

$$\mathcal{B}_{l_1, l_2} = \{T_n^{P_0, c, p} : n = l_1, l_1 + 1, \dots, l_2\} \subseteq A'$$

As a result, a set given as follows

$$\mathcal{S}^q = \{T_n^{P_0, c, p}(j) : \forall T_n^{P_0, c, p} \in \mathcal{B}_{l_1, l_2} \text{ and } j = q, q + 1, \dots, v, \text{ where } 1 \leq q \leq v\}$$

of multiple streams are generated to diffuse the channel  $C$  using bitwise XOR operation. The diffusion process is described as below

$$\mathcal{D}(\mathcal{S}^q; C) = \text{mod}(C + \text{mod}(\mathcal{S}^q, 256))$$

**Step.4.** Confusion: Before performing confusion process on the data  $\mathcal{D}$ ; each channel of the diffused image data  $\mathcal{D}(i, j) = \{P'(i, j)\}_{i=1, j=1}^{M, N}$  of size  $M \times N$  is divided into blocks with minimum size of  $2 \times 2$ , and then, permuted all with separately chosen elliptic curve  $E_{0, b}^\pi$   $y$  –coordinates. The process is explained in the following.

- (i). Select a set of integers  $\{d^{R'}, d^{G'}, d^{B'}\}$  with each less than  $\frac{M \times N}{2}$ , preferably 2.
- (ii). Convert each channel into blocks  $B'(i, j)$ , according to one of the integers given in Step.4(i).
- (iii). Choose pair of primes  $\pi_1$  and  $\pi_2$  for each channel. Define elliptic curve  $E_{0, b_1}^{\pi_1}$  and  $E_{0, b_2}^{\pi_2}$   $\pi_1, \pi_2 \equiv 2 \pmod{3}$ , and then pick the sets of  $y$  –coordinates of both ECs points.

- (iv). Transform each block location to disturb the partial information using Step 3 in each channel, namely  $D_R, D_G,$  and  $D_B$ . The mathematical representation of the permutation process is given by the following

For  $y_j \in E_{0,b_1}^{\pi_1}, y'_i \in E_{0,b_2}^{\pi_2}$  and  $y_j \leq r_1, y'_i \leq r_2$

$$B_T(y'_i, y_j) = (y'_i, y_j) * B'(i, j)$$

Otherwise

$$B_T(y'_{i+1}, y_{j+1}) = (y'_{i+1}, y_{j+1}) * B'(i, j)$$

Where  $B'(i, j)$  is the  $(i, j)$ th block of diffused image  $\mathcal{D}$ , whereas total number of blocks are  $r_1 \times r_2$ . After block scrambling process in Step.4 (iv), transformed image can be referred as  $\mathcal{D}_T$ . Finally, the transform image data  $\mathcal{D}_T$  is permuted traditionally with S-box generated as sketched in algorithm 1, which is presented as

$$e(S_p^{0,t,\rho}; \mathcal{D}_T) = \text{SubByte}(S_p^{0,t,\rho}; \mathcal{D}_T)$$

Perform all the above steps from (1-4) for each channel  $C$  to complete the encryption process and consequently obtain the ciphered image  $e(I_{u \times v})$ . In our scheme, the original digital image initially experiences diffusion process, and then scramble through traditional substitution via S-box discussed in section 4.3 and finally, obtain the encrypted image.

### 5.3 Performance Analyses of the Proposed Encryption Scheme

A best encryption scheme could be able to ensure security against all kinds of statistical, differential, exhaustive attacks. In this section, some security related experiments are conducted to examine the performance of the proposed technique. The numerical simulations of our algorithms are performed in an environment with Matlab 2019b on personal computer Intel® Core i7-7500U, CPU @ (2.70GHz-2.90GHz) with window 10 and 8GB RAM. the sample digital color images getting from database [19]. We used the sample images “Lena”, “Baboon”, “Pepper”, “Beans” and “House” with size  $256 \times 256 \times 3$ , otherwise specified. In our proposed encryption scheme, the secret keys  $d^R = d^G = d^B = 2, \pi_1^R = \pi_1^G = \pi_1^B = 167, \pi_2^R = \pi_2^G = \pi_2^B = 173, b_1^R = b_1^G = b_1^B = 24(\text{mod}167), b_2^R = b_2^G = b_2^B = 24(\text{mod}173), \rho = 521, t = 91, b = 0, Q = (460,74), p = 4079, a = 7, a' = 0, \alpha = n$

$H = \langle (20,99) \rangle, g = K \cap H^c$ . Figures (14-16), shows the original image data and its corresponding encrypted data.

### 5.3.1 Keyspace Analysis

The strength of crypto-algorithm is directly proportional to its secret large keyspace. A cryptosystem with large keyspace is able to withstand attacks through naïve approach and other cryptanalysis tried to break its security. In this context, our proposed mechanism masks the image data by a set of IPRNS (obtained via ECS-PRNSM), while confusion module is used to substitute each pixel of confussed image data, and thus produce an encrypted image. Therefore, our proposed algorithm not merely possesses the key space related to ECS-PRNSM and MS, it also depends on the parameters needed during their utilization in image encryption. In this connection, our proposed cryptosystem possesses total number of key parameters  $(d_1, d_2, \pi_1, \pi_2, t, a, \rho, P, p, P_0, g, b, p, i, j, \alpha, l_2, q)$  for grayscale image data. So, the minimum requirement to perform image data encryption shown earlier is  $2^{32} \times 2^{30} \times 2^{36} \times 2^{82} = 2^{180}$ . Consequently, the total key space size is  $2^{540}$ . It is noticeable that the key space allowance increases rapidly with tiny increment produced in any of the parameters  $(\pi_1, \pi_2, \rho, p, p)$  and the subgroup  $\langle P_0 \rangle$ . We can deduce that the key size is sufficient to counter common attacks in near future's computer.

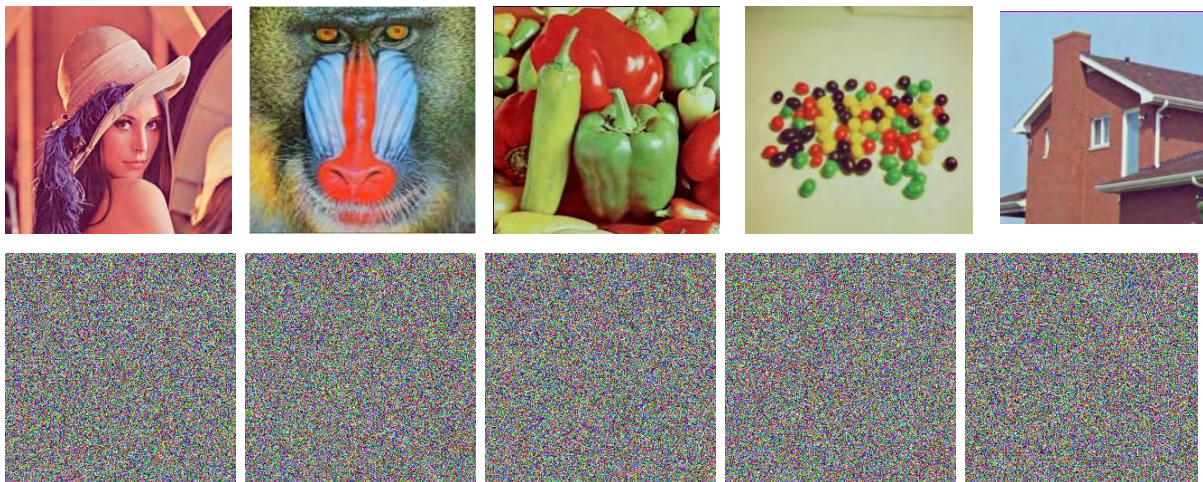


Figure 14. The first row of the dataset consists original digital images of dimensions  $256 \times 256$ , Lena, Baboon, Pepper, Beans and House; second row is the corresponding encrypted images.



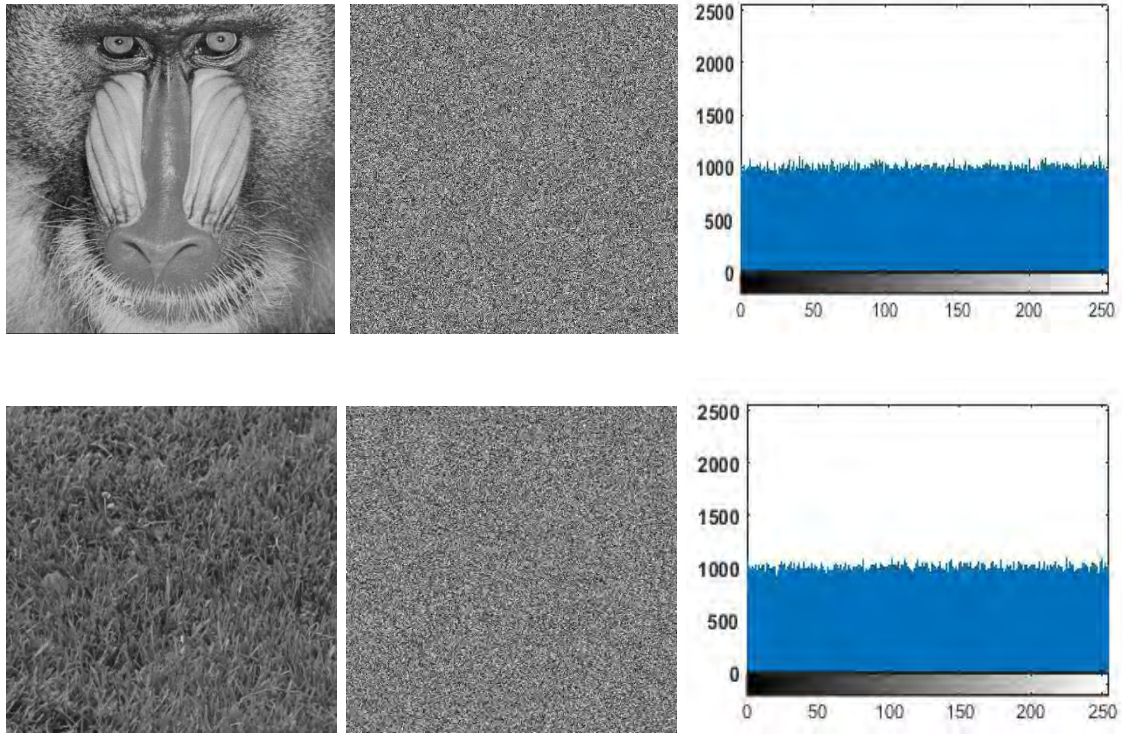


Figure 15. The first column of the dataset consists original grayscale images of dimensions  $512 \times 512$ , Baboon, Grass; second and third columns are the corresponding encrypted images and their histograms respectively

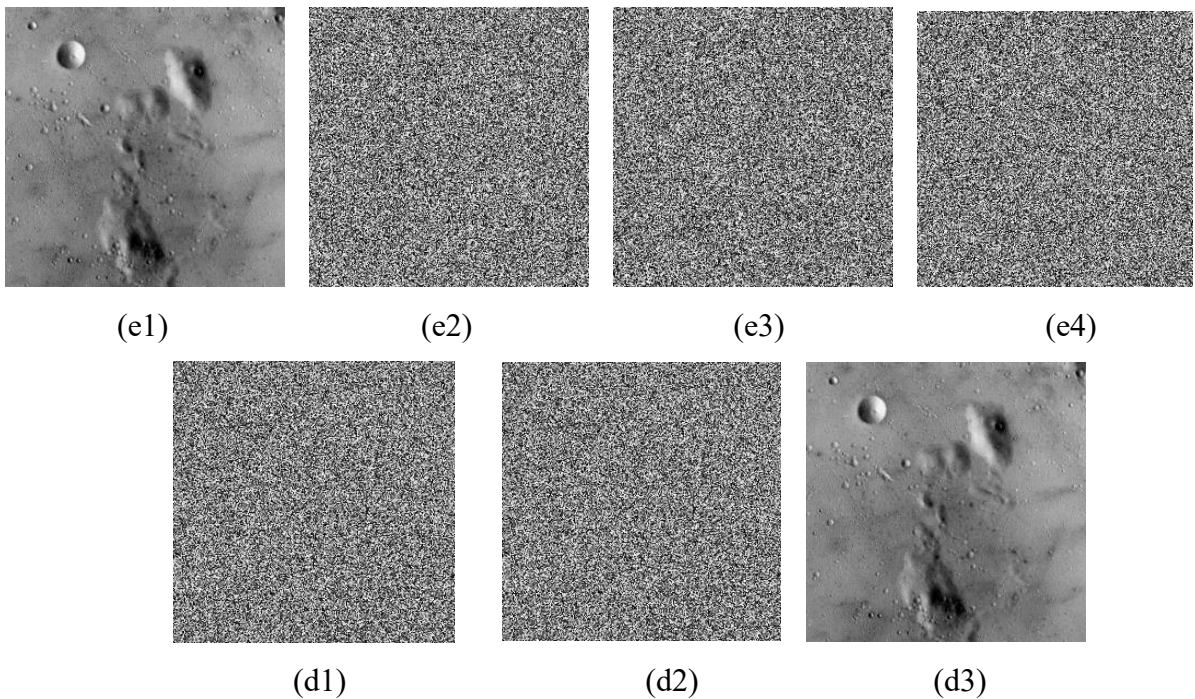


Figure 16. Key sensitivity analysis: (e1) Original image data; (e2) -(e3) Encrypted with one-bit change;(e4) Difference of image data in (e2) and (e3); (d1) -(d2) Decrypted with respect one another keys;(d3) Decrypted with actual key.

### 5.3.2 Key Sensitivity Analysis.

Key sensitivity analysis is one of the key measurements used to examine the strength of encryption system. In this way, we assume two keys  $i_1, i_2$  with only one-bit difference to encrypt the image ‘Moon Surface’. The encryption results are presented in Figure 16, where Figure 16(e2, e3) are encrypted images with keys  $i_1$  and  $i_2$  respectively. Consequently, it is observed from the difference Figure 16(e4) that both keys generated completely different encrypted images in Figure 16(e2, e3). Meanwhile, Figure 16(d1) is obtained by decrypting 16(e3) using key parameter  $i_2$  and 16(d1) is obtained by decrypting 16(e2) using key parameter  $i_1$ , indicating that the actual key parameters plain image data can be recovered. Hence, it is revealed that our proposed cryptosystem is highly sensitive to key parameters thus resistive against all known attacks.

### 5.3.3 Three-Dimensional Histogram

Histogram of an image is tool that provides graphical depiction of frequency distribution. It is almost used to examine the strength of cryptographic algorithm. A uniform histogram of an encryption algorithm can assure the security and prevent an adversary to generate an idea from the variation of encrypted image frequency distribution. Figure 17 shows the histogram distribution of original ‘Lena’, ‘Baboon’, ‘Pepper’, ‘Beans’, ‘House’ and corresponding encrypted images.

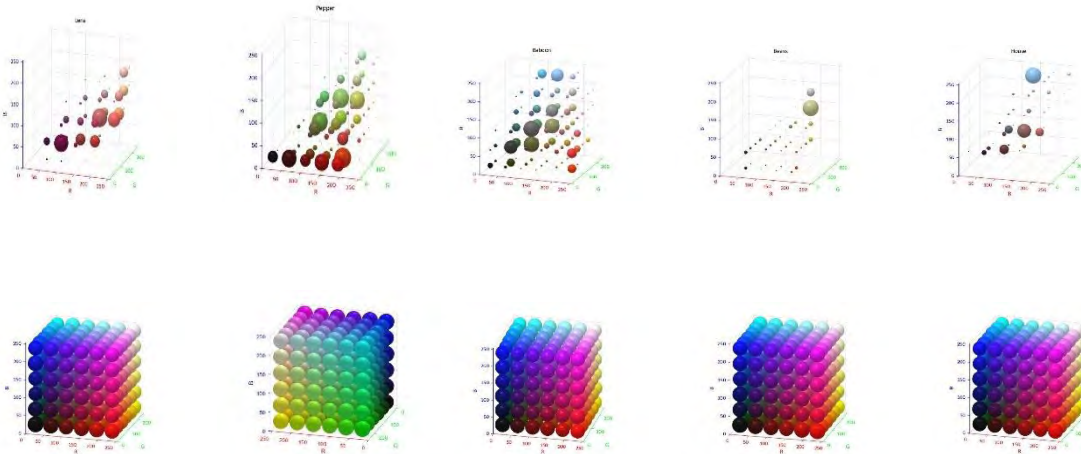


Figure 17. The first row of the dataset consists of the histogram of original digital images, Lena, Baboon, Pepper, Beans and House; second row is the corresponding histogram of the encrypted images.

Clearly, original image histogram distribution is significantly different when compared to encrypted image histogram, and the frequency values are uniformly distributed. Thus, our

proposed encryption system is capable of concealing the authentic information pattern. Accordingly, the proposed is able to successfully resist the statistical attackers.

### 5.3.4 Differential Analysis

Usually, a small change is made in the original image by adversaries and then observe the difference between the encrypted outcomes (that is, encrypted image of the test image and encrypted image of test with a small change). In such a way, the adversary examines the connection between the two encrypted images and test image. In this connection, the adversaries take advantage of differential cryptanalysis in decryption of encrypted image. Thus, it is necessary that our proposed encryption scheme must be robust against differential attacks, which indicates that it should be impossible for adversaries to detect the relation between original image and encrypted image. To measure the strength of encryption scheme against differential attacks, NPCR (number of pixels changing rate) and UACI (unified average changed intensity) are two common metrics used to compute the resistance, which are defined as follows

$$NPCR = \frac{\sum_{\xi_1, \xi_2} C(\xi_1, \xi_2)}{M \times N} \times 100\%$$

$$C(\zeta_1, \zeta_2) = \begin{cases} 1 & \text{if } \mathcal{B}_1(\xi_1, \xi_2) = \mathcal{B}_2(\xi_1, \xi_2) \\ 0 & \text{if } \mathcal{B}_1(\xi_1, \xi_2) \neq \mathcal{B}_2(\xi_1, \xi_2) \end{cases}$$

$$UACI = \frac{1}{M \times N} \sum_{\xi_1, \xi_2} \left[ \frac{|\mathcal{B}_1(\xi_1, \xi_2) - \mathcal{B}_2(\xi_1, \xi_2)|}{255} \right] \times 100\%$$

Where  $\mathcal{B}_1(\xi_1, \xi_2)$  and  $\mathcal{B}_2(\xi_1, \xi_2)$  are two encrypted images and the optimal numerical scores of NPCR and UACI are 99.60% and 33.40%, respectively. Using equations 4 and 5, we computed scores of NPCR and UACI of our proposed scheme given in Table 14. Moreover, the comparative scores with some existing cryptosystems shows that analysis scores are better up to some extent. Hence, our scheme has better resistance against differential attacks and feasible for security purpose.

Table 14. NPCR and UACI numerical values and their comparison

Schemes	Image	NPCR%			UACI%		
		R	G	B	R	G	B
	Lena	99.6429	99.6307	99.6047	33.3147	33.6654	33.6373
Our scheme	Baboon	99.2401	99.6231	99.6093	33.3694	33.3847	33.5375
	Pepper	99.5803	99.6322	99.5941	33.4724	33.5660	33.4971
	Beans	99.6307	99.5986	99.5758	33.5083	33.5451	33.5487
	House	99.6154	99.6078	99.5956	33.3678	33.3789	33.4359
Ref. [91]	Lena	99.612	99.5345	99.5578	33.4572	33.4715	33.4715
Ref. [92]	Lena	99.6158	99.6531	99.6322	33.8730	34.1650	34.4800
Ref. [93]	Lena	99.6300	99.6000	99.6100	33.4200	31.0700	32.1000
Ref. [94]	Lena	99.6155	99.5750	99.6323	32.9071	30.1891	27.3998

### 5.3.5 Information Entropy

There is high correlation of adjacent pixels values in the original image. To create high randomness in entire image data, one should need to mask the data using efficient crypto algorithm. The information entropy helps to calculate the randomness of pixels information in masked image, as the image information ranges between 0 and 255. Thus, for secure encryption scheme, the calculated score of entropy must be closed to amount 8. The calculation formula for information entropy is given below:

$$EA(m) = \sum_{m=0}^{255} [p(m) \times \log_2\left(\frac{1}{p(m)}\right)]$$

Where  $m$  is pixel value and  $p(m)$  is probability. We examined the proposed encryption scheme over entropy analysis, the fallouts are tabulated in Table 15. From the table, it can be seen that the entropy values for red, green and blue channel of the encrypted images are close to 8. Thus, the scheme sufficiently resists the entropy attacks. Besides, the results are compared with the results of existing scheme. The compression shows that the proposed scheme performed better comparatively the existing scheme presented in the literature.

### 5.3.1 Correlation

In any test/original image, correlation factor can be seen in one of the horizontal, diagonal or vertical directions between adjacent pixels. To reduce the correlation, one should make use of standard encryption algorithm and create high degree of disruption in the image. The numerical value of correlation coefficient lies on the real line bounded by  $\pm 1$ . The bounds

(that is,  $\pm 1$ ) of correlation coefficient exhibits strong correlation while nearest value to central point (that is, 0) indicates lowest degree of correlation among the adjacent pixels.

Table 15. Entropy numerical values and their comparison

Schemes	Dimension	Images	Original Image			Ciphred Image		
			R	G	B	R	G	B
	256×256	Lena	7.2763	7.5834	7.0160	7.9975	7.9976	7.9973
Our scheme	--	Baboon	7.6634	7.3871	7.6646	7.9975	7.9977	7.9973
	--	Pepper	7.3920	7.6150	7.1738	7.9972	7.9976	7.9974
	--	Beans	5.8591	6.2585	6.8553	7.9967	7.9971	7.9975
	--	House	6.4005	6.5603	6.4042	7.9970	7.9972	7.9973
	512 × 512	Grass	---	Gray	---	---	7.9994	---
	512 × 512	Baboon	---	Gray	---	---	7.9994	---
Ref. [93]	256 × 256	Lena	7.7317	7.7864	7.6481	7.9892	7.9902	7.9896
Ref. [95]	--	Lena	--	--	--	7.9973	7.9973	7.9971
Ref. [96]	--	Lena	7.2352	7.5683	6.9176	7.9967	7.9964	7.9943
Ref. [31]	--	Lena	7.3277	7.6048	7.1326	7.9971	7.9972	7.9973
Ref. [97]	512 × 512	Grass	---	Gray	---	---	7.9992	---
Ref. [9]	--	Baboon	---	Gray	---	---	7.9993	---

To compute the correlation coefficient of original image and encrypted image, we pick  $K = 10^4$  pairs of pixels values along all three directions from each channel of original color image and encrypted image and calculate correlation coefficient  $C_{uv}$  as follows.

$$C_{uv} = \frac{cov(u, v)}{\sqrt{D_u \circ D_v}}$$

$$cov(u, v) = \frac{1}{K} \sum_{i=1}^K (u_i - E(u))(v_i - E(v))$$

$$V_u = \frac{1}{K} \sum_{i=1}^K (u_i - E(u))^2$$

$$E(u) = \frac{1}{K} \sum_{i=1}^K u_i$$

Where  $u_i$  and  $v_i$  are pixel values of the  $i^{th}$  chosen adjacent pixels values,  $E(u)$  and  $V_u$  are expectation and variance of  $u$ , respectively.

Table 16. Comparison of correlation coefficient results of the proposed scheme with some existing techniques in three layers.

Schemes		Directions	Original Image			Encrypted Image		
			R	G	B	R	G	B
Our scheme	Lena	Horizontal	0.9514	0.9517	0.9157	-0.00072	0.00063	0.00064
		Diagonal	0.9309	0.9337	0.8830	0.00032	0.00035	0.000136
		Vertical	0.9757	0.9762	0.9500	-0.00012	0.00013	0.00026
	Baboon	Horizontal	0.9802	0.9819	0.9625	0.000035	0.000092	0.00012
		Diagonal	0.9344	0.9320	0.9018	0.000024	0.00032	-0.00037
		Vertical	0.9604	0.9619	0.9303	0.000022	0.000043	0.000012
	Pepper	Horizontal	0.9532	0.9743	0.9527	0.000300	-0.00002	0.00004
		Diagonal	0.9225	0.9550	0.9053	0.000020	0.00006	0.00003
		Vertical	0.9510	0.9783	0.9509	0.000400	0.00003	0.00061
	Beans	Horizontal	0.9570	0.9303	0.9608	0.000070	0.00004	0.00002
		Diagonal	0.9299	0.8758	0.9317	0.000050	0.00001	0.00001
		Vertical	0.9600	0.9402	0.9641	-0.00030	0.00008	-0.00012
		Horizontal	0.9682	0.9755	0.9642	0.000034	0.000071	0.000200
	House	Diagonal	0.9377	0.9474	0.9271	0.000051	0.000085	0.000044
		Vertical	0.9651	0.7202	0.9572	0.000032	0.000094	0.000066
	Vertical	0.9780	0.9694	0.9495	-0.0014	-0.0006	-0.24861	
Ref.[30]	Lena	Diagonal	0.9335	0.9179	0.8947	0.00043	-0.00043	-0.2168
		Horizontal	0.9558	0.9400	0.91894	0.0013	-0.00025	0.00696
		Vertical	0.9803	0.9594	0.9294	0.0203	-0.0025	0.0006
Ref.[58]	Lena	Diagonal	0.9668	0.9433	0.9099	-0.0073	-0.0131	0.0111
		Horizontal	0.9813	0.9691	0.9455	0.0092	0.0002	0.0076
		Vertical	0.9865	0.9858	0.9831	0.0025	-0.0017	-0.0043
Ref.[33]	Lena	Diagonal	0.9897	0.9765	0.9684	-0.0066	0.0020	0.0032
		Horizontal	0.9897	0.9871	0.9842	-0.0066	0.0041	-0.0020
		Vertical	0.979540	0.979282	0.966093	0.004776	0.000579	0.000194
Ref.[98]	Lena	Diagonal	0.970675	0.971043	0.949973	0.000232	0.004807	0.00404
		Horizontal	0.990224	0.990848	0.979408	0.001365	0.003294	0.002060
		Vertical	0.990224	0.990848	0.979408	0.000365	0.000294	0.005070

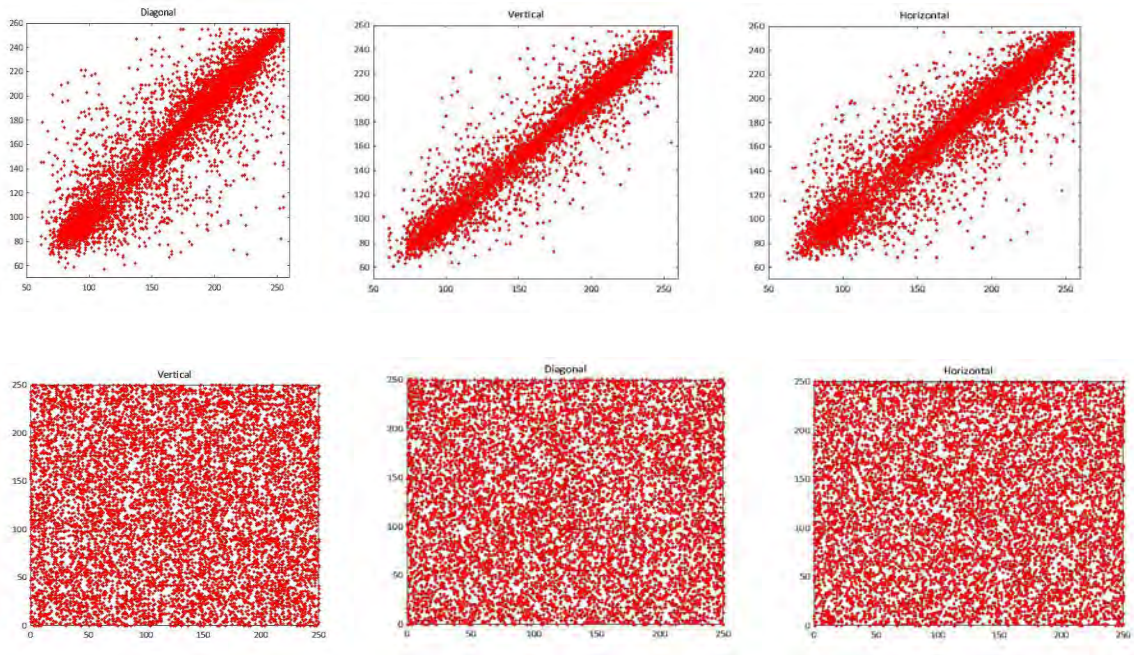


Figure 18. : Correlation distribution in all directions for red channel of Lena image of size  $256 \times 256$ . The first row indicates the red channel of the original digital image, second row represents the encrypted channel

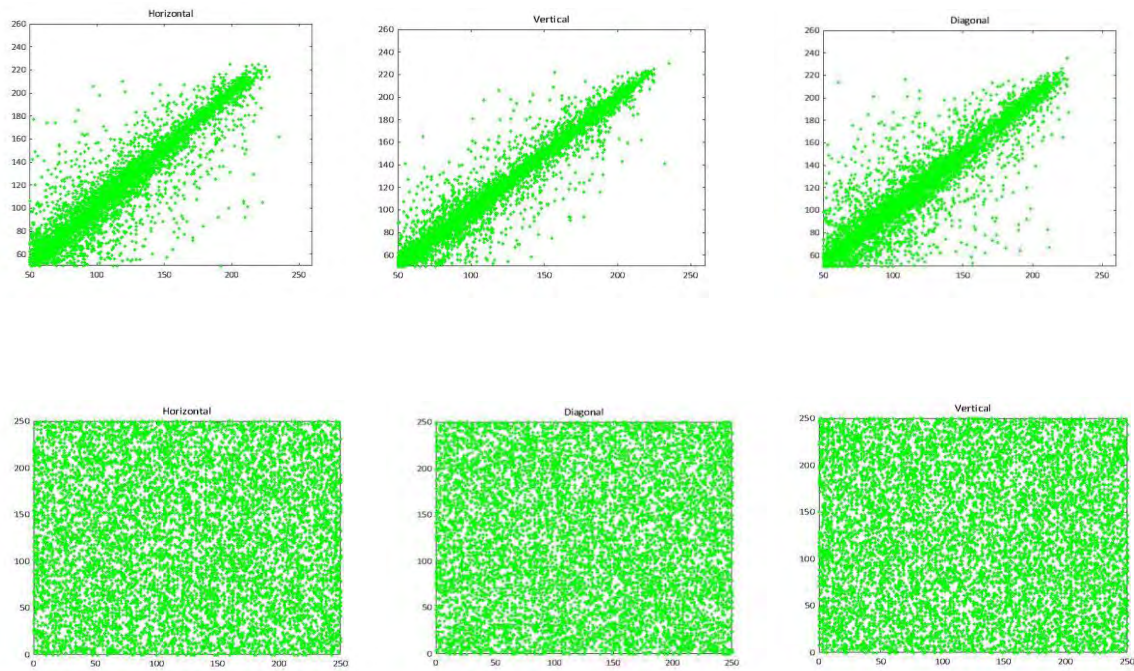


Figure 19. : Correlation distribution in all directions for green channel of Lena image of size  $256 \times 256$ . The first row indicates the green channel of the original digital image, second row represents the encrypted green channel.

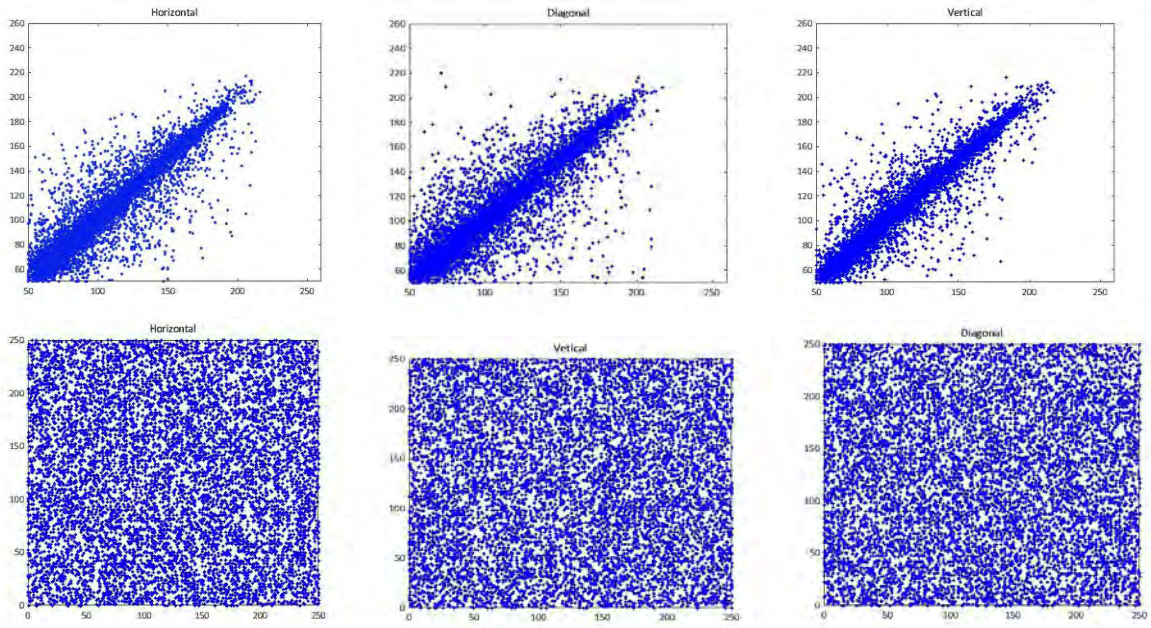


Figure 20. : Correlation distribution in all directions for blue channel of Lena image of size  $256 \times 256$ . The first row indicates the blue channel of the original digital image, second row represents the encrypted blue channel.

In Figures [18-20], first and second row indicate the horizontal, diagonal, and vertical pixels distributions of original and encrypted image channels of Lena  $256 \times 256$ . All figures' values in first row are diagonally distributed and describes the meaningful original image data. But the second row contains figures of encrypted image with data scattered over the whole space, reveals meaningless information for attackers. Furthermore, it is clearly shown from the Table 16, that the numerical values of correlation coefficient of each channel along all three directions occur between  $-0.0001$  and  $0.0001$ . As a result, our proposed encryption can reduce maximum degree of correlation among the adjacent pixels in comparison to schemes given in the literature

In the next chapter, we shall use an indexing technique over elliptic curves to introduce a computationally efficient mechanism for multiple PRNS and S-boxes. Further, we shall evaluate the statistical analysis to show the effectiveness of the proposed S-box, PRNS, and its image encryption application.



## Chapter 6

# Image Encryption by using Novel PRNs and S-boxes

## Modeling Techniques

This chapter deals with efficient pseudo-random numbers and S-boxes are one of the most significant building blocks, which are jointly adopted for image security. Multiple aspects pave the way to handle large-scale multimedia data. However, the computational work on multiple constructions may certainly lead to limits the required ciphering through-put. Therefore, reducing the computational time of both modules is the main requirement for an efficient cryptosystem. For this achievement, we exploited an indexing technique over elliptic curves to introduce a computationally efficient mechanism for multiple PRNS and S-boxes. Statistical results show that the proposed S-box mechanism is the most effective method that generates strong multiple S-boxes on minimum prime fields. Likewise, the PRNS's assessment indicates that the proposed mechanism is the highly productive model for generating multiple verified patterns on small prime fields in a single round. Furthermore, the experimental results show that the proposed algorithm provides desired key-space and less computational effort.

### 6.1 Motivation

In the era of 5G network, the security of sensitive information has gained widespread attention. The digital images, which are the key source of information, can be agreements, photographs, medical reports, contracts, or other types of scanned papers, with the highest rank of sensitivity. The privacy of digital images is of utmost importance while communicated among authorized parties in any system such as the cloud [100]. To deal security and privacy of such multimedia data gave rise to the various efficient encryption algorithms. These algorithms are further based on two different ideas: symmetric and asymmetric key-algorithm. In this connection, the prominent principal techniques used for the symmetric algorithm are the confusion and diffusion modules [78], [101]. The former operating module is normally employed after effective use of diffusion operation to break the relation between ciphered data and keys [78], [85], whereas data of both modules is the rang of pseudo-random number generator (PRNG). Therefore, well-designed PRNG on mathematically based mechanisms performs a principal role in modern image cryptography [101]–[103]. Consequently, various efficient algorithms are developed to generate S-boxes and pseudo-random number sequences [8], [87], [101], [104], [105]. S-boxes can have two

major categories: Static and dynamic S-box. A static S-box depends on fixed operating as well as generating modes while a dynamic S-box has both variable modes of operations. As a result, dynamic S-boxes algorithms are preferred mostly to increase the computational cost for cryptanalysts. Recently, Ibrahim et al. [101] designed an efficient technique for construction of key-dependent dynamic S-boxes using permuted elliptic curves. The author tried to minimize the computational cost for dynamic S-box generation. S.H. Alhandawi et al. [106], proposed an appropriate configuration S-box based on modified firefly algorithm. The authors claimed to have satisfactory cryptographic features. A novel algorithm has been developed with the help of group structure for secure S-box in terms of high nonlinearity [107]. Toughi et al. [6], proposed an image encryption algorithm with core modules PRNG and advanced encryption standard AES. The author in [108], used the chaotic model to design image encryption scheme with enough pseudo creation capability.

Due to multiple advantages such as non-periodicity, high sensitivity to input parameters, ergodicity, key sensitivity, chaotic systems, and ECs are extensively adopted for S-box and pseudo-random number generation in image encryption algorithms [9], [15], [71], [93], [101], [106]. The author in [7], designed a secure algorithm that can be suitable in either digital and optical environments. Wang et al. [109] suggested a cryptosystem based on multi-group techniques such as chaotic map, Fisher-Yates Shuffling, and DNA sequence encoding. The authors of this research study claimed to have high accuracy with fast convergence as an advantage of the encryption algorithm. Considering computational precision, chaotic maps can have the possibility to generate a random sequence within a short period. As a result, elliptic curve structure is quite better than chaotic maps to adopt for the generation of random sequences [10]. Reyad et al. [89], developed an idea based on ECs to get pseudo-random numbers that work efficiently in image cryptography. El-Latif et al. [90], utilized both cyclic ECs and hybrid-chaotic systems for developing an efficient image encryption scheme. Likewise, Haider et al. [78], made an effort to utilize ECs with the dynamic approach for the generation of random numbers and S-box.

In [6], [101], the authors generated PRNs with ECs group law operating tool (GL-OT) using a large prime field. Similarly, the schemes [78], [90], used recursive approach (RA) and (GL-OT) to find all points on ECs. Moreover, both techniques are further employed to generate S-box and PRNs. In other words, pure algebraic arithmetic operations are managed to facilitate these schemes. However, on the one hand, the RA and GL-OT over a large prime field can be very expensive computationally for output data such as S-box and PRNs modules, as it requires a sequence of arithmetic operations-but, on the other hand, a small fixed prime field

may fail to generate a large number of required data with efficient cryptographic features. Even though a scheme [78], considered these hurdles on a priority basis to reduce the computational efforts, it could hardly produce at most two strong dynamic S-boxes using a minimum fixed odd prime field.

Considering the aforementioned problems including large-spaced data encryption, we propose a novel cryptosystem based on ECs over small odd prime fields with indexing technique (IT) to counter existing limitations. In this cryptosystem, two independent mechanisms namely S-box and a set of pseudo-random numbers of streams are designed with totally different approaches using IT. It is worth mentioning that the S-box construction mechanism (SCM) generates multiple dynamic S-boxes in  $16 \times 16$  standard look up table using the fixed minimum odd prime field. Meanwhile, the PRN generation mechanism (PRNGM) also provides verified non-repeated random patterns; thus, confirming its efficiency regarding diffusion purpose for large-scale multimedia data. Furthermore, the outcome results from our applications of both modules also affirm the choice of SCM and PRNGM by using IT in various cryptographic applications.

## 6.2 Basic Concept

In this section, we recall some basic definition and results related to the main work our this chapter. For any given prime field  $F_p$  and  $a, b \in F_p$ , such that  $27b^2 + 4a^3 \not\equiv 0 \pmod{p}$ , an elliptic curve (EC)  $E(a, b, p)$  defined over  $F_p$  as a collection of all points  $P(x, y) \in F_p \times F_p$ , such that

$$y^2 \equiv (x^3 + ax + b) \pmod{p}$$

Each point on EC is symmetric about  $x$ -coordinate. In other words, any point  $P(x, y)$  on  $E(a, b, p)$  has corresponding point  $-P(x, y) = P(x, -y)$  on  $E(a, b, p)$ , termed as inverse of  $P(x, y)$ . Similarly, a special point  $\mathcal{O}$ , called “the point at infinity” which plays as the identity point to satisfy an abelian group criterion. For  $P_1$  and  $P_2$  on  $E(a, b, p)$ , the sum of  $P_1$  and  $P_2$  is defined as:

$$P_1 \oplus P_2 = \begin{cases} P_1 & \text{if } P_2 = \mathcal{O} \\ P_2 & \text{if } P_1 = \mathcal{O} \\ \mathcal{O} & \text{if } P_1 = -P_2 \\ P_s(x_s, y_s) & \text{if } P_1 = P_2 \\ P_d(x_d, y_d) & \text{if } P_1 \neq P_2 \end{cases}$$

where

$$(x_s, y_s) = (s^2 - 2x_1 \pmod{p}, d(x_1 - x) - y_1 \pmod{p})$$

$$(x_d, y_d) = (d^2 - x_1 - x_2 \pmod{p}, d(x_1 - x_3) - y_1 \pmod{p})$$

And

$$s = \frac{3x_1^2 + a}{2y_1} \pmod{p}, d = \frac{y_2 - y_1}{x_2 - x_1} \pmod{p}$$

**Theorem 6.1:** Let  $E(a, b, p)$  be an elliptic curve over the finite field  $F_p$ . Then the order of  $E(a, b, p) (F_p)$  satisfies

$$|p + 1 - \#E(a, b, p) (F_p)| \leq 2\sqrt{p}.$$

**Lemma 6.1.** [[1], page 4.33] An elliptic curve  $E(a, b, p)$  over a prime field  $F_p$  with  $p - 2 \equiv 0 \pmod{3}$  has exactly  $p + 1$  distinct points, where each integer in the field  $F_p$  appear once as  $y$ -coordinates.

**Theorem 6.2.** [[3], Example 9.5.2] Let  $p > 2$  be any prime integer and  $E(a, b, p) : y^2 = x^3 + ax + b$  is an elliptic curve over  $F_p$ . Then  $E(a, b, p)$  is not isomorphic to  $E(a', b', p)$  with  $a' = t^2a$  and  $b' = t^3b$ ; for any  $t \in F_p^*$  if and only if  $t$  is non-square in  $F_p^*$ .

### 6.3 Proposed Methodology for S-boxes and Pseudorandom Numbers Streams

In this section, we propose a crypto algorithm based mainly on two independent generation schemes for random data of a certain length. The detailed steps of each scheme are explained in the following sub-sections.

#### 6.3.1 SCM

Generating strong dynamic S-boxes is the most promising criterion for achieving efficient cryptosystems, and it plays a key role in nonlinear transformations, which are used for assessing well-designed crypto-algorithms [79]. For this reason, the generating dynamic S-boxes with the best cryptographic features are considered much more suitable in the modern cryptographic environment. To get multiple S-boxes, in this section, we propose a fast technique with the partial agreement of ECs group law to overcome the shortcomings of existing S-box constructions. The following description shows the proposed S-box mechanism.

1. For  $p$ , define ECs  $E_1(a_1, b_1, p)$  and  $E(0, a_2, p)$  over prime field  $F_p$ , with IT to generate all points.
2. Select a point  $Q \in E_2(0, a_2, p)$  at random approach and generates a sub-group  $\mathcal{M} = \langle Q \rangle$  using EC group law, i.e. Eq: (1).
3. Choose  $y$  – *coordinates* of both generated ECs and  $\mathcal{M}$  with ascending order of  $x$  – *coordinates*.
4. Choose  $t_s, t_n \in F_p$ , where  $t_i$  are squared and  $t_n$  are square-free. Likewise, we pick two points  $P_1, P_2 \in E(a_1, b_1, p)$  with  $y$  – coordinate of  $P_1$  is squared and  $P_2$  is square-free.

Table 17. Sample S-boxes

$< 97,73 >_{169,5}^{0,234,123}$																			$< 13,214 >_{121,45}^{0,234,166}$																		
52	14	216	154	240	4	25	209	206	58	254	248	230	205	156	193	44	160	212	183	142	193	31	218	83	97	56	255	38	98	224	169						
22	32	130	69	181	225	54	84	197	80	16	98	144	6	110	31	180	194	106	200	108	72	78	66	223	3	101	115	213	11	109	164						
179	236	150	255	37	122	47	180	172	211	50	3	251	188	48	93	155	242	15	231	131	226	153	179	18	138	249	94	150	203	102	113						
35	157	215	103	189	137	28	97	135	152	101	213	138	20	145	53	22	176	159	209	58	90	29	205	240	127	30	116	174	51	210	103						
147	91	160	220	198	141	63	186	119	49	104	120	153	95	187	148	89	91	4	35	134	197	67	81	157	6	172	7	37	148	79	125						
203	228	217	115	221	62	178	46	219	111	64	164	12	191	19	168	166	46	247	53	123	124	110	77	33	217	244	17	243	208	184	121						
15	9	163	100	136	89	192	176	107	68	55	129	1	244	67	44	10	188	162	88	133	202	21	186	154	65	146	206	112	69	2	175						
85	227	56	200	82	70	222	131	128	21	10	132	161	105	166	76	141	16	86	191	245	96	128	48	40	19	144	182	140	196	61	12						
133	26	212	108	243	42	109	142	126	17	113	235	162	202	134	245	28	68	45	241	119	254	85	42	47	36	20	50	132	120	84	156						
194	7	51	86	252	207	88	78	224	151	232	87	106	208	196	231	63	198	54	232	170	253	93	151	24	236	43	229	143	105	130	248						
184	36	242	57	182	250	116	72	77	34	24	71	247	83	38	39	230	39	168	1	149	199	73	26	192	251	76	74	111	80	62	187						
94	92	40	174	201	146	102	226	165	223	29	185	229	45	246	237	122	104	178	220	34	27	0	239	49	204	214	41	238	118	219	171						
79	33	99	13	241	199	41	125	190	234	249	27	23	238	11	60	246	161	52	59	185	233	114	158	75	23	181	14	137	117	9	237						
2	73	158	112	175	139	149	5	75	74	214	143	159	124	140	170	32	135	227	173	163	152	201	107	57	8	95	126	71	216	100	92						
43	90	239	66	123	167	96	171	233	173	169	218	65	183	155	30	189	87	147	222	5	99	221	13	252	225	82	215	136	60	55	165						
8	114	127	118	121	253	210	195	177	81	117	61	0	59	204	18	235	228	64	211	145	195	250	25	167	70	234	177	129	190	207	139						
$< 52,92 >_{4,19}^{0,211,235}$																			$< 172,109 >_{196,167}^{0,211,235}$																		
197	5	207	116	2	63	209	25	173	169	147	23	21	132	118	176	116	228	174	236	114	81	110	188	28	17	203	7	207	35	242	111						
228	227	66	109	128	187	18	123	158	154	79	175	237	3	58	243	92	176	152	230	235	197	149	40	196	249	195	161	112	27	65	155						
11	15	246	166	219	205	104	42	225	131	71	73	41	120	133	177	9	18	105	93	123	186	72	95	154	167	20	247	241	48	229	91						
61	161	253	121	251	72	83	122	157	188	153	135	98	90	60	171	137	77	248	86	141	23	39	224	26	187	38	127	117	217	171	98						
130	204	126	255	233	192	216	46	10	32	234	9	33	223	222	26	80	46	73	14	126	22	121	101	13	96	254	200	138	66	42	240						
142	47	213	8	24	241	201	36	137	95	31	20	236	254	89	160	118	139	190	76	253	31	246	156	169	113	49	54	146	153	132	158						
113	4	191	74	163	44	145	165	12	140	56	252	59	34	242	240	175	11	238	170	78	199	69	104	164	45	70	245	212	25	166	82						
146	49	38	155	156	172	75	244	170	54	84	212	27	230	232	221	63	5	6	234	206	57	134	201	59	168	52	220	226	103	21	124						
111	164	134	200	136	229	141	91	124	152	206	78	203	183	110	29	221	62	239	204	1	47	15	145	68	100	181	8	32	0	136	184						
245	210	238	231	167	28	211	69	86	217	239	43	162	40	143	107	87	4	210	177	97	243	2	172	227	208	94	251	182	205	215	64						
193	102	196	64	195	115	250	214	88	138	48	190	68	82	117	114	99	214	51	120	178	133	115	159	30	56	24	119	211	216	173	193						
148	93	125	77	224	184	180	55	194	149	103	62	159	151	127	70	165	180	34	55	37	19	147	67	202	33	122	183	148	225	162	255						
87	218	50	97	57	220	112	186	247	174	96	94	85	208	198	22	125	233	128	109	232	237	218	41	58	219	16	151	83	213	43	223						
144	179	182	106	215	99	80	101	108	1	45	235	168	150	76	92	60	84	79	102	129	108	90	250	192	144	198	36	12	53	44	163						
6	202	119	14	249	105	19	51	53	7	226	65	139	178	189	35	106	185	142	160	3	135	74	71	194	140	191	107	130	88	222	89						
30	39	185	0	199	67	17	181	16	81	248	13	129	100	52	37	252	85	29	50	131	143	75	231	150	209	10	179	189	157	244	61						

1. Perform arithmetic operation to generate two disjoint sets [78], which are defined as

$$A_{P_1} = \left\{ t_n^3 y_1 : n = 1, 2, 3, \dots, \frac{p-1}{2} \text{ and } y_1 \in P_1 \right\}$$

$$B_{P_2} = \left\{ t_s^3 y_2 : s = 1, 2, 3, \dots, \frac{p-1}{2} \text{ and } y_2 \in P_2 \right\}$$

2. Define multiple maps

$$\varphi_1 : (A_{P_1}, B_{P_2}) \rightarrow (\mathcal{M}, \mathcal{M})$$

$$\varphi_1(s_1, s_2) = (m_{s_1}, m_{s_2})$$

$$\varphi_2 : im(\varphi_1) \rightarrow (\mathcal{M}, \mathcal{M})$$

$$\varphi_2(\varphi_1(s_1, s_2)) = (\varphi_1(s_2)_{m'}, \varphi_1(s_1)_{m'}) \rightarrow (2)$$

The set  $(\mathcal{M}, \mathcal{M}) = \{(v_i, u_j) : \forall v_i, u_j \in \mathcal{M} \text{ such that } i = j\}$  and similarly, the set  $(A_{P_1}, B_{P_2})$ . Inspired by an isomorphic and non-isomorphic ECs approach in [78], the sets  $A_{P_1}$  and  $B_{P_2}$  clearly contained all those points which represent the  $y$ -coordinates of isomorphic and non-isomorphic ECs respectively. Similarly, in step 2, the partial engagement of EC group law in the proposed scheme is the appearance of both coordinates randomly one after another. However, these ideas are further jointly operated to accomplish the required

task, as shown in Step 6. As far as Step 6 is concerned, the mappings  $\varphi_1$  and  $\varphi_2$  are bijective, so is  $\varphi = \varphi_1 \circ \varphi_2$ . Finally, first dissimilar integral points between 0 and 256 are collated from the set  $im(\varphi_2)$  to form the required S-box  $\mathcal{M}_{y_1, y_2}^{a_1, b_1, b_2}$ , i.e, Eq. (2). It is noted that the proposed S-box construction mechanism generates large number of efficient S-boxes using fixed minimum odd prime field and sub-group  $\mathcal{M}$ . For instance,  $p = 257$ , the scheme is capable to generate more than 200 S-boxes with a minimum non-linearity score of 106 of each which are given in Table 17.

Table 18. Graphical representation of indexing technique (IT)

Column 1		Column 2	
$x^3 + x + 1 \text{ mod } 17$		$y^2 \text{ mod } 17$	
1.	3	1.	<b>1</b>
2.	11	2.	4
3.	14	3.	9
<b>4.</b>	<b>1</b>	4.	16
5.	12	5.	8
6.	2	6.	2
7.	11	7.	15
8.	11	8.	13
9.	8	9.	13
10.	8	10.	15
11.	0	11.	2
12.	7	12.	8
<b>13.</b>	<b>1</b>	13.	16
14.	5	14.	9
15.	8	15.	4
16.	16	16.	<b>1</b>
<b>17.</b>	<b>1</b>	17.	0

Table 19. Security analysis of the proposed S-boxes

Scheme	S – box	Min	Avg	Max	BIC	SAC	DP	LP
Our	$\langle 92,244 \rangle_{64,3}^{0,189,235}$	106	107.50	110	0.5069	0.4873	0.0390	0.1328
	$\langle 222,122 \rangle_{118,210}^{0,191,235}$	106	107.50	110	0.5017	0.4992	0.0468	0.1328
	$\langle 202,234 \rangle_{218,19}^{0,21,235}$	106	107.50	110	0.4996	0.4951	0.0468	0.1250
	$\langle 207,28 \rangle_{100,154}^{0,21,235}$	106	107.50	108	0.4990	0.5048	0.0390	0.1250
	$\langle 97,73 \rangle_{169,5}^{0,234,123}$	106	107.75	108	0.5051	0.5026	0.0468	0.1406
Ref.[110], 2020		106	106.50	108	0.50049	0.5009	0.0391	0.1328
Ref.[111], 2021		102	105.25	108	0.50872	0.5351	---	0.140625
Ref.[112], 2021		104	106.75	108	---	0.4976	0.03906	---
Ref.[101], 2021		106	107.75	110	---	---	---	---

### 6.3.2 PRNGM

In various cryptographic applications, especially data encryption and gambling, verified pseudo-random numbers play a significant role. In this context, pseudo-random numbers on

different mathematical structures including ECs are developed for a strong masking purpose in data encryption [6], [49], [113], [114]. Mostly, a single PRN pattern is formalized in a single round to get the possible diffusion creation requirement [6], [115]. However, it causes key space deficiency which is the utmost requisition for data protection against brute-force attacks, whereas accessing multi-PRN patterns in a single round on the group arithmetic operations specially ECs GL-OT is much time-consuming. Therefore, reducing time consumption as well as generating multi-PRN patterns using ECs, an indexing technique (IT) is proposed in this section. The following lines define the proposed algorithm.

1. Choose  $c, \hat{p}$  with  $\hat{p} \equiv 2 \pmod{3}, c \in F_{\hat{p}}$  and defines an EC  $E(0, c, \hat{p})$  over the prime field  $F_{\hat{p}}$  to generate exactly  $\hat{p} + 1$  non-repeated  $y -$  coordinates Lemma 6.1.
2. Form the sets

$$A_E = \left\{ (t_n^3 y_i)_{n=1}^{\frac{\hat{p}-1}{2}} : \forall y_i \in E^y ; t_n \text{ is non-square} \right\}$$

$$B_E = \left\{ (t_s^3 y_i)_{s=1}^{\frac{\hat{p}-1}{2}} : \forall y_i \in E^y ; t_s \in (F_{\hat{p}} \setminus \{0\})^2 \right\}$$

Where each sequence  $(t_n^3 y_i)_{n=1}^{\frac{\hat{p}-1}{2}}, (t_s^3 y_i)_{s=1}^{\frac{\hat{p}-1}{2}}$  consists of either squared or square-free points of the field  $F_{\hat{p}}$ . Similarly, one can generate a whole field  $F_{\hat{p}}$  for each  $y \in E^y$ .

3. Define a set

$$T = \left\{ (N_i; S_i) = ((y_{nj}); (z_{nj})): N_i \in A_E, S_i \in B_E \text{ and } (y_{nj}) \in (e_{t_j}^y), (z_{nj}) \in (e_{k_j}^y) \right\} \cup \{F_{\hat{p}} \setminus \{0\}\}$$

Now for any  $d_1, d_2, d_3, d_4 \in F_{\hat{p}}$  with  $d_1 < d_2, d_3 < d_4$  and  $\left| d_4 - \frac{\hat{p}-1}{2} \right| = \left| \frac{\hat{p}-1}{2} - d_3 \right|$ . Take  $(N_i; S_i) = W \in T$ . One can choose non-isomorphic and isomorphic ECs  $(e_j^y)_{j=d_3}^{d_4-d_3/2}, (e_k^y)_{k=d_4-d_3/2}^{d_4}$

We define a map

$$\theta_T: W \rightarrow (F_{\hat{p}} \setminus \{0\})^{\hat{p}-1}$$

$$\theta_T(W) = T^W = ((N_i; S_i)_{i=1}^{\hat{p}-1})^W = \left( ((y_j); (z_j))_{n=1, j=1}^{\hat{p}-1, \frac{\hat{p}-1}{2}} \right)^W = \left( ((s_j)_n)_{n=1, j=1}^{\hat{p}-1, \frac{\hat{p}-1}{2}} \right)^W = ((w_{(s_j)_n})_{n=1, j=1}^{\hat{p}-1, \frac{\hat{p}-1}{2}}) \pmod{256}.$$

**Case 1:** If  $d_3 < d_4$ . and a set

$$Y^W = \left\{ (w_{(s_j)_n})_{n=d_1, j=d_3}^{d_2, d_4} = \left( ((y_j); (s_k))_n \right)_{n=d_1, j=d_3, k=d_4-d_3/2}^{d_2, d_4-d_3/2, d_4} : \forall w \in W, y_{nj} \in e_j^y, z_{nk} \in e_k^y \right\} \subset \theta_T(W)$$

**Case 2:** If  $d_1 < d_2$ , we have

$$Y^W = \left\{ \left( w_{(s_j)_n} \right)_{n=d_1}^{d_2} = \left( (s_j)_n \right)_{n=d_1}^{d_2} : \forall w \in W; n = d_1, d_1 + 1, \dots, d_2 \right\} \subset \theta_T(W)$$

4. Select the consecutive  $L$  sequences of  $(\hat{p} - 1) - \text{length}$  to form a sequence of minimum  $10^6 - \text{length}$ .

**Proposition 6.1:** The mapping  $\theta_T$  does not generate a single similar pattern. So,  $\theta_T$  is one-one.

**Proof:**

**Case 1.** Suppose there exists  $h_1, h_2 \in (F_{\hat{p}} \setminus \{0\})^{\hat{p}-1}$  with  $h_1 \neq h_2$  such that  $s_{mh_1} = s_{mh_2}$ , for some  $d_1 \leq m \leq d_2 \Leftrightarrow v_{s_{h_1}} = y_{mj}$  and  $v_{s_{h_2}} = y_{mj}$ , for some  $v_{s_{h_1}}, v_{s_{h_2}} \in N_i$  or  $v_{s_{h_1}}, v_{s_{h_2}} \in S_i \Leftrightarrow v_{s_{h_1}} = v_{s_{h_2}}$ , for some  $v_{s_{h_1}}, v_{s_{h_2}} \in N_i$  or  $v_{s_{h_1}}, v_{s_{h_2}} \in S_i$ . Which is contradiction to the fact that both  $N_i, S_i$  have non-repeated elements by Lemma 6.1. If  $v_{s_{h_1}} = v_{s_{h_2}}$ , for some  $v_{s_{h_1}} \in N_i$  and  $v_{s_{h_2}} \in S_i$ . Again, contradiction that  $N_i \cap S_i = \emptyset$ . Similar arguments can be proved, for  $(t_{mg})$ .

**Case 2.** Similarly, for  $m_1 \neq m_2$  and fixed  $d \in (F_{\hat{p}} \setminus \{0\})^{\hat{p}-1}$ . Consider  $s_{m_1d} = s_{m_2d} \Leftrightarrow v_{s_d} = y_{m_1j}$  and  $v_{s_d} = y_{m_2j}$ , for some  $v_{s_d}, v_{s_d} \in N_i$  or  $v_{s_d}, v_{s_d} \in S_i \Leftrightarrow y_{m_1j} = y_{m_2j}$ , but  $y_{m_1j}, y_{m_2j} \in e_j^y$ . Contradiction to the fact in Theorem 6.2, which shows that  $\theta_T$  does not generate a single similar pattern. Hence,  $\theta_T$  is one-one.

The slight increment in the parameters  $d_1, d_2, d_3, d_4$  not merely provide sufficient randomness potency in each generated pattern, but also produce a large impact on the size of output data. This can be illustrated more accurately by seeking the relation between a single quantity in the sequence  $(y_{mj})$  and corresponding output sequence  $(v_{s_{md}})$ . Likewise, the

Table 20. Simulation results of PRNM by the NIST testing suit.

Test Name	Proportion	Pass/Fail
1. Frequency Test (Monobit)	100/100	Pass
2. Frequency Test within a Block	100/100	Pass
3. Run Test	97/100	Pass
4. Longest Run of Ones in a Block	98/100	Pass
5. Binary Matrix Rank Test	100/100	Pass
6. Discrete Fourier Transform (Spectral) Test	100/100	Pass
7. Non-Overlapping Template Matching Test	100/100	Pass
8. Overlapping Template Matching Test	100/100	Pass
9. Maurer's Universal Statistical test	100/100	Pass
10. Linear Complexity Test	100/100	Pass
11. Serial test:	100/100	Pass



12. Approximate Entropy Test	100/100	Pass
13. Cumulative Sums (Forward) Test	100/100	Pass
14. Cumulative Sums (Reverse) Test	100/100	Pass
15. Random Excursions Test:		
State		
-4	100/100	Pass
-3	100/100	Pass
-2	100/100	Pass
-1	100/100	Pass
+1	100/100	Pass
+2	100/100	Pass
+3	100/100	Pass
+4	100/100	Pass
16. Random Excursions Variant Test:		
State		
-9.0	100/100	Pass
-8.0	100/100	Pass
-7.0	100/100	Pass
-6.0	100/100	Pass
-5.0	100/100	Pass
-4.0	100/100	Pass
-3.0	100/100	Pass
-2.0	100/100	Pass
-1.0	100/100	Pass
+1.0	100/100	Pass
+2.0	100/100	Pass
+3.0	100/100	Pass
+4.0	100/100	Pass
+5.0	100/100	Pass
+6.0	100/100	Pass
+7.0	100/100	Pass
+8.0	100/100	Pass
+9.0	100/100	Pass

whole process is managed via IT rather than a single arithmetic operation; thus, firmly reduce the time complexity of the proposed algorithm.

Table 21. Time comparison of proposed technique with existing techniques w.r.to point generation.

$p$	Maximum/Minimum time(sec.) to generate $E(0,1,p) = t_{max}/t_{min}$				Maximum/Minimum time(sec.) to generate $E(1,1,p) = t_{max}/t_{min}$			
	Base Point	GL-OT	RA	IT	Base Point	GL-OT	RA	IT
1019	(27,187)	$t_{min} > 0.04$	$t_{min} > 0.4$	$t_{max} < 0.0151$	(1,375)	$t_{min} > 0.04$	$t_{min} > 0.4$	$t_{max} < 0.0153$
9929	(10,631)	$t_{min} > 1.9$	$t_{min} > 32$	$t_{max} < 0.6$	(3,4484)	$t_{min} > 1.9$	$t_{min} > 32$	$t_{max} < 0.5.6$
49991	(6,24197)	$t_{min} > 47$	$t_{min} > 880$	$t_{max} < 9.4$	(1,11512)	$t_{min} > 48$	$t_{min} > 882$	$t_{max} < 9.4$
65579	(17,26502)	$t_{min} > 94$	$t_{min} > 1380$	$t_{max} < 15$	(1,59417)	$t_{min} > 92$	$t_{min} > 1570$	$t_{max} < 15.2$
101117	(11,18479)	$t_{min} > 207.3$	$t_{min} > 4000$	$t_{max} < 35.7$	(10,24163)	$t_{min} > 207$	$t_{min} > 4000$	$t_{max} < 35.6$
526067	(85,34831)	$t_{min} > 5843$	$t_{min} > 24,000$	$t_{max} < 838$	(1,317782)	$t_{min} > 5994$	$t_{min} > 24,000$	$t_{max} < 839$

## 6.4 Performance Analysis of SCM and PRNGM

### 6.4.1 SCM Analysis

S-box that is used in the substitution module of the cryptosystem, is one of the most important components of the block cipher. It is the only nonlinear component in most of the encryption schemes that catered to the function of diffusion and confusion. Therefore, the security of such algorithms relies on the security strength of the S-box. To examine the strength of the S-box the general criteria are selected, which are nonlinearity (NL), bit independent criteria (BIC), linear approximation probability (LAP), strict avalanche criteria (SAC), and differential approximation probability (DAP). The NL test evaluates the minimum distance among the set of all affine Boolean functions and the output S-box Boolean functions. The SAC test examines the sensitivity of the S-box against a small variance in the input data. Similarly, the LAP and DAP tests measure the resistance of the S-boxes against linear and differential attacks respectively. We analyzed the generated S-box over these criteria to prove the efficiency of the proposed S-boxes. The resultant values are listed in Table 18. From Table 18, our S-boxes' non linearity scores are comparable with that of the schemes due to Ibrahim et al. [101]. Though, in this scheme, the S-boxes construction mechanism is developed using large field. On the other hand, the proposed scheme has almost better nonlinearity scores in all respect as compared to that of the schemes in [110]–[112]. Therefore, our S-box construction mechanism (SCM) is computationally suitable to generate multiple efficient S-boxes for large-scale image data.

### 6.4.2 PRNGM Analysis

The strength of pseudo-random numbers can be claimed based on some common statistical tools like NIST, Diehard, and TESTU01. A sequence is described as secure and strong in terms of cryptography. In this research study, the NIST testing tool is used to identify the randomness of EC-based sequences. For this purpose, we tested 100 different sequences that are generated in a single round. The rate of passing sequences in each test is almost 1, which is perhaps an astonishing passing rate as compared to that of the scheme in [8], [116]. Moreover, as far as the number of sequences is concerned, it can be smoothly increased up to 3000 by using a prime field consisting of 15 –bits entries. These facts prove that the proposed PRNGM is more suitable for large-scale multi-media data security.

### 6.4.3 National Institute of Standard and Technology (NIST)

NIST testing suite consists of 15 tests that are normally performed to identify the randomness of sequences. Generally, various techniques including cryptographic algorithms can be

adapted to generate these sequences. The NIST testing suit was published in 2001, as a result of joint teamwork between the NIST statistics department [117], and the computer security department. The simulation results of the testing tool on EC-based PRN are listed in Table 20.

## 6.5 Proposed Scheme in Image Encryption

Images are the visual content that required more attention during transmission, especially in military, commercial, medical fields. To consider its security and reliability, numerous mathematical structures are adopted to formalize image encryption schemes. Traditionally, chaotic and EC systems are utilized for designing pseudo-random numbers and S-box generation modules. Cryptosystems with only a substitution module S-box are not suitable for security enhancement of image data [118] as its visual content's nature is different in comparison to that of text data. For this purpose, a hybrid cryptosystem is a key requirement for image data transmission over public channels in recent decades. Generally, the hybrid cryptosystem is mostly based on S-box and PRN modules and found effective [78]. In this section, the aim is to demonstrate and validate the performance of the proposed SCM and PRNGM modules application in image encryption. Perhaps, a two-phase mechanism in a single round is employed on the image data to construct its ciphered version. The following steps are the complete description of the proposed encryption process

1. Expressed each pixel value of the plain/original image  $I_{M \times N}$  in binary form which is denoted by  $B_{M \times N}$ .
2. Initially, choose a sequence  $\left(w_{(s_j)_n}\right)_{n=d_1}^{d_2} = \left((s_j)_n\right)_{n=d_1}^{d_2}$ ;  $\forall w \in W$ , and  $Y^W \subseteq T$  (By Case 2, in section 6.3.2).

$$D_{M \times N} = \text{bitxor} \left( \left( w_{(s_j)_n} \right)_{n=d_1}^{d_2}, B_{M \times N} \right) \text{mod} 256 ;$$

The above equation shows the *bitwise xor* operation between image data and sequence terms with the  $i^{\text{th}}$  – term onward of the sequence  $\left(w_{(s_j)_n}\right)_{n=d_1}^{d_2}$ .

3. Apply Bitwise with recursive operation from bottom to top (from last entry to 1st one) of image data  $D_{M \times N}$  and get  $N'_{M \times N}$ .
4. Perform traditional substitution on the masked matrix  $N'_{M \times N}$  by the generated S-box discussed in section 3.1.

5. Then masks from the top to bottom via RA of the image data  $N'_{M \times N}$  top (from 1st entry to last one).

## 6.6 Performance Analysis of Image Encryption

To assess the security and feasibility of the proposed modules in image encryption, we perform various standardized tests such as entropy, histogram, correlation, NPCR, UACI, and second-order statistics to validate the randomized nature of the encrypted image. Moreover, the sensitivity feature regarding key as well as image data is analyzed and examine the resistance against attacks to chosen plaintext. The whole encryption process and its simulation experiments are investigated on MATLAB 2019b using *Intel*<sup>®</sup> Core(TM)i5 – 7500U CPU @ 2.70GHz 2.90 GHz Processor, 8.00 – GB RAM, Microsoft Windows 10 with 64 – bit operating system. In this study, six different grayscale images of  $256 \times 256$  dimensions are chosen, Baboon, Pepper, Lena, Man, Moon Surface, Boat, and purely all black and white grayscale images are tested; mostly obtained from the USC-SIPI Miscellaneous Image dataset. As far as demonstration is concerned, randomly selected secret keys with some fixed parameters are  $p = 257, \mathcal{M}_{y_1, y_2}^{a_1, b_1, b_2} = \langle 97, 73 \rangle_{169, 5}^{0, 234, 123}, \hat{p} = 4079, c = 1501, d_1 = 1, d_2 = 32, W = F_{\hat{p}} \setminus \{0\}, Y^W = \left\{ \left( w_{(s_j)_n} \right)_{n=d_1}^{d_2} = \left( (s_j)_n \right)_{n=d_1}^{d_2} : \forall w \in W; n = d_1, d_1 + 1, \dots, d_2 \right\}$ . Figure 21 and Figure 23 illustrate the encryption output of the proposed SCM and PRNGM application to sample images and their corresponding histograms.

### 6.6.1 Histogram Analysis

Visual/Graphical description of the tonal distribution in an image is known as an image histogram, which represents the grayscale frequencies. As the frequency of each grayscale in the encrypted image occurs equally likely, the more it shows the flat histogram and confirming its high resistance to common statistical attacks. Figure 23, consists of the corresponding histograms relative to images in Figure 22 (a-f). Consequently, the encrypted images histograms not only achieve almost the required flatness level but also confirm to have meaningless patterns as well.

### 6.6.2 Correlation Analysis

The correlation coefficient (CC) of an image is quantitative measurement between two adjacent pixels, which describes the degree of dependency among pixels distribution. In this way, 10000 adjacent pairs are chosen to examine CC in the Vertical, Diagonal and

Horizontal directions of the original image and encrypted image. The CCs for original and encrypted images are computed and shown in Table 23 while their visual representation can be seen in Figure 23. The results revealed that the proposed mechanism greatly reduced the correlation among adjacent pixels in the original images, which affirms its high resistance against all kind of statistical attacks. As a result, the proposed modules are more suitable for image encryption applications.

### 6.6.3 Information Entropy

Information Entropy is used to compute the degree of randomness and uncertainty of gray-scale values in the encrypted image. As the encrypted image data ranges between  $0 \sim 255$ , thus the ideal entropy score is  $8 \text{ bits}$ . Consequently, the more it gets close to  $8 \text{ bits}$ , the more is the encrypted image secure against common statistical attacks. In Table 23, the results of information entropy of the six gray-scale images and their corresponding encrypted data of sized  $256 \times 256$  indicate that each encrypted image attains best entropy score, thus proving the suitability of the proposed modules for data security. Also, it can be seen from Table 22 and Table 23, the entropy results of the encrypted images with all-white and all-black content by proposed modules are much better in comparison to some recent encryption schemes.

### 6.6.4 Differential Attack

Differential attack is one of the main techniques for attackers where they try to extract some similar or non-random patterns in the encrypted data generated from two almost identical plain inputs. If such pattern exists, the adversary may try to find the exact key or a loophole and break the security of the encryption algorithm. In this way, secure encryption algorithm generates almost random encrypted data even for a slight change in the input data to resist against differential attacks. In this context, the number of pixel change rate (NPCR) and unified average changing intensity (UACI) are the proper tools for computing the resistance of encryption algorithm against differential attacks. Table 23 shows the NPCR and UACI recorded scores of six different gray-images with dimension 256 of each. The NPCR simulation results of the proposed encryption method clearly lie above the optimal value 99.5893% while the UACI scores in the optimal interval [33.3730%,33.5541%]. This reveals the high dependency of the proposed encryption method on the original image data and could be more effective against differential attacks

### 6.6.5 Key Sensitivity Analysis

In efficient cryptographic algorithm, the larger key space plays vital role in its effectiveness in respect of brute-force attack [119]. From cryptanalysis perspective, the minimum number

of guesses to generate a key space are  $2^{128}$ . The key space of our introduced cryptosystem is chosen so large to get 512 bits, and thus the key space for our proposed cryptosystem is much greater than  $2^{128}$ . Consequently, our scheme is highly resistive to brute-force attacks. Encryption phase sensitivity is examined by ciphering image data with two different secret keys having slight change. We introduce a single bit change to one of the pixels in the pepper image and encrypt the image data, shown in Figure 21. In this experiment, the difference image in Figure 21(e) reveals the fact that slight changes in secret key generate almost different encrypted images data. As a result, the proposed cryptosystem is highly secret key sensitive.

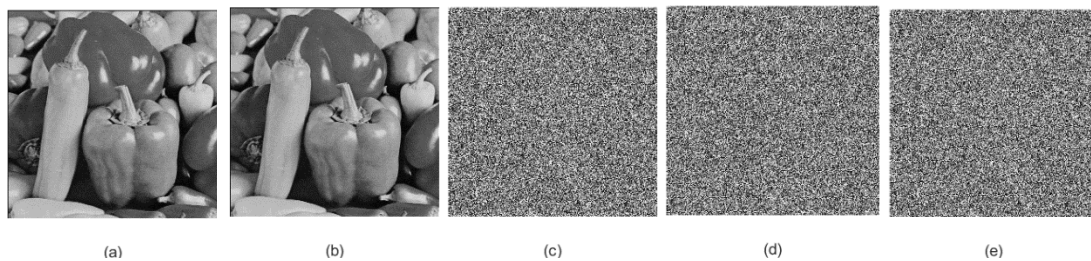


Figure 21. (a) Original Pepper image; (b) Original image from (a) with one bit change at position (2,240); (c) Encrypted image of (a); (d) Encrypted image of (b); (e) Difference image of (c) and (d).



Figure 22. (a)-(f) Tested images.

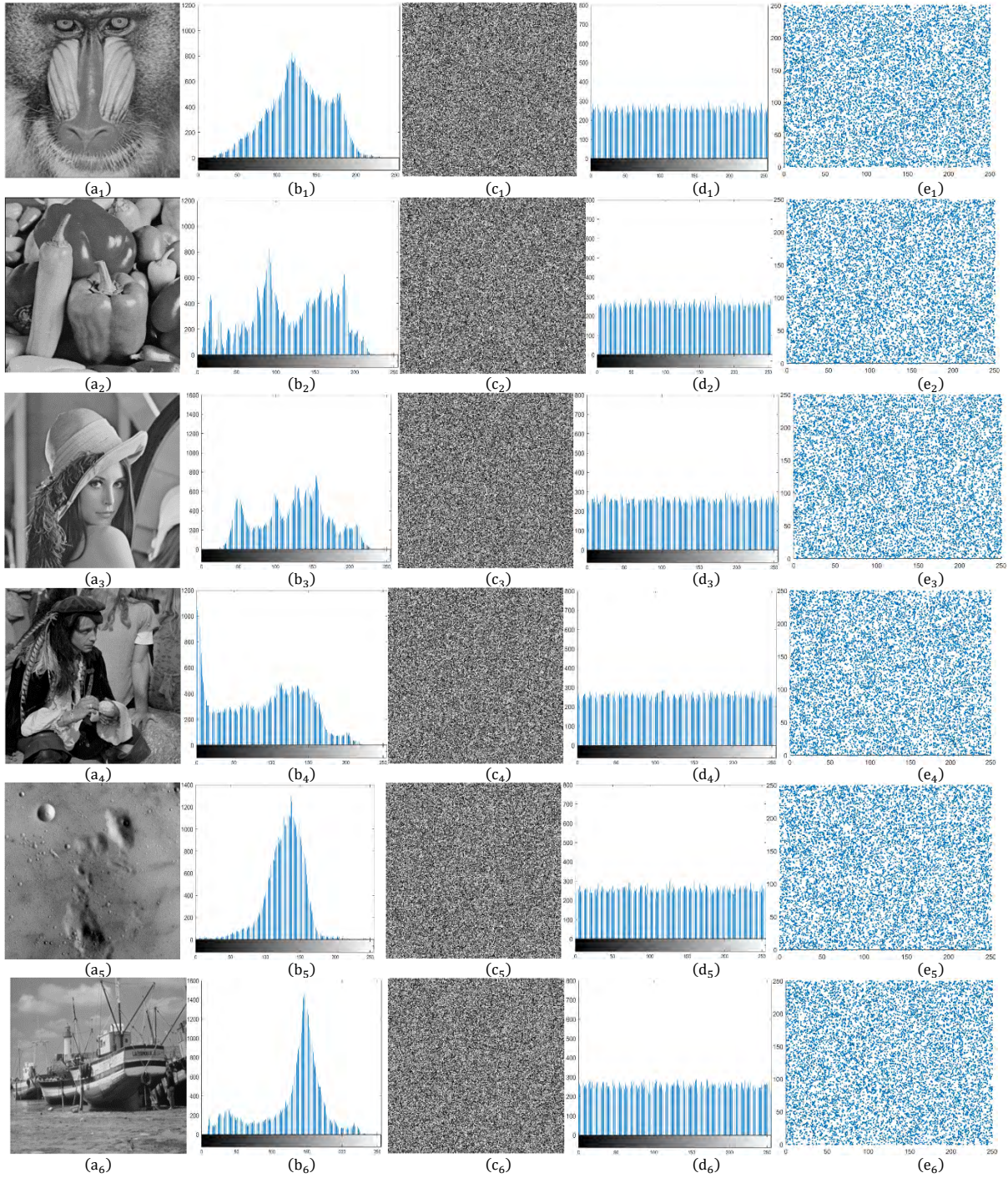


Figure 23.. (a<sub>1</sub>) Original image Baboon; (b<sub>1</sub>) Histogram of (a<sub>1</sub>); (c<sub>1</sub>) Encrypted Baboon; (d<sub>1</sub>) Histogram of (c<sub>1</sub>); (e<sub>1</sub>) Correlation of (c<sub>1</sub>); (a<sub>2</sub>) Original image Pepper; (b<sub>2</sub>) Histogram of (a<sub>2</sub>); (c<sub>2</sub>) Encrypted Pepper; (d<sub>2</sub>) Histogram of (c<sub>2</sub>); (e<sub>2</sub>) Correlation of (c<sub>2</sub>); (a<sub>3</sub>) Original image Lena; (b<sub>3</sub>) Histogram of (a<sub>3</sub>); (c<sub>3</sub>) Encrypted Lena; (d<sub>3</sub>) Histogram of (c<sub>3</sub>); (e<sub>3</sub>) Correlation of (c<sub>3</sub>); (a<sub>4</sub>) Original image Man; (b<sub>4</sub>) Histogram of (a<sub>4</sub>); (c<sub>4</sub>) Encrypted Man; (d<sub>4</sub>) Histogram of (c<sub>4</sub>); (e<sub>4</sub>) Correlation of (c<sub>4</sub>); (a<sub>5</sub>) Original image Moon; (b<sub>5</sub>) Histogram of (a<sub>5</sub>); (c<sub>5</sub>) Encrypted Moon; (d<sub>5</sub>) Histogram of (c<sub>5</sub>); (e<sub>5</sub>) Correlation of (c<sub>5</sub>); (a<sub>6</sub>) Original image Boat; (b<sub>6</sub>) Histogram of (a<sub>6</sub>); (c<sub>6</sub>) Encrypted Boat; (d<sub>6</sub>) Histogram of (c<sub>6</sub>); (e<sub>6</sub>) Correlation of (c<sub>6</sub>).

Table 22. Entropy, NPCR and UACI results of All-White and All-Black images

Scheme	Entropy		NPCR		UACI	
	All White	All Black	All White	All Black	All White	All Black
Our	7.997155	7.997565	99.60	99.61	33.45	33.72

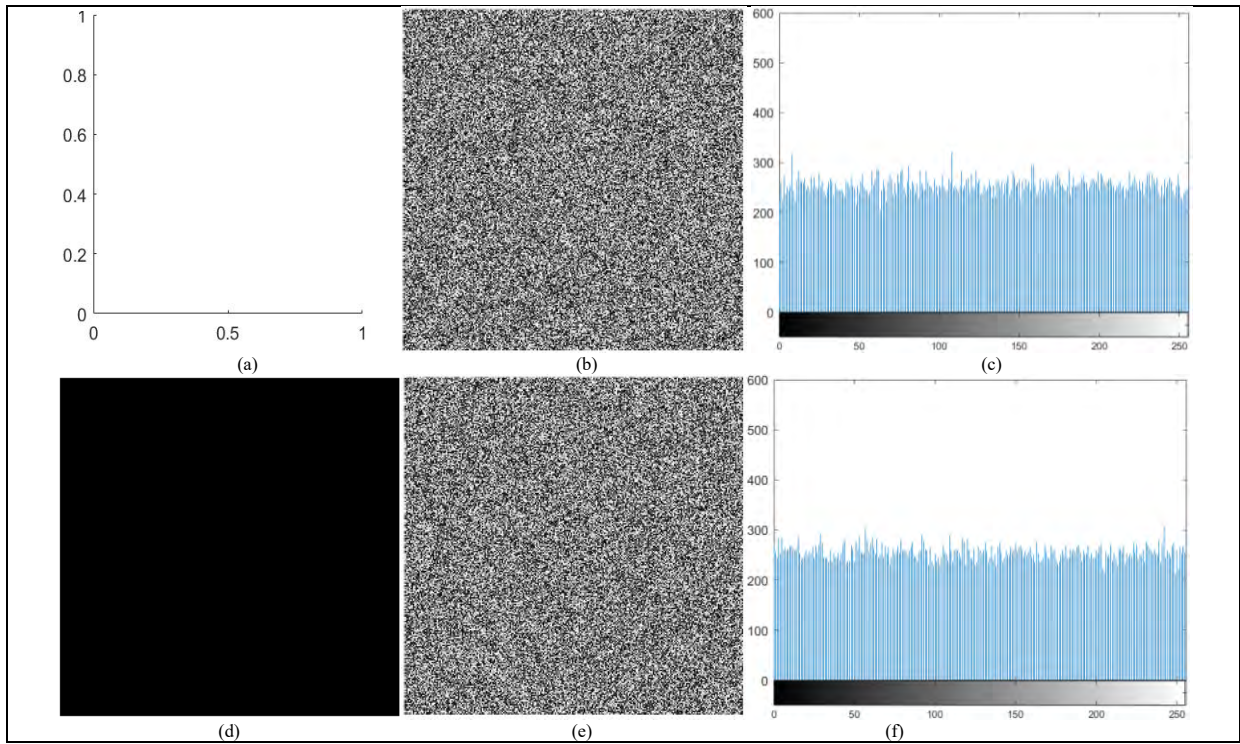


Figure 24. Proposed SCM and PRNM application: (a) “All-White”; (b) Encrypted image of (a); (c) Histogram of (b); (d) “All-Black”; (e) Encrypted image of (d); (f) Histogram of (e).

Table 23. Entropies, Correlations Coefficients, NPCR and UACI values

Original Image	Entropy	Correlation			NPCR	UACI
		Vertical	Diagonal	Horizontal		
Pepper	7.99777	0.0019	0.0035	0.0013	99.61	33.55
Baboon	7.99757	-0.0019	0.0016	0.0011	99.59	33.40
Lena	7.99779	0.0012	0.0006	0.0021	99.60	33.40
Man	7.99767	0.0020	0.0029	0.0027	99.57	33.42
Moon-Surface	7.99766	0.0034	0.0018	0.0040	99.60	33.47
Boat	7.99749	0.0004	0.0021	0.0032	99.67	33.63

Table 24. Comparison table for second order statistics and entropy with that of recent schemes

Plain Image	Scheme	Entropy	Correlation	Contrast	Homogeneity	Energy	Entropy		Ratio
							All White	All Black	
Baboon	Ours	7.2636	0.8621	0.4089	0.8403	0.1208			
Encrypted Baboon		<b>7.9980</b>	<b>-0.0078</b>	<b>10.5716</b>	<b>0.3865</b>	<b>0.0156</b>	<b>7.9998</b>	<b>7.9998</b>	
Ref.[101],2021		7.9976	0.0031	10.4148	0.3887	0.0156	---	---	1/3
Ref.[120], 2020		7.9817	-0.0128	10.4391	0.3889	0.0157	---	---	0/5
Ref.[121], 2019		7.9851	-0.0050	8.5792	0.4076	0.0175	---	---	1/4
Ref.[122], 2020		7.9553	-0.0087	10.3466	0.3895	0.0157	---	---	0/5
Ref.[7], 2020		---	---	---	---	---	7.9985	7.9985	0/2
Pepper	Ours	7.5553	0.9243	0.4359	0.8659	0.1012			
Encrypted Pepper		<b>7.9980</b>	<b>-0.0019</b>	<b>10.5003</b>	<b>0.3893</b>	<b>0.0156</b>	<b>7.9998</b>	<b>7.9998</b>	
Ref.[101], 2021		7.9969	0.0024	10.4172	0.3872	0.0156	---	---	1/3
Ref.[120], 2020		7.9545	-0.0061	10.5377	0.3894	0.0157	---	---	1/4
Ref.[121], 2019		7.9840	-0.0017	8.4985	0.4103	0.0175	---	---	1/4
Ref.[109], 2021		7.9973	---	---	---	---	7.9973	7.9974	0/3
Ref.[122], 2020		7.9566	-0.0075	10.3042	0.3899	0.0157	---	---	0/5

A ratio of  $1/3$  shows the advantage in one statistics of the competitor while the proposed scheme has got in three statistics over competitor



## 6.7 Comparison and Discussion

Generally, a random data with each entry is generated almost through number of arithmetic operations in many efficient cryptographic algorithms [6], [49], [75], [76], [78], [101], [103], [121], [123]. However, it increases the computational cost of the algorithm. Likewise, the schemes [6], [124] are configured using elliptic curve structure over large field. Avoid the excess use of arithmetic operations, we propose an EC cryptosystem based on indexing approach to obtain efficient dynamic S-box, PRNS, with reduced computational efforts. In addition, the prime field for S-box construction has been taken of minimum size, whereas PRNS are generated by assuming small prime fields. To analyze the strength of our scheme, we first deploy the IT to obtain each point lying on  $E(a, b, p): y^2 = x^3 + ax + b \pmod{p}$ . The indexing technique (IT) is processed as: Initially, defining two sequences  $\zeta = (y^2 \pmod{p})_{y=0}^{p-1}$  and  $\xi = (x^3 + ax + b \pmod{p})_{x=0}^{p-1}$ . Now, for any  $v \in \zeta \cap \xi$ , we have  $(x_j, y_i) \in E(a, b, p)$ , for all indexes  $x_j, y_i \in F_p$ ; where  $y_i^2 \pmod{p} = v = x_j^3 + ax_j + b \pmod{p}$ . For instance, we performed the indexing technique to generate all points using prime field  $F_{17}$ , as shown in Table 19. Then, we obtain the indexes of a common point in both columns, as shown in shaded cells. Since, for each index of a single common point  $\alpha \in F_p$  in column 1, there exist two indices having  $\alpha$  in Column:2 except for the common point appearing in the last index of Column 2, Table 19. For instance;  $\alpha = 1$  there are six pairs (4,1), (4,16), (13,1), (13,16), (17,1) and (17,16) that are the points lying on EC, where the last index can be treated as the additive identity of a prime field. Consequently, one can find out all the points accurately without use of any single group law operation. Subsequently, it will have a positive impact on the speed of proposed cryptosystem while execution in real time application. In this way, some primes are chosen and generate EC points using IT, GL-OT, and RA separately, whereas the generators are randomly selected for operating GL-OT, as shown in Table 21. The computational result in Table shows that IT takes less time in generating points lying on EC as compared to GL-OT and RA. Thus, the IT algorithm is much feasible to use for computing EC points over large primes. Secondly, our EC scheme uses minimum prime fields for the generation of multiple efficient S-boxes as the minimum size for a random sequence to get a standardized S-box is 256 with each integral point from the set [0,255] without repetition. Such an EC cryptosystem with minimum prime field for multiple efficient S-boxes has not been yet adopted in literature, to the best of author's knowledge. For instance, the EC scheme in [101] makes use of two operating modes for generating S-boxes with 106 minimum non-linearity scores over primes in the range of

[16,512] bits. Although, the same score is achieved using a fixed prime field containing 257 elements by our proposed scheme. Similarly, the PRNS scheme is proposed with the help of IT in this study as well. From Table 22 and Figure 24, the simulation results of PRNS based on entropy and histogram indicate that the proposed sequences satisfy the required randomness criteria. In addition, a hundred sequences of minimum required length  $10^6$  are obtained using 12 – bits prime only, which are then tested via NIST testing tool thus found best passing ratio in comparison with PRNS's ratio [8]. Likewise, TRNG is utilized to get multiple sequences using diffusive memristor [116] which are further assessed through NIST suit. It is revealed that the passing ratio of generated sequences in each test is less or equal to that of our proposed generated sequences. As a result, our proposed PRNGM acquires more capability of generating verified sequences; therefrom, confirms its suitability for secure cryptosystem [89]. To ensure the recommendation of our proposed algorithm in multimedia data security, some known statistical tests are employed on the encrypted multimedia data, and computed their numerical scores, as shown in Table 18, 20, 22, 23, and 24. Table 22 and 23, list the NPCR, UACI, correlation, and entropy scores for original images and their encrypted images. All these simulation results show that the proposed algorithm is highly secure. Similarly, Table 24 depicts the comparative study of proposed algorithm using entropy, correlation, and second order statistics scores with that of some recent cryptographic scheme [7], [101], [109], [120]–[122] which clearly indicates that our scheme shows more advantage in listed statistics over each competitor.

## Chapter 7

### Conclusion and Future Work

In this chapter, we presented the conclusion and future direction of the dissertation. In the first section of this chapter, we present the conclusion of the dissertation while the second section deals with the future directions. This chapter involves the detail and accurate explanation of the outcomes obtained in the dissertation. Some of the forthcoming prospective are also a part of this chapter.

Following are the main basic points established in this study, which can be categorized in the four main points.

1. Elliptic curve structures are used to generate verified PRNS and robust S-boxes to enhance the security strength of a cryptosystem.
2. Instead of generation a single S-box and pseudo random numbers sequence, the aim is to construct multiple number of S-boxes and pseudo random numbers of sequences by using simple as well as the core arithmetic operations of elliptic curves structure.
3. Designed some well-defined mathematical models with bijective features by utilizing PRNS and S-boxes.
4. These S-boxes and PRNS are used in multimedia data security by designing new algorithms for image encryption.

#### 7.1 Conclusion of Thesis

In this section, we discuss the significance role of EC structure in designing efficient techniques for generating S-box and PRNS. We developed S-box, PRN and permutation by using both group-theoretic, simple arithmetic, and indexing techniques of elliptic curves. In this connection, the y-coordinates of an elliptic curve followed by modulo 256 play a dynamic role in the proposed research study. Furthermore, we established some significant mathematical models for handling large-scale multimedia data for security aspects.

In chapter 2, we constituted S-box through elliptic curves. We developed a scheme based on PRN and permutation using both group-theoretic aspects (Isomorphic and Non-isomorphic) of elliptic curves, distinguishing the encryption schemes published in the recent past decades. The y-coordinate of the isomorphic class of a fixed EC is managed to generate multiple efficient S-boxes. Meanwhile some similar technique is used for the generation of PRNs over the non-isomorphic class of a fixed elliptic curve. The newly obtained S-box has better statistical and algebraic characteristics as compared to the existing ECC S-boxes.

In Chapter 3, we established an image encryption algorithm based on S-box and PRN, which are discussed in Chapter 2. Moreover, various permutations operations depending on the dimension of the original color image are created over the ECs preferably with different finite fields. The proposed cryptosystem has three main features:

- i- Simultaneous implements permutation operation independently along each channel of the original color image.
- ii- The confusion block is generated in the permuted image by dynamic S-box.
- iii- Masks the post-confused image by the proposed PRN.

Many researchers have tried to merge improved techniques to reduce the existing drawbacks in the previous work. In addition, we have already discussed the comparison of our proposed scheme with some existing schemes in the conclusion of Chapter 3. From which we conclude that our proposed scheme has strong resistance against some common statistical attacks. Further to all these, the proposed encryption scheme is better for security application purposes as it is equipped with a strong dynamic S-box in terms of nonlinearity. Finally, it can also be observed by the analyses that the diffusion property of the proposed method is surprisingly much better in the context of entropy and NPCR security analysis. Our proposed scheme could also be extended to the audio and video data.

In chapter 4, we discussed the group arithmetic operations using EC structure. Due to high impact of EC group law operations on security strength, the prime objective of EC structure is used in order to provide enough security to secrete data. By applying group theoretic technique, a cryptographic algorithm is good enough for randomness characteristics. For this purpose, we make use of some verified patterns to enhance the confusion-diffusion properties. For these achievements, we apply some concepts of group theory with EC to explore the hidden potential of subgroup coset model. The subgroup coset mechanism is exploited to establish the efficiency of both ECS-PRNSM and MS. The fabulous remark in the proposed mechanism is that the points occur more randomly one after another when generating whole subgroup, it's both coordinates also appear in similar fashion.

Consequently, there is no need of external mathematical operation to swap their points for their random purpose as presented in [103]. Subsequently, it is observed that the sub-group may be excellent selection to the base for MS and ECS-PRNSM some small prime fields. The proposed MS provides cryptographically strong S-boxes as compare to the some recent constructed S-boxes established in [78], [85]. Meanwhile, the ECS-PRNSM has a distinguishing feature towards a generated set of multiple independent random sequences with the best passing ratio in all tests [8], [88]. We also presented the graphical interpretation of consecutive pseudo random streams in which there is no similar pattern can be visualized as shown in Figure.12.

In Chapter 5, we presented a well-define mathematical model, which provides a key platform to generate a sufficient environment on a small prime for large, spaced multimedia data to get masked. Since the prime parameter is the principal component which stretched the size of the output data by producing a small change. Therefore, our scheme can be use for new challenges produced by internet of things (IoT) devices. As these devices not only required a quick response, but they also need a security strength during data transmission. The obtained MM designed with bijective features using randomly chosen keys. Therefrom, we revealed that the proposed scheme is in a best agreement with security analysis because of its large key space. Furthermore, the efficiency of the proposed encryption mechanism is tested using some standard and non-standard image database, selected from internet source including USC-SIPi images database [125]. From Table.4, we observed that the entropy results of the grayscale encrypted images are better than the schemes found in [9], [97]. The histogram analysis also indicates the efficient performance of the proposed ECS-PRNSM module. Specifically, the uniformness of encrypted image data can be recognized easily to view column three of Figure 15. From Table.4, it is concluded that our scheme has provided better results of entropy for different tested encrypted images.

In Chapter 6, the EC structure is generally employed in image encryption application. For this purpose, we reviewed some existing image encryption schemes based on EC using GL-OT. We established an EC-based algorithm using IT with partial engagement of GL-OT to reduce the time consumption/complexity. The proposed mechanism diffused each pixel value with PRNS module, and then created the confusion using S-box module. Both PRNS and S-box modules are designed by using isomorphic elliptic curves and sub-group respectively. The proposed scheme outperforms on the following main features:

- i- Performing efficient technique, rather GL-OT to generate EC points for both SCM and PRNGM modules.

- ii- Both SCM and PRNGM is processed through pure bijective models.
- iii- Minimum prime field is one of the prime features of proposed SCM.
- iv- Efficiency is enhanced on a small prime field of both SCM, PRNGM.
- v- Encryption performance is excellent in terms of security measures.

The efficiency of SCM and PRNGM is verified by conducting S-box and NIST testing tools respectively, and we found them more efficient relative to their own characteristics. Meanwhile, the encryption performance is examined by conducting some experimental tests on the encrypted image data. The simulated data present in chapter 6, indicates that the proposed modules generate highly secure encrypted data against the existing known attacks. Furthermore, the comparative study of our crypto system with some recent research also reveals that our scheme uses fewer number of arithmetic operations as compared to the schemes established in [6],[78],[101]. In short, due to high encryption speed our proposed encryption scheme play a better role in real-time encryption.

## 7.2 Perspective of Future Directions

During my research work, we realized that we shall not limit the scope of elliptic curves to symmetric encryption algorithms. But we can rather proceed parallelly to work on the EC asymmetric and efficient fully homomorphic encryption as well as core theoretic directions. In this connection some queries regarding these aspects are elaborated in the following:

1. Develop a relation between Carmichael and primitive elements in Galois ring to get a complete set consists of non-zero divisors.
2. Defining the elliptic curve points over the complete set so that every point has multiplicative inverse in each component of EC.
3. Designing a bilinear map over the points of EC that will probably satisfy both additive and multiplicative homomorphic properties.
4. Establish theoretic results that confirms the correctness of decryption process.
5. Semantic security of proposed algorithm will probably depend on the intractableness of both primitive elements as well as non-zero divisors of the complete set.

The above suggestions are developed by thoroughly inspection of well-known homomorphic algorithms namely Goldwasser-Micali (GM), ElGamal, Benaloh, Okamoto-Uchiyama, Paillier, and Boneh-Goh-Nissim Algorithms [126]. The core idea behind these algorithms are mostly depends on either residuosity class or integer problem. The stated algorithms are semantically secure and intractable. Moreover, these algorithms are either additively or multiplicatively homomorphic encryption algorithms. However, the GM and Benaloh

algorithms are both additive and multiplicative homomorphic by using an integer scalar  $s$ . It is noting that the Paillier and Boneh-Goh-Nissim algorithms play vital role in generating our idea for future research study.

## References

- [1] Washington, L. C. (2008). *Elliptic curves: number theory and cryptography*. CRC press.
- [2] Wenberg, S. L. (2013). *Elliptic curves and their cryptographic applications*.
- [3] Galbraith, S. D. (2012). *Mathematics of public key cryptography*. Cambridge University Press.
- [4] Gallian, J. (2010). *Contemporary Abstract Algebra*, Cengage Learning, Exercise 43 (p. 84). ISBN 978-0-547-16509-7.
- [5] Farwa, S., Bibi, N., & Muhammad, N. (2020). An efficient image encryption scheme using Fresnelet transform and elliptic curve based scrambling. *Multimedia Tools and Applications*, 79(37), 28225-28238.
- [6] Toughi, S., Fathi, M. H., & Sekhavat, Y. A. (2017). An image encryption scheme based on elliptic curve pseudo random and advanced encryption system. *Signal processing*, 141, 217-227.
- [7] Yu, S. S., Zhou, N. R., Gong, L. H., & Nie, Z. (2020). Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyperchaotic system. *Optics and Lasers in Engineering*, 124, 105816.
- [8] Brown, J., Zhang, J. F., Zhou, B., Mehedi, M., Freitas, P., Marsland, J., & Ji, Z. (2020). Random-telegraph-noise-enabled true random number generator for hardware security. *Scientific reports*, 10(1), 1-13.
- [9] Wang, X., Guan, N., Zhao, H., Wang, S., & Zhang, Y. (2020). A new image encryption scheme based on coupling map lattices with mixed multi-chaos. *Scientific reports*, 10(1), 1-15.
- [10] Jia, N., Liu, S., Ding, Q., Wu, S., & Pan, X. (2016). A new method of encryption algorithm based on chaos and ECC. *Journal of Information Hiding and Multimedia Signal Processing*, 7(3), 637-643.
- [11] Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of computation*, 48(177), 203-209.
- [12] Miller, V. S. (1985, August). Use of elliptic curves in cryptography. In *Conference on the theory and application of cryptographic techniques* (pp. 417-426). Springer, Berlin, Heidelberg.
- [13] Te Chiang, Y., Wang, H. S., & Wang, Y. N. (2013). A Chaotic-Based Pseudo-Random Bit Generator for Navigation Applications. *Applied Mechanics and Materials*, 311, 99.
- [14] Reyad, O., & Kotulski, Z. (2015, November). Image encryption using koblitz's encoding and new mapping method based on elliptic curve random number generator. In *International Conference on Multimedia Communications, Services and Security* (pp. 34-45). Spri.



- [15] Özkaynak, F. (2019). Construction of robust substitution boxes based on chaotic systems. *Neural Computing and Applications*, 31(8), 3317-3326.
- [16] Gao, T., and Chen, Z. (2008). Image encryption based on a new total shuffling algorithm. *Chaos, solitons & fractals*, 38(1), 213-220.
- [17] Indrakanti, S. P., and Avadhani, P. S. (2011). Permutation based image encryption technique. *International Journal of Computer Applications*, 28(8), 45-47.
- [18] Li, X., Wang, L., Yan, Y., and Liu, P. (2016). An improvement color image encryption algorithm based on DNA operations and real and complex chaotic systems. *Optik-International Journal for Light and Electron Optics*, 127(5), 2558-2565.
- [19] Wang, X. Y., Zhang, H. L., and Bao, X. M. (2016). Color image encryption scheme using CML and DNA sequence operations. *Biosystems*, 144, 18-26.
- [20] Jakimoski, G., and Kocarev, L. (2001). Chaos and cryptography: block encryption ciphers based on chaotic maps. *Ieee transactions on circuits and systems i: fundamental theory and applications*, 48(2), 163-169.
- [21] Tsafack, N., Kengne, J., Abd-El-Atty, B., Iliyasu, A. M., Hirota, K., & Abd EL-Latif, A. A. (2020). Design and implementation of a simple dynamical 4-D chaotic circuit with applications in image encryption. *Information Sciences*, 515, 191-217.
- [22] Li, L., Abd-El-Atty, B., Elseuofi, S., Abd El-Rahiem, B., & Abd El-Latif, A. A. (2019, May). Quaternion and multiple chaotic systems based pseudo-random number generator. In *2019 2nd International Conference on Computer Applications & Information Security*.
- [23] Peng, J., Abd El-Latif, A. A., Belazi, A., & Kotulski, Z. (2017, July). Efficient chaotic nonlinear component for secure cryptosystems. In *2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN)* (pp. 989-993). IEEE.
- [24] Belazi, A., Abd El-Latif, A. A., Diaconu, A. V., Rhouma, R., & Belghith, S. (2017). Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms. *Optics and Lasers in Engineering*, 88, 37-50.
- [25] Ye, Guodong, and Xiaoling Huang. 'An efficient symmetric image encryption algorithm based on an intertwining logistic map.' *Neurocomputing* 251 (2017): 45-53.
- [26] Azam, N. A., Hayat, U., and Ullah, I. (2018). An Injective S-Box Design Scheme over an Ordered Isomorphic Elliptic Curve and Its Characterization. *Security and Communication Networks*, 2018.
- [27] Shankar, K., and Eswaran, P. (2016). An efficient image encryption technique based on optimized key generation in ECC using genetic algorithm. In *Artificial Intelligence and Evolutionary Computations in Engineering Systems* (pp. 705-714). Springer, New.
- [28] Hayat, U., and Azam, N. A. (2019). A novel image encryption scheme based on an elliptic curve. *Signal Processing*, 155, 391-402.
- [29] Lee, L. P., and Wong, K. W. (2004). A random number generator based on elliptic

- curve operations. *Computers & Mathematics with Applications*, 47(2-3), 217-226.
- [30] Khan, M., Shah, T., and Batool, S. I. (2016). Construction of S-box based on chaotic Boolean functions and its application in image encryption. *Neural Computing and Applications*, 27(3), 677-685.
- [31] Ahmad, M., Bhatia, D., and Hassan, Y. (2015). A novel ant colony optimization-based scheme for substitution box design. *Procedia Computer Science*, 57, 572-580.
- [32] Gura, N., Patel, A., Wander, A., Eberle, H., and Shantz, S. C. (2004, August). Comparing elliptic curve cryptography and RSA on 8-bit CPUs. In *International workshop on cryptographic hardware and embedded systems* (pp. 119-132). Springer, Berlin, Heidel.
- [33] Nestor, T., De Dieu, N. J., Jacques, K., Yves, E. J., Iliyasu, A. M., El-Latif, A., & Ahmed, A. (2020). A multidimensional hyperjerk oscillator: Dynamics analysis, analogue and embedded systems implementation, and its application as a cryptosystem. *Se*.
- [34] Abd El-Latif, A. A., Abd-El-Atty, B., Mazurczyk, W., Fung, C., & Venegas-Andraca, S. E. (2020). Secure data encryption based on quantum walks for 5G Internet of Things scenario. *IEEE Transactions on Network and Service Management*, 17(1), 118-131.
- [35] Belazi, A., Abd El-Latif, A. A., Rhouma, R., & Belghith, S. (2015, August). Selective image encryption scheme based on DWT, AES S-box and chaotic permutation. In *2015 International wireless communications and mobile computing conference (IWCMC)* (pp. 6).
- [36] Belazi, A., & Abd El-Latif, A. A. (2017). A simple yet efficient S-box method based on chaotic sine map. *Optik*, 130, 1438-1444.
- [37] Patro, K. A. K., Banerjee, A., and Acharya, B. (2017, October). A simple, secure and time efficient multi-way rotational permutation and diffusion-based image encryption by using multiple 1-D chaotic maps. In *International Conference on Next Generatio*.
- [38] Peng, Zai-Ping, et al. 'A novel four-dimensional multi-wing hyper-chaotic attractor and its application in image encryption.' (2014): 240506-240506.
- [39] Liu, G., Yang, W., Liu, W., & Dai, Y. (2015). Designing S-boxes based on 3-D four-wing autonomous chaotic system. *Nonlinear Dynamics*, 82(4), 1867-1877.
- [40] Liu, H., & Liu, Y. (2014). Cryptanalyzing an image encryption scheme based on hybrid chaotic system and cyclic elliptic curve. *Optics & Laser Technology*, 56, 15-19.
- [41] El-Latif, A.A.A.; Niu, X. A Hybrid Chaotic System and Cyclic Elliptic Curve for Image Encryption. *AEU-Int*.
- [42] Khan, M., and Asghar, Z. (2018). A novel construction of substitution box for image encryption applications with Gingerbreadman chaotic map and S 8 permutation. *Neural Computing and Applications*, 29(4), 993-999.

- [43] Meier, W., and Staffelbach, O. (1989, April). Nonlinearity criteria for cryptographic functions. In *Workshop on the Theory and Application of Cryptographic Techniques* (pp. 549-562). Springer, Berlin, Heidelberg.
- [44] Abd EL-Latif, A. A., Abd-El-Atty, B., & Venegas-Andraca, S. E. (2019). A novel image steganography technique based on quantum substitution boxes. *Optics & Laser Technology*, 116, 92-102.
- [45] Adams, C., and Tavares, S. (1990). The structured design of cryptographically good S-boxes. *Journal of Cryptology*, 3(1), 27-41.
- [46] Weister, A. F., and Tavares, S. E. (1986). On the design of S-boxes [A], *Advances in Cryptology-CRYPTO'85* [C].
- [47] Abd El-Latif, A. A., Abd-El-Atty, B., Mazurczyk, W., Fung, C., & Venegas-Andraca, S. E. (2020). Secure data encryption based on quantum walks for 5G Internet of Things scenario. *IEEE Transactions on Network and Service Management*, 17(1), 118-131.
- [48] Wang, Y., Wong, K. W., Li, C., and Li, Y. (2012). A novel method to design S-box based on chaotic map and genetic algorithm. *Physics Letters A*, 376(6-7), 827-833.
- [49] Reyad, O., & Kotulski, Z. (2015). On pseudo-random number generators using elliptic curves and chaotic systems. *Applied Mathematics & Information Sciences*, 9(1), 31.
- [50] Chen, R. J., and Horng, S. J. (2010). Novel SCAN-CA-based image security system using SCAN and 2-D von Neumann cellular automata. *Signal Processing: Image Communication*, 25(6), 413-426.
- [51] Chen, T. H., and Li, K. C. (2012). Multi-image encryption by circular random grids. *Information Sciences*, 189, 255-265.
- [52] Zhou, Y., Panetta, K., Agaian, S., and Chen, C. P. (2013).  $(n, k, p)$ -Gray code for image systems. *IEEE transactions on cybernetics*, 43(2), 515-529.
- [53] Liao, X., Lai, S., and Zhou, Q. (2010). A novel image encryption algorithm based on self-adaptive wave transmission. *Signal Processing*, 90(9), 2714-2722.
- [54] Liu, H., and Wang, X. (2011). Color image encryption using spatial bit-level permutation and high-dimension chaotic system. *Optics Communications*, 284(16-17), 3895-3903.
- [55] Zhang, M., and Tong, X. (2014). A new chaotic map-based image encryption schemes for several image formats. *Journal of Systems and Software*, 98, 140-154.
- [56] Bhatnagar, G., Wu, Q. J., and Raman, B. (2013). Discrete fractional wavelet transforms and its application to multiple encryptions. *Information Sciences*, 223, 297-316.
- [57] Mehra, I., and Nishchal, N. K. (2014). Image fusion using wavelet transform and its application to asymmetric cryptosystem and hiding. *Optics express*, 22(5), 5474-5482.

- [58] Xuejing, K., & Zihui, G. (2020). A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system. *Signal Processing: Image Communication*, 80, 115670.
- [59] Ghadirli, H. M., Nodehi, A., and Enayatifar, R. (2019). An overview of encryption algorithms in color images. *Signal Processing*.
- [60] Faraoun, K. M. (2014). Fast encryption of RGB color digital images using a tweakable cellular automaton-based schema. *Optics & Laser Technology*, 64, 145-155.
- [61] Mohamed, N. A., El-Azeim, M. A., Zaghloul, A., & Abd El-Latif, A. A. (2015, November). Image encryption scheme for secure digital images based on 3D cat map and turing machine. In *2015 7th International Conference of Soft Computing and Pattern Recogni.*
- [62] Li, X., Wang, L., Yan, Y., and Liu, P. (2016). An improvement color image encryption algorithm based on DNA operations and real and complex chaotic systems. *Optik-International Journal for Light and Electron Optics*, 127(5), 2558-2565.
- [63] Kumar, M., Chhabra, P., & Garg, N. K. (2018). An efficient content based image retrieval system using BayesNet and K-NN. *Multimedia Tools and Applications*, 77(16), 21557-21570.
- [64] Chhabra, P., Garg, N. K., & Kumar, M. (2020). Content-based image retrieval system using ORB and SIFT features. *Neural Computing and Applications*, 32(7), 2725-2733.
- [65] Bansal, M., Kumar, M., Kumar, M., & Kumar, K. (2021). An efficient technique for object recognition using Shi-Tomasi corner detection algorithm. *Soft Computing*, 25(6), 4423-4432.
- [66] Kumar, M., Bansal, M., & Kumar, M. (2020). 2D object recognition techniques: state-of-the-art work. *Archives of Computational Methods in Engineering*, 2.
- [67] Monika, M. K., & Kumar, M. (2020). XGBoost: 2D-Object Recognition Using Shape Descriptors and Extreme Gradient Boosting Classifier. *Computational Methods and Data Engineering: Proceedings of ICMDE 2020, Volume 1*, 1227, 207.
- [68] Garg, D., Garg, N. K., & Kumar, M. (2018). Underwater image enhancement using blending of CLAHE and percentile methodologies. *Multimedia Tools and Applications*, 77(20), 26545-26561.
- [69] Nian-Sheng, L. (2011). Pseudo-randomness and complexity of binary sequences generated by the chaotic system. *Communications in Nonlinear Science and Numerical Simulation*, 16(2), 761-768.
- [70] Akhshani, A., Akhavan, A., Mobaraki, A., Lim, S. C., & Hassan, Z. (2014). Pseudo random number generator based on quantum chaotic map. *Communications in Nonlinear Science and Numerical Simulation*, 19(1), 101-111.
- [71] Ye, T., & Zhimao, L. (2018). Chaotic S-box: Six-dimensional fractional Lorenz–Duffing chaotic system and O-shaped path scrambling. *Nonlinear Dynamics*, 94(3), 2115-2126.

- [72] Zahid, A. H., & Arshad, M. J. (2019). An innovative design of substitution-boxes using cubic polynomial mapping. *Symmetry*, 11(3), 437.
- [73] Ramesh, A., & Jain, A. (2015, December). Hybrid image encryption using Pseudo Random Number Generators, and transposition and substitution techniques. In 2015 International Conference on Trends in Automation, Communications and Computing Technology (I-TAC).
- [74] Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell system technical journal*, 28(4), 656-715.
- [75] Hussain, I., Shah, T., Mahmood, H., & Gondal, M. A. (2013). A projective general linear group based algorithm for the construction of substitution box for block ciphers. *Neural Computing and Applications*, 22(6), 1085-1093.
- [76] ul Haq, T., & Shah, T. (2020).  $12 \times 12$  S-box Design and its Application to RGB Image Encryption. *Optik*, 164922. doi:10.1016/j.ijleo.2020.164922.
- [77] ul Haq, T., & Shah, T. (2020). Algebra-chaos amalgam and DNA transform based multiple digital image encryption. *Journal of Information Security and Applications*, 54, 102592.
- [78] Haider, M. I., Ali, A., Shah, D., & Shah, T. (2020). Block cipher's nonlinear component design by elliptic curves: an image encryption application. *Multimedia Tools and Applications*, 1-26.
- [79] Lai, X., & Massey, J. L. (1990, May). A proposal for a new block encryption standard. In *Workshop on the Theory and Application of Cryptographic Techniques* (pp. 389-404). Springer, Berlin, Heidelberg.
- [80] Adams, C.; Tavares, S. The Structured Design of Cryptographically Good S-boxes. *J. Cryptol.* 1990, 3, 27–41.
- [81] Matsui, M. Linear cryptanalysis method of DES cipher. In *Advances in Cryptology, Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques (EURO-CRYPT-93)*, Lofthus, Norway, 23–27 May 1993; Springer: Berlin/Heidelberg, German.
- [82] Webster, A.; Tavares, S.E. On the design of S-boxes. In *Conference on the Theory and Application of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 1985; pp. 523–534.
- [83] Çavuşoğlu, Ü., Zengin, A., Pehlivan, I., & Kaçar, S. (2017). A novel approach for strong S-Box generation algorithm design based on chaotic scaled Zhongtang system. *Nonlinear Dynamics*, 87(2), 1081-1094.
- [84] Özkaynak, F., Çelik, V., & Özer, A. B. (2017). A new S-box construction method based on the fractional-order chaotic Chen system. *Signal, Image and Video Processing*, 11(4), 659-664.
- [85] Abd el-Latif, A. A., Abd-el-Atty, B., Amin, M., & Iliyasu, A. M. (2020). Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics and

- cryptographic applications. *Scientific Reports*, 10(1), 1-16.
- [86] Wang, X., Çavuşoğlu, Ü., Kacar, S., Akgul, A., Pham, V. T., Jafari, S., .. & Nguyen, X. Q. (2019). S-box based image encryption application using a chaotic system without equilibrium. *Applied Sciences*, 9(4), 781.
- [87] Wang, Y., Liu, Z., Ma, J., & He, H. (2016). A pseudorandom number generator based on piecewise logistic map. *Nonlinear Dynamics*, 83(4), 2373-2391.
- [88] Jiang, H., Belkin, D., Savel'ev, S. E., Lin, S., Wang, Z., Li, Y., .. & Barnell, M. (2017). A novel true random number generator based on a stochastic diffusive memristor. *Nature communications*, 8(1), 1-9.
- [89] Reyad, O., Kotulski, Z., & Abd-Elhafiez, W. M. (2016). Image encryption using chaos-driven elliptic curve pseudo-random number generators. *Appl. Math. Inf. Sci.*, 10(4), 1283-1292.
- [90] Abd El-Latif, A. A., & Niu, X. (2013). A hybrid chaotic system and cyclic elliptic curve for image encryption. *AEU-International Journal of Electronics and Communications*, 67(2), 136-143.
- [91] Shah, D., Shah, T., & Jamal, S. S. (2019). A novel efficient image encryption algorithm based on affine transformation combine with linear fractional transformation. *Multidimensional Systems and Signal Processing*, 1-21.
- [92] Shah, D., & Shah, T. (2020). A novel discrete image encryption algorithm based on finite algebraic structures. *Multimedia Tools and Applications*, 1-20.
- [93] Liu, Q., & Liu, L. (2020). Color Image Encryption Algorithm Based on DNA Coding and Double Chaos System. *IEEE Access*, 8, 83596-83610.
- [94] Shah, T., Ali, A., Khan, M., Farooq, G., & de Andrade, A. A. (2020). Galois Ring  $\mathbb{Z}_8[x]/(x^3+8)$  Dependent  $24 \times 24$  S-Box Design: An RGB Image Encryption Application. *Wireless Personal Communications*, 113(2), 1201-1.
- [95] Shah, D., & Shah, T. (2020). Binary Galois field extensions dependent multimedia data security scheme. *Microprocessors and Microsystems*, 77, 103181.
- [96] Azimi, Z., & Ahadpour, S. (2020). Color image encryption based on DNA encoding and pair coupled chaotic maps. *Multimedia Tools and Applications*, 79(3), 1727-1744.
- [97] Ye, G., Jiao, K., Huang, X., Goi, B. M., & Yap, W. S. (2020). An image encryption scheme based on public key cryptosystem and quantum logistic map. *Scientific Reports*, 10(1), 1-19.
- [98] Zhang, Y. Q., He, Y., Li, P., & Wang, X. Y. (2020). A new color image encryption scheme based on 2DNLCML system and genetic operations. *Optics and Lasers in Engineering*, 128, 106040.
- [99] Ran, Q., Wang, L., Ma, J., Tan, L., & Yu, S. (2018). A quantum color image encryption scheme based on coupled hyper-chaotic Lorenz system with three impulse

- injections. *Quantum Information Processing*, 17(8), 188.
- [100] Xian, Y., & Wang, X. (2021). Fractal sorting matrix and its application on chaotic image encryption. *Information Sciences*, 547, 1154-1169.
- [101] Ibrahim, S., & Abbas, A. M. (2021). Efficient Key-dependent Dynamic S-Boxes Based on Permuted Elliptic Curves. *Information Sciences*.
- [102] Zahid, A. H., Al-Solami, E., & Ahmad, M. (2020). A novel modular approach based substitution-box design for image encryption. *IEEE Access*, 8, 150326-150340.
- [103] Ibrahim, S., & Alharbi, A. (2020). Efficient Image Encryption Scheme Using Henon Map, Dynamic S-Boxes and Elliptic Curve Cryptography. *IEEE Access*, 8, 194289-194302.
- [104] Ayubi, P., Setayeshi, S., & Rahmani, A. M. (2020). Deterministic chaos game: A new fractal based pseudo-random number generator and its cryptographic application. *Journal of Information Security and Applications*, 52, 102472.
- [105] Lu, Q., Zhu, C., & Deng, X. (2020). An efficient image encryption scheme based on the LSS chaotic map and single S-box. *IEEE Access*, 8, 25664-25678.
- [106] Alhadawi, H. S., Lambić, D., Zolkipli, M. F., & Ahmad, M. (2020). Globalized firefly algorithm and chaos for designing substitution box. *Journal of Information Security and Applications*, 55, 102671.
- [107] Razaq, A., Ullah, A., Alolaiyan, H., & Yousaf, A. (2021). A novel group theoretic and graphical approach for designing cryptographically strong nonlinear components of block ciphers. *Wireless Personal Communications*, 116(4), 3165-3190.
- [108] Lu, Y., Yu, K., & Lv, X. (2021). Image encryption with one-time password mechanism and pseudo-features. *Multimedia Tools and Applications*, 1-15.
- [109] Wang, X., & Li, Y. (2021). Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence. *Optics and Lasers in Engineering*, 137, 106393.
- [110] Lambić, D. (2020). A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design. *Nonlinear Dynamics*, 100(1), 699-711.
- [111] Hua, Z., Li, J., Chen, Y., & Yi, S. (2021). Design and application of an S-box using complete Latin square. *Nonlinear Dynamics*, 1-19.
- [112] Jiang, Z., & Ding, Q. (2021). Construction of an S-Box Based on Chaotic and Bent Functions. *Symmetry*, 13(4), 671.
- [113] S. Sathyanarayana , M.A. Kumar , K.H. Bhat ,Random binary and non-binary sequences derived from random sequence of points on cyclic elliptic curve over finite field  $GF(2^m)$  and their properties, *Inf. Secur. J.* 19 (2) (2010) 84–94 .
- [114] P. Ayubi, S. Setayeshi, and A. Masoud, *Journal of Information Security and*

- Applications Deterministic chaos game : A new fractal based pseudo-random number generator and its cryptographic application,” vol. 52, 2020.
- [115] Abd EL-Latif, A. A., Abd-El-Atty, B., & Venegas-Andraca, S. E. (2020). Controlled alternate quantum walk-based pseudo-random number generator and its application to quantum color image encryption. *Physica A: Statistical Mechanics and its Applications*, 547”.
- [116] Jiang, H., Belkin, D., Savel’ev, S. E., Lin, S., Wang, Z., Li, Y., .. & Xia, Q. (2017). A novel true random number generator based on a stochastic diffusive memristor. *Nature communications*, 8(1), 1-9.
- [117] Rukhin, A., Soto, J., Nechvatal, J., Smid, M., & Barker, E. (2001). A statistical test suite for random and pseudorandom number generators for cryptographic applications. Booz-allen and hamilton inc mclean va.
- [118] Li, C., Lin, D., & Lü, J. (2017). Cryptanalyzing an image-scrambling encryption algorithm of pixel bits. *IEEE MultiMedia*, 24(3), 64-71.
- [119] Stinson, D. R., & Paterson, M. (2018). *Cryptography: theory and practice*. CRC press.
- [120] “Razaq, A., Alolaiyan, H., Ahmad, M., Yousaf, M. A., Shuaib, U., Aslam, W., & Alawida, M. (2020). A novel method for generation of strong substitution-boxes based on coset graphs and symmetric groups. *IEEE Access*, 8, 75473-75490.
- [121] “Ullah, A., Javeed, A., & Shah, T. (2019). A scheme based on algebraic and chaotic structures for the construction of substitution box. *Multimedia Tools and Applications*, 78(22), 32467-32484.
- [122] Yousaf, M. A., Alolaiyan, H., Ahmad, M., Dilbar, M., & Razaq, A. (2020). Comparison of pre and post-action of a finite abelian group over certain nonlinear schemes. *IEEE Access*, 8, 39781-39792.
- [123] Shah, T., & Shah, D. (2019). Construction of highly nonlinear S-boxes for degree 8 primitive irreducible polynomials over  $\mathbb{Z}_2$ . *Multimedia Tools and Applications*, 78(2), 1219-1234.
- [124] S. Ibrahim and A. M. Abbas, Efficient Key-dependent Dynamic S-Boxes Based on Permuted Elliptic Curves, *Inf. Sci. (Ny)*, vol. 558, pp. 246–264, 2021, doi: 10.1016/j.ins.2021.01.014.
- [125] USC-SIPI. Image database. Available at <http://sipi.usc.edu/database/database.php> .
- [126] Koç, Ç. K., Özdemir, F., & Özger, Z. Ö. (2021). Partially Homomorphic Encryption (pp. 37-41). Springer.



## Turnitin Originality Report

Elliptic Curve Computation and Their Applications in Data Security  
Imran Haider .

by Muhammad



From PhD (PhD DRSML)

- Processed on 31-Aug-2023 08:19 PKT
- ID: 2154709818
- Word Count: 30743

## Similarity Index

17%

## Similarity by Source

Internet Sources:

10%

Publications:

14%

Student Papers:

3%

M. Imran Haider  
Focal Person (Turnitin)  
Quaid-i-Azam University  
Islamabad

## sources:

- 1 1% match (Internet from 13-Jun-2022)  
[https://www.researchgate.net/publication/343771261\\_XGBoost\\_2D-Object\\_Recognition\\_Using\\_Shape\\_Descriptors\\_and\\_Extreme\\_Gradient\\_Boosting\\_Classifier](https://www.researchgate.net/publication/343771261_XGBoost_2D-Object_Recognition_Using_Shape_Descriptors_and_Extreme_Gradient_Boosting_Classifier)
- 2 1% match (Internet from 31-Jan-2023)  
[https://www.researchgate.net/publication/299459499\\_Color\\_image\\_encryption\\_scheme\\_using\\_CML\\_and\\_DNA\\_sequence\\_operations](https://www.researchgate.net/publication/299459499_Color_image_encryption_scheme_using_CML_and_DNA_sequence_operations)
- 3 < 1% match (Internet from 15-Feb-2023)  
[https://www.researchgate.net/figure/Correlations-of-two-vertically-adjacent-pixels-in-the-original-image-and-in-the-ciphered\\_fig3\\_223151138](https://www.researchgate.net/figure/Correlations-of-two-vertically-adjacent-pixels-in-the-original-image-and-in-the-ciphered_fig3_223151138)
- 4 < 1% match (Internet from 06-Feb-2023)  
[https://www.researchgate.net/publication/268076685\\_On\\_Pseudo-Random\\_Number\\_Generators\\_Using\\_Elliptic\\_Curves\\_and\\_Chaotic\\_Systems](https://www.researchgate.net/publication/268076685_On_Pseudo-Random_Number_Generators_Using_Elliptic_Curves_and_Chaotic_Systems)
- 5 < 1% match (Internet from 18-Feb-2023)  
[https://www.researchgate.net/publication/309469292\\_An\\_efficient\\_and\\_secure\\_partial\\_image\\_encryption\\_for\\_wireless\\_multimedia\\_sensor\\_ne](https://www.researchgate.net/publication/309469292_An_efficient_and_secure_partial_image_encryption_for_wireless_multimedia_sensor_ne)
- 6 < 1% match (Internet from 15-Feb-2023)  
[https://www.researchgate.net/publication/223398112\\_A\\_novel\\_image\\_encryption\\_algorithm\\_based\\_on\\_self-adaptive\\_wave\\_transmission](https://www.researchgate.net/publication/223398112_A_novel_image_encryption_algorithm_based_on_self-adaptive_wave_transmission)
- 7 < 1% match (Internet from 15-Mar-2023)  
[https://www.researchgate.net/publication/323130392\\_A\\_Maximum\\_Feasible\\_Subsystem\\_for\\_Globally\\_Optimal\\_3D\\_Point\\_Cloud\\_Registration](https://www.researchgate.net/publication/323130392_A_Maximum_Feasible_Subsystem_for_Globally_Optimal_3D_Point_Cloud_Registration)
- 8 < 1% match (Hao Zhang, Zhenyu Li, Pengfei Yan, Xiaoqing Wang, Xingyuan Wang. "A plain-text independent color image encryption system with multi-thread permutation and multi-channel diffusion", International Journal of Modern Physics C, 2021)  
[Hao Zhang, Zhenyu Li, Pengfei Yan, Xiaoqing Wang, Xingyuan Wang, "A plain-text independent color image encryption system with multi-thread permutation and multi-channel diffusion". International Journal of Modern Physics C, 2021](https://www.researchgate.net/publication/358076685)
- 9 < 1% match (Umar Hayat, Naveed Ahmed Azam. "A novel image encryption scheme based on an elliptic curve", Signal Processing, 2019)  
[Umar Hayat, Naveed Ahmed Azam. "A novel image encryption scheme based on an elliptic curve". Signal Processing, 2019](https://www.researchgate.net/publication/358076685)
- 10 < 1% match (Tao Pan, Xiaojun Tong, Miao Zhang, Zhu Wang. "A joint image compression and encryption algorithm based on compression sensing and bit-plane embedding", Physica Scripta, 2022)  
[Tao Pan, Xiaojun Tong, Miao Zhang, Zhu Wang. "A joint image compression and encryption algorithm based on compression sensing and bit-plane embedding". Physica Scripta, 2022](https://www.researchgate.net/publication/358076685)
- 11 < 1% match (Internet from 01-May-2022)