

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Chain rings and Chaotic Systems Computations: Applications to Data Security



By

Tanveer ul Haq

**Department of Mathematics
Quaid-i-Azam University
Islamabad, Pakistan
2021**

Chain rings and Chaotic Systems Computations: Applications to Data Security



by

Tanveer ul Haq

Supervised by

Prof. Dr. Tariq Shah

**Department of Mathematics
Quaid-i-Azam University
Islamabad, Pakistan
2021**

Chain rings and Chaotic Systems Computations: Applications to Data Security



by

Tanveer ul Haq

A THESIS SUBMITTED IN THE PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE

DEGREE OF

DOCTOR OF PHILOSOPHY

IN

MATHEMATICS

Supervised by

Prof. Dr. Tariq Shah

Department of Mathematics

Quaid-i-Azam University

Islamabad, Pakistan

2021

Plagiarism Undertaking

I solemnly declare that research work presented in the thesis titled "**Chain rings and Chaotic Systems Computations: Applications to 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.

Tanveer

Student/Author Signature

Name: **Tanveer ul Haq**

Certificate of Approval

This is to certify that the research work presented in this thesis entitled Chain rings and Chaotic Systems Computations: Applications to Data Security was conducted by Mr. Tanveer ul Haq under the kind supervision of Prof. Dr. Tariq Shah. 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: Tanveer ul Haq

Signature: Tanveer

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: Akbar Azam

b) External Examiner 2:

Name: **Dr. Tahir Mehmood**

Designation: Assistant Professor

Office Address: Department of Mathematics & Statistics, Faculty of Basics Applied Sciences, International Islamic University, Islamabad.

Signature: Tahir Mehmood

c) Internal Examiner

Name: **Dr. Tariq Shah**

Designation: Professor

Office Address: Department of Mathematics, QAU Islamabad.

Signature: Tariq Shah

Supervisor Name:

Prof. Dr. Tariq Shah

Signature: Tariq Shah

Name of Dean/ HOD

Prof. Dr. Sohail Nadeem

Signature: Sohail Nadeem

Chain rings and Chaotic Systems Computations: Applications to Data Security

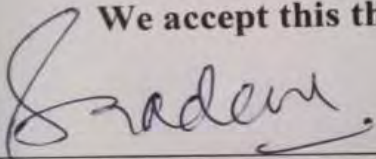
By

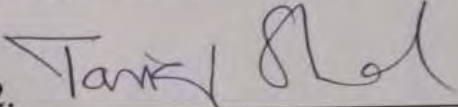
Tanveer ul Haq

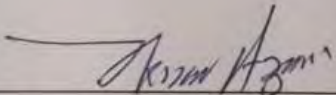
CERTIFICATE

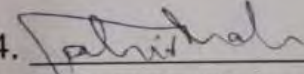
A THESIS SUBMITTED IN THE PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE DEGREE OF THE
DOCTOR OF PHILOSOPHY IN MATHEMATICS

We accept this thesis as conforming to the required standard

1. 
Prof. Dr. Sohail Nadeem
(Chairman)

2. 
Prof. Dr. Tariq Shah
(Supervisor)

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

4. 
Dr. Tahir Mehmood
(External Examiner)

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

Department of Mathematics & Statistics
International Islamic University, Islamabad.

**Department of Mathematics
Quaid-I-Azam University
Islamabad, Pakistan
2021**

Dedicated to

My Parents

Acknowledgment

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 veneration and devotion goes to our beloved **Prophet Muhammad**, peace be upon him, the source of humanity, kindness and guidance for the whole creatures and who declared it an obligatory duty of every Muslim to seek acquire knowledge.

I would like to take this opportunity to express my deepest gratitude to kind-hearted **Prof. Dr. Tariq Shah** who is my first supervisor; for the great opportunity he provided me pursuing a Doctoral degree; for his expertise in the area that has guided me throughout the study; and for his advice, inspiration and constant encouragement to complete this degree.

I extended my thanks to those participants who gave their valuable time, great effort and enthusiasm to participate in the pilot and the main study. They also provided useful comments and insights on the issue studied. Again, my sincere appreciation goes to them for their collective thoughts and experiences.

Furthermore, I wished to express my appreciation to Quaid-i-Azam University, who generously helped me by approving the scholarship to make this Doctoral study possible.

In addition, I also thanks to my Lab fellows and friends; Imran Haider, Dawood Shah, Muzzamil Haneef, Yasir Naseer Satti, Huma Jamil and Kiran Shahzadi for giving there valuable suggestions. Not only these Mathematicians of Quaid-i-Azam University but also I thanks to my friends Muhammad Taimor, Muhammad Abid, Nouman Iqbal , Nabeel Ahmad, Moin Hamid Bukhari, Ferhan khan, Abbas Khan, Shahzad, Arsalan, Ismail Khan from the Department of Statistics who refreshed me during the journey of Ph.D.

My utmost special thanks go to the most important and essential people of my life that is my family for their love, prayers, courage and moral support throughout the study. They are my beloved parents, and my loving brothers and sisters. Thank you for being there for me. Finally, I acknowledged the support from everyone in the Quaid-i-Azam University, Department of Mathematics. Please accept my gratitude, now and always.

Tanveer ul Haq
February 16, 2021

Preface

The purpose of cryptography is to maintain and transmit data in such a manner that it can be read and understood only by authorized recipients. Although it may be known that data is being transmitted, the content of that data should remain secret to unauthorized persons. Any secure encryption scheme contains the basic concepts of cryptography. It may provide integrity and confidentiality: it is essential to note that it will not provide availability explicitly. Authentication and non-repudiation might be given by cryptography. The cryptographic algorithm's anonymity does not have power. It is also proven that hidden algorithms are very weak. Public algorithms such as the Advanced Encryption Standard (AES) and the Triple Data Encryption Standard (TDES) are ciphers that have stood the test of time. In the last few decades, numerous simple cryptographic methods have been exploited in various fields. It is customarily used traditionally by authorities or controlled organizations to conceal confidential messages from adversaries. But once again, every single day, millions of classified and encoded conversations take place electronically. Accordingly, online security issues are growing so exponentially that there has been a need for information security, science and analysis to protect data from potential threats in contact schemes and computers. Cyber-security issues are now growing so exponentially a need for information security, network security and data protection mechanisms from unauthorized parties in computer systems has indeed been noticed. Cryptosystems are used to encrypt documents, photos, videos, banking records, proof of health, and much more. Mathematical thinking and the implementation of computer science are also focused on day-time cryptology and network security activities.

Nowadays most communications are frequently made on computers. As a result of advancements in technology, the transfer rate of digital data through cryptographic embedded devices such as smart cards is increasing rapidly and these devices are vulnerable to attacks. Cryptography provides various algorithms to secure the data. In the beginning (i.e. in the 1960s) of cryptography, secret communication was limited to the government. In the 1970s Horst Feistel (German Cryptographer) created a cipher at IBM called the Feistel cipher. This was the first commercially seen cipher of the cryptographic history seen in 1973. The U.S National Bureau of Standards (NBS), now call the National Institute of Standards and Technology (NIST), published a symmetric cipher in 1977 based on the Feistel cipher called the Data Encryption Standard (DES). It was considered to be highly secure and as a standard up to the end of the 20th century. In 1997 NIST call for ciphers, because of

the theoretical and exhaustive key search attacks on DES. In June 1998 fifteen candidates were accepted and after shortlisting in aug-1999, five were chosen. The shortlist includes; Rijndael Algorithm [1], RC6 algorithm [2], Serpent Algorithm [3], MARS algorithm [4] and Twofish algorithm [5].

To improve the complexity in S-boxes, the structure of Galois field is replaced by a more generalized structure of Galois ring. Firstly, Galois ring gets importance in coding theory in 1979 when Shankar [3] constructs the BCH codes over local ring \mathbb{Z}_p^k . Likewise; the BCH codes over finite unitary commutative rings are assembled by Andrade and Palazzo [7] in 1998. These constructions are equally focused on the maximal cyclic subgroup of the group of units of a Galois ring extension of a local ring. In this upshot, Shah et al. [8, 9] spread the work contained in [7] to a sequence of BCH codes over an ascending chain of finite Galois rings. For this purpose chain of the maximal cyclic subgroups of the chain of groups of units is considered. These assemblies are often generated on Galois fields with characteristic 2, hence there is a need of improvements and reforms in algebraic structures. To increase the complexity of S-boxes, the structure of Galois field is replaced with a more generic structure called the Galois ring. In 1997, when Shankar [3] constructs the BCH codes over local ring \mathbb{Z}_p^k , the Galois ring get its importance in coding theory. Similarly, Andrade and Palazzo [7] assembled the BCH codes over finite commutative rings with unit elements in 1998. The maximum cyclic subgroup of the group of units of a Galois ring extension of a local ring is similarly based on these constructions. In this context, Shah et al. [8, 9] extended the work found in [7] over an ascending chain of finite Galois rings to a sequence of BCH codes. The chain of the maximal cyclic subgroups of the chain of groups of units is considered for this reason.

A generalize structure of the sequence alphabet to a residue class polynomial ring over Galois field (GF) is given in [10]. According to [10], if $w(x)^k$, for $k > 1$, be the k^{th} power of an irreducible polynomial $w(x)$ over GF of degree m . Then, the residue class ring R is defined as $R = \frac{\mathbb{F}_2[x]}{\langle w(x)^k \rangle}$. This generalization provides a large choice of rings to construct frequency hopping sequences. These rings are called commutative chain rings. The ring $R_n = \frac{\mathbb{F}_2[x]}{\langle x^n \rangle}$ is a special case of R where $w(x) = x$ and $k = n$. An application of such rings is given in the construction of cyclic codes and Self-Dual codes in [11]. A cyclic code C of length m over R is a linear code with the property that if $c \in C$, the each rotation of bits of c will also yields to an element of C . Thus, if we consider the codewords to be

polynomials then the cyclic codes are ideal in the ring $R = \frac{\mathbb{F}_2[x]}{\langle w(x)^k \rangle}$. Furthermore, the design of byte based 4×4 S-box from finite commutative chain ring $R_8 = \frac{\mathbb{F}_2[x]}{\langle x^8 \rangle}$ is initiated by Shah et al. [12]. Here, in [12], the bit size of each entry in the S-boxes is greater than the size of the S-box (further explained in section 1.3) and is recently used in [13] (explained in chapter 5) for image encryption application.

The Rijndael algorithm (Advanced Encryption Standard-AES), is considered to be the most secure and fast text encryption tool. However, it fails to be a digital image encryption instrument, due to its worst time complexity, as compared to chaos (non-linear dynamical system) and S-box based image encryption schemes. On the other hands, the second competitor for the Advanced Encryption Standard, i.e., Serpent Algorithm is more secure than the Rijndael algorithm. But the time inferiority of the Serpent algorithm makes the Rijndael algorithm superior. For Serpent algorithm, initially, S-boxes were taken from the data encryption standard (DES) that resulted in Serpent-0 algorithm [3], a more secure Algorithm than triple-DES [14] having a key size of length 192 or 256 bits, presented at the 5th international workshop on Fast Software Encryption. After this, Serpent-1 [3] was designed which used new and stronger S-boxes with a different key schedule to resist different attacks like differential [15] and linear [16] techniques. Copious image encryption schemes based on the Rijndael algorithm and Serpent algorithm have been introduced by cryptographers [17-18]. However, in this thesis, a novel idea to improve Serpent algorithm by using elements of finite commutative chain ring $R_8 = \frac{\mathbb{F}_2[x]}{\langle x^8 \rangle}$ has been established. And then its application is investigated in RGB image encryption. The results of the encryption scheme ensure the security of the improved Serpent algorithm against different attacks like differential attack, brute force attack, etc. Moreover, the time analysis of displays the improvements in this newly introduced improved Serpent algorithm.

Furthermore, in this thesis, S-boxes of different sizes from multiple elements of the group of units of the finite commutative chain rings $\frac{\mathbb{F}_2[x]}{\langle x^{12} \rangle}$ and $\frac{\mathbb{F}_2[x]}{\langle x^{24} \rangle}$ are constructed. Therefore, it shows powerful algebraic complexity and has excellent properties of resisting all the well-known attacks. The size of these S-boxes are 12×12 and 24×24 . Whereas, a typical 8×8 S-box over Galois field $GF(2^8)$ has 2^8 8-bit strings and thus requires a storing memory of 8×2^8 bits. In continuation, a 12×12 S-box over Galois field $GF(2^{12})$ requires 12×2^{12} bits which is computer memory consuming. Thus, for the construction of 12×12 and 24×24 S-boxes, a method is realized through the multiplicative

group of units of chain rings $\frac{\mathbb{F}_2[x]}{\langle x^{12} \rangle}$ and $\frac{\mathbb{F}_2[x]}{\langle x^{24} \rangle}$, respectively. Using these schemes the computer memory occupies just 12×2^8 and 24×2^8 bits memory respectively, i.e., one and half times the memory occupied by a Galois field dependent S-boxes having input and out output bits of lengths 12 and 24. The existing literature on block ciphers of symmetric key cryptography are mainly depends on Galois fields of characteristic 2. However, some novel contributions on the area focusing on some other finite algebraic structures of Galois ring and finite group theory. The similarity of these structures with the Galois group is their single generating elements While, in many of the cases the most portion of the algorithms the XOR operations are also in compromising mod. Extraordinarily, in this work the structure of finite chain ring is considered, which is canonically an algebra over the binary field \mathbb{F}_2 . Thus here it is not only settled the XOR operation but also it created superfluous complexity due to non-cyclic subgroups of the chain ring.

The utility of the proposed S-boxes is given in digital image enciphering schemes. In case of 12×12 S-box, each 12-bit entry is extended to 24-bit by Exclusive-or i^{th} entry with $(i^{th} + 1) \bmod 257$ entry; for $i = 1$ to 256. Then the 24-bit extended table is split up into 3 8-bit vectors tables so that it fits Red (R), Green (G), and Blue (B) layer of color image pixels. Moreover, in case of 24×24 S-box, the different channels of color image are concatenated to for 24-bit matrix and then apply the 24×24 S-box to color digital medium. Here, addition coincides with the addition operation of Galois field \mathbb{F}_{2^k} and multiplication with local ring \mathbb{Z}_{2^k} to acquire the encrypted image.

Chaos means disorder. Nowadays, the notion of chaos and DNA plays a prominent role in application point of view in different fields like Physics, Biology, Engineering and technology etc. the 1D Chaotic maps get fame because of its simplicity, high randomness and high sensitivity to initial conditions. They are used to create diffusion in data. The only drawback of this concept is its low non-linear behavior. However, in parallel, there are many positive aspects like ergodicity, mixing, highly sensitive dependence on initial conditions and management parameter, unpredictability, random-like behavior of output etc., that are analogous to the confusion and diffusion properties of Claude Shannon [6] which strengthen the concept of Chaos and DNA based encryption methodologies. As there are many advantages of chaotic maps, hence they are used here in parallel with chain ring S-boxes to increase the security of a data encryption process.

The continuation of the study is formulated as follows: the overview on cryptography and algebra structure is given in Chapter 1. In chapter 2, the algebraic cipher for the creating chain ring $\frac{\mathbb{F}_2[x]}{\langle x^{12} \rangle}$ dependent 12×12 S-box and its application to color image is given. Chapter 3 consists of a new 12×12 S-box design over chain ring with a novel image encryption scheme. Chapter 4 extends the idea to 24×24 S-box construction and its application to the color digital images. The application of 4×4 S-box obtained from elements of commutative chain ring $\frac{\mathbb{F}_2[x]}{\langle x^8 \rangle}$ to SERPENT algorithm is given in chapter 5. Accordingly a successful image encryption scheme on SERPENT algorithm is also included in chapter 5. The analyses of the proposed encryption algorithms (Chapters 2-5) are given in chapter 6. Chapter 7 includes the concluding remarks and indicates some future directions for further extensions of the ideas developed in this work.

Research Profile

Published work related to this thesis

1. ul Haq, T., & Shah, T. (2020). 12×12 S-box Design and its Application to RGB Image Encryption. *Optik*, 164922. **DOI:**10.1016/j.ijleo.2020.164922
2. 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. **DOI.org**/10.1016/j.jisa.2020.102592
3. Shah, T., Haq, T. U., & Farooq, G. (2020). Improved SERPENT Algorithm: Design to RGB Image Encryption Implementation. *IEEE Access*, 8, 52609-52621. **DOI:** 10.1109/ACCESS.2020.2978083

Conference publications

1. Shah, T., ul Haq, T., & Farooq, G. (2018, September). Serpent Algorithm: An Improvement by 4×4 S-Box from Finite Chain ring. In 2018 International Conference on Applied and Engineering Mathematics (ICAEM) (pp. 1-6). IEEE. **DOI:** 10.1109/ICAEM.2018.8536293
2. Shah, D., ul Haq, T., & Shah, T., "Image Encryption Based on Action of Projective General Linear Group on a Galois Field $GF(2^8)$," 2018 International Conference on Applied and Engineering Mathematics (ICAEM), Taxila, 2018, pp. 38-41, **DOI:** 10.1109/ICAEM.2018.8536281

List of abbreviations.....	4
List of Tables.....	5
List of Figures.....	7

Table of Contents

1 Overview on cryptography and algebraic notion of classes of finite rings	10
1.1 Cryptography: An overview.....	10
1.1.1 Historic background	10
1.1.2 Modern symmetric key ciphers	12
1.1.3 Chaos and DNA based crypto-algorithms	14
1.2 Finite commutative rings with identity	16
1.2.1 Rings.....	16
1.2.2 Ideal	19
1.2.3 Quotient rings	20
1.2.4 Galois field extension	21
1.2.5 Algebra of Galois field extension and its matrix algebra representation	24
1.2.6 Galois ring	27
1.2.7 Finite commutative chain ring.....	33
1.3 S-box based over chain ring.....	36
1.4 Motivation and objectives of this thesis.....	38
2 Design of 12-bit S-box over chain ring and its application to digital images	41
2.1 Construction of S-box over chain ring	41
2.2 Multiplicative group of chain ring	42
2.3 Algorithm for S-box construction	42
2.4 12-bit chain ring dependent RGB image encryption.....	43
2.4.1 Encryption algorithm.....	44
2.4.2 Decryption algorithm.....	46
3 Chain ring-chaos amalgam and DNA transform: A functionality in multiple image encryption	47
3.1 Generation of random sequences using chaos and chain ring-based S-box.....	48
3.2 S-box construction algorithm using 12-bit chain ring.....	48
3.3 1D mixed chaotic map.....	49
3.4 Proposed multiple image encryption.....	52

4	Design of 24-bit replacement-matrix over chain ring: An encryption application to astronomical visual	55
4.1	24-by-24-replacement-matrix generation over chain ring	56
4.1.1	Multiplicative group of chain ring.....	56
4.1.2	Construction of S-box.....	56
4.2	24-bit chain ring dependent astronomical RGB image encryption	58
4.2.1	Encryption algorithm.....	58
4.2.2	Decryption algorithm.....	59
5	Chain ring based improved SERPENT algorithm: A digital image encryption implementation.....	61
5.1	Improved SERPENT algorithm	61
5.1.1	Key structure.....	62
5.1.2	Linear transformation	63
5.2	Digital image encryption scheme using improved SERPENT algorithm	63
6	Strength determination of newly introduced data security algorithms.....	66
6.1	Statistical analysis	66
6.1.1	Key-space analysis	67
6.1.2	Histogram analysis	67
6.1.3	Intensity histogram analysis	74
6.1.4	Correlation analysis	78
6.2	Noise analysis.....	85
6.2.1	Salt and Pepper analysis	85
6.2.2	Speckle noise	89
6.2.3	Shot noise/Poisson noise	92
6.3	Occluded attack.....	94
6.4	Differential analyses.....	96
6.4.1	Number of pixels change rate (NPCR).....	96
6.4.2	UACI	96
6.5	Texture analysis of the proposed scheme for encryption.....	97
6.5.1	Contrast.....	97
6.5.2	Energy.....	98
6.5.3	Homogeneity	98
6.5.4	Entropy	99

6.6 Analysis on experimental work.....	99
6.6.1 MSE	100
6.6.2 PSNR	100
6.6.3 Cross correlation (Normalized), NK	100
6.6.4 Average difference (AD).....	100
6.6.5 Structural content (SC).....	101
6.6.6 Maximum difference (MD)	101
6.6.7 Absolute error (Normalized), NAE	101
6.6.8 Root mean square error.....	101
6.6.9 Universal quality index (UQI).....	102
6.6.10 Mutual information (MI)	102
6.6.11 Structural similarity (SSIM).....	102
6.7 Randomness test for cipher	104
7 Conclusion	109
References	111
Index.....	119

List of abbreviations

$(R, +, \cdot)$	Ring with binary operations $+$ and \cdot
I	Ideal
$\langle a_1, a_2, \dots, a_n \rangle$	Ideal generated by the elements a_1, a_2, \dots, a_n of the unitary commutative ring R
$\langle a \rangle$	Principal ideal generated by the element a of the unitary commutative ring R
\mathcal{M}	Maximal Ideal
P	Prime ideal
\mathbb{N}	Multiplicative monoid of natural numbers
\mathbb{Z}	Ring of rational integers
\mathbb{R}	Field of real numbers
\mathbb{C}	Field of complex numbers
\mathbb{Z}_n	Ring of integers modulo n having characteristic n
\mathbb{Z}_{p^s}	The local ring of integers modulo p^s having characteristic p^s (p is a prime and $s \in \mathbb{N}$)
S_n	Symmetric group on n objects
$R[x]$	Polynomial ring in the indeterminate x and coefficients from the ring R
$F[x]$	Polynomial ring in the indeterminate x and coefficients from the field F , the Euclidean domain
\mathbb{Z}_p	Field of integers modulo p having characteristic the prime p
$GF(p^m) = \mathbb{F}_{p^m}$	Galois field of characteristic p with p^m elements (p is a prime and $m \in \mathbb{N}$) ($\mathbb{Z}_p = GF(p^1)$)
$GR(p^s, m)$	Galois ring of characteristic p^s with p^{sm} elements (p is a prime and $s, m \in \mathbb{N}$)
$GF(p^m)[x]$	Polynomial ring in the indeterminate x and coefficients from $GF(p^m)$
$GR(p^s, m)[x]$	Polynomial ring in the indeterminate x and coefficients from $GR(p^s, m)$
$\mathcal{R}_n = \frac{\mathbb{F}_2[x]}{\langle x^n \rangle}$	Finite chain ring having elements in n - binary bits form
S-box	Substitution box
RGB	Red, Green and Blue layers of a color image

List of Tables

Table 1. DNA encoding rule	14
Table 2. Addition in $\frac{\mathbb{Z}_2[x]}{\langle x^2 \rangle}$	31
Table 3. Multiplication in $\frac{\mathbb{Z}_2[x]}{\langle x^2 \rangle}$	31
Table 4. Addition in $\frac{\mathbb{Z}_2[x]}{\langle x+x^2 \rangle}$	32
Table 5. Multiplication in $\frac{\mathbb{Z}_2[x]}{\langle x+x^2 \rangle}$	32
Table 6. Addition in $\frac{\mathbb{Z}_2[x]}{\langle x+x^3 \rangle}$	32
Table 7. Multiplication in $\frac{\mathbb{Z}_2[x]}{\langle x+x^3 \rangle}$	32
Table 8. Addition in $\mathbb{F}_2 + u\mathbb{F}_2$	38
Table 9. Multiplication in $\mathbb{F}_2 + u\mathbb{F}_2$	38
Table 10. Multiplicative Group $M_{G_{12}}$ of units of Chain ring R_{12}	42
Table 11. S-box obtained from Multiplicative Group $M_{G_{12}}$ of units of Chain ring R_{12}	43
Table 12. proposed S-box obtained from the elements of multiplicative group of commutative chain ring	49
Table 13. Triplet T_1	51
Table 14. Triplet T_2	51
Table 15. Triplet T_3	51
Table 16. Chain ring R_{24} multiplicative Group $M_{G_{24}}$	57
Table 17. S-box generated from Multiplicative Group $M_{G_{24}}$ of units of Chain ring R_{24}	57
Table 18. Correlation of Lena Original and Encrypted Image using 12-bit S-box	78
Table 19. Correlation of Fruits Original and Encrypted Image	79
Table 20. Multiple's image Correlation using Algebra-Chaos Amalgam and DNA Transform	80
Table 21. Lena image Correlation using Algebra-Chaos Amalgam and DNA Transform	80
Table 22. Baboon's image Correlation using Algebra-Chaos Amalgam and DNA Transform	80
Table 23. Fruits image Correlation using Algebra-Chaos Amalgam and DNA Transform	80
Table 24. Aeroplane's image Correlation using Algebra-Chaos Amalgam and DNA Transform	80
Table 25. Lena Original and Encrypted Image correlation using Improved SERPENT Algorithm	82
Table 26. Baboon Original and Encrypted Image correlation using Improved SERPENT Algorithm	82
Table 27. Earth's image correlation using 24-bit S-box	83
Table 28. Sun Original and encrypted image Correlation using 24-bit S-box	83
Table 29. Differential analyses for $\frac{\mathbb{F}_2[x]}{\langle x^{12} \rangle}$ Dependent color images techniques	97
Table 30. Second order texture analyses for given and enciphered images	98
Table 31. Comparing entropy for proposed schemes with existing schemes	99
Table 32. Image quality measures for encrypted image (Lena.jpg) resulting from chapter 2	103
Table 33. Quality measures analysis for encrypted image (Lena.jpg) resulting from chapter 2	103
Table 34. Image Quality Measures for $\frac{\mathbb{F}_2[x]}{\langle x^{24} \rangle}$ Dependent encrypted Astronomical Images	103
Table 35. Image quality measures for RGB image (Lena.jpg) resulting from chapter 5	104
Table 36. NIST test results for 12×12 S-box Dependent RGB Image Encryption	105
Table 37. NIST test results for Algebra-Chaos Amalgam and DNA Transform encrypted multiple Image	106
Table 38. NIST test results for 24-by-24-replacement-matrix dependent Image Encryption	107
Table 39. NIST test results for improved SERPENT algorithm dependent RGB Lena encrypted	108

List of Figures

Figure 1. Link diagram of the whole thesis	40
Figure 2. Flow chart of 12×12 S-box dependent color image encryption	45
Figure 3. Lena and fruits original images and there corresponding ciphered images	46
Figure 4. (a) and (b) are the bifurcation and Lyapunov exponent diagram (resp.) of 1D mixed logistic map. ..	50
Figure 5. RGB multiple image encryption scheme using Algebraic-Chaotic Triplet and DNA sequences	53
Figure 6. Lena, Baboon, Fruits and Aeroplane original images and there corresponding encrypted images....	54
Figure 7. RGB image encryption scheme using the proposed 24×24 S-box.....	60
Figure 8. Earth, Stars, Moon and Sun original image and there corresponding ciphered images	60
Figure 9. RGB image encryption scheme using chain ring-based SERPENT algorithm.....	64
Figure 10. Lena, Baboon, Fruits and Aeroplane original images and there corresponding encrypted images..	65
Figure 11. (a) and (e) are original and encrypted multiple image respectively. Histogram pins in (b) and (f) represents Red Channel of (a) and (e) respectively. Similarly, (c), (d) and (g), (h) shows the histogram pins of green and blue layers of original and encrypted multiple image respectively.....	68
Figure 12. (a) and (e) are original and encrypted color Lena image respectively. Histogram pins in (b) and (f) represents Red Channel of (a) and (e) respectively. Similarly, (c), (d) and (g), (h) shows the histogram pins of green channel and blue channel of original and encrypted Lena image respectively.	68
Figure 13. (a) and (e) are original and encrypted color Baboon image respectively. Histogram pins in (b) and (f) represents Red Channel of (a) and (e) respectively. Similarly, (c), (d) and (g), (h) shows the histogram pins of green and blue layers of original and encrypted Baboon image respectively.	69
Figure 14. (a) and (e) are original and encrypted color Fruits image respectively. Histogram pins in (b) and (f) represents Red Channel of (a) and (e) respectively. Similarly, (c), (d) and (g), (h) shows the histogram pins of green and blue layers of original and encrypted Fruits image respectively.	69
Figure 15. (a) and (e) are original and encrypted color Aeroplane image respectively. Histogram pins in (b) and (f) represents Red Channel of (a) and (e) respectively. Similarly, (c), (d) and (g), (h) shows the histogram pins of green and blue layers of original and encrypted Aeroplane image respectively.	69
Figure 16. (a) is Lena Original Image. (b),(c),(d) are its corresponding Red, Green and Blue layers. (e), (f), (g), and (h) are the 3D histograms of (a), (b), (c) and (d) respectively. (i) is Lena Encrypted Image where (j), (k) and (l) are its Red, Green and Blue layers respectively. (m), (n), (o) and (p) are the 3D histograms of (i), (j), (k) and (l) respectively.....	70
Figure 17. (a) is Fruits Original Image. (b),(c),(d) are its corresponding Red, Green and Blue layers. (e), (f), (g), and (h) are the 3D histograms of (a), (b), (c) and (d) respectively. (i) is Fruits Encrypted Image where (j), (k) and (l) are its Red, Green and Blue layers respectively. (m), (n), (o) and (p) are the 3D histograms of (i), (j), (k) and (l) respectively.....	71
Figure 18. (b), (c) and (d) shows the histogram pins of Red Green and Blue layers of the original Lena color image. (f), (g) and (h) represent the histogram pins of Red Green and Blue layers of the encrypted Lena RGB image. (j), (k) and (l) represent the histogram pins of Red Green and Blue layers of the decrypted Lena RGB image.....	72
Figure 19. (b), (c) and (d) shows the histogram pins of Red Green and Blue layers of the original Baboon color image. (f), (g) and (h) represent the histogram pins of Red Green and Blue layers of the encrypted Baboon RGB image. (j), (k) and (l) represent the histogram pins of Red Green and Blue layers of the decrypted Baboon RGB image.....	72
Figure 20. Earth image and its Red, Green, Blue channels are shown in (a), (b), (c), (d) respectively. Their corresponding 3D histograms are shown in (e), (f), (g), (h). Similarly, Earth ciphered image and its red, green,	

blue channels are given in (i), (j), (k) and (l). Their corresponding 3D histograms are given in (m), (n), (o) and (p) respectively.....	73
Figure 21. Stars image and its Red, Green, Blue channels are shown in (a), (b), (c), (d) respectively. Their corresponding 3D histograms are shown in (e), (f), (g), (h). Similarly, Stars ciphered image and its red, green, blue channels are given in (i), (j), (k) and (l). Their corresponding 3D histograms are given in (m), (n), (o) and (p) respectively.....	74
Figure 22. Subfigure (a) and (e) are Intensity histogram pins original and ciphered Multiple image respectively. Intensity histogram pins of original multiple RGB image layers are given in (b), (c) & (d) respectively. Similarly, that of encrypted image is in (f), (g) & (h) respectively.	75
Figure 23. Subfigure (a) and (e) are Intensity histogram pins original and ciphered Lena image respectively. Intensity histogram pins of Lena RGB image layers are given in (b), (c) & (d) respectively. Similarly, that of encrypted image is in (f), (g) & (h) respectively.....	75
Figure 24. Subfigure (a) and (e) are Intensity histogram pins original and ciphered Baboon image respectively. Intensity histogram pins of Baboon RGB image layers are given in (b), (c) & (d) respectively. Similarly, that of encrypted image is in (f), (g) & (h) respectively.....	75
Figure 25. Subfigure (a) and (e) are Intensity histogram pins original and ciphered Fruits image respectively. Intensity histogram pins of Fruits RGB image layers are given in (b), (c) & (d) respectively. Similarly, that of encrypted image is in (f), (g) & (h) respectively.....	75
Figure 26. Subfigure (a) and (e) are Intensity histogram pins original and ciphered Aeroplane image respectively. Intensity histogram pins of Aeroplane RGB image layers are given in (b), (c) & (d) respectively. Similarly, that of encrypted image is in (f), (g) & (h) respectively.	76
Figure 27. 3D intensity histogram of Lena image having size 256×256 . (a) and (e) presents 3D intensity histogram of Lena original and encrypted image respectively. (b), (c) and (d) are 3D intensity histogram of RGB layers (respectively) of Lena original image. (f), (g) and (h) are 3D intensity histograms of RGB layers (respectively) of Lena encrypted image.....	76
Figure 28. 3D intensity histogram of Fruits image having size 256×256 . (a) and (e) presents 3D intensity histogram of Fruits original and encrypted image respectively. (b), (c) and (d) are 3D intensity histogram of RGB layers (respectively) of Fruits original image. (f), (g) and (h) are 3D intensity histograms of RGB layers (respectively) of Fruits encrypted image.	76
Figure 29. Subfigure (a) and (e) are Intensity histogram pins original and ciphered Lena image respectively. Intensity histogram pins of Lena RGB image layers are given in (b), (c) & (d) respectively. Similarly, that of encrypted image is in (f), (g) & (h) respectively.....	77
Figure 30. Subfigure (a) and (e) are Intensity histogram pins original and ciphered Baboon image respectively. Intensity histogram pins of Baboon RGB image layers are given in (b), (c) & (d) respectively. Similarly, that of encrypted image is in (f), (g) & (h) respectively.....	77
Figure 31. Earth Original image and its red, green and blue layers 3D intensity histogram are given in (a), (b), (c) and (d) respectively. Whereas, Earth enciphered image and its red, green and blue layers intensity histogram are given in (e), (f), (g) and (h) respectively.....	77
Figure 32. Sun Original image and its red, green and blue layers 3D intensity histogram are given in (a), (b), (c) and (d) respectively. Whereas, Sun enciphered image and its red, green and blue layers intensity histogram are given in (e), (f), (g) and (h) respectively.....	77
Figure 33. (H) (a-f): (Horizontal) Correlation of pixels for original and encrypted 256×256 Lena image	78
Figure 34. (V) (a-f): (Vertical) Correlation of pixels for original and encrypted 256×256 Lena image.....	79
Figure 35. (D) (a-f): (Diagonal) Correlation of pixels for original and encrypted 256×256 Lena image.....	79

Figure 36. Original multiple image Red, Green and Blue layers Horizontal correlation are shown by (a), (b), (c) respectively. Whereas, that of encrypted are shown in (d), (e), (f) respectively.	81
Figure 37. Original multiple image Red, Green and Blue layers vertical correlation are shown by (a), (b), (c) respectively. Whereas, that of encrypted are shown in (d), (e), (f) respectively.	81
Figure 38. Original multiple image Red, Green and Blue layers diagonal correlation are shown by (a), (b), (c) respectively. Whereas, that of encrypted are shown in (d), (e), (f) respectively	81
Figure 39. (a), (b), (c) represents Horizontal correlation of RGB layers of Lena Original image and (d), (e), (f) are the horizontal correlation of RGB layers of encrypted Lena image.	82
Figure 40. (a), (b), (c) represents Vertical correlation of RGB layers of Original Lena image and (d), (e), (f) are the Vertical correlation of RGB layers of encrypted Lena image.....	83
Figure 41. (a), (b), (c) represents Diagonal correlation of RGB layers of Original Lena image and (d), (e), (f) are the Diagonal correlation of RGB layers of encrypted Lena image.....	83
Figure 42. (a), (b), (c) show horizontal Correlation of pixels of Earth image and (d), (e), (f) show Vertical Correlation of pixels of Earth ciphered image	84
Figure 43. (a), (b), (c) show Vertical Correlation of pixels of Earth image and (d), (e), (f) show Vertical Correlation of pixels of Earth ciphered image	84
Figure 44. (a), (b), (c) show diagonal Correlation of pixels of Earth image and (d), (e), (f) show diagonal Correlation of pixels of Earth ciphered image	84
Figure 45. (a), (b), (c) show horizontal Correlation of pixels of Sun image and (d), (e), (f) show horizontal Correlation of pixels of Sun ciphered image.....	84
Figure 46. (a), (b), (c) show vertical Correlation of pixels of Sun image and (d), (e), (f) show vertical Correlation of pixels of Sun ciphered image	85
Figure 47. (a), (b), (c) show diagonal Correlation of pixels of Sun image and (d), (e), (f) show diagonal Correlation of pixels of Sun ciphered image.....	85
Figure 48. (a), (b) and (c) shows the encrypted images of color Lena image with minimum, default and maximum salt & pepper noise. (d), (e) and (f) shows the decrypted images of color Lena image with minimum, default and maximum salt & pepper noise.....	86
Figure 49. (a), (b) and (c) shows the encrypted images of color Fruits image with minimum, default and maximum salt & pepper noise. (d), (e) and (f) shows the decrypted images of color Fruits image with minimum, default and maximum salt & pepper noise.....	86
Figure 50. (a), (b) and (c) represent encrypted images containing Salt and Pepper noise whereas (d), (e) and (f) are there decrypted images respectively.....	87
Figure 51. Column 1-3 represent small, default and maximum noisy encrypted image of Lena, Baboon, Fruits and Aeroplane respectively. The corresponding decrypted images are shown in column 4-6.....	88
Figure 52. Earth enciphered images are given in (a), (b) and (c) with small, default and large salt & pepper noise. Earth deciphered images are given in (d), (e) and (f) with small, default and large salt & pepper noise.	89
Figure 53. (a), (b) and (c) shows the encrypted images of color Lena image with minimum, default and maximum Speckle noise. (d), (e) and (f) shows the decrypted images of color Lena image with minimum, default and maximum Speckle noise.	90
Figure 54. (a), (b) and (c) shows the encrypted images of color Fruits image with minimum, default and maximum Speckle noise. (d), (e) and (f) shows the decrypted images of color Fruits image with minimum, default and maximum Speckle noise.	90

Figure 55. (a), (b) and (c) represent encrypted images containing Speckle noise whereas (d), (e) and (f) are there decrypted images respectively..... 91

Figure 56. Earth enciphered images are given in (a), (b) and (c) with small, default and large Speckle noise. Earth deciphered images are given in (d), (e) and (f) with small, default and large Speckle noise..... 92

Figure 57. (a) and (b) shows the encrypted images of color Lena and color Fruits image with Poisson noise respectively. (c) and (d) represents the decrypted images (a) and (b) respectively. 93

Figure 58. (a), (b), (c) and (d) represent encrypted images containing Poisson noise whereas, (e), (f), (g) and (h) are there decrypted images respectively..... 93

Figure 59. Earth enciphered digital image with Photon noise is given in (a) and its corresponding deciphered Earth image is given in (b)..... 94

Figure 60. (a), (b), (c) and (d) shows the encrypted images of color Lena image with 25% occluded from above, left, bottom and right respectively. (e), (f), (g) and (h) shows the decrypted images of (a), (b), (c) and (d) respectively..... 95

Figure 61. (a), (b), (c) and (d) shows the encrypted images of color Lena image with 50% occluded from top, bottom right and left respectively. (e), (f), (g) and (h) shows the decrypted images of (a), (b), (c) and (d) respectively..... 95

Figure 62. (a) and (b) shows the encrypted images of color Lena image occluded from center. (c) and (d) are upper triangular and lower triangular occluded respectively. (e), (f), (g) and (h) shows the decrypted images of (a), (b), (c) and (d) respectively..... 95

Chapter 1

Overview on cryptography and algebraic notion of classes of finite rings

The theory of rings is mainly divided into the classes of non-associative rings and associative rings. Though, the associative class is further divided into commutative and non-commutative rings. Our main focus in this work is on the structure of associative commutative rings having an identity, particularly the finite commutative rings with identity. This chapter includes some elementary topics in commutative ring theory, and it is dedicated to finite local rings. The chain rings being a class of local rings are the main subject of this work. The fundamental concepts on local rings in the form of definitions, remarks, notes, lemmas, propositions, and theorems in this chapter are taken from [19, 20, 21, 22, 23]. All these are discussed in the second phase of this chapter. The main goal of this research is on developing the cryptographic algorithms for block ciphers of symmetric key cryptography. Conventionally the confusion part, the main area, of the block cipher encryption algorithm depends on the algebraic structure of finite cyclic Galois group. However, in most recent literature other than finite cyclic Galois group some other finite group structures are also used in the construction of block ciphers but these structures are also of cyclic nature. Despite the cyclic behavior the finite chain rings are the main source of generating non-cyclic subgroups. This chapter starts with basic ideas and different practicing block ciphers used in symmetric key cryptography.

1.1 Cryptography: An overview

1.1.1 Historic background

Cryptography is often referred to as the art of secret writing. The word, cryptography, is taken from the Greek words: *kryptos* meaning “secret” and *graphein* meaning “writing”. Historically, it was widely used in the military to share secret signals in ways that the enemies could not understand even if they capture the signals. Before 1970, cryptography was preserved to the military and government. In WWII Japan used the best non-scientific cryptographic tools; the Enigma and the naval code respectively; to understand opponent’s conversations. But with the passage of time and the creation of public ciphers cryptography also got its fame in public. In this digital era, individual’s interactions of personal and confidential information over the internet are at high risk. Therefore, modern cryptography comes to make a confidential data transfer between authorized persons. It not only

secures the websites but also ensures safe electronic transmission and transactions. Cryptology is the field of creating and solving codes. Cryptography and cryptanalysis are the two branches of cryptology. *Cryptanalysis* is the art of finding access to secret information without knowing the key. With the help of efficient cryptanalysis, security breaches in algorithms can be identified and hacks. Modern ciphers are extensively cryptanalyzed before bringing it for public use to ensure their maximum security. Cyber vulnerabilities are created when insufficient attention is paid to the security of software applications.

Mathematics is playing a major role to develop strong cryptographic algorithms. These algorithms are designed around computational hardness assumptions which become infeasible to break by any known practical means. Prime factorization, modular arithmetic, maximum distance separable (MDS) and other special codes of coding theory, algebraic structures like finite fields, Galois rings and chain rings are used pervasively in designing strong cryptosystems against various attacks. Following are the key terminologies associated with cryptography.

The understandable information that is to be conveyed to the receiving end is called the *plaintext*. The random, distorted and non-meaningful text which is delivered to the receiver is termed *ciphertext*. The set of characters that is used to alter the information to the ciphered text and back to plain text is called a *key*. The process of converting meaningful information into understandable data by using a certain procedure and a key is known as *encryption*. Whereas, *decryption* is the process of getting back the original information by following a certain procedure and a key. *Cipher* is an algorithm based on a set of mathematical procedures and is used to perform encryption or decryption. Claude Shannon in his report “The mathematical theory of cryptography” introduced two major characteristics of a secure cipher [24]. The first one is the *Confusion*, which points out the interrelationship between the plain text and the key wise; i.e. a single character of a plaintext should depend on many components of a given key. The second is *diffusion*, which creates a drastic change in cipher text even on the slightest change of plaintext. This behavior is often known as “*Avalanche effect*”. Theoretically, it implies that on changing the *i*-th bit of plain text, the probability of the *j*-th bit to get affected is one half.

Cryptography is sub-divided into two categories. The *secret key cryptography* uses only one key throughout the entire process of enciphering and deciphering. It is also referred to as private or secret key cryptography. The rijndael algorithm is considered to be one of the finest secret key ciphers. Other famous symmetric ciphers are: DES; Triple DES; RC6; Blowfish; Twofish; and Serpent. The

second category is *asymmetric key cryptography*. In this technique, a key pair is used by each user to encrypt and decrypt data. One key is made public and is distributed over the network so that anyone who intends to encrypt the message can use this key. The RSA is one of the most popular examples of asymmetric algorithms; others in the list are DSA, PKCs and elliptic curve techniques, etc.

1.1.2 Modern symmetric key ciphers

Symmetric or conventional algorithms are those algorithms where the encryption key can be computed from the decryption key and vice versa. In most symmetric algorithms, the encryption key and the decryption key are the same. These algorithms, also called secret-key algorithms, single-key algorithms, or one-key algorithms, require that before communication both the sender and receiver agree on a key. Symmetric algorithm's protection depends on the key; revealing the key means that messages can be encrypted and decrypted by anyone. The key must remain secret for as long as contact needs to remain secret. The symmetric key encryption uses is further divided into two categories namely; the stream ciphers and block cipher.

I. Stream ciphers

A standard stream cipher encrypts plaintext one byte at a time, although it is possible to construct a stream cipher to work on one bit at a time or on units larger than one byte at a time. A key in this structure is input to a pseudorandom bit generator that generates a stream of seemingly random 8-bit numbers. The generator's output, called a keystream, is combined with the plaintext stream one byte at a time using the bitwise exclusive-OR (XOR) operation. For example, if the next byte generated by the generator is 01101100 and the next plaintext byte is 11001100, then the resulting cipher text byte is:

$$\begin{array}{r}
 11001100 \text{ plaintext} \\
 \oplus \quad \underline{01101100} \text{ key stream} \\
 \hline
 10100000 \text{ ciphertext}
 \end{array}$$

Decryption requires the use of the same pseudorandom sequence:

$$\begin{array}{r}
 10100000 \text{ ciphertext} \\
 \oplus \quad \underline{01101100} \text{ key stream} \\
 \hline
 11001100 \text{ plaintext}
 \end{array}$$

II. Block ciphers

Block ciphers are the type of algorithms that take a block of plaintext and encrypt it into a block of cipher text usually of the same size. The strength of the algorithm, however, does not depend on the size of the block that we take but it relies on the size of the key. An endorsed length of a block is usually a multiple of 8. And the blocks are often padded to reach that certain length. A block cipher uses a pair of algorithm; one for encrypting plain text and the other for decrypting the ciphered text. To annotate the whole mechanism through a single expression; suppose \check{E} and \check{D} represents two algorithms, plaintext block and cipher key be represented by \check{P} and \check{K} , respectively, where \check{P} is of size n -bit and \check{K} is a k -bit word. The entire encryption process can be condensed as

$$\check{E}_k(\check{P}) := \check{E}(\check{K}, \check{P}): \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$$

The decryption method takes the ciphered text \check{C} as an input with k -bit key and produces a decrypted text. The decryption process can be condensed by the following expression:

$$\check{E}_k^{-1}(\check{C}) = \check{D}_k(\check{C}) := \check{D}(\check{K}, \check{C}) := \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$$

So for all keys \check{K} the following property must satisfy

$$\check{D}_{\check{K}}(\check{E}_{\check{K}}) = \check{P}$$

Block ciphers are beneficial due to their fast and secure implementation. These are simple and easy to implement.

One of the particular block ciphers is the substitution-permutation network (SPN). It consists of alternating rounds of substitution followed by the permutation. Substitution creates confusion [Shannon] while mixing the key bits with plaintext. Whereas, permutation operation takes the output bits of S-boxes and permutes them before forwarding them to the next stage. S-boxes are made one to one to guarantee the inverse. A good S-box must satisfy the avalanche effect.

The core values of cryptography include some essential information security services. These include confidentiality, integrity, authentication and non-repudiation. Confidentiality is referred to as secretes of the information. While sending the data over a network, the foremost necessity is to protect it from the eavesdropper. Confidentiality can be obtained through physical methods but in cryptography, its true source is mathematical algorithm and encryption. During the data transmission, there is a chance of it being modified due to the invasion of third parties called adversaries. So data *integrity* ensures that the acquired data is not altered during transmission. In cryptography, data integrity is obtained by using a hash algorithm. The most commonly used hash algorithms are SHA-2, SHA-3, and

MD5. *Authentication* provides the identity of the sender and other related parameters such as username, passwords, etc. The methods used to acquire the authentication include password authentication protocol (PAP), Authentication token and protocol based on secret key cryptography, Diffie Hellman authentication, etc. Non-repudiation service ensures the validity of transmitted information. *Non-repudiation* makes it very hard to successfully deny the source of the message as well as its integrity. Digital signatures are used to achieve non-repudiation. Digital signatures can only be created by a single person hence the denial becomes impossible.

1.1.3 Chaos and DNA based crypto-algorithms

There are four types of nucleic acid bases of a DNA sequence namely Adenine (A), Thymine (T), Cytosine (C) and Guanine (G). In these nucleic acid bases, A is complementary to T and G is complementary to C. In binary numbers, 0 is complementary to 1, so 00 to 11. Similarly, 01 is complementary to 10. A 24 combination set forms by mapping the four bases A, T, C and G to 00, 01, 10 and 11. Out of these 24 combinations, eight groups satisfy the Watson-Crick complement rule [25]. The pixel of an image represents a byte. After converting these bytes originating from an image, they can easily be encoded by the DNA rules. For example, if we have a pixel value 214 then its binary representation is [11010110]. According to encoding rule 3, its corresponding DNA sequence is [TGGC]. Now looking in table 2, according to rule 1, [TGGC] is equal to [10111100] in binary having decimal value 188. This is the encrypted text. Moving to the decoding process, the pixel values are again achieved by using the DNA sequence rules in reverse.

Table 1. DNA encoding rule

Rules	1	2	3	4	5	6	7	8
A	01	00	00	01	10	11	10	11
T	10	11	11	10	01	00	01	00
C	00	01	10	11	11	10	00	10
G	11	10	01	00	00	01	11	01

The addition, subtraction and multiplication operation of the DNA encoding rules coincides with modulo 4 operations.

The pretended fundamental aspects of digital medium such as high redundancy, bulk data capacity and strong correlation among nearby pixels weaken the text encryption algorithms for image encryption purposes. With the prompt communication of digital images via open networks, the images security during transmission became an important issue and appeals much attention of cryptographers. To overcome this deficit, many encryption schemes have been developed. Among the current state-of-the-art for image encryption approaches extensively used for SP-Network are; algebra

based S-box design, chaotic systems and DNA transform. Consequently, some schemes comprise of these three notions could be seen in [25-27]. Encryption based on these two aspects are valued because an S-box and DNA sequences bear the responsibility of creating confusion in different layer of an RGB image, whereas the chaotic systems are highly sensitive to initial conditions and produces pseudo randomness and aperiodicity.

Chaos means disorder. Nowadays, the notion of chaos and DNA plays a prominent role in application point of view in different fields like Physics, Biology, Engineering and technology etc. the 1D Chaotic maps get fame because of its simplicity, high randomness and high sensitivity to initial conditions. They are used to create diffusion in data. The only drawback of this concept is its low non-linear behavior. However, in parallel, there are many positive aspects like ergodicity, mixing, highly sensitive dependence on initial conditions and management parameter, unpredictability, random-like behavior of output etc., that are analogous to the confusion and diffusion properties of Claude Shannon [6] which strengthen the concept of Chaos and DNA based encryption methodologies.

As DNA molecules have the characteristics of extraordinary information density and vast parallelism therefore, it is used in parallel with chaos to make a secure transmission of digital images [29]. In general, the chaotic systems are divided into two main categories i.e. the low dimensional chaotic systems [30] and high dimensional chaotic systems (more than one dimensional chaotic system) [31]. The 1st category consists of one-dimension chaotic maps. These structures are simple and can be implemented easily. The only drawback of these maps is their small key-space size that weakens the security level [32]. For example, Wang et al. cryptanalyzed an image encryption scheme in [32]. Besides, in digital computers, periodic behavior of the chaotic systems may degrade with the finite precision [33]. The image encryption ciphers comprise of DNA and high dimensional chaos may also comprise of some deficiencies. For example, Som et al. [34] encryption scheme is based on DNA and the Arnold cat map. But in [35] it is proven that the Arnold cat map has some drawbacks as its iteration times are limited, which makes the encryption technique not applicable for all plain images. Moreover, the schemes based on DNA transformations are stationary for all pixels in several digital image cryptosystems, i.e. they are fixed [36], or they form a secret key with 3-bit and therefore it is insecure in front of brute force or plaintext attack [37].

1.2 Finite commutative rings with identity

The study of commutative rings with identity is concerned with objects possessing two binary operations (called addition and multiplication) related by the distributive laws. It is the first study analogues to the basic points of development in the structure of rings and fields. In particular the rings, subrings, quotient rings, ideals, local rings, fields, Galois fields, Galois rings and chain rings are discussed in this section.

1.2.1 Rings [18, definition 1.28]

A non-empty set R equipped with two binary operations say addition (+) and multiplication (\cdot), denoted by $(R, +, \cdot)$, is said to be a ring if.

- a. $(R, +)$ is an abelian group.
- b. (R, \cdot) is a semi group.
- c. The binary operation (\cdot) is distributive over binary operation (+), that is, for $a, b, c \in R$

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

$$(b + c) \cdot a = b \cdot a + c \cdot a$$

Remark 1

- i. A ring $(R, +, \cdot)$ is a commutative ring if its multiplication binary operation \cdot is commutative, that is, $a \cdot b = b \cdot a$ for all $a, b \in R$.
- ii. We say R is a ring with 1 (or ring with identity) if there exists an identity with respect to the binary operation multiplication, that is, there exists $1 \in R$ such that for all $a \in R$ we have $a \cdot 1 = 1 \cdot a = a$.
- iii. A subset \mathcal{S} of a ring R is said to be a subring of R if \mathcal{S} itself form a ring under the same binary operations hold in R
- iv. Let $(R, +, \cdot)$ be a ring and let $\mathcal{S} \subseteq R$. Then $(\mathcal{S}; +, \cdot)$ is a subring of R if (and only if) \mathcal{S} is non-empty and the following hold:
 - a. $a + b \in \mathcal{S}$ for any $a, b \in \mathcal{S}$
 - b. $a - b \in \mathcal{S}$ for any $a, b \in \mathcal{S}$
 - c. $ab \in \mathcal{S}$ for any $a, b \in \mathcal{S}$
- v. Let $(R, +, \cdot)$ be a commutative ring and $a, b \in R$. If $a \cdot b = 0$ such that $a \neq 0$ and $b \neq 0$ then we say that a and b are zero divisor of each other.

- vi. Let R be a commutative ring with identity. An element $u \in R$ is unit element in R if there exist $v \in R$ such that $uv = vu = 1$.
- vii. A commutative ring with identity is said to be an integral domain if it has no zero divisors. A very useful example of integral domain is the ring of integers \mathbb{Z} .
- viii. A commutative ring \mathbb{F} with identity is said to be a field if $(\mathbb{F} \setminus \{0\}, \cdot)$ is a group. Furthermore, a field is divided into two sub categories based on the number of elements it contained.

Some examples of rings and subrings are given below.

- i. Matrix rings: For a commutative ring R with identity, $M_n(R)$ is matrix ring under the usual matrix addition and multiplication of square matrices of order n is a non-commutative ring (unless $n = 1$). It is no longer a ring if we limit it to invertible matrices, since then there is no zero for inclusion.
- ii. Ring of polynomials: Polynomials, with coefficients form a commutative ring R with identity under the usual addition and multiplication form a commutative ring in one indeterminate x denoted as $R[x]$. The polynomial ring $R[x]$ has identity as the coefficient ring R has the multiplicative identity.
- iii. Modular arithmetic: Binary arithmetic on $\{0,1\}$ provides us with a 2-element unit commutative ring. More general, if we consider the addition and multiplication of mod n on $\{0,1,\dots,n-1\}$, we get a commutative ring.
- iv. Let R be any abelian group with group operation $+$. Define $ab = 0$ for all $a, b \in R$; then R is a ring.
- v. $n\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\}$ is a subring of \mathbb{Z} for any $n \in \mathbb{N}$.
- vi. Let R_1 and R_2 be rings. Define binary operations on $R_1 \times R_2$ coordinate wise: for $r_1, r'_1 \in R_1$ and $r_2, r'_2 \in R_2$, let $(r_1, r_2) + (r'_1, r'_2) := (r_1 + r'_1, r_2 + r'_2)$, $(r_1, r_2) \cdot (r'_1, r'_2) := (r_1 \cdot r'_1, r_2 \cdot r'_2)$. Accordingly, $R_1 \times R_2$ is a ring.
- vii. In the polynomial ring $R[x]$, the polynomials of even degree form a subring, but the polynomials of odd degree do not form a subring because $x \cdot x = x^2$ is not of odd degree.

A non-zero polynomial $f(x) = \sum_{i=0}^n a_i x^i$ has degree n if $n \geq 0$ and the leading coefficient $a_n \neq 0$. The zero polynomial is defined by convention to have degree $-\infty$. Alternatively, one may say that the

degree of the zero polynomial is undefined; in that case, one will need to make minor changes to some of the results below.

Polynomials are added component-wise, and multiplied using the “convolution” formula

$$\sum_{i=0}^m a_i x^i + \sum_{i=0}^n b_i x^i = \sum_{i=0}^{\max(m,n)} (a_i + b_i) x^i$$

$$\left(\sum_{i=0}^m a_i x^i \right) \cdot \left(\sum_{j=0}^n b_j x^j \right) = \sum_{k=0}^{mn} c_k x^k, \text{ where } c_k = \sum_{i+j=k} a_i b_j$$

The ring of polynomials in indeterminate x with coefficients in the ring R is denoted by $R[x]$.

Theorem 1 [18, theorem 1.51]

Let R be a ring. Then:

1. $R[x]$ is commutative if and only if R is commutative.
2. $R[x]$ is a ring with identity if and only if R has an identity element.
3. $R[x]$ is an integral domain if and only if R is an integral domain.

Let R be a commutative ring with identity and let $f(x) \in R[x]$. An element $c \in R$ is a root of the polynomial $f(x)$ if $f(c) = 0$. In other words $f(x)$ is divisible by the linear polynomial $x - c$.

Proposition 1 [20, proposition 1.3.1]

Let $\mathbb{F}[x]$ be the polynomial ring in one indeterminate x over the field \mathbb{F} . The units in $\mathbb{F}[x]$ are exactly the non-zero elements of \mathbb{F} .

Theorem 2 [18, definition 1.52]

Let \mathbb{F} be a field, and $f(x), g(x) \in \mathbb{F}[x]$. Suppose that $g(x) \neq 0$. There are unique polynomials $q(x), r(x) \in \mathbb{F}[x]$ such that

$$f(x) = g(x)q(x) + r(x), \text{ and } \deg r(x) < \deg g(x).$$

Theorem 3 [20, theorem 1.4.4]

Let \mathbb{F} be a field, and $f(x) \in \mathbb{F}[x]$, where $\deg f(x) = n \geq 0$.

- i. (The Root Theorem) c is a root of $f(x)$ in \mathbb{F} if and only if $x - c \mid f(x)$.
- ii. $f(x)$ has at most n roots in \mathbb{F} .

1.2.2 Ideal [18, definition 1.33]

Let R be a commutative ring with identity. A non-empty subset $I \subseteq R$ is said to be an ideal of R if

- a. $a - b \in I$ for all $a, b \in I$.
- b. $ra \in I$ for all $r \in R$ and $a \in I$.

Remark 2

- i. Every ideal is a subring but its converse is not true in general.
- ii. In a field \mathbb{F} there is no proper ideal.

Types of ideals [18]

1. An ideal generated by a single element is called principal ideal mathematically, if $a \in R$ then $I = \{ra \mid r \in R\}$ is principal ideal. Mostly represented by $\langle a \rangle$.
2. An integral domain is a principal ideal domain (PID) if its each ideal is a principal ideal.
3. A (proper) ideal, P , of a unitary commutative ring R is said to be a prime ideal if, for any $a, b \in R$ such that $ab \in P$ imply either $a \in P$ or $b \in P$.
4. A proper ideal \mathcal{M} in a unitary commutative ring R is called a maximal ideal if there is no proper ideal of R , say J , such that $\mathcal{M} \subset J \subset R$.

Proposition 2 [18, proposition 1.47]

If $I \subset \mathbb{Z}$ is an ideal, then $I = \langle a \rangle$ for some $a \in \mathbb{Z}$ (and we may assume $a \geq 0$).

Examples

- a) The set $2\mathbb{Z}$ of even integers is an ideal of the ring \mathbb{Z} .
- b) Let R be a commutative ring with identity and J be the set of all polynomials in the polynomial ring $R[x]$ with zero constant term, that is, if $f(x) \in J$, then $f(x) = \sum_{i=1}^n a_i x^i$. Thus, the set J is an ideal of $R[x]$ and it is represented as $xR[x]$, the ideal generated by the indeterminate x . In case of $\mathbb{Z}[x]$, the ideal $x\mathbb{Z}[x]$ is the principal prime ideal in $\mathbb{Z}[x]$, however, for any field \mathbb{F} , the ideal $x\mathbb{F}[x]$ is the principal maximal ideal in $\mathbb{F}[x]$.

Proposition 3 [20, proposition 1.2.3]

An ideal $\langle p \rangle = p\mathbb{Z} \subset \mathbb{Z}$ is a prime ideal if and only if p is a prime.

Definition 1 [20, Proposition 8.1.3]

Let I be an ideal of \mathbb{Z} . One possibility is that $I = \langle 0 \rangle$, the ideal consisting of just the single element 0 and appropriately called the zero ideal.

Definition 2 [20, definition 1.2.12]

Let I be an ideal in a commutative ring R with identity. Then the set

$$\sqrt{I} := \{r \in R \mid r^n \in I \text{ for some integer } n > 0\}$$

is an ideal of R (as it is easy to check) called the radical of I ; it contains I . An ideal J is called a radical ideal if $\sqrt{J} = J$.

Proposition 4 [20, proposition 1.2.13]

A maximal ideal M in a unitary commutative ring R is a radical ideal.

1.2.3 Quotient rings [20, definition 1.2.4]

Let R be a commutative ring with identity and I be its ideal. Then a quotient ring (also called a residue-class ring) is a ring denoted as $\frac{R}{I} = \{r + I : r \in R\}$ having respectively the binary operations addition and multiplication as $(r + I) + (s + I) = r + s + I$ and $(r + I)(s + I) = rs + I$. There is a natural projection $\pi: R \rightarrow \frac{R}{I}$ defined as $\pi(r) = r + I$. If the ring R is \mathbb{Z} and the ideal is $n\mathbb{Z}$, the quotient ring is $\frac{\mathbb{Z}}{n\mathbb{Z}_n} (\cong \mathbb{Z}_n)$. Let \mathbb{F} be a field, and $f(x) \in \mathbb{F}[x]$. $\langle f(x) \rangle$ is the set of all multiples (by polynomials) of $f(x)$, the (principal) ideal generated by $f(x)$. The quotient $\frac{\mathbb{F}[x]}{\langle f(x) \rangle}$ form a ring called quotient ring. It is as if you've set multiples of $f(x)$ equal to 0. If $f(x) \in \mathbb{F}[x]$, then $a(x) = f(x) + \langle f(x) \rangle$ is the coset of $f(x)$ with respect to the ideal $\langle f(x) \rangle$.

Define $a(x) = b(x) \pmod{f(x)}$ ($a(x)$ is congruent to $b(x) \pmod{f(x)}$) to mean that $f(x) \mid (a(x) - b(x))$. In other words it means $a(x)$ and $b(x)$ is congruent mod $f(x)$ if they differ by a multiple of $f(x)$. In equation form, this says $a(x) - b(x) = k(x) \cdot f(x)$ for some $k(x) \in \mathbb{F}[x]$, or $a(x) = b(x) + k(x) \cdot f(x)$ for some $k(x) \in \mathbb{F}[x]$.

Theorem 4 [18, theorem 1.47]

Let R be a commutative ring with identity. Then:

1. *An ideal M of R is a maximal ideal if and only if $\frac{R}{M}$ is a field.*
2. *An ideal P of R is a prime ideal if and only if $\frac{R}{P}$ is an integral domain.*
3. *Every maximal ideal of R is a prime ideal.*
4. *If R is a principal ideal domain, then $\frac{R}{\langle p \rangle}$ is a field if and only if p is a prime element of R .*

1.2.4 Galois field extension [18, definition 1.41]

If a field has infinite number of elements, we call it an infinite field and the most fundamental and famous examples are \mathbb{Q} , \mathbb{R} , and \mathbb{C} . It is easily checked that $\mathbb{Q}(i) = \{a + ib \mid a, b \in \mathbb{Q}\}$ is an infinite field with respect to the addition and multiplication of complex numbers. The polynomial $1 + x^2$ is irreducible over \mathbb{Q} . Therefore, $\frac{\mathbb{Q}[x]}{\langle 1 + x^2 \rangle}$ is a field. This field is isomorphic to $\mathbb{Q}(i)$. The polynomial $1 + x^2$ is irreducible in \mathbb{R} . So, $\frac{\mathbb{R}[x]}{\langle 1 + x^2 \rangle}$ is a field whose elements are $x_0 + x_1\alpha$, where x_0 and x_1 are in \mathbb{R} , and α is a root of the polynomial $1 + x^2 \in \mathbb{R}[x]$. It is clear that this infinite field is isomorphic to the field \mathbb{C} of complex numbers. The other examples of infinite fields extensions includes; $\mathbb{Q}[\pi], \mathbb{Q}[e], \mathbb{Q}[i], \mathbb{Q}[\sqrt{d}], \mathbb{Q}[i\sqrt{d}]$. Though, the field $\mathbb{Q}[\sqrt{d}]$ is simple quadratic algebraic field extension of the rational field \mathbb{Q} in the real field \mathbb{R} . Similarly, the fields $\mathbb{Q}[i], \mathbb{Q}[i\sqrt{d}]$ are quadratic algebraic field extension of the rational field \mathbb{Q} in the complex field \mathbb{C} , whereas the fields $\mathbb{Q}[\pi], \mathbb{Q}[e]$ are transcendental field extensions of \mathbb{Q} in \mathbb{R} .

A field that has finite number of elements is known as a finite field and most famous examples are the fields of integers modulo a prime p . A finite field is also called a Galois field. The naming “Galois field” is largely used (in honor of the French mathematician Évariste Galois). Several notations exist for a Galois field. A Galois field of cardinal q ($q = p^m$, p is prime integer and m is a positive integer) is generally represented as \mathbb{F}_q or $GF(q)$, where GF stands for Galois field.

Theorem 3 [18, theorem 2.8]

The group of non-zero elements of the Galois field $GF(p^m)$ is cyclic.

Theorem 6 [19, theorem 2.2]

The cardinal q of a Galois field is necessarily of the form $q = p^m$, where p a prime integer and m is a positive integer. Furthermore, for every prime integer p and a positive integer m , there exists a Galois field containing p^m elements.

Theorem 7 [19, theorem 2.8]

$GF(p^m)$ is a subfield of $E = GF(p^n)$ if and only if m is a divisor of n .

Proposition 5 [19, proposition 2.2]

All Galois fields of the same cardinal are isomorphic. Thus, for any prime number p (p even or odd) and any integer m greater than or equal to 1, there exists one Galois field (and only one, up to an isomorphism) of cardinal p^m .

A Galois field is thus entirely determined by its cardinal. Therefore, all Galois fields with the same cardinal p^m (p is prime and $m \geq 1$) are denoted by the same symbol, namely, either $GF(p^m)$ or \mathbb{F}_{p^m} for $m \geq 2$ and \mathbb{F}_p for $m = 1$.

Corollary 1 [20, corollary 2.1.1]

Any Galois field \mathbb{F}_p of cardinal p with p a prime number is isomorphic to \mathbb{Z}_p .

A Galois field \mathbb{F}_p of cardinal p is referred to as a prime field (it has no proper sub-fields).

Example

The two fields of lowest cardinal are \mathbb{F}_2 and \mathbb{F}_3 . The next field of prime cardinal is \mathbb{F}_5 (or \mathbb{Z}_5).

Definition 4 [18, definition 1.49]

A single-variable or univariate polynomial with leading coefficient 1 is called a monic polynomial.

Therefore, a monic polynomial has the form

$$x^n + c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \dots + c_2x^2 + c_1x^1 + c_0$$

Theorem 8 [18, theorem 3.20]

Let p be a prime and n a positive integer. Then $x^{p^n} - x$ is the product of all monic irreducible polynomials over \mathbb{F}_p whose degree divides n .

If $f(x) = x^2 - 2 \in \mathbb{Q}[x]$, then $\frac{\mathbb{Q}[x]}{\langle x^2-2 \rangle} (\cong \mathbb{Q}[\sqrt{2}])$ form a quotient ring which is in fact the extension field of \mathbb{Q} in real field. If $f(x) = x^2 + 1$ in $\mathbb{Q}[x]$, then $\frac{\mathbb{Q}[x]}{\langle x^2+1 \rangle} (\cong \mathbb{Q}[\sqrt{-1}])$ form a quotient ring which is in fact the extension field of \mathbb{Q} in complex field.

Definition 5 [18, definition 1.81]

Let α be an element in a field E containing the field $GF(p)$. We call the monic polynomial of smallest degree which has coefficients in $GF(p)$ and α as a root, the minimal polynomial of α .

Definition 6 [18, definition 1.57]

A polynomial $f(x)$ that cannot be written as a product of two other polynomials of smaller degree than degree of $f(x)$ is called an irreducible polynomial.

Definition 7 [18, definition 2.9]

The element x of the Galois field $GF(p^m)$ is called a primitive element if it is a generator of the Galois cyclic group $(GF(p^m)^*, \cdot)$. In other words, there does not exist an integer j such that $j < p^m - 1 \mid x^j = 1$ and all the powers x^i for $i = 1, 2, \dots, p^m - 1$ are distinct.

The polynomials $P_2(x) = 1 + x^2$ in $\mathbb{F}_2[x]$, $P_3(x) = 2 + 2x + x^3$ in $\mathbb{F}_3[x]$ and $P_4(x) = 1 + x + x^2 + x^3 + x^4$ in $\mathbb{F}_2[x]$ are non-primitive irreducible polynomials. Consequently the corresponding Galois cyclic groups of the extension fields $\frac{\mathbb{F}_3[x]}{\langle P_2(x) \rangle}$, $\frac{\mathbb{F}_3[x]}{\langle P_3(x) \rangle}$ and $\frac{\mathbb{F}_2[x]}{\langle P_4(x) \rangle}$ are not generated by the roots of $P_2(x)$, $P_3(x)$, and $P_4(x)$, respectively.

Remark 3

- i. If α is a primitive element of $GF(p^m)$, then its inverse α^{-1} is a primitive element too.
- ii. A primitive element of $GF(p^m)$ cannot belong to a sub-field of $GF(p^m)$.

Examples of non-primitive elements

- a) Let $x = 2$ be an element of the field $GF(7^1) = \mathbb{F}_7$. This element is not a primitive element of \mathbb{F}_7 since $x^3 \equiv 1 \pmod{7}$.
- b) Let $x = \alpha$ be a root of the prime polynomial $1 + x^2$ over $\mathbb{F}_3[x]$. The element x is not a primitive element of $GF(3^2) = \frac{\mathbb{F}_3[x]}{\langle 1+x^2 \rangle}$ since $x^4 \equiv 1 \pmod{3}$.
- c) Let $x = \alpha$ be a root of the prime polynomial $1 + x + x^2 + x^3 + x^4$ over \mathbb{F}_2 . The element x is not a primitive element of $GF(2^4) = \frac{\mathbb{F}_2[x]}{\langle 1+x+x^2+x^3+x^4 \rangle}$ as $x^5 = 1$.
- d) Let $x = \alpha$ be a root of the prime polynomial $2 + 2x + x^3$ over \mathbb{F}_3 . The element x is not a primitive element of $GF(3^3) = \frac{\mathbb{F}_3[x]}{\langle 2+2x+x^3 \rangle}$ as $x^{13} \equiv 1 \pmod{3}$.

In the five preceding examples, the element x does not generate the corresponding cyclic group $(GF(p^m)^*, \cdot)$.

Examples of primitive elements

- a) Let $x = 3$ be an element of the field $GF(7^1) = \mathbb{F}_7$. This element is a primitive element since it generates all the non-zero elements of \mathbb{F}_7 . The element $x = 5$ is another primitive element of \mathbb{F}_7 .
- b) Let α be a root of the polynomial $1 + x + x^3 \in \mathbb{F}_2[x]$. The elements of the field $GF(2^3) = \frac{\mathbb{F}_2[x]}{\langle 1+x+x^3 \rangle}$ are
 - i. $0, \alpha, \alpha^2, 1 + \alpha = \alpha^3, \alpha + \alpha^2 = \alpha^4, 1 + \alpha + \alpha^2 = \alpha^5, 1 + \alpha^2 = \alpha^6, 1 = \alpha^7$
 - ii. So that α is a primitive element of $\frac{\mathbb{F}_2[x]}{\langle 1+x+x^3 \rangle}$. The elements $\alpha^2, \alpha^3, \dots, \alpha^6$ are another primitive elements of $\frac{\mathbb{F}_2[x]}{\langle 1+x+x^3 \rangle}$.

Theorem 9 [20]

The number of primitive elements of the Galois field $GF(p^m)$ is $\phi(p^m - 1)$, where ϕ is the Euler function.

Proof

The proof follows from the isomorphism $(GF(p^m))^* \cong C_{p^m-1}$ and the fact that the cyclic group C_n has $\phi(n)$ generators.

Corollary 2 [20, proposition 1.3.9]

A primitive polynomial over prime field \mathbb{F}_p is irreducible over \mathbb{F}_p , but an irreducible polynomial is not necessarily primitive (there are irreducible polynomials that are not primitive).

Proposition 6 [20, proposition 2.1.4]

For any Galois field $GF(p^m)$, there exists at least one primitive polynomial $P_m(x)$ of degree m over \mathbb{F}_p . The m roots of a primitive polynomial $P_m(x)$ over \mathbb{F}_p are primitive elements of $GF(p^m)$.

Proposition 7 [20]

The number of primitive polynomials of the Galois field $GF(p^m)$, i.e. the number of primitive polynomials of degree m over \mathbb{F}_p , is $\frac{1}{m} \phi(p^m - 1)$, where ϕ is the Euler function.

1.2.5 Algebra of Galois field extension and its matrix algebra representation

[21, definition 11.1] Let \mathbb{F} be a field and V be an additive abelian group. For all $a, b \in \mathbb{F}$ and $v_1, v_2 \in V$, V is said to be vector space over \mathbb{F} , if the scalar multiplication map $\mathbb{F} \times V \rightarrow V$ defined by $(a; v) \mapsto av$ satisfy the following conditions.

1. $a(v_1 + v_2) = av_1 + av_2$
2. $ab(v) = a(bv)$
3. $(a + b)v = av + bv$
4. $1v = v$

A non-empty subset B of the vector space V is said to be base of V if the vectors in B are linearly independent and B is the spanning set of V . The cardinality of B is defining the dimension of the space V . The dimension of the vector space V is finite if the set B is finite otherwise V is an infinite dimensional vector space.

A vector space A over a field \mathbb{F} is said to be an algebra if A is a ring and $a(v_1v_2) = v_1(av_2)$. If the algebra A over \mathbb{F} is such that $(A \setminus \{0\}, \cdot)$ is a group, we call it a division algebra. Every field is algebra over itself and every field is an algebra over its subfield.

Let R be a commutative ring with identity and M be an additive abelian group. For all $r, s \in R$ and $m_1, m_2 \in M$, M is said to be module over R , if the scalar multiplication map $R \times M \rightarrow M$ defined by $(r; m) \mapsto rm$ satisfy the following conditions.

1. $r(m_1 + m_2) = rm_1 + rm_2$
2. $rs(m) = r(sm)$
3. $(r + s)m = rm + sm$
4. $1m = m$

A module M is said to be an algebra over the ring R if M is a ring and $a(v_1v_2) = v_1(av_2)$. Every ring is algebra over itself and every ring is an algebra over its subring. A module is free if it possess a base. Every vector space is an example of a free R-module.

The so-obtained Galois field $\frac{\mathbb{F}_p[x]}{\langle P_m(x) \rangle}$ is the unique (up to isomorphism) extension of degree m of the base field \mathbb{F}_p by the element α , a root of the prime polynomial $P_m(x)$ (α is the residue class of x modulo $P_m(x)$). It is convenient to use the notation $\frac{\mathbb{F}_p[x]}{\langle P_m(x) \rangle}$ for describing the field $GF(p^m)$. The p^m elements of $GF(p^m)$ are represented by residue classes of polynomials in $\mathbb{F}_p[x]$. The residue classes are obtained by effecting the relevant additions and multiplications modulo p and modulo $P_m(\alpha) = 0$. The addition of elements of $GF(p^m)$ is that of vectors in a vector space over \mathbb{F}_p . The product of elements is the remainder of the division by $P_m(x)$ of the product in $\mathbb{F}_p[x]$. Indeed, all the calculations in $GF(p^m)$ are made by using $P_m(\alpha) = 0$ and $pa(\alpha) = 0$ for any $a(\alpha)$ in $GF(p^m)$. In this regard, let us suppose that, in a calculation, an element α^k appears with $k \geq m$. Then, the k power of α can be decreased by repeated use of

$$\alpha^m = -(c_0 + c_1\alpha + \cdots + c_{m-1}\alpha_{m-1})$$

(That corresponds to $P_m(\alpha) = 0$) in $\alpha^k = \alpha^{k-m}\alpha^m$ and of $py = 0$, where y is any positive power of α . Finally, intermediate calculations and the realization of the elements of $GF(p^m) = \frac{\mathbb{F}_p[x]}{\langle P_m(x) \rangle}$ depend on primitive irreducible polynomial $P_m(x)$. However, for fixed p , all the possible choices of $P_m(x)$ of the same degree m give isomorphic realizations of $GF(p^m)$.

Proposition 8 [18]

For any given Galois field $GF(p^m)$, $m \geq 2$, it is possible to construct a matrix realization (or linear representation) of the field by matrices of dimension $m \times m$ with matrix elements in \mathbb{F}_p .

The matrix representation indicated in Proposition 8 can be understood as follows. To the element α , the root of $P_m(x)$, the following $m \times m$ matrix is originated.

$$A = \begin{bmatrix} 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & \cdots & 0 & -c_2 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -c_{m-1} \end{bmatrix}$$

where c_0, c_1, \dots, c_{m-1} are the coefficients in the prime polynomial

$$P_m(x) = c_0 + c_1x + \cdots + c_{m-1}x_{m-1} + x_m$$

with $c_0, c_1, \dots, c_{m-1} \in \mathbb{F}_p$.

The matrix representation X of the element

$$y = y_0 + y_1\alpha + \cdots + y_{m-1}\alpha_{m-1}$$

of $\frac{\mathbb{F}_p[x]}{\langle P_m(x) \rangle}$ is then given by

$$Y = y_0I + y_1A + \cdots + y_{m-1}A_{m-1}$$

Whereas $y_0, y_1, \dots, y_{m-1} \in \mathbb{F}_p$ and I is the $m \times m$ identity matrix. Through the correspondence

$x \leftrightarrow X$, the laws $+$ and \cdot of $GF(p^m) = \frac{\mathbb{F}_p[x]}{\langle P_m(x) \rangle}$ are replaced by the addition and multiplication

modulo p of matrices, respectively.

Example

Let us consider the field $GF(2^3) = \frac{\mathbb{F}_2[x]}{\langle 1+x+x^3 \rangle}$. In this case, the prime polynomial $P_3(x)$ of $\mathbb{F}_2[x]$ is

$$P_3(x) = 1 + x + x^3, \text{ where } c_0 = 1, c_1 = 1, c_2 = 0$$

Therefore, the element α , a root of the polynomial $1 + x + x^3 \in \mathbb{F}_2[x]$, is represented by the 3×3 matrix

$$A = \begin{bmatrix} 0 & 0 & -1 \\ 1 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \text{ mod } 2$$

More generally, the element

$$x = x_0 + x_1\alpha + x_2\alpha^2$$

of $\frac{\mathbb{F}_2[x]}{\langle 1+x+x^3 \rangle}$ is represented by the 3×3 matrix

$$X = x_0I + x_1A + x_2A^2$$

This yields the following representation

$$\begin{aligned}
0 \leftrightarrow O &= \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad 1 \leftrightarrow I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \\
a \leftrightarrow A &= \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \quad b \leftrightarrow b = A^2 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}, \\
c \leftrightarrow C &= I + A = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \quad e \leftrightarrow E = I + A + A^2 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}, \\
f \leftrightarrow F &= I + A^2 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \quad d \leftrightarrow D = A + A^2 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}
\end{aligned}$$

of the field $\frac{\mathbb{F}_2[x]}{\langle 1+x+x^3 \rangle}$.

Note that

$$\begin{aligned}
a \leftrightarrow A, \quad b \leftrightarrow B = A^2, \quad c \leftrightarrow C = A^3 \quad d \leftrightarrow D = A^4, \\
e \leftrightarrow E = A^5, \quad f \leftrightarrow F = A^6, \quad 1 \leftrightarrow I = A^7
\end{aligned}$$

Therefore, the matrix A generates a group (with respect to matrix multiplication) isomorphic to the cyclic group C_7 , in agreement with the fact that α is a primitive element.

1.2.6 Galois ring

Definition 8 [20, definition 1.2.9]

A unitary commutative ring R with a unique maximal ideal \mathcal{M} is called a local ring, with residue field $K = \frac{R}{\mathcal{M}}$. It is straight forward to verify that $\mathcal{M} = \{r \in R | r \text{ is not a unit}\}$.

Proposition 9 [20, proposition 1.2.11]

1. Let \mathcal{R} be a unitary commutative ring and $\mathcal{M} \neq (0)$ an ideal such that each $r + \mathcal{M} \in \frac{\mathcal{R}}{\mathcal{M}}$ is a unit. Then \mathcal{R} is a local ring and \mathcal{M} is its maximal ideal.
2. Let \mathcal{R} be a unitary commutative ring and \mathcal{M} a maximal ideal such that each element of the set $1 + \mathcal{M} := \{1 + x | x \in \mathcal{M}\}$ is a unit in \mathcal{R} . Then \mathcal{R} is a local ring.

Definition 9 [21, section 2.1]

A commutative ring R with unit element is known to be a Galois ring if set of all its zero divisors, including 0, constitutes a principal prime ideal $\langle p \rangle$ with p prime.

Examples of Galois ring

i. $GR(2^2, 1) = \mathbb{Z}_4$

If $m = 1$, the ring $GR(p^s, 1)$ and local ring \mathbb{Z}_{p^s} are isomorphic. Consider $p = s = 2$ that corresponds to the ring \mathbb{Z}_4 . It is easy to verify that any \mathbb{Z}_4 part can be written as $a = t_0 + 2 \times t_1$; $t_0, t_1 \in \mathbb{Z}_2$ where the operations $+$ and \times are performed in \mathbb{Z}_4 ($t_1 \in \mathbb{Z}_2$). A principal ideal is the zero divisors (0 and 2) of the unitary ring \mathbb{Z}_4 . \mathbb{Z}_4 is, thus, a Galois ring.

ii. $GR(2^1, 4) = \frac{\mathbb{Z}_2[x]}{\langle 1+x+x^4 \rangle}$

The Galois field $GF(2^4) = \frac{\mathbb{F}_2[x]}{\langle 1+x+x^4 \rangle}$ of characteristic 2 and cardinal 16, is also a Galois ring in the sense that $1 + x + x^4$ is obviously a monic basic primitive polynomial over \mathbb{Z}_2 and the unique zero divisor 0 constitutes a principal ideal (here 0 plays the role of $p = 2$). Therefore $GF(2^4) = GR(2^1, 4)$.

iii. $GR(2^2, 2) = \frac{\mathbb{Z}_2[x]}{\langle 1+x+x^2 \rangle}$

The polynomial $1 + x + x^2$ is clearly a monic basic primitive polynomial over \mathbb{Z}_4 . The ring $GR(2^2, 2) = \frac{\mathbb{Z}_4[x]}{\langle 1+x+x^2 \rangle}$ (not to be confused with the field $GR(2^2) = \frac{\mathbb{F}_4[x]}{\langle 1+x+x^2 \rangle}$) is of characteristic $2^2 = 4$ and has $(2^2)^2 = 16$ elements.

iv. $GR(2^2, 3) = \frac{\mathbb{Z}_2[x]}{\langle 3+x+2x^2+x^3 \rangle}$

The monic polynomial $P_3(x) = 3 + x + 2x^2 + x^3$ in $\mathbb{Z}_2[x]$ admits the image $\overline{P_3(x)} = 1 + x + x^3$ in $\mathbb{Z}_2[x]$, an irreducible polynomial over \mathbb{Z}_2 . Therefore, $P_3(x)$ is a monic basic irreducible polynomial. Thus, the ring $GR(2^2, 3)$ is a Galois ring of characteristic $2^2 = 4$ with $(2^2)^3 = 64$ elements. Let α be a root of $P_3(x)$. This root is an element of order $2^3 - 1 = 7$ of $GR(2^2, 3)$.

v. $GR(2^2, m)$

To define a structure of m qubits $GR(2^2, m)$, the Galois ring $GR(2^2, m)$ is of interest in quantum information (also referred to as R_4^m in quantum information). It has a characteristic of $2^2 = 4$, has $(2^2)^m = 4^m$ elements and corresponds to $GR(2^2, m) = \frac{\mathbb{Z}_2[x]}{p_m(x)}$ where $p_m(x)$ is a monic simple irreducible degree m polynomial in $\mathbb{Z}_2[x]$ (his image is an irreducible polynomial over \mathbb{Z}_2 under the homomorphism $\mathbb{Z}_2[x]$) The Galois ring $GR(2^2, m)$ is an expansion of the \mathbb{Z}_2 ring's degree m .

vi. The rings \mathbb{Z}_4 , \mathbb{Z}_8 and \mathbb{Z}_9 are commutative with a unit element for which the set of zero divisors form a principal ideal $\langle p = 2 \rangle$, $\langle p = 2 \rangle$ and $\langle p = 3 \rangle$, respectively. Therefore, $\mathbb{Z}_4 (= \mathbb{Z}_{2^2})$, $\mathbb{Z}_8 (= \mathbb{Z}_{2^3})$ and $\mathbb{Z}_9 (= \mathbb{Z}_{3^2})$ are Galois rings. Moreover, $\langle p = 2 \rangle$, $\langle p = 2 \rangle$ and $\langle p = 3 \rangle$ are maximal ideals of \mathbb{Z}_{2^2} , \mathbb{Z}_{2^3} and \mathbb{Z}_{3^2} , respectively.

More precisely, the integers modulo ring \mathbb{Z}_{p^s} with p prime and s positive integer is a Galois ring (1 is the identity of \mathbb{Z}_{p^s} ; the zero divisors including 0 of \mathbb{Z}_{p^s} form the principal ideal p of the finite ring \mathbb{Z}_{p^s} ; indeed, p is the unique maximal ideal of \mathbb{Z}_{p^s}). The \mathbb{Z}_{p^s} Galois ring has number of elements p^s and is characteristic p^s .

We have $\mathbb{Z}_{p^1} = \mathbb{F}_p$ in the special case $s = 1$, for which the only zero divisor is the trivial zero divisor. The principal ideal (here, $p = 0$) is the zero ideal \mathbb{Z}_p . Consequently, \mathbb{Z}_p constitute a Galois ring. More precisely, the Galois field \mathbb{F}_p is the Galois ring \mathbb{Z}_p .

Proposition 10 [23, proposition 3.1]

It is possible to make an element of the ring \mathbb{Z}_{p^s} with p prime number and s positive integer as $a = d_0 + d_1p + \dots + d_{s-1}p^{s-1}$.

Where each coefficient d_i belongs to the field \mathbb{F}_p ($i = 0, 1, \dots, s - 1$) and the operation of addition and multiplication coincides to the ring \mathbb{Z}_{p^s} .

Example

For $s = 2$ and $p = 2$, we readily verify that

$$\forall a \in \mathbb{Z}_{2^2} : a = d_0 + 2d_1, d_i \in \mathbb{F}_2 (i = 0, 1)$$

so that the elements a , denoted as (d_0, d_1) , of \mathbb{Z}_{2^2} are

$$0 = (0, 0), \quad 1 = (1, 0), \quad 2 = (0, 1), \quad 3 = (1, 1)$$

Similarly for $s = 3$, $p = 2$,

$$\forall a \in \mathbb{Z}_{2^3} : a = d_0 + 2d_1 + 2^2d_2, d_i \in \mathbb{F}_2 (i = 0, 1, 2)$$

and the elements a , denoted as (d_0, d_1, d_2) , of \mathbb{Z}_{2^3} are

$$\begin{aligned} 0 &= (0, 0, 0), & 1 &= (1, 0, 0), & 2 &= (0, 1, 0), & 3 &= (1, 1, 0) \\ 4 &= (0, 0, 1), & 5 &= (1, 0, 1), & 6 &= (0, 1, 1), & 7 &= (1, 1, 1) \end{aligned}$$

Let $P_m(x)$ be a primitive degree m , monic polynomial over the Galois ring \mathbb{Z}_{p^s} (with m and s positive integers, p prime number). Then, a Galois ring denoted as $GR(p^s, m)$ is the residue class ring $(p^s)^m = p^{sm}$. Characteristic of this ring is ps and cardinal $(p^s)^m = p^{sm}$. Any element a of $GR(p^s, m)$ can be written as

$$a = a_0 + a_1\alpha + \cdots + a_{m-1}\alpha_{m-1}, \quad a_i \in \mathbb{Z}_{p^s} \ (i = 0, 1, \dots, m-1)$$

Whereas, order of α is $p^m - 1$ (i.e. $\alpha^{p^m - 1} = 1$) which is a root of $P_m(x)$, with $P_m(x)$ dividing $x^{p^m - 1} - 1$ in $\mathbb{Z}_{p^s}[x]$.

Element of proof

The $GR(p^s, m)$ zero divisors, including the trivial zero divisor 0, constitute the $GR(p^s, m)$ principal ideal \mathfrak{p} (in general, the only $GR(p^s, m)$ maximum ideal). The Galois ring $GR(p^s, m)$ is known as Galois extension of degree m of the ring \mathbb{Z}_{p^s} of characteristic p^s . The ring \mathbb{Z}_{p^s} is called a prime ring. The Galois ring $GR(p^s, m)$ is the unique (up to isomorphism) extension of degree m of the ring \mathbb{Z}_{p^s} of integers modulo p^s .

The configuration of a Galois ring is defined by its properties

$$\text{Char}(GR(p^s, m)) = \text{Char}(\mathbb{Z}_{p^s}) = p^s$$

that is for p^s , positive power of a prime number p and its cardinal

$$\text{Card}(GR(p^s, m)) = p^{sm}$$

that is a positive power $(p^s)^m = p^{sm}$ of the characteristic p^s ($s \geq 1$ and $m \geq 1$)

In the case $s = 1$, the Galois ring

$$GR(p, m) = \frac{\mathbb{Z}_p[x]}{\langle P_m(x) \rangle} = \frac{\mathbb{F}_p[x]}{\langle P_m(x) \rangle} = GF(p^m)$$

is a Galois field, viz. the Galois field $GF(p^m)$, a field of characteristic p with p^m elements. A Galois field is a general a Galois ring in this respect.

Lastly, for $s = m = 1$, the Galois ring

$$GR(p, 1) = \frac{\mathbb{Z}_p[x]}{\langle P_1(x) \rangle}$$

is a field, viz. the prime field \mathbb{F}_p .

Proposition 11 [20, proposition 3.1.3]

A Galois ring sub-ring is a Galois ring. The Galois ring $GR(p^s, l)$ is a sub-ring of the Galois ring $GR(p^s, m)$ if and only if l divides m .

The notation we are using to indicate that $GR(p^s, l)$ as a sub-ring of $GR(p^s, m)$ is $GR(p^s, l) \subset GR(p^s, m)$. The Galois rings $GR(p^s, l)$ and $GR(p^s, m)$ has the same characteristic p^s . It is necessary to remember that the sub-ring numbers of $GR(p^s, m)$ is the same to the positive divisors of m .

Example

The Galois ring $GR(p^s, m)$ contains the Galois ring \mathbb{Z}_{p^s} as a sub-ring. Also note that

$$\mathbb{Z}_{p^s} = GR(p^s, 1!) \subset GR(p^s, 2!) \subset GR(p^s, 3!) \subset \dots$$

since $n!$ divides $(n + 1)!$ for $n \in \mathbb{N}_1$. For $s = 1$, we have that

$$\mathbb{F}_p = GF(p^{1!}) \subset GF(p^{2!}) \subset GF(p^{3!}) \subset \dots$$

in terms of Galois fields.

Examples of chain rings which are not the Galois rings

Characteristic of the ring $\frac{\mathbb{Z}_2[x]}{\langle x^2 \rangle}$ is 2. The entries of this ring are of the type $a_0 + a_1\alpha$ where a_0 and a_1 belong to \mathbb{Z}_2 . Therefore, they are $0, 1, \alpha, 1 + \alpha$. The table of $+$ and \times for $\frac{\mathbb{Z}_2[x]}{\langle x^2 \rangle}$ are provide by Tables 2 and table 3, respectively. As recently disclosed, the ring $\frac{\mathbb{Z}_2[x]}{\langle x^2 \rangle}$ is not isomorphic to the ring \mathbb{Z}_4 (The two rings have same table of \times , but distinct $+$ table.).

Table 2. Addition in $\frac{\mathbb{Z}_2[x]}{\langle x^2 \rangle}$

+	0	1	α	$1 + \alpha$
0	0	1	α	$1 + \alpha$
1	1	0	$1 + \alpha$	α
α	α	$1 + \alpha$	0	1
$1 + \alpha$	$1 + \alpha$	α	1	0

Table 3. Multiplication in $\frac{\mathbb{Z}_2[x]}{\langle x^2 \rangle}$

\times	0	1	α	$1 + \alpha$
0	0	0	0	0
1	0	1	α	$1 + \alpha$
α	0	α	0	α
$1 + \alpha$	0	$1 + \alpha$	α	1

The set $\{0, \alpha\}$ of the two zero divisors of $\frac{\mathbb{Z}_2[x]}{\langle x^2 \rangle}$ constitutes principal ideal, but this ideal with p prime is not of type p . Therefore, the ring $\frac{\mathbb{Z}_2[x]}{\langle x^2 \rangle}$ is not a Galois ring.

- i. The characteristic of the ring $\frac{\mathbb{Z}_2[x]}{\langle x+x^2 \rangle}$ is 2. The entries of this ring are of the form $0, 1, \alpha, 1 + \alpha$, and the table of $+$ and \times are provided in the form of tables 4 and table 5, respectively. The ring $\frac{\mathbb{Z}_2[x]}{\langle x+x^2 \rangle}$ has a single unit element, two non-trivial ideals ($\{0, \alpha\}$ and $\{0, 1 + \alpha\}$) and three zero divisors ($0, \alpha$ and $1 + \alpha$). The 3 zero divisors should not make up an ideal as $\frac{\mathbb{Z}_2[x]}{\langle x+x^2 \rangle}$ is not a Galois ring.

Table 4. Addition in $\frac{\mathbb{Z}_2[x]}{\langle x+x^2 \rangle}$

+	0	1	α	$1 + \alpha$
0	0	1	α	$1 + \alpha$
1	1	0	$1 + \alpha$	α
α	α	$1 + \alpha$	0	1
$1 + \alpha$	$1 + \alpha$	α	1	0

Table 5. Multiplication in $\frac{\mathbb{Z}_2[x]}{\langle x+x^2 \rangle}$

\times	0	1	α	$1 + \alpha$
0	0	0	0	0
1	0	1	α	$1 + \alpha$
α	0	α	α	0
$1 + \alpha$	0	$1 + \alpha$	0	$1 + \alpha$

Observe that $\frac{\mathbb{Z}_2[x]}{\langle x+x^2 \rangle}$ is neither isomorphic to $\frac{\mathbb{Z}_2[x]}{\langle x^2 \rangle}$ nor to \mathbb{Z}_4 : both the + and \times tables of $\frac{\mathbb{Z}_2[x]}{\langle x+x^2 \rangle}$ differ from those of the ring \mathbb{Z}_4 .

- ii. The ring $\frac{\mathbb{Z}_2[x]}{\langle x+x^3 \rangle}$ is of characteristic $2^1 = 2$. Its contains elements in the form $a_0 + a_1\alpha + a_2\alpha^2$ with $a_0, a_1, a_2 \in \mathbb{Z}_2$, are

$$0, 1, a = \alpha, b = \alpha^2, c = 1 + \alpha, d = 1 + \alpha^2, e = \alpha + \alpha^2, f = 1 + \alpha + \alpha^2$$

Table 6. Addition in $\frac{\mathbb{Z}_2[x]}{\langle x+x^3 \rangle}$

+	0	1	a	b	c	d	e	f
0	0	1	a	b	c	d	e	f
1	1	0	c	d	a	b	f	e
a	a	c	0	e	1	f	b	d
b	b	d	e	0	f	1	a	c
c	c	a	1	f	0	e	d	b
d	d	b	f	1	e	0	c	a
e	e	f	b	a	d	c	0	1
f	f	e	d	c	b	a	1	0

Table 7. Multiplication in $\frac{\mathbb{Z}_2[x]}{\langle x+x^3 \rangle}$

\times	0	1	a	b	c	d	e	f
0	0	0	0	0	0	0	0	0
1	0	1	a	b	c	d	e	f
a	0	a	b	a	e	0	e	b
b	0	b	a	b	e	0	e	a
c	0	c	e	e	d	d	0	d
d	0	d	0	0	d	d	0	d
e	0	e	e	e	0	0	0	e
f	0	f	b	a	c	d	e	1

- iii. A finite (commutative) ring with unity for which the set of zero divisors is $\{0,2,3,4\}$ is the ring \mathbb{Z}_6 . This set doesn't quite represent a \mathbb{Z}_6 ideal. Consequently, \mathbb{Z}_6 is not a Galois ring

1.2.7 Finite commutative chain ring

In [22], if all the ideals form a chain under inclusion for a commutative unital ring then it is called a chain ring. Finite chain rings are exactly local finite rings whose maximal ideal is principal. Particular examples of a broader class of finite commutative rings with identity are the Galois rings and Quasi-Galois rings. Since they are finite and their ideals form a chain under inclusion, such rings are called finite chain rings. In algebraic number theory, these rings appear as quotient rings of rings of integers in computational fields as well as in Pappian-Hjelmslev plane geometry.

Consider just commutative, associative rings with identity. It is easy to see that the radical N is principal and \mathcal{R} is local, i.e., $\frac{\mathcal{R}}{N}$ is a field if and only if \mathcal{R} is a chain ring. ring of integers modulo p^n is an example of such rings, here p is a prime. Another example of chain rings are the rings $\mathcal{R}(p^n, r) = \frac{\mathbb{Z}_{p^n}[x]}{\langle f(x) \rangle}$, where the polynomial $f(x)$ is monic of degree r and irreducible modulo the prime p . After Janusz [38] (and independently Raghavendran [39]) we call this ring a Galois ring of characteristic p^n and rank r . These rings were perhaps first noticed by Krull in 1924 [40]. Note that $GR(p, r) = GF(p^r)$ and $GR(p^n, r)$ is uniquely determined by p, n , and r (see Krull [40, pp. 83ff]).

The following construction can be used to obtain all finite chain rings. Let p be a prime, and the integers $n, r > 0$, and $f(x) \in \mathbb{Z}_{p^n}[x]$ a monic polynomial of degree r whose image in $\mathbb{Z}_p[x]$ is irreducible. Then $GR(p^n, r) = \frac{\mathbb{Z}_{p^n}[x]}{\langle f(x) \rangle}$ is a ring whose structure depends only on p, n , and r . $GR(p^n, r)$ is called a Galois ring of characteristic p^n and rank r [39, 41]. $GR(p^n, r)$ is a local ring whose maximal ideal is $pGR(p^n, r)$. The finite chain rings are of the form

$$\frac{GR(p^n, r)[x]}{\langle g(x), p^{n-1} x^t \rangle} \quad (1)$$

Whereas $g(x) \in GR(p^n, r)[x]$ is an Eisenstein polynomial of degree k , i.e., $g \in x^k - p(a_{k-1}x^{k-1} + \dots + a_0)$ ($a_i \in GR(p^n, r)$ and a_0 is a unit of $GR(p^n, r)$), $t = k$ when $n = 1$, and $1 \leq t \leq k$ when $n \geq 2$. The integers p, n, r, k, t are called the invariants of the chain ring in (1).

The Galois ring $GR(p^n, r)$ is a local ring with maximal ideal $pGR(p^n, r)$ and $\frac{GR(p^n, r)}{pGR(p^n, r)} = GF(p^r)$. Its group of units $GR(p^n, r)^*$ comprises of single cyclic subgroup T^* of order $p^r - 1$.

\mathcal{R} can denote a finite chain ring with a nonzero radical \mathcal{N} in what follows. (If $\mathcal{N} = 0$, then \mathcal{R} is a field, of course.) We now state some chain ring \mathcal{R} facts and will use the notation throughout.

- i. \mathcal{R} has prime power characteristic p^n , i.e., the identity of \mathcal{R} has additive order p^n .
- ii. If the characteristic of \mathcal{R} is p^n , then $\mathcal{R} \cong GR(p^n, r)$, a Galois ring.
- iii. The radical \mathcal{N} is the collection of \mathcal{R} 's nilpotent entities and $\frac{\mathcal{R}}{\mathcal{N}} = GF(p^r)$.
- iv. Let $\theta = \mathcal{N} - \mathcal{N}^2$. Then, $\mathcal{N} = (\theta)$ and every ideal of \mathcal{R} is of the form $\mathcal{N}^i = (\theta^i)$. Hence if m is the index of nilpotency of \mathcal{N} , then for each a in \mathcal{N} , there is a unique nonnegative integer $i < m$ such that $a = u\theta^i$ where u is a unit of \mathcal{R} .
- v. \mathcal{R} contains a unique subring S such that $\frac{S}{pS} \cong \frac{\mathcal{R}}{\mathcal{N}}$. S has radical (p) and (hence) is isomorphic to $GR(p^n, r)$.
- vi. If $\theta = \mathcal{N} - \mathcal{N}^2$, $\mathcal{R} = S \oplus S\theta \oplus \dots \oplus S\theta^{k-1}$ is an S -module direct sum where K is the greatest integer $i < m$ (= index of nilpotency of \mathcal{N}) such that $p \in \mathbb{N}^i$. It follows that $\theta^k = p(a_{k-1}\theta^{k-1} + \dots + a_1\theta + a_0)$, where $a_i \in S$ and a_0 is a unit in S , i.e., θ satisfies the Eisenstein polynomial

$$f(x) = x^k - p(a_{k-1}\theta^{k-1} + \dots + a_1\theta + a_0)$$

If $1, \theta^1, \theta^2, \dots, \theta^{k-1}$ is a basis for \mathcal{R} over S , we call \mathcal{R} an Eisenstein extension of S of degree k . In general, however, there is an integer $t = m - (n-1)k > 0$ such that

$$S\theta^i \cong S \quad \text{if} \quad 0 \leq i < t$$

and

$$S\theta^i \cong \frac{S}{p^{n-1}S} \quad \text{if} \quad k \geq i \geq t$$

In other words

$$\mathcal{R} \cong \frac{S[x]}{\langle f(x), p^{n-1}x^t \rangle}. \quad \text{Conversely, any such quotient ring}$$

is indeed a chain ring (Krull [40, pp. 84-85].

- vii. Consider the units group of \mathcal{R} is represented by \mathcal{R}^* . Obviously, the \mathcal{R}^* includes non-nilpotent entries of \mathcal{R} , i.e., $\mathcal{R}^* = \mathcal{R} - \mathcal{N}$. The subgroup $1 + \mathcal{N}$ of \mathcal{R}^* is a p -group and $\frac{\mathcal{R}^*}{(1 + \mathcal{N})} \cong \left(\frac{\mathcal{R}}{\mathcal{N}}\right)^*$ is of cardinality $p^r - 1$ and also is cyclic. Hence, $\mathcal{R}^* \cong \left(\frac{\mathcal{R}}{\mathcal{N}}\right)^* \times (1 + \mathcal{N})$.
- viii. \mathcal{R} has order p^{mr} , \mathcal{N} has order $p^{(m-1)r}$, and \mathcal{R}^* has order $p^{mr} - p^{(m-1)r}$.
- ix. We call the integers p, n, r, k, t defined above the invariants of \mathcal{R} .

x. $\mathcal{R} = \frac{GR(p^n, r)[x]}{\langle g(x), p^{n-1}x^t \rangle}$ be a finite chain ring.

We list them below for ease.

p^n is the characteristic of \mathcal{R} .

p^r is cardinality of $\frac{\mathcal{R}}{\mathcal{N}}$.

m is the index of nilpotency of \mathcal{N} .

k is the greatest integer $i \leq m$ such that $p \in \mathcal{N}^i$.

$m = (n - 1)k + t, 1 \leq t \leq k$.

Theorem 10

If the total number of finite chain rings is denoted by N having the invariant p, n, r, k, t . And assume that p/k and that either $n > 2$ or $n = 2$ and $t = k$. Then

$$\frac{p^r}{r} \leq N \leq (1 - p^{-r})p^{r(m-k)},$$

where $m = (n - 1)k + t$.

Theorem 11 [42, Theorem 2.1]

Consider the ring

$$\mathcal{R} = \frac{GR(p^n, r)[x] = \mathbb{Z}_{p^n}[w][x]}{\langle f(x) = x^k - p(a_{k-1}\theta^{k-1} + \dots + a_1\theta + a_0), p^{n-1}x^t \rangle} \quad (2)$$

where $f(x)$ is an Eisenstein polynomial (i.e., a_0 is a unit element), $1 \leq t \leq k$ when $n \geq 2$, and $t = k$ when $n = 1$. v is a finite commutative chain ring, and conversely, any finite commutative chain ring is of the form (2).

Lemma 1 [43, lemma 1]

If $n = 1$, then $S = GF(p^r)$ and $\mathcal{R} \cong \frac{S[x]}{\langle x^k \rangle}$.

Proposition 12 [42, proposition 2.3]

Let \mathcal{R} denote the finite commutative chain ring with the parameters in Notation 2.2.

i. The chain of ideals of \mathcal{R} is of the form

$$0 = \langle x^{k(n-1)+t} \rangle \subseteq \langle x^{k(n-1)+t-1} \rangle \subseteq \dots \subseteq \langle x \rangle \subseteq \mathcal{R}$$

Whereas $\langle x^k \rangle = \langle p \rangle$

ii. $|\mathcal{R}| = p^{r(k(n-1)+t)}$ and $|\langle x \rangle| = p^{r(k(n-1)+t-1)}$. Also, $\frac{\mathcal{R}}{\langle x \rangle} \cong \mathbb{F}_{p^r}$.

iii. The largest Galois ring in \mathcal{R} is $GR(p^n, r)[x]$ and it is called the coefficient ring of \mathcal{R} .

A generalize structure of the sequence alphabet to a residue class polynomial ring over Galois field (GF) is given in [10]. Let $w(x)^k$, for $k > 1$, be the k^{th} power of an irreducible polynomial $w(x)$ over GF of degree m . Then, the residue class ring \mathcal{R} of [10] is defined as $\mathcal{R} = \frac{\mathbb{F}_2[x]}{\langle w(x)^k \rangle}$. This generalization provides a large choice of rings to construct frequency hopping sequences. These rings are called commutative chain ring. The ring $\mathcal{R}_n = \frac{\mathbb{F}_2[x]}{\langle x^n \rangle}$ is a special case of \mathcal{R} where $w(x) = x$ and $k = n$. An application of such rings is given in the construction of cyclic codes and Self-Dual codes in [11]. Furthermore, the design of byte based 4×4 S-box from finite commutative chain ring $\mathcal{R}_8 = \frac{\mathbb{F}_2[x]}{\langle x^8 \rangle}$ is initiated by Shah et al. [12] and recently used in [13] for image encryption application.

Some examples of finite chain rings

1. Equation (1) is an example of chain ring.

$$2. \mathcal{R} = \frac{\mathbb{Z}_3[x]}{\langle x^2-3 \rangle}, \mathcal{S} = \frac{\mathbb{Z}_3[x]}{\langle x^2-6 \rangle}$$

Both \mathcal{R} and \mathcal{S} are finite chain rings with invariants $(p, n, r, k, t) = (3, 2, 1, 2, 2)$

3. Galois rings and Quasi-Galois rings.

4. $2\mathbb{Z}_8$

5. $\mathbb{F}_2 + u\mathbb{F}_2$

$$6. \frac{\mathbb{F}_2[u]}{\langle x^k \rangle} \quad 7. \frac{\mathbb{F}_2[u]}{\langle x^k-1 \rangle}$$

1.3 S-box based over chain ring

For the construction of cyclic codes, the finite chain rings of form $\frac{\mathbb{F}_2[x]}{\langle x^k \rangle}$ have recently been used in coding theory. In coding theory, Bonnecaze and Udaya[11] provide the basis for the creation of cyclic and self-dual codes on the chain ring $\mathbb{F}_2 + x\mathbb{F}_2$. Meanwhile numerous code theorist have used these type of rings to design codes, e.g. in [44] constacyclic and cyclic codes are constructed over finite chain ring $\mathbb{F}_2 + x\mathbb{F}_2 + x^2\mathbb{F}_2$, while the construction of cyclic codes over finite chain rings $\mathbb{F}_2 + x\mathbb{F}_2$ and $\mathbb{F}_2 + x\mathbb{F}_2 + x^2\mathbb{F}_2$ is discussed in [45]. The simplex codes over the finite chain ring $\sum_{n=0}^s x^n \mathbb{F}_2$ are investigated in [46], however simplex codes having symbols from four elements chain ring $\mathbb{F}_2 + x\mathbb{F}_2$ are given in [47]. The cyclic codes over chain ring $\mathbb{F}_2 + x\mathbb{F}_2 + x^2\mathbb{F}_2 + \dots + x^{k-1}\mathbb{F}_2$ are addressed in [48], whereas $(1 + x)$ constacyclic and cyclic codes over chain ring $\mathbb{F}_2 + x\mathbb{F}_2$ are presented in [49]. While the linear codes over finite chain ring $\mathbb{F}_2 + x\mathbb{F}_2 + x^2\mathbb{F}_2$ of constant Lee weight are considered in [50]. Though in more general setting, the cyclic codes over finite chain ring

$\mathbb{F}_p + x\mathbb{F}_p + x^2\mathbb{F}_p + \dots + x^{k-1}\mathbb{F}_p$ are introduced in [51], however, ultimately in almost with complete sense, in [52] cyclic codes of arbitrary length are designed over finite chain ring $\mathbb{F}_q + x\mathbb{F}_q + x^2\mathbb{F}_q + \dots + x^{k-1}\mathbb{F}_q$. Also, on negacyclic and constacyclic codes over finite chain rings is given in [53].

In algebra, a function that assume values from a two-element set (usually $\{0,1\}$) as well as the function itself, we call the function a Boolean algebra. The normal succession from the single output Boolean function definition is the expansion of that theory to several Boolean output functions, referred to as an S-box. The relation between the input and the output bits gives rise to different kinds of S-boxes in terms of dimension and exclusivity. An $n \times m$ S-box is a function $\zeta : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ that convert n -bit input to m -bit output, whereas a total of inputs is $2n$ bit and the outputs is $2m$ bit. An S-box is then essentially a set of m -bit Boolean single output functions combined in a structured manner. The dimension of an S-box would have an effect on the distinction between the output and the input that will affect the properties of the S-box. S-box with $n \times m$ dimension will have some repeated values if cryptosystems $n < m$. Whereas, in case if $n = m$, then the S-box may either have unique values or may have a repetition in values. The only possibility that an S-box is reversible is that it has bijection [54]. Since it is the only nonlinear component of an algorithm, therefore it is focused mainly in while designing by researchers. Thus extreme vulnerabilities in the replacement matrices will then take to a weak cryptosystem. To check the power of cryptographic algorithms, the S-boxes are used as a gauging tool. Therefore, in order to secure cryptosystems, the construction of S-boxes must be cryptographically efficient. In literature, multiple constructions and parameters are proposed to synthesize S-boxes. The Rijndael [1] S-box is based on the $x \mapsto x^{-1}$ mapping, where x^{-1} lies in \mathbb{F}_2^8 field and denotes the multiplicative inverse of x . There are many methods in the \mathbb{F}_2^8 field to find the multiplicative inverse. An algorithm is given in [55] by which the measurements of multiplicative inverses in field \mathbb{F}_2^8 are reduced to the finding in field $\mathbb{F}_2^4 = GF(2^4)$ of multiplicative inverses. Adams and Tavares [56] define a construction methodology for strongly nonlinear bijective S-boxes, but an improved construction approach is given in [57] for nonlinear resilient S-boxes.

Let \mathcal{R}_k represents the chain ring $\frac{\mathbb{F}_2[x]}{\langle x^k \rangle} = \mathbb{F}_2 + x\mathbb{F}_2 + x^2\mathbb{F}_2 + \dots + x^{k-1}\mathbb{F}_2$. It contains 2^k elements. Here the polynomial x has nilpotency k i.e. $x^k = 0$. The ascending chain of ideals in \mathcal{R}_k becomes $\langle 0 \rangle = x^k\mathcal{R}_k \subset x^{k-1}\mathcal{R}_k \subset \dots \subset x\mathcal{R}_k \subset \mathcal{R}_k$, and hence \mathcal{R}_k with only maximal ideal $x\mathcal{R}_k$ form a chain ring. One can check easily that the cardinality of $x^{k-1}\mathcal{R}_k$ is double the cardinality of $x^{k-2}\mathcal{R}_k$. In

particular, the chain ring $\mathcal{R}_2 = \frac{\mathbb{F}_2[x]}{\langle x^2 \rangle} = \mathbb{F}_2 + x\mathbb{F}_2$ has the elements $\{0, 1, \alpha, \bar{\alpha} = 1 + \alpha\}$, where $\alpha^2 = 0$, having unit elements $\{1, \bar{\alpha} = 1 + \alpha\}$. The chain ring \mathcal{R}_2 share properties with \mathbb{Z}_4 and \mathbb{F}_4 . The multiplication operation of \mathcal{R}_2 coincides with \mathbb{Z}_4 whereas, the addition operation coincides with \mathbb{F}_4 . The operations of addition and multiplication in \mathcal{R}_2 are given bellow in Tables 8 and Table 9 respectively.

Table 8. Addition in $\mathbb{F}_2 + u\mathbb{F}_2$

\times	0	1	u	\bar{u}
0	0	0	0	0
1	0	1	u	\bar{u}
u	0	u	1	u
\bar{u}	0	\bar{u}	u	0

Table 9. Multiplication in $\mathbb{F}_2 + u\mathbb{F}_2$

+	0	1	\bar{u}	u
0	0	1	\bar{u}	u
1	1	0	u	\bar{u}
\bar{u}	\bar{u}	u	0	1
u	u	\bar{u}	1	0

Using the Chain rings, different S-boxes have been constructed by Shah et al. [12]. These S-boxes are also used for image encryption and watermarking [58].

The ring $\mathcal{R}_8 = \frac{\mathbb{F}_2[x]}{\langle x^8 \rangle} = \mathbb{F}_2 + x\mathbb{F}_2 + x^2\mathbb{F}_2 + \dots + x^7\mathbb{F}_2$ is a commutative chain ring having 2^8 elements. Since the nilpotency of x is 8 therefore, it follows that $\langle 0 \rangle \subset x^7\mathcal{R}_8 \subset x^6\mathcal{R}_8 \subset \dots \subset x\mathcal{R}_8 \subset \mathcal{R}_8$. Moreover, $\frac{\mathcal{R}_8}{x\mathcal{R}_8} \cong \mathbb{F}_2$ is the residue field of \mathcal{R}_8 . It shares some properties with local ring \mathbb{Z}_{2^3} and the Galois field \mathbb{F}_{2^3} . Subsequently, the operation of addition in \mathcal{R}_8 coincides with \mathbb{F}_{2^3} and multiplication with \mathbb{Z}_{2^3} . For instance the copious 8×8 S-boxes in [58] are generated by the elements $1 + x^3 + x^6$ and $1 + x^2 + x^4 + x^5 + x^7$ from the multiplicative group of the chain ring \mathcal{R}_8 . Since these S-boxes are generated by more than one element, therefore, shows more algebraic complexity as compared to other existing S-boxes. Thus these type of S-boxes may replace many existing S-box depending crypto-algorithms to increase their algebraic complexity and hence the algorithms security.

1.4 Motivation and objectives of this thesis

Nowadays, for secure communication, various ciphers are available in the literature. Several of these ciphers are based on the principle of diffusion and confusion given by Shannon [1, 2]. Confusion involves makes the connection between a given cipher key and the corresponding encrypted text complex. However, linking the conversion that spreads the statistical status of a text is termed as

diffusion. S-box is a key non-linear module of an encryption scheme that results confusion in data. Many algorithms are programmed to build this non-linear aspect in modern ciphers to maximize the uncertainty. These assemblies are regularly held in the Galois 2-marked fields, that is why there is a need for change in the algebraic structures. To improve the complex behavior of the S-boxes, the Galois field structure is swapped by a modified structure known as Galois ring. First, the Galois ring get rank in writing when Shankar [59], in 1979, built BCH (Bose–Chaudhuri–Hocquenghem) codes over the local-ring \mathbb{Z}_p^k . Similarly; BCH codes over the commutative rings was compiled by Palazzo and Andrade [7]. This construction is paid equal attention in the subgroups of Galois ring extension of the local ring \mathbb{Z}_p^k . Meanwhile, Sha et al. [9] broadcast the contribution in [7] to a sequence of BCH codes over chain of sequence of Galois rings. Hence, for the determination, a cyclic subgroup taken from unit elements of the Galois ring is considered.

The standard 8-bit look-up table is a matrix of cardinality 16 established over Galois field $GF(2^8)$ and hence therefore, it requires a memory of 8×2^8 bits. The 12×12 S-box constructed over the Galois field $GF(2^{12})$ requires 12×2^{12} bit space and thus requires a large computer memory. Similarly, for a 24 – bit S-box over the Galois field $GF(2^{24})$ requires 24×2^{24} bits space. On the other hand, a lowest cyclic group of Galois ring units was first castoff in [6] for the creation of S-boxes. Design of 4 by 4 S-box over Galois rings $GR(2^2, 2)$ and $GR(2^2, 4)$ are considered and their uses are seen in visual applications. S-boxes of size 4×4 has been designed from chain ring $\frac{\mathbb{F}_2[u]}{\langle u^8 \rangle}$ by Shah et al. in [12] and most lately utilized in [58] to encipher an image. In [60], shah et al. created a 24×24 S-box over Galois ring $GR(2^3, 8)$ but this algorithm fails in the decryption process, as the inverse elements for the S-box do not exist.

The focus of this thesis is on presenting approaches for designing various bit S-boxes of small size by working with algebraic substructures (the chain ring). The construction of bijective Boolean functions on these substructures makes the problem more complex. The new functions are explored to meet the requirement of design criteria related to assessing their strength against linear and differential cryptanalysis. We will give the applications of designed s-boxes in the field information security. Moreover, a comparative analysis of the designed s-boxes with existing optimal 8-bit and 4-bit s-boxes will be presented to validate the presented concept and its positive features. For a better understanding of the motivation and objective of the current research work, a link diagram is plotted in figure 1 which describes the association among the different ciphers.

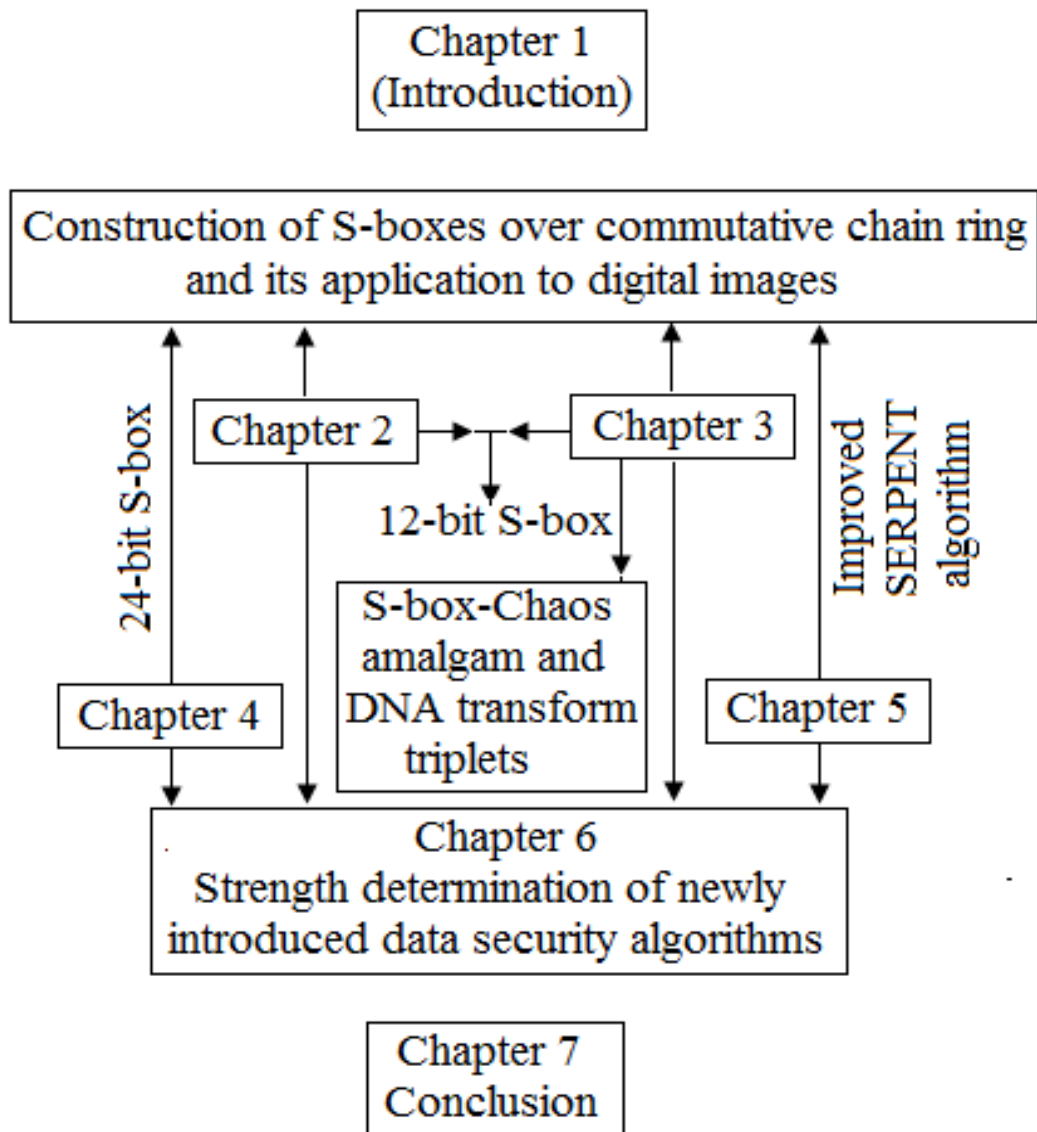


Figure 1. Link diagram of the whole thesis

Chapter 2

Design of 12-bit S-box over chain ring and its application to digital images

An S-box is the main non-linear component of symmetric block cipher that is liable for producing confusion in data. Numerous algorithms are established for the creation of this non-linear component to upsurge confusion in contemporary symmetric ciphers. These assemblies are frequently created on Galois fields with characteristic 2, hence there is a requirement of enhancements and reforms in algebraic structures. Customarily, 8×8 S-box is a 16×16 look up table over Galois field $GF(2^8)$, algebra over the binary field F_2 . A 12×12 S-box over Galois field $GF(2^{12})$ is not effective as it requires large computer memory to be functional for data replacing instead of an 8×8 S-box. To improve the complexity in S-boxes, there is a need of introducing new generalized structures of Galois ring. One of the particular class of Galois ring is the commutative chain ring. The finite commutative chain ring $\frac{\mathbb{F}_2[x]}{\langle x^{12} \rangle}$ is fundamentally an algebra over the binary field \mathbb{F}_2 . In this chapter we considered the advantage and devise a novel method of 12×12 S-box design over the unit elements of finite commutative chain ring $\frac{\mathbb{F}_2[x]}{\langle x^{12} \rangle}$. The newly obtained S-box has greater confusion ability than existing 8×8 S-boxes. To observe this effect, an RGB image encryption application is given. In the proposed encryption scheme, we doubled the bits of 12×12 S-box from 12 to 24 for creating confusion in the data. Consequently, a new method of color image encryption is designed by which 24 binary bits are utilized at the place of byte. Whereas for diffusion we apply the linear permutation $P = (i \times 32) \bmod 257$ and finally bitwise Exclusive-or operation is operationalized. Analysis reveals that the proposed image encryption approach might switch many 8×8 S-box based digital medium enciphering schemes.

2.1 Construction of S-box over chain ring

The key element used in most block ciphers is the S-box. The task is to replace a bunch of input data bits with a totally new output of the same size. So the replacement reveals a misleading relation between a given bits data and an outcome bits data. As used in the iterative round feature, the central aim of an S-box is to increase the intensity necessary to discover a statistical order in the replaced results. S-boxes are capable of securing an encryption algorithm by keeping outstanding encryption

stuffs.

In this chapter, by using the $R_{12} = \frac{F_2[x]}{\langle x^8 \rangle}$, a 12×12 S-box is constructed. Also, the newly developed S-box is used in an image encryption scheme.

2.2 Multiplicative group of chain ring

Till now, the S-boxes constructed with the help of the commutative chain ring $R_8 = \frac{F_2[x]}{\langle x^8 \rangle} = \sum_{i=0}^7 x^i F_2$ have cardinality 16 and each element is represented by a byte. However, in this study, the look-up table comprises 256 elements and each entry is of 12-bits. The generator of the S-box is the subgroup $H_{G_{12}} = \langle 1 + u^4 + u^5 + u^{11}, 1 + u^3, 1 + u + u^2 + u^4 + u^5 + u^{11} \rangle$ of multiplicative group $M_{G_{12}}$ of units of R_{12} and is given in Table 10.

Table 10. Multiplicative Group $M_{G_{12}}$ of units of Chain ring R_{12}

2097	1281	3377	1	9	65	585	2103	1301	155	273	3143	325	555	257	3895
21	2971	17	2887	1093	2347	2489	1137	2041	3337	1345	3913	1209	369	2809	1447
3813	587	2593	2263	1461	3579	2353	679	3045	2379	2849	4055	181	1787	823	1045
1947	1041	1863	69	1323	1025	1079	277	3227	1297	71	1349	3627	3751	4069	1355
3873	983	1205	2811	3121	2471	2789	3659	3617	1239	437	507	2447	3517	1091	2457
3711	2925	883	2313	1679	189	1859	153	383	1645	115	1527	85	1627	1361	3463
5	2283	321	759	1365	3419	1105	2695	1285	1003	2639	765	1155	4057	447	45
4019	2889	1359	4093	1923	1753	3775	3373	3251	2207	2509	19	2857	3695	2077	547
185	1951	1229	787	553	367	1309	291	3175	1957	139	609	3351	2293	827	1393
2919	677	2955	865	2583	3573	2107	3935	2701	1235	361	1455	3933	2787	3833	95
1933	2003	2153	2735	605	2531	2703	1213	2883	1177	3455	621	3187	1033	1423	2493
2115	3481	639	3949	3955	3831	341	347	81	1671	261	4075	1089	2551	1109	2651
337	391	1029	1259	2383	3069	2947	729	703	2349	179	1609	1615	1789	2179	3033
3519	1069	947	2975	205	3859	1577	3439	285	3363	3513	1183	3533	3091	3881	623
3101	3619	1895	1701	1931	1889	1559	2549	1083	113	103	933	3211	1633	279	3317
3899	3167	909	3027	3177	1711	1629	1507	1017	863	3725	2259	1385	2479	2909	1763

2.3 Algorithm for S-box construction

To construct the R_{12} S-box we define two mappings; $f: M_{G_{12}} \rightarrow M_{G_{12}}$ by $f(a) = a^{-1}$ and $g: M_{G_{12}} \rightarrow M_{G_{12}}$ by $g(a) = \beta a$. Thus $(gof)(a) = (\beta a)^{-1}$, where $M_{G_{12}}$ is the multiplicative group of unit elements of the ring R_{12} , and $\beta = 1 + u^3$. Table 11, obtained from $(gof)(H_{G_{12}})$, is the proposed S-box constructed from R_{12} .

Table 11. S-box obtained from Multiplicative Group $M_{G_{12}}$ of units of Chain ring R_{12}

3377	2561	2097	1	585	65	9	2347	1093	2887	17	2971	21	3895	257	555
325	3143	273	155	1301	2103	2809	369	1209	3913	1345	3337	2041	1137	2489	507
437	1239	3617	3659	2789	2471	3121	2811	1205	983	3873	1355	4069	3751	3627	1349
71	1297	3227	277	1079	1025	1323	69	1863	1041	1947	1045	823	1787	181	4055
2849	2379	3045	679	2353	3579	1461	2263	2593	587	3813	1447	3251	3373	3775	1753
923	4093	1359	2889	4019	45	447	4057	1155	765	2639	1003	1285	2695	1105	3419
365	759	321	2283	5	3463	1361	1627	85	1527	115	1645	383	153	1859	189
679	2313	883	2925	3711	2457	1091	3517	2447	1763	2909	2479	1385	2259	3725	863
017	1507	1629	1711	3177	3027	909	3167	3899	3317	279	1633	3211	933	103	113
083	2549	1559	1889	1931	1701	1895	3619	3101	623	3881	3091	3533	1183	3513	3363
285	3439	1577	3859	205	2975	947	1069	3519	3033	2179	1789	1615	1609	179	2349
703	729	2947	3069	2383	1259	1029	391	337	2651	1109	2551	1089	4075	261	1671
81	347	341	3831	3955	3949	639	3481	2115	2493	1423	1033	3187	621	3455	1177
883	1213	2703	2531	605	2735	2153	2003	1933	95	3833	2787	3933	1455	361	1235
701	3935	2107	3573	2583	865	2955	677	2919	1393	827	2293	3351	609	139	1957
175	291	1309	367	553	787	1229	1951	185	547	2077	3695	2857	19	2509	2207

2.4 12-bit chain ring dependent RGB image encryption

An SP-network is a series of mathematical operations linked in a block cipher. Such a network comprises of two operations the substitution and the permutation. This system was devised by Shannon [6] who termed this arrangement a mixing transformation. The work of S-box is to provide confusion in the plain-image/plain-text while the permutation is responsible for diffusion in the output after getting the substitution operation. Due to the weakness of permutation-only cryptosystems against well-known attacks and for the enhancement of security level a significant substitution process is often introduced. Various block ciphers are constructed that uses the process of substitution. These ciphers includes Rijndael algorithm (AES), Serpent Algorithm, TwoFish algorithm, Data encryption standart (DES), Triple DES etc.

The correspondence and storing of RGB digital medium needs cryptography to carry out their confidentiality because of unreliable networks. The implementation of an infrequent form of enciphering for color images based on 12×12 S-box obtained from chain ring R_{12} is one of the fundamental approaches of this section. With the same 8×8 S-box, each layer of an RGB image is treated for the prerequisite of the customary procedures, whereas, three different random sequences from 12×12 S-box are used for each channel of the RGB image in this novel scheme. A linear permutation $P = (i \times 32) \text{ mod } 257$ is added to the replacement result in the next section of diffusion

and then from an exclusive-or operation encrypted image is achieved.

2.4.1 Encryption algorithm

The encryption technique is a little bit different. Firstly, we mapped each entry of R_{12} S-box on a 24-bit vector and then used it for image encryption. Steps of the proposed image encryption scheme is given as under.

- a) Take the proposed 12×12 S-box.
- b) Exclusive-or i^{th} entry with $(i^{th} + 1) \bmod 257$ entry; for $i = 1$ to 256. This process will produce a 2^{nd} table of order 16 having each entry of 12 bit.
- c) Concatenate the two tables to get a 24-bit extended look-up table.
- d) Split the 24-bit extended table to 3 8-bit tables namely the left, middle and right 8-bits.
- e) Take a 256 order RGB image.
- f) Separate its red, green and blue Layers.
- g) Make substitution of red, green and blue channel with Left, Middle and Right Sequence respectively.
- h) Apply the linear permutation $P = (i \times 32) \bmod 257$
- i) Exclusive-or the results with Left, Right, and middle sequence
- j) Replace with pixels of image.
- k) Combine the three encrypted layers to get the encrypted image.

The presented scheme for encryption of an image is given in figure 2. The enciphered images using this scheme is given in figure 3

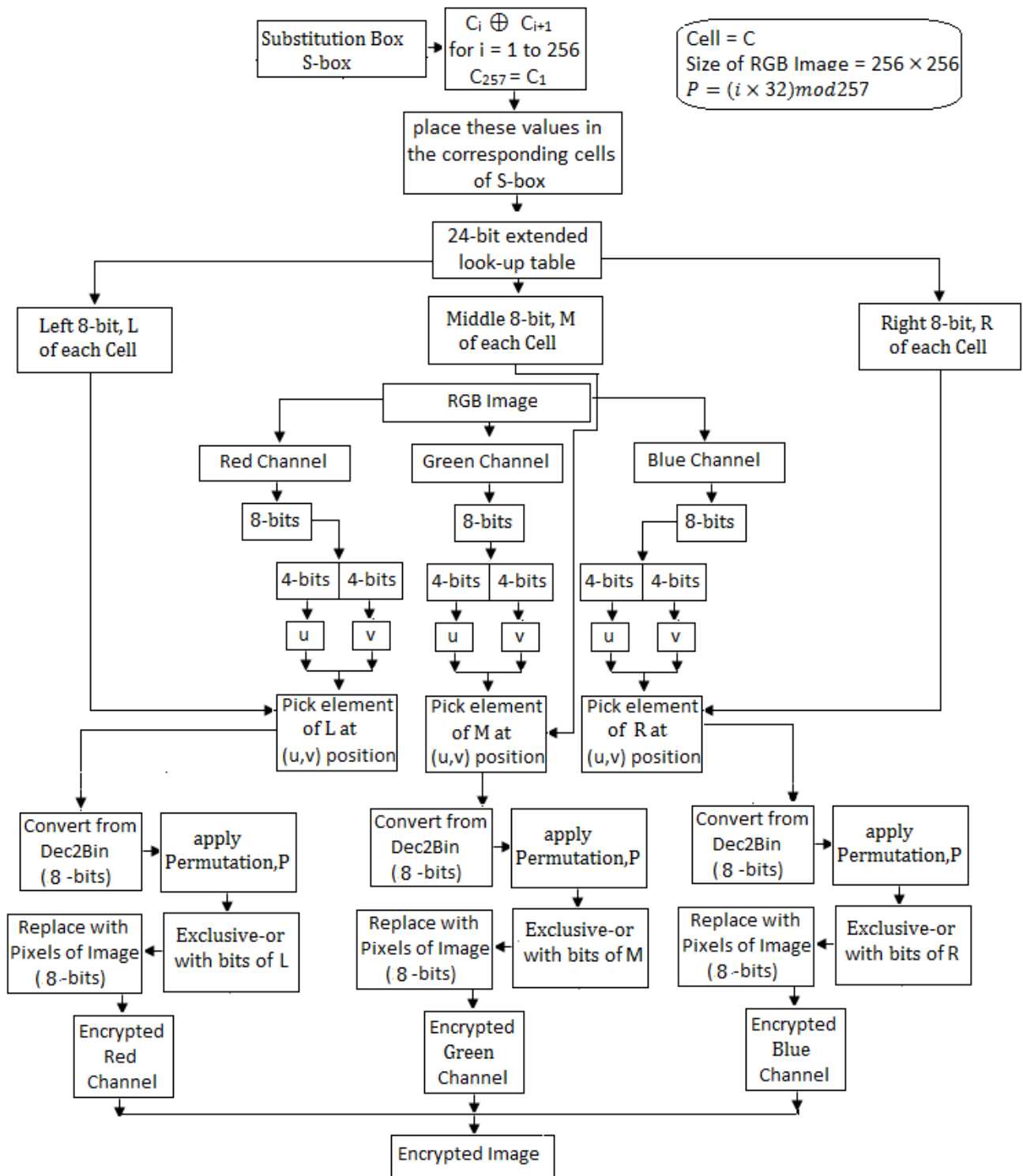


Figure 2. Flow chart of 12×12 S-box dependent color image encryption

2.4.2 Decryption algorithm

The decryption algorithm of the proposed work follows the following steps:

- a) Take the proposed 12×12 S-box.
- b) Exclusive-or i^{th} entry with $(i^{th} + 1) \bmod 257$ entry; for $i = 1$ to 256. This process will produce a 2^{nd} table of order 16 having each entry of 12 bit.
- c) Concatenate the two tables to get a 24-bit extended look-up table.
- d) Split the 24-bit extended table to 3 8-bit tables namely the left, middle and right 8-bits.
- e) Take the encrypted image.
- f) Separate its red, green and blue Layers.
- g) Exclusive-or the results with Left, Right, and middle sequence
- h) apply the inverse linear permutation $P^{-1} = (i \times 8) \bmod 257$
- i) since the S-box contain elements of multiplicative group of chain ring therefore inverse exist. Take inverse tables of Left, Middle and Right Sequence and make its substitution in red, green and blue channel respectively.
- j) Replace with pixels of image.

Combine the three decrypted layers to get the original image.

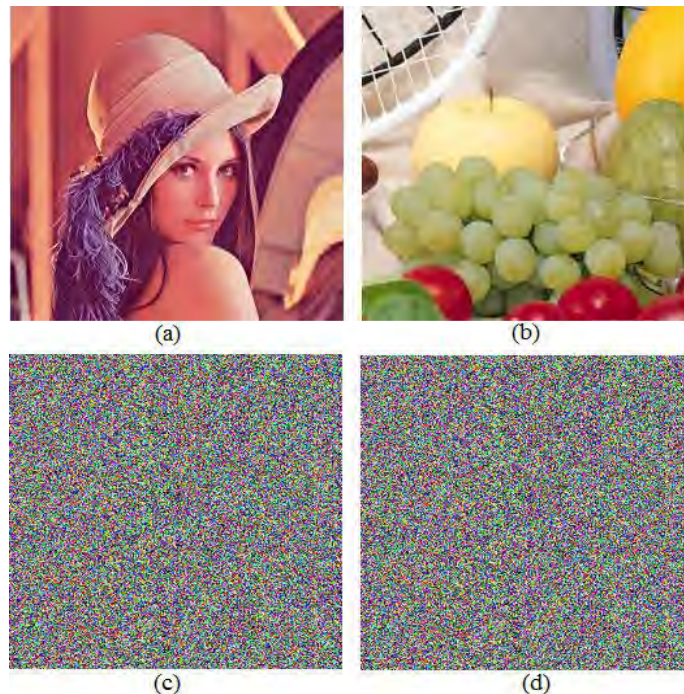


Figure 3. Lena and fruits original images and there corresponding ciphered images

Chapter 3

Chain ring-chaos amalgam and DNA transform: A functionality in multiple image encryption

The pretended fundamental aspects of digital medium such as high redundancy, bulk data capacity and strong correlation among nearby pixels weaken the text encryption algorithms for image encryption purposes. To overcome this deficit, many encryption schemes have been developed by cryptographers. Among the current state-of-the-art for image encryption approaches extensively used SP-Network includes; algebra-based S-box design, chaotic systems and DNA transform. However, the algebra-based structure (S-boxes) are valued because of their high non-linear behavior. But since these S-boxes uses a single generator for its construction thus they gave birth to a less complex algebraic structure and thus, seldom, unsecure encryption algorithm.

On the other hand, chaos and DNA based image encryption algorithms are widely used for secure digital image communication. These two notions play a prominent role in application point of view in different fields like Physics, Biology, Engineering and technology, etc. They are used to create diffusion in data. Not only diffusion but also an arithmetic way of creating confusion is available by using these two concepts [26]. The only drawback of this concept is its low non-linear behavior. However, in parallel, there are many positive aspects like ergodicity, mixing, highly sensitive dependence on initial conditions and management parameter, unpredictability, random-like behavior of output etc., that are analogous to the confusion and diffusion properties of Claude Shannon [6] which strengthen the concept of Chaos and DNA based encryption methodologies.

This section suggests a novel color multiple image encryption scheme using “Algebra-Chaos Amalgamated 256-length-12-bit random sequence” and DNA Transform. The proposed random sequence (S-box) has the property of occupying small computer memory space as regards to the existing S-boxes. Moreover, for simplicity and novelty, 1D sin chaotic map and 1D logistic map are mixed to create a new 1D mixed chaotic map. Initially, a 12×12 (256-length-12-bit) S-box is designed by the unit elements of a chain ring, and then it is mixed with the 1-D mixed chaotic map that results triplets T_1, T_2 and T_3 of high random behavior. A multiple digital image encryption is performed by using the triplet for substitution-permutation along with DNA transform. The proposed

image encryption technique enhances key-space size. Moreover, the arisen investigational data show that the proposed technique of encryption for digital medium has extra ordinary resistance against the well-known attacks.

3.1 Generation of random sequences using chaos and chain ring-based S-box

One of the main roles of S-box is the creation of data confusion. It plays a role of non-linear component in many symmetric block ciphers like in [1]. The S-box is a lookup table that takes one value as an input and returns a new value, different from the input value, as an output. Thus, the replacement spectacles a disorder link between a given data and a received data. It enhances the strength of a cipher against many statistical attacks like differential attacks. An S-box has the admirable property of offering shielding to an algorithm with strong encryption stuffs.

In this study a 12×12 S-box is generated from the element of multiplicative group of commutative chain ring $R_{12} = \frac{\mathbb{F}_2[x]}{\langle x^{12} \rangle}$. Also, a 1D mixed chaotic map is defined. Furthermore, 3 byte based random sequences are generated from the proposed S-box by mixing it with 1D mixed chaotic map. Moreover, to fix rank of the newly designed sequences, a block of standard color images is encrypted in parallel with DNA transform. The analysis result shows that the proposed scheme has extraordinary resistance against all the well-known attacks.

3.2 S-box construction algorithm using 12-bit chain ring

Many standard S-boxes are developed using the algebraic structure of Galois field (see [61]). Some S-boxes are also constructed with the help of chaotic maps (see [62]). Recently, byte based 4×4 S-boxes has also been constructed over commutative chain ring $\frac{GF(q)[x]}{\langle x^k \rangle} = \sum_{i=0}^{k-1} x^i GF(q)$ [18] which develop a new era of S-boxes. Their application can be seen in image encryption and watermarking techniques [12]. However, in this study, a 12-bit entries S-box is constructed with cardinality 256. We found 3 generators that form a subgroup $H_{G_{12}}$, having order 256, of the multiplicative group $M_{G_{12}}$ of chain ring R_{12} . Where,

$$R_{12} = \frac{\mathbb{F}_2[x]}{\langle x^{12} \rangle} \quad (3)$$

These 3 generators are:

$$\langle 1 + u + u^2 + u^3 + u^4 + u^5 + u^6 + u^7 + u^8 + u^9 + u^{10} + u^{11}, 1 + u^4 + u^5 + u^8, 1 + u^5 + u^7 + u^9 + u^{10} + u^{11} \rangle$$

For the S-box construction purpose, we define two mappings $f: H_{G_{12}} \rightarrow H_{G_{12}}$ by:

$$f(a) = a^{-1} \tag{4}$$

and $g: H_{G_{12}} \rightarrow H_{G_{12}}$ by the equation:

$$g(a) = \beta a \tag{5}$$

Where $a \in H_{G_{12}}$ and $\beta=1010100011 \in H_{G_{12}}$. In polynomial form $\beta = 1 + u^2 + u^4 + u^8 + u^9 = 49$.

Thus,

$$(gof)(a) = (\beta a)^{-1} \tag{6}$$

generates the proposed S-box. Table 12 is the proposed S-box obtained from the composition gof .

Table 12. The proposed S-box obtained from the elements of multiplicative group of commutative chain ring

1045	3135	1089	3267	1349	4047	81	243	277	831	1345	4035	69	207	337	1011
3747	3315	419	2579	4083	1023	997	1301	741	3637	21	2613	1071	3903	1839	607
63	3679	3185	321	2417	1761	65	737	1171	963	2963	2851	195	1827	3509	1093
3253	3429	325	2405	1759	3279	1503	1967	975	2991	2913	1361	3681	2289	1105	3313
3491	675	2323	1299	1765	2021	2869	3893	2863	2095	3423	351	3441	2161	2017	993
1939	2195	2083	1059	2229	2485	2149	3173	2527	2783	2223	1199	2657	3937	2545	3569
1	2371	1073	1169	1281	1603	3155	3843	2757	851	4067	3	3013	435	227	3075
4037	83	771	995	3507	3299	3781	1269	261	3919	1525	5	3151	37	725	293
1029	79	245	1285	847	1061	1749	1317	3359	2555	783	465	3615	15	1233	111
1919	879	3087	209	287	3855	1489	3183	2943	3951	1825	1297	627	545	17	3443
177	2433	1457	1041	371	801	273	3699	1201	3457	2403	3891	1685	1635	51	1941
467	2691	3795	3123	917	1379	819	661	3539	1667	723	2981	341	3007	2725	85
2239	629	3973	885	1109	1215	4005	1365	1983	1653	2949	1909	3311	3265	4079	255
2497	1695	143	1439	3327	3521	239	4095	2241	2719	3215	2463	1329	1025	1347	49
257	2627	2977	401	3745	4001	1425	1555	2721	3923	691	3763	501	2005	981	543
2175	1151	1569	2177	433	2659	2435	1411	3749	2693	3717	1007	3983	911	305	145

3.3 1D mixed chaotic map

1D logistic map and sin chaotic map are famous simple chaotic equation with a high complex chaotic behavior. These two equations are mixed to get a low dimension chaotic map. The general equation of 1D mixed chaotic map is:

$$x_{n+1} = \alpha \sin(x_n(1 - x_n)) \tag{7}$$

Where α is a control parameter and its value lie in $(0, 4]$. The x_0 is the initial value taken from the unit interval $[0,1]$, whereas x_{n+1} are the scattered output values.

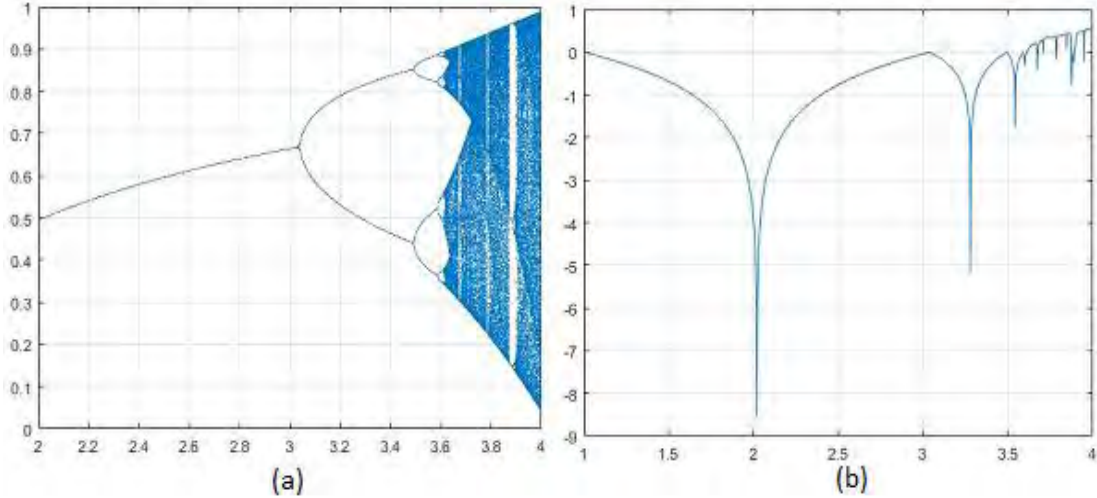


Figure 4. (a) and (b) are the bifurcation and Lyapunov exponent diagram (resp.) of 1D mixed logistic map.

The confirmation of a chaotic behavior can be estimated from the bifurcation diagram and Lyapunov exponent. The diagrams of these two notions are given in fig. 4(a) and 4(b). There are two main drawbacks of the 1D chaotic maps i.e. short limit of the chaotic range $[3.57,4]$ and non-chaotic behavior of the parameter α . This can be verified by the diagram of Lyapunov exponent in fig.4 (b). The quantitative evaluation of a chaotic performance is measure by its Lyapunov exponent. A positive value of Lyapunov exponent shows that the system is chaotic and a larger positive value represents better chaotic performance. As shown in fig. 4. (b), for $\alpha < 3.57$ the Lyapunov exponents of the logistic map is less than zero which shows a non-chaotic behavior. However, the results are in non-uniform structure obtained from the chaotic sequences. As shown in fig. 4. (a), the output range of the logistic sequence is within $[0,1]$ and shows a non-uniform distribution. In the encryption technique, the generated chaotic sequences are mixed with the proposed S-box random sequences that enlarge the key-space. As a result, the 1D logistic map achieve the goal of a large key-space size. i.e. greater than 2^{100} .

Mixing (mixing strategy is given in points of section 4) the proposed S-box obtained from commutative chain ring with 1D mixed chaotic map gives birth to triplet T_1, T_2 and T_3 . These triplets are random sequences (entries ranging 0-255 in decimal) given in Table 13-15.

Table 13. Triplet T_1

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

Table 14. Triplet T_2

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

Table 15. Triplet T_3

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

3.4 Proposed multiple image encryption

Nowadays, Asymmetric cryptography is one of the key approaches of protecting data. Nevertheless, A symmetric algorithm called Advanced encryption algorithm is used as a standard. These algorithms are valued because they are fast comparatively. One of the key components of these ciphers is S-box. The S-boxes are focused because they produce non linearity in a symmetric cipher. This distinct feature makes an algorithm secure against various cryptanalysis attacks and fast-growing computer technologies. An S-box can be constructed in different ways i.e. by using Galois field or chaotic maps etc. Till now, the strongest constructed S-box has non-linearity 112. The upper bond of the non-linearity is 120. Shah et al. constructed many such S-boxes having non-linearity 112 and gives their practical applications see [63]. Nowadays, Small S-boxes have been constructed using elements of chain ring. In this paper, a novel method for constructing 12×12 S-box from Chain ring is given. Furthermore, a triplet (3 random sequences) of 8×8 S-boxes is generated using the proposed S-box and Chaotic sequences. In addition, theses 3 random sequences are used in parallel with DNA transforms in an RGB image encryption scheme and overcome with outshine results.

Image encryption is considered to be a shield against the online communications fears of images. One aim of the paper is to explore the idea of image encryption using chain ring and chaotic-map based triplet and DNA sequences. The procedure of the proposed scheme given as under:

1. Convert the 12×12 S-box to binary.
2. Split each 12-bit vector of the proposed S-box to three 8-bit vectors i.e. 1 to 8 bit, 3 to 10-bit and 5 to 12-bit portion to construct 3 matrices M_1, M_2 and M_3 each of order 16×16 .
3. Originate Chaotic sequence (Seq) of order 256×256 . Extend and Squeeze values of Seq in the range 0-255 by using the equations:

$$R_1 = [Seq \times 65536](mod256)$$

Make sub-blocks of R_1 of size 16×16 .

4. Take unique integers after Multiplying M_1 with each block of R_1 under modulo 256. This will be the first Triplet, T_1 . Similarly, we can get Triplet, T_2 and Triplet, T_3 by using M_2 and M_3 respectively.
5. In image encryption, First use the DNA sequences randomly and then make substitution-permutation on red, green and blue channels respectively of RGB image using the Triplet T_1, T_2 and T_3 .

Fig. 5 represents the flow chart of the proposed color image encryption scheme. Whereas, Fig. 6. is the original and encrypted multiple images using the proposed scheme.

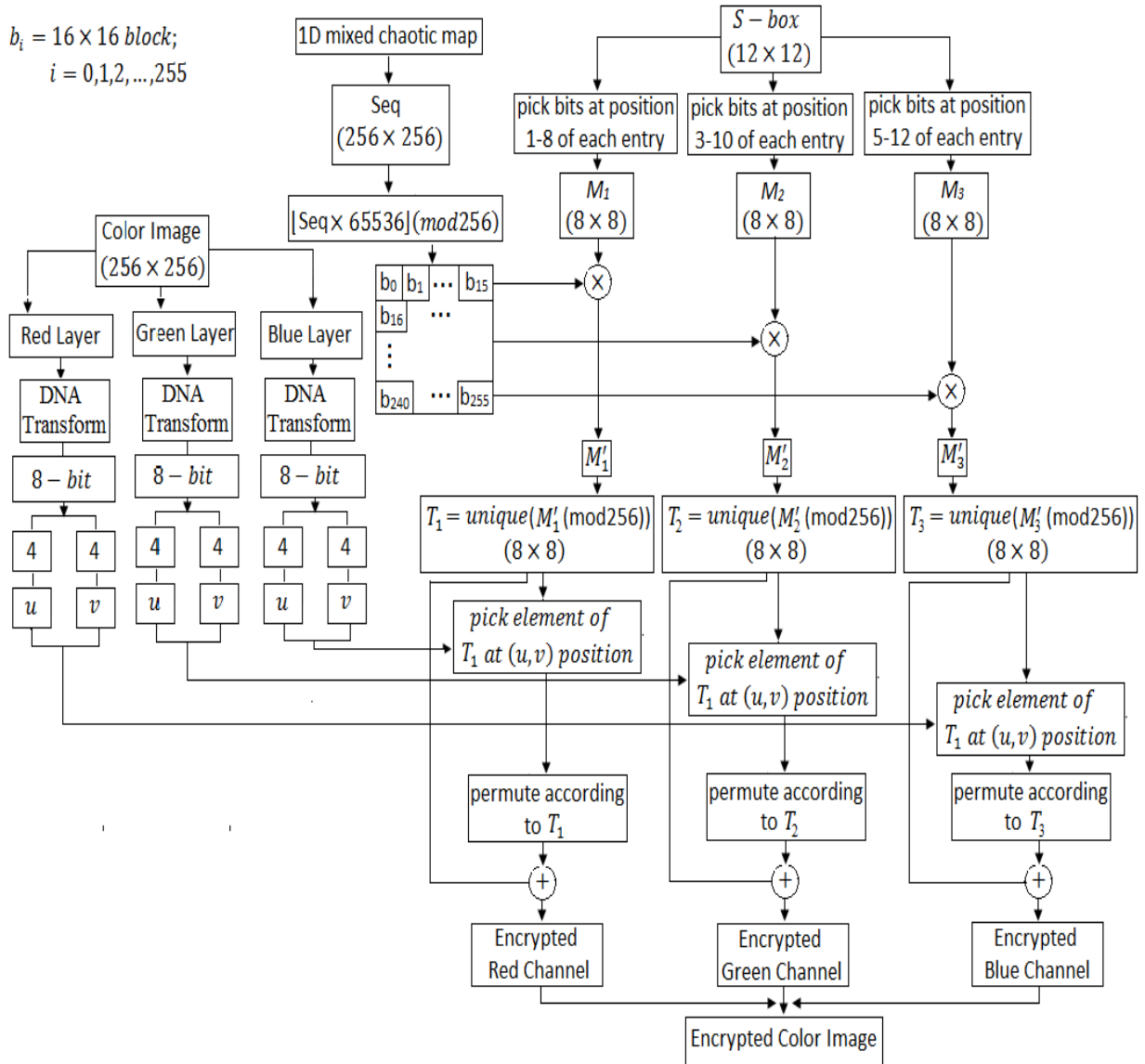


Figure 5. RGB multiple image encryption scheme using Algebraic-Chaotic Triplet and DNA sequences

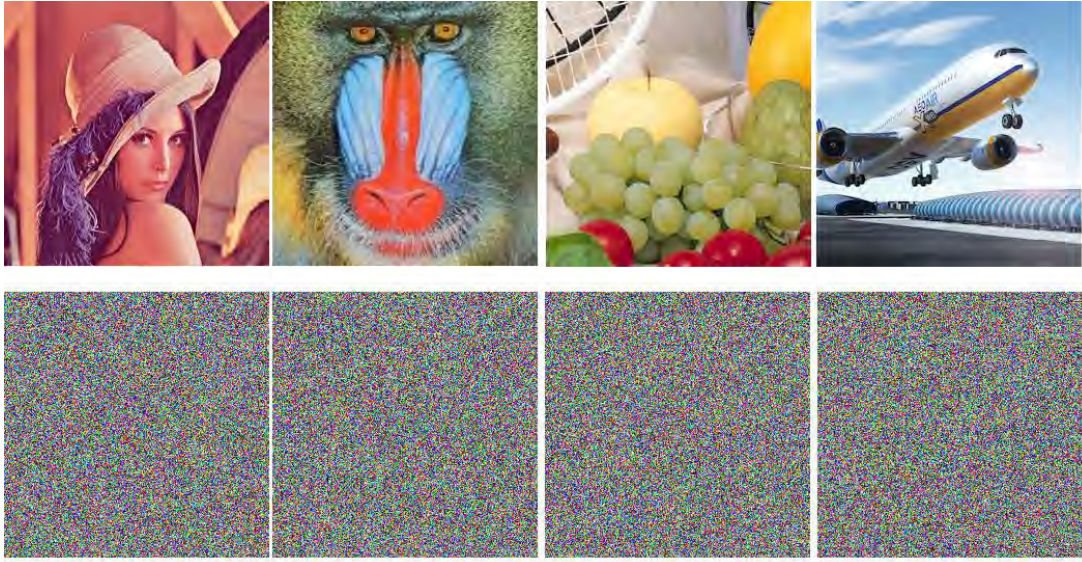


Figure 6. Lena, Baboon, Fruits and Aeroplane original images and there corresponding encrypted images

Chapter 4

Design of 24-bit replacement-matrix over chain ring: An encryption application to astronomical visual

In this new era, millions online secret and confidential communications happens every single day. The information may include images, text and videos. Therefore, cyber-security fears are rising so fast that a need of information safety, network security and data protection systems in computer systems from illegal persons has been observed. Daytime cryptology and IT security procedures are often established on mathematical thinking and on the application of computer science. Thus, to defeat such mathematical thinking, there is a need of secure cryptographically mathematical structures. For this purpose, various algorithms based over Galois field S-boxes have been developed by the cryptographers. Typically, they introduced 8×8 S-box over Galois field. These S-boxes are square matrix of order 16 designed having algebra over the binary field F_2 . But since these algorithms uses a single generator to construct the whole S-box, thus is therefore not much secure. Moreover, in case of these S-boxes, an n -bit vector length requires $n \times 2^n$ bit computer memory. In particular, a 24×24 S-box over $GF(2^{24})$ requires 24×2^{24} bit computer memory. Thus, designing S-box of vector length greater than 8-bit produces an infeasibility of the computer memory.

Thus to overcome these difficulties, the unit elements of finite commutative chain ring is considered. As the finite commutative chain ring is primarily algebra over F_2 so we take the benefit and establish a new scheme of 24-by-24-replacement-matrix (Customarily known as an 24×24 S-box) design over commutative chain ring of the form $\frac{\mathbb{F}_2[u]}{\langle u^{24} \rangle}$ that holds 24×2^8 computer memory calls. Also, the proposed S-box is generated by 2 elements of chain ring and hence gives additional algebraic complexity to the replacement structure. The designed S-box shows high confusion ability than any customarily S-boxes. To gauge this effect, various digital astronomical RGB images are encrypted and the results are analyzed. In the planed ciphering scheme, firstly, we extract different layers of a color astronomical image and then concatenate the layers to form a 256×256 matrix having each entry of 24-bits. Thus, a novel method of RGB image ciphering scheme is functionalized that use 24 binary bits instead of 8 bits. Diffusion is attained by applying the linear permutation $P = (i \times 32) \bmod 257$ and finally, an operation of bitwise Exclusive-or is performed. Thus, the results of

analysis guarantees that the suggested encryption scheme approach to the peak values and may replace many S-box based image encryption techniques.

4.1 24-by-24-replacement-matrix generation over chain ring

An S-box is the most important tool used in block ciphers. Its function is to insert bits into the input data of the same size but different collection. So that installation shows an integrated connection between the input data and the output data. The main purpose of an S-box is to strengthen the power essential for the detection of any mathematical pattern in protected information. S-boxes are capable of providing protected encryption algorithm by capturing the best encryption tools.

Here, we build a 24×24 S-box over \mathcal{R}_{24} . The built-in S-box is used to encrypt the image.

4.1.1 Multiplicative group of chain ring

To date, S-boxes have been constructed with the help of the chain ring $R_{24} = \frac{F_2[u]}{\langle u^{24} \rangle} = \sum_{i=0}^{23} u^i F_2$ has cardinality 256 and vector length 24-bit. However, here, the S-box is made up of 256 entries having 24-bit size of each vector. The look-up table is generated by the subgroup $H_{G_{24}} = \langle 259, 1677721 \rangle = \langle 1 + u^7 + u^8, 1 + u + u^4 + u^5 + u^8 + u^9 + u^{12} + u^{13} + u^{16} + u^{17} + u^{20} \rangle$ of multiplicative group $M_{G_{24}}$ of units of R_{24} and its entries are shown in Table 16.

4.1.2 Construction of S-box

S-box is a key non-linear module of an encryption scheme that results confusion in data. Many ciphers are designed for the assembly of this non-linear component to enhance confusion block ciphers especially the symmetric block ciphers. 4×4 S-box, with entries in bytes, over the unit elements of commutative chain ring were first constructed in [12]. In this section, a 24×24 S-box is constructed over units of commutative chain ring. For the construction purpose of \mathcal{R}_{24} S-box we take the mappings; $f: M_{G_{24}} \rightarrow M_{G_{24}}$ and $g: M_{G_{24}} \rightarrow M_{G_{24}}$ defined by $f(a) = a^{-1}$ and $g(a) = \beta a$ respectively. Thus, $(gof)(a) = (\beta a)^{-1}$, where $M_{G_{24}}$ is the multiplicative group of unit elements of the ring R_{24} , and $\beta = 1682175 = 1 + u + u^4 + u^5 + u^7 + u^9 + u^{11} + u^{13} + u^{14} + u^{15} + u^{16} + u^{17} + u^{18} + u^{19} + u^{20}$. Table 17 obtained from $(gof)(H_{G_{24}})$, is the suggested look-up table generated over the chain ring R_{24} .

Table 16. Chain ring R_{24} multiplicative Group $M_{G_{24}}$

3355563	6750205	5569799	9	2331	589869	1781111	153	39083	1639165	2750983	2313	594459	601389	3562103	39321
1586091	1835005	5504263	589833	1771803	2359341	7089527	1638553	2857131	6554365	3078663	592137	1184283	2370861	4282999	1677721
164547	345157	4950479	5592401	2797299	5308437	7542079	65	16835	4260165	4343503	1105	286195	5313813	6695487	16705
4293315	4211781	297423	283985	5877491	4456469	4986175	4259905	4407747	262469	870095	5309521	7822835	4461845	5843519	4276545
5091947	6602173	1080263	4934473	1479899	3106413	1558455	8388569	8378731	5832893	7060679	585	151515	4787053	5271735	9945
2536043	5881277	5733319	150345	5084379	4351597	2148279	2555865	1366379	6553789	2931911	4784713	5853147	2362221	6779063	5842649
1257731	282629	6092047	1052689	2105651	4280405	1287679	1118465	2241027	5526789	2750991	273	70195	1115477	3562239	4097
1061123	86021	5502223	69649	1253683	1331285	7120383	1052929	2175491	5330181	2554383	1114385	3281459	4457813	4807423	69633
2261931	6565885	232711	626697	702747	2543661	3890551	1085593	2173099	4969213	952839	1677577	3383835	7798061	6695543	2457
623531	1650685	298247	36873	1161499	774189	5004663	626841	665771	3592957	625159	1087753	2662939	6028589	1124983	1640857
7189187	267333	1604047	5326161	3579635	4542485	2090303	4526145	6255043	1069381	6403791	1315921	2649587	1393941	8051263	5591361
3060419	4265029	5732815	17745	4562675	5263381	2155839	266305	1864131	5591365	3061455	4527185	5991923	17685	4577855	1331521
619	159165	7015367	3595081	9435	2405997	6010807	5992409	158059	7327933	6343879	7180873	2424795	1235821	7078071	3454681
7012971	4156861	2886599	8379209	5973211	4830829	7124919	159705	6908267	5427389	2608327	2396745	8388571	8379245	5963959	7190233
259	65541	197903	17	4403	1114197	3364351	257	66051	66821	395791	4369	1122867	1135957	6728447	65537
196867	262149	787727	1114129	3346739	4456533	5002751	65793	131587	263429	592399	1118481	2236979	4478293	1682175	1

Table 17. S-box generated from Multiplicative Group $M_{G_{24}}$ of units of Chain ring R_{24}

1677721	39321	4276545	16705	5842649	9945	69633	4097	1640857	2457	1331521	5591361	7190233	3454681	1	65537
3355563	1586091	164547	4293315	5091947	2536043	1257731	1061123	2261931	623531	7189187	3060419	619	7012971	259	196867
6750205	1835005	345157	4211781	6602173	5881277	282629	86021	6565885	1650685	267333	4265029	159165	4156861	65541	262149
5569799	5504263	4950479	297423	1080263	5733319	6092047	5502223	232711	298247	1604047	5732815	7015367	2886599	197903	787727
9	589833	5592401	283985	4934473	150345	1052689	69649	626697	36873	5326161	17745	3595081	8379209	17	1114129
2331	1771803	2797299	5877491	1479899	5084379	2105651	1253683	702747	1161499	3579635	4562675	9435	5973211	4403	3346739
589869	2359341	5308437	4456469	3106413	4351597	4280405	1331285	2543661	774189	4542485	5263381	2405997	4830829	1114197	4456533
1781111	7089527	7542079	4986175	1558455	2148279	1287679	7120383	3890551	5004663	2090303	2155839	6010807	7124919	3364351	5002751
153	1638553	65	4259905	8388569	2555865	1118465	1052929	1085593	626841	4526145	266305	5992409	159705	257	65793
39083	2857131	16835	4407747	8378731	1366379	2241027	2175491	2173099	665771	6255043	1864131	158059	6908267	66051	131587
1639165	6554365	4260165	262469	5832893	6553789	5526789	5330181	4969213	3592957	1069381	5591365	7327933	5427389	66821	263429
2750983	3078663	4343503	870095	7060679	2931911	2750991	2554383	952839	625159	6403791	3061455	6343879	2608327	395791	592399
2313	592137	1105	5309521	585	4784713	273	1114385	1677577	1087753	1315921	4527185	7180873	2396745	4369	1118481
594459	1184283	286195	7822835	151515	5853147	70195	3281459	3383835	2662939	2649587	5991923	2424795	8388571	1122867	2236979
601389	2370861	5313813	4461845	4787053	2362221	1115477	4457813	7798061	6028589	1393941	17685	1235821	8379245	1135957	4478293
3562103	4282999	6695487	5843519	5271735	6779063	3562239	4807423	6695543	1124983	8051263	4577855	7078071	5963959	6728447	1682175

4.2 24-bit chain ring dependent astronomical RGB image encryption

The Substitution Permutation network (SPN) is a connection of mathematical functions connected in a cipher. This system consists of two functions namely permutation & substitution. This arrangement was developed by Shannon [6], called mixed transformation. The function of an S-box is to offers strong confusion in a digital medium while permutation overlooks the diffusion effect. As the permutation-only ciphering schemes are weak against known attacks, and also due to the development in the security threats, a major super strengthen algorithm for encryption is often introduced.

Because of the insecurity in transmission channels, the sharing of astronomical digital color images requires enciphering by adopting a secure system. One of the key conclusions of this work is the creation of a ciphering scheme for digital images based on a 24×24 S-box set over chain ring R_{24} . In literature, an enciphering scheme for each layer of a color image is provided by using an 8×8 S-box, however in this work all the 3 layers are combined and is followed by a random sequence of size 24×24 . Next in diffusion section, a linear permutation $P = (i \times 32) \bmod 257$ on the replacement outcome is functionalized to achieve the encrypted image.

4.2.1 Encryption algorithm

The following steps are used to perform encryption using the proposed scheme.

- l) Generate the 24×24 look-up table.
- m) Take an RGB image of order 256.
- n) Split the image into its red, green and blue layers. This results 3 different collection of bytes.
- o) Concatenate the bytes of the 3 layers in their corresponding cells to form 24-bit matrix of dimension 256×256 .
- p) Split the new matrix to submatrices of order 16.
- q) Apply the chain ring-based S-box on each submatrix.
- r) Operate the linear permutation $P = (i \times 32) \bmod 257$.
- s) Exclusive-or the results with the proposed S-box.
- t) Split the 24-bits to 8-bit three vectors that represent the different layer respectively.
- u) Exchange pixels with its corresponding bytes.
- v) Reconstruct the encrypted channel to achieve the desired encrypted image.

Illustration:

- 1) Let the S-box: $S = \begin{bmatrix} 1677721 & 39321 \\ 3355563 & 1586091 \end{bmatrix}$
 $= \begin{bmatrix} 000110011001100110011001 & 000000001001100110011001 \\ 001100110011001110101011 & 000110000011001110101011 \end{bmatrix}$
- 2) And consider the image:
Let "I" be is a color image with R, G and B layers such that:
Red channel, $R = \begin{bmatrix} 131 & 43 \\ 55 & 122 \end{bmatrix} = \begin{bmatrix} 10000011 & 00100011 \\ 00110111 & 01111010 \end{bmatrix}$
Green channel, $G = \begin{bmatrix} 31 & 4 \\ 135 & 12 \end{bmatrix} = \begin{bmatrix} 00011111 & 00000100 \\ 10000111 & 00001100 \end{bmatrix}$
Blue channel, $B = \begin{bmatrix} 11 & 83 \\ 85 & 222 \end{bmatrix} = \begin{bmatrix} 00001011 & 01010011 \\ 01010101 & 11011110 \end{bmatrix}$
- 3) Concatenate bytes of R, G and B in their corresponding cells to form 24-bit image i.e.
Concatenate image, $C = \begin{bmatrix} 100000110001111100001011 & 001000110000010001010011 \\ 001101111000011101010101 & 011110100000110011011110 \end{bmatrix}$
- 4) Apply S-box on C by using the operations of chain ring we get:
 $C' = \begin{bmatrix} 100000110001111100001011 & 001000110000010001010011 \\ 001101111000011101010101 & 011110100000110011011110 \end{bmatrix}$
- 5) Apply permutation on C' .
- 6) Now exclusive-or the S-box with the result of step 5.
- 7) Split each 24-bit vector to 8-bit vectors that results the R, G and B encrypted channels of the plain digital image.
- 8) Combine these layers to get the enciphered digital RGB image.

Figure 7 reveals the flow chart of the presented scheme. Figure 8 represents various original images and there corresponding enciphered images using the proposed technique.

4.2.2 Decryption algorithm

In the decryption process, we moves in the reverse direction. First, split the encrypted image into its different layers and combined them to a matrix of order 256. Split the matrix into submatrices of order 16 and exclusive-or the proposed S-box. After that, apply the inverse permutation followed by substitution from chain ring based S-box. Finally, combine the submatrices and split each entry into 8-bit three vectors that will gives the deciphered channels of the image.

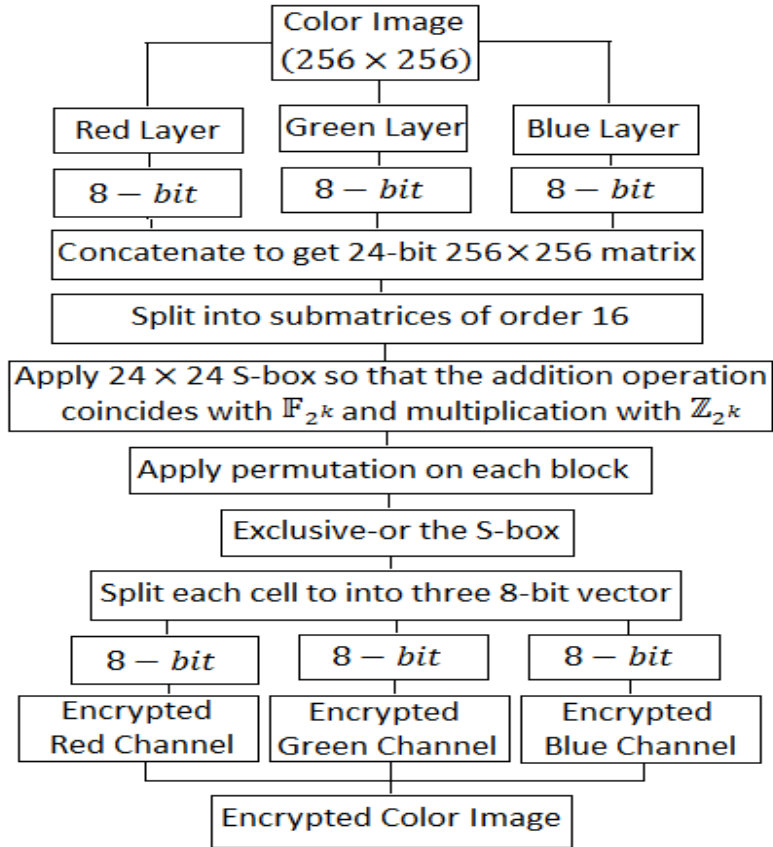


Figure 7: RGB image encryption scheme using the proposed 24×24 S-box

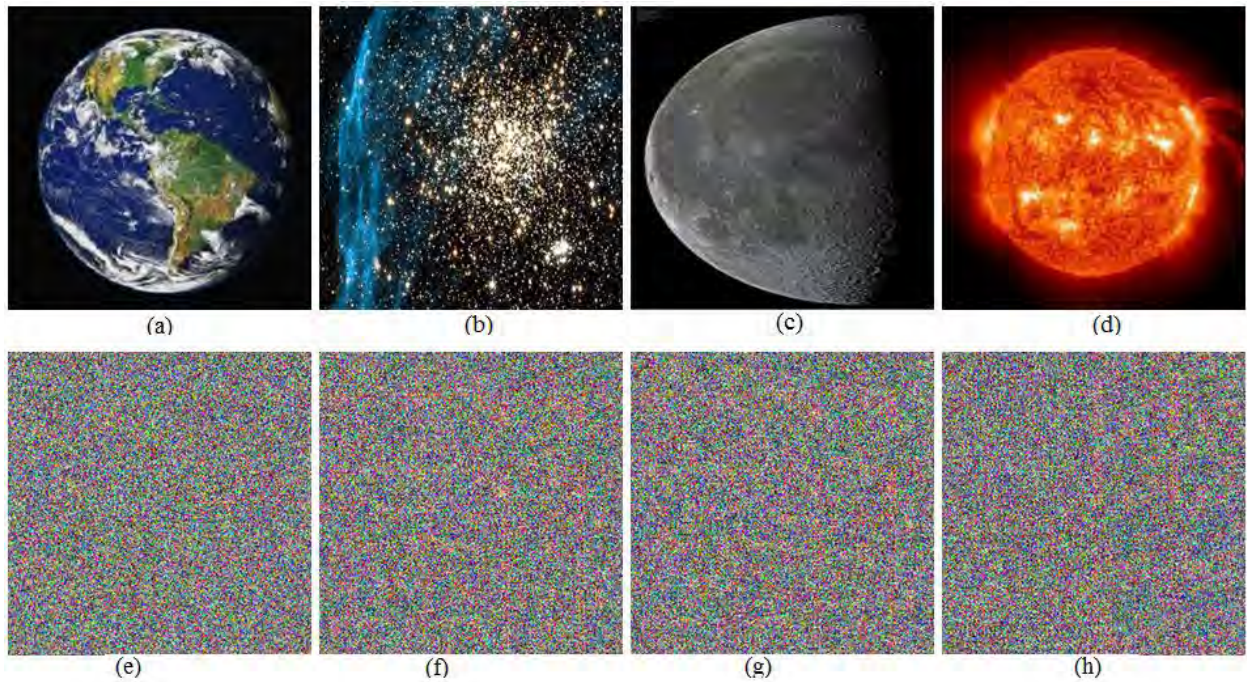


Figure 8. Earth, Stars, Moon and Sun original image and there corresponding ciphered images

Chapter 5

Chain ring based improved SERPENT algorithm: A digital image encryption implementation

The annexation of chaos is considered as the prodigious development in the field of secure data transmission. The chaotic dynamical systems have the property of state periodicity, randomness, and non-convergence. Accordingly, these special features of chaos are fairly suitable in data encryption. Nonetheless, meanwhile, cryptanalysts also challenge these algorithms and try to retrieve the original data. As a result, the real-time data transmission over networks and internet by different segments of life like aerospace, military, governmental and private organizations having personal data increase the demand of strong and fast ciphers. As a consequence, the symmetric block ciphers paid extra attention.

The algorithms Rijndael (Advanced Encryption Standard-AES), SERPENT and TWOFISH are similarly known to be the best in terms of data protection. In certain cryptographic fields, however, they pay less interest due to their time consumption inferiority, such as digital image enciphering techniques. In this part of the study, relying on chain ring-based S-boxes dealing with 8-bit vectors instead of 4-bit, we present a time-decreasing improved SERPENT algorithm variant. In a chain ring, the multiplicative substructures have several generators and hence the S-boxes dependent on the chain ring increase the algebraic complexity of the cipher. In addition to that, the algorithm is used in a wireless RGB image encryption program where operations are done throughout the chain ring. Compared to the latest popular RGB image encryption methods, the digital image tests suggest that the planned system takes less time (i.e. 8.2 microseconds for enciphering and 5.8 microseconds for deciphering of a 128-bit block). Also, it is noted in the inquiry into the proposed RGB image encryption method (chapter 6) that the given scheme is very resistant to statistical and differential attacks.

5.1 Improved SERPENT algorithm

The Serpent Algorithm is a block cipher. It is considered to be the most secure, even more than the Rijndael algorithm. As Serpent algorithm was a competitor for AES however its slow speed makes a reason of its failure and thus Rijndael was chosen as an AES. Despite there are many uses of Serpent algorithm; for instance, it is used in image encryption [13].

The chain ring-based algorithm was developed by Shah et al. [12] it is also a block cipher that encrypt a block of size 128-bit by using a key of size 256 bits. The algorithm consists of three basic functions namely, the initial permutation, the round function and the final permutation. The cryptosystem comprises of S-boxes obtained from multiplicative group of commutative Chain ring of the form $R_8 = \frac{F_2[x]}{\langle x^8 \rangle} = F_2 + xF_2 + x^2F_2 + \dots + x^7F_2$. Throughout the algorithm, the operations of addition and multiplication coincides with the operations of chain ring i.e. the multiplication operation of R_8 coincides with \mathbb{Z}_{2^8} , the local ring of integers modulo, whereas, the addition operation coincides with Galois field F_{2^8} . In addition, the substitution from the S-boxes also differs from the literally substitution. For substitution, the S-box is operated with a block of 128-bits and the result appears in the chain ring R_8 . The internal structure of the chain ring-based SERPENT algorithm is discussed below.

$$\begin{aligned}
B'_0 &= IP(P) \\
B'_{(i+1)} &= LT(S_{(imod4)}(B'_i \oplus K'_i)); 0 \leq i \leq 20 \\
B'_{32} &= S_3(B'_{21} \oplus K'_{21}) \oplus K'_{22} \\
C &= FP(B'_{22})
\end{aligned}$$

In the above equations; P stands for Plain Text, B'_i for Data block, \oplus stands for Exclusive-or operation, K'_i for sub keys, S for S-box, LT for Linear Transformation, FP for Final Permutation, and C for Cipher Text.

5.1.1 Key structure

The subkeys K'_i are generated from the supplied key. If the key is of 256-bit, split it into 64-bit vectors $w'_{(-4)}$, $w'_{(-3)}$, $w'_{(-2)}$ and $w'_{(-1)}$. Now find the pre-keys w'_i ; $i = 0, 1, 2, \dots, 46$ using the affine recurrence:

$$w'_i = (w_{(i-4)} \oplus w_{(i-1)}\phi, \phi \oplus i, i) \lll 5$$

Where $\phi = (\sqrt{5} + 1)/2$, and \lll represent left rotation of bits. Using the pre-keys, the subkeys are generated by using the equation:

$$K'_i = IP(S_{(1-i) \bmod 4}(w_{2i}, w_{2i+1})); 0 \leq i \leq 22$$

In case or shortage of bits in the supplied key, a “1” is appended in the left followed by as many zeros as required to become a 256-bit key.

5.1.2 Linear transformation

The linear transformation (LT) is adopted from the original Serpent algorithm designed by Eli Biham (Technion Israeli Institute of Technology), Ross Anderson (University of Cambridge Computer Laboratory) and Lars Knudsen (University of Bergen, Norway) see [3]. Split the given input of 128-bit to 32-bit blocks named x_0, x_1, x_2 and x_3 respectively. Now perform the following transformations:

$$\begin{aligned}x_0 &= x_0 \lll 13 \\x_2 &= x_2 \lll 3 \\x_1 &= x_1 \oplus x_0 \oplus x_2 \\x_1 &= x_1 \lll 1 \\x_3 &= x_3 \lll 7 \\x_0 &= x_0 \oplus x_1 \oplus x_3 \\x_2 &= x_2 \oplus x_3 \oplus (x_1 \lll 7) \\x_0 &= x_0 \lll 5 \\x_2 &= x_2 \lll 22\end{aligned}$$

Now rejoin the x_0, x_1, x_2 , and x_3 resulting from the above equations to get the result obtained from *LT*.

5.2 Digital image encryption scheme using improved SERPENT algorithm

Nowadays, one of the best approaches for hiding data is the use Asymmetric cryptography. Nevertheless, A symmetric algorithm called Advanced encryption algorithm is used as a standard. Numerous image encryption schemes based on Rijndael algorithm and SERPENT algorithm are available in literature. Nevertheless, contrary to chaos and S-box-based encryption algorithms, they require time. In this section, a novel image encryption scheme based on chain ring SERPENT algorithm is introduced. The image encryption scheme is as follows:

1. Read a color image and extract its Red (R), Green (G) and Blue (B) layer.
2. Convert each layer into binary and split it into blocks of 128 bits.
3. Apply the initial permutation $[i \times 64 \pmod{127}]$.
4. Exclusive-or the key k'_0 , execute the chain ring S-box and apply the linear transformation.

5. Execute step 4 till 22nd round. In the 22nd round, after applying S-box, exclusive-or the sub key K'_{22} and apply the final permutation $[i \times 64(mod127)]$ to get the cipher text of block 128-bit.
6. Collect the encrypted data and revert it into bytes that will represent the cipher R, G and B layers.
7. Concatenate the enciphered R, G, B channels to get the encrypted color image.

Flow chart and enciphered images of the encryption scheme is given Figure 9 and figure 10 respectively.

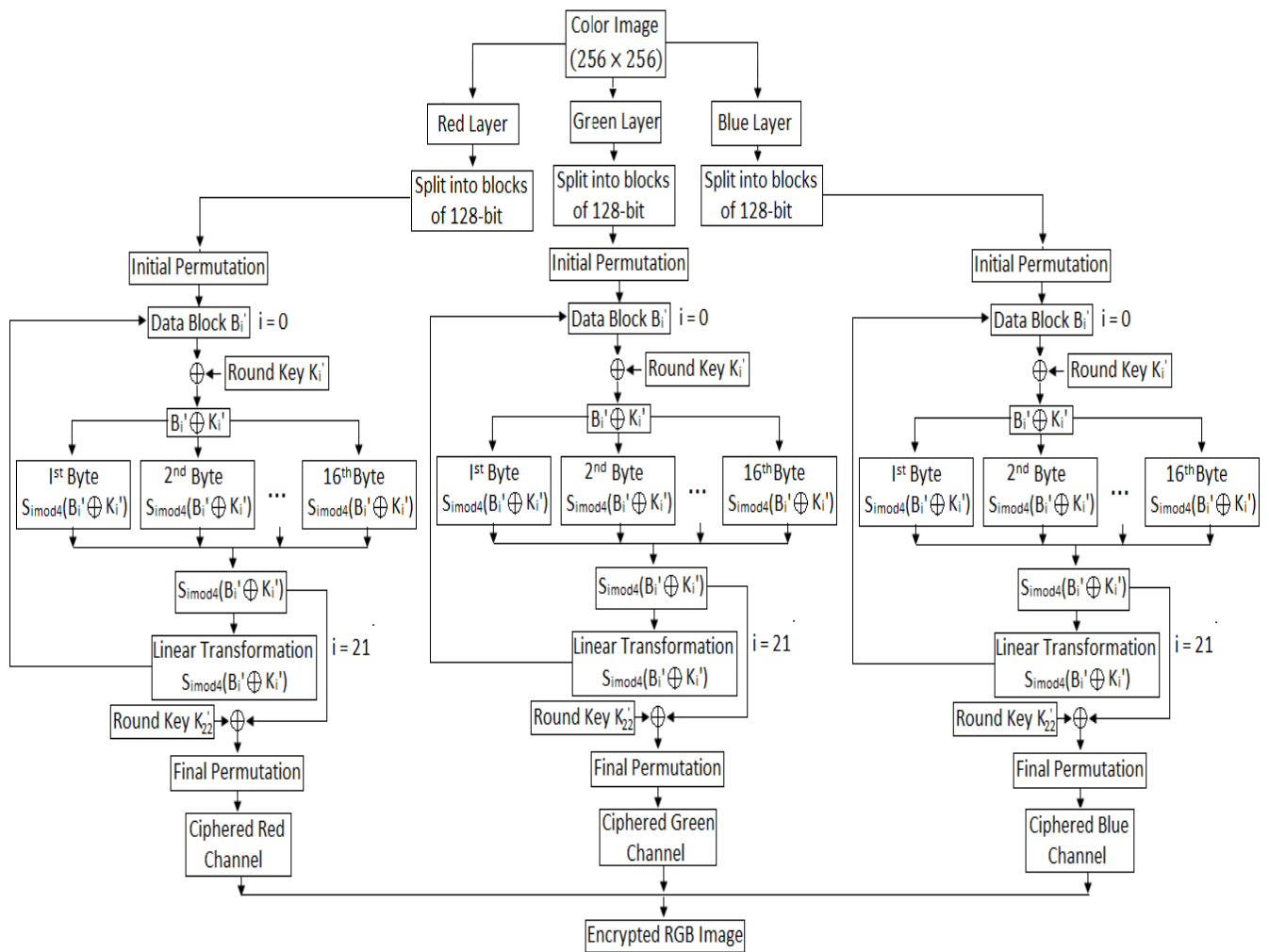


Figure 9. RGB image encryption scheme using chain ring-based SERPENT algorithm

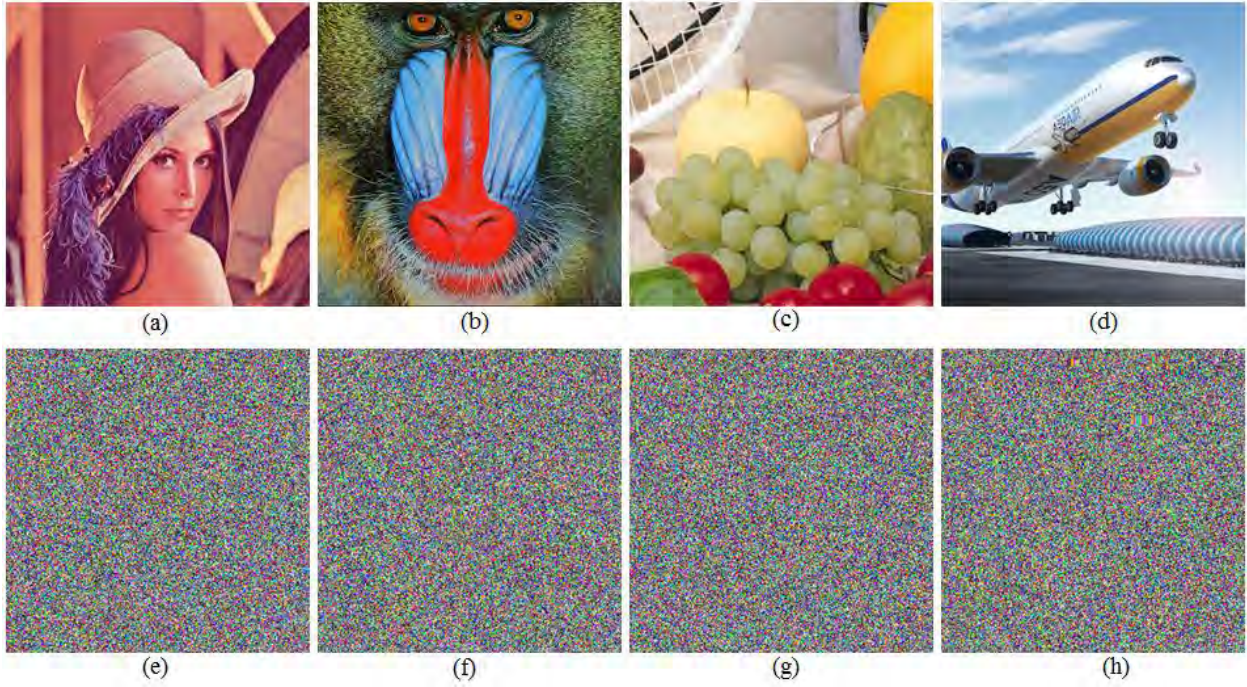


Figure 10. Lena, Baboon, Fruits and Aeroplane original images and there corresponding encrypted images

Chapter 6

Strength determination of newly introduced data security algorithms

With the rapid advancement of electronic data sharing, information security in data storage and transmission is becoming more critical. It is necessary to secure sensitive image data from unauthorized access due to the large sharing of images in communication. We examined the image encryption algorithms given in chapters 2-5 in this section of the thesis.

When an encryption algorithm is applied to an image, its pixel values alter as compared to the original image. These adjustments must be rendered irregularly by a good encryption algorithm to optimize the change in pixel values between the plain and the enciphered digital medium. It must also be composed of entirely random patterns that do not show any of the characteristics of the original image to obtain the encrypted image. One of the important metrics (of this chapter) in examining an encrypted image is the visual inspection: The more hidden the features of the image are, the better the encryption algorithm is.

Besides, diffusion is also an important parameter that must be calculated to judge the randomization of the encryption algorithm. The relationship between the enciphered plain digital image is too complicated if an algorithm has a strong diffusion characteristic, and it cannot easily be predicted. A bit is altered in the plain image to calculate the diffusion of any algorithm. It catches the change obtained among the ciphered digital image and the original digital image. This chapter also contains some basic characteristics of the encryption algorithms, such as noise immunity and processing time, which can be calculated by some other tests.

6.1 Statistical analysis

Guaranteeing the resistance of an encryption technique against statistical analysis is of major importance for checking the security of an algorithm. In case, if a scheme withstands against all the statistical attacks then it is considered to be secure. Among the statistical investigation of image processing algorithms, histogram analysis and adjacent pixels correlation are of key importance.

6.1.1 Key-space analysis

One of the basic attacks for destroying the security of a cryptosystem is the brute force attack. The brute force attack is feasible only when a cryptosystem has a small key-space size i.e. less than 2^{100} . In addition, an encryption algorithm must be sensitive to any small change in order to withstand the brute force attack. Our proposed encryption scheme comprises of 4 security keys namely: α, x_0 , Chain ring S-box and DNA sequences. The elements $\alpha \in (0, 4]$ and $x_0 \in [0, 1]$ have key-space size of $10^{16} \times 10^{16}$. Since for each triplet, one can choose different initial conditions therefore the total key-space size originating from logistic map becomes $10^{16} \times 10^{16} \times 10^{16} \times 10^{16} \times 10^{16} = 10^{69}$.

The chain ring has a total of 2^{12} elements whereas the DNA transform has 8 kinds of encoding rules. Thus, the total key-space size of “Algebra-Chaos Amalgam and DNA Transform based Multiple Digital Image Encryption” scheme is:

$$\text{Key-Space size} = (10^{69}) \times 2^{12} \times 8 \approx 2^{245}$$

For modified serpent algorithm the key space size is:

$$\text{Key-Space size} = 2^{256}$$

This clarify that the presented scheme shows great resistance against brute force attack.

6.1.2 Histogram analysis

Pixels of a digital image can be represented by bytes. When values of bytes are represented by bars in a panel, we call it a histogram of bytes of the image or histogram of the corresponding image. It was firstly introduced in [64]. For determining the protection of image encryption schemes, the uniformity of the image histogram of an encrypted data is the finest feature. If the histogram bars are uniform, the encryption is considered to be good and hence resists statistical attacks. Whereas, an unsecure encryption is the one having non-uniform bars. In the Algebra-Chaos Amalgam and DNA Transform based Multiple Digital Image Encryption, we analyze 512×512 dimensional multiple RGB image. We split the combined image in to its sub-images and checked their histograms one by one. The histogram of original parts and encrypted parts of a multiple image is shown in Fig. 11.

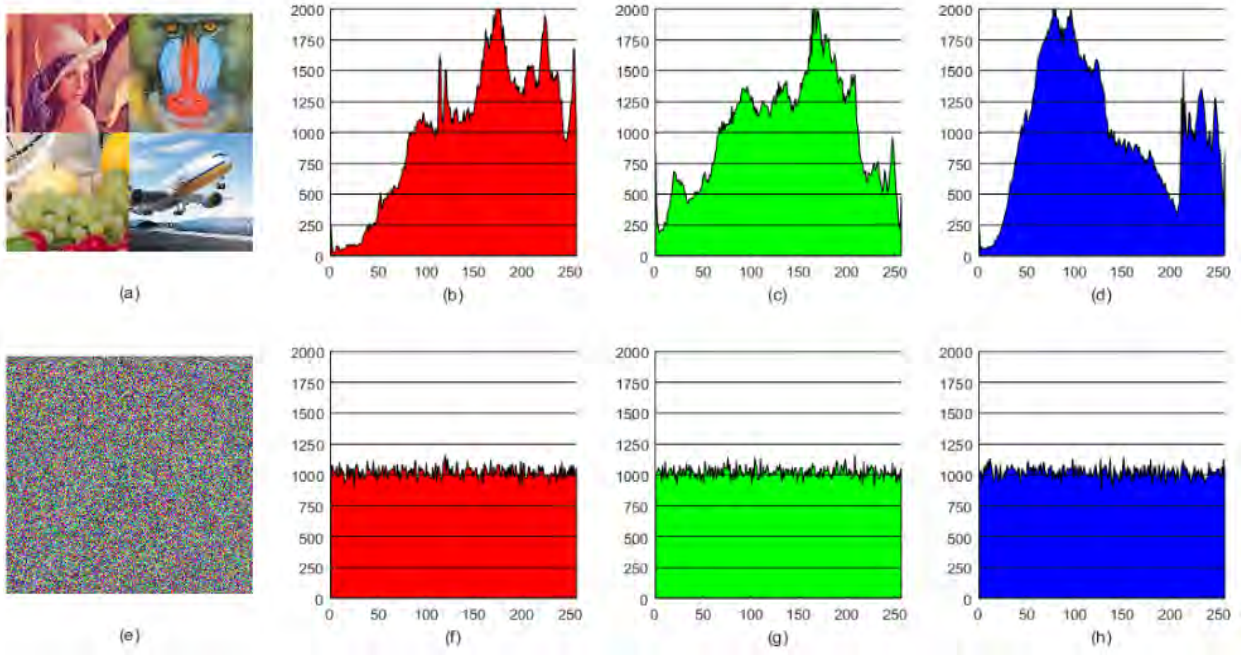


Figure 11. (a) and (e) are original and encrypted multiple image respectively. Histogram pins in (b) and (f) represents Red Channel of (a) and (e) respectively. Similarly, (c), (d) and (g), (h) shows the histogram pins of green and blue layers of original and encrypted multiple image respectively.

In Fig. 11, the sharp edges histograms represent R, G, B layers of the plain digital multiple image whereas, the flat one corresponds to the encrypted multiple image layers. The flat histogram of encrypted images is an evident of the fact that the ciphering technique is satisfactory and can resist all the well-known attacks.

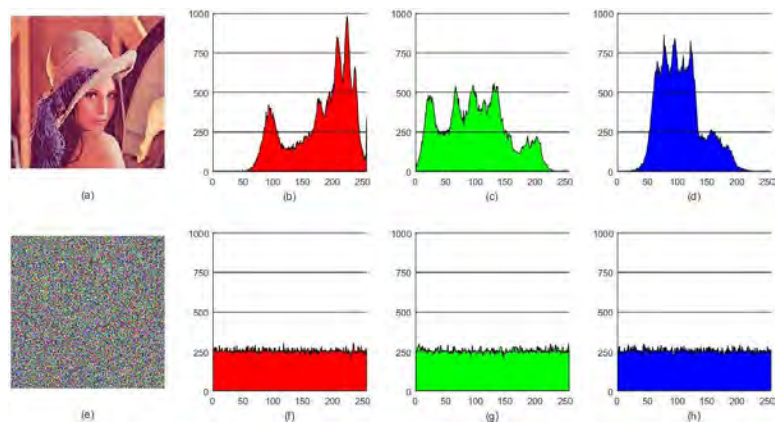


Figure 12. (a) and (e) are original and encrypted color Lena image respectively. Histogram pins in (b) and (f) represents Red Channel of (a) and (e) respectively. Similarly, (c), (d) and (g), (h) shows the histogram pins of green channel and blue channel of original and encrypted Lena image respectively.

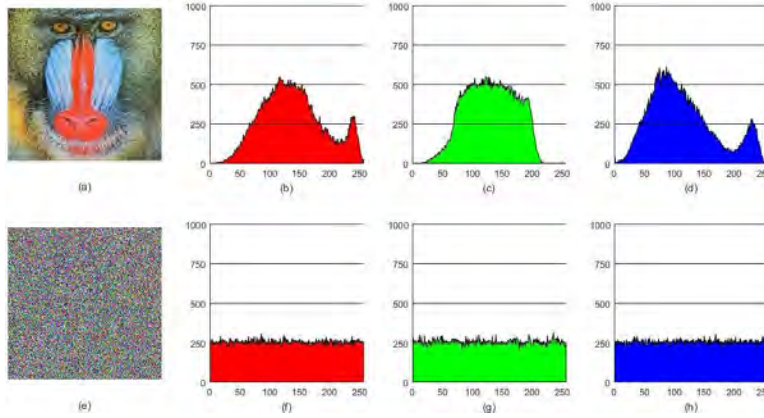


Figure 13. (a) and (e) are original and encrypted color Baboon image respectively. Histogram pins in (b) and (f) represents Red Channel of (a) and (e) respectively. Similarly, (c), (d) and (g), (h) shows the histogram pins of green and blue layers of original and encrypted Baboon image respectively.

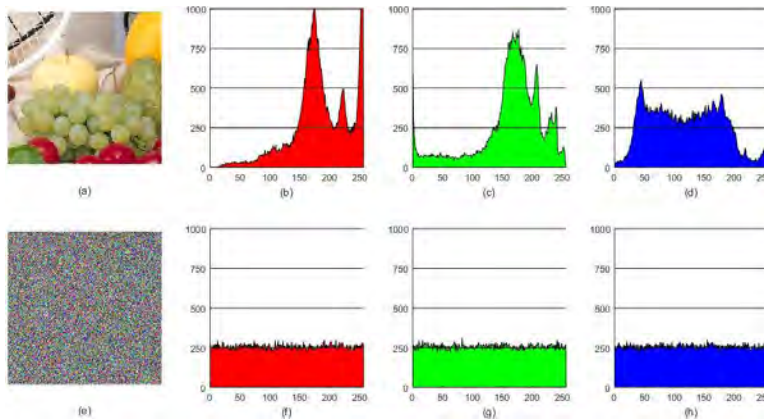


Figure 14. (a) and (e) are original and encrypted color Fruits image respectively. Histogram pins in (b) and (f) represents Red Channel of (a) and (e) respectively. Similarly, (c), (d) and (g), (h) shows the histogram pins of green and blue layers of original and encrypted Fruits image respectively.

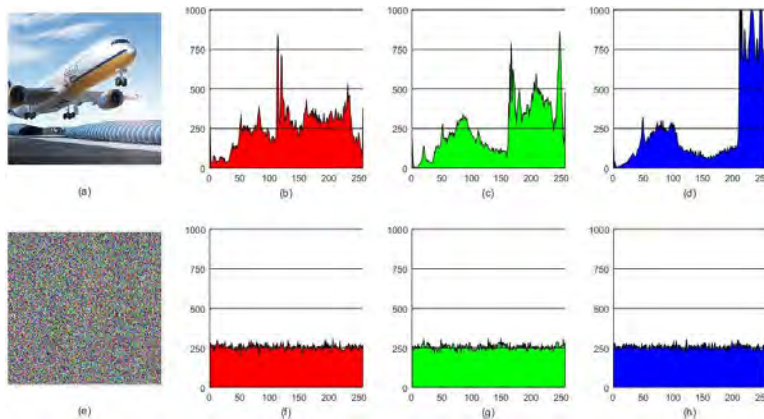


Figure 15. (a) and (e) are original and encrypted color Aeroplane image respectively. Histogram pins in (b) and (f) represents Red Channel of (a) and (e) respectively. Similarly, (c), (d) and (g), (h) shows the histogram pins of green and blue layers of original and encrypted Aeroplane image respectively.

In Fig. 12-15. (a) and (e) are original and encrypted color images respectively. (b), (c), (d) and (f), (g), (h) shows the histogram pins of Red, green and blue layers of original and encrypted

image respectively. Fig. 12-15 shows that the histogram pins of encrypted images are almost parallel and hence can show strong resistance to cryptanalysts.

In case of 12×12 S-box Design and its Application to RGB Image Encryption, we examined the images of Lena and Fruits. In Figure 16 (Lena Image) and Figure 17 (Fruits Image), i.e. the plain and encrypted images and their different layers, the three-dimensional (3-D) histograms are provided to study the uniformity of encrypted images. The trickles of histograms in an image keep the aspects of data distribution of pixel. To stop distinguishing any supporting data from the vulnerable histogram from the rival, a perfect encrypted image should have a standardized histogram spreading. Therefore, applying a mathematical assault on a proposed encryption scheme would not bounce any comprehension.

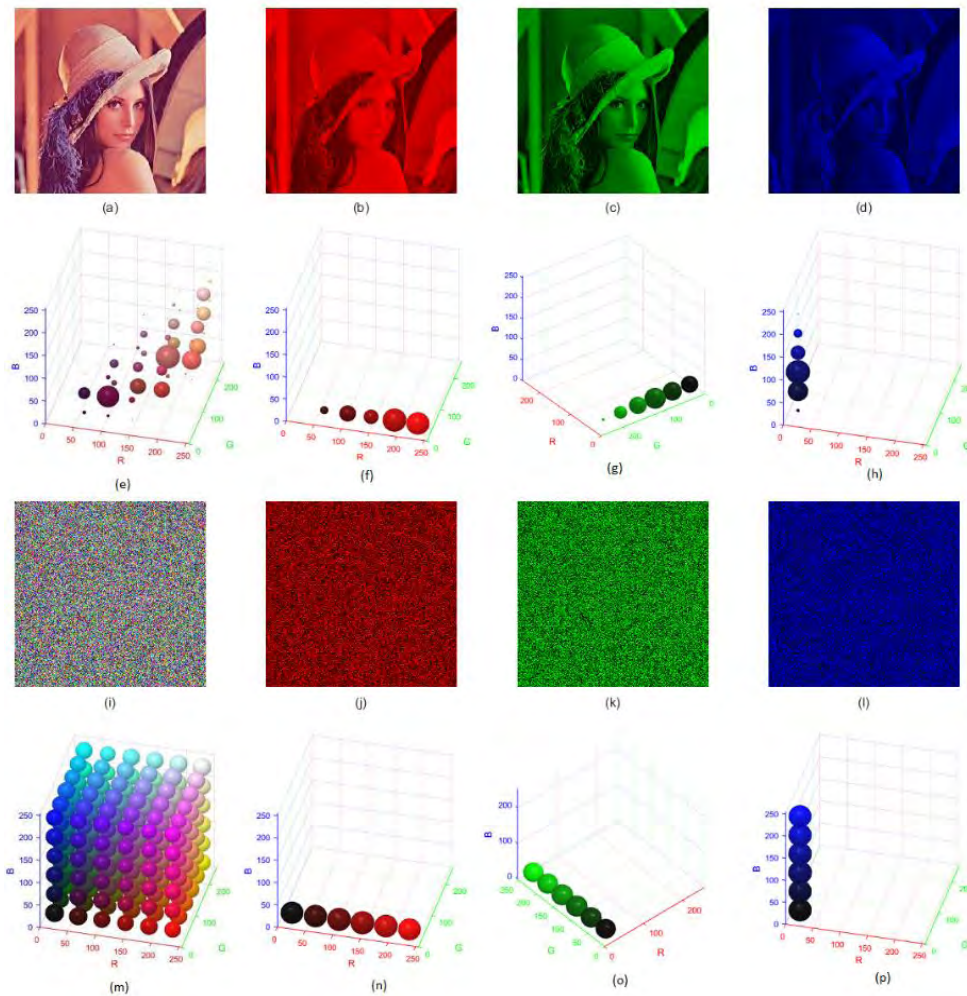


Figure 16. (a) is Lena Original Image. (b),(c),(d) are its corresponding Red, Green and Blue layers. (e), (f), (g), and (h) are the 3D histograms of (a), (b), (c) and (d) respectively. (i) is Lena Encrypted Image where (j), (k) and (l) are its Red, Green and Blue layers respectively. (m), (n), (o) and (p) are the 3D histograms of (i), (j), (k) and (l) respectively.

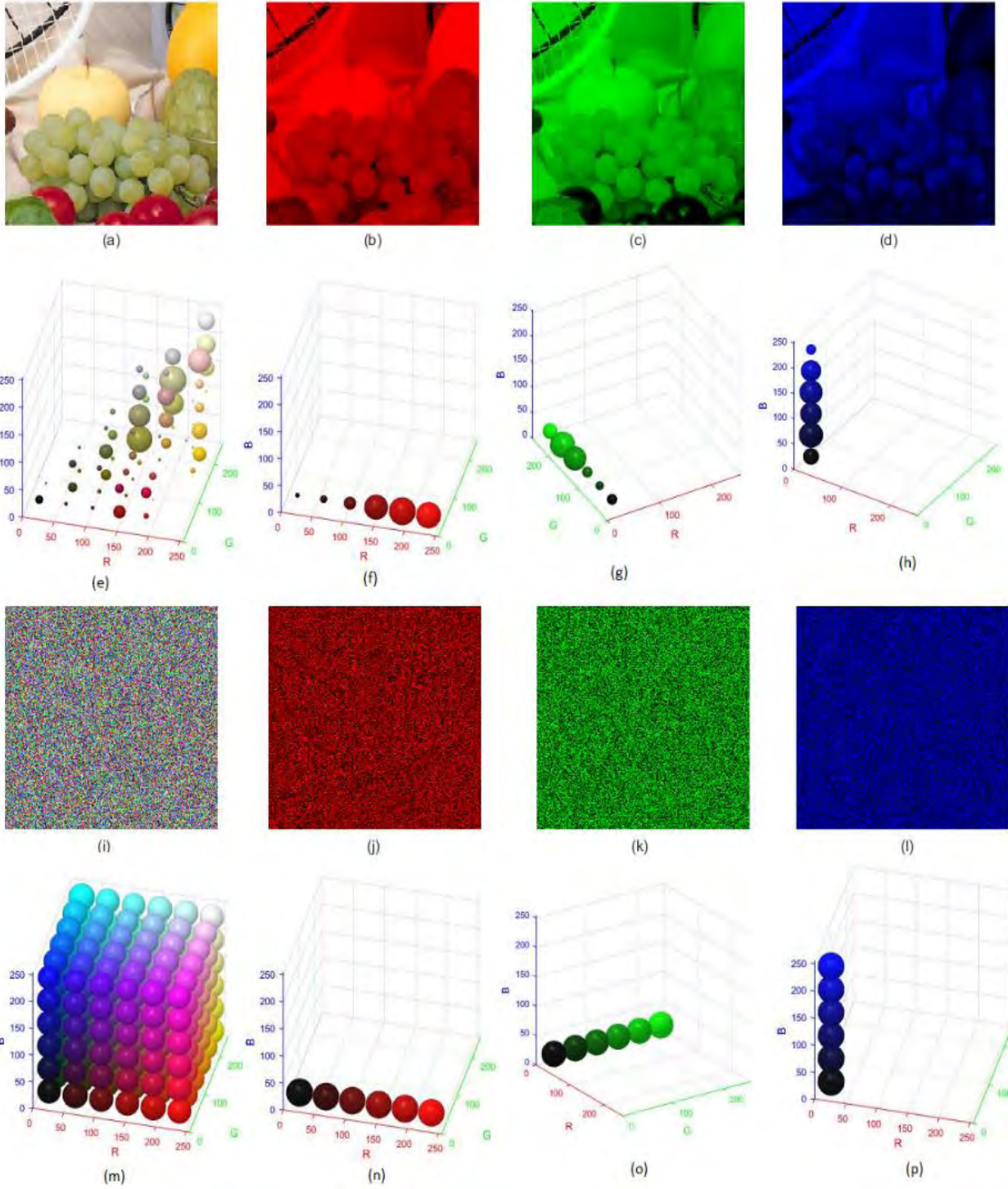


Figure 17. (a) is Fruits Original Image. (b),(c),(d) are its corresponding Red, Green and Blue layers. (e), (f), (g), and (h) are the 3D histograms of (a), (b), (c) and (d) respectively. (i) is Fruits Encrypted Image where (j), (k) and (l) are its Red, Green and Blue layers respectively. (m), (n), (o) and (p) are the 3D histograms of (i), (j), (k) and (l) respectively.

In case of *Improved SERPENT Algorithm: Design to RGB Image Encryption Implementation*, we examined color Lena and Baboon image for histogram analysis. These images are given in figure 18 and figure 19 respectively. In this case, we also provide the decrypted image of the corresponding images.

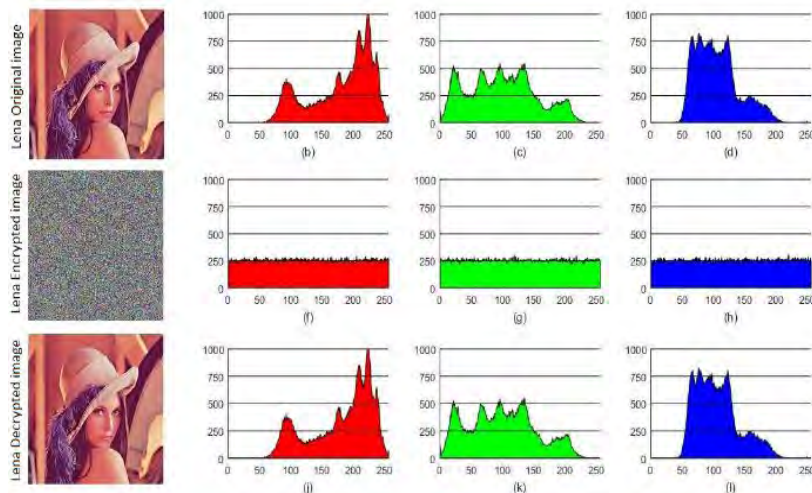


Figure 18. (b), (c) and (d) shows the histogram pins of Red Green and Blue layers of the original Lena color image. (f), (g) and (h) represent the histogram pins of Red Green and Blue layers of the encrypted Lena RGB image. (j), (k) and (l) represent the histogram pins of Red Green and Blue layers of the decrypted Lena RGB image.

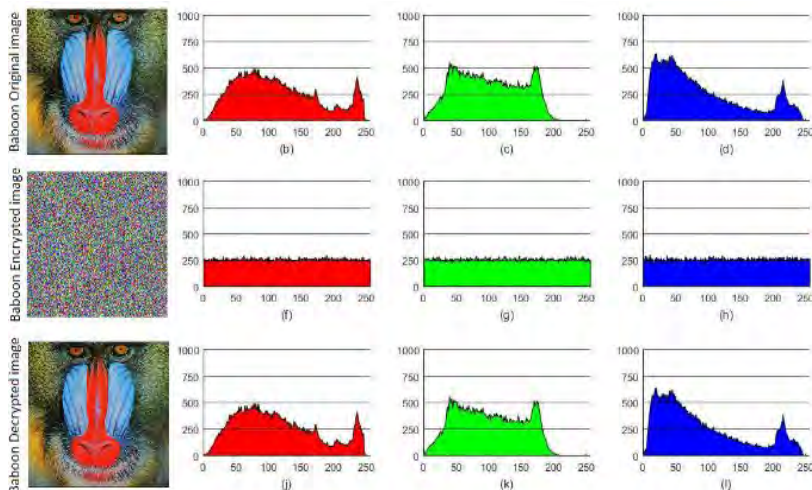


Figure 19. (b), (c) and (d) shows the histogram pins of Red Green and Blue layers of the original Baboon color image. (f), (g) and (h) represent the histogram pins of Red Green and Blue layers of the encrypted Baboon RGB image. (j), (k) and (l) represent the histogram pins of Red Green and Blue layers of the decrypted Baboon RGB image.

In figures (18-19), (b), (c) and (d) shows the histograms pins of red, green and blue layers of the original images. (f), (g), (h) are encrypted image histogram pins whereas, (j), (k) and (l) are the decrypted image histogram pins. The histogram of the encrypted image ensures that the encryption scheme is resist the brute force attack.

In case of *24-by-24 S-box design*, we examined color Earth and Stars image for histogram analysis. These images are given in figure 20 to figure 21. In this case, we also provide the decrypted image of the corresponding images.

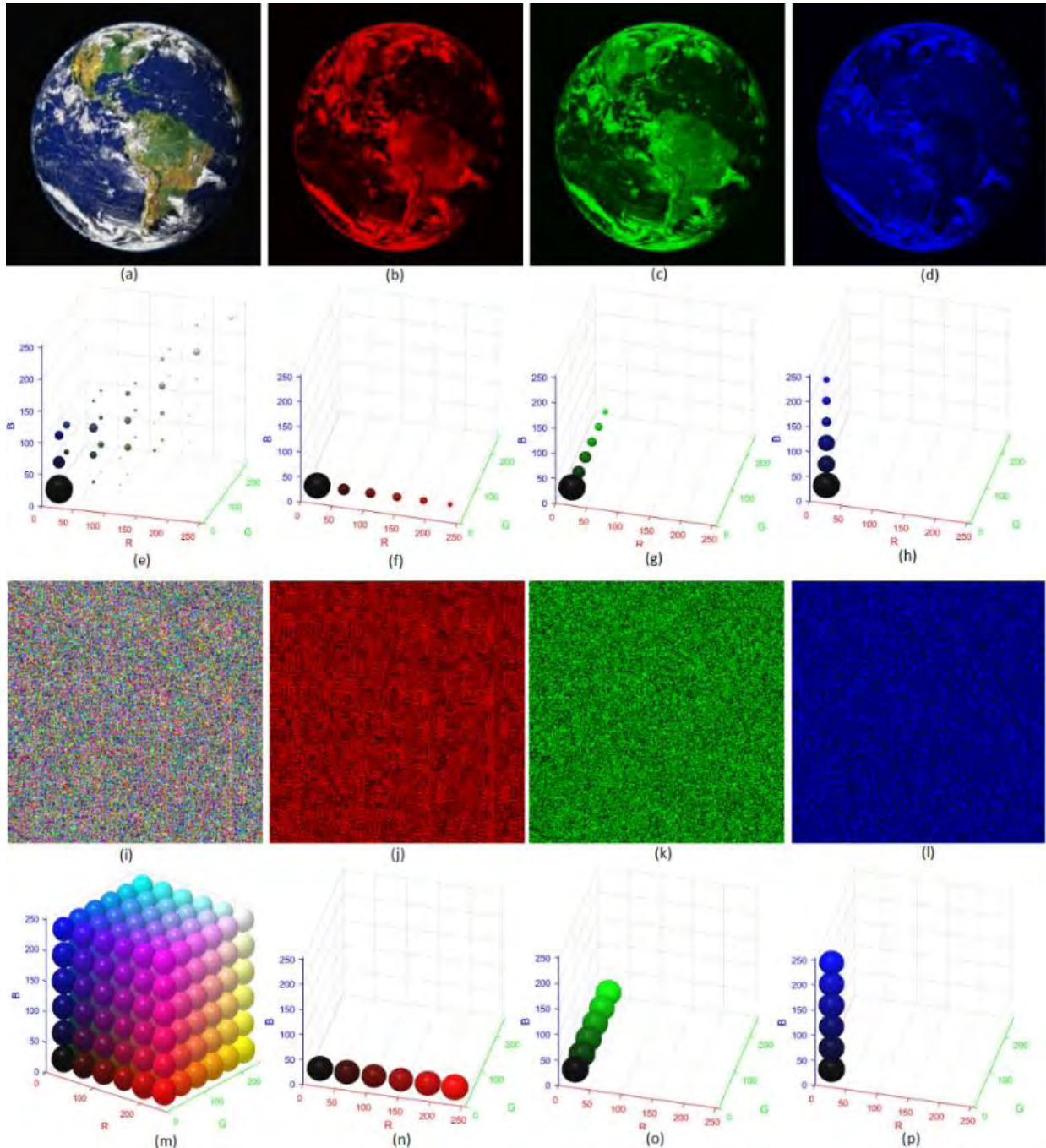


Figure 20. Earth image and its Red, Green, Blue channels are shown in (a), (b), (c), (d) respectively. Their corresponding 3D histograms are shown in (e), (f), (g), (h). Similarly, Earth ciphered image and its red, green, blue channels are given in (i), (j), (k) and (l). Their corresponding 3D histograms are given in (m), (n), (o) and (p) respectively.

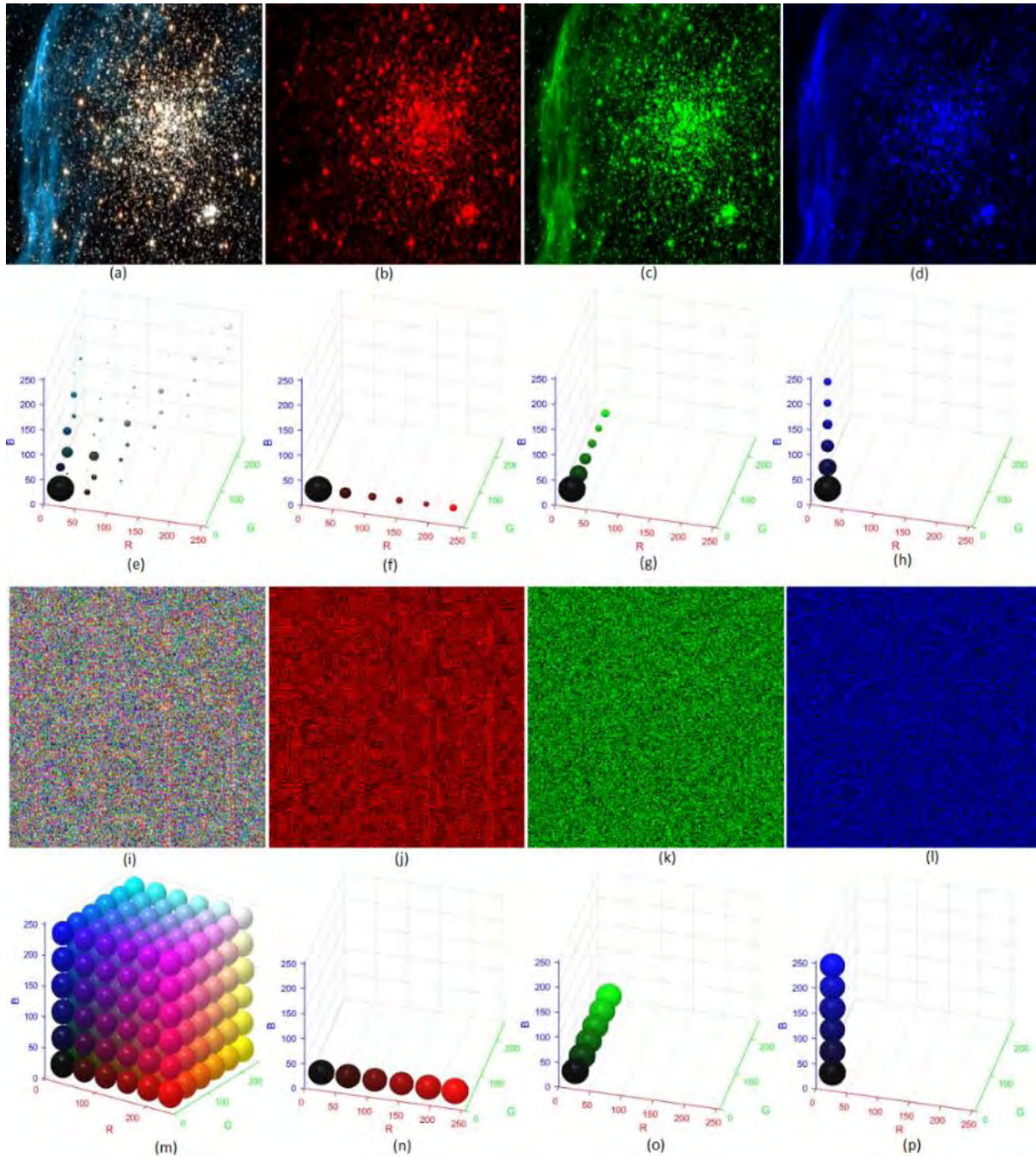


Figure 21. Stars image and its Red, Green, Blue channels are shown in (a), (b), (c), (d) respectively. Their corresponding 3D histograms are shown in (e), (f), (g), (h). Similarly, Stars ciphered image and its red, green, blue channels are given in (i), (j), (k) and (l). Their corresponding 3D histograms are given in (m), (n), (o) and (p) respectively.

6.1.3 Intensity histogram analysis

The pixels show of a digital image is controlled by the intensity of more layers of the image. It gives the information about pixels. The pixels appearance is controlled by the color depth of the image. A uniform intensity histogram guarantees strength of an encryption technique. The intensity histogram of original and ciphered multiple color images are shown in Fig. 22.

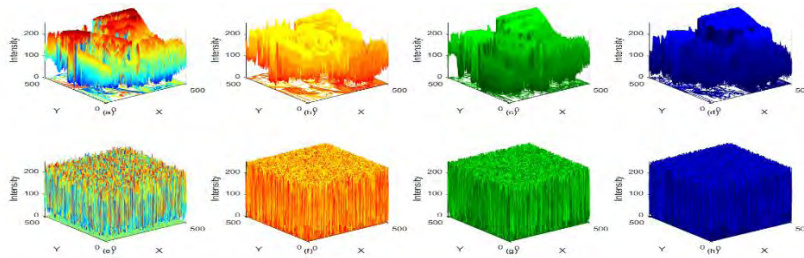


Figure 22. Subfigure (a) and (e) are Intensity histogram pins original and ciphered Multiple image respectively. Intensity histogram pins of original multiple RGB image layers are given in (b), (c) & (d) respectively. Similarly, that of encrypted image is in (f), (g) & (h) respectively.

Clearly, the encrypted image layers have a uniform intensity bars which ensures the strength of the presented image encryption scheme against eavesdroppers.

Fig. 23-26 represents the intensity histograms of sub-parts of the multiple RGB primary and ciphered image with their corresponding Red, Green & Blue layers intensity histograms.

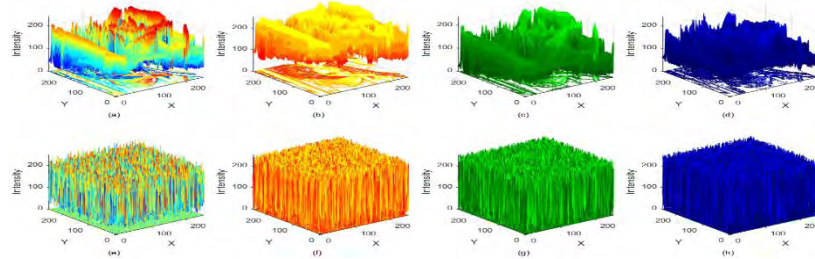


Figure 23. Subfigure (a) and (e) are Intensity histogram pins original and ciphered Lena image respectively. Intensity histogram pins of Lena RGB image layers are given in (b), (c) & (d) respectively. Similarly, that of encrypted image is in (f), (g) & (h) respectively.

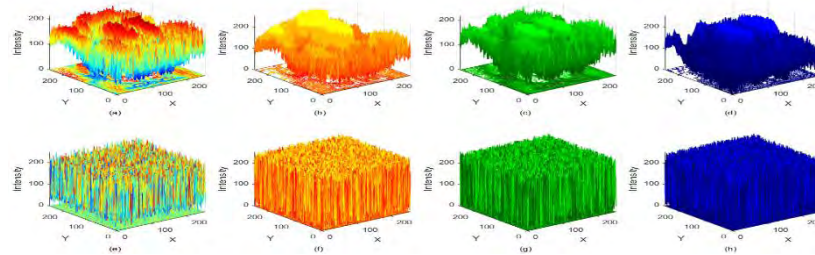


Figure 24. Subfigure (a) and (e) are Intensity histogram pins original and ciphered Baboon image respectively. Intensity histogram pins of Baboon RGB image layers are given in (b), (c) & (d) respectively. Similarly, that of encrypted image is in (f), (g) & (h) respectively.

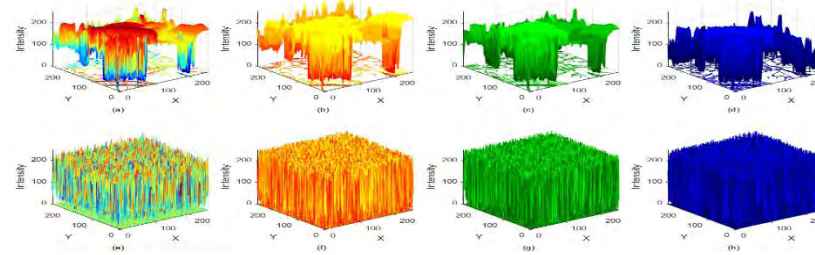


Figure 25. Subfigure (a) and (e) are Intensity histogram pins original and ciphered Fruits image respectively. Intensity histogram pins of Fruits RGB image layers are given in (b), (c) & (d) respectively. Similarly, that of encrypted image is in (f), (g) & (h) respectively.

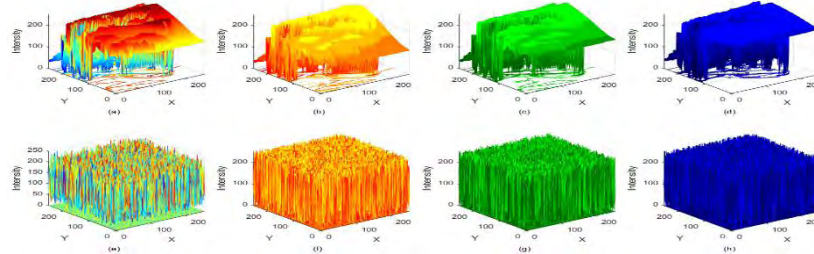


Figure 26. Subfigure (a) and (e) are Intensity histogram pins original and ciphered Aeroplane image respectively. Intensity histogram pins of Aeroplane RGB image layers are given in (b), (c) & (d) respectively. Similarly, that of encrypted image is in (f), (g) & (h) respectively.

In each fig. 23-26, the first row shows the intensity histogram of original image and its red, green and blue channels respectively. Whereas, the 2nd row of each figure shows the corresponding encrypted image and its RGB channels respectively. Figures clearly shows that the original image intensity histogram has sharp edges whereas, there corresponding encrypted image intensity histogram has flat edges. Thus, it shows that the encrypted images are resisting various cryptanalytic attacks.

In case of 12×12 S-box Design and its Application to RGB Image Encryption, we examined the intensity histogram of Lena and Fruits images. The 3D intensity histograms of these images and their corresponding layers are shown in figure 27-28.

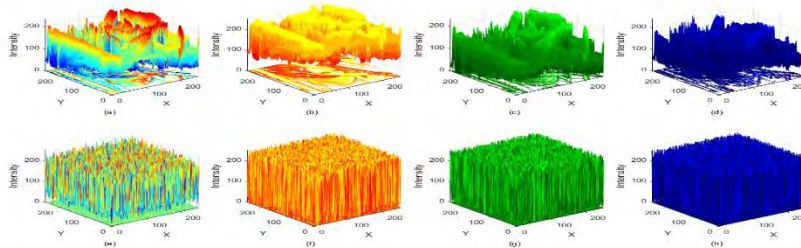


Figure 27. 3D intensity histogram of Lena image having size 256×256 . (a) and (e) presents 3D intensity histogram of Lena original and encrypted image respectively. (b), (c) and (d) are 3D intensity histogram of RGB layers (respectively) of Lena original image. (f), (g) and (h) are 3D intensity histograms of RGB layers (respectively) of Lena encrypted image.

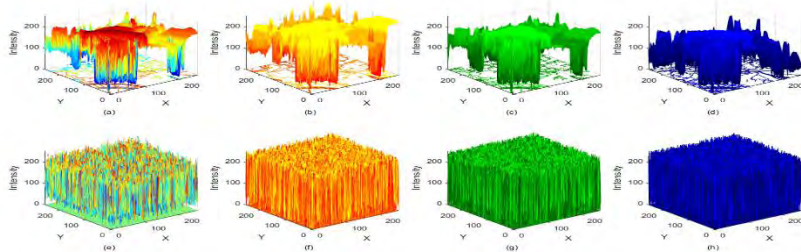


Figure 28. 3D intensity histogram of Fruits image having size 256×256 . (a) and (e) presents 3D intensity histogram of Fruits original and encrypted image respectively. (b), (c) and (d) are 3D intensity histogram of RGB layers (respectively) of Fruits original image. (f), (g) and (h) are 3D intensity histograms of RGB layers (respectively) of Fruits encrypted image.

In case of Improved SERPENT Algorithm: Design to RGB Image Encryption Implementation, we examined color Lena, and Baboon image for intensity histogram analysis. The intensity

histogram of Lena original and encrypted image is given in figure 29 and figure 30. Figure 29-30 shows the intensity histogram of baboon, plain and ciphered digital images respectively.

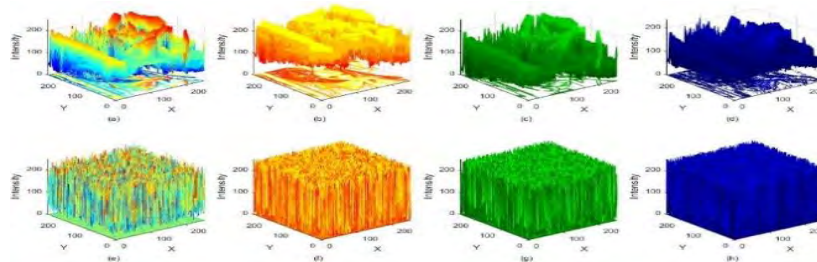


Figure 29. Subfigure (a) and (e) are Intensity histogram pins original and ciphered Lena image respectively. Intensity histogram pins of Lena RGB image layers are given in (b), (c) & (d) respectively. Similarly, that of encrypted image is in (f), (g) & (h) respectively.

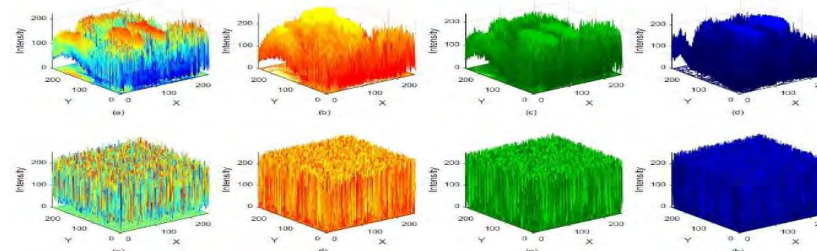


Figure 30. Subfigure (a) and (e) are Intensity histogram pins original and ciphered Baboon image respectively. Intensity histogram pins of Baboon RGB image layers are given in (b), (c) & (d) respectively. Similarly, that of encrypted image is in (f), (g) & (h) respectively.

In case of *24-by-24 S-box encryption to Astronomical images*, we examined color Earth and Sun image for intensity histogram analysis and are shown in fig 31-32.

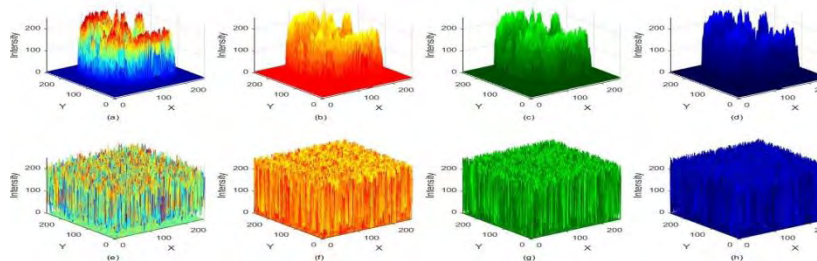


Figure 31. Earth Original image and its red, green and blue layers 3D intensity histogram are given in (a), (b), (c) and (d) respectively. Whereas, Earth enciphered image and its red, green and blue layers intensity histogram are given in (e), (f), (g) and (h) respectively.

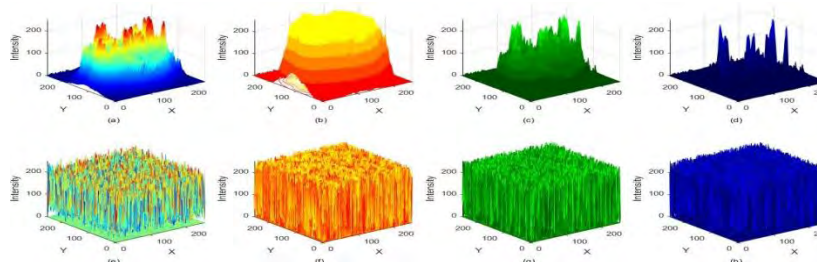


Figure 32. Sun Original image and its red, green and blue layers 3D intensity histogram are given in (a), (b), (c) and (d) respectively. Whereas, Sun enciphered image and its red, green and blue layers intensity histogram are given in (e), (f), (g) and (h) respectively.

6.1.4 Correlation analysis

The correlation provides the relation between an image's adjacent pixels. Correlation effects occur in the close-up interval $[-1,1]$ [see 65]. Tables 18 and Tables 19 have the findings of the correlation coefficients for 256×256 images of Lena and Fruits, respectively, showing the strength of the proposed encryption scheme. The study reveals that the correlation findings of our current encryption method are up to the mark and can be contrasted with existing Chaos and DNA encryption systems.

There are excellent ties between their touching pixels in the digital communication media details. An encryption algorithm should be able to interact with the vertical, horizontal, and diagonal linking pixels in images. For well-correlated pixels, a coefficient value of ± 1 is used, whereas the correlation coefficient of the non-correlated pixels is near to 0. In the provided scheme, the similarity scores reveal that the neighboring pixels of the enciphered digital images are more identical to 0, thus the suggested algorithm stunningly de-associates the adjacent pixels in the enciphered images and fulfills the operational encryption structure necessity.

In case of 12×12 S-box Design and its Application to RGB Image Encryption the correlation table for adjacent pixels are given in table 18-19 for different images.

Table 18. Correlation of Lena Original and Encrypted Image using 12-bit S-box

(a): Horizontal Correlation of Lena Original and Encrypted Image				(b): Vertical Correlation of Lena Original and Encrypted Image				(c): Diagonal Correlation of Lena Original and Encrypted Image				
		Red	Green	Blue		Red	Green	Blue		Red	Green	Blue
Original Image	R	0.9360	0.8021	0.6349	R	0.9422	0.8422	0.6546	R	0.9922	0.8049	0.5974
	G	0.5991	0.9288	0.8656	G	0.6557	0.9456	0.9166	G	0.5564	0.9711	0.7861
	B	0.6188	0.8227	0.8877	B	0.6843	0.8690	0.9147	B	0.6068	0.8116	0.9814
Encrypted Image	R	0.000087	0.0014	-0.0014	R	0.00022	0.0059	0.0018	R	0.00083	-0.0083	0.0016
	G	0.0088	-0.00028	-0.0024	G	0.0076	0.00065	0.0052	G	0.0077	-0.0002	-0.0028
	B	0.0040	0.0082	0.000076	B	0.0036	0.0004	0.00064	B	-0.0035	-0.0010	0.00063

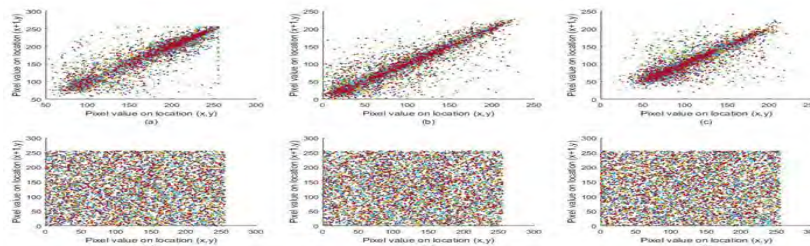


Figure 33. (H) (a-f): (Horizontal) Correlation of pixels for original and encrypted 256×256 Lena image

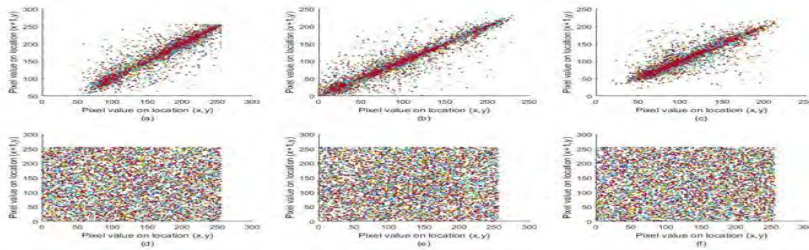


Figure 34. (V) (a-f): (Vertical) Correlation of pixels for original and encrypted 256×256 Lena image

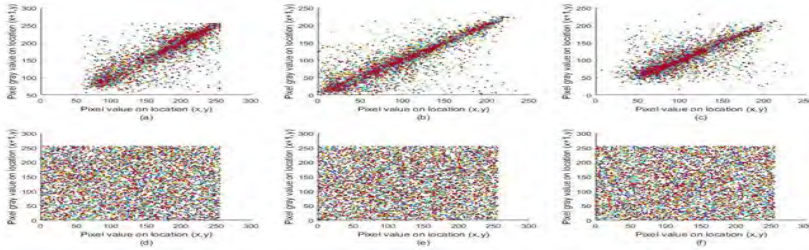


Figure 35. (D) (a-f): (Diagonal) Correlation of pixels for original and encrypted 256×256 Lena image

The distribution of the correlation between two horizontally adjacent pixels in the original image and the encrypted image is shown in Figure 33. From the analysis of these correlation images, it is clear that the planned technique is able of disconnecting the bond between the adjacent pixels, which is a remarkable accomplishment of the proposed enciphering method. The vertical correlation shows that the correlation distributions of Lena in each direction are shown in Figures 34, while the diagonal correlation distributions of the encrypted picture of Lena are shown in each direction in Figures 35. As all the dots are assembled along the diagonal in first row of figures 33-34, which means the pixels are well correlated. However, in the 2nd row of Figures 33-34 the dots are scattered through the entire plane, suggesting that in the encrypted images the correlation is greatly diminished.

Table 19. Correlation of Fruits Original and Encrypted Image

(a): Fruits Original and Encrypted Image Horizontal Correlation				(b): Fruits Original and Encrypted Image Vertical Correlation				(c): Fruits Original and Encrypted Image Diagonal Correlation				
		Red	Green	Blue		Red	Green	Blue		Red	Green	Blue
Original Image	R	0.9796	0.7179	0.5526	R	0.9616	0.7215	0.5467	R	0.9477	0.7020	0.5327
	G	0.5759	0.9738	0.9779	G	0.5221	0.9711	0.9670	G	0.5445	0.9546	0.9700
	B	0.5254	0.7218	0.9777	B	0.5294	0.7020	0.9815	B	0.5566	0.6795	0.9463
Encrypted Image	R	0.0005	0.0067	-0.0029	R	-0.0010	0.0001	-0.0056	R	-0.0005	0.0035	0.0043
	G	-0.0097	-0.0089	0.0042	G	0.0035	0.0016	-0.0025	G	0.0001	0.0002	0.0017
	B	-0.0003	0.0003	0.0066	B	0.0015	-0.0020	0.0043	B	-0.0017	-0.0011	-0.0016

In case of *Algebra-Chaos Amalgam and DNA Transform based Multiple Digital Image Encryption* the correlation table for adjacent pixels are given in table 20-24 for various images.

Table 20 Multiple's image Correlation using Algebra-Chaos Amalgam and DNA Transform

(a): Multiple Original and Encrypted Image Horizontal Correlation				(b): Multiple Original and Encrypted Image Vertical Correlation				(c): Multiple Original and Encrypted Image Diagonal Correlation				
	Red	Green	Blue		Red	Green	Blue		Red	Green	Blue	
Original Image	R	0.9542	0.5879	0.3852	R	0.9468	0.6062	0.3759	R	0.928	0.5838	0.3231
	G	0.3868	0.9663	0.9688	G	0.3701	0.9507	0.9633	G	0.3332	0.9358	0.9376
	B	0.3407	0.7677	0.9769	B	0.3275	0.7727	0.9661	B	0.358	0.7744	0.9505
Encrypted Image	R	-0.0076	0.0031	0.0155	R	-0.0098	-0.0063	0.0174	R	-0.0005	0.0028	0.0009
	G	-0.0122	0.0165	0.0325	G	0.0058	-0.0007	-0.0023	G	0.0014	-0.0042	-0.0051
	B	0.0009	0.006	0.01	B	0.0015	-0.007	-0.0004	B	0.0019	0.0148	-0.0069

Table 21. Lena image Correlation using Algebra-Chaos Amalgam and DNA Transform

(a): Horizontal Correlation of Multiple Original and Encrypted Image				(b): Vertical Correlation of Multiple Original and Encrypted Image				(c): Diagonal Correlation of Multiple Original and Encrypted Image				
	Red	Green	Blue		Red	Green	Blue		Red	Green	Blue	
Original Image	R	0.936	0.8021	0.6349	R	0.9422	0.8422	0.6546	R	0.9922	0.8049	0.5974
	G	0.5991	0.9288	0.8656	G	0.6557	0.9456	0.9166	G	0.5564	0.9711	0.7861
	B	0.6188	0.8227	0.8877	B	0.6843	0.869	0.9147	B	0.6068	0.8116	0.9814
Encrypted Image	R	0.0002	0.0038	-0.0001	R	0.0013	-0.0059	0.001	R	0.0017	-0.0027	-0.0023
	G	0.0049	-0.007	0.0088	G	0.0006	0.001	-0.0019	G	-0.0035	-0.0001	-0.0011
	B	0.0029	0.0023	-0.0022	B	0.0031	-0.0011	0.005	B	0.0022	0.0013	0.0034

Table 22. Baboon's image Correlation using Algebra-Chaos Amalgam and DNA Transform

(a): Horizontal Correlation of Multiple Original and Encrypted Image				(b): Vertical Correlation of Multiple Original and Encrypted Image				(c): Diagonal Correlation of Multiple Original and Encrypted Image				
	Red	Green	Blue		Red	Green	Blue		Red	Green	Blue	
Original Image	R	0.9551	0.3023	0.1362	R	0.94	0.3273	0.1312	R	0.9116	0.2775	0.1214
	G	0.1325	0.9232	0.939	G	0.1436	0.8933	0.9341	G	0.1029	0.8574	0.9069
	B	0.1299	0.7627	0.9511	B	0.1232	0.7478	0.9387	B	0.1182	0.7475	0.924
Encrypted Image	R	-0.0025	0.0066	-0.0005	R	0.0029	0.0064	0.0009	R	-0.0025	0.0016	0.0054
	G	0.0005	-0.003	-0.003	G	-0.0011	-0.0046	-0.0061	G	-0.0019	-0.0017	0.0028
	B	0.0007	0.001	0.0054	B	-0.0001	0.001	0.0072	B	0.0008	-0.0059	0.0012

Table 23. Fruits image Correlation using Algebra-Chaos Amalgam and DNA Transform

(a): Horizontal Correlation of Multiple Original and Encrypted Image				(b): Vertical Correlation of Multiple Original and Encrypted Image				(c): Diagonal Correlation of Multiple Original and Encrypted Image				
	Red	Green	Blue		Red	Green	Blue		Red	Green	Blue	
Original Image	R	0.9796	0.7179	0.5526	R	0.9616	0.7215	0.5467	R	0.9477	0.702	0.5327
	G	0.5759	0.9738	0.9779	G	0.5221	0.9711	0.967	G	0.5445	0.9546	0.97
	B	0.5254	0.7218	0.9777	B	0.5294	0.702	0.9815	B	0.5566	0.6795	0.9463
Encrypted Image	R	-0.003	-0.003	0.0019	R	-0.0066	-0.002	-0.0002	R	-0.0021	-0.0018	0.0011
	G	-0.0011	0.0002	0.0031	G	0.0007	0.0022	0.0045	G	0.0014	-0.0031	0.0028
	B	0.0002	0.0039	-0.0003	B	0.0011	0.0039	0.0002	B	-0.0024	-0.0029	-0.0006

Table 24. Aeroplane's image Correlation using Algebra-Chaos Amalgam and DNA Transform

(a): Horizontal Correlation of Multiple Original and Encrypted Image				(b): Vertical Correlation of Multiple Original and Encrypted Image				(c): Diagonal Correlation of Multiple Original and Encrypted Image				
	Red	Green	Blue		Red	Green	Blue		Red	Green	Blue	
Original Image	R	0.9666	0.9253	0.7951	R	0.929	0.8871	0.7755	R	0.9277	0.8443	0.752
	G	0.8025	0.9758	0.9826	G	0.7918	0.9584	0.9717	G	0.7678	0.9421	0.9331
	B	0.8159	0.9373	0.9799	B	0.7743	0.9044	0.9541	B	0.7483	0.8859	0.9409
Encrypted Image	R	-0.0084	0.0012	0.0043	R	0.0017	-0.0003	-0.0011	R	-0.0055	0.001	-0.0054
	G	-0.0007	0.0163	0.0031	G	-0.0008	0.0038	-0.0013	G	-0.0028	-0.0015	0.0042
	B	0.0025	-0.002	0.0028	B	-0.0028	0.0001	0.0027	B	-0.01	0.0137	0.0012

As an affective digital image cyphering plan has a value of correlation of near to zero. Hereby, from Tables 20-24 it is clear that different attacks like differential attack is resisted by the proposed scheme.

Fig. 36, 37 & 38 gives horizontal, vertical and diagonal correlation plots, respectively.

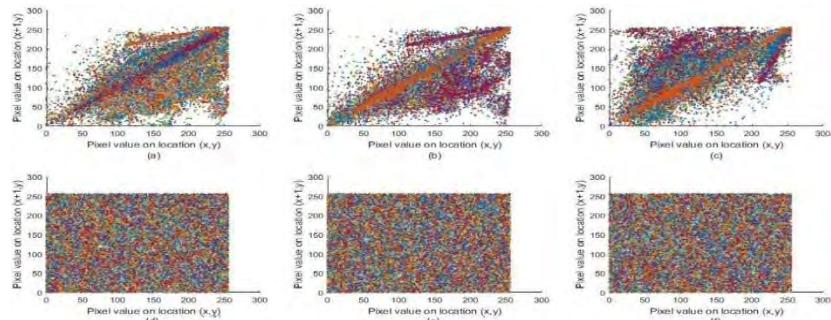


Figure 36. Original multiple image Red, Green and Blue layers Horizontal correlation are shown by (a), (b), (c) respectively. Whereas, that of encrypted are shown in (d), (e), (f) respectively.

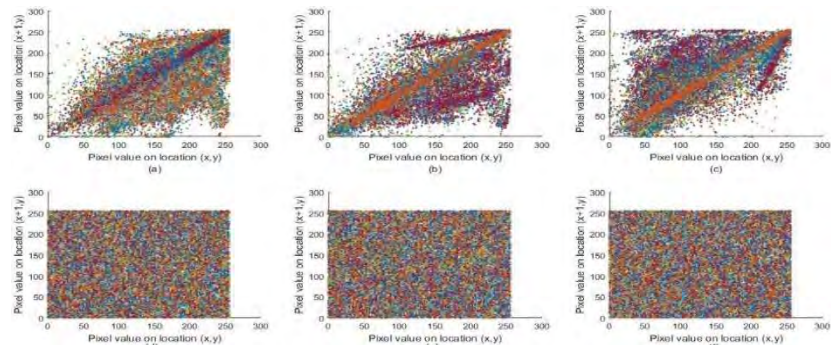


Figure 37. Original multiple image Red, Green and Blue layers vertical correlation are shown by (a), (b), (c) respectively. Whereas, that of encrypted are shown in (d), (e), (f) respectively.

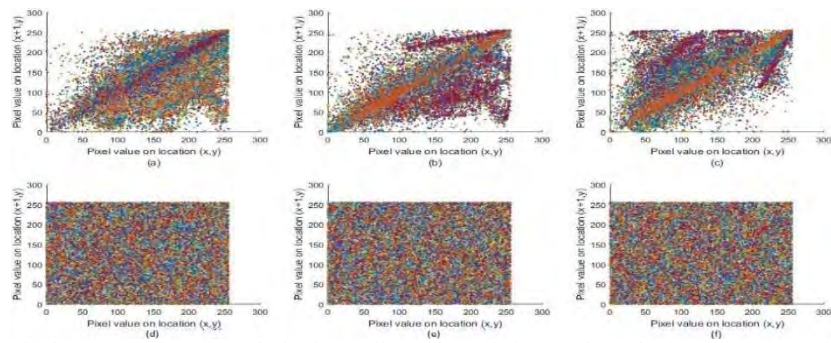


Figure 38. Original multiple image Red, Green and Blue layers diagonal correlation are shown by (a), (b), (c) respectively. Whereas, that of encrypted are shown in (d), (e), (f) respectively

Fig. 36-38 represents the correlation of Original multiple image Red, Green and Blue layers (1st row) with encrypted red green and blue layers (corresponding 2nd row) respectively. It is clear from these figures that the original correlation scatter plot is not uniform whereas, the encrypted

correlation plots are uniform. Therefore, this fact guarantees that the presented scheme gives full resistance to any of the existing plaintext search attack.

In case of *Improved SERPENT Algorithm: Design to RGB Image Encryption Implementation* the correlation table for adjacent pixels of various standard images are given in table 25-26 for various images.

Table 25. Lena Original and Encrypted Image correlation using Improved SERPENT Algorithm

(a): Lena Original and Encrypted Image Horizontal Correlation				(b): Lena Original and Encrypted Image Vertical Correlation				(c): Lena Original and Encrypted Image Diagonal Correlation				
	Red	Green	Blue		Red	Green	Blue		Red	Green	Blue	
Original Image	R	0.9371	0.8177	0.6292	R	0.9575	0.8333	0.6234	R	0.893	0.7699	0.5489
	G	0.6098	0.9288	0.8402	G	0.6163	0.9464	0.9106	G	0.611	0.89	0.7861
	B	0.5917	0.7805	0.8257	B	0.6706	0.8717	0.9288	B	0.6132	0.8299	0.8391
Encrypted Image	R	0.007	-0.0221	-0.0187	R	0.007	0.0055	-0.0008	R	-0.0034	-0.0019	-0.0023
	G	0.0064	-0.0054	-0.0268	G	-0.0306	-0.0009	0.063	G	0.0004	0.0121	-0.0046
	B	0.003	0.0034	-0.0022	B	0.0096	-0.0033	0.0002	B	-0.0037	-0.0055	0.0088

Table 26. Baboon Original and Encrypted Image correlation using Improved SERPENT Algorithm

(a): Baboon Original and Encrypted Image Horizontal Correlation				(b): Baboon Original and Encrypted Image Vertical Correlation				(c): Baboon Original and Encrypted Image Diagonal Correlation				
	Red	Green	Blue		Red	Green	Blue		Red	Green	Blue	
Original Image	R	0.9229	0.1094	0.1362	R	0.8778	0.0187	-0.0939	R	0.8649	0.2775	0.1214
	G	0.1325	0.8039	0.879	G	0.1436	0.7461	0.8572	G	0.1029	0.7074	0.9069
	B	-0.0292	0.6394	0.8741	B	0.1232	0.6661	0.8606	B	0.1182	0.66	0.8431
Encrypted Image	R	0.0062	0.0072	-0.0073	R	0.0078	-0.002	-0.0023	R	-0.009	-0.0007	0.0044
	G	0.0005	-0.0002	0.0085	G	0.0018	0.0008	-0.001	G	0.0061	0.0081	0.0009
	B	0.0039	0.0022	0.0074	B	0.009	-0.0035	-0.0005	B	0.0008	0.0096	0.0046

Since a good digital image encryption scheme has correlation values near 0. Therefore, tables 25-26 are evident of the fact that the presented scheme resists different attacks like differential attack.

Figures 39, 40 and 41 are scatter plot of horizontal, vertical and diagonal component of the original and encrypted Lena image respectively.

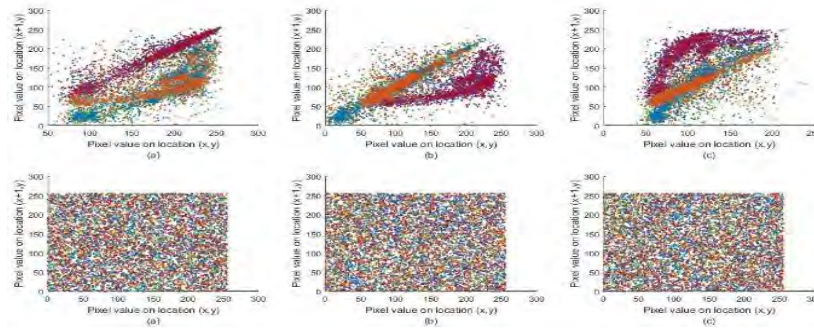


Figure 39. (a), (b), (c) represents Horizontal correlation of RGB layers of Lena Original image and (d), (e), (f) are the horizontal correlation of RGB layers of encrypted Lena image.

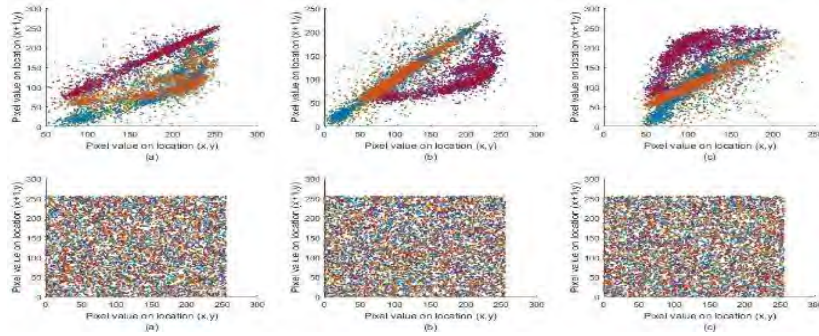


Figure 40. (a), (b), (c) represents Vertical correlation of RGB layers of Original Lena image and (d), (e), (f) are the Vertical correlation of RGB layers of encrypted Lena image.

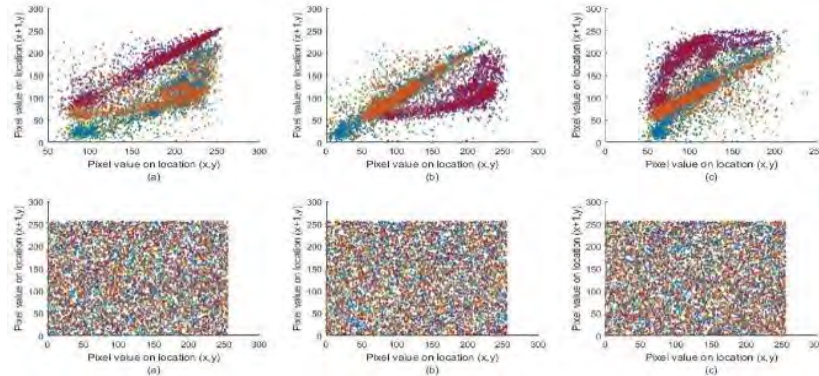


Figure 41. (a), (b), (c) represents Diagonal correlation of RGB layers of Original Lena image and (d), (e), (f) are the Diagonal correlation of RGB layers of encrypted Lena image.

In case of “Astronomical images digital Image Encryption Implementation” the correlation table for adjacent pixels of various standard images are given in table 27-28 for various images.

Table 27. Earth’s image correlation using 24-bit S-box

(a): Horizontal Correlation of Earth’s Original and Encrypted Image				(b): Vertical Correlation of Earth’s Original and Encrypted Image				(c): Diagonal Correlation of Earth’s Original and Encrypted Image				
		Red	Green	Blue		Red	Green	Blue		Red	Green	Blue
Original Image	R	0.953178	0.949018	0.813458	R	0.939407	0.933721	0.821358	R	0.921649	0.92582	0.794213
	G	0.82139	0.951948	0.950711	G	0.799829	0.957385	0.940488	G	0.79302	0.92609	0.920302
	B	0.811764	0.857943	0.957416	B	0.825163	0.852307	0.947158	B	0.793473	0.831137	0.935001
Encrypted Image	R	-0.01177	-0.02107	0.0522	R	0.006762	0.003168	-0.01657	R	0.0011859	-0.002453	0.0024458
	G	-0.01947	0.029483	-0.01211	G	-0.0538	0.037244	0.005917	G	-0.003781	-0.000652	0.0057911
	B	0.011615	-0.01867	0.063903	B	-0.00916	-0.0199	-0.06829	B	0.0027882	0.0020721	0.004244

Table 28. Sun Original and encrypted image Correlation using 24-bit S-box

(a): Horizontal Correlation of Sun Original and Encrypted Image				(b): Vertical Correlation of Sun Original and Encrypted Image				(c): Diagonal Correlation of Sun Original and Encrypted Image				
		Red	Green	Blue		Red	Green	Blue		Red	Green	Blue
Original Image	R	0.9962	0.8175	0.4682	R	0.9964	0.8074	0.4388	R	0.9930	0.8103	0.4653
	G	0.4450	0.9833	0.9264	G	0.4728	0.9831	0.9356	G	0.4589	0.9691	0.8745
	B	0.4772	0.7210	0.9290	B	0.4761	0.7264	0.9272	B	0.4716	0.7217	0.8513
Encrypted Image	R	-0.0055	0.0042	-0.0009	R	0.0001	-0.0037	-0.0009	R	-0.0036	0.0036	-0.0025
	G	0.0060	0.0037	-0.0008	G	-0.0008	0.00026	-0.0039	G	-0.0002	-0.0018	-0.0055
	B	-0.0002	-0.0026	-0.0035	B	-0.0005	-0.0023	-0.0011	B	-0.0023	0.0002	-0.0009

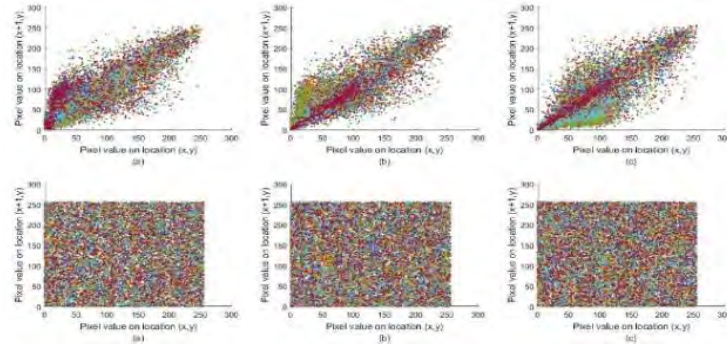


Figure 42. (a), (b), (c) show horizontal Correlation of pixels of Earth image and (d), (e), (f) show Vertical Correlation of pixels of Earth ciphered image

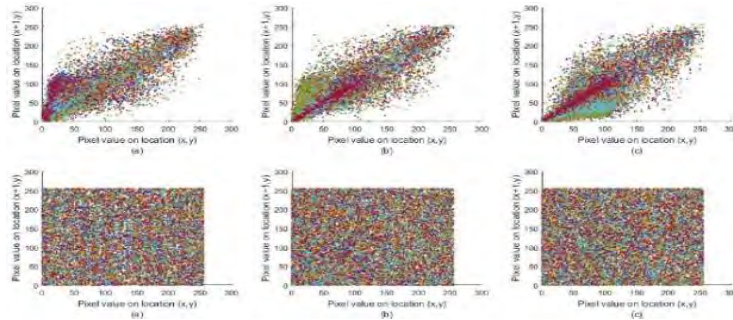


Figure 43. (a), (b), (c) show Vertical Correlation of pixels of Earth image and (d), (e), (f) show Vertical Correlation of pixels of Earth ciphered image

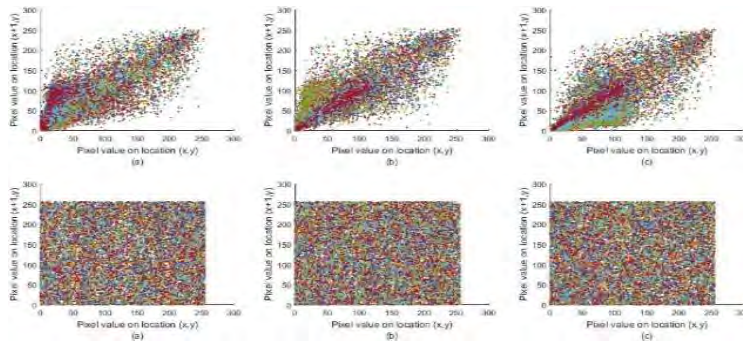


Figure 44. (a), (b), (c) show diagonal Correlation of pixels of Earth image and (d), (e), (f) show diagonal Correlation of pixels of Earth ciphered image

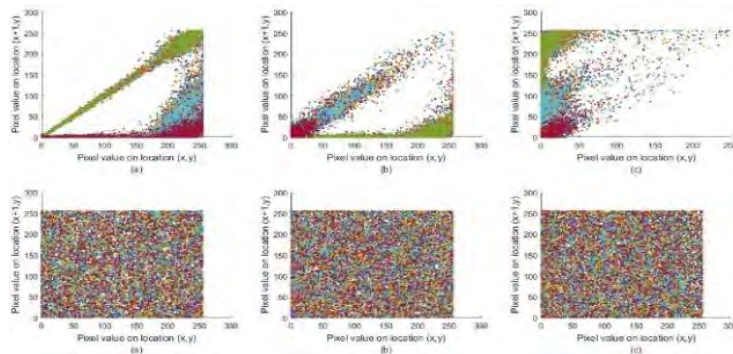


Figure 45. (a), (b), (c) show horizontal Correlation of pixels of Sun image and (d), (e), (f) show horizontal Correlation of pixels of Sun ciphered image

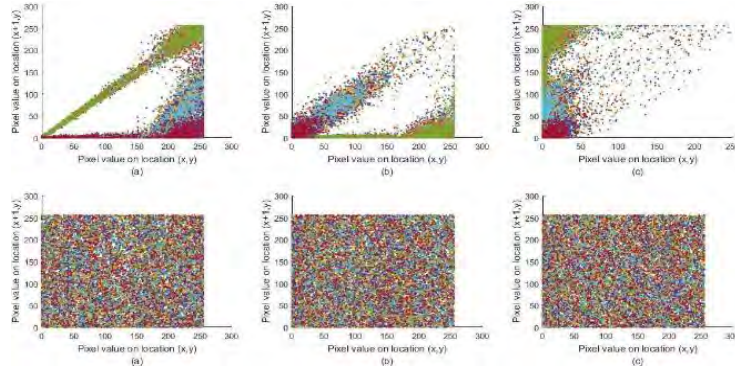


Figure 46. (a), (b), (c) show vertical Correlation of pixels of Sun image and (d), (e), (f) show vertical Correlation of pixels of Sun ciphered image

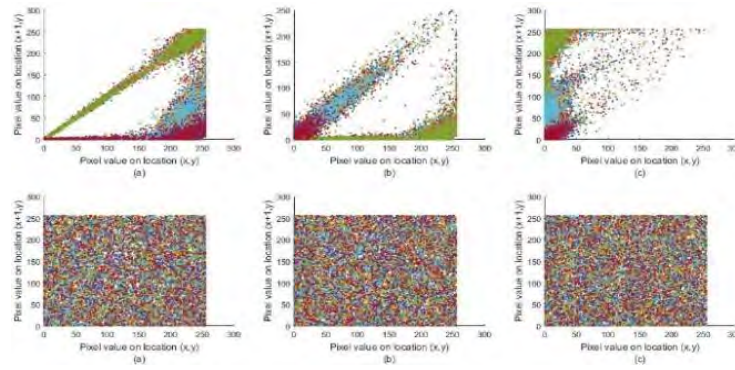


Figure 47. (a), (b), (c) show diagonal Correlation of pixels of Sun image and (d), (e), (f) show diagonal Correlation of pixels of Sun ciphered image

Figure 47 shows correlation of neighbor pixels of astronomical plain digital images and there corresponding enciphered images.

6.2 Noise analysis

This section analyzes the behavior of our encryption-decryption system with noises. Some form of noise is always there in a channel of transmission [66]. An encrypted image must be adversely affected by some noises throughout the transmission. Therefore, the decryption algorithm of the proposed scheme must be noise-resistant in such a manner that the images after decryption is in human understandable form even if the noise contaminates it while transmitting. Hence, in this section, it is to be proven that in order to generate an image which is recognizable from the encrypted image containing noise, the decryption system is capable enough. The following types of noises are considered for analysis:

6.2.1 Salt and Pepper analysis

Impulsive noise or the one with fat-tail distribution is occasionally known as Salt-and-Pepper noise/Spike noise [67]. An image having such noise is characterized by bright regions having dark pixels and dark regions having bright pixels. Such noise can be the result of analog to

digital converter errors, transmission's bit errors etc. Techniques like dark frame subtraction, median filtering, combined filtering of median & mean and interpolation around the bright or dark pixels can be used to eliminate such noise. Different encrypted images (and their corresponding deciphered images) affected with low, default and high salt noises are respectively shown in Figure 48 and Figure 51. Figures indicate that the deciphered images can still be recognized, even after the ciphered images are affected by the noise.

In case of 12×12 S-box Design and its Application to RGB Image Encryption the Salt and Pepper noise added to Lena and Fruits encrypted image and its corresponding ciphered images is shown in figure 48-49.

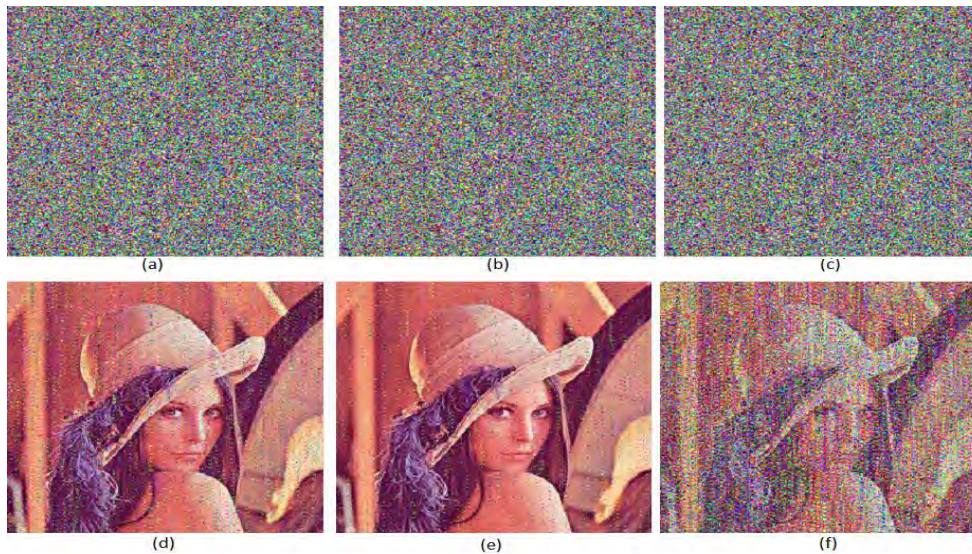


Figure 48. (a), (b) and (c) shows the encrypted images of color Lena image with minimum, default and maximum salt & pepper noise. (d), (e) and (f) shows the decrypted images of color Lena image with minimum, default and maximum salt & pepper noise.

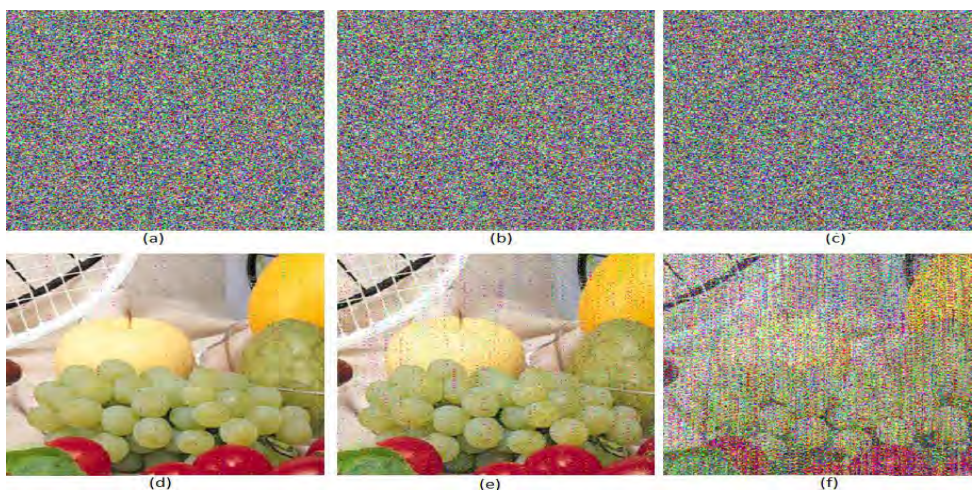


Figure 49. (a), (b) and (c) shows the encrypted images of color Fruits image with minimum, default and maximum salt & pepper noise. (d), (e) and (f) shows the decrypted images of color Fruits image with minimum, default and maximum salt & pepper noise.

In case of *Algebra-Chaos Amalgam and DNA Transform based Multiple Digital Image Encryption* the Salt and Pepper noise added to Lena encrypted image and its corresponding ciphered images is shown in figure 50.

Different cipher images that are affected by such type of noise is shown in the 1st, 2nd and 3rd columns of Fig. 50 with minimum, default and high salt and Pepper noise respectively. This Fig. 50 also shows that the encrypted images after being affected by the noise is recognizable in the decrypted form. Last three columns indicate the decrypted form of the corresponding cipher images.

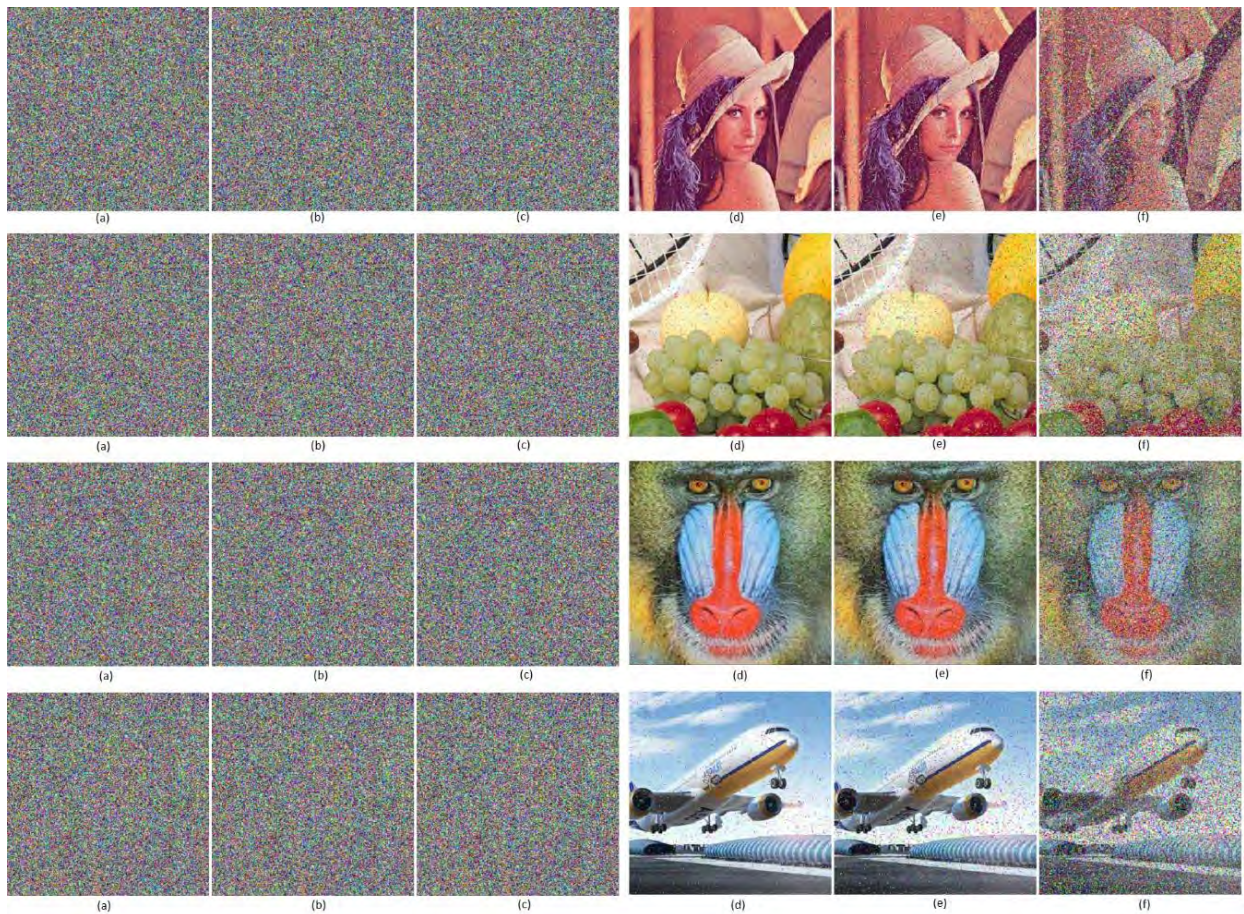


Figure 50. (a), (b) and (c) represent encrypted images containing Salt and Pepper noise whereas (d), (e) and (f) are there decrypted images respectively.

In each row of Fig. 50. (a), (b) and (c) represent encrypted images containing Salt and Pepper noise whereas (d), (e) and (f) are there decrypted images respectively. The decrypted images show that after adding Salt and Pepper noise to encrypted images, the decrypted images are recognizable.

In case of *Improved SERPENT Algorithm: Design to RGB Image Encryption Implementation* the Salt and Pepper noise added to Lena, Baboon, Fruits and Aeroplane encrypted image and its corresponding ciphered images is shown in figure 51.

We apply this noise attack to some standard images and get figure 51. In figure 51, the 1st, 2nd and 3rd column shows the encrypted image with low, average and maximum noise respectively. Whereas the 4th, 5th and 6th column are their corresponding decrypted images.

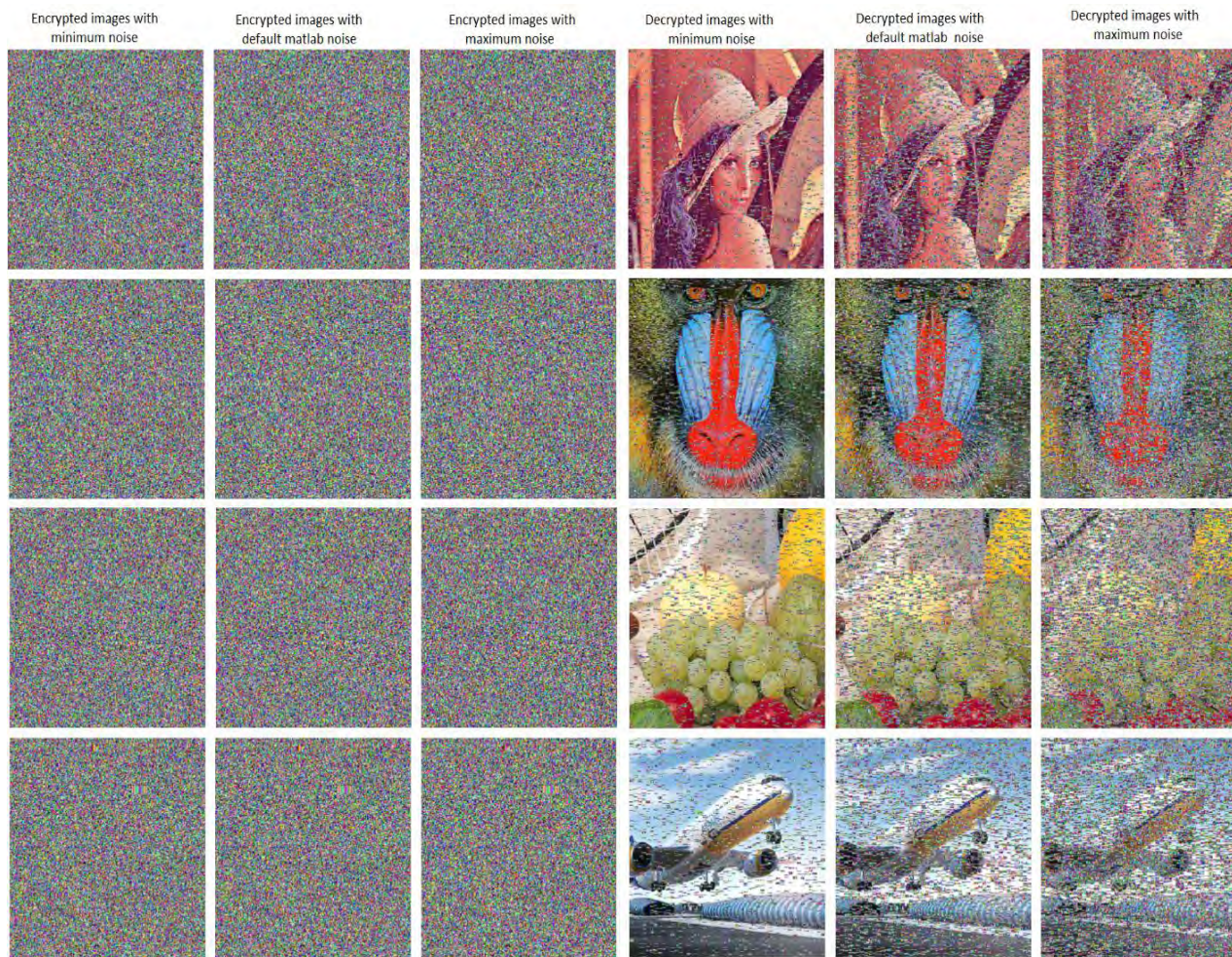


Figure 51. Column 1-3 represent small, default and maximum noisy encrypted image of Lena, Baboon, Fruits and Aeroplane respectively. The corresponding decrypted images are shown in column 4-6.

From figure 51, one can easily judge that in each case of noise addition we can retrieve the original image and the decrypted image is in human-readable form.

In case of *24-by-24 S-box encryption scheme* the salt and pepper noise is added to Earth encrypted image. The Earth's ciphered images are constantly affected by low; high, and default salt noise shown in 1st row of Figure 52. However, 2nd row of the Figure 52 shows decrypted

images of the corresponding plain images. It is clearly shown from statistics that decrypted visuals are still in recognizable form even the encrypted images are provoked by noise.

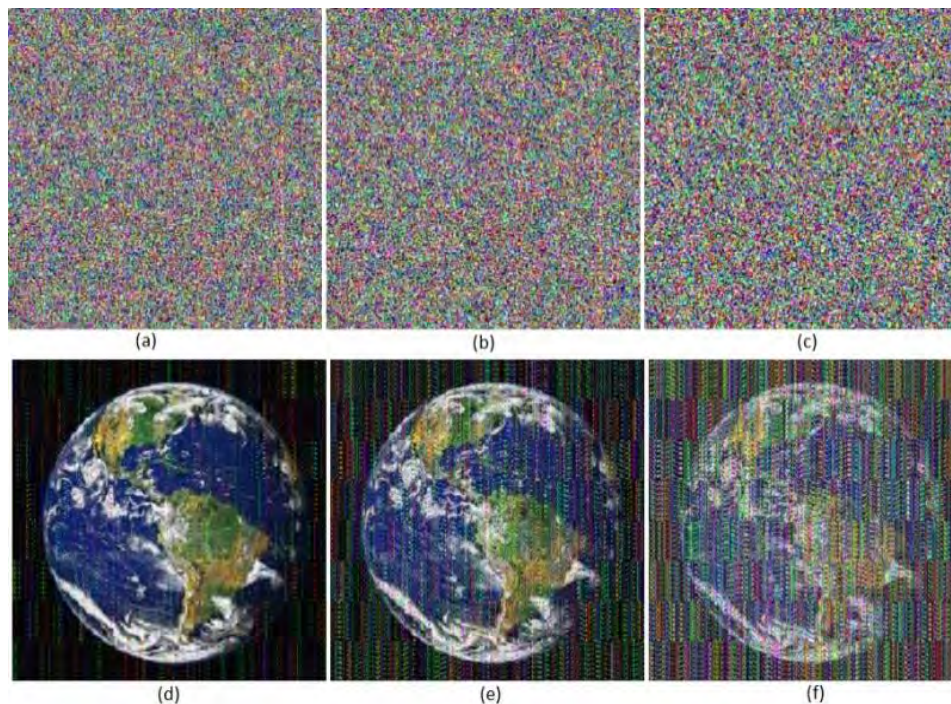


Figure 52. Earth enciphered images are given in (a), (b) and (c) with small, default and large salt & pepper noise. Earth deciphered images are given in (d), (e) and (f) with small, default and large salt & pepper noise.

6.2.2 Speckle noise

It is a rough or granulated noise exists in the images intrinsically and spoils the images' quality [68]. Constructive and destructive interference that are indicated as bright and dark dots in the images causes this noise. Different encrypted images affected with low, default and high speckle noises respectively are given in the Figures 53-56. Deciphered forms of the respective encrypted images are shown in second row of the Figures 52-56. It is indicated in the figures that even if the ciphered images are affected by the said noise, the de-ciphered images can still be recognized.

In case of *12×12 S-box Design and its Application to RGB Image Encryption* the Speckle noise added to Lena, and Fruits encrypted image and its corresponding ciphered images is shown in figures 53-54.

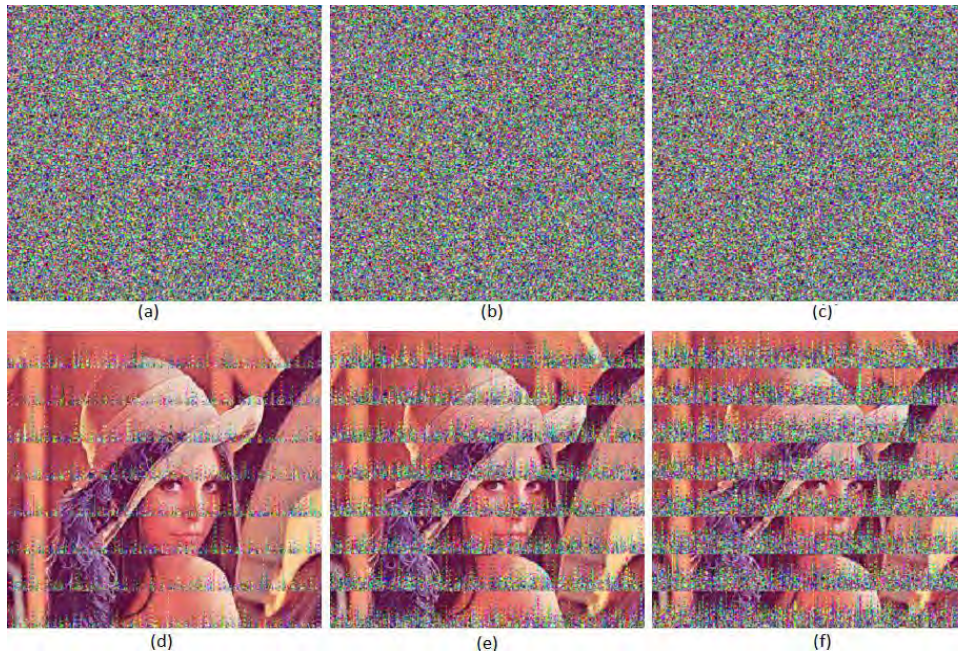


Figure 53. (a), (b) and (c) shows the encrypted images of color Lena image with minimum, default and maximum Speckle noise. (d), (e) and (f) shows the decrypted images of color Lena image with minimum, default and maximum Speckle noise.

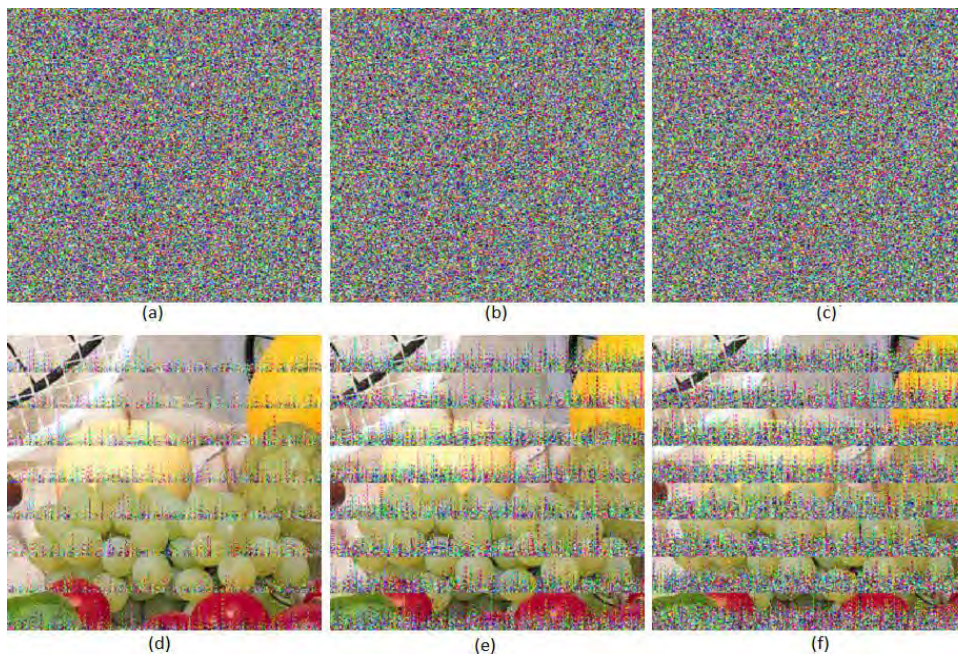


Figure 54. (a), (b) and (c) shows the encrypted images of color Fruits image with minimum, default and maximum Speckle noise. (d), (e) and (f) shows the decrypted images of color Fruits image with minimum, default and maximum Speckle noise.

In case of *Algebra-Chaos Amalgam and DNA Transform based Multiple Digital Image Encryption* the speckle noise added to Lena, Fruits, Baboon and Aeroplane encrypted image and its corresponding ciphered images is shown in figure 55.

Fig. 55 shows that the decrypted images are in human-readable form even if the encrypted images are affected with Speckle noise.

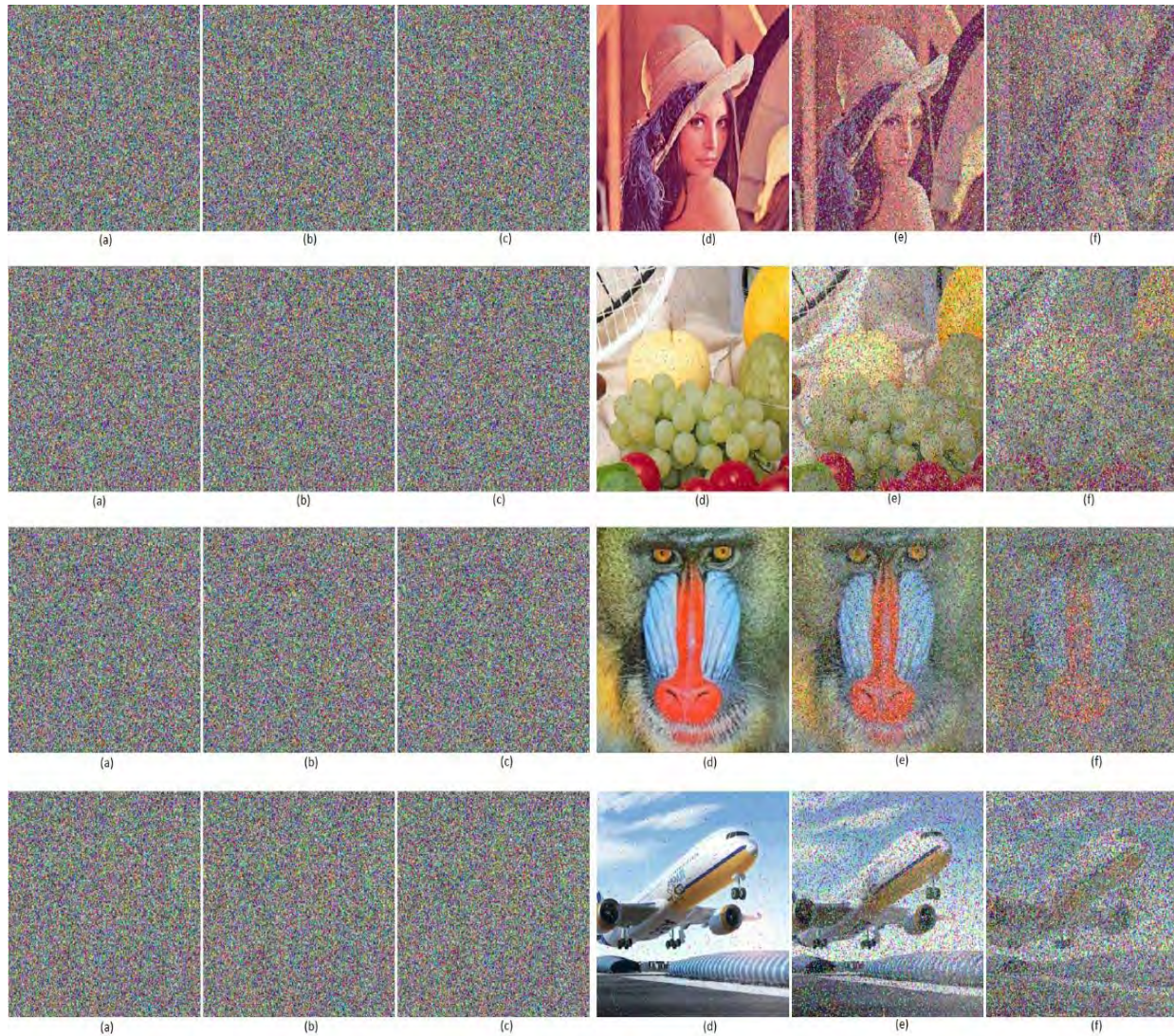


Figure 55. (a), (b) and (c) represent encrypted images containing Speckle noise whereas (d), (e) and (f) are their decrypted images respectively.

Each row in Fig. 56. (a), (b) and (c) represent encrypted images containing Speckle noise whereas (d), (e) and (f) are their decrypted images respectively. The decrypted images show that after adding Speckle noise to encrypted images, the decrypted images are recognizable.

In case of *24-by-24 S-box RGB Image Encryption* the Speckle noise added to earth encrypted image and its corresponding ciphered images are obtained by using the encrypted algorithm. The results for minimum, default and maximum speckle noise added to earth image is shown in figure 56.

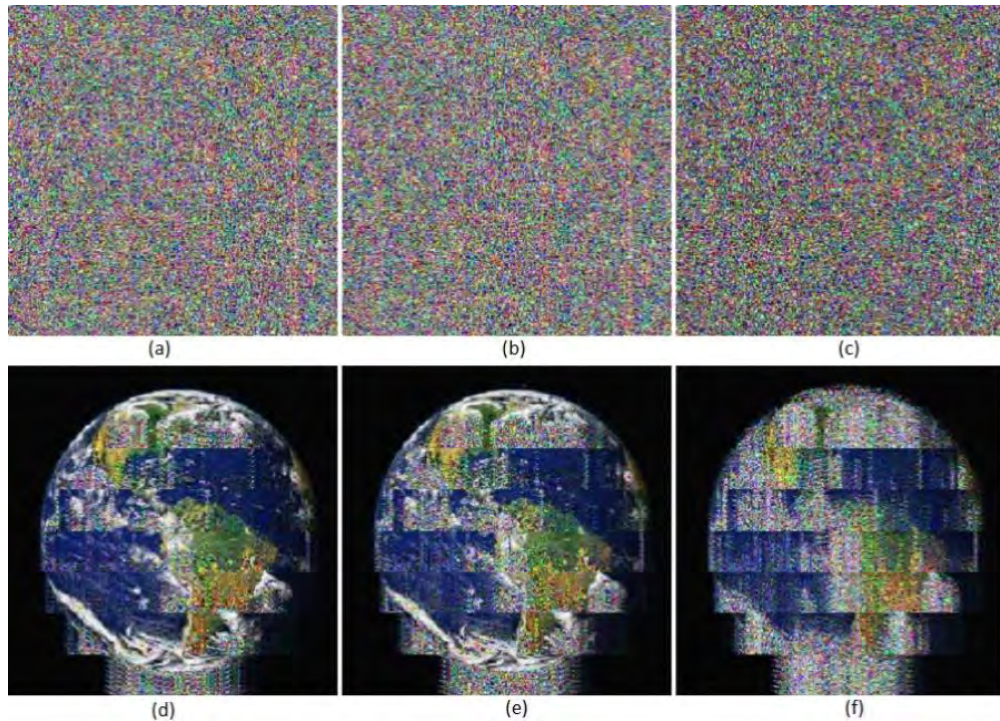


Figure 56. Earth enciphered images are given in (a), (b) and (c) with small, default and large Speckle noise. Earth deciphered images are given in (d), (e) and (f) with small, default and large Speckle noise.

6.2.3 Shot noise/Poisson noise

Image taken from an image sensor have dominant noise in the form of darker parts, caused by statistical quantum fluctuations i.e. photons' number's variation that is sensed at a particular level of exposure [69]. Such a noise is called photon shot noise. The root mean square value of shot noise is directly proportional to the image intensity's square root. Furthermore, these noises are independent of each other at different pixels. Poisson distribution is followed by a shot noise and hence also called Poisson noise. In Figure 57;(a) and (b) shows the encrypted images of color Lena and color Fruits image with Poisson noise respectively in the first row. Their respective decrypted forms are shown in the 2nd row. It is clearly proved in Figure 57 that even if ciphered images are affected by Poisson/Shot noise, the deciphered imaged are still recognizable. In case of 12×12 S-box Design and its Application to RGB Image Encryption the Poisson noise added to Lena, and Fruits encrypted image and its corresponding ciphered images is shown in figure 57.

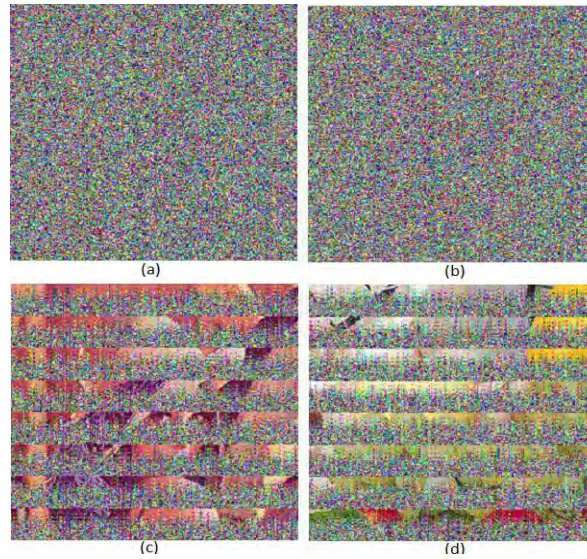


Figure 57. (a) and (b) shows the encrypted images of color Lena and color Fruits image with Poisson noise respectively. (c) and (d) represents the decrypted images (a) and (b) respectively.

In case of Algebra-Chaos amalgam and DNA transform based multiple digital image encryption the poisson noise added to Lena, and Fruits encrypted images and their corresponding ciphered images are shown in figure 58.

In Fig. 58, a maximum Poisson noise is added to encrypted images (i.e. the first column) whereas, the second column shoes the corresponding decrypted noisy images.

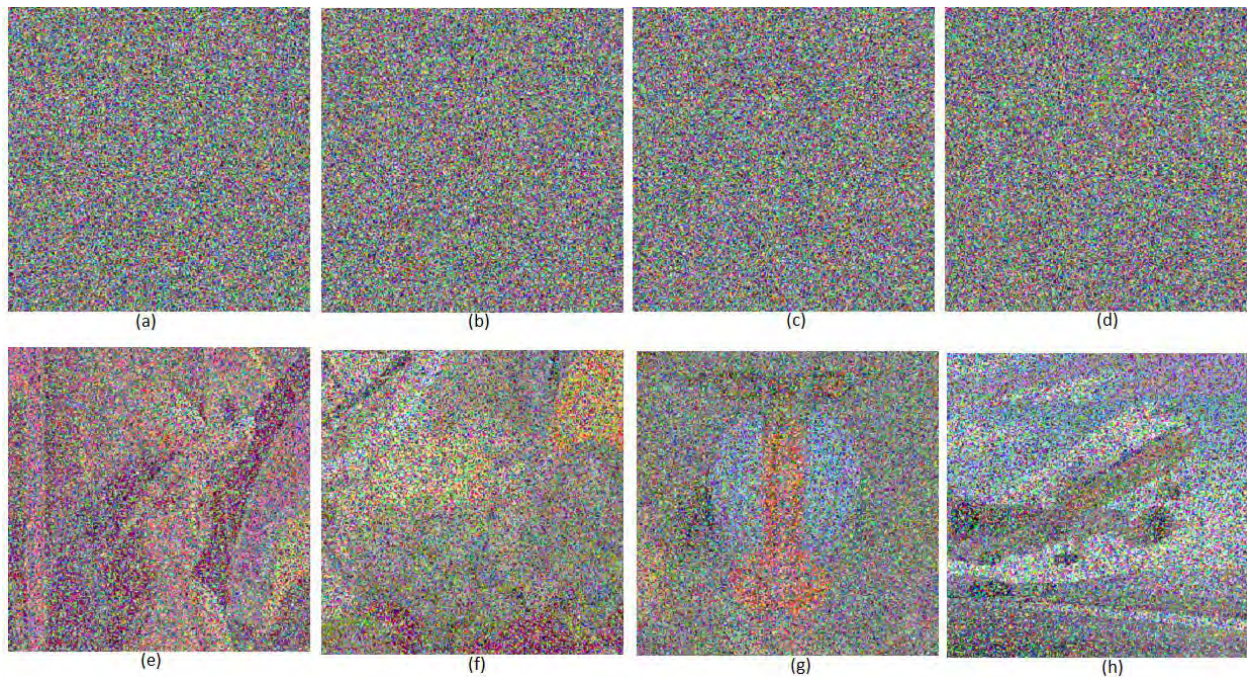


Figure 58. (a), (b), (c) and (d) represent encrypted images containing Poisson noise whereas, (e), (f), (g) and (h) are there decrypted images respectively.

Fig. 58 clearly proves that the decrypted images are recognizable even if the encrypted images are affected with Poisson noise.

From figure 59, it is easy to analyze that the deciphered images are in human readable form even if the Poisson noise is added to the ciphered (*using 24-by-24 replacement matrix*) image.

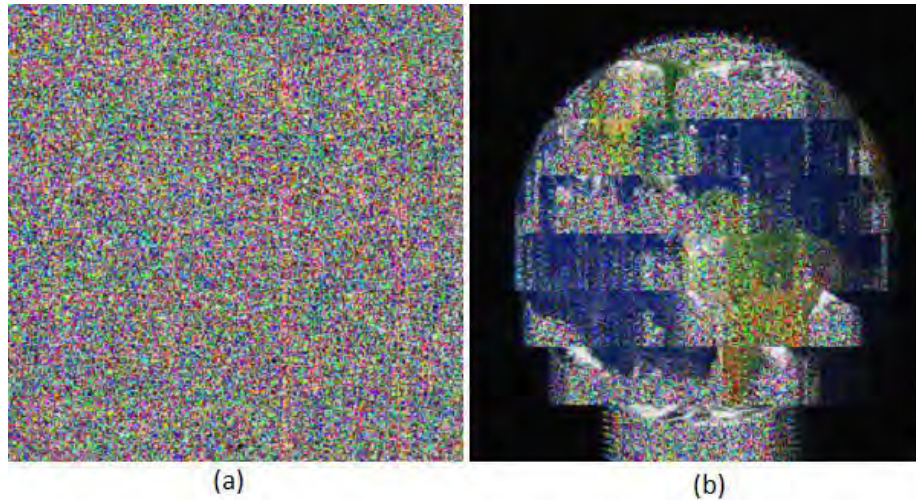


Figure 59. Earth enciphered digital image with Photon noise is given in (a) and its corresponding deciphered Earth image is given in (b).

6.3 Occluded attack

This section comprises of the robustness attack when data is occluded [70]. The encrypted RGB is first occluded with 25% and then with 50%. The occlusion is performed from top, left, bottom and right for 25% and from top, bottom, right and left for 50%. The occluded figures are shown figure 60-62. These occluded encrypted images are then decrypted with the inverse of proposed program. Clearly, figure 60-62 shows that the decrypted images after occlusion are understandable. This analysis insures the strength of the planned scheme against the occluded attack on color digital image data. Moreover, the proposed scheme is robust against from center. Also, for 50% upper diagonal, lower diagonal the attack is examined. The enciphered and deciphered Lena images cutted from centers and diagonals are shown in figure 62. Thus, the below figures analysis indicates that the proposed scheme is robust against the occlusion attack.

In case of 12×12 S-box Design and its Application to RGB Image Encryption the occluded attack is given in the figures 60-62.

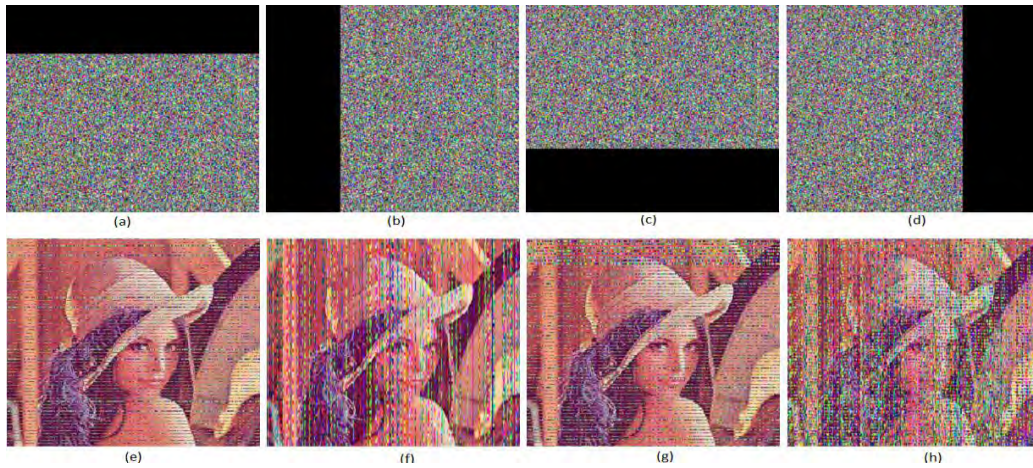


Figure 60. (a), (b), (c) and (d) shows the encrypted images of color Lena image with 25% occluded from above, left, bottom and right respectively. (e), (f), (g) and (h) shows the decrypted images of (a), (b), (c) and (d) respectively.

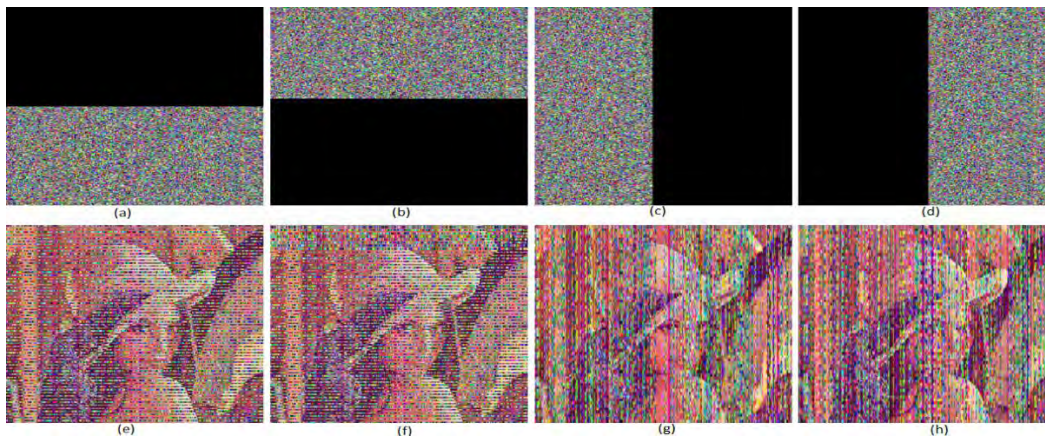


Figure 61. (a), (b), (c) and (d) shows the encrypted images of color Lena image with 50% occluded from top, bottom right and left respectively. (e), (f), (g) and (h) shows the decrypted images of (a), (b), (c) and (d) respectively.

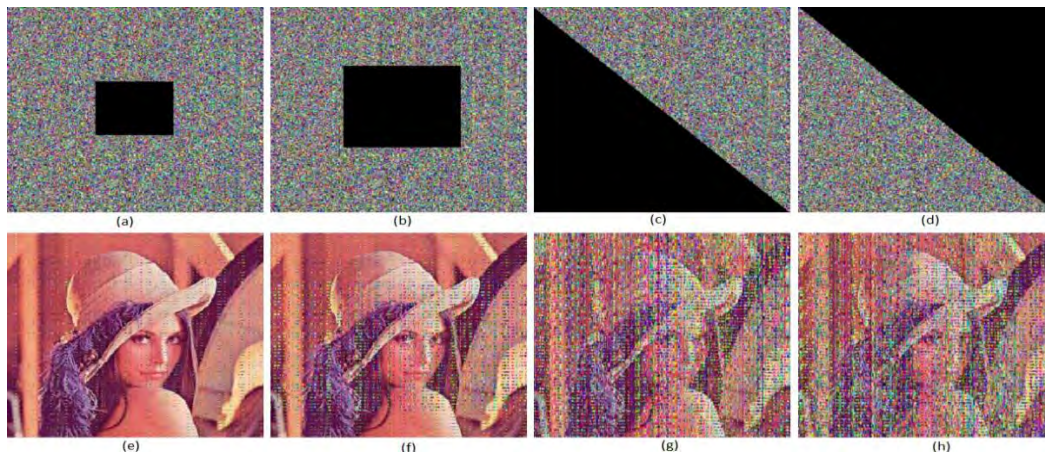


Figure 62. (a) and (b) shows the encrypted images of color Lena image occluded from center. (c) and (d) are upper triangular and lower triangular occluded respectively. (e), (f), (g) and (h) shows the decrypted images of (a), (b), (c) and (d) respectively.

6.4 Differential analyses

A plain image can be retrieved by various attacks. One of the most robust attack, regarding to retrieving an image, is the differential analysis. Differential analysis is further divided into two subcategories, namely; the number of pixels change rate (NPCR) and the unified average changing intensity (UACI).

6.4.1 Number of pixels change rate (NPCR)

The 'Number of Pixels Change Rate' [71] gives value of change in the no. of pixels of cyphered digital images when a little disturbance in the primary original image occurs. The Number of Pixels Change Rate value close to 99.609 percent is illustrate the best sensitivity of a cryptosystem and therefore offers great resistance to hackers. The NPCR of these two images is defined as

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{M \times N}, \text{ where } D(i,j) = \begin{cases} 0, & \text{if } C_1(i,j) = C_2(i,j) \\ 1, & \text{if } C_1(i,j) \neq C_2(i,j) \end{cases}$$

Where C_1 and C_2 are two ciphred images resulting from plain image and one-pixel difference in plain image respectively.

6.4.2 UACI

The UACI [71] directs the average intensity of difference between plain image and ciphred image. As the UACI value moves towards 33.4635% the algorithm exposes its power against differential attacks. The NPCR and UACI values can be measure by the relation:

$$\text{UACI} = \frac{1}{M \times N} \sum_{i,j} \left[\frac{|C_1(i,j) - C_2(i,j)|}{255} \right]$$

Where C_1 and C_2 are two ciphred images resulting from plain image and one-pixel difference in plain image respectively.

Table 29. Differential analyses for $\frac{F_2[x]}{\langle x^{12} \rangle}$ Dependent color images in comparison with existing encryption techniques

Schemes		NPCR			UACI		
		Red	Green	Blue	Red	Blue	Green
Proposed	(Chapter 2)	0.9966	0.9963	0.9962	0.334	0.3338	0.334
Proposed	(Chapter 3)	0.996429	0.995956	0.995285	0.327633	0.300491	0.275669
Proposed	(Chapter 4)	99.5880	99.6109	99.6277	0.4003	0.3874	0.3705
Proposed	(Chapter 5)	99.6206			0.3053		
Ref. [72]		0.9961	0.9955	0.9969	0.3346	0.3339	0.3354
Ref. [73]		0.985	0.985	0.985	0.321	0.321	0.321
Ref. [74]		0.9468	0.9568	0.9868	0.3346	0.345	0.3549
Ref. [75]		0.9958 (average)			0.3051 (average)		
Ref. [76]		0.9960	0.9961	0.9961	0.3356	0.3345	0.3349
Ref. [77]		0.9961	0.9960	0.9960	0.3346	0.3350	0.3347
Ref. [78]		0.9960	0.9960	0.9960	0.3336	0.3343	0.3337
Ref. [79]		0.9963	0.9960	0.9960	0.3360	0.3330	0.3340
Ref. [80]		0.9960	0.9959	0.9959	0.3344	0.3346	0.3347
Ref. [81]		0.9966	0.9954	0.9967	0.3312	0.3400	0.3390
Ref. [82]		99.8022			0.333		
Ref. [83]		99.419			0.333		
Ref. [84]		99.6198			0.3158		

From table 29, it is clear that the NPCR and the UACI values of the suggested $\frac{F_2[x]}{\langle x^{12} \rangle}$ encryption technique are in the limiting period. In order to fix the rank of the proposed scheme, a comparison with symmetric key cryptosystems is also given in table 29.

6.5 Texture analysis of the proposed scheme for encryption

Texture is the utmost valued characteristics of a digital image. Besides with color, it defines the appearance of surface of a digital picture. Analysis of Texture can be made by adopting different ways like Fourier or wavelet approach. Nevertheless, the finest examination is interesting as it is verified to be related to the way of human system (HS) of vision observing texture, a very starting line to texture, and it has a very important use in segmentation of image.

There are 5 different features of an image that are filed to define texture: Contrast, Energy, Homogeneity and Entropy

6.5.1 Contrast

This term is used by the observers to differentiate the bits and parts of a digital image. The unpredictability of an encrypted image is directly proportional to the value of contrast level. Contrast of maximum value implies robust encryption. Its value increases as the confusion in data increases. Therefore, this factor of an image processing can be improved by using S-boxes of good quality. The mathematical form of contrast is given by the equation:

$$C = \sum_m \sum_n (m - n)^2 f(m, n)$$

For constant image; Contrast=0.

6.5.2 Energy

The localized change of an RGB image gives the energy of a digital medium. Mathematically, it can be defined as the component in GLCM (gray-level co-occurrence matrix) squared summation & is given by the equation following equation.

$$E = \sum_m \sum_n f^2(m, n),$$

where m and n image pixels. The function $f(m, n)$ gives the number of GLCM.

Remark 4

For a constant image the energy is 1.

6.5.3 Homogeneity

The pixels of a digital medium are scattered positively. The homogeneity analysis rates the affinity of dispersed pixels of GLCM to GLCM diagonal. It is also known as “Gray Tone Spatial Dependency Matrix”. It is used to measure the number of assembling of pixel gray levels in tabular form. The homogeneity of an image can be calculated by the equation given bellow.

$$H^* = \sum_m \sum_n \frac{f(m, n)}{1 - |m - n|}$$

The homogeneity & contrast & energy of plain multiple digital medium & encrypted multiple digital mediums under consideration is shown in table 30.

Table 30. Second order texture analyses for given and enciphered images

Evaluated Images	Texture analyses		Plain color components of image			Cipher color components of image		
			R	G	B	R	G	B
Lena Image	Contrast	Chapter 2	0.52284	0.564982	0.501088	10.1692	9.98445	10.3386
		Chapter 3	0.394088	0.386226	0.391248	10.4563	10.4677	10.4014
		Chapter 4	0.490918	0.409123	0.4671212	10.2123	10.8727	10.0121
Earth Image		Chapter 5	0.404013	0.406342	0.39951	10.8742	10.4637	10.4865
Lena Image	Energy	Chapter 2	0.12659	0.089339	0.153123	0.01569	0.01575	0.01565
		Chapter 3	0.100595	0.0905074	0.0930154	0.0156312	0.0156311	0.0156354
		Chapter 4	0.11093	0.097849	0.1068233	0.0129348	0.019708	0.0198752
Earth Image		Chapter 5	0.329216	0.25941	0.25941	0.0159002	0.0156558	0.0157072
Lena Image	Homogeneity	Chapter 2	0.84602	0.844884	0.849049	0.39096	0.39218	0.38921
		Chapter 3	0.87704	0.879246	0.87606	0.389739	0.389804	0.391806
		Chapter 4	0.874234	0.889073	0.85324	0.398073	0.379801	0.376980
Earth Image		Chapter 5	0.875259	0.871894	0.871802	0.391037	0.390769	0.391608

6.5.4 Entropy

Entropy is a phenomenon that evaluates disorder and randomness in a mechanism of a quantity. An optimal level of disorder in different layers of a digital medium is achieved by using different tools like chaotic maps or S-boxes. The entropy for function is defined by the equation

$$H = \sum_{i=0}^n f(x_i) \log_b f x_i,$$

Where x_i = Calculation of Histogram

For a better encryption scheme the entropy value approaches 8. The results in table 31 shows entropy of a sub-RGB-image of size 256×256 i.e. Lena image. From the output data, it is obvious that the scheme proposed is a best to oppose all the well know attacks. To fix the rank of the offered technique, a comparative similarity with Chaos-DNA encryption scheme is also given in the table 31.

Table 31. Comparing entropy for proposed schemes with existing schemes

	Images	Red	Green	Blue	Average	
Proposed	Chapter 2	Lena	7.99614	7.99408	7.99686	7.99569
	Chapter 3	Lena	7.9984	7.9986	7.9984	7.9994
	Chapter 4	Earth	7.9900	7.9972	7.9964	7.9982
	Chapter 5	Lena	7.9992			
Lena existing schemes	Ref. [85]		7.9973	7.9969	7.9971	7.9971
	Ref. [86]		7.9893	7.9896	7.9903	7.9897
	Ref. [87]		7.9973	7.9972	7.9969	7.9971
	Ref. [88]		7.9896	7.9893	7.9896	7.9896
	Ref. [89]		7.9901	7.9912	7.9921	7.9113
	Ref. [90]		7.3894	7.5280	7.5131	7.4768

The entropy findings for 256×256 color images are given in Table 31, showing the strength of the proposed enciphering method. The analysis shows that the entropy values of our current encryption scheme are almost similar to optimal amounts. Whereas, the comparison guarantee that the entropy effects of our suggested approach are stronger than the schemes cited.

The entropy results of the 256×256 Astronomical color image (Earth) is provided in Table 31 showing the strength of the suggested ciphering technique. It is evident from the astronomical images analysis that the entropy of our proposed ciphering system is close to the appropriate level.

6.6 Analysis on experimental work

This section comprises of the experimental analysis of the offered encryption system. To check the strength of the proposed scheme, we take a 256×256 Lena color image and its corresponding encrypted image using the proposed scheme to examine the security measures.

Several image analyses are performed in this section to guarantee the strength of the offered technique. These analyses are listed below.

6.6.1 MSE

The Mean square error (MSE) gives the cumulative squared difference between two images i.e. plain image $P(x, y)$ and ciphered image $C(x, y)$. Mathematically, for an $M \times N$ image, the MSE can be calculated by the formula:

$$MSE = \frac{1}{M \times N} \sum_{y=1}^M \sum_{x=1}^N [P(x, y) - C(x, y)]^2$$

A large MSE value means better enciphering algorithm.

6.6.2 PSNR

Noise in any medium affects the signal representation [91]. Peak signal-to-noise ratio (PSNR) gives the ratio between the power of signal and noise. It can be calculated by the formula:

$$PSNR = 10 \log_{10} \frac{MAX_1^2}{\sqrt{MSE}}$$

6.6.3 Cross correlation (Normalized), NK

Using correlation function, we can also find that how much an image is similar to another image [92]. In equation below, input connection to the output and vice versa can be calculated through NK, i.e.

$$NK = \frac{\sum_{y=1}^M \sum_{x=1}^N O(x, y) \times E(x, y)}{\sum_{y=1}^M \sum_{x=1}^N [I(x, y)]^2}$$

Where $O(x, y)$ and $E(x, y)$ is the original and encrypted image respectively having dimensions M, N .

6.6.4 Average difference (AD)

By [91], average of plain digital image (PDI) & ref. signal is called average difference. It can be calculated by the equation:

$$AD = \frac{\sum_{y=1}^M \sum_{x=1}^N [O(x, y) - E(x, y)]}{M \times N}$$

Whereas $O(x, y)$ is the original image, $E(x, y)$ is its corresponding encrypted image and $M \times N$ is their dimension respectively.

6.6.5 Structural content (SC)

In light of [91], the similarity between two images can be calculated with the help of structural content (SC). Its measure also based on correlation of adjacent pixels of an image. It is calculated by the formula:

$$SC = \frac{\sum_{y=1}^M \sum_{x=1}^N [O(x, y)]^2}{\sum_{y=1}^M \sum_{x=1}^N [E(x, y)]^2}$$

$O(x, y)$ and $E(x, y)$ represents original and encrypted image respectively. Whereas $M \times N$ gives image dimensions.

6.6.6 Maximum difference (MD)

By [93], maximum difference (MD) gives the extreme value of error in signals. It is obtained by the equation:

$$MD = \max|O(x, y) - E(x, y)|,$$

where $O(x, y)$ & $E(x, y)$ is the primary & ciphered image respectively having dimensions M, N .

6.6.7 Absolute error (Normalized), NAE

According to [93], The NAE among original and encrypted digital image can be calculated by:

$$NAE = \frac{\sum_{y=1}^M \sum_{x=1}^N |I(x, y) - C(x, y)|}{\sum_{y=1}^M \sum_{x=1}^N |I(x, y)|}$$

Whereas, $O(x, y)$ = original digital image, $E(x, y)$ = encrypted image. M, N gives the peripherals of the image.

6.6.8 Root mean square error

RMSE stands for “Root Mean Square Error”. It calculates the “square root of mean of the square of all the errors”. it is used frequently for an excellent wide range in numerical forecasts. It is calculated by using the relation:

$$RMSE = \sqrt{\frac{\sum_{y=1}^M \sum_{x=1}^N [I(x, y) - C(x, y)]^2}{M \times N}}$$

where $O(x, y)$ and $E(x, y)$ is the original and encrypted image respectively having dimension $M \times N$.

6.6.9 Universal quality index (UQI)

In view of the article [94], the UQI produce discontinuities among original and encrypted image in 3 categories: structural comparisons, luminance & contrast. Universal Quality Index for two images O & E might be defined as

$$UQI(O, E) = \frac{4\mu_I\mu_C\mu_{IC}}{(\mu_I^2 - \mu_C^2)(\sigma_I^2 - \sigma_C^2)},$$

where μ_I, μ_C represents the avg. values of noisy & plain images respectively. & σ_I, σ_C show the SD (standard deviation) of noisy & plain images respectively.

6.6.10 Mutual information (MI)

By [94], the quantity of information about the primary image using ciphered image can be quantified by the mutual information. The MI between original & ciphered images is defined as:

$$MI(I, C) = \sum_{y \in C} \sum_{x \in I} p(x, y) \log_2 \frac{p(x, y)}{p(x)p(y)},$$

Here $p(x, y)$ = joint probability function of O and E , further $p(x)$ and $p(y)$ are the MPD functions of O & E respectively.

6.6.11 Structural similarity (SSIM)

In the view of the article [71], SSIM is an improve edition of UQI. It gives the resemblance between two images. The SSIM index is measured in various parts of an image. The calculation among two parts X and Y of equal size $N \times N$ is

$$SSIM(X, Y) = \frac{(2\mu_X\mu_Y + c_1)(2\sigma_X\sigma_Y + c_2)}{(\mu_X^2 + \mu_Y^2 + c_1)(\sigma_X^2 + \sigma_Y^2 + c_2)},$$

where μ_X is the average of X , μ_Y is the average of Y , σ_X^2 is the variance of X , σ_Y^2 is the variance of Y , σ_{XY} is the covariance of X and Y , $c_1 = (k_1L)^2$ and $c_2 = (k_2L)^2$ are the variables to stabilize the division with small value of denominator, L is the vibrant range of the pixel values, $(k_1, k_2) = (0.01, 0.03)$ by default. The range of SSIM index falls in the interval $[-1, 1]$. In case of identical images, the SSIM value is 1.

Table 32. Image quality measures for encrypted image (Lena.jpg) resulting from chapter 2

Chapter 2	Quality measure	Encryption by 3 S-boxes based			Optimal values		
		R	G	B	R	G	B
	MSE	10464.9	8800.42	7119.13	10057.2	9898.89	6948.19
	PSNR	7.93344	8.68577	9.60653	8.1060	8.1749	9.7120
	NCC	0.659928	1.00477	1.08877	0.6725	1.0031	1.0923
	AD	52.099	-28.9701	-22.2615	50.0448	-31.4276	-19.7989
	SC	1.61341	0.585158	0.569553	1.5787	0.5582	0.5711
	MD	255	230	221	236	210	210
	NAE	0.464243	0.776223	0.667141	0.4537	0.8310	0.6628
	RMSE	102.298	93.8105	84.375	100.286	99.4932	83.3558
	UQI	0.00129749	0.00252274	-0.0012504	-0.0050	-0.0077	0.0107
	MI	0.485519	0.641922	0.46649	5.6534	7.2283	6.0723
	SSIM	0.0110091	0.0111818	0.00925915	0.0078	0.0053	0.0187

The results of Image Quality Measures (Table 32) for proposed $\frac{F_2[x]}{\langle x^{12} \rangle}$ Dependent RGB Image Encryption of Lena image (256×256 jpg) are nearly approaching the optimal values.

Table 33. Quality measures analysis for encrypted image (Lena.jpg) resulting from chapter 2

Chapter 3	Quality measure	Encryption by random sequence based			Optimal values		
		R	G	B	R	G	B
	MSE	9863.64	9213.34	9549.73	10057.2	9898.89	6948.19
	PSNR	8.19043	8.48663	8.33089	8.106	8.1749	9.712
	NCC	0.700693	0.773679	0.7937	0.6725	1.0031	1.0923
	AD	34.3988	10.7819	1.38493	50.0448	-31.4276	-19.7989
	SC	1.35704	1.05022	0.950311	1.5787	0.5582	0.5711
	MD	255	255	255	236	210	210
	NAE	0.501848	0.569466	0.622491	0.4537	0.831	0.6628
	RMSE	99.3159	95.9861	97.7227	100.286	99.4932	83.3558
	UQI	-0.0005487	0.000813647	-0.00035072	-0.005	-0.0077	0.0107
	MI	0.189529	0.198777	0.193972	5.6534	7.2283	6.0723
	SSIM	0.00951297	0.0105679	0.00932973	0.0078	0.0053	0.0187

The results of Image Quality Measures (Table 33) for proposed $\frac{F_2[x]}{\langle x^{12} \rangle}$ based chaotic triplet and DNA Dependent RGB multiple Image Encryption are nearly approaching the optimal values.

Table 34. Image Quality Measures for $\frac{F_2[x]}{\langle x^{24} \rangle}$ Dependent encrypted Astronomical Images

Chapter 4	Quality measure	Enciphered images			Optimum values		
		R	G	B	R	G	B
	MSE	15769	14179.5	13227.9	10057	9898	6948
	PSNR	6.15278	6.61419	6.9159	8.106	8.17	9.71
	NCC	1.05216	1.02282	1.02297	0.659053	1.00999	1.08712
	AD	-79.6818	-70.4299	-62.8331	52.081	-28.9503	-22.4915
	SC	0.274184	0.318857	0.359002	1.59765	0.572897	0.56569
	MD	247	246	212	255	219	224
	NAE	2.07158	1.77113	1.51164	0.470065	0.79014	0.678703
	RMSE	125.574	119.078	115.013	103.347	95.1163	85.5092
	UQI	-0.001831	-0.00089475	-0.00521278	-0.003312	-0.002023	-0.002502
	MI	0.652859	0.670646	0.678174	0.493561	0.615849	0.497248
	SSIM	0.0030514	0.00514979	0.00221279	0.0076417	0.0076128	0.0084967

Table 35. Image quality measures for RGB image (Lena.jpg) resulting from chapter 5

Chapter 5	Quality measure	Encryption by improved SERPENT algorithm based			Optimal values		
		R	G	B	R	G	B
	MSE	10630	9155.2	7196.8	10057	9898	6948
	PSNR	7.8653	8.5141	9.5593	8.106	8.17	9.71
	NAE	0.4678	0.7932	0.6739	0.4537	0.83	0.66
	MI	0.4855	0.6883	0.3935	5.6534	7.22	6.07
	UQI	0.0006	0.0008	0.0002	-0.005	-.007	0.01
	SSIM	0.0103	0.0092	0.0096	0.0078	0.005	0.01
	NCC	0.6598	0.9960	1.1022	0.6725	1.003	1.09
	AD	52.248	-28.60	-23.21	50.044	-31.4	-19.7
	SC	1.6011	0.5826	0.5581	1.5787	0.55	0.57
	MD	255	247	211	236	210	210
	RMSE	103.10	95.682	84.834	100.28	99.49	83.3

The results of IQM (Table 36) for proposed chain ring-based SERPENT algorithm dependent RGB Lena image encryption are nearly to optimal values.

6.7 Randomness test for cipher

The safety level of a cryptosystem can be judged by discovering its period, complexity, distribution and output data. An arranged algorithm is secure if it uniformly distributes data, it shows high complexity and long period. In this paper, these objectives are measured by using the NIST SP 800-22 [95] test. This test also includes some subclasses. As a specimen, the Lena color image is taken into account. Results of the test shows that the encrypted Lena image using chain ring-based serpent algorithm passes all the security threats. And hence can replace many cryptosystems based on Rijndael and Serpent algorithm. Results of NIST test on RGB images considered for experiment in chapter 2-5 is shown in table 37-40 respectively.

Table 36. NIST test results for 12 × 12 S-box Dependent RGB Image Encryption

Test		P – values for color encryptions of ciphered image			Results
		Red	Green	Blue	
Frequency		0.80028	0.56921	0.26838	Pass
Block frequency		0.89407	0.89723	0.67542	Pass
Rank		0.29191	0.29191	0.29191	Pass
Runs (M=10,000)		0.15443	0.95365	0.25995	Pass
Long runs of ones		0.7127	0.7127	0.7127	Pass
Overlapping templates		0.85988	0.85988	0.85988	Pass
No overlapping templates		0.9983	0.99995	0.99995	Pass
Spectral DFT		0.30979	0.081659	0.77167	Pass
Approximate entropy		0.89423	0.082762	0.83699	Pass
Universal		0.99822	0.99607	0.99179	Pass
Serial	p values 1	0.42777	0.014493	0.071555	Pass
Serial	p values 2	0.80926	0.00089833	0.18426	Pass
Cumulative sums forward		0.24343	0.33	0.22433	Pass
Cumulative sums reverse		0.99741	1.0748	1.4341	Pass
Random excursions	X = -4	0.24004	0.51206	0.3577	Pass
	X = -3	0.20417	0.43367	0.41976	Pass
	X = -2	0.070092	0.71	0.43535	Pass
	X = -1	0.31641	0.50138	0.58854	Pass
	X = 1	0.76596	0.48113	0.58412	Pass
	X = 2	0.3668	0.0070887	0.23173	Pass
	X = 3	0.27631	0.17547	0.32912	Pass
	X = 4	0.31369	0.51086	0.01716	Pass
Random excursions variants	X = -5	0.78404	0.27133	0.90231	Pass
	X = -4	0.45867	0.30749	0.55418	Pass
	X = -3	0.33622	0.30367	0.51008	Pass
	X = -2	0.63501	0.14891	0.33872	Pass
	X = -1	0.84952	0.071861	0.46145	Pass
	X = 1	0.80028	0.48393	0.78242	Pass
	X = 2	0.88387	0.95396	0.70986	Pass
	X = 3	0.97744	0.53125	0.59251	Pass
	X = 4	0.82966	0.096304	0.91687	Pass
	X = 5	0.5836	0.071861	0.82992	Pass

Table 37. NIST test results for Algebra-Chaos Amalgam and DNA Transform based multiple encrypted Image

Test		P – values for RGB ciphering of encrypted image			Results	
		Red	Green	Blue		
Frequency		0.54795	0.0071895	0.681	Pass	
Block frequency		0.84514	0.033826	0.95477	Pass	
Rank		0.29191	0.29191	0.29191	Pass	
Runs (M=10,000)		0.66207	0.42124	0.26952	Pass	
Long runs of ones		0.7127	0.7127	0.7127	Pass	
Overlapping templates		0.85988	0.85988	0.81567	Pass	
No overlapping templates		0.93985	0.99561	0.93985	Pass	
Spectral DFT		0.24574	0.24574	0.14679	Pass	
Approximate entropy		0.40755	0.48998	0.8963	Pass	
Universal		0.99854	0.99706	0.99639	Pass	
Serial	p values 1	0.81918	8.3174e-05	0.16061	Pass	
Serial	p values 2	0.78752	0.41828	0.16876	Pass	
Cumulative sums forward		0.27743	0.2772	0.21991	Pass	
Cumulative sums reverse		0.89099	1.9933	1.002	Pass	
Random excursions	X = -4	0.46586	0.016563	0.10946	Pass	
	X = -3	0.59692	0.0032622	0.42539	Pass	
	X = -2	0.044496	0.12159	0.025198	Pass	
	X = -1	0.48043	0.62756	0.60827	Pass	
	X = 1	0.81345	0.75335	0.93347	Pass	
	X = 2	0.085479	0.7301	0.56178	Pass	
	X = 3	0.37951	0.24725	0.48626	Pass	
	X = 4	0.76149	0.56196	0.53804	Pass	
	Random excursions variants	X = -5	0.54113	0.35833	0.32006	Pass
		X = -4	0.54954	0.35454	0.27523	Pass
X = -3		0.60184	0.61561	0.21205	Pass	
X = -2		0.77283	0.90619	0.31731	Pass	
X = -1		0.55967	0.75946	0.84739	Pass	
X = 1		0.93359	0.91871	0.92334	Pass	
X = 2		0.88523	0.90619	0.73888	Pass	
X = 3		0.91098	0.89109	0.79625	Pass	
X = 4		0.94977	0.46359	0.51269	Pass	
X = 5		0.75994	0.30743	0.50058	Pass	

Table 38. NIST test results for 24-by-24-replacement-matrix dependent Image Encryption

Test		P – values for RGB ciphering of encrypted image			Results
		Red	Green	Blue	
Frequency		0.32694	0.039833	0.029112	Clear
Block frequency		0.21345	0.39661	0.41337	Clear
Rank		0.29191	0.29191	0.29191	Clear
Runs (M=10,000)		0.22308	0.26942	0.80937	Clear
Long runs of ones		0.7127	0.7127	0.7127	Clear
Overlapping templates		0.85988	0.81567	0.85988	Clear
No overlapping templates		0.96777	0.97809	0.98974	Clear
Spectral DFT		0.66336	0.042221	0.46816	Clear
Approximate entropy		0.063995	0.45473	0.84787	Clear
Universal		0.99825	0.99202	0.99083	Clear
Serial	p values 1	0.20104	0.013754	0.028519	Clear
Serial	p values 2	0.61101	0.85007	0.7675	Clear
Cumulative sums forward		0.35256	0.44907	0.019358	Clear
Cumulative sums reverse		0.61835	1.9513	0.21269	Clear
Random excursions	X = -4	0.20067	0.37725	0.82703	Clear
	X = -3	0.94862	0.66736	0.010449	Clear
	X = -2	0.84338	0.2535	0.25166	Clear
	X = -1	0.58412	0.35903	0.85773	Clear
	X = 1	0.95363	0.65197	0.80938	Clear
	X = 2	0.89767	0.77492	0.84257	Clear
	X = 3	0.93199	0.17585	0.33449	Clear
	X = 4	0.96189	0.75433	0.78491	Clear
Random excursions variants	X = -5	0.00040695	0.9608	0.62763	Clear
	X = -4	0.00025963	0.91126	0.67996	Clear
	X = -3	0.0015654	0.59784	0.87076	Clear
	X = -2	0.0064956	0.73348	0.88864	Clear
	X = -1	0.033895	0.76808	0.54429	Clear
	X = 1	0.34578	0.55535	0.46685	Clear
	X = 2	0.2763	0.79843	0.5754	Clear
	X = 3	0.34278	0.64439	0.5508	Clear
	X = 4	0.42268	0.65573	0.27132	Clear
	X = 5	0.4795	0.65825	0.21017	Clear

Table 39. NIST test results for improved SERPENT algorithm dependent RGB Lena encrypted

Test		P – values for color encryptions of ciphered image			Result
		Red	Green	Blue	
					Pass
Frequency		0.48662	0.80028	0.22949	Pass
Block frequency		0.2131	0.03382	0.85842	Pass
Rank		0.29191	0.29191	0.29191	Pass
Runs (M=10,000)		0.80618	0.97558	0.73447	Pass
Long runs of ones		0.7127	0.7127	0.7127	Pass
Overlapping templates		0.85988	0.81656	0.85988	Pass
No overlapping templates		0.99286	0.99981	0.99286	Pass
Spectral DFT		0.24574	1	0.46816	Pass
Approximate entropy		0.051717	0.70021	0.627	Pass
Universal		0.98081	0.99786	0.99015	Pass
Serial	p values 1	0.028585	0.19802	0.13723	Pass
Serial	p values 2	0.003685	0.036812	0.15085	Pass
Cumulative sums forward		0.093972	0.23925	0.10903	Pass
Cumulative sums reverse		1.1616	0.61835	0.91758	Pass
Random excursions	X=-4	3.44E-15	0.23068	0.62685	Pass
	X=-3	0.59692	0.00326	0.61437	Pass
	X=-2	0.00277	0.5435	0.93691	Pass
	X=-1	0.7127	0.81889	0.92276	Pass
	X=1	0.91792	0.94	0.01848	Pass
	X=2	0.98624	0.88524	0.8646	Pass
	X=3	0.99314	0.034476	0.50562	Pass
	X=4	0.9955	0.030622	0.62013	Pass
Random excursions variants	X=-5	0.13361	0.31711	0.3017	Pass
	X=-4	0.70546	0.28483	0.62559	Pass
	X=-3	1	0.19229	1	Pass
	X=-2	0.77283	0.16568	0.82306	Pass
	X=-1	0.61708	0.19836	0.89728	Pass
	X=1	0.31731	0.34556	0.3017	Pass
	X=2	0.5637	0.48824	0.37109	Pass
	X=3	0.65472	0.75901	0.18421	Pass
	X=4	0.70546	0.82052	0.04543	Pass

Table 37 to table 40 shows that the proposed encryption techniques are given in the chapters 2,3, and 5 clears the entire NIST tests and hence guarantee the security of the presented scheme.

Chapter 7

Conclusion

In this part of the thesis a summary of the proposed research work is given. As the existing literature on symmetric key cryptography which is mainly depends on Galois fields of characteristic 2. However, there is also some new developments on the area focusing on other algebraic structures; like Galois ring and finite group theory. In almost all these algebraic structures are delivering through their cyclic group substructures. Whereas, in some cases the most portion of the algorithms the XOR operations are also in compromising mod. Remarkably, in this thesis the structure of finite chain ring is used which has the base binary field $GF(2)$, which is not only settled the XOR operation but also created extra complexity due to non-cyclic subgroups of the chain ring. With all these innovations instead 8-bit dependency in creation of S-box we increased it to 12-bits and then to the 24-bits.

A classic 8×8 S-box is a 16×16 look-up table over Galois field $GF(2^8)$ and therefore the memory constraint for storage of 2^8 8-bit string is 8×2^8 bits. Similarly, for $GF(2^{12})$ this figure reaches a large number i.e. 12×2^{12} bits. In chapter 2, a 12×12 S-box is generated by using 3 generators of the chain ring $\frac{\mathbb{F}_2[x]}{\langle x^{12} \rangle}$ that occupy 12×2^8 bits of computer memory. The multiple generators enhance the algebraic complexity of the work. The utility of this 12×12 S-box is agreed in color image encryption scheme. The objective of chapter 3 is to construct a chain ring-chaos amalgamated series of S-boxes and its functionality in multiple image encryption schemes in parallel to the DNA transform. In chapter 4, the study of 12-bit S-boxes is taken to a larger structure i.e. 24-bit. Here, a 24-by-24-replacement-matrix (S-box) over unit elements of commutative chain ring of the form $\frac{\mathbb{F}_2[x]}{\langle x^{24} \rangle}$ is constructed that holds 24×2^8 computer memory calls. Also, the proposed S-box is generated by 2 elements of chain ring and hence gives additional algebraic complexity to the replacement structure. The use of this 24×24 S-box has been agreed to the privacy of digital RGB images (for experiment astronomical images have been considered). The objective of chapter 2, chapter 3 and chapter 4 is to create S-boxes of high algebraic complexity and low consumption area.

Chapter 5 comprises of application of chain ring based S-box in symmetric algorithm called the serpent algorithm. As there is a time execution deficiency in symmetric key block ciphers

therefore they are not favorable in digital image encryption. However, in the 5th chapter of this thesis, the chain ring based constructed S-boxes is used in the serpent algorithm that improved the time execution efficiency cipher. The S-boxes are evaluated on 8-bit data block instead of 4-bit block that speedup various portions of the algorithm (e.g. key structure and the loops) and thereby the whole algorithm time execution improves. Besides, multiple generators used for the construction of S-boxes result increase in the algebraic complexity of the S-boxes and hence the algorithm. Also, dealing with a 64-bit block instead of 32-bit block in the improved SERPENT algorithm makes it speedy. Furthermore, a new image encryption scheme using improved SERPENT algorithm is presented. By coinciding addition operation with the addition of F_{2^k} and multiplication with of \mathbb{Z}_{2^k} , while applying the S-boxes, the algebraic complexity of the improved SERPENT algorithm is enhanced and hence the confusion in a digital image is uplifted.

In chapter 6, to fix the rank of the novel encryption schemes, a comparison of the strength determination of newly introduced data security algorithms (chapter 2-5) with existing schemes is made. The results show that the presented encryption schemes have an upper hand on the existing Image encryption schemes.

The above study sets the grounds for the 24-by-24 S-boxes in information security applications. This can be extended by modifying and designing the existing cryptography, watermarking and steganography application that use 8×8 S-boxes by replacing them with 24-bit S-boxes. Furthermore, these S-boxes may cause modifications in different symmetric key crypto-algorithms. Consequently, these newly designed algorithms will be used to secure sensitive data like images, audios, and videos. Some other algebraic structures, such as Galois ring, can also be found for the construction of such S-boxes to enhance their strength. Moreover, there is a space for discovering different cryptanalysis techniques for such S-boxes.

References

1. Daemen, J., & Rijmen, V. (1998, September). The block cipher Rijndael. In *International Conference on Smart Card Research and Advanced Applications* (pp. 277-284). Springer, Berlin, Heidelberg.
2. Rivest, R. L., Robshaw, M. J., Sidney, R., & Yin, Y. L. (1998, August). The RC6™ block cipher. In *First Advanced Encryption Standard (AES) Conference* (p. 16).
3. Anderson, R., Biham, E., & Knudsen, L. (1998). Serpent: A proposal for the advanced encryption standard. *NIST AES Proposal, 174*, 1-23.
4. Hall, J., & Mars, P. (1998, May). Satisfying QoS with a learning based scheduling algorithm. In *1998 Sixth International Workshop on Quality of Service (IWQoS'98)(Cat. No. 98EX136)* (pp. 171-173). IEEE.
5. Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C., Ferguson, N., & Stay, M. (2000). The Twofish team's final comments on AES Selection. *AES round, 2(1)*, 1-13.
6. Shannon, C. E. (1949). Communication theory of secrecy systems. *The Bell system technical journal, 28(4)*, 656-715.
7. De Andrade, A. A., & Palazzo Jr, R. (1999). Construction and decoding of BCH codes over finite commutative rings. *Linear Algebra and Its Applications, 286(1-3)*, 69-85.
8. Andrade, A. A. D., Shah, T., & Qamar, A. (2012). Constructions and decoding of a sequence of BCH codes. *Mathematical Sciences Research Journal, 234-250*.
9. Shah, T., Qamar, A., & de Andrade, A. A. (2012). Construction and decoding of BCH codes over chain of commutative rings. *Mathematical Sciences, 6(1)*, 51.
10. Udaya, P., & Siddiqi, M. U. (1998). Optimal large linear complexity frequency hopping patterns derived from polynomial residue class rings. *IEEE Transactions on Information Theory, 44(4)*, 1492-1503.
11. Bonnecaze, A., & Udaya, P. (1999). Cyclic codes and self-dual codes over $F/\text{sub } 2/+uF/\text{sub } 2$. *IEEE Transactions on Information Theory, 45(4)*, 1250-1255.
12. Shah, T., Jahangir, S., & de Andrade, A. A. (2017). Design of new 4×4 S-box from finite commutative chain rings. *Computational and Applied Mathematics, 36(2)*, 843-857.
13. Shah, T., Haq, T. U., & Farooq, G. (2020). Improved SERPENT Algorithm: Design to RGB Image Encryption Implementation. *IEEE Access, 8*, 52609-52621.

14. Coppersmith, D., Johnson, D. B., & Matyas, S. M. (1996). A proposed mode for triple-DES encryption. *IBM Journal of Research and Development*, 40(2), 253-262.
15. Kocher, P., Jaffe, J., & Jun, B. (1998). Introduction to differential power analysis and related attacks.
16. Knudsen, L. R., & Mathiassen, J. E. (2000, April). A chosen-plaintext linear attack on DES. In *International Workshop on Fast Software Encryption* (pp. 262-272). Springer, Berlin, Heidelberg.
17. Li, J., & Liu, H. (2013). Colour image encryption based on advanced encryption standard algorithm with two-dimensional chaotic map. *IET information security*, 7(4), 265-270.
18. Lidl, R., & Niederreiter, H. (1997). *Finite fields* (Vol. 20). Cambridge university press.
19. Conrad, K. (2013). Finite fields. *order*, 73, 343.
20. Bini, G., & Flamini, F. (2012). *Finite commutative rings and their applications* (Vol. 680). Springer Science & Business Media.
21. Dummit, D. S., & Foote, R. M. (2004). *Abstract algebra* (Vol. 3). Hoboken: Wiley.
22. Hou, X. D., Leung, K. H., & Ma, S. L. (2003). On the groups of units of finite commutative chain rings. *Finite Fields and Their Applications*, 9(1), 20-38.
23. Janusz, G. J. (1966). Separable algebras over commutative rings. *Transactions of the American Mathematical Society*, 122(2), 461-479.
24. J. Qian, L. Zhang and S. Zhu, *(1+u) constacyclic and cyclic over $F_2 + uF_2$* . Applied Mathematics Letters, **19**(8) (2006), 820-823
25. Fu, X. Q., Liu, B. C., Xie, Y. Y., Li, W., & Liu, Y. (2018). Image encryption-then-transmission using DNA encryption algorithm and the double chaos. *IEEE Photonics Journal*, 10(3), 1-15.
26. Tian, Y., & Lu, Z. (2017). Novel permutation-diffusion image encryption algorithm with chaotic dynamic S-box and DNA sequence operation. *AIP Advances*, 7(8), 085008..
27. Ullah, A., Jamal, S. S., & Shah, T. (2018). A novel scheme for image encryption using substitution box and chaotic system. *Nonlinear Dynamics*, 91(1), 359-370.
28. 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.

29. Huang, X., & Ye, G. (2014). An image encryption algorithm based on hyper-chaos and DNA sequence. *Multimedia tools and applications*, 72(1), 57-70.
30. Liu, L., & Miao, S. (2018). A new simple one-dimensional chaotic map and its application for image encryption. *Multimedia Tools and Applications*, 77(16), 21445-21462.
31. Jithin, K. C., & Sankar, S. (2020). Colour image encryption algorithm combining Arnold map, DNA sequence operation, and a Mandelbrot set. *Journal of Information Security and Applications*, 50, 102428.
32. Wang, H., Xiao, D., Chen, X., & Huang, H. (2018). Cryptanalysis and enhancements of image encryption using combination of the 1D chaotic map. *Signal processing*, 144, 444-452.
33. Zhang, Y. Q., Wang, X. Y., Liu, J., & Chi, Z. L. (2016). An image encryption scheme based on the MLNCML system using DNA sequences. *Optics and Lasers in Engineering*, 82, 95-103.
34. Som, S., Kotal, A., Chatterjee, A., Dey, S., & Palit, S. (2013, September). A colour image encryption based on DNA coding and chaotic sequences. In *2013 1st International Conference on Emerging Trends and Applications in Computer Science* (pp. 108-114). IEEE.
35. Wu, X., Kan, H., & Kurths, J. (2015). A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps. *Applied Soft Computing*, 37, 24-39.
36. Zhang, Q., & Wei, X. (2013). A novel couple images encryption algorithm based on DNA subsequence operation and chaotic system. *Optik*, 124(23), 6276-6281.
37. Zhang, Y., Xiao, D., Wen, W., & Wong, K. W. (2014). On the security of symmetric ciphers based on DNA coding. *Information Sciences*, 289, 254-261.
38. Janusz, G. J. (1966). Separable algebras over commutative rings. *Transactions of the American Mathematical Society*, 122(2), 461-479.
39. Raghavendran, R. (1969). Finite associative rings. *Compositio Mathematica*, 21(2), 195-229.
40. Krull, W. (1924). Algebraische Theorie der Ringe. II. *Mathematische Annalen*, 91(1-2), 1-46.

41. Janusz, G. J. (1966). Separable algebras over commutative rings. *Transactions of the American Mathematical Society*, 122(2), 461-479.
42. Martinez-Moro, E., Otal, K., & Özbudak, F. (2018). Additive cyclic codes over finite commutative chain rings. *Discrete Mathematics*, 341(7), 1873-1884.
43. Clark, W. E., & Liang, J. J. (1973). Enumeration of finite commutative chain rings. *Journal of Algebra*, 27(3), 445-453.
44. Qian, J. F., Zhang, L. N., & Zhu, S. X. (2006). Constacyclic and cyclic codes over $F_2 + uF_2 + u^2F_2$. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 89(6), 1863-1865.
45. T. Abualrub and I. Saip, *Cyclic coacquired a great consideration in algebraic coding theory over the rings $F_2 + uF_2$ and $F_2 + uF_2 + u^2F_2$* . *Design Codes and Cryptography*, **42** (2007), 273-287
46. Al-Ashker, M. M. (2005). Simplex Codes over the Ring $F_2 + uF_2$. *Simplex Codes over the Ring $F_2 + uF_2$* , 30(2).
47. M. Al-Ashker, *Simplex codes over $F_2 + uF_2$* . *The Arabian Journal for Science and engineering*, **3** (2005), 227-285
48. M. Al-Ashker and M. Hamoudeh, *Cyclic codes over $F_2 + uF_2 + \dots + uk-1F_2$* . *Turk. J. Math*, **33** (2011), 737-749
49. J. Qian, L. Zhang and S. Zhu, *(1+u) constacyclic and cyclic over $F_2 + uF_2$* . *Applied Mathematics Letters*, **19**(8) (2006), 820-823
50. Naji, A. (2002, August). Linear codes over $F_2 + uF_2 + u^2F_2$ of Constant Lee weight. In *The second conference of the Islamic University on Mathematical Science-Gaza* (pp. 27-28).
51. J. Qian, L. Zhang and S. Zhu, *Cyclic codes over $F_p + uF_p + \dots + uk-1F_p$* . *IEICE Trans. Fundamentals*, **3** (2005), 795-779.
52. M. Al-Ashker and J. Chen, *Cyclic codes of arbitrary length over $F_q + uF_q + \dots + uk-1F_q$* . *Palistine Journal of Mathematics*, **2**(1) (2013), 72-80.
53. F. M. Abu Dahrouj, *Negacyclic and constacyclic codes over finite chain rings*. Master of Mathematics Thesis, The Islamic University of Gaza, 2008.
54. I. Hussain, T. Shah, *Literature survey on nonlinear components and chaotic nonlinear compotents of block cipher*. *Nonlinear dyn.*, **74** (2013), 869-904.

55. V. Rijmen, *Efficient Implementation of the Rijndael S-box*. Katholieke Universiteit Leuven, Dept. ESAT, Kard. Mercierlaan 94, B-3001 Heverlee, Belgium.
56. C. Adams and S. Tavares, *The structured design of cryptographically good Sboxes*. J. Cryptology, **3** (1990), 27-41.
57. K.C. Gupta and P. Sarkar, *Improved Construction of Nonlinear Resilient SBoxes*. Cryptology Research Group Applied Statistics Unit Indian Statistical Institute 203, B.T. Road Kolkata 700108, India.
58. Khan, M., Shah, T., & Batool, S. I. (2017). A new approach for image encryption and watermarking based on substitution box over the classes of chain rings. *Multimedia Tools and Applications*, *76*(22), 24027-24062
59. P. Shankar, On BCH codes over arbitrary integer rings (Corresp.), IEEE Transactions on Information Theory, *25* (1979) 480-483.
60. Shah, T., Ali, A., Khan, M., Farooq, G., & de Andrade, A. A. (2020). Galois Ring $\mathbb{Z}_8[x]/(x^3+8)$ Dependent 24×24 S-Box Design: An RGB Image Encryption Application. *Wireless Personal Communications*, *113*(2), 1201-1224.
61. Qureshi, A., & Shah, T. (2017). S-box on subgroup of Galois field based on linear fractional transformation. *Electronics Letters*, *53*(9), 604-606.
62. Hussain, I., Anees, A., Al-Maadeed, T. A., & Mustafa, M. T. (2019). Construction of s-box based on chaotic map and algebraic structures. *Symmetry*, *11*(3), 351.
63. 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.
64. Pearson, K. (1920). The fundamental problem of practical statistics. *Biometrika*, *13*(1), 1-16.
65. Aldrich, J. (1995). Correlations genuine and spurious in Pearson and Yule. *Statistical science*, *10*(4), 364-376.
66. Stroebel, L. D., & Zakia, R. D. (1993). *The Focal encyclopedia of photography*.
67. Gonzalez, R. C., & Woods, R. E. (2007). Image processing. *Digital image processing*, *2*, 1.

68. Forouzanfar, M., & Abrishami-Moghaddam, H. (2011). Ultrasound speckle reduction in the complex wavelet domain.
69. MacDonald, L. (Ed.). (2006). *Digital heritage*. Routledge.
70. Patro, K. A. K., & Acharya, B. (2018). Secure multi-level permutation operation based multiple colour image encryption. *Journal of information security and applications*, 40, 111-133.
71. Wu, Y., Noonan, J. P., & Aghaian, S. (2011). NPCR and UACI randomness tests for image encryption. *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)*, 1(2), 31-38.
72. Chai, X. L., Gan, Z. H., Yuan, K., Lu, Y., & Chen, Y. R. (2017). An image encryption scheme based on three-dimensional Brownian motion and chaotic system. *Chinese Physics B*, 26(2), 020504.
73. Enayatifar, R., Guimarães, F. G., & Siarry, P. (2019). Index-based permutation-diffusion in multiple-image encryption using DNA sequence. *Optics and Lasers in Engineering*, 115, 131-140.
74. Hussain, I., Shah, T., & Gondal, M. A. (2012). Image encryption algorithm based on PGL (2, GF (2⁸)) S-boxes and TD-ERCS chaotic sequence. *Nonlinear Dynamics*, 70(1), 181-187.
75. Bisht, A., Dua, M., & Dua, S. (2019). A novel approach to encrypt multiple images using multiple chaotic maps and chaotic discrete fractional random transform. *Journal of Ambient Intelligence and Humanized Computing*, 10(9), 3519-3531.
76. Wu, X., Kan, H., & Kurths, J. (2015). A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps. *Applied Soft Computing*, 37, 24-39.
77. Chai, X. L., Gan, Z. H., Lu, Y., Zhang, M. H., & Chen, Y. R. (2016). A novel color image encryption algorithm based on genetic recombination and the four-dimensional memristive hyperchaotic system. *Chinese Physics B*, 25(10), 100503.
78. ur Rehman, A., Liao, X., Ashraf, R., Ullah, S., & Wang, H. (2018). A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2. *Optik*, 159, 348-367.

79. Wang, X. Y., Zhang, H. L., & Bao, X. M. (2016). Color image encryption scheme using CML and DNA sequence operations. *Biosystems*, *144*, 18-26.
80. Kadir, A., Aili, M., & Sattar, M. (2017). Color image encryption scheme using coupled hyper chaotic system with multiple impulse injections. *Optik*, *129*, 231-238.
81. Kalpana, J., & Murali, P. (2015). An improved color image encryption based on multiple DNA sequence operations with DNA synthetic image and chaos. *Optik*, *126*(24), 5703-5709.
82. Yousif, I. A. (2019). Proposed A Permutation and Substitution Methods of Serpent Block Cipher. *Ibn AL-Haitham Journal For Pure and Applied Science*, *32*(2), 131-144.
83. Tayel, M., Dawood, G., & Shawky, H. (2018, September). A proposed serpent-elliptic hybrid cryptosystem for multimedia protection. In *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (pp. 387-391). IEEE.
84. Çavuşoğlu, Ü., Kaçar, S., Zengin, A., & Pehlivan, I. (2018). A novel hybrid encryption algorithm based on chaos and S-AES algorithm. *Nonlinear Dynamics*, *92*(4), 1745-1759.
85. Chai, X., Fu, X., Gan, Z., Lu, Y., & Chen, Y. (2019). A color image cryptosystem based on dynamic DNA encryption and chaos. *Signal Processing*, *155*, 44-62.
86. Enayatifar, R., Abdullah, A. H., & Isnin, I. F. (2014). Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. *Optics and Lasers in Engineering*, *56*, 83-93.
87. Chai, X. L., Gan, Z. H., Lu, Y., Zhang, M. H., & Chen, Y. R. (2016). A novel color image encryption algorithm based on genetic recombination and the four-dimensional memristive hyperchaotic system. *Chinese Physics B*, *25*(10), 100503.
88. Yao, L., Yuan, C., Qiang, J., Feng, S., & Nie, S. (2017). An asymmetric color image encryption method by using deduced gyrator transform. *Optics and Lasers in Engineering*, *89*, 72-79.
89. Wu, J., Liao, X., & Yang, B. (2017). Color image encryption based on chaotic systems and elliptic curve ElGamal scheme. *Signal Processing*, *141*, 109-124.
90. Mishra, D. C., Sharma, R. K., Suman, S., & Prasad, A. (2017). Multi-layer security of color image based on chaotic system combined with RP2DFRFT and Arnold Transform. *Journal of information security and applications*, *37*, 65-90.

91. Huynh-Thu, Q., & Ghanbari, M. (2008). Scope of validity of PSNR in image/video quality assessment. *Electronics letters*, 44(13), 800-801.
92. Wang, Z., & Bovik, A. C. (2002). A universal image quality index. *IEEE signal processing letters*, 9(3), 81-84.
93. Eskicioglu, A. M., & Fisher, P. S. (1995). Image quality measures and their performance. *IEEE Transactions on communications*, 43(12), 2959-2965.
94. Wang, Z., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P. (2004). Image quality assessment: from error visibility to structural similarity. *IEEE transactions on image processing*, 13(4), 600-612.
95. Pareschi, F., Rovatti, R., & Setti, G. (2012). On statistical tests for randomness included in the NIST SP800-22 test suite and based on the binomial distribution. *IEEE Transactions on Information Forensics and Security*, 7(2), 491-505.

Index

A

algebra, 24
Algebra of Galois field extension
and its matrix algebra
representation, 24
asymmetric key cryptography, 12
Avalanche effect, 11
average difference, 100

B

Block ciphers, 13

C

cardinality, 24
Chaos, 15
Cipher, 11
ciphertext, 11
commutative ring, 16
Confusion, 11
Cryptanalysis, 11
Cryptography, 10

D

decryption, 11
diffusion, 11
division algebra, 24

E

Entropy, 99

F

field, 17
Finite commutative chain ring, 33
finite field, 21

G

Galois field, 21

Galois field extension, 21

H

high dimensional chaotic systems,
15
histogram, 67

I

Ideal, 19
integral domain, 17
irreducible polynomial, 22

L

local ring, 27
low dimensional chaotic, 15

M

Matrix rings, 17
maximal ideal, 19
maximum difference, 101
minimal polynomial, 22
module, 25

N

NPCR, 96

O

Occluded attack, 94

P

plaintext, 11
Poisson noise, 92
prime ideal, 19
primitive element, 22
principal ideal, 19
principal ideal domain, 19
PSNR, 100

Q

Quotient rings, 20

R

radical, 20
residue-class ring, 20
Ring of polynomials, 17
ring with identity, 16
Rings, 16
Root Mean Square Error, 101
Root Theorem, 18

S

Salt-and-Pepper noise, 85
secret key cryptography, 11
Shot noise, 92
spanning set, 24
Speckle noise, 89
Spike noise, 85
SP-network, 43
Stream ciphers, 12
subring, 16
Substitution Permutation network,
58
symmetric key ciphers, 12

U

UACI, 96
unit element, 17

V

vector space, 24

Z

zero divisor, 16
zero ideal, 19

Turnitin Originality Report

Chain rings and Chaotic Systems Computations: Applications to Data Security by turnitin

Tanveer Ul Haq

From CL QAU (DRSML)

- Processed on 27-Dec-2021 09:13 PKT
- ID: 1735819985
- Word Count: 33384

Similarity Index
16%
Similarity by Source

Internet Sources:
13%
Publications:
8%
Student Papers:
5%

Tariq Shah
PROFESSOR
 Department of Mathematics
 Quaid-i-Azam University
 Islamabad

Focal Person (Turnitin)
 Quaid-i-Azam University
 Islamabad

sources:

- 1 2% match (publications)
 Tariq Shah, Asif Ali, Majid Khan, Ghazanfar Farooq, Antonio Aparecido de Andrade. "Galois Ring \mathbb{Z}_8 Dependent 24×24 S-Box Design: An RGB Image Encryption Application". *Wireless Personal Communications*, 2020
- 2 1% match ()
 Majid Khan, Hafiz Muhammad Waseem. "A novel image encryption scheme based on quantum dynamical spinning and rotations". *PLoS ONE*
- 3 1% match (Internet from 28-Aug-2020)
https://mafiadoc.com/finite-commutative-rings-and-their-applications_5ca2f20f097c474d348b456e.html
- 4 1% match (Internet from 30-Jul-2021)
<https://techscience.com/cmc/v67n1/41192/pdf>
- 5 1% match (publications)
 Tanveer ul Haq, Tariq Shah. "4D mixed chaotic system and its application to RGB image encryption using substitution-diffusion". *Journal of Information Security and Applications*, 2021
- 6 1% match (Internet from 27-Oct-2019)
<https://repositorio.unesp.br/bitstream/handle/11449/165588/WOS000400272300002.pdf?isAllowed=y&sequence=1>
- 7 < 1% match ()
 Shenli Zhu, Guojun Wang, Congxu Zhu. "A Secure and Fast Image Encryption Scheme Based on Double Chaotic S-Boxes". *Entropy*
- 8 < 1% match ()
 Shuting Cai, Lingqing Huang, Xuesong Chen, Xiaoming Xiong. "A Symmetric Plaintext-Related Color Image Encryption System Based on Bit Permutation". *Entropy*
- 9 < 1% match ()
 Sameh S. Askar, Abdel A. Karawia, Abdulrahman Al-Khedhairi, Fatemah S. Al-Ammar. "An Algorithm of Image Encryption Using Logistic and Two-Dimensional Chaotic Economic Maps". *Entropy*
- 10 < 1% match ()
 Cheng-Yi Lin, Ja-Ling Wu. "Cryptanalysis and Improvement of a Chaotic Map-Based Image Encryption System Using Both Plaintext Related Permutation and Diffusion". *Entropy*
- 11 < 1% match (student papers from 24-May-2015)
 Submitted to Higher Education Commission Pakistan on 2015-05-24
- 12 < 1% match (student papers from 30-May-2014)
 Submitted to Higher Education Commission Pakistan on 2014-05-30