

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

**IN THE NAME OF ALLAH, THE MOST
BENEFICENT, THE ETERNALLY MERCIFUL**

*Non-associative Structures for the Development
and Application of Cryptosystems*



Sadam Hussain

Department of Mathematics

Quaid-I-Azam University

Islamabad, Pakistan

2022

*Non-associative Structures for the Development
and Application of Cryptosystems*



Sadam Hussain

Supervised By

Prof. Dr. Tariq Shah

Department of Mathematics

Quaid-I-Azam University

Islamabad, Pakistan

2022

*Non-associative Structures for the Development
and Application of Cryptosystems*



A thesis submitted to Department of Mathematics,
Quaid-i-Azam University, Islamabad, in the partial fulfilment of
the requirement for the degree of
DOCTOR OF PHILOSOPHY

in

Mathematics

By

Sadam Hussain

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

2022

Author's Declaration

I Sadam Hussain hereby state that my PhD thesis titled Non-Associative Structures for the Development and Application of Cryptosystems is my own work and has not been submitted previously by me for taking any degree from the Quaid-I-Azam University Islamabad, Pakistan or anywhere else in the country/world.

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



Name of Student: Sadam Hussain

Date: 25-03-2022

Plagiarism Undertaking

I solemnly declare that research work presented in the thesis titled "Non-Associative Structures for the Development and Application of Cryptosystems" is solely my research work with no significant contribution from any other person. Small contribution/help wherever taken has been duly acknowledged and that complete thesis has been written by me.

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

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

Student/Author Signature: _____



Name: Sadam Hussain

Non-Associative Structures for the Development and Application of Cryptosystems

By

Sadam Hussain

CERTIFICATE

A THESIS SUBMITTED IN THE PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE DEGREE OF THE

DOCTOR OF PHILOSOPHY IN MATHEMATICS

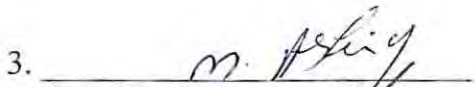
We accept this dissertation as conforming to the required standard

1. 

Prof. Dr. Tariq Shah
(Chairman)

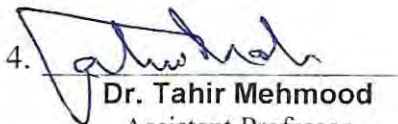
2. 

Prof. Dr. Tariq Shah
(Supervisor)

3. 

Brig. Dr. Muhammad Ashiq
National University of Science & Technology
(NUST) MCS (Campus) Rawalpindi

(External Examiner)

4. 

Dr. Tahir Mehmood
Assistant Professor
Department of Mathematics & Statistics,
International Islamic University Islamabad.

(External Examiner)

Department of Mathematics

Quaid-I-Azam University

Islamabad, Pakistan

2022

Certificate of Approval

This is to certify that the research work presented in this thesis entitled Non-Associative Structures for the Development and Application of Cryptosystems was conducted by Mr. Sadam Hussain 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.

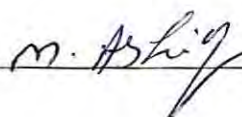
Student Name: Sadam Hussain

Signature: 

External committee:

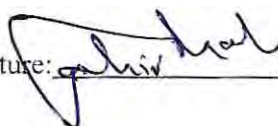
a) External Examiner 1:

Name: **Brig. Dr. Muhammad Ashiq**
Office Address: National University of Science and
Technology (NUST) MCS (Campus) Rawalpindi.

Signature: 

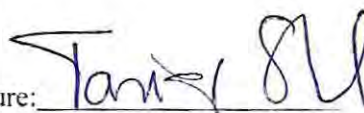
b) External Examiner 2:

Name: **Dr. Tahir Mehmood**
Designation: Assistant Professor
Office Address: Department of Mathematics & Statistics,
International Islamic University Islamabad.

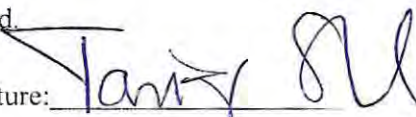
Signature: 

c) Internal Examiner

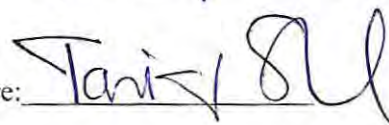
Name: **Dr. Tariq Shah**
Designation: Professor
Office Address: Department of Mathematics, QAU Islamabad.

Signature: 

Supervisor Name:
Prof. Dr. Tariq Shah

Signature: 

Name of Dean/HOD:
Prof. Dr. Tariq Shah

Signature: 

Dedicated to

My

Beloved Parents

Acknowledgement

All praises to Almighty Allah, the most Merciful and the more Beneficent, who created this universe and gave us the idea to discover it. First, I am highly grateful to Allah Almighty who helped and blessed me more than I deserve.

I deem it a great honour to express my deepest sense of gratitude to my honourable supervisor and Chairman of Department of Mathematics **Prof Dr. Tariq Shah** for his kind and able guidance, valuable comments and encouraging altitude throughout my research work.

Special thanks to **Dr. Adnan Javed and Dr Yasir Naseer** for his help in this work.

I would like to express my appreciation to the faculty members and the administration of Mathematics department, Quaid-i-Azam University, Islamabad.

This acknowledgment would be incomplete unless I offer my humble veneration to my family especially to my **wife**, brothers **Sufyan Javed** and **Zaman Javed** and **Sisters** for their endless love, care and supporting spiritually throughout my life and academic career.

Sincere thanks to all my friends and classmate's especially **Dr. Atta Ullah, Dr. Sajjad Shaukat Jamal, Dr. Muhammad Asif, Dr. Mubsher Umer, Dr. Bilal Ahmed, Muhammad Tanveer, Muzammil Hanif** and my **Lab Fellows** for their necessary cooperation in the accomplishment of my dissertation

Last but not the least, I would like to thank one of my best teacher and friend **Dr. Umer Shoaib** (Assistant Professor in GCU Faisalabad), who have been a source of encouragement and motivation to complete the degree of Doctor of Philosophy.

Sadam Hussain

March 2022

Preface

The absolute achievements of information sciences in last few decades are extensive deployment of soft and small computing devices in general public along with the speedy communication channel. An easy approach to valuable digital data had to face some security apprehensions. Frequent transmission and communication of information bears problems like copyright protection, false ownership claims and alteration in valued information, integrity, confidentiality, non-repudiation, access control and authenticity. All of these and many more of this type of security issues are the matter of concern for researchers as well as for officials. The security of data is preserved in such vulnerable situations by making use cryptography. Cryptography works generally on mechanisms of converting meaningful information into non readable form and vice versa. There are two main types of cryptography are symmetric and asymmetric key cryptography. These two types bifurcated on the basis of keys. Same key is used for encryption and decryption in a symmetric key cryptography whereas different set of keys are used in both these procedures in asymmetric key cryptosystems. Stream ciphers and block ciphers are the two broad categories of symmetric key cryptography. In block cryptograms, the procedure of enciphering is done for blocks of data with different sizes. The only nonlinear and complex part of block cryptosystem capable of generating hurdles for cryptanalysts is the substitution box (S-box).

After the development of advanced encryption standard, the need of new encryption standard is diminished because of its robustness and strength against cryptanalyses. However, its security can be enhanced by using chaos based S-boxes instead of algebraic S-boxes. S-box is the nonlinear component of block cipher responsible for creating confusion in the systems. It can have different dimensions depending upon the need of algorithm. It is produced in the form of square matrix from a mathematical structure. Nonlinear mathematical systems are suitable candidates for the generation of S-boxes.

In literature, large number of articles are available expressing research work of scientists related to cryptography and chaos. But they are more vulnerable to cyber threats like brute force and linear attacks due to the low key space, small chaotic range and involvement of fewer number of variables. These drawbacks motivated many cryptographers to use nonlinear algebraic systems, which hamper all such deficiencies and threats.

This thesis primarily focuses on the generation of S-boxes from non-associative structures and the second aim is to design encryption and watermarking techniques by using these nonlinear

components of block cipher. At the first stage of this thesis, block ciphers and non-associative structures are mainly discussed. Moreover, important properties of S-box on the perspective of mathematics are also discussed. A new non-associative structure power associative loop is used for the construction of S-boxes are introduced in chapter second of this thesis. This scheme is used for the construction of highly non-linear components of block ciphers. This scheme provides both confusion and diffusion characteristics. Investigational conclusions authenticate the competence of the predicted algorithms.

Chapter 3 introduces the construction of the S-box from another type of non-associative structure. Compared with other complex structure-based constructions, this method of developing a strong encryption S-box utilizes a simple and single transformation. The main advantage of using a non-associative structure in stable communication is that it can provide you with more unpredictable and random data.

An application of image encryption and watermarking are discussed in chapter four. In chapter five of this thesis, a new cryptographic scheme is proposed whose model is the same as presented in Rijndael algorithm by Joan Daemen and Vincent Rijmen. In the design of this cipher, we have used inverse property loop instead of extended binary Galois field. The complete description of encryption and decryption of this cryptographic scheme is given in this chapter. In chapter six of this thesis, another transformation that is Mobius transformation is applied on a non-associative structure for the construction of highly non-linear substitution boxes. This transformation helps us to achieve maximum nonlinearity of substitution boxes over non-associative structures. A novel image encryption scheme is presented in chapter seven. For this scheme, an encryption standard is proposed whose model is the same as presented by Eli Biham, Ross Anderson, and Lars Knudsen. The proposed method is simple and speedy in terms of computations, meanwhile, it affirms higher security and sensitivity. All the standard analyses were found promising in analysing the suggested scheme of encryption. This thesis has been ended with chapter eight which includes the conclusions and the future directions.

Contents

Chapter 1.....	5
Block Ciphers and some Non-associative Algebraic Structures: An Overview.....	5
1.1 Introduction	5
1.2 Aims of this Research.....	7
1.3 Review of S-box Theory	8
1.3.1 Theory of Boolean Functions	9
1.3.2 Characteristics of Boolean Functions.....	9
1.3.3 The S-box	19
1.3.4 Cryptographic Properties of S-box.....	20
1.4 Basic Terminologies of Non-associative Structures.....	23
1.5 Boolean Operations	28
Chapter 2.....	30
Construction Scheme of S-boxes over IP-loops	30
2.1 Introduction	30
2.2 Why we use IP-loop	31
2.2.1 Non-group Smallest IP-loop.....	32
2.3 Model of IP-loop based S-boxes	33
2.4 Statistical and differential Analyses.....	37
2.4.1 Differential Attacks.....	39
Chapter 3.....	41
Watermarking and Image Encryption Applications of IP-loop based S-boxes	41
3.1 Introduction	41
3.2 Secure Information Transmission.....	42
3.2.1 Steganography.....	42

3.2.2	Cryptography	42
3.2.3	Watermarking	42
3.3	Types of Digital Watermarking.....	43
3.4	Techniques of Watermarking.....	45
3.5	Watermarking Application of Proposed S-box.....	46
3.6	Image Encryption of IP-loop based S-boxes	48
3.6.1	Homogeneity	48
3.6.2	Energy	49
3.6.3	Correlation.....	49
3.6.4	Contrast.....	49
3.6.5	Entropy.....	50
Chapter 4.....		53
IP-loops Modifying AES		53
4.1	Introduction	53
4.2	Design for $n \times n$ S-boxes.....	54
4.3	Description of Encryption Algorithm.....	58
4.3.1	SubBytes () Transformation:.....	58
4.3.2	ShiftRows () Transformation.....	59
4.3.3	MixColumns () Transformation.....	59
4.3.4	Round Key Binding () Transformation.....	61
4.4	Inverse Cipher.....	61
4.4.1	InvShiftRows () Transformation.....	61
4.4.2	InvSubBytes () Transformation	62
4.4.3	InvMixColumns () Transformation.....	63
4.4.4	InvRoundKeyBinding () Transformation	64

4.5	Key Schedule.....	64
4.5.1	Inverse Key Schedule.....	66
4.5.2	Security Analyses of Proposed Encryption Algorithm.....	67
4.6	Cipher Example.....	69
Chapter 5.....		72
S-boxes over Power Associative Loop: A first step towards use of Non-associative Algebra		72
5.1	Introduction.....	72
5.2	Design of Proposed Model.....	73
5.2.1	Symmetric Group of degree 16.....	75
5.3	Analyses of S-box.....	79
5.3.1	Algebraic Analyses of S-box.....	79
5.3.2	Differential Analyses.....	84
5.3.3	Cryptanalysis.....	86
5.3.4	Histogram Analysis.....	89
5.4	Majority Logic Criterion Test.....	90
Chapter 6.....		93
Designing of Non-linear Block Cipher's Component over PA-loop through Mobius Transformation.....		93
6.1	Introduction.....	93
6.2	Preliminaries.....	94
6.2.1	Design of S-Boxes over PA-loop.....	94
6.3	Analyses of S-box.....	102
6.3.1	Algebraic Analyses of S-box.....	102
6.3.2	Differential Analysis.....	106
6.3.3	Cryptanalysis.....	108

6.4	Histogram Analysis.....	110
6.5	Majority Logic Criterion Test.....	111
Chapter 7.....		114
Redefining Serpent Algorithm by PA-loop with Image Encryption Application		114
7.1	Introduction	114
7.2	Cipher Scheme	116
7.3	Investigational Upshots and Simulation Analyses.....	121
7.3.1	Key Space Analysis.....	121
7.3.2	Key Sensitivity Analysis.....	121
7.3.3	Correlation Analysis	121
7.4	Histogram Analysis.....	123
7.5	Differential Analyses	125
7.5.1	NPCR AND UACI.....	125
7.6	Chi-Square Test	126
7.7	Time Execution Performance	127
7.8	Information Entropy	128
Chapter 8.....		129
Conclusion and Future Directions		129
8.1	Conclusion	130
8.2	Future directions.....	132
References		133

Chapter 1

Block Ciphers and some Non-associative Algebraic Structures: An Overview

The objective of secure communication in today's world is the well-defined goal of every communicating party. The primitive idea in attaining this objective is the generation of nonlinear components of block cipher designed with the help of non-associative structures the main concern of this thesis. In this chapter, a brief discussion about non-associative structures and cryptography is given right after highlighting the objective and structure of this thesis. Secondly, the Substitution box (S-box) and its cryptographic properties along with the basics of cryptography are given.

1.1 Introduction

Due to the progress of multimedia technologies the world is shrinking into a global village. With the access of multimedia data to everyone through the internet and many other existing sources, the security of multimedia data has become a challenge. This challenge attracted researchers to strengthen the security of multimedia data through secure algorithms. In past, when communication is mostly done through textual data, the security of data was still an issue. Now the communication of data through different advanced mediums is still unsecure. To reduce the security threats, the researchers utilized cryptographic techniques for secure communication. These techniques are available in the literature.

Cryptography provides all the necessary tools to secure multimedia data. Cryptography offers the luxury of confidentiality, integrity, and authentication of data. Confidentiality kept your data private and secured from illegal access. Integrity makes sure that the data is unaltered in its

original form. It makes sure that the data cannot be changed unintentionally or intentionally. Authentications make sure that the receiver is an authorized person.

The encryption schemes are categorized by the dimensions of the input stream and key distribution rules. Single key sharing schemes between sender and receiver are symmetric ciphers, whereas pairs of keys utilized disjointedly for encryption and decryption between communicating parties are named asymmetric ciphers. Stream and block ciphers are two main types of symmetric ciphers depending on the nature of the input stream (continuous bitstream or blocks of data) used.

Cipher construction is the main focus of researchers to prevent the data from unauthorized access. As mentioned earlier, the intentions of hackers are to have illegal access to the information and secretly change the original information and claim for fake authentication. Hackers may also intend to destroy original data or modifications in original data, that the happening of some specific event. A weak constructed cipher intended to secure data may be permitted these actions to occur, or it may also be possible that some portion of cipher is made weak intentionally. Strong cryptanalytic attacks against cipher systems have been verified to be successful under the right circumstances.

The strength of every single part of the construction of a cipher determined the overall security strength of the cipher. For example, the information storage capacity, the key management, the nature of cipher and the construction procedure of cipher etc. So, the security of every single part of the cipher mechanism contributes to the overall security strength of the cipher. Deficiency in any part of cipher can cause the failure of security.

S-boxes and Boolean functions are the fundamental part of modern cryptographic cipher mechanisms and are widely utilized nowadays. The relative relation between all these cipher frameworks describes through the output string. More generally, a S-box is usually intricate with

dissimilar Boolean functions with a single output. It is similar to a Boolean function mapped on a single bit.

Stream ciphers utilized Boolean functions regularly to generate keystream. Stream ciphers used Boolean functions because they produce a single keystream by combining the linear input feedback shift securely. These Boolean functions preserve cryptographic properties, and they secure the keystream from different attacks.

Hash functions are combinedly used with Boolean functions for their iterative characteristics which result as compression. Due to compression, the computational process becomes extremely fast.

Block ciphers have an outstanding role in the designing of any cryptosystem. In cryptography, the nonlinearity in the system is provided through S-boxes. In block ciphers, the encryption process is carried out in blocks of a fixed length, so the immediate choice for this deed is S-boxes. They provide a technique for substituting numerous input bits of information to attain a different resulting bits string.

1.2 Aims of this Research

The study presented in this dissertation has the following key aims:

1. To design constraint-free models for S-boxes based on algebraic structures.
2. To apply new algebraic structures to designed novel techniques for the construction of a bunch of S-boxes appropriate for several cryptographic ciphers.
3. To design those S-boxes that have confusion as well as diffusion capability. Due to this ability, they are named S-boxes.
4. To provide mathematical justification of bit permutations.

5. To design new methods for obtaining a large number of S-boxes using different algebraic structures and the designed component of block cipher. This segment will be a S-box having suitable cryptographic properties. The challenge of acquiring such features consists of the production and designing of S-boxes which have proven the mandatory measure of residences as nicely as of a suitably expansive size that they can resistant against threats in the lengthy run. Also, the methods for accomplishing such robust cryptosystems ought to be computationally effective.
6. To construct new methods for image processing (image encryption, steganography, and watermarking) with the usage of 1, 2, 3, 4, and 5. To execute these consequences as alternative and replacement procedure in the diagram of quite a number of block ciphers for image handling. The reason is to make use of the opinions and information obtained from the investigational results in the growth of S-boxes to make greater the safety measures of existing ciphers as nicely as to layout new ciphers in the discipline of encryption and copyright protection.
7. A new cryptographic scheme is proposed whose model is the same as presented in Rijndael Algorithm by Joan Daemen and Vincent Rijmen. In the design of this Cipher, we have used an Inverse Property Loop (IP-loop) instead of an Extended Binary Galois Field.

1.3 Review of S-box Theory

Before starting the review of S-box theory, hypotheses, and formulae about S-box, it is very crucial to discuss those notions which help us in the understanding of S-box theory. S-box theory is based upon the theory of Boolean functions. In the first part, we presented some dynamic ideas about the Boolean function. This includes the cryptographic properties of Boolean functions and

the relationship between different cryptographic properties. In the second part, we discussed the hypothesis about S-boxes and various cryptographic characteristics of S-boxes.

1.3.1 Theory of Boolean Functions

Boolean functions theory is an extensive area. This part does not mean the complete review of Boolean functions. Rather, the theory presented in this segment is a complete taxonomy of that which is essential for readers to comprehend this dissertation. Particularly, some important cryptographic qualities have been reviewed which are appropriate for this thesis.

1.3.2 Characteristics of Boolean Functions

The main theme of this section is to discuss some basic definitions and the most important theorems about the encryption properties of Boolean functions. This includes the definition of certain logical functions and various representations used to represent logical functions.

Suppose $GF(2)^r$ be an r -dimensional vector space. A Boolean function $\tau(v)$ is a mapping.

$$\tau: GF(2)^r \rightarrow GF(2)$$

where $GF(2)^r$ is the Galois field consists of 2^r elements and $v = (v_1, \dots, v_r)$.

The total number of non-repeated r -variable Boolean functions is 2^{2^r} . It is very interesting to observe that if r input bits increase, the total Boolean function output space increase rapidly. Boolean functions have many representations, but the truth table and the polarity truth are the most utilized forms.

Definition 1.1 [1] Suppose $\tau(v)$ be a Boolean function of r -variable. The binary outcome as output vector of $\tau(v)$ is the truth table for $\tau(v)$ and it consists of 2^r elements from $GF(2)$.

Definition 1.2 [1] Suppose $\tau^*(v)$ represents the polarity truth table of a Boolean function of r -variable $\tau(v)$ then $\tau^*(v)$ consists of the 2^r elements lies from the set $\{-1,1\}$. It can be obtained by mapping the Boolean function 0 to 1 and 1 to -1 or equivalent function using the truth table:

$$\tau^*(v) = (-1)^{\tau(v)}$$

Another very useful Boolean function measurement tool is Hamming weights. The following definitions and results determine the effectiveness of Hamming weights related to Boolean capabilities and cryptographic properties of cryptanalysis.

Definition 1.3 [1] Hamming weight ($W(\tau^*)$ or $W(\tau)$) of a Boolean function $\tau(v)$ of r -variable is the number of 1s in the polarity truth table or the number of -1s in the truth table.

$$W(\tau^*) = 2^{r-1} - 0.5 \sum_v \tau(v) = \sum_v \tau(v)$$

Hamming distance is used to find similarities between two Boolean functions.

Definition 1.4 [1] Suppose the Hamming distance of two functions $\tau \in Z_2^r$ and $\tau' \in Z_2^r$ be represented by $d(\tau, \tau')$. Then $d(\tau, \tau')$ is categorized as the number of positions in the truth table where the functions differ.

$$d(\tau, \tau') = W(\tau \oplus \tau')$$

The concept of correlation is very important because it provides an alternative method of determining the degree of similarity between two Boolean functions.

Let τ and τ' be two Boolean functions, then they are uncorrelated if the value of the correlation coefficient between them is zero. Equivalently, if the valuation of τ is independent of the information of τ' . However, if the valuation for the correlation coefficient to be 1 or -1 ensures that there is the flawless positive connection ($\tau = \tau'$) individually or an impeccable negative connection ($\tau = -\tau'$), between the two functions.

Definition 1.5 [1] Suppose $\mathcal{C}(\tau, \tau')$ represents the correlation between $\tau \in Z_2^r$ and $\tau' \in Z_2^r$, the two Boolean functions. It is given by:

$$\begin{aligned}
\mathcal{C}(\tau, \tau') &= 2P\left((\tau'(v) = \tau(v))\right) - 1 \\
&= 2\left[\frac{2^r - d(\tau, \tau')}{2^r}\right] - 1 \\
&= 2\left(1 - \frac{d(\tau, \tau')}{2^r}\right) - 1 \\
&= 1 - \frac{d(\tau, \tau')}{2^{r-1}}
\end{aligned}$$

here $d(\tau, \tau')$ indicates the distance between the Boolean functions τ and τ' . It is also expressed as:

$$\begin{aligned}
\mathcal{C}(\tau, \tau') &= 1 - \frac{d(\tau, \tau')}{2^{r-1}} \\
&= 1 - \frac{\sum_v (\tau'(v) \oplus \tau(v))}{2^{r-1}} \\
&= \frac{2^r - 2 \sum_v (\tau(v) \oplus \tau'(v))}{2^r} \\
&= \frac{\sum_v 1 - 2 \sum_v (\tau(v) \oplus \tau'(v))}{2^r} \\
&= \frac{\sum_v (1 - 2(\tau(v) \oplus \tau'(v)))}{2^r} \\
&= \frac{\sum_v \tau^*(v) \tau'^*(v)}{2^r}
\end{aligned}$$

Therefore, the correlation coefficient always lies in $[-1, 1]$. The outcome of the correlation coefficient gives 1 if the hamming distance between two functions is zero. Similarly, the value -1 of a correlation coefficient is obtained if the hamming distance between the two functions is 2^r . The correlation becomes a very important tool especially in connection to the concept of an imbalance in a Boolean function when analysed in term of pair of functions.

Algebraic Normal Form (ANF)

Algebraic normal form (ANF) is another important representation of Boolean functions. For each ANF representation, the Boolean function has only one truth table. ANF provides a Boolean function in the form of a unique XOR sum of AND product of input variables [2].

Definition 1.6 [1] If ANF representation of r -variables Boolean function $\tau(v)$ consists of all r variables then it is known as nondegenerate function and if it does not contain all r variables it is known as degenerate.

The algebraic complexity and algebraic degree of Boolean function are directly proportional to each other.

Definition 1.7 [1] Suppose $\deg(\tau)$ represents the algebraic degree of a Boolean function, $\tau(v)$. An algebraic degree is defined as "the number of variables in the highest product term of the function's ANF having a nonzero coefficient.

Lemma 1.8 [3] Suppose $\tau(v)$ be an r -variable Boolean function. Then $\deg(\tau) < r$ if and only if $2/W(\tau)$.

Hamming weight should not be even for all r -variable Boolean functions of degree r according to the above lemma.

The connection between algebraic degree and hamming weight for a Boolean function is defined by the theorem [3]

Theorem 1.9 [3] Suppose $\tau(v)$ be an r -variable Boolean function and $\deg(\tau) > 0$. Then $2^{\lfloor \frac{r-1}{\deg(\tau)} \rfloor} W(\tau)$.

The r -dimensional space of the Boolean function has a subspace of the set of all the affine functions. This affine function subspace also contains the linear functions. The algebraic degree of affine functions is one.

Definition 1.10 [3] Suppose a, b be vectors in V_2^r . A Boolean function having representation $J_a(b) = a \cdot b = a_1 b_1 \oplus a_2 b_2 \oplus \dots \oplus a_r b_r$ is known as r-variable linear function.

Here the product is just a dot product of vectors $a, b \in V_2^r$.

Any linear function and its complement are affine functions, but the converse does not hold in general.

Definition 1.11 [3] Suppose a, b be vectors in V_2^r and $a_0 \in V_2^r$. Then a Boolean function having representation $\tau(b) = a_0 \oplus J_a(b) = a_0 \oplus (a \cdot b) = a_0 \oplus a_1 b_1 \oplus a_2 b_2 \oplus \dots \oplus a_r b_r$ is known as r-variable affine function. Clearly, $\tau(b)$ is even linear if $a_0 = 0$.

It is quite advantageous to have a transformation that preserves quite a lot of cryptographic properties and altering others. Affine transformation is categorized as such transformation.

Definition 1.12 [3] Suppose $\tau(v)$ be r-variable Boolean function. Then the affine transformation is defined as the resulting function $\tau'(v)$ by the following expression

$$\tau'(v) = \tau(Tv \oplus b)$$

Where T is a $r \times r$ binary invertible matrix and $v, b \in V_2^r$. If $b = 0$, it is again linear. Also, if for some $a \in V_2^r$, the projected translation $\tau'(v) = \tau(Tv \oplus b) \oplus a$, the output vector will not nullify the affine transformation. Also, the sum of an affine Boolean function with a Boolean function is an affine transformation as a result.

Definition 1.13 [3] Let τ and τ' be two distinct Boolean functions. Then τ and τ' to be in the same equivalence class if and only if there exists some c, d, f and T such that the following equivalence relation holds:

$$\tau'(v) = \tau(Tv \oplus c) \oplus d \cdot v \oplus f$$

Where $c, d \in F_2^r$, $f \in F_2$, and $T_{r \times r}$ is an invertible matrix.

1.3.2.1 Walsh Hadamard Transform

Another very vital representation of the Boolean function which described the information differently is the Walsh Hadamard Transform (WHT). The WHT of each Boolean function is mutually exclusive, and the function is expressed as its correlation with all linear functions [3]. It is presented in the next section that the advantages of WHT indirectly determining some qualities and properties of Boolean functions.

Definition 1.14 [3] Suppose that $K(a)$ be the WHT of the polarity truth table $\tau^*(v)$ of the Boolean function. WHT evaluates a function and its correlation with the set of all the linear functions. It is expressed as

$$\begin{aligned} K(a) &= \sum_v (-1)^{\tau(v)} (-1)^{J_a(v)} \\ &= \sum_v \tau^*(v) J_a^*(v) \end{aligned}$$

Where $J_a^*(v) \in \{-1, 1\}$ and $a \in V_2^r$. Thus, for all a , $K(a) \in \mathcal{R}$ having a range $[2^{-r}, 2^r]$.

Definition 1.15 [3] Suppose $\ell_a(v)$ represents a linear Boolean function and for some $a \in V_2^r$, then it is expressed as:

$$\ell_a(v) = a_1 v_1 \oplus a_2 v_2 \oplus \dots \oplus a_r v_r$$

Where \oplus represents addition modulo 2 and $a_j v_j$ is bitwise AND for i_{th} bits of a and v .

1.3.2.2 Cryptographic properties of a Boolean function

➤ Balance

The most fundamental cryptographic properties anticipated to be shown by Boolean functions is balance.

Definition 1.16 [3] An r -variable Boolean function τ , is known as balanced if $W(\tau) = 2^{r-1}$, or, $\#\{v: \tau(v) = 0\} = \#\{v: \tau(v) = 1\}$.

An r -variable Boolean function τ is imbalance if $W(\tau) \neq 2^{r-1}$. It is also defined as:

$$\begin{aligned} \mathbb{I}(\tau) &= 2^{r-1}(\mathcal{C}(\tau(v), 0)) = |W(\tau) - 2^{r-1}| \\ &= 2^{r-1} \left(1 - \frac{d(\tau(v), 0)}{2^{r-1}} \right) \\ &= 2^{r-1} - d(\tau(v), 0) \\ &= |2^{r-1} - W(\tau)| \end{aligned}$$

Where 0 is considered as the zero Boolean function. The scalar value between the zero Boolean function and correlation coefficient τ is proportional to $\mathbb{I}(\tau)$. Any function having zero imbalance is balanced and with constant function, it does not correlate.

➤ **Nonlinearity**

Nonlinearity is one of the most important and ideal cryptographic characteristics of Boolean functions, which can be demonstrated by the hamming distance between the Boolean function and the position of each related function. The concept of nonlinearity of Boolean function is presented by W. Meier and O. Staffelbach [4].

Definition 1.17 [4] The minimum Hamming distance between the set of all r -variable affine functions and an r -variable Boolean function τ . Mathematically, it is defined as

$$NL(\tau) = 0.5(2^r - K_{max})$$

where K_{max} is the maximum absolute value in the Walsh-Hadamard transform vector.

Nonlinearity can be evaluated based on various existing standards for Boolean functions. It also contains the minimum distance to the affine function and the order of the Boolean function. every linear system can be easily cracked by linear cryptanalysis. The Boolean function is the most effective way to measure nonlinearity because it means that a small change in the truth table will

result in a small change in the minimum distance. To obtain more nonlinearity, the minimum distance must be reduced to an affine function [4].

An important description of Boolean functions in correspondence to their cryptographical features is in terms of the autocorrelation function. This feature of the Boolean function is attained through the derivative. The effect of the result of the Boolean function in the variable direction is realized by the derivative of the Boolean function according to the change of its input data.

Definition 1.18 [1] Suppose $\tau(v)$ be the Boolean function and $\mathcal{r}(s)$ denote autocorrelation function of $\tau(v)$ then $\mathcal{r}(s)$ is expressed as:

$$\mathcal{r}(s) = \sum_v \tau^*(v) \tau^*(v \oplus s), v, s \in \{0, 1, \dots, 2^{r-1}\}$$

The autocorrelation function describes that how much the directional derivative corresponding to the input of a Boolean function deviates concerning $s, \forall v \in \{0, 1, \dots, 2^{r-1}\}$. The definition of autocorrelation categorizes two important features of Boolean functions parallels to the value of s . If $s \neq 0$, then $\mathcal{r}(s) = 2^r \mathcal{C}(\tau(v), \tau(v \oplus s))$ which means the correlation between $\tau(v)$ and $\tau(v \oplus s)$ is proportional to autocorrelation. On the other side, if $s = 0$ then AC is 2^r . This implies that there is no alteration in the function corresponding to s . Autocorrelation is essential for studying Boolean functions in cryptography because cryptanalysis abuses its unbalanced derivatives.

The absolute index is the most important amount of cipher that the autocorrelation function can observe. It is used to evaluate the avalanche characteristics and states the absolute maximum value other than zero for the autocorrelation function $|AC_{max}|$ such that $\mathcal{r}_{max}(s) \in [0, 2^{r-1}]$. The AC function can also be utilized to derive the absolute indicator.

➤ **Avalanche Property**

The avalanche characteristic is one of the most important characteristics of the Boolean function proposed by Feistel [5]. The Boolean function τ justify that the avalanche criterion is holding if and only if the change of the input bit changes half of the average output bit.

The Avalanche property provides confusion in the expected result. It allows us to get randomness in the results. The effect of changing the input bit on the output bit of the Boolean function can be estimated by considering the derivative of the Boolean function. The derivative expression of the Boolean function is defined as follows.

$$d_s \tau(v) = \tau(v) \oplus \tau(v \oplus s)$$

Definition 1.19 [1] Suppose $\mathcal{A}_{y_j}(\tau)$ represents the avalanche effect for a Boolean function $\tau(v)$ corresponding to a variable y_j . Then \mathcal{A}_{y_j} is expressed by the equation.

$$\mathcal{A}_{y_j} = \text{prob}(\tau(v) \oplus \tau(v \oplus y_j) = 1), \forall v$$

➤ **Completeness**

The concept of the completeness property of a Boolean function is presented by Davida and Kam [6]. They claim that each output of the Boolean function depends on all the input bits of the Boolean function. According to the claim, "If there is a pair of input bits for each input y bit and output x bit of a Boolean function, they differ only in the y bit, but their output is different in the x bit, the function has a good completeness effect".

Definition 1.20 [1] A function $\mathbb{Z}_2^r \rightarrow \mathbb{Z}_2^s$ is complete if and only if

$$\sum_{v \in \mathbb{Z}_2^r} \tau(v) \oplus \tau(v \oplus C_j^r) > (0, 0, \dots, 0), \quad \forall j = 1, 2, \dots, r$$

where the summation and greater-than ($>$) both are applied pair wise.

➤ **Strict Avalanche Criteria**

The idea of SAC was originally proposed by Webster and Tavares [7]. In fact, they combine the characteristics of avalanches with the integrity of Boolean functions. When cryptographers want to map the τ r bit complexity to one bit, they use SAC. According to SAC, changing the single input bit may change half of the output bits. Therefore, the optimal probability of SAC is half [8].

Definition 1.21 [1] An r -variable Boolean function τ is known as fulfil SAC, if $\forall s W(s) = 1, \sum_v \tau(v)\tau(v\oplus s) = 2^{r-1}$.

➤ **Correlation Immunity and Resilience**

Correlation immunity evaluates the degree of independence between the output bits of a Boolean function and the linear combination of inputs [8]. More precisely, a Boolean function $\tau(v)$ with a correlation of i^{th} order immune if it does not depend upon any of the subsets with input variable i ($1 \leq i \leq r$).

Definition 1.22 [1] For Boolean function $\tau(v)$ of r -variable having WHT polarity $K^*(x)$, it is a necessary and sufficient condition for the function to be of i^{th} order correlation immune that $K^*(x) = 0$ for each non-zero x , $W(x) \leq r$. In cryptography, it is very important to have a correlation immune Boolean function to provide resistance against divide and conquer attacks [8].

A function is Resilience if it is balanced and has correlation immune.

Definition 1.23 [1] For an r -variable Boolean function $\tau(v)$ having WHT polarity $K^*(x)$. It is the necessary and sufficient condition for the function to be r -resilient that for all $\forall x$ with $W(x) \leq r$, we must have $K^*(x) = 0$.

1.3.3 The S-box

In this section, the S-box theory will be discussed. The basic description of the S-box theory is presented for the support of research development. This section also discusses the encryption capabilities of the S-box.

➤ **Definition of S-box**

S-box is a usual advancement from single input theory to multiple output Boolean functions. Using the ratio of input and output bits in terms of singularity and dimensionality, different types of S-boxes can be obtained. We have listed some important S-box definitions below and briefly described some of the important types of S-boxes.

In this overview, a nonlinear transformation with m input bits result in n output bits is an $m \times n$ S-box.

$$F: \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^n$$

Therefore, a fixed combination of m unique output Boolean function is called an S-box. The possible inputs and outputs for an $m \times n$ S-box are 2^m and 2^n respectively. An $m \times n$ S-box F is indexed as $F[j]$ ($j \in [0, 2^m - 1]$), each input consists of n bit composition is usually described as a rectangular $2^{\frac{m}{2}} \times 2^{\frac{n}{2}}$ dimensional matrix.

The position of the output bits of the Boolean function is described as follows:

For the function g_j assigned to a binary vector of length 2^m , consider the m functions g_1, g_2, \dots, g_m . Then $F = [g_1, g_2, \dots, g_m]$ is the S-box with g_j as the column vectors, usually described as a $2^m \times m$ bit matrix. Any input $u = u_1, u_2, \dots, u_m$ results as an output $v = v_1, v_2, \dots, v_m$ through the assignment $h_j(u_1, u_2, \dots, u_m) = v_j$.

According to the input and output bits of the S-box, we can classify S-box into one-to-one, envelope, and bijection. The definition of each category is given below.

Consider an S-box F with the dimension $m \times n$, here m input and n are output bits. For $m < n$ then F is said to one-one S-box if it has different output entries. In this case, it is impossible for F to have all outputs as its entries.

If input bits are greater than the output bits of S-box F then there is a repetition in the entries of the S-box. If F covers all the outputs entries, then it is called onto.

Lastly, the input and output bits are equal ($m = n$) then two possibilities occur.

- a) The S-box F covers all input bits results as a different output bit which shows that it covers all possible distinct entries.
- b) The S-box F mapped different input bits to similar output bits, then F does not contain all entries and has repeated entries.

For the first case with distinct entries, F is called bijective. Similarly, F is both one-to-one and onto then is called bijective. This situation arises only when both input and output bits are same and such a S-box is renown as invertible S-box.

1.3.4 Cryptographic Properties of S-box

1.3.4.1 Nonlinearity of S-box

Suppose C_l represents the set of all nontrivial linear combinations of the columns of an S-box S , then the nonlinearity of S will be $N_L(S) = \min N_L(g)$, where $g \in C_l$. In a simpler way, the smallest possible Hamming distance between the entire affine functions of r variables and the component function of S-box S is equal to its nonlinearity $N_L(S)$. This generalization is carefully connected with linear attacks as in linear attack hackers try to drive linear equations to approximate the S-box.

It is an important observation that the nonlinearity is left and right affine invariant for S-boxes and its value will not be changed by adding an affine function to an S-box S . Similarly, for

$P: \mathbb{Z}_2^q \rightarrow \mathbb{Z}_2^r$ to be an onto linear (or affine) function it can also be justified that $N_L(S \circ P) = 2^{q-r} N_L(S)$.

The equation connecting the nonlinearity of Boolean function and the maximum magnitude of the Walsh transform has the following comparison.

$$N_L(S) = 2^{r-1} - 0.5 \max_{x \in (V_2^t); z \in (V_2^r)} \left| \sum_{v \in V_2^r} (-1)^{x \cdot F(v) \oplus z \cdot v} \right|$$

Therefore, the nonlinearity of S-box S and its inverse S^{-1} are equal if and only if S is a bijection and $r = t$.

1.3.4.2 Algebraic Degree for an S-box

The algebraic degree of an S-box should be high, in order to resist against cryptanalytic attacks. The next definition provides the description of the algebraic degree of an S-box.

Definition 1.24 [1] Suppose an $t \times r$ S-box $S = (\tau_0, \tau_1, \dots, \tau_{r-1})$ with Boolean functions τ_i ($1 \leq i \leq r-1$) of t variables and h_j contained all linear combinations of τ_i ($h = 0, 1, 2, \dots, r-1$) (including τ_i). Then algebraic degree, $d_g(S_t, r)$, for S can be defined by the following expression.

$$d_g(S_t, r) = \min_h \{d_g(h_j)\} \quad (1 \leq j \leq 2r-1)$$

1.3.4.3 Autocorrelation of S-box

The autocorrelation of an S-box is the supreme autocorrelation for all linear combinations of each Boolean function of an S-box.

Suppose an $t \times r$ S-box $S = (\tau_0, \tau_1, \dots, \tau_{r-1})$ with Boolean functions τ_i ($1 \leq i \leq r-1$) of t -variable and H_j contains all linear combinations of each Boolean function of S . The autocorrelation, $AC(S_t, r)$, for S can be defined by the equation.

$$AC(S_t, r) = \max_H \{f(H_j)\} \quad (j = 1, \dots, 2r-1)$$

Definition 1.25 [1] A function $\tau: V_2^r \rightarrow V_2^t$ is complete if and only if for every i ($1 \leq i \leq r$) τ must satisfy the inequality:

$$\sum_{v \in V_2^r} \tau(v) \oplus \tau(v \oplus C_i^r) > (0, 0, 0, \dots, 0)$$

Where C_i^r is the vector, whose hamming weight is the unit at the i_{th} position.

This represents the necessity of each single output bit on the whole set of input bits. Hence for a complete function, it is a necessary condition that each expression of output bit depends on the input bits to comprehend all the input bits for a Boolean function.

Definition 1.26 (Avalanche effect) [1]. A function $\tau: V_2^r \rightarrow V_2^t$ has avalanche effect if and if it satisfied the equation:

$$\forall i, \sum_{v \in V_2^r} W(\tau(v) \oplus \tau(v \oplus C_i^r)) = r2^{r-1}, \quad (1 \leq i \leq r)$$

Where C_i^r is the vector, whose hamming weight is the unit at the i_{th} position. It mean nearly half of the output bits alter when we take the complement of one input bit.

1.3.4.4 Strict Avalanche Criterion (SAC)

If a single variation in input creates series of alterations in the entire substitution permutation network, the avalanche effect is observed that is nearly half of the resulting bits have change values by a single change.

A function $\tau: V_2^r \rightarrow V_2^r$ satisfied SAC if the following relation holds:

$$\forall i, \sum_{v \in V_2^r} \tau(v) \oplus \tau(v \oplus C_i^r) = (2^{r-1}, 2^{r-1}, 2^{r-1}, \dots, 2^{r-1}) \quad (1 \leq i \leq r)$$

Especially, the function $\tau: V_2^r \rightarrow V_2^r$ satisfied SAC suggests that τ is a robust Boolean S-box. It means the probability of complimenting one input bit should deviate nearly half of the

output bits. If an S-box satisfied SAC and has completeness property, then it is considered a robust S-box.

If any relation between input and output bits exists, then cryptanalysts utilizing plaintext attacks can search for the secret key utilizing the relationship between input and output bits.

1.3.4.5 Bit Independence Criterion (BIC)

The independence of pair-wise avalanche vectors and the variations of input bit are the significant aspects of the bit independence criterion. The basic theme of the bit independence criterion (BIC) is the complementation of a single input bit.

A function $\tau: V_2^r \rightarrow V_2^r$ satisfies BIC if $\forall m, n, t \in \{1, 2, 3, \dots, r\}$ with $n \neq t$, altering m input bits made n and t output bits to vary separately. It is very important in BIC analysis, to focus on avalanche vector A^{em} which is the correlation of n_{th} and t the modules in the output bits.

The parameter A^j of BIC affected by the change in the m_{th} input bit on the output bits n and t is defined by [4]:

$$BIC(p_t, p_m) = \max_{1 \leq n \leq r} |C(p_t^{en}, p_r^{en})|$$

More generally:

$$BIC(\tau) = \max_{1 \leq n, t \leq r} BIC(p_t, p_m)$$

This relationship shows the closeness for τ to satisfy the BIC. The values for $BIC(\tau)$ remain in the interval $[0, 1]$. The value 0 is considered as ideal and 1 as foulest.

1.4 Basic Terminologies of Non-associative Structures

Definition 1.27 [9] Let $S \neq \emptyset$ be set and “ $*$ ” be operation on S then $*$ is called binary operation on S if and only if

$$\forall s_1, s_2 \in S \Rightarrow s_1 * s_2 \in S$$

If “ * ” a binary operation on S , then $(S,*)$ is called groupoid.

Definition 1.28 [9] A groupoid $(S,*)$ is called Semigroup if it is associative, that is

$$\forall s_1, s_2, s_3 \in S, (s_1 * s_2) * s_3 = s_1 * (s_2 * s_3)$$

Definition 1.29 [9] A semigroup $(S,*)$ is called a monoid if there is a unique element $e \in S$ satisfying.

$$e * s = s * e = s, \forall s \in S$$

e is called the identity element of set S .

Definition 1.30 [9] A monoid $(S,*)$ is called a group if, for each element $s_1 \in S$, there is a unique element s_2 in S which satisfying $s_1 * s_2 = s_2 * s_1 = e$.

Example 1.1 The sets $\mathbb{Z}, \mathbb{Q}, \mathbb{R},$ and \mathbb{C} are all groups under the binary operation of “ + ”.

$(\mathbb{Z}_m, + \text{mod } m)$ is also group with 0 as an identity element, here $\mathbb{Z}_m = \{0, 1, 2, \dots, m - 1\}$. For each $s_1 \in \mathbb{Z}_m$ has an inverse $-s_1$ which holds $s_1 + (-s_1) \equiv 0 \text{ mod}(m)$. But the set \mathbb{Z}_m is not a group under the binary operation “ \cdot ” mod m .

Remark 1.31 The sets (\mathbb{N}, \cdot) and (\mathbb{Z}, \cdot) are monoid only but not groups. Here operation “ \cdot ” is a simple multiplication of numbers.

Definition 1.32 [9] Let L be a non-void set together with a binary operation $*$ $(x, y) \rightarrow x * y$. Then L is called quasigroup if the following axioms are satisfied.

1. The equation $x * y = z$ determines a unique element $y \in L$ for given $x, z \in L$.
2. The equation $x * y = z$ determines a unique element $x \in L$ for given $y, z \in L$.

Example 1.2

*	1	2	3
1	3	1	2
2	2	3	1
3	1	2	3

Definition 1.33 [9] A quasigroup is said to be a loop if it has a two-sided identity element $e \in L$ for example.

$$e * x = x * e = x \text{ for all } x \in L.$$

Example 1.3

*	0	1	2	3	4
0	0	1	2	3	4
1	1	3	0	4	2
2	2	4	3	1	0
3	3	2	4	0	1
4	4	0	1	2	3

Definition 1.34 [9] A subset H of a loop $(L,*)$ is called a subloop if it is itself a loop under the same binary operation.

Definition 1.35 [9] Suppose L be a loop and $a \in L$, Then a mappings $L_a: L \rightarrow L$ and $R_a: L \rightarrow L$ s.t $L_a(x) = ax$ and $R_a(x) = xa$ are called the left and right translation respectively.

Proposition 1.36 [9] Suppose L be a loop and H is a non-void subset of L . Then the following axioms are equivalent

1. H is a subloop of L .
2. If $x, y \in H$, implies that $xy, xR(y)^{-1}$ and $xL(y)^{-1}$ are all in H .
3. For any elements x, y, z of loop L , in an equation $xy = z$ if any two of these are in H ,

Then the third element also belongs to H .

Remark 1.37 [10] Lagrange's theorem does not hold in a loop.

Example 1.4

*	e=1	2	3	4	5	6	7
e=1	1	2	3	4	5	6	7
2	2	3	1	6	7	5	4
3	3	1	2	7	6	4	5
4	4	7	6	5	1	2	3
5	5	6	7	1	4	3	2
6	6	4	5	3	2	7	1
7	7	5	4	2	3	1	6

a	1	2	3	4	5	6	7
a⁻¹	1	3	2	5	4	7	6

This loop of order 7 has 3 subloops of order 3.

*	1	2	3		*	1	4	5		*	1	6	7
1	1	2	3		1	1	4	5		1	1	6	7
2	2	3	1		4	4	5	1		6	6	7	1
3	1	2	3		5	1	4	5		7	1	6	7

Definition 1.38 [9] Suppose $(L,*)$ be a loop and $x, y \in L$. Then (x, y) is called the commutator of x, y in L and is defined as,

$$xy = (yx)(x, y)$$

Definition 1.39 [9] Suppose $(L,*)$ be a loop and $x, y, z \in L$. Then (x, y, z) is called the Associator of x, y, z in L and is defined as,

$$(xy)z = \{x(yz)\}(x, y, z)$$

Definition 1.40 [9] The commutator-associators subloop of loop L , denoted as L' , is generated by a set of all associators and all commutator of loop L . So

$$L' = \langle (L, L, L), (L, L) \rangle$$

Definition 1.41 [9] Left nucleus of loop L is an associative subloop of L defined as

$$N_\lambda(L) = \{x \in L, (x, a, b) = 1, \text{ for all } a, b \in L\}$$

Definition 1.42 [9] Middle nucleus of loop L is an associative subloop of L defined as

$$N_\mu(L) = \{x \in L, (a, x, b) = 1, \text{ for all } a, b \in L\}$$

Definition 1.43 [9] Right nucleus of loop L is an associative subloop of L defined as

$$N_\rho(L) = \{x \in L, (a, b, x) = 1, \text{ for all } a, b \in L\}$$

Definition 1.44 [9] Nucleus of loop L is an associative subloop of L defined as

$$N(L) = N_\lambda(L) \cap N_\mu(L) \cap N_\rho(L)$$

Definition 1.45 [9] Center of the loop is denoted by $Z(L)$ and defined as

$$Z(L) = \{x \in N(L), (a, x) = 1, \text{ for all } a \in L\}$$

Definition 1.46 [9] Let $(L, *)$ be loop and H be subloop of loop L , then H is called normal subloop if the following axioms hold.

$$Ha = aH, (Ha)b = H(ab), (aH)b = a(Hb) \text{ and } b(aH) = (ba)H$$

Definition 1.47 [9] A loop $(L, *)$, where $*$ denotes the binary operation is called as IP-loop if

$\forall u, v \in L$ it satisfies following axioms:

i. $u * e = u = e * u$

ii. $u * u^{-1} = e = u^{-1} * u$

iii. Left inverse property existence i.e. $u^{-1} * (u * v) = v$

iv. Right inverse property existence i.e., $(v * u) * u^{-1} = v$

Remark 1.48 The following properties hold in an IP-loop.

- $(u^{-1})^{-1} = u$

- $(uv)^{-1} = v^{-1}u^{-1}$
- $N(L) = N_\lambda(L) = N_\mu(L) = N_\rho(L)$

Definition 1.49 [9] Let $(L,*)$ be a loop then for three elements $u, v, w \in L$ is termed to be Weak Inverse Property (WIP) if the following two equations are satisfied:

- $uv * w = e$
- $u * vw = e$

Definition 1.50 [9] The loop $(L,*)$ is said to be PA-loop if the subloop generated by any element a of L is a cyclic subgroup. i.e.

$$a * a^2 = a^2 * a$$

Thus, the cyclic groups are a special case of this class. As in PA-loops, every subloop generated by a single element is a cyclic subgroup.

1.5 Boolean Operations

Definition 1.51 [11] AND Operation

Suppose $X = \{0,1\}$, then a mapping $\wedge: X \times X \rightarrow X$ is called AND Operation. Its output is 1 only when both inputs are 1 otherwise its output is 0. Its truth table is given below:

s	t	s \wedge t
1	1	1
1	0	0
0	1	0
0	0	0

Definition 1.52 [11] OR Operation

Suppose $X = \{0,1\}$, then a mapping $\vee: X \times X \rightarrow X$ is called OR Operation. Its output is 0 only when both inputs are 0 otherwise its output is 1. Its truth table is given below:

S	T	$s \vee t$
1	1	1
1	0	1
0	1	1
0	0	0

Definition 1.53 [11] XOR Operation

Suppose $X = \{0,1\}$, then a mapping $\oplus: X \times X \rightarrow X$ is called XOR Operation. Its output is 1 when both inputs are different otherwise its output is 0. Its truth table is given below:

s	t	$s \oplus t$
1	1	0
1	0	1
0	1	1
0	0	0

Chapter 2

Construction Scheme of S-boxes over IP-loops

This chapter is organized as follows: Section 1, contains an introduction. Section 2 describes the algebraic structure of IP-loop and proposed S-boxes and the methods to analyses the newly developed S-boxes are presented and a comparison of these S-boxes with some of the prevalent S-boxes used in different security systems is discussed in section 4.

2.1 Introduction

With the access of information to every corner of the world through the internet, securing information and the procedures of securing information are the most important themes presently. Every moment, trillions of PINs are created throughout the world for information protection. Any advancement in this area will not be enough. To serve this cause, the most prominent studies are in the field of cryptography. The role of cryptography is very important as it hides the original information and converts it to an unreadable form (cipher text). Only lawful persons can interpret it by using an exact secret key. Occasionally the information is scratched by cryptanalysis, mostly known as codebreaking. Of late, most of the cryptographic systems are indestructible. In advanced cryptography block ciphers contribute a key role in symmetric (private key-based) cryptosystems. In such cryptosystems, only the receiver and the sender know the key [12-13].

In 1997, the National Institute of Standard and Technology (NIST) first started the symmetric key encryption or decryption algorithm. Later in 2001, NIST esteemed the Rijndael method as the

Advanced Encryption Standard (AES) [14] as it is unbreakable as compared to Data Encryption Standard (DES) [15].

The S-box is the only nonlinear section of a block cipher, which is responsible for producing confusion. Numerous procedures are established for the construction of nonlinear mechanisms to rise confusion in recent block ciphers. Retrieval of the unidentified key sequence is convenient provided that the block cipher has a linear relationship between the plaintext and the ciphertext. [16-25]. The S-box design is mainly based on the Galois field with characteristic 2, so the basic algebraic structure needs to be improved and modified. To increase the complexity of S-boxes, it makes sense to replace the Galois field with a more general Galois ring configuration. Firstly, the Galois ring attained importance in algebraic coding theory in 1979, when Shankar [26] established a relationship among the BCH codes over local ring \mathbb{Z}_p^k and the prime field \mathbb{Z}_p . Later in 1999, Andrade and Palazzo [23] constructed the BCH codes over finite unitary commutative rings. Both constructions are fixated to the maximal cyclic subgroup of the group of units of a Galois ring extension of a local ring. Look at the construction of the S-box based on the Galois field and Galois ring, there is an inverse zero constraint. To solve this problem, a piecewise inversion map is used, which makes the calculation more complicated to understand. This deficiency is removed in this work. The IP-loops-based S-box shows good robustness in terms of its complexity and is very useful in cryptosystems.

2.2 Why we use IP-loop

This chapter proposes an innovative idea of constructing S-boxes over IP-loops of different orders. The non-associativity and the existence of zero-element inversion and the uniqueness of each element inversion are the main features of the proposed structures. With these characteristics, the structure is more generalized as compared with the Galois field and Galois ring. If you consider

the mathematical structure of the S-box based on the Galois field and the Galois ring, there is a deficiency of inverse of zero. To solve this problem, a piecewise inversion map is used, which makes the calculation more complicated, but this work overcomes this deficiency. The S-boxes constructed using this algebraic structure have good characteristics, which shows it is useful in cryptosystems.

2.2.1 Non-group Smallest IP-loop

The smallest IP-loop which is not a group is of order 7 it is given in Table 2.1. Notably, the order of the loop is not divisible by the order of the sub-loop. This structure has proper sub-loops $\{1,2,3\}$, $\{1,4,5\}$ and $\{1,6,7\}$. Associativity will not hold in this structure, for example, $(2 * 2) * 4 = 3 * 4 = 7$ while $2 * (2 * 4) = 2 * 6 = 5$. Non-associativity allow to construct more structures than what occurs for associative structures like Groups, Rings, and Fields. This phenomenon increases rapidly as the size increases. Table 2.2 shows how much fast increase is occurring when we are going up to order 8 and forwards [9, 10].

Table 2.1: The smallest IP-loop of order 7 with their inverses.

*	e = 1	2	3	4	5	6	7	a	a⁻¹
e = 1	1	2	3	4	5	6	7	1	1
2	2	3	1	6	7	5	4	2	3
3	3	1	2	7	6	4	5	3	2
4	4	7	6	5	1	2	3	4	5
5	5	6	7	1	4	3	2	5	4
6	6	4	5	3	2	7	1	6	7
7	7	5	4	2	3	1	6	7	6

Table 2.2: Comparison table of different structures of the given order.

Size	Associative Structure (Group)	Non-associative (IP-loop)	Size	Associative Structure (Group)	Non-associative (IP-loop)
1	1	1	8	5	8
2	1	1	9	2	7
3	1	1	10	2	47
4	2	2	11	1	49
5	1	1	12	5	2684
6	2	2	13	1	10342
7	1	2	14	—	—

2.3 Model of IP-loop based S-boxes

Many techniques can be used to create confusion in a security system, using an S-box is one of the most efficient technique. The S-boxes are constructed using formulas, systematic calculations, and mathematical tools. For the improvement of the worth, many people have worked in this field and so far, many S-boxes have been generated. The procedure of the S-box construction is given below in three steps.

- Inversion function $\alpha: L \rightarrow L$

- linear scalar multiple function $\beta: L \rightarrow L$
- $\beta \circ \alpha: L \rightarrow L$.

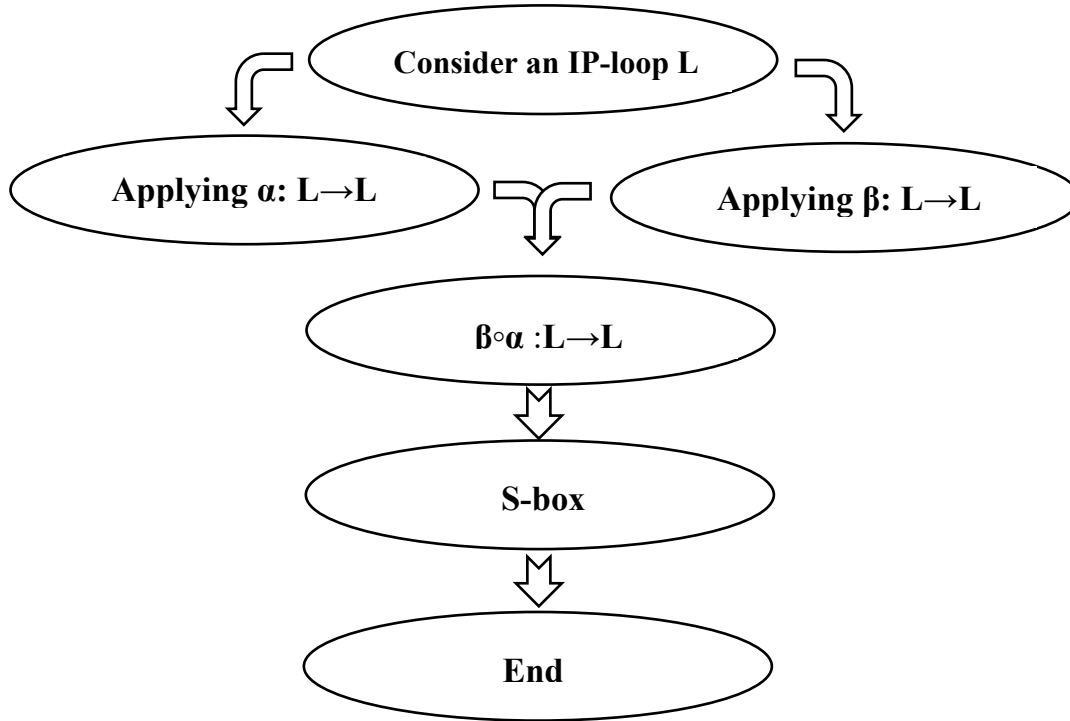


Fig. 2.1: Diagram of the proposed model

In the first step, the inverse function mapped elements of the loop into their inverses. And secondly, the scalar linear multiple function is treated as a Left translation. Then taking XOR with the elements of the loop. In the third step by a composition of the first two steps gives us an S-box. By changing the elements of the loop, we obtained different S-boxes.

Table 2.3: IP-loop L_{16} .

*	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	2	3	0	7	10	13	12	14	6	15	8	4	9	11	5
2	2	3	0	1	14	8	11	15	5	10	9	6	13	12	4	7
3	3	0	1	2	12	15	9	4	11	13	5	14	7	6	8	10

4	4	7	11	15	5	6	0	14	10	3	1	13	9	8	2	12
5	5	13	8	12	6	0	4	11	2	15	14	7	3	1	10	9
6	6	10	14	9	0	4	5	1	13	12	8	2	15	11	7	3
7	7	15	12	4	10	13	1	8	9	0	3	5	14	2	6	11
8	8	11	5	14	15	2	12	9	0	7	13	1	6	10	3	4
9	9	6	13	10	3	11	14	0	7	8	4	15	2	5	12	1
10	10	9	15	6	13	1	7	2	4	14	11	12	0	3	5	8
11	11	14	4	8	2	9	15	13	3	5	12	0	10	7	1	6
12	12	5	7	13	8	14	3	6	15	1	0	10	11	4	9	2
13	13	12	9	5	1	7	10	3	6	11	2	4	8	14	15	0
14	14	8	6	11	9	12	2	10	1	4	7	3	5	15	0	13
15	15	4	10	7	11	3	8	5	12	2	6	9	1	0	13	14

In Table 2.3, the IP-loop of order sixteen is given. This IP-loop is non-associative and the inverse of zero is zero. The composition map is defined by the following equation.

$$\beta \circ \alpha(x) = 5x^{-1} \oplus 6 \quad (2.1)$$

By using the following process entries of the S-box are obtained. Table 2.5 shows 16 distinct values of the 4×4 S-box.

Table 2.4: Construction of proposed S-box over L_{16} .

L_{16}	$\beta \circ \alpha(x) = 5(x)^{-1} \oplus 6$	Entries of Proposed S-box
0	$\beta \circ \alpha(0) = 5(0)^{-1} \oplus 6$	3
1	$\beta \circ \alpha(1) = 5(1)^{-1} \oplus 6$	10
.	.	.
.	.	.
14	$\beta \circ \alpha(14) = 5(14)^{-1} \oplus 6$	12
15	$\beta \circ \alpha(15) = 5(15)^{-1} \oplus 6$	7

Table 2.5: Proposed S-box over L_{16} .

3	10	14	11
2	6	0	9
4	13	5	1
8	15	12	7

Similarly, by using the IP-loop of order 256 (L_{256}), we construct 8×8 S-box by using equation 2.1 which is given below.

$$\beta \circ \alpha(x) = 5(x)^{-1} \oplus 6$$

Table 2.6: Construction of proposed S-box over L_{256} .

L_{256}	$\beta \circ \alpha(x) = 5(x)^{-1} \oplus 6$	Entries of Proposed S-box
0	$\beta \circ \alpha(0) = 5(0)^{-1} \oplus 6$	3
1	$\beta \circ \alpha(1) = 5(1)^{-1} \oplus 6$	1
.	.	.
.	.	.
.	.	.
254	$\beta \circ \alpha(254) = 5(254)^{-1} \oplus 6$	209
255	$\beta \circ \alpha(255) = 5(255)^{-1} \oplus 6$	80

Table 2.7: Proposed S-box over L_{256} .

3	1	13	64	185	246	67	94	123	71	144	201	153	156	59	24
14	235	175	39	18	216	215	100	56	152	194	242	135	124	33	7
53	134	219	245	52	68	82	181	98	226	87	178	223	148	137	29
164	173	91	50	77	74	101	4	119	206	34	252	203	171	151	191

189	184	157	121	227	231	233	195	165	15	150	57	139	69	78	2
118	131	17	20	99	40	180	212	83	103	164	126	141	202	192	239
75	247	51	243	158	30	230	45	222	104	32	93	198	142	55	111
251	155	107	21	120	90	63	62	161	47	146	162	72	183	228	127
129	159	48	92	35	136	95	229	5	115	211	125	138	37	170	205
65	61	160	70	79	112	23	250	38	196	8	19	9	253	156	240
197	224	0	46	66	132	109	110	73	97	143	102	108	26	128	31
255	217	25	89	236	182	113	172	237	163	84	114	49	179	186	193
190	210	27	238	106	122	28	220	174	96	213	234	54	187	188	147
249	44	154	76	177	225	16	41	167	130	12	105	85	208	254	214
200	58	36	6	241	140	248	88	133	116	218	117	60	207	145	199
43	221	86	244	149	204	11	10	81	232	22	168	169	42	209	80

2.4 Statistical and differential Analyses

In this section, we perform the necessary evaluations so that the newly constructed S-box fulfils the standard conditions and compares it with some cryptographically strong S-boxes, namely: AES S-box, APA S-box, and Gray S-box [25, 52-53]. S-box 4x4 based on 16-order IP-loop has a maximum nonlinearity of 4, a minimum of 2, and an average of 3, as shown in Table 2.8. The nonlinearity of the 8x8 S-boxes has a default value. The upper limit is 112 and the lower limit is 100; in our case, the average value is 103.75 (S-box on IP-loop of order 256). As the Strict Avalanche Criterion (SAC) studies encryption performance, it measures the encryption strength and the degree of change of the output bit when the input bit changes. If the input bit changes slightly, it may be mandatory. The SAC comparison is shown in Table 2.9. The comparison shows that the value of AES S-box is 0.504, which is the same as the S-box through IP-loop of order 256. Thus, the SAC analysis of the proposed S-box is better than Skipjack, Prime, and Xyi [46,47,51]. The results of the differential approximation probability (DP) analysis of IP-loop based S-box has

a value of 0.03906. Table 2.9 shows DP analysis of our proposed S-box and comparison with other well-known S-boxes. Table show DP analysis of our proposed S-box is better [46,47,51].

Table 2.8: Nonlinearity of proposed 4×4 S-box over IP-loop of order 16.

0	1	2	3
2	3	4	4

Table 2.9: Comparison of Nonlinearity, SAC and DP analyses.

S-boxes	SAC		Nonlinearity	DP	
	Average	Min. Value		Square Deviation	Max DP
Proposed	0.5046	0.3906	103.75	0.0246	0.03906
Ref [25]	0.504	0.48	112	0.011	0.0156
Ref [46]	0.499	0.464	105.75	0.018	0.0468
Ref [47]	0.502	0.47	99.5	0.017	0.281
Ref [51]	0.503	0.47	105	0.015	0.0468

According to the Bit Independence Criterion (BIC) to extract information about the validity of variables, we compare these variables in pairs, here we exchange the input bits and check the independence of the output bits. The feature of bit independence is more popular because the more bit parity increases, the greater the problem of identifying the security structure. The following table 2.10 compares BIC with some cryptographically strong S-boxes, it can be seen that the BIC results have a minimum value and an average value of 98 and 103.929 respectively. The standard deviation analysis of our proposed S-box is 2544, which is better and better than [46,47,51].

Table 2.10: BIC and LP Analyses of proposed S-box.

S-boxes	BIC		LP		
	Average	Min value	Square Deviation	Max LP	Max value
IP-loop	103.929	98	2.5344	0.1289	161
Ref [25]	112	112	0	0.062	144
Ref [46]	101.71	94	3.53	0.132	162
Ref [47]	104.14	102	1.767	0.109	156
Ref [51]	103.78	98	2.743	0.156	168

The method of linear approximation probability (LP) is used to investigate the imbalance of an incident. The LP method is very useful for determining the maximum imbalance in event results. Table 2.10 shows the LP results of some more advanced S-boxes. The maximum LP of the proposed S-box is 161, which shows that linear attacks can be countered. These S-boxes are comparable to the best S-boxes on the market.

2.4.1 Differential Attacks

Hackers usually try to make small changes to the original image and use the proposed technique to encrypt the original image; after the encryption process is over, they compare the encrypted image with changes and the encrypted image without changes; in this way, they try to find the connection between the original image and the encrypted image. These types of attacks are called differential attacks. In order to calculate the impact of pixel changes in the original image on the encrypted image, this is calculated based on two prominent analyses, NPCR and UACI.

Table 2.11: Differential analyses of the proposed structure.

S-boxes	Proposed	Ref [25]	Ref [30]	Ref [46]	Ref [51]
NPCR	99.7222	99.6826	99.7192	99.6155	99.5972
UACI	33.4960	34.1209	35.4084	33.5205	33.3427

Table 2.11 shows that the NPCR analysis of the proposed S-box is superior to all other S-boxes shown in the comparison. These S-boxes are AES, S8 AES, Prime and Xyi respectively [25,30,46,51]. The optimal NPCR is 99.99, and the proposed S-box NPCR is almost optimal as compared to other S-boxes. The required UACI value is 33.33. Table 2.11 shows that the proposed S-box UACI is closed to the UACI value of AES, S8-AES, Prime, and Xyi. The comparison shows that compared with these S-boxes the proposed S-box has higher resistance against differential attacks.

Chapter 3

Watermarking and Image Encryption Applications of IP-loop based S-boxes

This chapter is organized as follows: Introduction of watermarking is given in section 1, In section 2, applications of watermarking have been discussed. In section 3, types of watermarking are discussed. Techniques of watermarking are presented in section 4. Section 5 designates the methodology for the novel watermarking technique by using the application of the proposed S-box. Section 6 presents the statistical analyses of the proposed S-box.

3.1 Introduction

In the modern era, the ways for transferring data have been changed due to the vast technology of the internet and communication. Due to this vast technology, the disputes raise for reliability and integrity of information or data. In recent epochs, for passing data digital communication plays a vital role it. To communicate secretly a lot of internet tactics are used. So, the refuge of information against unlawful access has prime importance in this era. Hence, for the security of this data, many techniques would be used to hide data. In order to hide data, the most commonly used techniques are image encryption, watermarking, cryptography, and steganography. As the exertion of the S-box is generally seen in many ciphers like DES and AES. Whereas the use of S-box in applications of encryption is broadly accomplished, a fascinating approach to the digital watermarking process is presented in this chapter.

3.2 Secure Information Transmission

The hiding of information means to communicate information with the help of any digital media or by hiding. Digital media includes images, audio, a video, or simply a plain text file. Information hiding is a universal term covering many sub-disciplines. The most used techniques for hiding messages, information, or data are Steganography, Cryptography, and watermarking [62, 67, 68].



3.2.1 Steganography

The art of converting communications is termed steganography. By the alteration of properties of message or data, steganography embeds the message within an alternative object which is referred to as cover work. The output given by them is known as stegogramme.

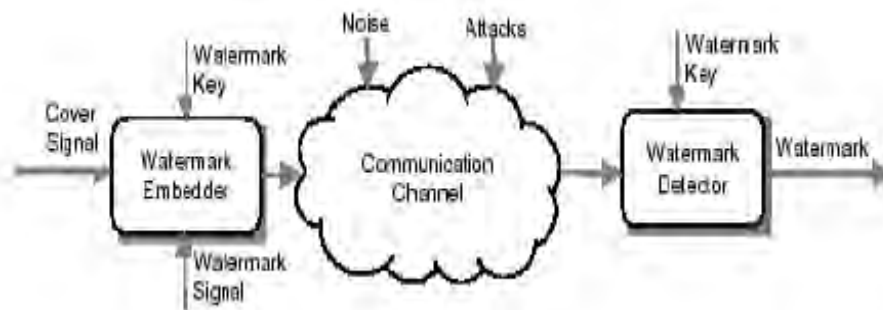
3.2.2 Cryptography

In cryptography, with the use of an encryption key the conversion of plaintext message to ciphertext should be similarly done by the sender, the receiver decrypts the ciphertext to plain text.

3.2.3 Watermarking

The technique used for the insertion of information into data or images is known as digital watermarking. Later, this information could be detected by using computing operations for making allegations about data. In host data, the watermark is hidden in such a way that it's difficult to separate it from data and so it is impervious to several operations not degrading the host file. The system of a digital watermarking system involves two types of a watermark embedder and a

watermark detector. In watermark embedding, it embeds a watermark into the cover signal and the detector watermark detects the existence of signal of the watermark. In the process of watermark detection and embedding a key known as a watermark key is used which has a one-to-one correspondence with the signal of a watermark. For every watermark signal, a unique key is used. The used key is private which should be known to only authorized parties and it also gives surety for the detection of watermark signals by the authorized parties.



3.3 Types of Digital Watermarking

Digital watermarking can be categorized into three types [67]:

- Visible watermarking
- Robust(invisible) watermarking
- Fragile(invisible) watermarking
- **Visible Watermarking**

In visible watermarking a transparent coat is applied onto the image which is visible to the viewer.

It is used for ownership indication protection for copyright.

- **Fragile Watermarking**

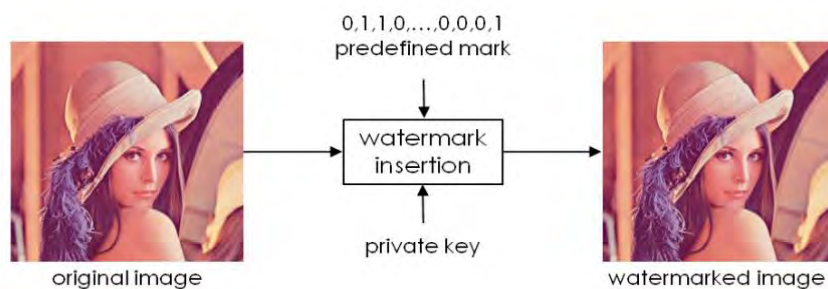
If the hidden watermark in the host signal is damaged by passing through certain manipulations then it is known as a fragile watermark.

▪ Robust Watermarking

In Robust watermark information embedding into a file could not be destroyed or damaged easily. Though no mark is indestructible, the robustness of the system is measured by the required number of alterations used to remove the mark which exhibits the file as unworkable. Hence the mark should be hidden in that part of the file where the removal can easily be observed.

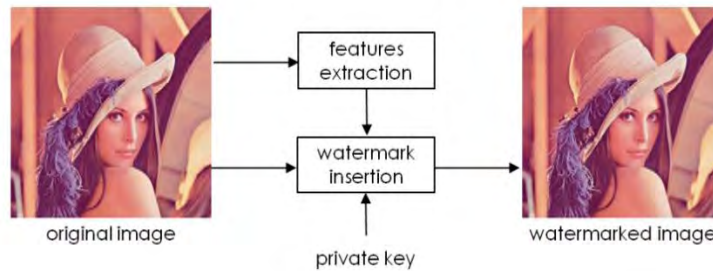
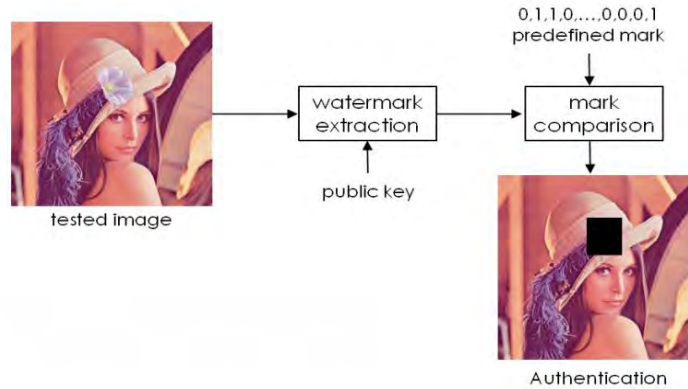
Watermark Embedding

Mostly, a watermark consists of a sequence of binary data which is inserted with the help of a key into the host signal. In this process, the embedding information routine executes bit changes in signal, resolute by the watermark and key to produce a watermarked signal.



Watermark Extraction

Watermark extraction is a technique that attempts to extract the watermark from the attacked signal. During transmission, if the signal was unchanged then the watermark present in it should be easily extracted. In the extraction process, the inputs are watermarked images and private or public keys.



3.4 Techniques of Watermarking

According to the embedding of data, the watermarking techniques are categorized into two types:

- i. Spatial domain technique
- ii. Transform domain technique

- **Spatial Domain Technique**

In the spatial domain technique, the image is presented in terms of pixels. By the modification of colour and intensity value for few selected pixels, this watermarking technique embeds a watermark. With the comparison to transform domain technique spatial domain watermarking technique is very simple, having a less computing time but against algebraic attacks, it is less strong. To any image, it could be easily applied. The most significant methodology of this technique is the least significant bit (LSB) [68].

- **Least Significant Bit**

The easiest and simplest technique of spatial domain watermarking is LSB in which by selecting any random pixel of the cover image can embed a watermark in LSB's. The following are the steps used for embedding watermark in the original image with the help of LSB are:

- i. Conversion of RGB image into Gray-scale-image
- ii. Create double accuracy for the image.
- iii. Shifting high significant bits of watermark image to less significant bits.
- iv. Making host image LSB's zero.
- v. Adding (step 3) watermarked image shifting version to modified host image (step4).

- **Transform Domain Technique**

In this watermarking technique, relatively to a pixel value, the coefficients transform coefficients are modified. For the detection of the watermark, the inverse transformation is applied. The most commonly used transform techniques are DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform), DFT (Discrete Fourier Transform) etc.

3.5 Watermarking Application of Proposed S-box

The detailed algorithm of the suggested S-box is illustrated in Fig 3.1. By the establishment of a matrix consisting of unit pixels, the image has been processed. After this, convert each element of the matrix in binary form. The induced watermarking algorithm on the image offered in this dissertation consists of per pixel 8 bits. In this algorithm, the S-box transformation is appealed over 4 LSB's of every image pixel. By Fig. 3.1, it can be seen that in this process the partition of 4 LSB's in two paired LSB's should be done, the values possible range in these pairs is {0,1,2,3}. Those values help in the selection of the S-box column or row for the identification of substituted elements. So, the image bits should be replaced with bits taken from S-box, hence it completes the

nonlinear transformation. This way should be repeated for each pixel in the image. Then transform the resulting matrix into the image after that display and save the watermarked image.

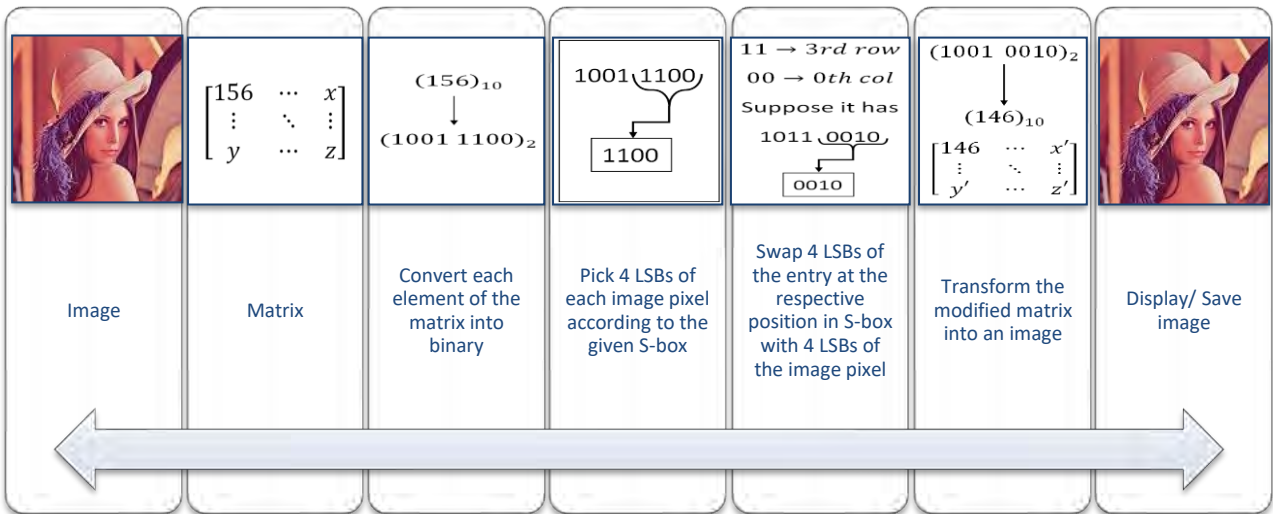


Fig. 3.1: Watermarking algorithm of suggested S-box.

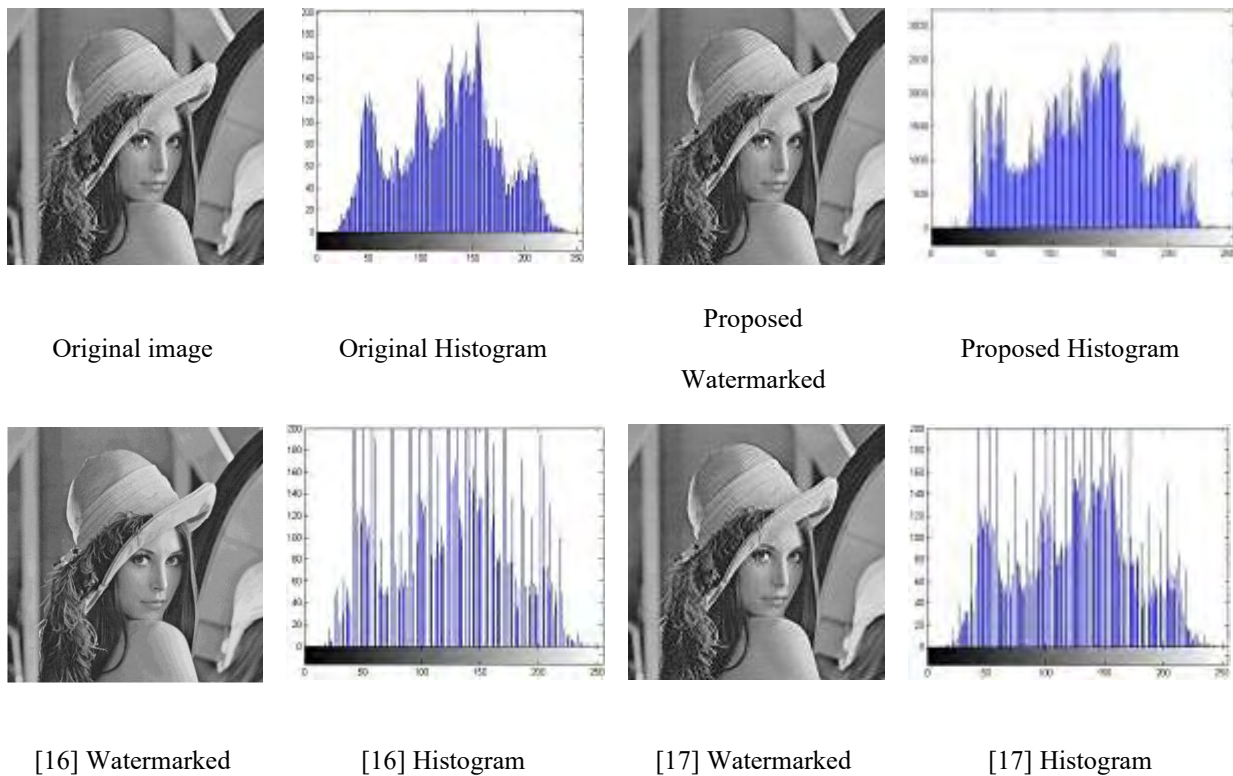


Fig. 3.2: The original image, watermarked images, and their histograms.

Table 3.1: MLC analysis of original and watermarked image of Lena with different S-boxes.

MLC	Entropy	Contrast	Correlation	Energy	Homogeneity
Original Image	7.4881	0.8650	0.8163	0.0948	0.8110
Proposed Watermarked	7.4682	0.8550	0.8362	0.0903	0.8230
Watermarked Image [16]	7.0014	0.7145	0.6591	0.0722	0.8152
Watermarked Image [17]	7.3244	0.8145	0.8115	0.0837	0.8112

3.6 Image Encryption of IP-loop based S-boxes

In [30] Shah et al. (2011) have given a majority logic criterion (MLC). MLC analysis measures the suitability of S-box in the encryption process. In MLC, statistical analysis is performed on plain and encrypted data. MLC is very useful for studying statistical prospects such as encryption methods, data manipulation, changes, etc. MLC defines an evaluation standard for evaluating the results of various statistical analyses, such as energy, homogeneity, correlation, entropy, contrast and the last one is absolute average deviation.

3.6.1 Homogeneity

The data image has a natural distortion having a relation to that image contents. The analysis of homogeneity measures the nearness of elements distribution in Grey-level co-occurrence matrix (GLCM) to GLCM diagonal. This process is called a spatial Gray tone-dependent matrix. The further extension of this process should be done from GLCM in process entries. The mathematical form of homogeneity is as follows:

$$H = \sum_k \sum_l \frac{\eta(k,l)}{1+|k-l|} \quad (3.1)$$

Here k, l presents the pixels in image, and η is the presentation of several GLCM matrices [30].

3.6.2 Energy

For the calculation of encrypted image, energy analysis should be used. In this process GLCM is used, square elements sum in GLCM is termed as energy. The mathematical formulation of energy analysis is given as:

$$E = \sum_k \sum_l \eta^2(k, l) \quad (3.2)$$

For constant images, it should be 1.

3.6.3 Correlation

In this analysis three different types are involved: horizontal, vertical, and diagonal. For the partial regions' analysis, the whole image includes in the process. It measures the neighbor correlation pixels with the attention of the whole image texture. Its mathematical form is given as:

$$K = \sum_{k,l} \frac{(k-\pi k)(l-\pi l)\eta(k,l)}{\rho_k \rho_l} \quad (3.3)$$

3.6.4 Contrast

The contrast value allows the viewer to detect the hidden object in the image. An amount of level contrast in an image steeps the artifacts which allow identification of the image clearly. When the image passes through encryption the level of randomness increased, which results in the increment of high contrast value. Due to the substitution of non-linear mappings the objects present in the image are completely distorted. The whole reading concludes that the high level of contrast in encrypted image depicts strong encryption power. In mathematical form, contrast is defined as:

$$\hat{C} = \sum_k \sum_l (k - l)^2 \eta(k, l) \quad (3.4)$$

3.6.5 Entropy

The measured amount of randomness can be evaluated by entropy. The high amount of randomness cause difficulty in detection of image [25]. The non-linear part of the S-box increased the amount of randomness of image, its mathematical representation is as follows:

$$\hat{E} = \sum_{k=0}^n \Omega(u_k) \log_a \Omega(u_k) \quad (3.5)$$

Where u_k is signification of histogram calculations.

Table 3.2 and Table 3.3 shows that the MLC of 4×4 S-box proposed by IP-loop is comparable to the S-boxes constructed by Galois field and Galois ring. This shows that the proposed S-box satisfies all the criteria appropriate for the standard and can be used for secure communication.

Table 3.4 Shows the MLC of our 16×16 S-box over IP-loop and a comparison of results is made with others well-known standard S-boxes like AES, S_8 AES, X_{yi} and Prime is shown in Table 3.4.

The proposed S-box has better results than some of the standard S-boxes, which is observed from Table 3.4. Fig. 3.3 and Fig. 3.4 show encryption of Lena image with our proposed S-boxes and comparable with different S-boxes and corresponding Histogram, respectively.

Table 3.2: MLC of LSB's of Lena grey 512×512 image by S-boxes over IP-loop, $GF(2^4)$ and $GR(4,4)$

MLC	Contrast	Correlation	Energy	Homogeneity	Entropy
MSB Image					
Plain image	0.2293	0.9502	0.1316	0.9055	7.4455
IP-loop	2.2665	0.9788	0.1632	0.9178	5.8599
S-box					
S-box	0.2491	0.9778	0.1689	0.9181	5.9698
on $GF(2^4)$					
S-box on	3.322085	0.087904	0.024477	0.483523	4.73018
$GR(4,4)$					

Table 3.3: MLC of MSB's of Lena grey 512×512 image by S-boxes over IP-loop, $GF(2^4)$ and $GR(4,4)$

MLC→ MSB Image↓	Contrast	Correlation	Energy	Homogeneity	Entropy
Plain image	0.2293	0.9502	0.1316	0.9055	7.4455
IP-loop S-box	2.5615	0.7980	0.1670	0.8230	5.8582
S-box on $GF(2^4)$	1.6909	0.8864	0.1887	0.8477	5.7457
S-box on $GR(4,4)$	2.0590	0.7962	0.3258	0.8729	5.0659

Table 3.4: Statistical analysis results used by MLC of 16×16 S-box.

S-boxes	Entropy	Contrast	Correlation	Energy	Homogeneity	MAD
Proposed	7.9633	8.5969	0.0019	0.0174	0.4070	38.5638
Ref [25]	7.7301	7.3220	0.0879	0.0244	0.4835	36.3631
Ref [30]	7.7094	8.1685	0.2309	0.0227	0.4870	43.5660
Ref [46]	7.6595	6.3683	0.0996	0.0260	0.4984	36.3082
Ref [51]	7.6850	7.0652	0.1384	0.0310	0.4928	27.4974

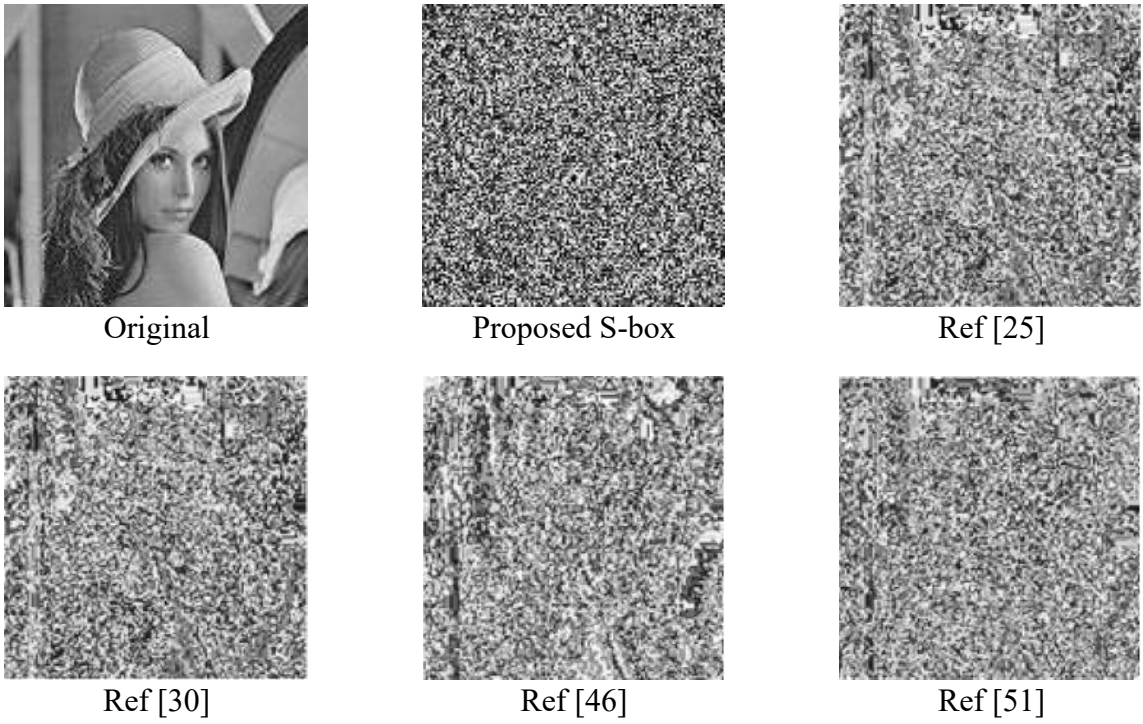


Fig. 3.3: Plain image and encrypted image by using various S-boxes.

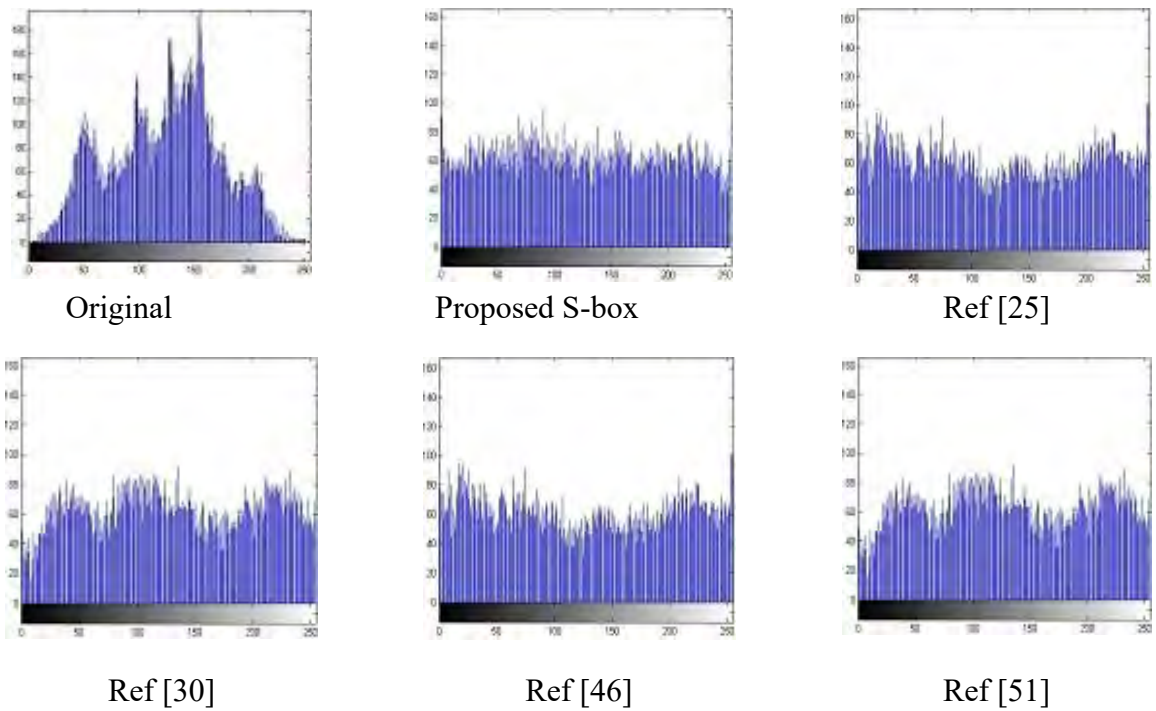


Fig. 3.4: Histogram of the corresponding images in Fig. 3.3

Chapter 4

IP-loops Modifying AES

This chapter is described as follows: Section 1, presents an introduction. Section 2 offers the design of $n \times n$ proposed S-boxes. The detailed encryption scheme of the proposed model is discussed in section 3, while section 4 presents the decryption model of the proposed scheme. The key schedule for the new model is presented in section 5 and in section 6 cipher example this new model is discussed.

4.1 Introduction

Communication over the globe is becoming a basic need of populaces. Fast-growing technological-based soft computing devices for this purpose are being invented by various companies in a bulk quantity every passing day. A variety of messages in terms of pictures, notifications of civil governments, secret and confidential military movement information, and medical reports are transported by individuals as well as organizations via electronic media. The ultimate loss and theft of valuable data are causing serious concern among populaces.

Secure communication has attracted many research centres including the national institute of standards NIST and military cyber units etc. to intervene in this grim matter. This journey is not very old as it started in the late sixty's. Many recent developments in this field include various encryption standards. Several encryption standards like data encryption standard DES [15], triple DES [69] and advanced encryption standard AES [70]. Among them, AES is the most secure until now.

The construction of the nonlinear component of block cipher also known as S-box in AES is based on extended binary Galois field. This section produces confusion in the cryptosystem. It is one of the desired attributes declared by the theory of Shannon [71], whereas the second one is diffusion which is achieved via column mixing, repetition of rounds, and permutation. These two are used to gauge the strength of a cipher. Keeping this analogy, many recent developments have been published for the design of the S-box [72-75].

4.2 Design for $n \times n$ S-boxes

The S-boxes are the basic building blocks in private key cryptosystems. All the symmetric key cryptosystems use the process of S-boxes to create confusion in the algorithm. As a result, several methods are appeared to design S-box. For this purpose, cryptographers use different algebraic structures and try to increase the security of these S-box. So, Binary Galois Field Extension $GF(2^8)$, Local associative Algebras, Pseudo-Random Number Generators (PRNG), and Elliptic curves have been used to construct S-box. Here an S-box is constructed over the IP-loop. Following transformations have been used in the design of S-box.

- 1- Inversion map: Inverts the elements of IP-loop by using the mapping, $\sigma: L \rightarrow L$ as:

$$\sigma(x) = x^{-1}, \quad \forall x \in L \quad (4.1)$$

- 2- Right Translation map: Operate right translation map with a fixed element of the loop to inverse generating in 1st step by mapping, $\varphi_u : L \rightarrow L$ as:

$$\varphi_u(x) = (u * x) \oplus v, \quad x \in L \quad (4.2)$$

where u, v are fixed elements of L .

- 3- Compose both mappings $\varphi_u \sigma : L \rightarrow L$ as:

$$\varphi_u(\sigma(x)) = (u * x^{-1}) \oplus v \quad (4.3)$$

The 1st step inverts the elements of L and 2nd step perform the left translation with XOR of the fixed element of L . The composition of these two steps gives us the elements of the required S-box. We can produce a variety of S-boxes by changing the values of elements $u, v \in L$. Table 4.1 gives the IP-loop of order 16. This is a non-associative Loop in which the inverse of zero element is itself.

Table 4.1: IP-loop of order 16.

*	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	2	3	0	7	10	13	12	14	6	15	8	4	9	11	5
2	2	3	0	1	14	8	11	15	5	10	9	6	13	12	4	7
3	3	0	1	2	12	15	9	4	11	13	5	14	7	6	8	10
4	4	7	11	15	5	6	0	14	10	3	1	13	9	8	2	12
5	5	13	8	12	6	0	4	11	2	15	14	7	3	1	10	9
6	6	10	14	9	0	4	5	1	13	12	8	2	15	11	7	3
7	7	15	12	4	10	13	1	8	9	0	3	5	14	2	6	11
8	8	11	5	14	15	2	12	9	0	7	13	1	6	10	3	4
9	9	6	13	10	3	11	14	0	7	8	4	15	2	5	12	1
10	10	9	15	6	13	1	7	2	4	14	11	12	0	3	5	8
11	11	14	4	8	2	9	15	13	3	5	12	0	10	7	1	6
12	12	5	7	13	8	14	3	6	15	1	0	10	11	4	9	2
13	13	12	9	5	1	7	10	3	6	11	2	4	8	14	15	0
14	14	8	6	11	9	12	2	10	1	4	7	3	5	15	0	13
15	15	4	10	7	11	3	8	5	12	2	6	9	1	0	13	14

The mapping to construct elements of the S-box is given by the following equation.

$$\varphi_u(\sigma(x)) = 7 * (x)^{-1} \oplus 11 \quad (4.4)$$

Table 4.2: Construction of proposed S-box over L_{16} .

L_{16}	$\varphi_u(\sigma(x)) = 7 * (x)^{-1} \oplus 11$	Entries of Proposed S-box
0	$\varphi_u(\sigma(0)) = 7 * (0)^{-1} \oplus 11$	12
1	$\varphi_u(\sigma(1)) = 7 * (1)^{-1} \oplus 11$	15
.	.	.
.	.	.
.	.	.
14	$\varphi_u(\sigma(14)) = 7 * (14)^{-1} \oplus 11$	13
15	$\varphi_u(\sigma(15)) = 7 * (15)^{-1} \oplus 11$	9

The generated S-box over L_{16} is given by the following table.

Table 4.3: Proposed S-box in the form of 4×4 matrix.

12	15	7	4
10	6	1	11
2	3	5	14
8	0	13	9

In the same way, the S-box used in the AES algorithm can be generated from the non-associative IP-loop of order 256. Here we construct the S-box by fixing the elements $231, 181 \in L$.

The composition map is given by the equation:

$$\varphi_{231}(\sigma(x)) = (231 * x^{-1}) \oplus 181 \quad (4.5)$$

The process is given as follows:

Table 4.4: Construction of proposed S-box over L_{256} .

L_{256}	$\varphi_{231}(\sigma(x)) = (231 * x^{-1}) \oplus 181$	<i>Proposed S – box</i>
0	$\varphi_{231}(\sigma(0)) = (231 * 0^{-1}) \oplus 181$	147
1	$\varphi_{231}(\sigma(1)) = (231 * 1^{-1}) \oplus 181$	71
2	$\varphi_{231}(\sigma(2)) = (231 * 2^{-1}) \oplus 181$	1
.	.	.
.	.	.
.	.	.
254	$\varphi_{231}(\sigma(254)) = (231 * 254^{-1}) \oplus 181$	117
255	$\varphi_{231}(\sigma(255)) = (231 * 254^{-1}) \oplus 181$	121

Table 4.5: Proposed S-box in the form of 16×16 matrix.

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

20	134	63	177	230	226	240	241	227	3	231	143	181	211	234	201
250	109	116	33	243	178	180	106	66	127	212	255	232	126	117	121

Similarly, we construct the bulk of S-boxes by using different values of $u, v \in L$.

4.3 Description of Encryption Algorithm

In this cipher, the encryption scheme consists of 10 iterative rounds. The input of 128-bits is taken as a state array. Before the start of 1st round, the encipher key is operated which was initially selected to encrypt data, and then the round function is performed. In this cipher, the round function consists of 10 rounds. The final round is slightly different from others. After doing all of these rounds the result is output. Each round is performed with different keys which are generated in a key schedule by using the initial encipher key. The encryption scheme uses the following transformation for encryption.

SubBytes (), ShiftRows (), MixColumns (), RoundKeyBinding (). In 10th round, the MixColumn () operation is not performed.

4.3.1 SubBytes () Transformation:

In this transformation, the bytes of state are substituted with bytes of S-box (The process of S-box designing is given above). It is a non-linear step. i.e. for the bytes k_i and k_j of the state $SubByte(k_i) * SubByte(k_j) \neq SubByte(k_i * k_j)$. In this transformation, an invertible S-box is used. The SubBytes () transformation is bijective. Each element of loop L is mapped onto some element of loop L . So, each element of loop L can be inverted in the decryption process.

For example, the byte of a state i.e. $k_i = (65)_{16}$ can be substituted by using S-box in Table 4.3 as:

$$S((65)_{16}) = (54)_{16}$$

S-box has no fixed points i.e. there is no byte in L such that $S(k_i) = k_i$. Even the identity element of loop L is substituted to some element of L , other than the identity element.

$$S((0)_{16}) = (147)_{16}$$

4.3.2 ShiftRows () Transformation

In the process of the ShiftRows (), there is a byte shift that is cyclic across the rows of state. 1st row will be unchanged. The ShiftRows () transformation is given as follows:

$$j_{r,c}^* = j_{r,(c+shift(r,Nb))\text{mod}Nb}, \quad 0 \leq r < 4, \quad 0 \leq c < Nb \quad (4.6)$$

Here $Nb = 4$ and r show the row number which decides $shift(r, Nb)$ (shift value). Shift value is given by.

$$shift(1, 4) = 1; \quad shift(2, 4) = 2; \quad shift(3, 4) = 3;$$

ShiftRows () operation rotates the bytes of rows towards the right according to the rule given above. In this operation, Row n is moved n rounds right. So, every new column which is generated after this operation is created with bytes from all columns of state. This transformation keeps the columns away from linear independence. The ShiftRows () transformation weakens the division of cipher into four independent block ciphers.

4.3.3 MixColumns () Transformation

It is a column-wise transformation. This transformation is performed with the help of disassociative property of the IP-loop. We have divided this transformation into further three sub-transformations. In the sub-transformation, two bytes of a column are mixed at a time. Mathematically the transformations are given as follows:

$$l_{r,c}^2 * l_{r+1,c} = l_{r,c}^* \quad (4.7)$$

$$l_{r,c} * l_{r+1,c}^2 = l_{r+1,c}^* \quad (4.8)$$

By using the above transformations, the 1st Sub-transformation is given in following Fig.

$l_{0,0}$	$l_{0,1}$	$l_{0,2}$	$l_{0,3}$	$l_{0,0}^2 * l_{1,0}$	$l_{0,1}^2 * l_{1,1}$	$l_{0,2}^2 * l_{1,2}$	$l_{0,3}^2 * l_{1,3}$
$l_{1,0}$	$l_{1,1}$	$l_{1,2}$	$l_{1,3}$	$l_{0,0} * l_{1,0}^2$	$l_{0,1} * l_{1,1}^2$	$l_{0,2} * l_{1,2}^2$	$l_{0,3} * l_{1,3}^2$
$l_{2,0}$	$l_{2,1}$	$l_{2,2}$	$l_{2,3}$	$l_{2,0}^2 * l_{3,0}$	$l_{2,1}^2 * l_{3,1}$	$l_{2,2}^2 * l_{3,2}$	$l_{2,3}^2 * l_{3,3}$
$l_{3,0}$	$l_{3,1}$	$l_{3,2}$	$l_{3,3}$	$l_{2,0} * l_{3,0}^2$	$l_{2,1} * l_{3,1}^2$	$l_{2,2} * l_{3,2}^2$	$l_{2,3} * l_{3,3}^2$

Fig. 4.1: MixColumns () 1st Sub operation

The 2nd Sub-transformation is given in following Fig.4.1. In this transformation we let

$$l_{i,j}^2 * l_{h,k} = m_{i,k} \quad (4.9)$$

$m_{0,0}$	$m_{0,1}$	$m_{0,2}$	$m_{0,3}$	$m_{0,0}^2 * m_{2,0}$	$m_{0,1}^2 * m_{2,1}$	$m_{0,2}^2 * m_{2,2}$	$m_{0,3}^2 * m_{2,3}$
$m_{1,0}$	$m_{1,1}$	$m_{1,2}$	$m_{1,3}$	$m_{1,0}^2 * m_{3,0}$	$m_{1,1}^2 * m_{3,1}$	$m_{1,2}^2 * m_{3,2}$	$m_{1,3}^2 * m_{3,3}$
$m_{2,0}$	$m_{2,1}$	$m_{2,2}$	$m_{2,3}$	$m_{0,0} * m_{2,0}^2$	$m_{0,1} * m_{2,1}^2$	$m_{0,2} * m_{2,2}^2$	$m_{0,3} * m_{2,3}^2$
$m_{3,0}$	$m_{3,1}$	$m_{3,2}$	$m_{3,3}$	$m_{1,0} * m_{3,0}^2$	$m_{1,1} * m_{3,1}^2$	$m_{1,2} * m_{3,2}^2$	$m_{1,3} * m_{3,3}^2$

Fig. 4.2: MixColumns () 2nd Sub Operation

The 3rd Sub-transformation is given in the following Fig.4.2. In this transformation we let

$$m_{i,j}^2 * m_{h,k} = n_{i,k} \quad (4.10)$$

$n_{0,0}$	$n_{0,1}$	$n_{0,2}$	$n_{0,3}$	$n_{0,0}^2 * n_{3,0}$	$n_{0,1}^2 * n_{3,1}$	$n_{0,2}^2 * n_{3,2}$	$n_{0,3}^2 * n_{3,3}$
$n_{1,0}$	$n_{1,1}$	$n_{1,2}$	$n_{1,3}$	$n_{1,0}^2 * n_{2,0}$	$n_{1,1}^2 * n_{2,1}$	$n_{1,2}^2 * n_{2,2}$	$n_{1,3}^2 * n_{2,3}$
$n_{2,0}$	$n_{2,1}$	$n_{2,2}$	$n_{2,3}$	$n_{1,0} * n_{2,0}^2$	$n_{1,1} * n_{2,1}^2$	$n_{1,2} * n_{2,2}^2$	$n_{1,3} * n_{2,3}^2$
$n_{3,0}$	$n_{3,1}$	$n_{3,2}$	$n_{3,3}$	$n_{0,0} * n_{3,0}^2$	$n_{0,1} * n_{3,1}^2$	$n_{0,2} * n_{3,2}^2$	$n_{0,3} * n_{3,3}^2$

Fig. 4.3: MixColumns () 3rd Sub Operation

This transformation operates on four bytes as input and the resulting output is also four bytes and uses an invertible linear transformation. In this transformation, each input byte modifies the four

bytes of output. ShiftRows () and MixColumns () transformations combined provide diffusion in the cipher.

4.3.4 Round Key Binding () Transformation

Round Key Binding () transformation is the loop operation in which the bytes of state matrix are combined with bytes of the key. If $k_i, 0 \leq i < 16$ are key bytes and $s_i, 0 \leq i < 16$ are the state byte. Round Key Binding () transformation is as follows:

$$R_{k_i}(s_i) = k_i * s_i \quad (4.11)$$

Each Round Key consists of 4 words. In each round, different keys are used which is constructed by the process of Key Schedule. 4 words of round key and the columns of state combined as follows:

$$[l_{0,c}^*, l_{1,c}^*, l_{2,c}^*, l_{3,c}^*] = [w_{round * Nb + c}] * [l_{0,c}, l_{1,c}, l_{2,c}, l_{3,c}] \quad 0 \leq c < 4$$

Here, keywords are denoted by $[w_i]$ and number of *round* is in the range $0 \leq round \leq Nr$. Before the start of the round function, the initial key is added where $round = 0$. In all rounds, the round keys are added where $1 \leq round \leq Nr$ and $l = round * Nb$.

4.4 Inverse Cipher

All the transformations used above are invertible and one can easily find the plaintext from the ciphertext applying the inverse process. The inverse cipher or Decryption cipher of the encryption algorithm consists of the following transformations InvShiftRows (), InvSubBytes (), InvMixColumns () and InvRoundkeyBinding (). These transformations are explained in the following paragraphs.

4.4.1 InvShiftRows () Transformation

The inverse process of ShiftRows () is the InvShiftRows () transformation. In this transformation, the bytes of the state are rotated left cyclically according to the rule except for the 1st row. 1st row

$r = 0$ will be unchanged. The rotation of bytes of the following rows are given by $Nb - shift(r, Nb)$ and $shift(r, Nb)$ depends upon the row numbers as follows:

$$shift(1, 4) = 1; \quad shift(2, 4) = 2; \quad shift(3, 4) = 3;$$

4.4.2 InvSubBytes () Transformation

InvSubBytes () operation is the inverse process of the SubBytes () transformation, in which the bytes of the state are updated from the bytes of the inverse S-box. The process of constructing the inverse S-box is the same as constructing S-box by using the inverse map. First applying the inverse of the linear map and then apply the inversion map for the construction of the inverse S-box.

$$\left(\varphi_u(\sigma(x))\right)^{-1} = \sigma^{-1}(\varphi_u^{-1}(x)) = (u^{-1} * (x \oplus v))^{-1} \quad (4.12)$$

Where $u, v \in L$ are the fixed elements of IP-loop which are used for the construction of the S-box.

As $u, v \in L$ are the fixed elements of IP-loop. So the used structure of IP-loop is known by the authorized person at the decryption end and he can easily find the inverse of u and then find the inverse S-box for decryption.

In the S-box, we have constructed in Sub bytes (), $u = 231$ and $v = 181$ used as fixed elements of IP-loop. The inverse of 231 is 141 in IP-loop we have used. So, the inverse mapping for the construction of inverse S-box in InvSubBytes () step is given by:

$$\sigma^{-1}(\varphi_u^{-1}(x)) = (231^{-1} * (x \oplus 181))^{-1} = (141 * (x \oplus 181))^{-1}$$

The inverse S-box is given in the following table.

Table 4.6: Proposed inverse S-box in the form of 16×16 matrix.

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

4.4.3 InvMixColumns () Transformation

InvMixColumns () is inverse process of MixColumns () operation. This transformation applies on the state in column-wise manner. The MixColumn () transformations are given by:

$$l_{r,c}^2 * l_{r+1,c} = l_{r,c}^* \quad (4.13)$$

$$l_{r,c} * l_{r+1,c}^2 = l_{r+1,c}^* \quad (4.14)$$

Here, $l_{r,c}^*$, $l_{r+1,c}^2$ are the output values. By using the power-associativity and di-associativity of the IP-loop, the inverse of MixColumn () transformation can be easily done, which is described as follows:

From Eq. (4.13), we can get.

$$l_{r,c} = l_{r+1,c}^* * (l_{r+1,c}^{-1})^2 \quad (4.15)$$

By using this value Eq. (4.14), we get.

$$\begin{aligned} (l_{r+1,c}^* * (l_{r+1,c}^{-1})^2)^2 * l_{r+1,c} &= l_{r,c}^* \\ (l_{r+1,c}^*)^2 * (l_{r+1,c}^{-1})^4 * l_{r+1,c} &= l_{r,c}^* \\ (l_{r+1,c})^3 &= (l_{r+1,c}^*)^2 * (l_{r,c}^*)^{-1} \\ l_{r+1,c} &= \left((l_{r+1,c}^*)^2 * (l_{r,c}^*)^{-1} \right)^{1/3} \\ l_{r,c} * \left(\left((l_{r+1,c}^*)^2 * (l_{r,c}^*)^{-1} \right)^{1/3} \right)^2 &= l_{r+1,c}^* \\ l_{r,c} &= l_{r+1,c}^* * \left(\left(l_{r,c}^* * \left((l_{r+1,c}^*)^2 \right)^{-1} \right)^{1/3} \right)^2 \end{aligned} \quad (4.16)$$

4.4.4 InvRoundKeyBinding () Transformation

The inverse process of RoundKeyBinding () transformation is called InvRoundKeyBinding () transformation. This transformation is also a loop operation in which the state matrix bytes are combined with inverses key bytes. If k_i , $0 \leq i < 16$ are key bytes and s_i , $0 \leq i < 16$ are state bytes. InvRoundKeyBinding () transformation is given as follows:

$$R_{k_i^{-1}}(s_i) = k_i^{-1} * s_i \quad (4.17)$$

4 inverse round keywords are combined with state columns as follows:

$$[l_{0,c}^*, l_{1,c}^*, l_{2,c}^*, l_{3,c}^*] = [w_{round * Nb + c}]^{-1} * [l_{0,c}, l_{1,c}, l_{2,c}, l_{3,c}] \quad 0 \leq c < 4$$

Here, keywords are denoted by $[w_i]$ and the number of *round* is in the range $0 \leq round \leq Nr$.

4.5 Key Schedule

In the Encryption algorithm, a 128-bit key is used, which is combined with the state in each round as there are 10 rounds in the cipher and key ties with state 10 times in each encryption process. It

is a detriment to tie the same key in each round. Some transformations are applied on the key to making nonlinearity in key to use it in different rounds. This process of key transformation is known as the Key Schedule. Here, we discuss the expansion of cipher key K of length 128-bits and generates 11 subkeys (one initial key and 10 new subkeys), one key (initial key) is for key whitening used before the start of the round function, and the remaining 10 subkeys for 10 rounds.

The algorithm takes the cipher key K as input and breaks it in four blocks or rows of 16 bytes, called words $w [\]$. Then apply the transformations known as WordRotation (), SubWord (), and RoundConstantBinding[i] and generates 44 words denoted by $w[0], w[1], \dots, w[42], w[43]$. The bytes of the initial key are $k_0, k_1, k_2, \dots, k_{15}$. Where K_0 is the original key selected for the encryption. The bytes of this key generated the first four elements of the key array w . The other elements of array can be computed as follows:

It is clear from Fig. that the first word of the subkey $w[4i]$, $i = 1, 2, 3, \dots, 10$. Is computed as follows:

$$w[4i] = w[4(i - 1)] * g(w[4i - 1]) \quad (4.18)$$

Here $w()$ is a linear function. It takes four bytes as input and output are also four bytes. A recursive process is used to construct the other three words of the subkey.

$$w[4i + j] = w[4(i - 1)] * w[4i - 1 + j] , \quad i = 1, 2, \dots, 10 , \quad j = 1, 2, 3$$

The function $g()$ consists of the 3 operations SubWord (), WordRotation () and RoundConstantBinding[i].

Subword () is an operation in which the input word consists of four bytes and manipulates each of these bytes from the S-box and produces a four-byte output word.

WordRotation () operation takes a four-byte input word i.e. $[a_0, a_1, a_2, a_3]$ and applies a cyclic permutation on the bytes of the word, and produces a four-byte output word i.e. $[a_1, a_2, a_3, a_0]$.

RoundconstantBinding[i] operation consists of around constant word array $\{\{ii\}, \{00\}, \{00\}, \{00\}\}$ where $\{ii\}$ is an element of L and apply as Right translation to the 1st byte of the word $w[4i]$. The values of round coefficient $\{ii\}$ for the subkeys of the different rounds of the are given by:

$$RoundConstantTie[1] = (11)_{16}$$

$$RoundConstantTie[2] = (22)_{16}$$

$$RoundConstantTie[3] = (33)_{16}$$

⋮

$$RoundConstantTie[10] = (AA)_{16}$$

This function $w(\)$ is used for two purposes:

- 1- To add the nonlinearity in the Key Schedule.
- 2- To remove the symmetry in the AES.

4.5.1 Inverse Key Schedule

Inverse Key Schedule is the inverse process of Key Schedule. All the transformations in Key Schedule are invertible and easily inverted by using inverse mappings. The inverse process of Word Rotation () is the same as an inversion of the SubBytes () step as explained in the previous section. The inverse of the SubWord () step is also the same as the inverse of the SubBytes () step is explained in the previous section.

The operation of Binding Round Constant () is invertible. Let $y = \{ii\}$ is the round constant and operated to the 1st-byte x of the word $w[4i]$ and the new byte generated is z and given by:

$$z = y * x$$

Since y is the element of L and L is IP-loop. So, its inverse is also an element of IP-loop L . i.e. $y^{-1} \in L$. The inverse mapping is given by:

$$y^{-1} * z = y^{-1} * (y * x)$$

$$x = y^{-1} * z \quad (4.19)$$

Here, y is the round constant and z is the output byte, both are known by the person at the decryption end. So, he can easily find the original byte by the process mentioned above.

4.5.2 Security Analyses of Proposed Encryption Algorithm

All the cryptographic primitives are used for the sack of information security. With the modern advancement in cryptanalysis techniques and computation speeds, the security of many cryptosystems is compromised. So, the cryptographers are working to construct new secure cryptographic primitives and improving the structures of the existing cryptographic primitives to meet the security needs of this era. Therefore, new techniques are applied in this field such as the arrival of quantum cryptography. In quantum cryptography, quantum bits are used, whose values are not restricted at 0 and 1 but can be varied between 0 and 1. This is the most advanced form of cryptography and many cryptographers are working in this field. Some new foundations are also introduced in modern cryptography.

In this chapter, we have presented a new scheme for encryption in the symmetric key cryptosystem. This new scheme worked on the lines of the Rijndael Algorithm (AES) but was based on a different algebraic structure. It also uses a key of length 128-bits and encrypts a 128-bit block of data at a time. The encryption scheme consists of 10 rounds as AES. Each round contains the four components SubBytes () Transformation, ShiftRows () Transformation, MixColumns () Transformation and RoundKeyBinding () Transformation. 10 different subkeys are generated by a Key Schedule to use in each round of round function. Therefore, as for the internal structure of this scheme, it has the same security parameters as in AES. But in this cipher, we have used a different algebraic structure known as Non-associative IP-loop of order 256 instead of the Galois field $GF2^8$. Which makes it different from AES and in some prospectus more secure. In the complete cipher scheme, we have used the binary operation, from which the

Non-associative IP-loop is formed, Binary multiplication under modulo primitive irreducible polynomial.

Table 4.7: Comparison of no. of binary Galois fields and non-associative IP-loop.

<i>n</i>	8	16	32	64	128	256
<i>M(n)</i>	0	5	71	4262	?	?
<i>GF(n)</i>	1	1	3	3	9	8

The main points of the new algorithm are:

- 1- This algorithm also uses the key of 128 bits which is enough secure under the brute force attack due to the large key space of 2^{128} .
- 2- It is a simple and flexible cipher with good performance.
- 3- The cipher is designed expecting to protect against known attacks and with conservative design.
- 4- The new cipher does not have only 128 bits key. But the loop of order 256 is also used as a key. Because without any knowledge of Loop used in Cipher, No one can decipher the text even if he knows a key.
- 5- In AES, we have only limited structures of Binary Galois Field of order 256. But in this cipher, we have used IP-loop of order 256, of which we have a large number of Moufang loops of order 256.
- 6- Since in this cipher, the binary operation depends upon the Loop, which is used in our encryption scheme. This loop is non-commutative, in which the same numbers operated in different ways can give us different results. So, it is also difficult to get any information from the energy consumed in this operation.
- 7- This study will bring the cryptographers toward the algebraic structures other than Binary Galois Field and diversify the basis of the symmetric cryptography from the Binary Galois Field.

8- This study will also boost up the research in the Non-associative Algebraic Structures and their uses in different scientific and technology areas.

4.6 Cipher Example

The following diagram shows the values in the State array as the Cipher progresses for a block length and a Cipher Key length of 16 bytes each (i.e., $Nb = 4$ and $Nk = 4$).

Input = Logical Thoughts

In Hexadecimal form: 76 111 67 69 63 61 108 20 54 68 111 75 67 68 74 73

Cipher Key = Pure Mathematics

In Hexadecimal form: 50 75 72 65 20 77 61 74 68 65 109 61 74 69 63 73

The values of round keys are taken from the Round Key Schedule Given in the previous section.

Legend for Cipher (Encrypt)

Input: Cipher Input

s_box: State after SubBytes ()

s_row: State after ShiftRows ()

m_col: State after MixColumns ()

rk_bd: State after RoundKeyBinding ()

output: Cipher Output

AES-128($Nk=4, Nr=10$)

```

Logical Thoughts
Pure Mathematics
Round 0
input[76, 111, 103, 105, 99, 97, 108, 32, 84, 104, 111, 117, 103, 104, 116, 115]
k_sch[80, 117, 114, 101, 32, 77, 97, 116, 104, 101, 109, 97, 116, 105, 99, 115]
rk_bd[16, 48, 65, 26, 71, 126, 81, 56, 88, 25, 0, 66, 39, 1, 67, 22]
Round1
s_box[209, 1, 90, 114, 162, 134, 154, 118, 238, 26, 141, 30, 206, 173, 70, 213]
s_row[209, 1, 90, 114, 134, 154, 118, 162, 141, 30, 238, 26, 213, 206, 173, 70]
m_col[209, 1, 90, 114, 134, 154, 118, 162, 141, 30, 238, 26, 213, 206, 173, 70]

```

```
k_sch[23, 186, 163, 47, 87, 163, 200, 111, 123, 156, 185, 116, 27, 173, 216, 91]
rk_bd[208, 31, 80, 57, 84, 15, 216, 187, 113, 202, 94, 175, 137, 135, 246, 29]
Round2
s_box[239, 197, 210, 74, 117, 77, 124, 227, 193, 144, 230, 163, 59, 23, 180, 217]
s_row[239, 197, 210, 74, 77, 124, 227, 117, 230, 163, 193, 144, 217, 59, 23, 180]
m_col[239, 197, 210, 74, 77, 124, 227, 117, 230, 163, 193, 144, 217, 59, 23, 180]
k_sch[255, 242, 45, 81, 250, 97, 213, 96, 149, 253, 118, 64, 240, 30, 242, 39]
rk_bd[22, 119, 249, 52, 31, 92, 60, 82, 96, 9, 31, 189, 249, 90, 110, 163]
Round3
s_box[213, 78, 192, 129, 197, 254, 109, 242, 137, 46, 197, 91, 192, 158, 38, 204]
s_row[213, 78, 192, 129, 254, 109, 242, 197, 197, 91, 137, 46, 204, 192, 158, 38]
m_col[213, 78, 192, 129, 254, 109, 242, 197, 197, 91, 137, 46, 204, 192, 158, 38]
k_sch[69, 65, 239, 176, 247, 78, 88, 128, 116, 227, 74, 236, 248, 237, 148, 251]
rk_bd[176, 173, 54, 80, 149, 174, 1, 195, 222, 79, 170, 30, 119, 124, 134, 141]
Round4
s_box[12, 223, 181, 210, 251, 167, 173, 96, 39, 226, 156, 157, 78, 142, 19, 67]
s_row[12, 223, 181, 210, 167, 173, 96, 251, 156, 157, 39, 226, 67, 78, 142, 19]
m_col[12, 223, 181, 210, 167, 173, 96, 251, 156, 157, 39, 226, 67, 78, 142, 19]
k_sch[190, 132, 31, 116, 29, 182, 75, 204, 17, 93, 21, 44, 221, 162, 129, 187]
rk_bd[186, 217, 147, 191, 152, 162, 168, 65, 11, 178, 229, 74, 60, 54, 128, 91]
Round5
s_box[183, 64, 235, 71, 80, 212, 236, 90, 62, 4, 123, 146, 109, 181, 143, 198]
s_row[183, 64, 235, 71, 212, 236, 90, 80, 123, 146, 62, 4, 198, 109, 181, 143]
m_col[183, 64, 235, 71, 212, 236, 90, 80, 123, 146, 62, 4, 198, 109, 181, 143]
k_sch[63, 27, 238, 71, 116, 193, 185, 251, 81, 214, 142, 183, 198, 0, 15, 18]
rk_bd[180, 145, 167, 173, 46, 146, 57, 33, 69, 89, 63, 142, 168, 115, 130, 84]
Round6
s_box[116, 155, 151, 223, 113, 243, 74, 201, 222, 218, 69, 103, 236, 177, 135, 117]
s_row[116, 155, 151, 223, 243, 74, 201, 113, 69, 103, 222, 218, 117, 236, 177, 135]
m_col[116, 155, 151, 223, 243, 74, 201, 113, 69, 103, 222, 218, 117, 236, 177, 135]
k_sch[209, 40, 59, 175, 189, 161, 144, 102, 206, 3, 58, 189, 88, 3, 61, 151]
rk_bd[147, 69, 108, 84, 26, 93, 141, 64, 93, 128, 171, 88, 119, 168, 160, 43]
Round7
s_box[235, 222, 10, 117, 114, 194, 67, 110, 194, 143, 196, 238, 78, 236, 168, 50]
s_row[235, 222, 10, 117, 194, 67, 110, 114, 196, 238, 194, 143, 50, 78, 236, 168]
m_col[235, 222, 10, 117, 194, 67, 110, 114, 196, 238, 194, 143, 50, 78, 236, 168]
k_sch[103, 21, 134, 77, 140, 214, 34, 7, 86, 213, 28, 212, 110, 212, 117, 35]
rk_bd[154, 45, 96, 251, 96, 182, 222, 42, 120, 243, 176, 92, 58, 185, 155, 158]
Round8
s_box[112, 25, 137, 176, 137, 16, 39, 102, 9, 179, 12, 254, 18, 187, 104, 240]
s_row[112, 25, 137, 176, 16, 39, 102, 137, 12, 254, 9, 179, 240, 18, 187, 104]
m_col[112, 25, 137, 176, 16, 39, 102, 137, 12, 254, 9, 179, 240, 18, 187, 104]
k_sch[35, 91, 35, 55, 211, 193, 17, 30, 141, 122, 77, 182, 155, 238, 2, 157]
rk_bd[99, 211, 83, 57, 218, 255, 235, 55, 129, 231, 134, 251, 84, 116, 64, 108]
Round9
```



```
s_box[161, 199, 234, 74, 100, 32, 68, 225, 175, 79, 19, 176, 117, 42, 110, 10]
s_row[161, 199, 234, 74, 32, 68, 225, 100, 19, 176, 175, 79, 10, 117, 42, 110]
m_col[161, 199, 234, 74, 32, 68, 225, 100, 19, 176, 175, 79, 10, 117, 42, 110]
k_sch[160, 252, 175, 71, 103, 21, 136, 121, 148, 91,193, 139, 115, 165, 195, 104]
rk_bd[3, 206, 136, 9, 192, 28, 16, 29, 49, 135, 133, 61, 111, 227, 151, 51]
Round10
s_box[189, 84, 3, 46, 0, 237, 209, 217, 57, 23, 75, 89, 34, 107, 207, 97]
s_row[189, 84, 3, 46, 237, 209, 217, 0, 75, 89, 57, 23, 97, 34, 107, 207]
m_col[189, 84, 3, 46, 237, 209, 217, 0, 75, 89, 57, 23, 97, 34, 107, 207]
k_sch[112, 244, 173, 212, 67, 205, 1, 237, 235, 196, 194, 28, 142, 49, 17, 48]
rk_bd[199, 195, 134, 165, 95, 231, 88, 96, 38, 241, 151, 5, 230, 3, 158, 9]
```

output in string Å |ãÑ_pX` &±ùENQμETX×HT

Chapter 5

S-boxes over Power Associative Loop: A first step towards use of Non-associative Algebra

The chapter is arranged as follows: Section 1 presents an introduction; the algebraic structure of PA-loops and the construction of proposed S-boxes are discussed in section 2. In section 3, the strength of the newly proposed S-boxes is assessed and compared with other well-known S-boxes. The application of proposed S-boxes in the image encryption scheme and majority logic criterion is performed in Section 4.

5.1 Introduction

In symmetric-key cryptography, the purpose of the S-box is to create confusion and increasing the security of the whole cryptographic system. For this reason, many algebraic S-boxes are constructed on algebra associative of Galois field. The PA-loop is used for the construction of S-boxes in this chapter. Compared with cyclic groups and Galois fields, this new structure has outstanding characteristics, including the inversion of zero element, non-associativity, and fewer constraints. Compared with existing S-boxes, PA-loop based S-boxes are relatively easy to construct, and the above-mentioned properties provide many structures for the construction of highly non-linear S-boxes. The various algebraic and statistical analyses are used to evaluate the proposed S-boxes. The Proposed S-box is cryptographically stronger and can be used in various secure communication techniques.

5.2 Design of Proposed Model

In any cryptosystem, confusion can be generated with the help of different methods. However, S-box is considered the best source of confusion. In the literature, we have seen many S-boxes merely depend on the Galois field. Few structures depend upon the algebra \mathbb{Z}_2^n of n copies of the binary field \mathbb{Z}_2 . Both classes are associative and hence have limited impact as depicted in Table 5.1. Due to the property of non-associativity, the number of PA-loops is quite larger than the groups and the Galois field. It provides more choices to design a variety of S-boxes by using different structures of PA-loops [28].

Any of the cryptosystems would become more secure and able to resist malicious attacks with this diversity of S-boxes.

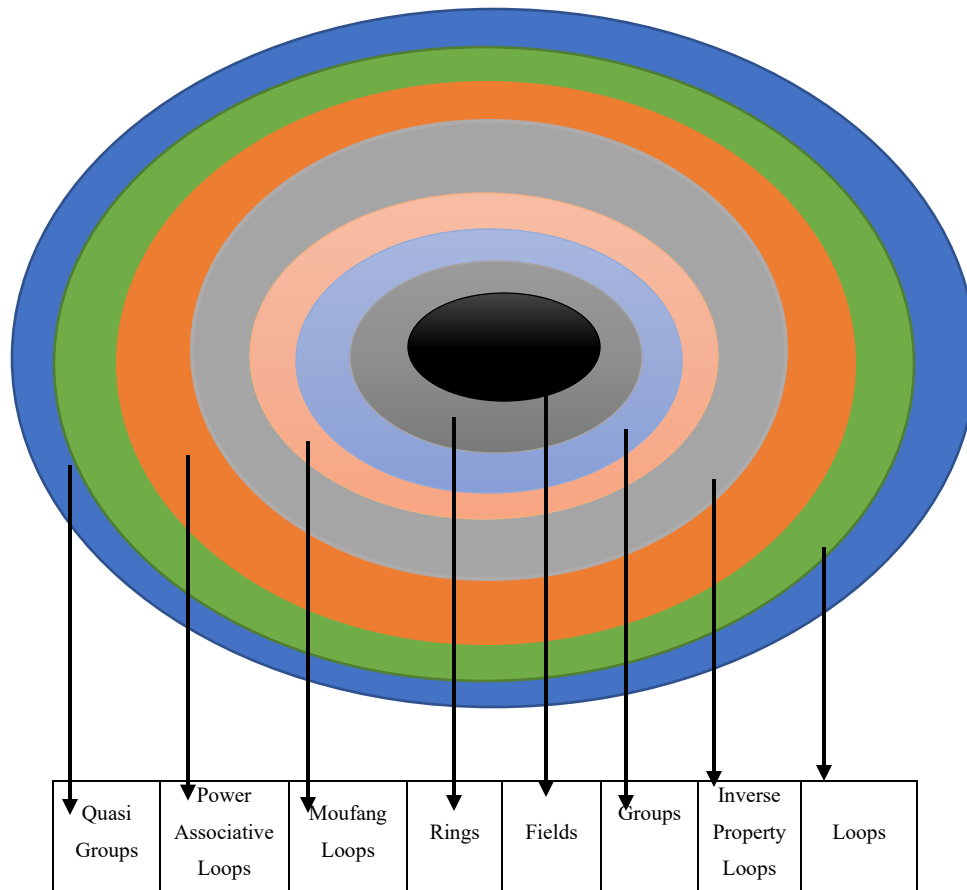


Fig. 5.1: Graphical description of associative and non-associative structures.

Table 5.1: Classification of associative and non-associative structures of order n .

n.	Loop of order n	Non-Associative Loops of order n	Groups of order n
8	11	6	5
12	8	3	5
15	3	2	1
16	2052	2038	14
18	6	1	5
20	8	3	5
21	4	2	2
24	≥ 103	≥ 88	15
27	13	8	5
28	7	3	4
30	≥ 6	≥ 2	4

The steps for the formation of S-box by using PA-loops L is defined as:

- 1) Firstly, we have to give an inversion mapping.

$$B: L \rightarrow L \text{ as } \beta(y) = y^{-1}, \text{ where } y \in L. \quad (5.1)$$

- 2) Secondly, the linear scalar multiple mapping

$$\gamma: L \rightarrow L \text{ is given by } \gamma(y) = cy \oplus d \quad (5.2)$$

where $y, c, d \in L$, and $c \neq 0, d$ are arbitrary scalars and \oplus is an XOR operation.

- 3) The composition mapping $\gamma\circ\beta: L \rightarrow L$ is obtained by $\gamma\circ\beta(y) = cy^{-1} \oplus d$.
- 4) Apply S_{16} permutation on given 4×4 and 16×16 table.

5.2.1 Symmetric Group of degree 16

Symmetric group S_{16} is a group of permutations of degree 16 which is used to create more randomness in our obtained S-boxes. It also gives us more variety of highly non-linear S-boxes by using different permutations. We got $16!$ (20922789888000) different S-boxes with the help of this permutation group. In the case of 4×4 S-box, the S_{16} permutation will be operated on all entries of the S-box. While in the case of 16×16 S-box, we have to apply the permutation on each row or column.

Now we take a PA-loops L of order 16 which is given in Table 5.2. Define a mapping $\gamma\circ\beta: L \rightarrow L$ by $\gamma\circ\beta(y) = 7y^{-1} \oplus 13$ here \oplus is an XOR of two numbers. Table 5.3 gives the mechanism for the construction of the S-box. In Fig. 5.2, the flow chart shows the construction scheme of 4×4 S-boxes. This Table also depicts different 4×4 S-boxes by applying different permutations of S_{16} . Similarly, we can construct 16×16 S-boxes over a PA-loop of order 256 as depicted in Table 5.4. We apply different permutations of order 16 like permutation-1 (1,13,5,11,9,0,3,12,7,4,15,10,6,14,8,2), permutation-2 (1,6,2,4,0,5,12,3,8,11,14,10,9)(7,15,13), permutation-3 (1,5,2,15,6,14,11,10,3,0)(4,13,8,9,12,7) on rows of 16×16 S-box as shown in Fig. 5.3 and then shift the first row into last row, second row into second last row and so on to get the permuted S-box. This used permutation is named permutation 1. Fig. 5.3 shows the flow chart and different S-boxes after applying different permutations of S_{16} .

Table 5.2: PA-loop of order 16.

*	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	0	3	2	11	6	5	8	7	12	13	4	9	10	15	14
2	2	3	4	10	6	9	0	1	12	14	7	5	15	8	11	13
3	3	2	11	13	5	12	1	0	9	15	8	6	14	7	4	10
4	4	11	6	5	0	3	2	15	14	13	12	1	10	9	8	7

5	5	6	1	9	3	10	11	4	13	7	14	2	8	15	0	12
6	6	5	0	12	2	13	4	11	10	8	15	3	7	14	1	9
7	7	8	12	0	15	11	10	13	4	5	2	14	6	3	9	1
8	8	7	9	1	14	4	13	10	11	6	3	15	5	2	12	0
9	9	12	14	15	13	7	8	5	6	0	11	10	1	4	2	3
10	10	13	7	8	12	14	15	2	3	11	0	9	4	1	5	6
11	11	4	5	6	1	2	3	14	15	10	9	0	13	12	7	8
12	12	9	15	14	10	8	7	6	5	1	4	13	0	11	3	2
13	13	10	8	7	9	15	14	3	2	4	1	12	11	0	6	5
14	14	15	13	11	8	0	9	12	1	2	5	7	3	6	10	4
15	15	14	10	4	7	1	12	9	0	3	6	8	2	5	13	11

Table 5.3: S-box over PA-loop of order 16.

y	$\gamma \circ \beta(y) = 7y^{-1} \oplus 13$	S-box
0	$7(0)^{-1} \oplus 13 = 7(0) \oplus 13$	10
1	$7(1)^{-1} \oplus 13 = 7(1) \oplus 13$	5
2	$7(2)^{-1} \oplus 13 = 7(6) \oplus 13$	7
3	$7(3)^{-1} \oplus 13 = 7(7) \oplus 13$	0
.	.	.
.	.	.
.	.	.
15	$7(15)^{-1} \oplus 13 = 7(8) \oplus 13$	9

Table 5.4: S-box over PA-loop of order 256.

y	$\gamma \circ \beta(y) = 7y^{-1} \oplus 13$	S-box
0	$7(0)^{-1} \oplus 13 = 7(0) \oplus 13$	10
1	$7(1)^{-1} \oplus 13 = 7(1) \oplus 13$	81
2	$7(2)^{-1} \oplus 13 = 7(3) \oplus 13$	32

3	$7(3)^{-1} \oplus 13 = 7(2) \oplus 13$	53
.	.	.
.	.	.
.	.	.
255	$7(255)^{-1} \oplus 13 = 7(254) \oplus 13$	198

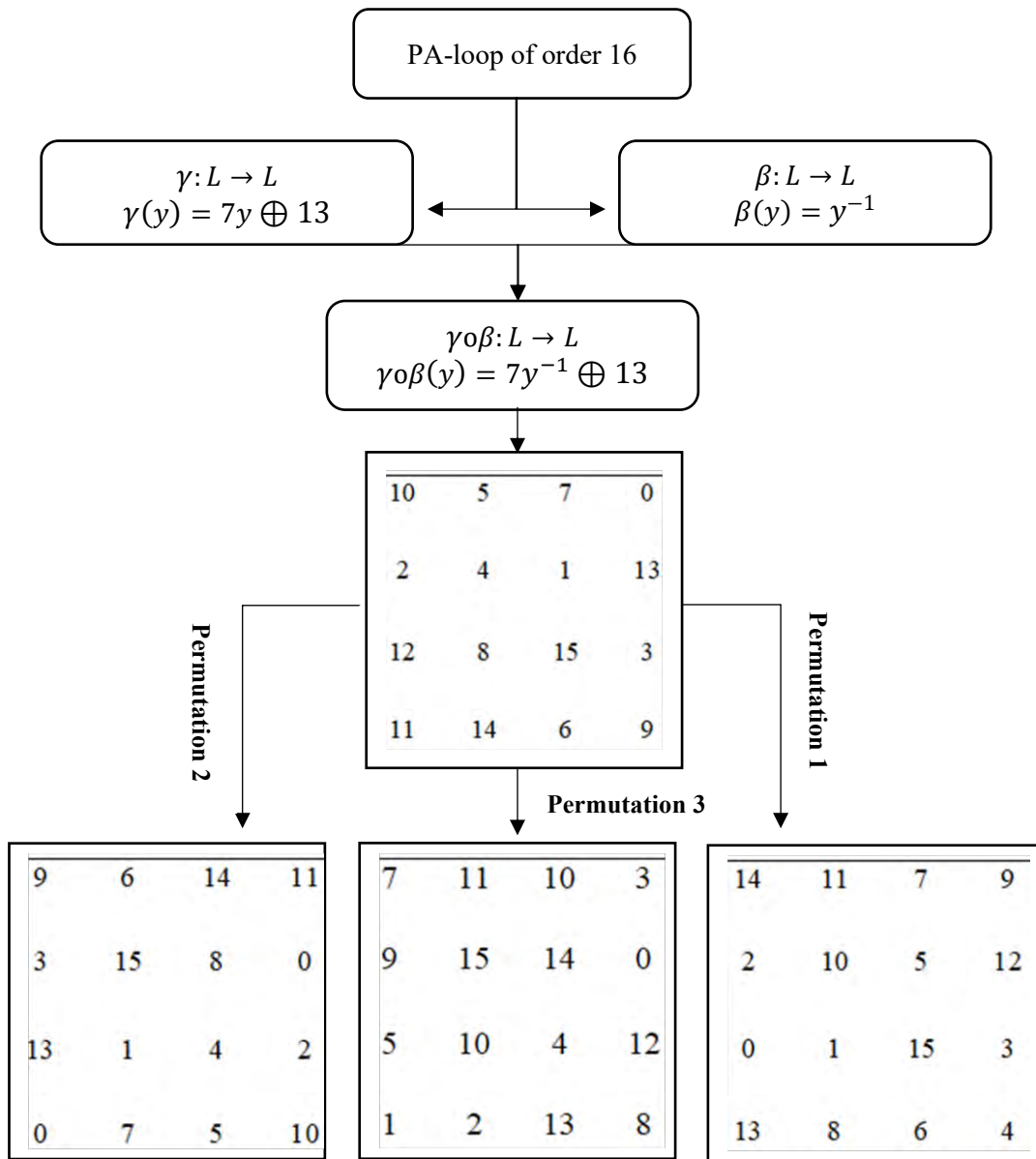


Fig. 5.2: Flow chart of newly designed 4×4 S-boxes.

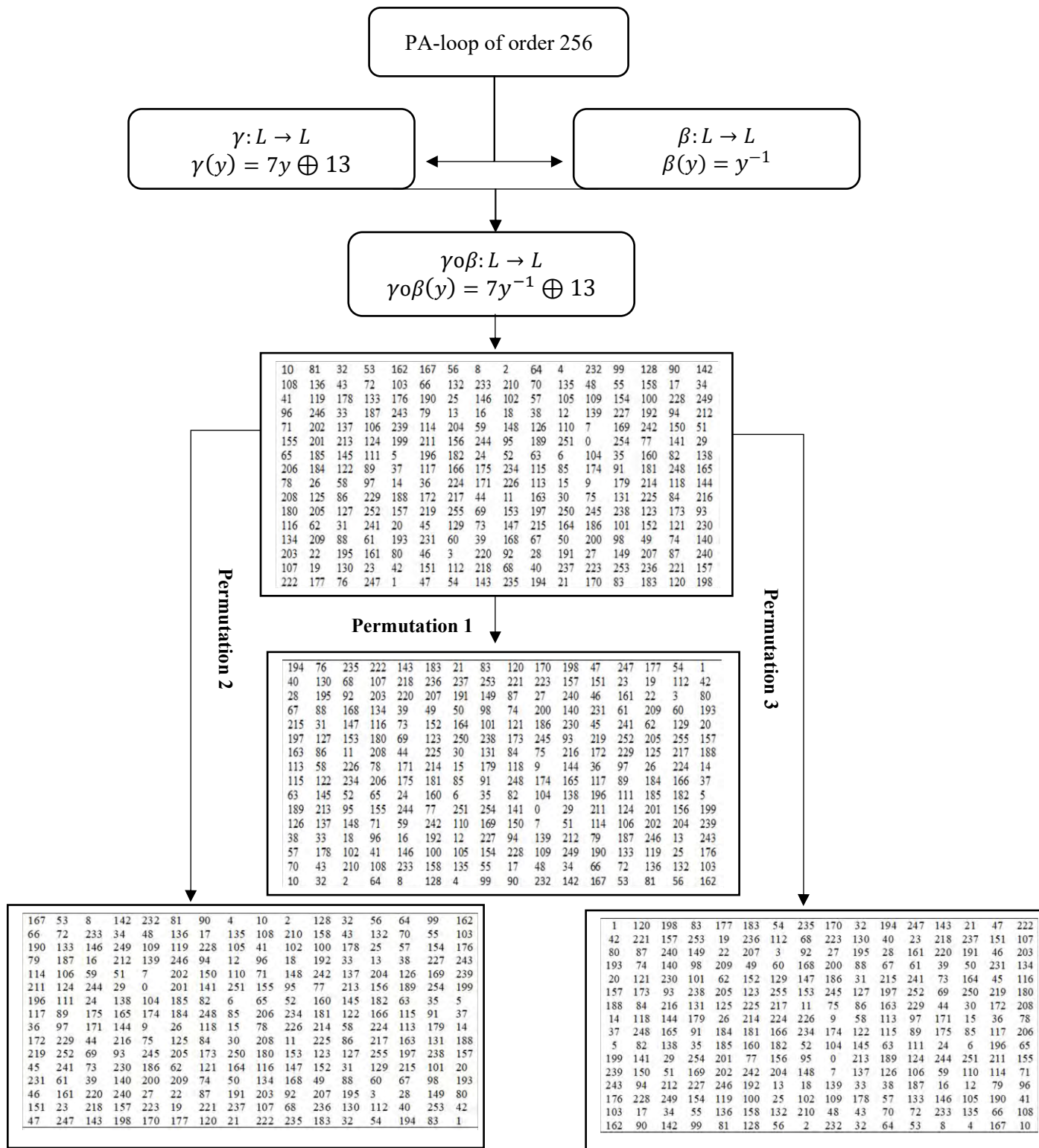


Fig. 5.3: Flow chart of newly designed 16×16 S-boxes

5.3 Analyses of S-box

It is mandatory to analyse the strength of newly constructed S-boxes. Here, we analyse the S-boxes by using different algebraic, statistical, differential and histogram analyses. These analyses are discussed in the upcoming subsections.

5.3.1 Algebraic Analyses of S-box

1) Nonlinearity

It is the most imperative property of a cryptosystem. Principally, the nonlinearity of an outstanding cryptographic system is higher [30]. It measures the confrontation of a system being expressed as a set of linear equations and hence confirms resistance against linear cryptanalysis. Using the theory of Boolean functions, for a Boolean function u , the nonlinearity is defined as follow:

$$NL_u = d(u, f_i) = \min d(u, \delta); \quad \delta \in f_i \quad (5.3)$$

where f_i is the collection of affine Boolean transformations.

Table 5.5 shows the nonlinearity of our new S-box in comparison with various existing S-boxes.

Moreover, Fig. 5.4 is the graphical illustration of nonlinearity analyses.

2) Bit Independent Criterion

The statistical property of output bit independent criterion (BIC) for an S-box given by Webster and Tavares [33] is delineated as, for a certain collection of avalanche vectors, altogether the avalanche variables should be pairwise autonomous. This principle gives the impression to highlight the proficiency of the confusion function.

Table 5.6 gives the outcomes of the BIC analysis of our new S-box. The BIC of the new S-box is up to the standard as compared to different S-boxes. Moreover, the minimum, average and square deviation value of BIC analysis is given in Table 5.7. This table also provides a comparison of the new S-box with other reputed S-boxes. Fig. 5.5 is the graphical representation of this comparison.

3) Strict Avalanche Criterion Analytically

For any of the S-box, strict avalanche criterion (SAC) is satisfied if a change in a single input bit gives an impact on half of the output bits. When S-box is applied to build an S-P network, then a single change on the input of the network causes an avalanche of changes [30]. Table 5.8 shows the outcomes of the SAC analysis of the proposed S-box. In addition to this, the average, minimum, and square deviation values of SAC in comparison with other S-boxes are shown in Table 5.9. In Fig. 5.6 the graphical representation of the SAC comparison between proposed and other S-boxes are provided.

Table 5.5: Nonlinearity Analysis of newly designed S-box with other S-boxes.

S-boxes	F₀	F₁	F₂	F₃	F₄	F₅	F₆	F₇	Average
Proposed S-box	108	105	110	104	106	106	106	110	106.87
Ref [16]	110	106	104	98	108	106	104	96	104
Ref [17]	104	106	106	106	110	104	100	108	105.5
Ref [18]	106	108	110	110	108	104	100	108	106.75
Ref [24]	104	105	105	105	102	103	102	104	103.75
Ref [25]	112	112	112	112	112	112	112	112	112
Ref [44]	106	106	106	106	106	106	108	108	106.5
Ref [45]	112	110	112	112	112	110	112	112	111.5
Ref [46]	104	104	108	108	108	104	104	106	105.75
Ref [47]	94	100	104	104	102	100	98	94	99.5

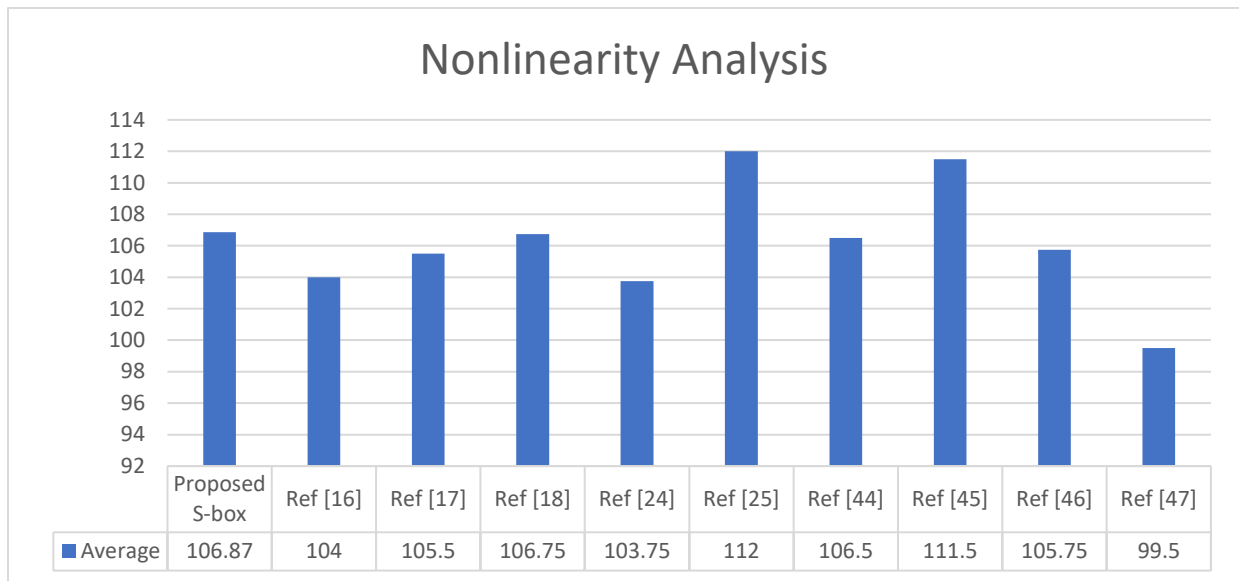


Fig. 5.4: Nonlinearity Analysis

Table 5.6: Bit Independent Criterion of newly designed S-box.

-	107.000	108.000	104.000	108.000	108.000	108.000	106.000
107.000	-	107.000	103.000	105.000	109.000	105.000	107.000
108.000	107.000	-	106.000	108.000	106.000	108.000	104.000
104.000	103.000	106.000	-	108.000	106.000	108.000	104.000
108.000	105.000	108.000	108.000	-	108.000	104.000	106.000
108.000	109.000	106.000	106.000	108.000	-	102.000	104.000
108.000	105.000	108.000	108.000	104.000	102.000	-	104.000
106.000	107.000	104.000	104.000	106.000	104.000	104.000	-

Table 5.7: BIC Analysis of newly designed S-box with other S-boxes.

S-boxes	Average	Minimum Value	Square Deviation
Proposed	106.107	102	1.87729
Ref [16]	106.27	104	1.578
Ref [17]	106	102	2.138

Ref [18]	106.27	104	1.578
Ref [24]	103.929	101	2.052
Ref [25]	112	112	0
Ref [44]	104.071	100	2.2349
Ref [45]	111.3	110	0.934
Ref [46]	104.14	102	1.767
Ref [47]	101.71	94	3.53

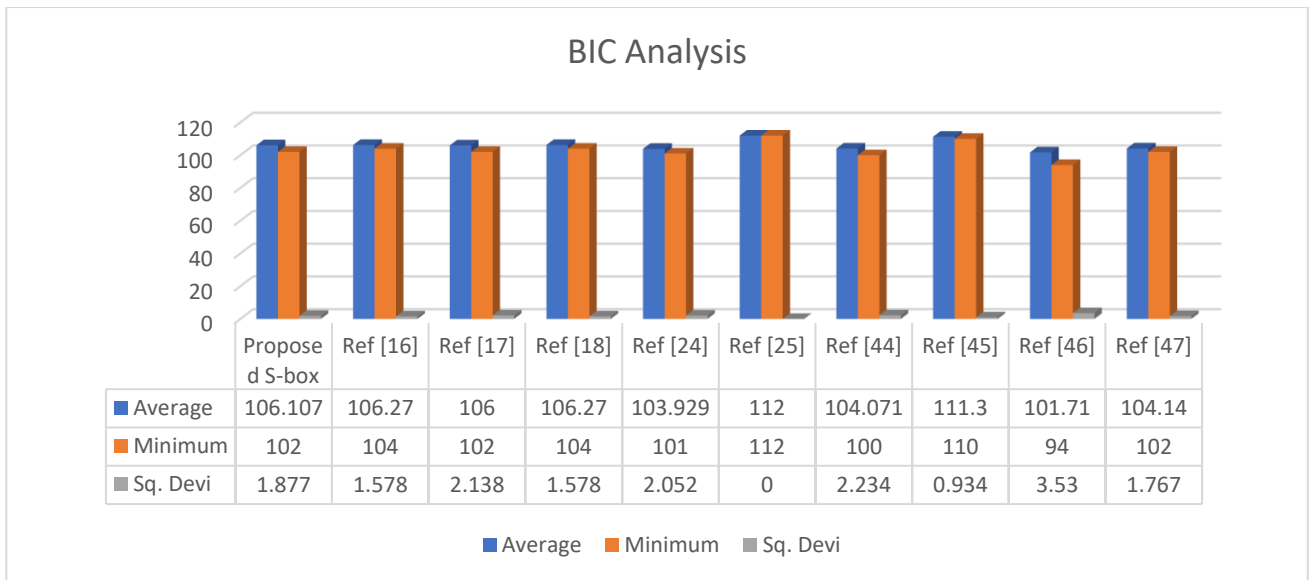


Fig. 5.5: Bit Independent Criterion Analysis

Table 5.8: Strict Avalanche Criterion of newly designed S-box.

0.507	0.539	0.507	0.445	0.492	0.492	0.507	0.515
0.492	0.523	0.523	0.476	0.476	0.460	0.507	0.531
0.539	0.429	0.523	0.460	0.507	0.523	0.445	0.515
0.554	0.476	0.523	0.492	0.539	0.507	0.492	0.515
0.539	0.492	0.523	0.523	0.492	0.476	0.507	0.515

0.523	0.460	0.507	0.523	0.523	0.539	0.523	0.531
0.523	0.523	0.523	0.523	0.539	0.507	0.507	0.515
0.523	0.507	0.507	0.492	0.507	0.429	0.507	0.500

Table 5.9: SAC Analysis of newly designed S-box with other S-boxes.

S-boxes	Minimum Value	Average	Square Deviation
Proposed S-box	0.437	0.509	0.013
Ref [16]	0.390	0.493	0.020
Ref [17]	0.462	0.500	0.015
Ref [18]	0.401	0.504	0.018
Ref [24]	0.429	0.505	0.013
Ref [25]	0.484	0.504	0.018
Ref [44]	0.421	0.500	0.018
Ref [45]	0.437	0.505	0.016
Ref [46]	0.499	0.464	0.018
Ref [47]	0.502	0.47	0.017

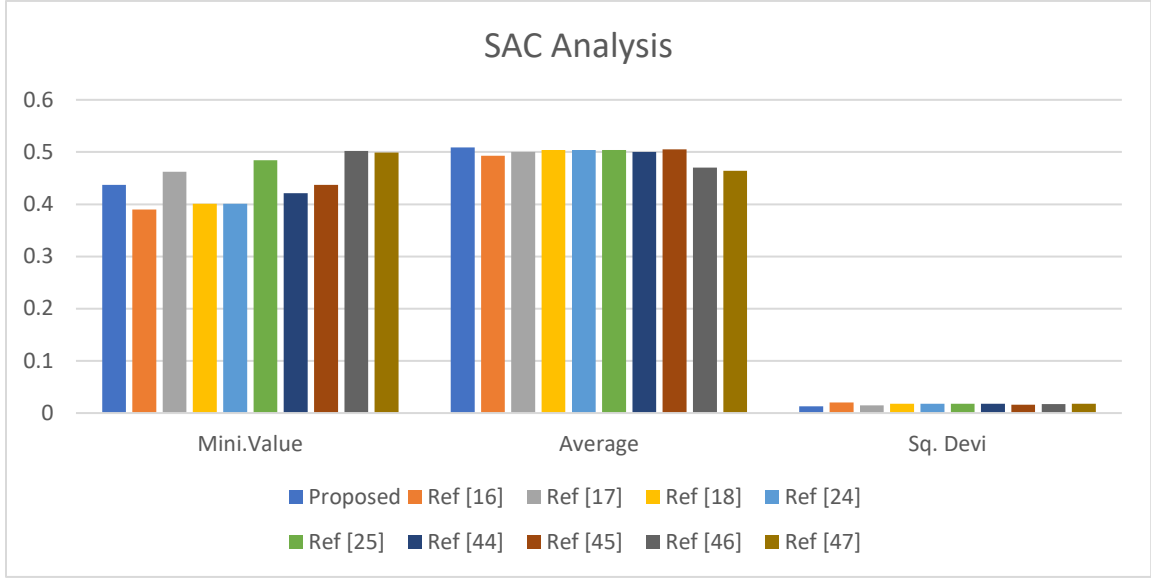


Fig. 5.6: Strict Avalanche Criterion Analysis

5.3.2 Differential Analyses

To assess the strength of the cryptosystem, we have examined the impact of differential attacks on our system. The differential attack comes into the category of plaintext chosen attacks where the attacker evaluates the outcomes that come back to the known ciphertext. Here, the results of the two most renowned tests i.e., Unified Averaged Changed Intensity (UACI) and Number of Pixel Change Rate (NPCR) are discussed to identify the resistance of the system against differential attacks [34]. These tests are given below:

1) UACI Analysis

The representation of this analysis can be given as:

$$\mathcal{U}(E^1, E^2) = \frac{1}{L_1 \times W_1} \left[\sum_{x_1, y_1} \frac{|E^1(x_1, y_1) - E^2(x_1, y_1)|}{255} \right] \times 100\% \quad (5.4)$$

$$D_b(x_1, y_1) = \begin{cases} 0, & \text{if } E^1(x_1, y_1) = E^2(x_1, y_1) \\ 1, & \text{if } E^1(x_1, y_1) \neq E^2(x_1, y_1) \end{cases} \quad (5.5)$$

2) NPCR Analysis

The NPCR analysis is represented as:

$$\mathcal{N}(E^1, E^2) = \sum_{x_1, y_1} \frac{D_b(x_1, y_1)}{L_1 \times W_1} \times 100\% \quad (5.6)$$

Where L_1 and W_1 show the width and height of an image respectively. The symbol D_b represents the bipolar array. Moreover, E^1 and E^2 depict two encrypted images. For $E^1 = E^2$, value of $D_b = 0$ else $D_b = 1$. The values of UACI and NPCR of the proposed S-box in comparison with other well-known S-boxes are given in Table 5.10. In Table 5.11, the comparative analyses of the proposed method with AES are given.

Table 5.10: NPCR and UACI Analyses of newly designed S-box with other S-boxes.

Algorithms	NPCR	UACI
Proposed	99.61	33.08
Ref [32]	99.58	28.62
Ref [33]	98.47	32.21
Ref [34]	99.42	24.94
Ref [35]	99.54	28.27
Ref [36]	99.60	33.42
Ref [48]	99.30	33.40
Ref [49]	99.59	33.45
Ref [50]	99.60	33.46

Table 5.11: Comparison of NPCR and UACI Analyses of the proposed technique with AES.

Images	Loc.	NPCR		UACI	
		Proposed	AES	Proposed	AES
	First	99.60	99.61	30.56	33.54
Cameraman	Mid	99.63	99.62	37.43	33.53

	Last	99.62	99.59	34.55	33.53
	First	99.01	99.61	30.56	33.54
Lena	Mid	99.62	99.62	37.42	33.53
	Last	99.63	99.59	34.56	33.53
	First	99.02	99.61	30.59	33.54
Baboon	Mid	99.63	99.62	37.43	33.53
	Last	99.61	99.59	34.55	33.53

5.3.3 Cryptanalysis

1) Linear Approximation Probability

It estimates the extreme quantity of the imbalance of an incident. The similarity of the input bits chosen by the mask Γ_x and the similarity of the output bits chosen by the mask Γ_y must be equal.

According to [30], the probability of bias of a given S-box is defined as:

$$LP = \# \max_{\Gamma_x, \Gamma_y \neq 0} \left| \frac{\#\{x | x \cdot \Gamma_x = S(x) \cdot \Gamma_y - \frac{1}{2}\}}{2^s} \right| \quad (5.6)$$

Where Γ_x & Γ_y are the contributions and production masks, respectively, 2^s is a total entity. Table 5.12 shows the comparison of the LP value of the proposed S-box in comparison with other S-boxes. Whereas Fig. 5.7 is the graphical representation of this comparison.

2) Differential Approximation Probability

The differential approximation probability of a given S-box (i.e., DPs) is a measure for differential uniformity and is defined as:

$$DP(\Delta x \rightarrow \Delta y) = \left\lceil \frac{\#\{x \in X | S(x) \oplus S(x \oplus \Delta x) = \Delta y\}}{2^m} \right\rceil \quad (5.7)$$

Table 5.13 depicts the DP values of the proposed S-box and Table 5.14 is the comparison of the maximum DP value of the new S-box with other S-boxes. Fig. 5.8 shows the graph of Table 5.14 comparisons.

Table 5.12: Linear Approximation Probability Analysis of S-boxes.

S-boxes	Proposed S-box	Ref [16]	Ref [17]	Ref [18]	Ref [24]	Ref [25]	Ref [44]	Ref [45]	Ref [46]	Ref [47]
Max Value	157	160	160	161	159	144	162	146	166	156
Max LP	0.113	0.125	0.132	0.125	0.121	0.062	0.132	0.070	0.148	0.109

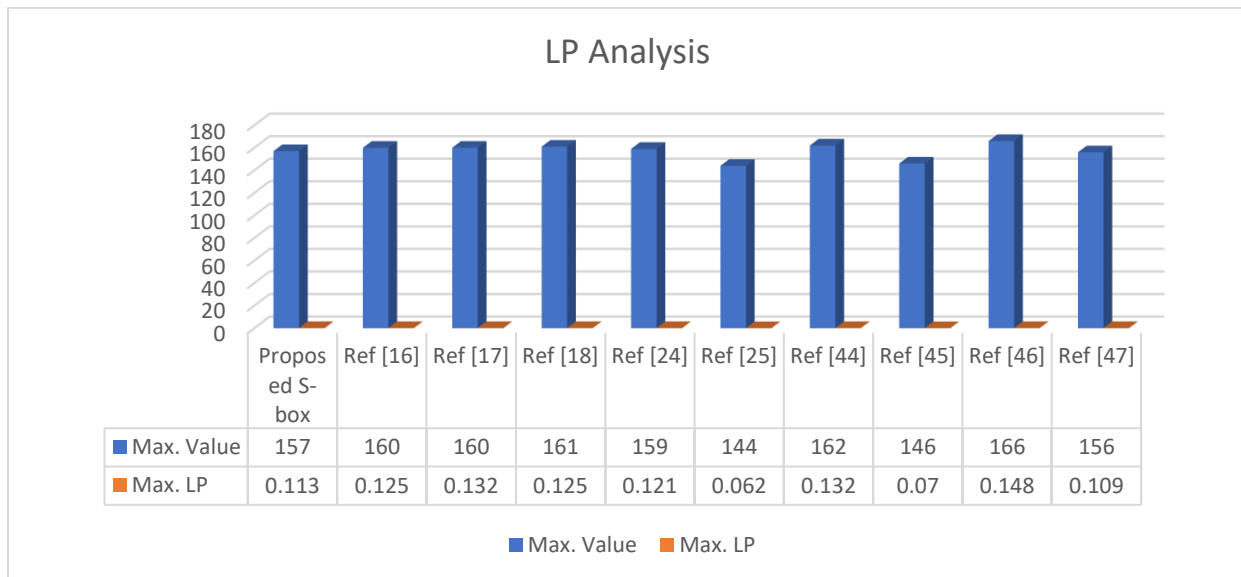


Fig. 5.7: Linear Approximation Probability Analysis

Table 5.13: Differential Approximation Probability of newly designed S-box.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
.015	.015	.015	.015	.023	.023	.023	.015	.023	.023	.023	.023	.015	.015	0.023	0.015
.023	.015	.015	.023	.023	.023	.031	.023	.023	.015	.031	.023	.015	.015	0.015	0.015

.015	.031	.023	.015	.023	.015	.023	.023	.023	.023	.023	.023	.015	.023	0.023	0.015
.015	.015	.031	.015	.023	.023	.023	.023	.023	.031	.031	.023	.015	.023	0.031	0.023
.023	.015	.023	.023	.023	.015	.023	.015	.023	.023	.031	.023	.023	.031	0.023	0.023
.023	.023	.023	.015	.023	.031	.023	.023	.031	.015	.023	.023	.023	.023	0.023	0.015
.023	.015	.023	.023	.023	.031	.031	.023	.015	.023	.023	.031	.023	.023	0.023	0.015
.023	.023	.023	.031	.023	.039	.023	.023	.031	.023	.023	.023	.023	.015	0.015	0.015
.015	.023	.031	.015	.023	.023	.023	.023	.015	.031	.023	.023	.023	.023	0.023	0.015
.023	.023	.031	.023	.023	.015	.023	.015	.023	.023	.023	.031	.023	.023	0.023	0.023
.015	.023	.023	.023	.015	.031	.023	.023	.031	.023	.031	.023	.023	.023	0.031	0.023
.023	.023	.031	.023	.023	.023	.023	.031	.023	.023	.031	.023	.023	.023	0.023	0.015
.023	.023	.023	.015	.023	.023	.023	.015	.023	.023	.023	.023	.023	.031	0.023	0.023
.015	.023	.023	.039	.023	.023	.023	.023	.031	.023	.023	.023	.023	.023	0.023	0.023
.015	.023	.015	.023	.015	.023	.023	.031	.023	.023	.023	.031	.023	.023	0.023	0.015
.023	.023	.023	.023	.023	.023	.023	.023	.031	.023	.023	.031	.023	.015	0.015	-

Table 5.14: Comparison of DP Analysis of newly designed S-box with other S-boxes.

S-boxes	Proposed S-box	Ref [16]	Ref [17]	Ref [18]	Ref [24]	Ref [25]	Ref [44]	Ref [45]	Ref [46]	Ref [47]
Max DP	0.0312	0.125	0.0242	0.0267	0.0390	0.011	0.039	0.015	0.0468	0.281

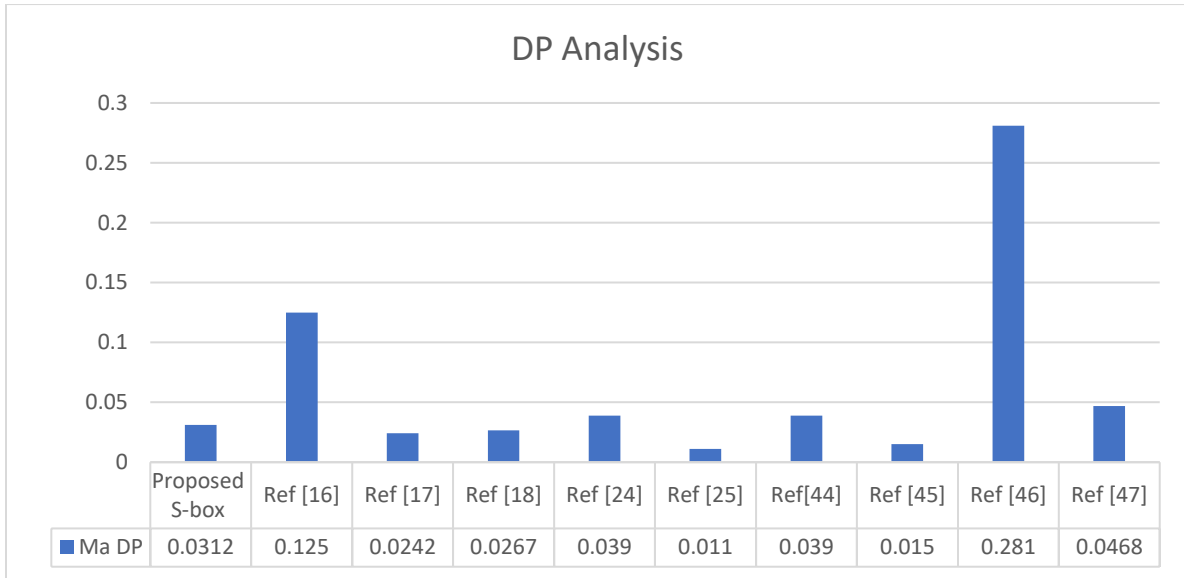


Fig. 5.8: Differential Approximation Probability Analysis

5.3.4 Histogram Analysis

The graphical comparison of plaintext and encrypted image can be given by histogram analysis. Any of the cryptosystems encrypts plaintext image into an image that has random pixels. After the process of encryption, the purpose of histogram analysis is to show the dispersal of these pixels [37]. In this work, Fig. 5.9 (a) and 5.9 (b) show the plaintext and encrypted images (encrypted with proposed S-box) of Lena respectively. Fig.5.9 (b) is encrypted well enough to give not a hint of the original image. Moreover, Fig. 5.9 (c) and 5.9 (d) are the histograms of plaintext and encrypted images. The histogram of the cipher image in Fig. 5.9(d) is uniformly distributed and hence assures the quality of our S-box encryption.

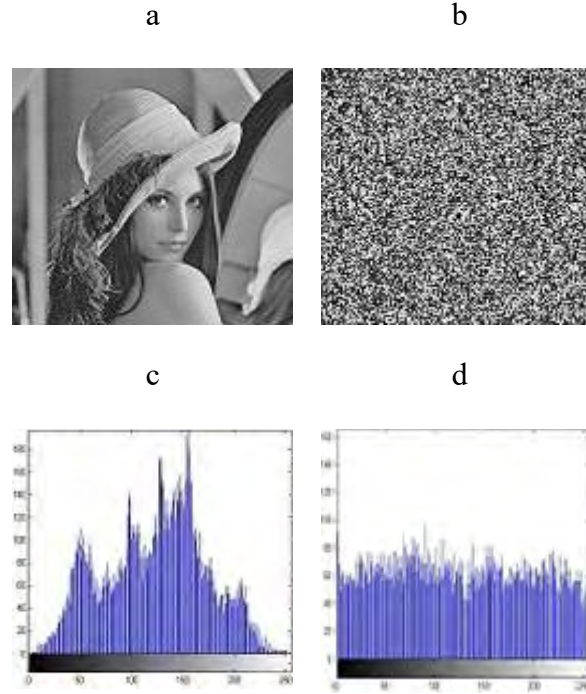


Fig. 5.9: a) Original Lena image b) Encrypted Lena image c) Lena image histogram d) Encrypted Lena image histogram.

5.4 Majority Logic Criterion Test

In [30], the detailed explanation of the majority logic criterion (MLC) is represented. These analyses give a comparison of plaintext images and encrypted images and hence give the true assessment of an encryption scheme. Generally, homogeneity, energy, correlation, contrast, and entropy are used for MLC analyses. The outcomes of these analyses indicate the strength of the encryption scheme and hence involved S-box. The results show that our proposed S-boxes are secure and best suited for the encryption process. The 256×256 image of Lena is used for these analyses. Table 5.15 and Table 5.16 give the MLC results of the Lena image with the help of proposed 4×4 while Table 5.17 shows the MLC results 16×16 PA-loop S-box, respectively. These tables also indicate the comparison of the proposed technique with other existing S-boxes. Moreover, Fig. 5.10 shows encrypted images (with proposed S-box and other well-known S-boxes) and their histograms.

Table 5.15: Results of MLC Analyses on Lena grey image.

LSB	MLC				
Image	Homogeneity	Entropy	Energy	Contrast	Correlation
Plain image	0.9055	7.4455	0.1316	0.2293	0.9502
Proposed	0.9090	5.9629	0.1613	0.2876	0.9770
Ref [24]	0.9178	5.8599	0.1632	2.2665	0.9788
GF (2⁴)	0.9181	5.9698	0.1689	0.249	0.9778
GR (4,4)	0.4835	4.7302	0.0245	3.322	0.0879

Table 5.16: Results of MLC Analyses on Lena grey image.

MSB	MLC				
Image	Homogeneity	Entropy	Energy	Contrast	Correlation
Plain image	0.9055	7.4455	0.1316	0.2293	0.9502
Proposed	0.7935	5.9217	0.2036	2.9692	0.7590
Ref [24]	0.8230	5.8582	0.1670	2.5615	0.7980
GF (2⁴)	0.8477	5.7457	0.1887	1.6909	0.8864
GR (4,4)	0.8729	5.0659	0.3258	2.0590	0.7962

Table 5.17: Results of MLC Analyses by 16×16 S-box.

S-boxes	Entropy	Contrast	Correlation	Energy	Homogeneity	MAD
Proposed	7.9353	9.9764	0.0487	0.0161	0.4131	38.4556
Ref [24]	7.9633	8.5969	0.0019	0.0174	0.4070	38.5639
Ref [25]	7.7301	7.3220	0.0879	0.0244	0.4835	36.3630
Ref [30]	7.7094	8.1685	0.2309	0.0227	0.4870	43.5662
Ref [47]	7.6595	6.3683	0.0996	0.0260	0.4984	36.3084

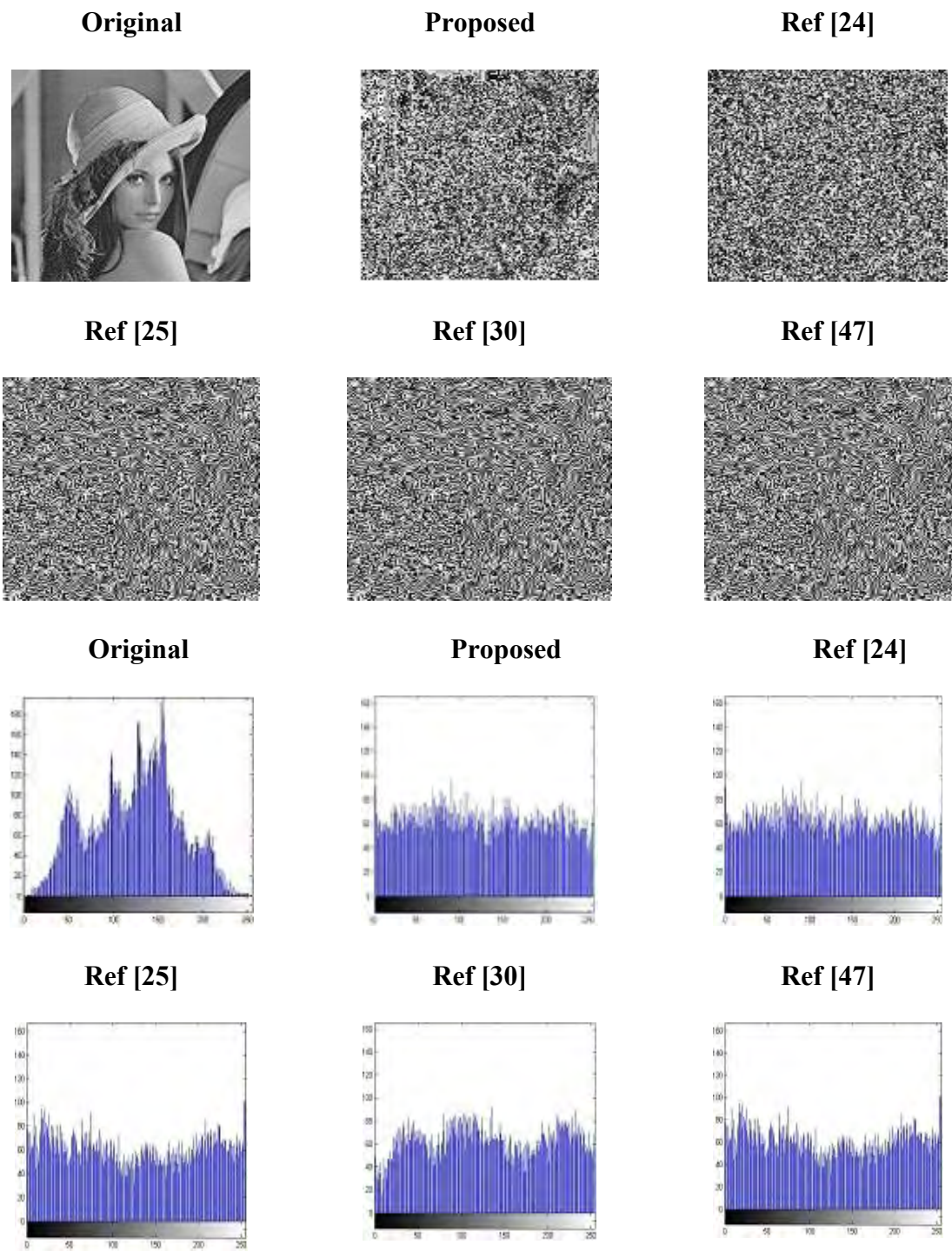


Fig. 5.10: Encrypted images and 8 respective histograms.

Chapter 6

Designing of Non-linear Block Cipher's Component over PA-loop through Mobius Transformation

This chapter is set as follows: Introduction is given in section 1. In section 2 preliminaries and construction scheme with the help of Mobius transformation. In section 3 we examine the strength of our S-boxes and compared them with other well-known S-boxes using algebraic and statistical analyses. In section 4, we used our proposed S-boxes in image encryption and assess the strength of newly designed S-boxes using the majority logic criterion.

6.1 Introduction

The role of the S-box is to create confusion in symmetric cryptography and hence support the security of the whole system. Due to this reason, several statistical and algebraic S-boxes are constructed over different structures. Most of them are based on associative structures. In this chapter, the PA-loop utilizing Mobius transformation is utilized for the erection of S-boxes. This structure consists of admirable features including the non-associativity, inverse of zero, and more variety of Cayley's tables as compared to associative structure local rings and Galois field. As compared to existing S-boxes in the literature the S-boxes based on PA-loop are comparatively easy to construct and have a bulk of nonlinear components of block cipher due to more variety of structures due to above mention properties. The strength of newly designed S-boxes is measured using different standard algebraic and statistical analyses available in the literature. The proposed construction successfully cleared all these tests.

6.2 Preliminaries

In this section, the definition of Mobius transformation is presented.

Mobius Transformation

Mobius transformation is mathematically express as

$$\varphi(y) = \frac{\alpha y + \beta}{\gamma y + \sigma}, \text{ where } \alpha, \beta, \gamma, \sigma \in L \quad (6.1)$$

Where L is PA-loop and $\alpha\sigma - \beta\gamma \neq 0$.

6.2.1 Design of S-Boxes over PA-loop

In different cryptosystems, different methods are used to generate confusion in the data. However, S-boxes are the best source for confusion in the literature. Most of these structures are depend upon the Galois field and some are belonging to \mathbb{Z}_2^n which is n topples of binary field \mathbb{Z}_2 . These classes are associative therefore show limited impact as shown in Table 6.1. PA-loop has more structures as compared to groups and Galois field due to non-associative, which give us different choices to design S-boxes.

Table 6.1: Classification of Associative and Non-Associative structures of order n.

n.	IP-loop of order n	Non-Associative Loops of order n	Groups of order n	Fields of order n
1	1	0	1	1
2	1	0	1	1
3	1	0	1	1
4	2	0	2	1
5	1	5	1	1
6	2	109	2	0
7	2	746	1	1

8	8	982	5	1
10	49	1245	2	0
11	50	1987	1	1
12	2689	2684	5	0
13	1034	2342	1	0
16	1884	2038	14	1

The variety of S-boxes makes the cryptosystems secure and helps to resist spiteful attacks. For the constructions of S-boxes, many techniques are given the literature from which Mobius transformation is one of them. To create several different S-boxes by Mobius transformation which is the action of a projective general linear group on a PA-loop of order 16 and 256. The mathematical expression of this technique is given below:

$$\varphi: PGL(2, L_n) \times L_n \rightarrow L_n \quad (6.2)$$

$$\varphi(y) = \frac{a*y \oplus b}{c*y \oplus d}, a * d - b * c \neq 0, a, b, c, d \in L_n \quad (6.3)$$

Value of a and c are to be fixed 4 and 9 respectively but b and d vary from 0 to $n - 1$. Take the values of $y = 0: n - 1$ then use the table of PA-loop see value corresponding to $a * y, c * y$ after that convert the system into a binary number. Apply XOR in numerator and denominator and simplify utilizing the table of PA-loop. After simplification exponent gives us a new transformed S-box. We construct **131028** S-boxes by varying the values of b and d . The flow chart of this scheme is given in Fig. 6.1.

In table 6.2 we consider a PA-loop order 16. Define an equation (6.2) as:

$$\varphi: PGL(2, L_{16}) \times L_{16} \rightarrow L_{16}$$

by

$$\varphi(y) = \frac{a*y \oplus b}{c*y \oplus d}, a * d - b * c \neq 0, a, b, c, d \in L_{256} \quad (6.4)$$

here * is a binary operation on PA-loop, $a = 4, c = 9$ and \oplus is a XOR of two numbers. The construction mechanism of the S-box is given in table 3 for fixed values of $b = 5, d = 13$. Table 6.4 shows the new design small S-box.

Table 6.2: 16 order PA-loop.

*	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	0	3	2	11	6	5	8	7	12	13	4	9	10	15	14
2	2	3	4	10	6	9	0	1	12	14	7	5	15	8	11	13
3	3	2	11	13	5	12	1	0	9	15	8	6	14	7	4	10
4	4	11	6	5	0	3	2	15	14	13	12	1	10	9	8	7
5	5	6	1	9	3	10	11	4	13	7	14	2	8	15	0	12
6	6	5	0	12	2	13	4	11	10	8	15	3	7	14	1	9
7	7	8	12	0	15	11	10	13	4	5	2	14	6	3	9	1
8	8	7	9	1	14	4	13	10	11	6	3	15	5	2	12	0
9	9	12	14	15	13	7	8	5	6	0	11	10	1	4	2	3
10	10	13	7	8	12	14	15	2	3	11	0	9	4	1	5	6
11	11	4	5	6	1	2	3	14	15	10	9	0	13	12	7	8
12	12	9	15	14	10	8	7	6	5	1	4	13	0	11	3	2
13	13	10	8	7	9	15	14	3	2	4	1	12	11	0	6	5
14	14	15	13	11	8	0	9	12	1	2	5	7	3	6	10	4
15	15	14	10	4	7	1	12	9	0	3	6	8	2	5	13	11

Table 6.3: Designing structure of new design S-box over PA-loop of order 16.

x	$\varphi(x) = \frac{4 * x \oplus 5}{9 * x \oplus 13}$	S-box
0	$\frac{4 * (0) \oplus 5}{9 * (0) \oplus 13} = \frac{1}{4}$	4
1	$\frac{4 * (1) \oplus 5}{9 * (1) \oplus 13} = \frac{15}{1}$	15
2	$\frac{4 * (2) \oplus 5}{9 * (2) \oplus 13} = \frac{3}{3}$	1
3	$\frac{4 * (3) \oplus 5}{9 * (3) \oplus 13} = \frac{0}{2}$	0
.	.	.
.	.	.
.	.	.
15	$\frac{4 * (15) \oplus 5}{9 * (15) \oplus 13} = \frac{7}{14}$	6

Table 6.4: New design 4×4 S-box.

4	15	1	0
5	2	11	14
10	13	9	7
3	12	8	6

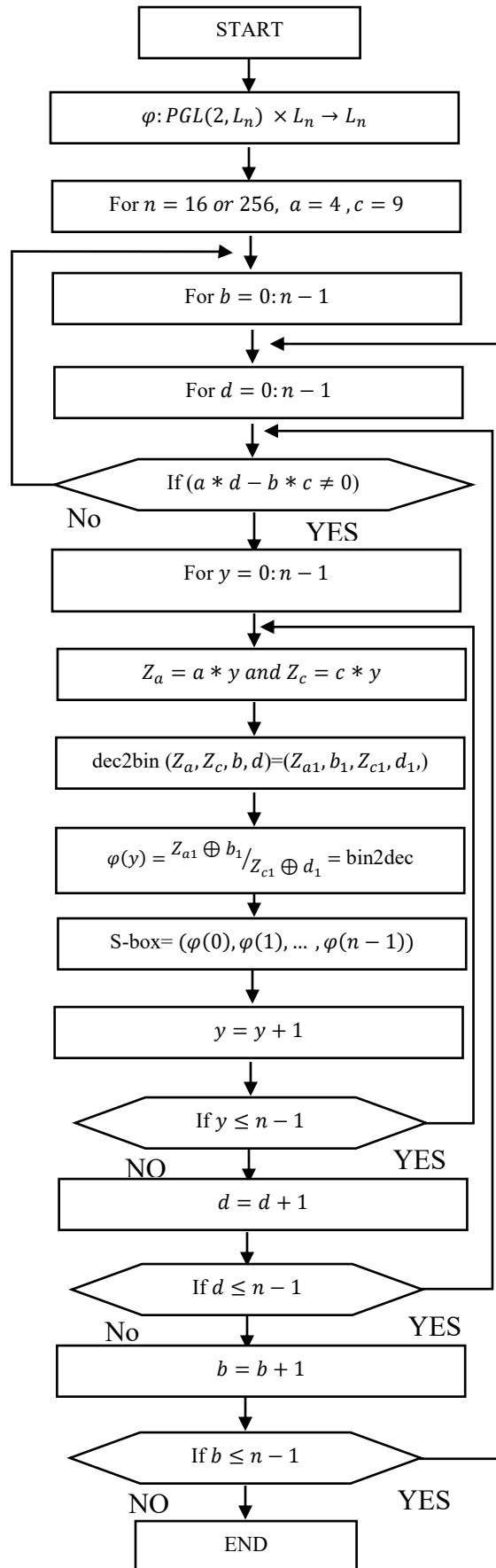


Fig. 6.1: Flow chart of newly designed S-boxes.

Similarly, we can construct 8 bits S-boxes over a PA-loop of order 256 as explained in Table 6.5.

We may change the values of $a, b, c,$ and d for getting more varieties of S-boxes. Here we give examples of three different S-boxes obtained by changing the value of parameters of a mapping.

Table 6.5: Designing structure of new S-box over PA-loop of order 256.

x	$\varphi(x) = \frac{4 * x \oplus 5}{9 * x \oplus 13}$	S-box
0	$\frac{4 * (0) \oplus 5}{9 * (0) \oplus 13}$	194
1	$\frac{4 * (1) \oplus 5}{9 * (1) \oplus 13}$	76
2	$\frac{4 * (2) \oplus 5}{9 * (2) \oplus 13}$	235
3	$\frac{4 * (3) \oplus 5}{9 * (3) \oplus 13}$	222
.	.	.
.	.	.
.	.	.
255	$\frac{4 * (255) \oplus 5}{9 * (255) \oplus 13}$	162

Table 6.6(a): New design 16×16 S-box 1.

194	76	235	222	143	183	21	83	120	170	198	47	247	177	54	1
40	130	68	107	218	236	237	253	221	223	157	151	23	19	112	42
28	195	92	203	220	207	191	149	87	27	240	46	161	22	3	80
67	88	168	134	39	49	50	98	74	200	140	231	61	209	60	193
215	31	147	116	73	152	164	101	121	186	230	45	241	62	129	20

197	127	153	180	69	123	250	238	173	245	93	219	252	205	255	157
163	86	11	208	44	225	30	131	84	75	216	172	229	125	217	188
113	58	226	78	171	214	15	179	118	9	144	36	97	26	224	14
115	122	234	206	175	181	85	91	248	174	165	117	89	184	166	37
63	145	52	65	24	160	6	35	82	104	138	196	111	185	182	5
189	213	95	155	244	77	251	254	141	0	29	211	124	201	156	199
126	137	148	71	59	242	110	169	150	7	51	114	106	202	204	239
38	33	18	96	16	192	12	227	94	139	212	79	187	246	13	243
57	178	102	41	146	100	105	154	228	109	249	190	133	119	25	176
70	43	210	108	233	158	135	55	17	48	34	66	72	136	132	103
10	32	2	64	8	128	4	99	90	232	142	167	53	81	56	162

Table 6.6(b): New design 16×16 S-box 2.

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

210	16	247	115	98	118	90	120	133	153	125	10	168	25	58	145
20	227	63	231	230	181	240	234	134	3	177	143	226	211	241	201
250	66	116	212	243	232	180	117	109	127	33	255	178	126	106	253

Table 6.6(c): New design 16×16 S-box 3.

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

6.3 Analyses of S-box

The strength of newly designed S-boxes is examined with the help of standard statistical, differential, algebraic, and histogram analyses. We reviewed these analyses in the forthcoming subsections. The outcomes of these analyses validate that our proposed S-boxes have satisfied all the criteria and show resistance against different attacks. These S-boxes are used for secure communication in different cryptosystems.

6.3.1 Algebraic Analyses of S-box

➤ Nonlinearity

The nonlinearity of our new S-boxes is given in table 6.7 and shows a comparison with various existing S-boxes. The graphical representation of nonlinearity analysis is given in Fig. 6.2.

Table 6.7: Comparison nonlinearity analysis with other S-boxes of newly designed S-boxes.

S-boxes	0	1	2	3	4	5	6	7	Average
Proposed S-box 1	108	105	110	104	106	106	106	110	106.87
Proposed S-box 2	110	112	110	112	110	110	112	110	110.75
Proposed S-box 3	110	112	112	112	112	112	110	112	111.5
Ref. [25]	112	112	112	112	112	112	112	112	112
Ref. [27]	112	112	112	112	112	112	112	112	112
Ref. [18]	106	108	110	110	108	104	100	108	106.75
Ref. [24]	104	105	105	105	102	103	102	104	103.75
Ref. [46]	104	104	108	108	108	104	104	106	105.75
Ref. [47]	94	100	104	104	102	100	98	94	99.5

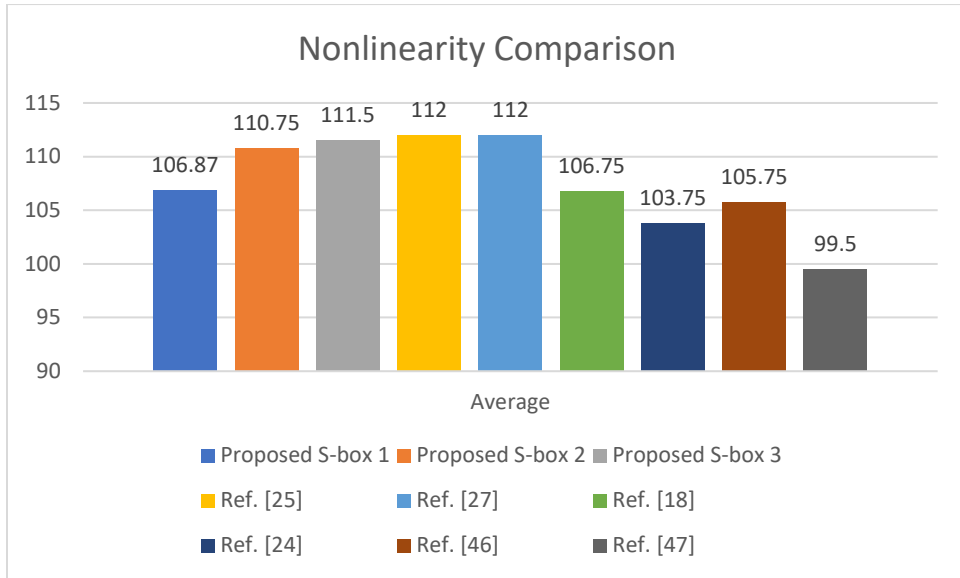


Fig. 6.2: Nonlinearity analysis.

➤ **Bit independent criterion**

The nonlinearity of BIC analysis of the newly designed S-box is given in table 6.8. Moreover, the comparison of BIC in terms of minimum, average, square deviation values is given in Table 6.9.

The graphical representation of BIC analysis is given in Fig. 6.3.

Table 6.8: Bit Independent Criterion of newly designed S-box 3.

-	112.000	112.000	112.000	112.000	112.000	112.000	112.000
112.000	-	112.000	112.000	112.000	112.000	112.000	110.000
112.000	112.000	-	110.000	112.000	112.000	112.000	112.000
112.000	112.000	110.000	-	112.000	112.000	112.000	110.000
112.000	112.000	112.000	112.000	-	112.000	110.000	112.000
112.000	112.000	112.000	110.000	112.000	-	112.000	112.000
112.000	112.000	112.000	112.000	112.000	112.000	-	112.000
112.000	110.000	112.000	110.000	112.000	112.000	112.000	-

Table 6.9: BIC Analysis of newly designed S-box with other S-boxes.

S-boxes	Average	Minimum Value	Square Deviation
Proposed S-box 1	106.107	102	1.87729
Proposed S-box 2	110.5	108	1.14953
Proposed S-box 3	111.5	110	0.69985
Ref. [25]	112	112	0
Ref. [27]	112	112	0
Ref. [18]	106.27	104	1.578
Ref. [24]	103.929	101	2.052
Ref. [46]	101.71	94	3.53
Ref. [47]	104.14	102	1.767

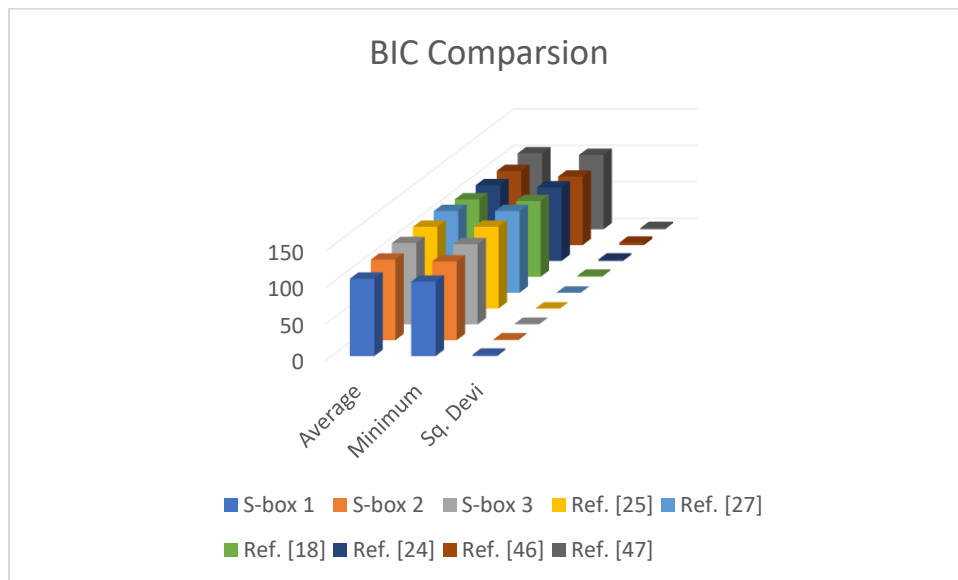


Fig. 6.3: Bit independent criterion analysis.

➤ **Strict avalanche criterion (SAC)**

If the solo input bit creates a change in almost half of the output bits, SAC is considered satisfactory. When the S-P network is constructed using the S-box, then a solo change on the input

of the network causes an avalanche of changes. The results of SAC analysis of the proposed S-box are given in table 6.10. Moreover, the average, minimum, and square deviation values of SAC of newly designed S-boxes and comparison with other S-boxes are enumerated in Table 6.11. Fig. 6.4 shows the pictorial representation of the proposed S-boxes and comparison with other S-boxes of SAC analysis.

Table 6.10: Strict Avalanche Criterion of newly designed S-box.

.5000	.4375	.4843	.4843	.5000	.4531	.4687	.5156
.5000	.4531	.4687	.4843	.5468	.4531	.4687	.4531
.4531	.4843	.5781	.5781	.4375	.4418	.4531	.4687
.4843	.5156	.4531	.4531	.4531	.4531	.5000	.5156
.5156	.5156	.5000	.4843	.4531	.4843	.4687	.4843
.4375	.5000	.4843	.4843	.4531	.4843	.4843	.5000
.5312	.5000	.5468	.5468	.4843	.5000	.5000	.5451
.4687	.5468	.4843	.4843	.4843	.4843	.4531	.5156

Table 6.11: SAC analysis of newly designed S-box with other S-boxes.

S-boxes	Minimum Value	Average	Square Deviation
Proposed S-box 1	.437	.509	.013
Proposed S-box 2	.489	.534	.017
Proposed S-box 3	.487	.545	.016
Ref. [25]	.390	.493	.020
Ref. [27]	.462	.500	.015
Ref. [18]	.401	.504	.018

Ref. [24]	.429	.505	.013
Ref. [46]	.502	.47	.017
Ref. [47]	.499	.464	.018

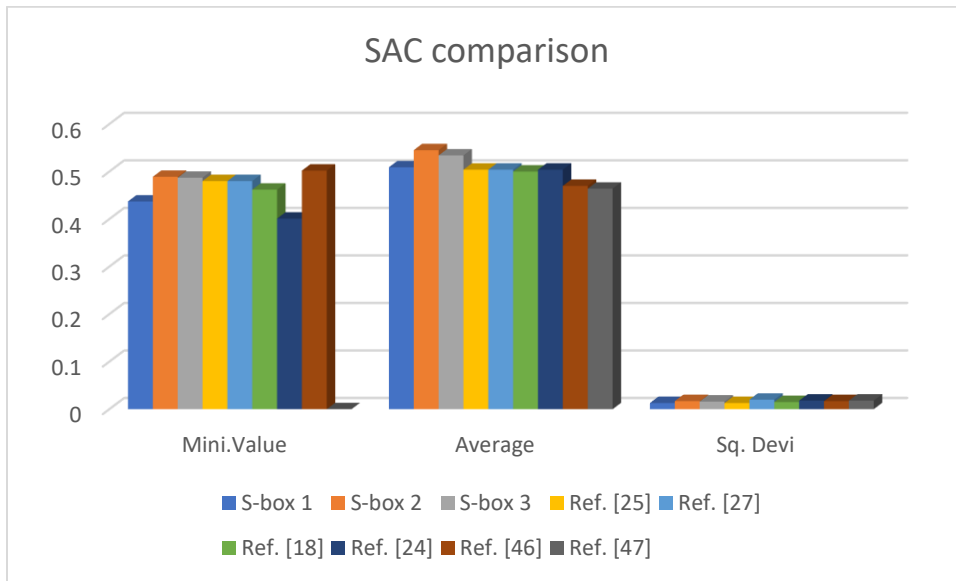


Fig. 6.4: Strict avalanche criterion analysis.

6.3.2 Differential Analysis

In differential analysis, we inspected the impact of differential attacks on our system. Differential attacks categorize as a chosen-plaintext attack where the attacker tries to recognize the original text from the ciphertext. Here, the two most valuable tests i.e., Unified averaged changed intensity (UACI) and Number of changing pixel rate (NPCR) are presented to determine the resistance of the system against differential attacks.

For the newly designed S-boxes values of UACI and NPCR and evaluation with other well-known S-boxes are given in Table 6.12. Table 6.13 shows the relative analysis of newly designed S-boxes with AES is given.

Table 6.12: NPCR AND UACI Analysis of newly designed S-box with other S-boxes.

Algorithms	NPCR	UACI
Proposed S-box 1	99.61	33.08
Proposed S-box 2	99.65	33.17
Proposed S-box 3	99.66	33.3
Ref. [29]	99.58	28.62
Ref. [30]	98.47	32.21
Ref. [31]	99.42	24.94
Ref. [32]	99.54	28.27
Ref. [33]	99.60	33.42
Ref. [34]	99.30	33.40
Ref. [35]	99.59	33.45

Table 13: Comparison of NPCR and UACI Analysis of newly designed S-boxes with AES.

Images	Loc.	NPCR		UACI	
		Proposed	Ref. [25]	Proposed	Ref. [25]
	First	99.60	99.61	30.56	33.54
Camera man	Mid	99.63	99.62	37.43	33.53
	Last	99.62	99.59	34.55	33.53
	First	99.01	99.61	30.56	33.54
Lena	Mid	99.62	99.62	37.42	33.53
	Last	99.63	99.59	34.56	33.53
	First	99.02	99.61	30.59	33.54
Baboon	Mid	99.63	99.62	37.43	33.53
	Last	99.61	99.59	34.55	33.53

6.3.3 Cryptanalysis

➤ Linear Approximation Probability (LP)

The LP value of newly designed S-boxes and comparison with other S-boxes are given in table 6.14 whereas, the graphical representation of this comparison is shown in Fig. 6.5.

Table 6.14: LP Analysis of newly designed S-boxes with other S-boxes.

S-boxes	Proposed S-box 1	Proposed S-box 2	Proposed S-box 3	Ref. [25]	Ref. [27]	Ref. [18]	Ref. [25]	Ref. [46]	Ref. [47]
Max Value	157	150	146	144	144	161	159	166	156
Max LP	0.113	0.085	0.070	0.062	0.062	0.125	0.121	0.148	0.109

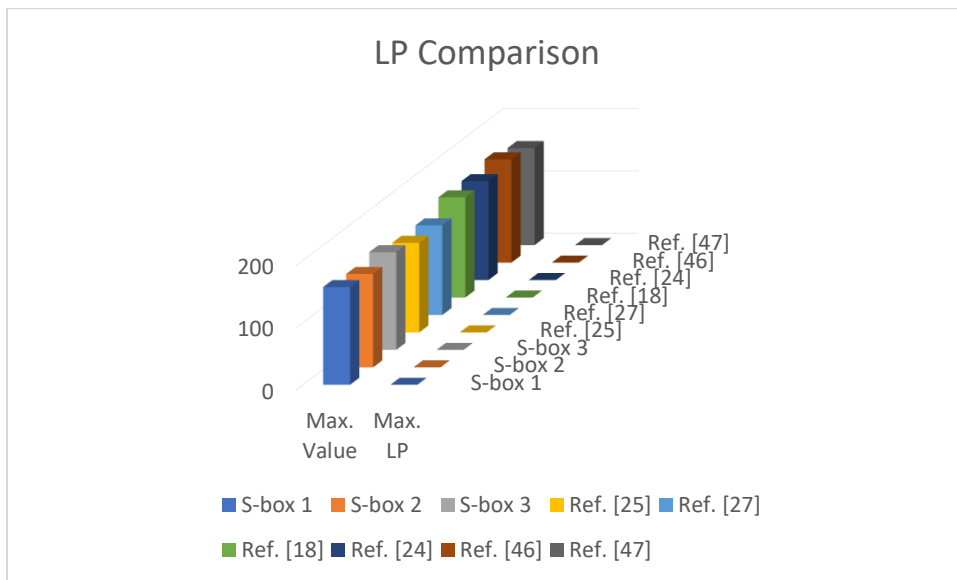


Fig. 6.5: Linear approximation probability analysis.

➤ **Differential approximation probability (DP)**

Tables 6.15 and 6.16 display the DP values of newly designed S-boxes and the comparison of maximum DP value of newly designed S-boxes with other S-boxes. The graphical representation of table 16 is shown in Fig. 6.6.

Table 6.15: Differential approximation probability of newly designed S-box.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
.015	.007	.015	.015	.015	.015	.015	.015	.007	.015	.015	.007	.015	.015	.015	.015
.015	.015	.007	.007	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015
.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015
.015	.015	.015	.015	.015	.015	.07	.015	.015	.015	.015	.015	.015	.015	.015	.015
.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015
.015	.015	.015	.015	.015	.015	.015	.007	.015	.015	.015	.015	.015	.015	.015	.015
.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015
.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015
.015	.015	.015	.015	.007	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015
.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015
.015	.015	.015	.015	.007	.015	.015	.015	.015	.015	.015	.015	.015	.007	.015	.015
.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015
.015	.015	.015	.015	.015	.015	.007	.015	.015	.015	.015	.007	.015	.015	.015	.015
.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.007	.015
.015	.007	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015	.015

Table 6.16: DP Analysis of newly designed S-box with other S-boxes.

S-boxes	Proposed S-box 1	Proposed S-box 2	Proposed S-box 3	Ref. [25]	Ref. [27]	Ref. [18]	Ref. [25]	Ref. [46]	Ref. [47]
Max DP	0.0312	0.0234	0.0234	0.0156	0.0156	0.0267	0.390	0.281	0.0468

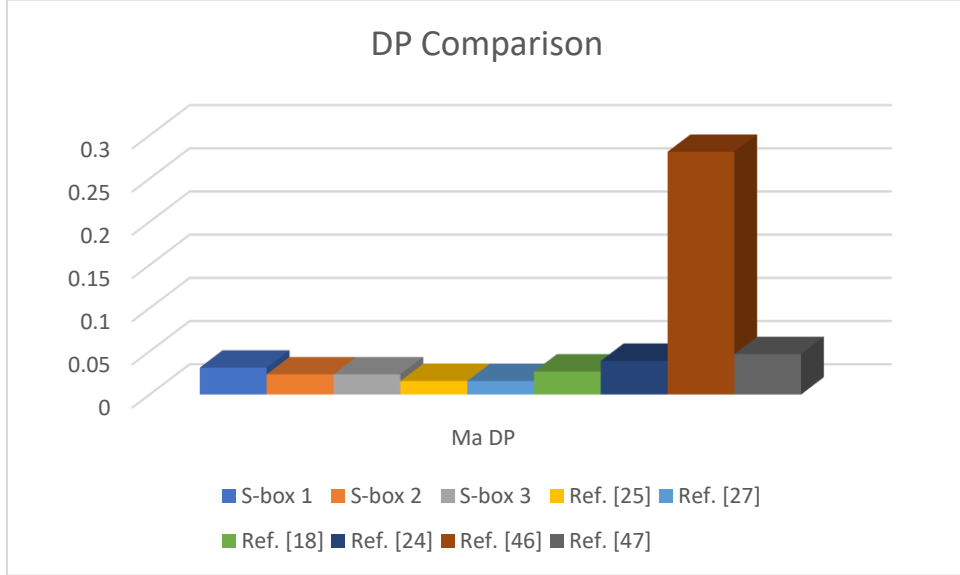
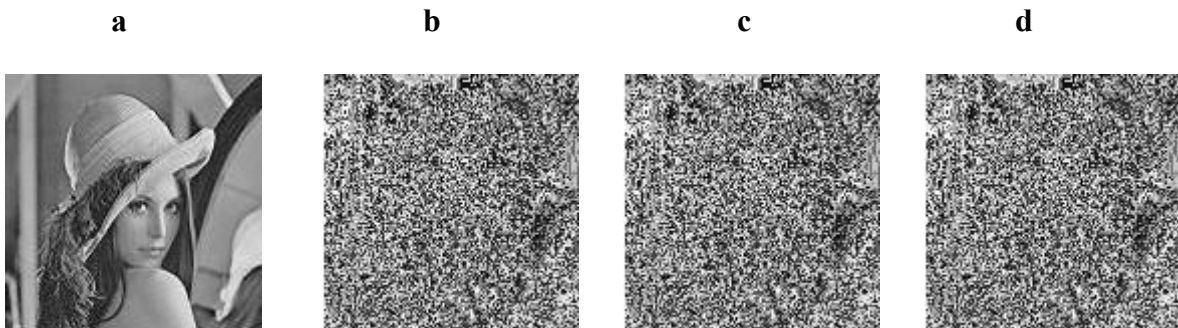


Fig. 6.6: Differential approximation probability analysis.

6.4 Histogram Analysis

Histogram analysis measures the dispersal of pixels after the encryption of digital data pixel. In Fig. 6.7 plain image and encrypted images of Lena, which are encrypted with newly designed S-boxes are given. Moreover, histograms of plain images and encrypted images are also given in Fig. 6.7. The uniform distribution of encrypted images histogram assures the encryption quality of newly designed S-boxes.



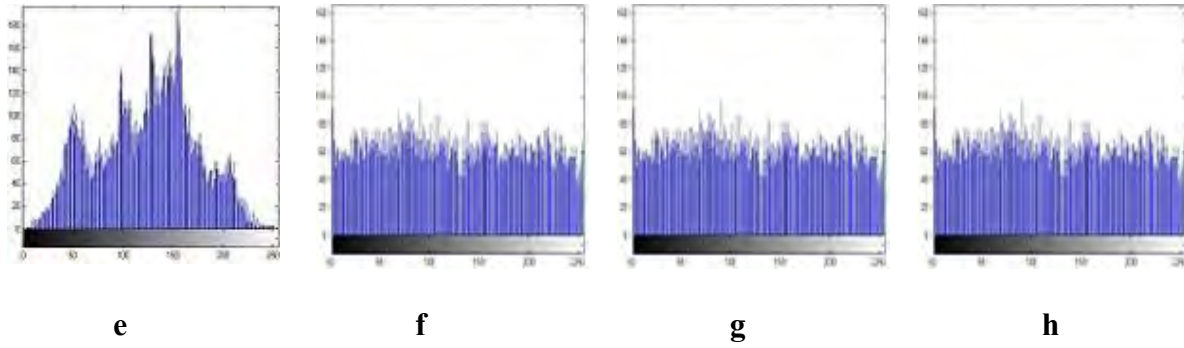


Fig. 6.7: a) Original Lena image b-d) Encrypted Lena image by S-box 1-3

e) Histogram of Lena image f-h) Histogram of Lena image Encrypted by S-box 1-3.

6.5 Majority Logic Criterion Test

The majority logic criterion (MLC) explains the comparison between plain image and encrypted image and gives an accurate evaluation of the encryption scheme. The results of these analyses show the performance and strength of the encryption scheme and hence used S-boxes. For these analyses, we used here 256×256-pixel Lena image. Table 6.17 and Table 6.18 shows the MLC analysis of Lena grey image encrypted by 4 × 4 S-box while Table 6.19 represents the MLC analysis Lena grey image encrypted by 16× 16 S-box. In all three tables comparisons with other well-known S-boxes are also given which show that our proposed technique has better results and is good for encryption. Encrypted image and histogram of Lena with newly designed S-box and comparison with other well-known S-boxes are given in Fig. 6.8.

Table 6.17: Results of MLC analyses on Lena grey image with 4 × 4 S-box.

LSB Image	MLC				
	Homogeneity	Entropy	Energy	Contrast	Correlation
Plain image	0.9055	7.4455	0.1316	0.2293	0.9502
Proposed	0.9090	5.9629	0.1613	0.2876	0.9770
Ref. [24]	0.9178	5.8599	0.1632	2.2665	0.9788

GF (2⁴)	0.9181	5.9698	0.1689	0.2491	0.9778
GR (4,4)	0.4835	4.7302	0.0245	3.3221	0.0879

Table 6.18: Results of MLC analyses on Lena grey image with 4 × 4 S-box.

MSB Image	MLC				
	Homogeneity	Entropy	Energy	Contrast	Correlation
Plain image	.9055	7.4455	.1316	0.2293	.9502
Proposed	.7935	5.9217	.2036	2.9692	.7590
Ref. [24]	.8230	5.8582	.1670	2.5615	.7980
GF (2⁴)	.8477	5.7457	.1887	1.6909	.8864
GR (4,4)	.8729	5.0659	.3258	2.0590	.7962

Table 6.19: Results of MLC analyses by 16×16 S-box.

S-boxes	Entropy	Contrast	Correlation	Energy	Homogeneity	MAD
Proposed	7.9353	9.9764	.0487	.0161	.4131	38.3543
Ref. [24]	7.9633	8.5969	.0019	.0174	.4070	38.5639
Ref. [25]	7.7301	7.3220	.0879	.0244	.4835	36.3630
Ref. [27]	7.7094	8.1685	.2309	.0227	.4870	43.5662
Ref. [47]	7.6595	6.3683	.0996	.0260	.4984	36.3084

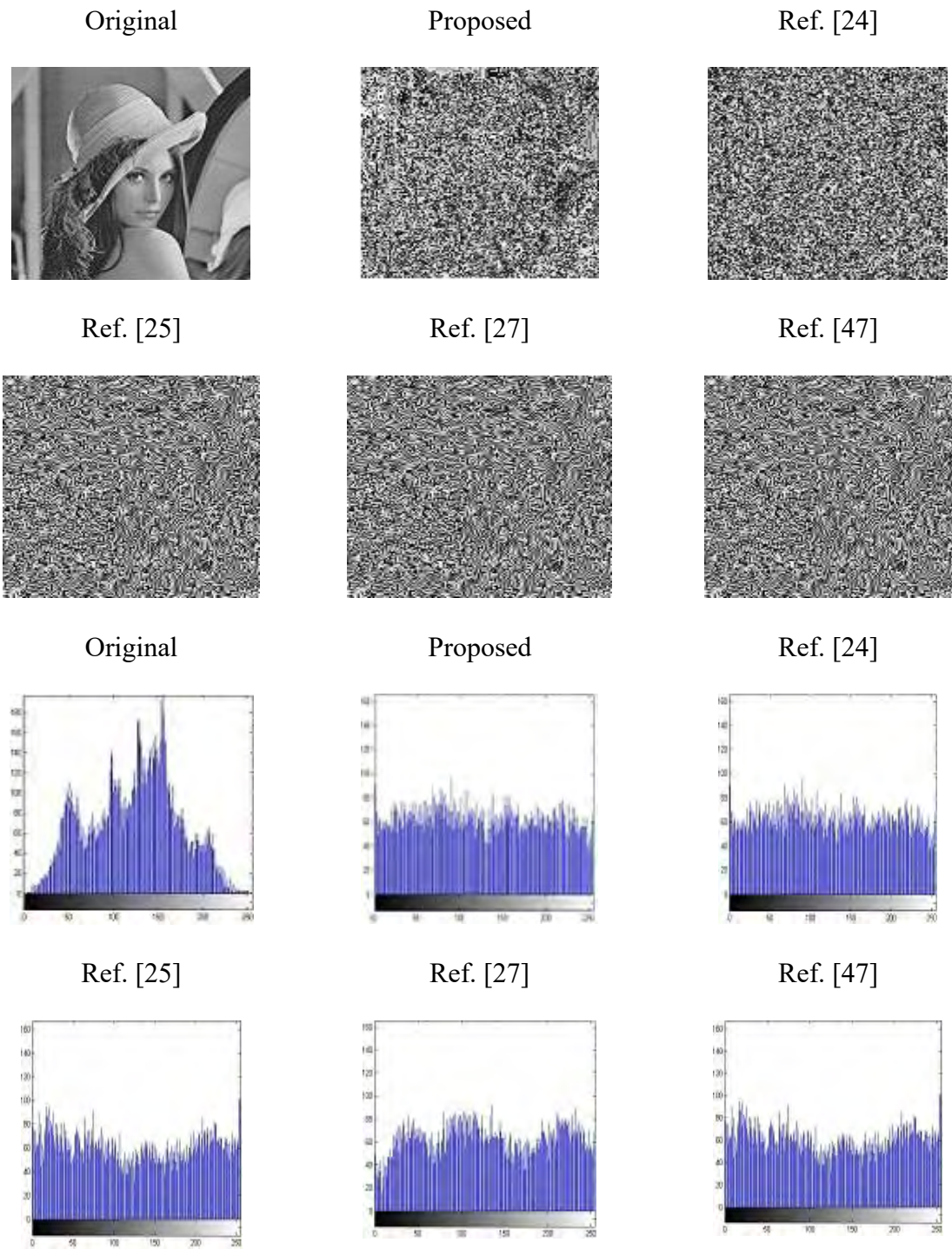


Fig. 6.8: Encrypted images and their respective histograms.

Chapter 7

Redefining Serpent Algorithm by PA-loop with Image Encryption Application

This chapter is set as follows: Introduction of image encryption is given in section 1. Section 2 elaborates the proposed scheme. In section 3 investigational upshots and simulation analyses examine the strength of our cipher scheme and compared it with other well-known schemes. Histogram and differential analyses are given in sections 4 and 5, Chi-square test and time execution performance of proposed scheme are discussed in section 6,7 and last section 8 information entropy test for the proposed scheme is discussed.

7.1 Introduction

Extensive deployment of soft computing devices has changed the overall communication pattern around the globe. All these devices are connected via the internet relying on an unsecure medium. The exponential growth of soft computing devices has got some disadvantages like insecure communications, violation of copyright protection, and alteration of invaluable information. Even the communication in terms of images is also exaggerated by such threats. Generally, to reduce the impact of these, encryption is considered a healthier tactic to attain a higher security level. For that reason, image encryption has achieved extensive importance in Internet communication, medical imaging, multimedia systems, telemedicine, etc.

Encryption schemes are usually categorized into two main divisions, spatial domain and frequency domain. The permutation of positions, the transformation of pixel values, and their amalgamation is used in the spatial domain. Literature reveals many encryption schemes in this domain, but the

prominent schemes are 2D cellular automata-based methods [91], tree structure-based schemes [92], and chaos-based crypt systems [93-95]. In [96], the quadtree structure is used for encryption which in result reduced the processing time of both encryption and decryption. But it has not gained space in international standards. Similarly, many chaos-based schemes [97-99] are proposed due to specific attributes like sensitivity to initial conditions, randomness, ergodicity and complex bifurcation pattern. Certain loopholes appearing in such cryptosystems can be minimized by using higher-dimensional chaotic systems. Usual encryption schemes based on chaotic maps generally use two processes i.e. substitution and diffusion, that are iterated for a certain value. Pixels of images are substituted by the outcomes from chaotic maps which are altered in the diffusion stage by a certain sequential rearrangement. One small alteration in pixels results in total dissimilar output after certain iterations. Such kinds of schemes are very common in literature [100]. Some techniques make use of their proposed structure. Still, speed and security is an issue in such schemes. These drawbacks create space for new cryptosystems.

After spending a successful period, DES [15] algorithm at the start of 21st century lost its popularity. The first allegation on it was of shorter key length i.e. 56-bit key, which can be traced by exhaustive key search in the ever-increasing growth of fast computing devices. Although, this was addressed by introducing triple DES. But another objection was its application in software encryption, although its creation was designed for hardware enciphering.

Due to this drawback, NIST in the US welcomed the new and vibrant inheritor algorithm, which was later called advanced encryption standard (AES). The distinction of AES on predecessor was due to the two reasons, first, it was speedy enough to cope up with new technological development of the 21st century and meanwhile, it did not compromise on security. Moreover, the variation in key size as well as block size made it more interesting as well as challenging to attackers.

Image encryption using block cipher-based serpent algorithm is presented in [91] A proposal algorithm for images protection is depending on the block cipher serpent algorithm in Feistel network structure. Then another scheme for the improvement of serpent algorithm and design to RGB image encryption implementation is present in [102].

In the struggle of creating new variants, many researchers have focused themselves to block size. The variation in block size like doubling it to 256 bits in one way or the other is desired. A similar procedure is used to create a block cipher of 512 bits.

7.2 Cipher Scheme

We encrypt a 128-bit plaintext M to a 128-bit ciphertext C in 16 rounds under the control of S-boxes which are constructed over PA-loop in [89] and using a group of permutations of degree 16 (S_{16}) as a Key. First, we change 128-bit to 16-byte and then convert it into decimal which gives 16 numbers $\{m_1, m_2, m_3, \dots, m_{16}\}$ between 0 to 255. Now the round 1 is starting from here. The first row of S-box which has 16 entries $\{s_1, s_2, s_3, \dots, s_{16}\}$ are applied on $m_i * s_i$, where $*$ is a binary operation on PA-loop L_{256} and $i = 1, 2, 3, \dots, 16$. $m_i * s_i \in L_{256} = \{0, 1, 2, \dots, 255\}$, after it a permutation $P_1 \in S_{16}$ is applied on it which permute $m_i * s_i$, $i = 1, 2, 3, \dots, 16$. In this way, the first round is completed and we have 16 numbers $\{n_1, n_2, n_3, \dots, n_{16}\}$ between 0 to 255. In round 2, the second row of S-box and permutation P_2 is used and the above method is repeated for $\{n_1, n_2, n_3, \dots, n_{16}\}$, similarly, we perform the 16th round, in the last round we select the 16th row of S-box and permutation P_{16} for further utilization using the same pattern to obtained $\{y_1, y_2, y_3, \dots, y_{16}\}$ that lies in the range 0 to 255. This is 16 bytes or 128-bit ciphertext. In an image encryption scheme we use three different S-boxes which are constructed by using the scheme in [17] for the encryption of different layers are given below.

Table 7.1(a): S-box 1.

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

Table 7.1(b): S-box 2.

165	216	29	114	142	192	244	88	71	224	167	62	122	76	186	102
173	144	157	222	221	85	152	128	61	160	170	131	93	75	150	42
108	72	237	137	57	111	81	46	96	164	86	195	44	64	138	94
112	80	208	34	31	207	74	169	38	171	139	12	51	21	110	225
54	56	95	35	248	13	213	140	146	129	78	26	166	37	4	97
48	19	136	193	43	203	30	99	22	151	103	14	69	55	147	65
36	40	87	209	202	17	91	217	185	233	196	251	23	218	77	121
82	219	141	119	239	6	179	187	32	132	236	205	47	254	50	252
27	24	84	223	161	68	1	79	124	155	204	188	228	15	176	92
73	11	49	220	39	189	45	148	83	172	105	9	2	199	245	162
28	135	130	229	159	238	198	107	52	235	194	242	70	191	5	175

206	197	59	100	104	7	60	123	156	149	8	154	190	174	183	182
18	41	89	113	0	200	53	246	101	249	184	67	163	215	158	214
210	16	247	115	98	118	90	120	133	153	125	10	168	25	58	145
20	227	63	231	230	181	240	234	134	3	177	143	226	211	241	201
250	66	116	212	243	232	180	117	109	127	33	255	178	126	106	253

Table 7.1(c): S-box 3.

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

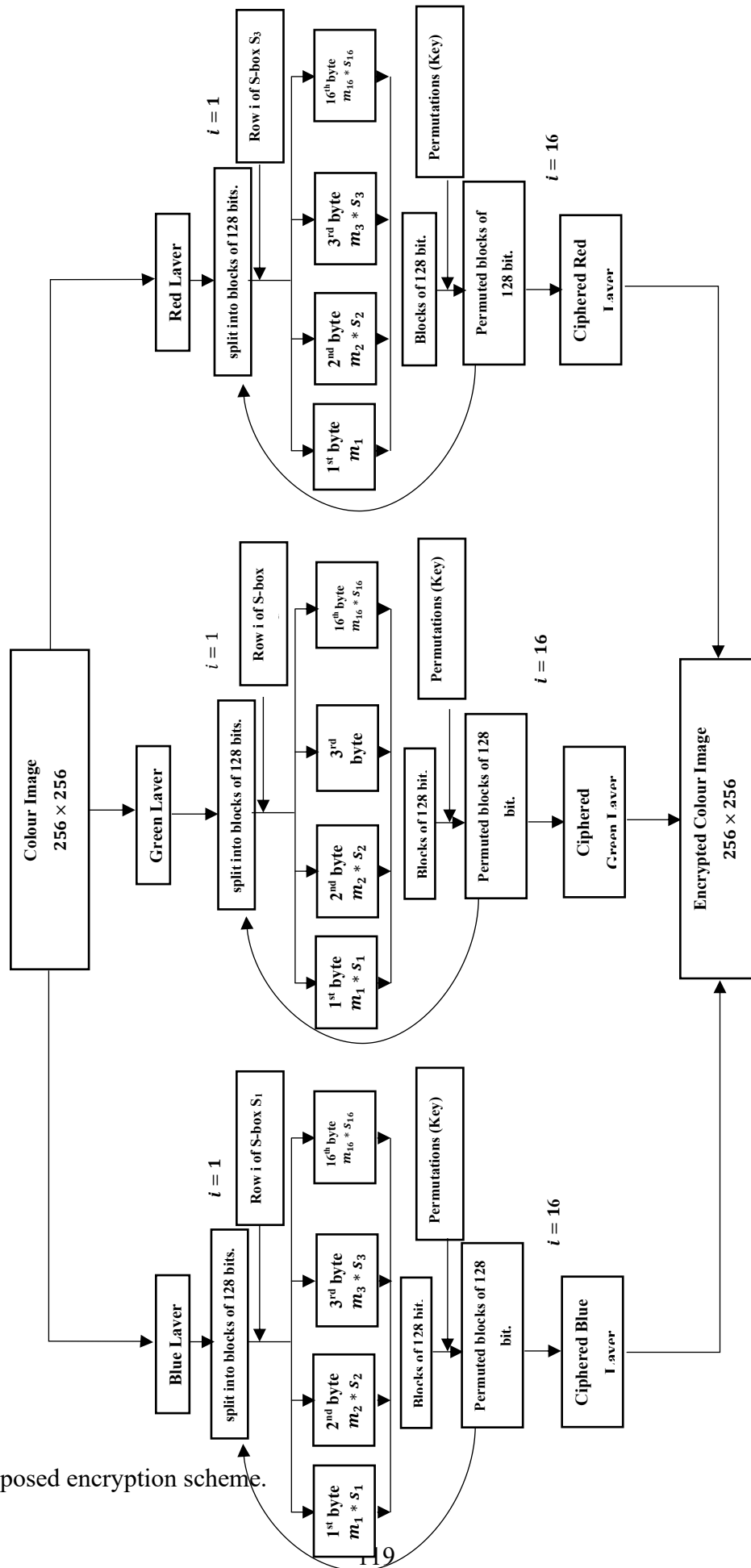


Fig. 7.1. Proposed encryption scheme.

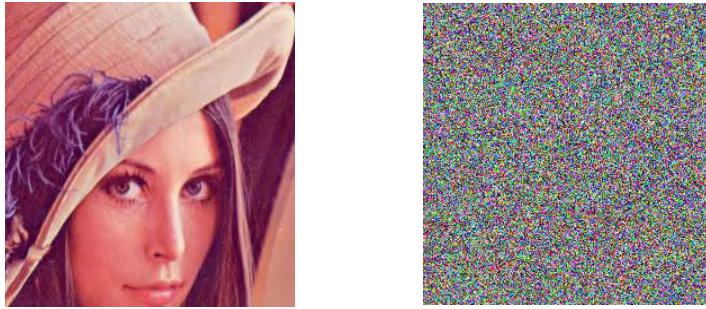


Fig. 7.2. Original and Encrypted Lena Image of dimension 256×256

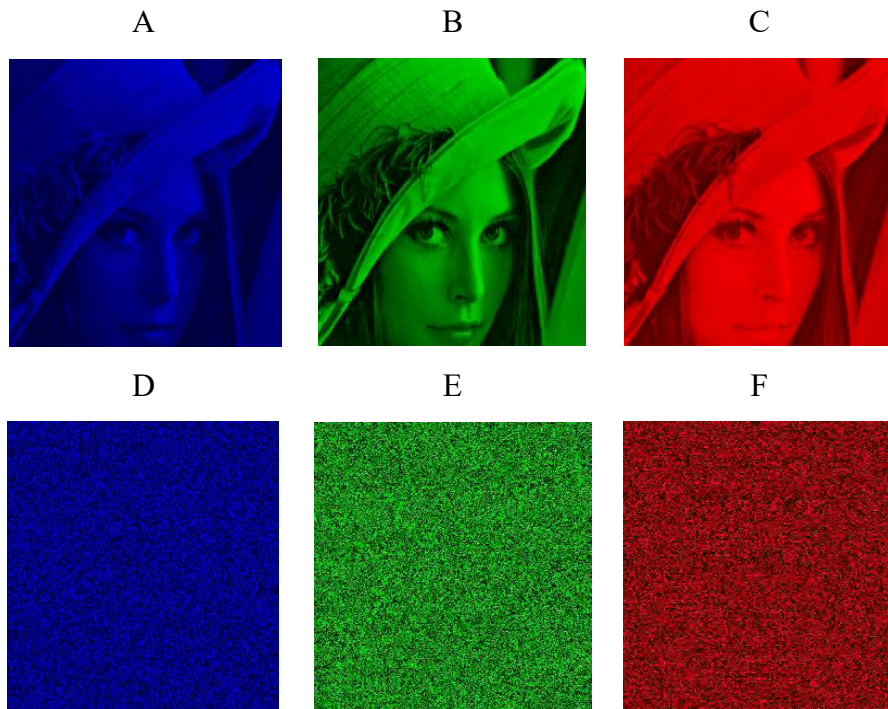


Fig. 7.3. Layer-wise original images of Lena (A)-Blue, (B)-Green, (C)-Red, (D)-Encrypted Blue, (E)- Encrypted Green, (F)- Encrypted Red



Fig. 7.4. Original and Encrypted Baboon Image of size 256×256 .

7.3 Investigational Upshots and Simulation Analyses

In any investigation of designed cryptosystems, the ultimate gauge is to measure the outcomes of different analyses. The astonishing fact connected to any research is the disclosure of false outcomes after a long and hectic tiresome job. Sometimes, for scientists and engineers, it becomes hard to identify the wrong step. Still, it's an interesting task for many. The efficacy of any scheme is established right after the complete investigation of analyses. For this argument, simulation analyses of the proposed scheme are given hereafter.

7.3.1 Key Space Analysis

In this analysis, the total number of keys used in the algorithm is debated. If the total volume of keys used in a cryptosystem is higher than it bears more strength against any exhaustive key search. For a chaotic cryptosystem, the key space greater than 2^{100} [104] is proposed as secure enough.

7.3.2 Key Sensitivity Analysis

Key sensitivity is an essential criterion to be fulfilled by a robust cryptosystem. This assures that any wrong guess will change the output obtained from enciphering algorithm. Conversely, with a wrong set of keys, the decryption should generate a different and wrong original input. IP-loop used in this article successfully satisfies the sensitivity test.

7.3.3 Correlation Analysis

Pixels are building blocks of images. These are numeric values that are highly correlated with neighboring pixels in all three directions i.e. horizontally, vertically, and diagonally. In an enciphered image, the correlation values must approach zero. This is the main objective of the cryptographic algorithm to achieve in any scheme of image encryption proposed by researchers. As result, the rearrangement of pixel values to the original one becomes extremely difficult for an assaulter.

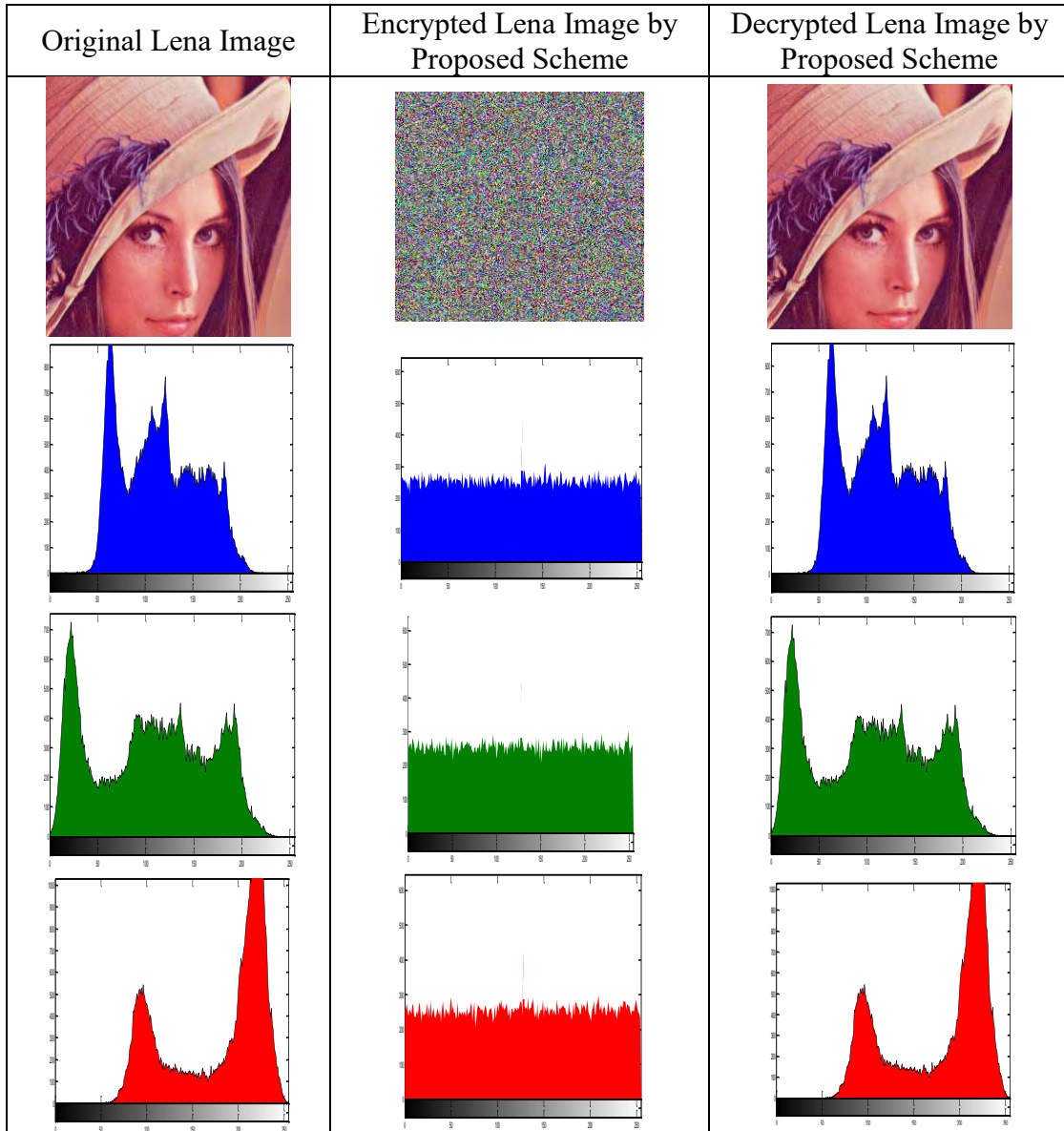


Fig. 7.5: layer-wise analysis of Lena image and their histograms.

Table 7.2 Correlation analysis of proposed scheme compare other well-known schemes.

Image	Layer	Horizontal			Vertical			Diagonal		
		Blue	Green	Red	Blue	Green	Red	Blue	Green	Red
Original Lena image	Blue	0.826	0.781	0.591	0.928	0.872	0.671	0.839	0.829	0.613
	Green	0.840	0.928	0.609	0.911	0.945	0.616	0.786	0.890	0.611
	Red	0.629	0.817	0.937	0.823	0.833	0.958	0.623	0.833	0.957
Encrypted Lena Image by the proposed scheme	Blue	0.0069	0.022	0.0001	0.0055	0.781	0.591	0.0006	-0.0262	-0.0175
	Green	-0.0023	-0.022	-0.0175	0.00034	0.928	0.609	0.0001	0.0078	0.0006

	Red	-0.0055	-0.0002	0.0003	0.00023	-0.0262	-0.022	-0.0023	0.0003	0.0002
Encrypted Lena Image by Ref. [102]	Blue	-0.0024	-0.0032	0.0035	0.0002	-0.0034	0.0092	0.0081	-0.0052	-0.0031
	Green	-0.0261	-0.0055	0.0069	0.0631	0.0002	-0.0302	-0.0043	0.0123	0.0002
	Red	-0.0183	-0.022	0.0078	0.0003	0.0055	0.0078	-0.0021	-0.0023	-0.0031
Encrypted Lena Image by Ref. [100]	Blue	-0.0001	0.0002	0.0001	-0.0002	0.0002	0.0003	0.00023	0.00034	-0.0002
	Green	-0.0004	-0.0004	0.0005	-0.0003	0.0006	-0.0005	0.0006	-0.0005	-0.0005
	Red	0.0001	0.0007	-0.0006	0.0002	-0.0005	0.0006	-0.0005	0.0008	0.0002
Encrypted Lena Image by Ref. [104]	Blue	-0.0099	-0.0034	-0.0066	-0.0035	-0.0067	-0.0097	-0.0068	-0.0095	-0.0038
	Green	-0.0260	-0.0220	-0.0175	-0.0023	-0.0176	-0.0262	-0.0176	-0.0262	-0.0225
	Red	-0.0072	-0.0201	-0.0016	-0.0205	-0.0017	-0.0073	-0.0017	-0.0073	-0.0203

7.4 Histogram Analysis

Histogram analysis of an image provides information about tonal distribution. This graph is obtained by plotting the total amount of pixels in a certain tone along the y-axis whereas the x-axis represents a single tonal value. The lighter and darker portion of images is represented on the left and right side of graph respectively. The scheme of encryption tries to distort the original combination of pixels which makes the histogram flat as well after these operations.

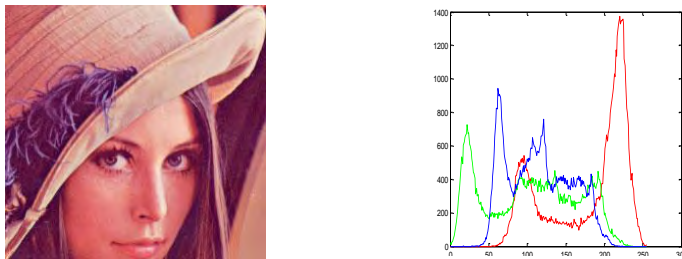
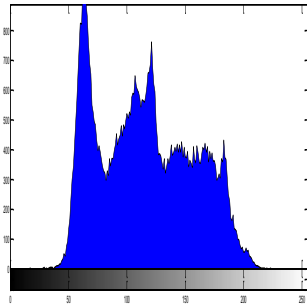


Fig. 7.6: Histogram of original Lena image.

Blue Image (Original)



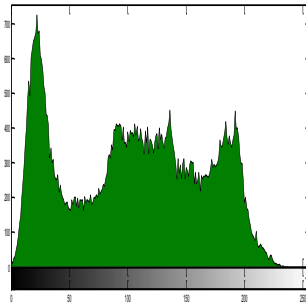
Histogram of Blue layer



Blue Image (Original)



Histogram of Green layer



Red Image (Original)



Histogram of Red layer

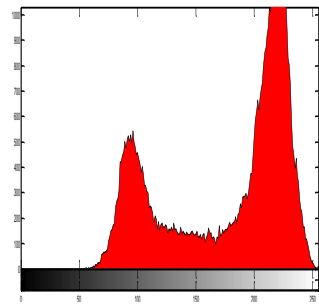
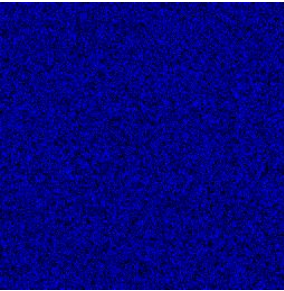
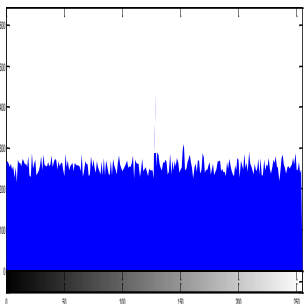


Fig. 7.7: Layer wise view of Lena image and their histograms

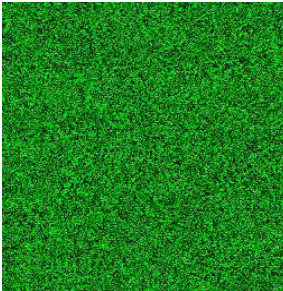
Encrypted Image (Blue)



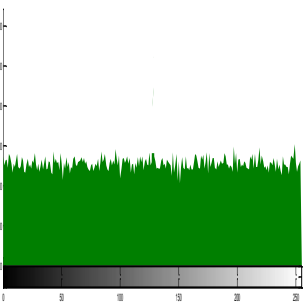
Histogram of Blue layer



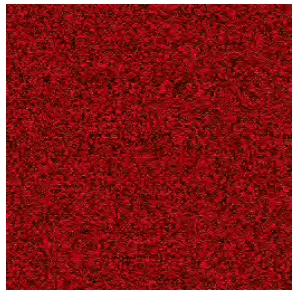
Encrypted Image (Green)



Histogram of Green layer



Encrypted Image (Red)



Histogram of Red layer

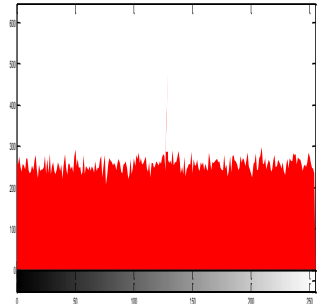
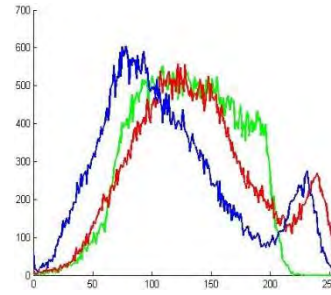


Fig. 7.8: Encrypted Lena image layer-wise and their histograms.

Original Baboon image



Original Histogram



Encrypted Baboon image



Encrypted Histogram

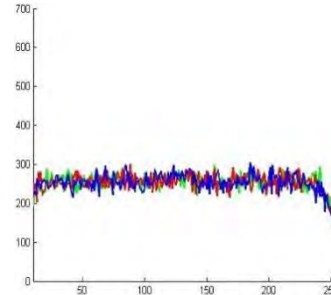


Fig. 7.9: Histogram Analysis of the original and Encrypted Baboon image.

7.5 Differential Analyses

Differential analyses are sometimes also known as sensitivity analyses. These are used to retrace/retrieve an original image. There are two major divisions of these namely number of pixels change rate (NPCR) and unified average changing intensity (UACI).

7.5.1 NPCR AND UACI

NPCR measures the effect of change on an encrypted image by varying only a single bit. It tells us the number of pixels changed by this increment [87]. Its standard value showing a good encryption scheme lies nearer to 99 using its formula mentioned at the end of this paragraph. This affirms its strength against differential analysis. Whereas unified average change intensity (UACI) measures the difference of intensities between original and enciphered images. Its value that is considered acceptable lies nearer to 33%.

Table 7.3 NPCR and UACI analyses of the proposed scheme.

Images	Layer	NPCR			UACI		
		Proposed	Ref [102]	Ref [104]	Proposed	Ref [102]	Ref [104]
Lena	Blue	99.61	99.60	99.63	33.54	30.56	33.63
	Green	99.62	99.62	99.64	33.53	34.42	33.51
	Red	99.59	99.58	99.60	33.53	34.56	33.57
Baboon	Blue	99.61	99.01	99.57	33.54	30.59	33.51
	Green	99.62	99.62	99.61	33.53	33.43	33.59
	Red	99.59	99.63	99.62	33.53	34.55	33.66
Airplane	Blue	99.61	99.02	99.60	33.54	30.56	33.60
	Green	99.62	99.63	99.63	33.53	33.43	33.59
	Red	99.59	99.61	99.62	33.53	34.55	33.63

7.6 Chi-Square Test

Since pixels are building blocks of digital images. These are highly correlated with each other in neighboring regions to produce a certain kind of shade. Their distribution in terms of uniformity is measured statistically by using the Chi-square test while the same is analyzed pictorially in histogram analysis. In the Chi-square test, the observed and expected values are used to attain a significance level. The formula is given as:

$$X^2 = \sum_{i=0}^{255} \frac{(\text{expected value} - \text{Observed value})^2}{\text{expected value}} \quad (7.1)$$

Here, i represent the intensity level of the image and the expected value is 256 for 256×256 images. The outcomes are verified in the chi-square distribution table with 0.05 and 0.01 significance levels. For 255 degrees of freedom, the critical values with 0.05 and 0.01 probability are 293.2478 and 310.457 respectively. Table 7.4 shows the chi-square values generated from the encrypted Lena image using the proposed scheme. It also reveals that the hypothesis is accepted with 0.05 and 0.01 levels of significance, which means the pixel distribution is uniform.

Table 7.4 CHI-SQUARE Analyses of the proposed scheme.

Image	Layer	$\chi^2 - Value$	$P - Value$	Decision
Original Image	Blue	256.00	0.529	Accepted
	Green	255.9883	0.529	Accepted
	Red	250.9375	0.439	Accepted
Encrypted Image	Blue	244.8673	0.329	Accepted
	Green	245.6417	0.325	Accepted
	Red	244.4384	0.323	Accepted

7.7 Time Execution Performance

The present-day world is focusing on the time taken by the machines to complete their assignment. Old fashioned devices consume more time and hence energy in achieving their goals. The same is the idea here that any proposed scheme should execute its job in a short interval of time. For bigger real-life data, the execution time should be minimized to seconds and even lesser. For calculating the time of the proposed work, we use a system having Processor: Intel R CoreTMi7-8565U CPU @ 1.8GHz 1.99 GHz, RAM: 8 GB, and operating system: 64 Bit operating system ×64-based processor. The language used here is python version 3.6.

Table 7.5 Time execution Analyses of the proposed scheme.

Images	Used Schemes	Encryption Time (sec)	Decryption Time (sec)
Lena Image	Proposed	8.92672	8.89861
	Ref [102]	10.07052	10.1475
	Modified Serpent Ref [104]	31.31250	15.3593
	Classical Serpent Ref [104]	63.0000	63.8281
	Classical AES Ref [25]	52.68941	52.52367

7.8 Information Entropy

This analysis deals with the level of randomness achieved. The amount of randomness gives the impression of the true efficacy of a cryptosystem. Information entropy (IE) calculates this randomness and unpredictability as defined by the equation defined below, where the probability of random variable u_j is used to calculate IE. The best optimal value of an encrypted image is 8. Any kind of enciphering technique generating the outcomes of IE nearer to 8 is considered as robust and secure. Such encrypted images are when observed pictorially, generate a flat histogram curve i.e. authenticating randomness and unpredictability. Table 7.6 represents the outcomes of IE of the proposed scheme vs some well-known cryptosystems.

$$IE(H) = -\sum P(u_j) \log_2 P(u_j) \quad (7.2)$$

Where $P(u_j)$ denotes the probability of a r.v u at j th index.

Table 7.6 Information Entropy Analyses of the proposed scheme.

Images	Layer	Proposed	Ref [102]	Ref [100]	Ref [104]
Lena Image	Blue	7.9895	7.9888	7.9889	7.9885
	Green	7.9894	7.9890	7.9982	7.9882
	Red	7.9891	7.9882	7.9981	7.9893
Baboon Image	Blue	7.9987	7.9990	7.9977	7.9985
	Green	7.9988	7.9989	7.9974	7.9969
	Red	7.9978	7.9987	7.9981	7.9973
Pepper Image	Blue	7.9972	7.9988	7.9968	7.9987
	Green	7.9990	7.9991	7.9972	7.9977
	Red	7.9989	7.9992	7.9986	7.9972

Chapter 8

Conclusion and Future Directions

A brief and accurate description of the results obtained in this dissertation is discussed in this chapter. Moreover, some questions that arise during this research work are also included.

The main objectives achieved by this research presented here can be categorized into the following four categories.

1. Introducing non-associative algebraic structures for the construction of strong and secure S-boxes to enhance encryption security level incorporating them.
2. The aim is to construct a more secure and large number of S-boxes instead of achieving a single S-box using a group of permutation and group action techniques over non-associative structures.
3. By utilizing these non-associative structures modify the designs of the Rijndael algorithm presented by Joan Daemen and Vincent Rijmen and the Serpent algorithm presented by Eli Biham, Ross Anderson, and Lars Knudsen.
4. To design novel image encryption and watermarking techniques in multimedia security using these S-boxes.

8.1 Conclusion

In the beginning, non-associative structure IP-loop, is introduced for the design of a highly nonlinear component of a block cipher. The ultimate goal is to enhance the security level of various crypto algorithms. The interesting feature of this structure is the availability of a large number of IP-loops due to the non-associativity. For example, S-boxes over IP-loop with 256 elements, it takes millions of years to find all possible IP-loops of order 256. These constructions have better security analysis and portray a high level of randomness.

As for as chapter three is concerned, a watermarking scheme and majority logic criterion are used to examine the strength of S-boxes constructed over IP-loop. The ways for transferring data have been changed due to the vast technology of the internet and communication. Due to this vast technology, disputes arise for the reliability and integrity of information or data. These S-boxes show excellent confusion and diffusion properties in image encryption. In the proposed technique of watermark, the plain image is not necessarily needed amid the extraction procedure. Mostly it is observed that a private key is used to generate the arbitrary arrangement during the insert process. Which shows that the projected technique lies in the category of blind watermarking. The simulation results have made sure the strength against different signal attacks and strategies of the suggested scheme.

In chapter four a cryptographic encryption standard is proposed whose model is the same as presented in Rijndael Algorithm by Joan Daemen and Vincent Rijmen. The modification lies in the design of the cipher, we have used IP-loop instead of extended binary Galois field. The encryption and decryption scheme are modified using a single binary operation of IP-loop and the XOR Boolean operator. Our proposed mathematical structure is superior to Galois field in terms of complexity and can create arbitrary randomness due to a larger key space. Moreover, IP-loop is non-isomorphic and has more than one Cayley table representation as compared to the Galois field.

This in result confirms the resistance against cryptanalytic attacks specifically on mathematical structures.

As for as chapter five is concerned construction technique for S-boxes by utilizing a PA-loop another non-associative structure is presented. This includes fewer constraints as compared to the Galois field and cyclic groups like non-associativity and inverse of zero element and it is more general than IP-loop. This technique generates more S-boxes as compared to the many other existing algorithms. In addition to this, the implementation of an asymmetric group enhances the quantity of these components having competitive strength with well-known S-boxes.

In chapter six of this dissertation, Mobius transformation is used to construct highly nonlinear S-boxes over PA-loop. The utilization of these structures for the construction of S-boxes yielded fruitful results like high nonlinearity, appropriate BIC and SAC outcomes and excellent LP and DP values. This encourages to utilization of non-associative structures in AES, DES, Serpent, and as well as any other cryptosystems.

In the last chapter, an image encryption scheme based on the serpent algorithm is presented. In this scheme, we used the S-boxes which we constructed in chapter six. This scheme has less round due to which time execution is shorted as compared to serpent but show better results. The advantage of using this structure is it includes 128 bits keys along with a PA-loop of order 256. If an attacker has the knowledge of the key but does not have any information about the loop, he cannot succeed to break this. Moreover, the proposed mathematical system is noncommutative making it harder to break. Different analyses were used to investigate the proposed scheme to verify its strength. All the standard tests were showing fruitful results ensuring their practical applications.

8.2 Future directions

While going through this research work few questions come to mind but remained unanswered. These questions may be an extension of this research done in our dissertation or may be well thought out in the future. Some of these questions are given below.

1. Construct robustness and secure component for block ciphers (S-boxes) using non-associative structures having optimal nonlinearity and a greater number of input bits to resist the several linear and differential attacks.
2. To utilize these special types of block ciphers in multimedia security such as image encryption application, watermarking, audio and video steganography.
3. Utilization of various non-associative structures like Moufang loop, Weak IP-loop for the construction of S-boxes.

References

- [1] Burnett, L. D. (2005). Heuristic optimization of Boolean functions and S-boxes for cryptography (Doctoral dissertation, Queensland University of Technology).
- [2] Jansen, C. J. A., & Boekee, D. E. (1987). The algebraic normal form of arbitrary functions over finite fields. In Proc. 8th Symposium of Information Theory in the Benelux.
- [3] Hussain, I., & Shah, T. (2013). Literature survey on nonlinear components and chaotic nonlinear components of block ciphers. *Nonlinear Dynamics*.
- [4] Meier, W., & Staffelbach, O. (1989). Nonlinearity criteria for cryptographic functions. In Workshop on the Theory and Application of Cryptographic Techniques. Springer, Berlin, Heidelberg.
- [5] Feistel, H. (1973). Cryptography and computer privacy. *Scientific American*.
- [6] Kam, J. B., & Davida, G. I. (1979). Structured design of substitution-permutation encryption networks. *IEEE Transactions on Computers*.
- [7] Biham, E., Anderson, R., & Knudsen, L. (1998). Serpent: A new block cipher proposal. In International workshop on fast software encryption. Springer, Berlin, Heidelberg.
- [8] Mar, P. P., & Latt, K. M. (2008). New analysis methods on strict avalanche criterion of S-boxes. *World Academy of Science, Engineering and Technology*.
- [9] Pflugfelder, H. O. (2000). Historical notes on loop theory. *Commentationes Mathematicae Universitatis Carolinae*.
- [10] Asif, A., & Slaney, J. (2008). Counting loops with the inverse property. *Quasigroups and Related Systems*.
- [11] Bruch, H. Richard. (1971). A survey of binary systems. Berlin: Springer.
- [12] Al-Saidi, N. M., Said, M. R. M., & Mohammed, A. J. (2012). Finite and Infinite Field Cryptography Analysis and Applications. In International Conference on Applied Mathematics and Pharmaceutical Sciences.

- [13] Shannon, C. E. (1949). Communication theory of secrecy systems. Bell system technical journal.
- [14] Rijmen, V., & Daemen, J. (2001). Advanced encryption standard. Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology.
- [15] Standard, D. E. (1999). Data encryption standard. Federal Information Processing Standards Publication.
- [16] Ullah, A., Jamal, S. S., & Shah, T. (2017). A novel construction of a S-box using a combination of chaotic maps with improved chaotic range. *Nonlinear Dynamics*.
- [17] Shah, T., Qamar, A., & Hussain, I. (2013). S-box on maximal cyclic subgroup of units of a Galois ring. *Zeitschrift für Naturforschung A*.
- [18] Jamal, S. S., Shah, T., & Attaullah, A. (2017). A group action method for construction of strong S-box. *3D Research*.
- [19] Hussain, I., Shah, T., & Mahmood, H. (2010). A new algorithm to construct secure keys for AES. *International Journal of Contemporary Mathematical Sciences*.
- [20] Naseer, Y., Shah, T., Shah, D., & Hussain, S. (2019). A Novel Algorithm of Constructing Highly Nonlinear Sp-boxes. *Cryptography*.
- [21] Hussain, I., Shah, T., Mahmood, H., & Gondal, M. A. (2013). A projective general linear group-based algorithm for the construction of S-box for block ciphers. *Neural Computing and Applications*.
- [22] Ahmad, M., Doja, M. N., & Beg, M. S. (2018). ABC optimization-based construction of strong substitution-boxes. *Wireless Personal Communications*.
- [23] De Andrade, A. A., & Palazzo Jr, R. (1999). Construction and decoding of BCH codes over finite commutative rings. *Linear Algebra and Its Applications*.

- [24] Naseer, Y., Shah, T., Hussain, S., & Ali, A. (2019). Steps Towards Redesigning Cryptosystems by a Non-associative Algebra of IP-loops. *Wireless Personal Communications*.
- [25] Daemen, J., & Rijmen, V. (2013). *The design of Rijndael: AES-the advanced encryption standard*. Springer Science & Business Media.
- [26] Shankar, P. (1979). On BCH codes over arbitrary integer rings. *IEEE Transactions on Information Theory*.
- [27] Hussain, I., Shah, T., Mahmood, H., & Gondal, M. A. (2012). Construction of S8 Liu J S-boxes and their applications. *Computers & Mathematics with Applications*.
- [28] Kinyon, M. K., & Kunen, K. (2006). Power-associative, conjugacy closed loops. *Journal of Algebra*.
- [29] Altaleb, A., Saeed, M. S., Hussain, I., & Aslam, M. (2017). An algorithm for the construction of S-box for block ciphers based on projective general linear group. *AIP Advances*.
- [30] Hussain, I., Shah, T., Gondal, M. A., & Mahmood, H. (2012). Generalized majority logic criterion to analyze the statistical strength of S-boxes. *Zeitschrift für Naturforschung*.
- [31] Huang, C. K., Liao, C. W., Hsu, S. L., & Jeng, Y. C. (2013). Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system. *Telecommunication Systems*.
- [32] Loukhaoukha, K., Chouinard, J. Y., & Berdai, A. (2012). A secure image encryption algorithm based on Rubik's cube principle. *Journal of Electrical and Computer Engineering*.
- [33] Sathishkumar, G. A., & Sriraam, D. N. (2011). Image encryption based on diffusion and multiple chaotic maps. *arXiv preprint arXiv*.
- [34] Huang, C. K., & Nien, H. H. (2009). Multi chaotic systems-based pixel shuffle for image encryption. *Optics communications*.

- [35] Daemen, J., & Rijmen, V. (2002). The design of Rijndael (Vol. 2). New York: Springer-verlag.
- [36] Fouda, J. A. E., Effa, J. Y., Sabat, S. L., & Ali, M. (2014). A fast-chaotic block cipher for image encryption. *Communications in Nonlinear Science and Numerical Simulation*.
- [37] Kadhim, F. A., Abdul-Majeed, G. H., & Ali, R. S. (2017, March). Enhancement CAST block algorithm to encrypt big data. In *2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT)*. IEEE.
- [38] Farhan, A. K., Al-Saidi, N. M., Maolood, A. T., Nazarimehr, F., & Hussain, I. (2019). Entropy Analysis and Image Encryption Application Based on a New Chaotic System Crossing a Cylinder. *Entropy*.
- [39] Farhan, A. K., Ali, R. S., Natiq, H., & Al-Saidi, N. M. (2019). A New S-box Generation Algorithm Based on Multistability Behavior of a Plasma Perturbation Model. *IEEE Access*.
- [40] Asif, M., & Shah, T. (2019). BCH Codes with computational approach and its applications in image encryption. *Journal of Intelligent & Fuzzy Systems*.
- [41] Shah, D., Shah, T., & Jamal, S. S. (2019). A novel efficient image encryption algorithm based on affine transformation combine with linear fractional transformation. *Multidimensional Systems and Signal Processing*.
- [42] Akhtar, T., Din, N., & Uddin, J. (2019). S-box design based on chaotic maps and cuckoo search algorithm. In *2019 International conference on advanced communication technologies and networking (CommNet)*. IEEE.
- [43] Shafique, A. (2020). A new algorithm for the construction of S-box by using chaotic map. *The European Physical Journal Plus*.
- [44] Lambić, D. (2020). A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design. *Nonlinear Dynamics*.

- [45] Javeed, A., Shah, T., & Ullah, A. (2020). Construction of non-linear component of block cipher by means of chaotic dynamical system and symmetric group. *Wireless Personal Communications*.
- [46] Kim, J., & Phan, R. C. W. (2009). Advanced differential-style cryptanalysis of the NSA's skipjack block cipher. *Cryptologia*.
- [47] Abuelyman, E. S., Alsehibani, A. A. S., & Arabia, S. (2008). An optimized implementation of the S-box using residue of prime numbers. *International Journal of Computer Science and Network Security*.
- [48] Hussain, I., Anees, A., AlKhalidi, A. H., Algarni, A., & Aslam, M. (2018). Construction of chaotic quantum magnets and matrix Lorenz systems S-boxes and their applications. *Chinese Journal of Physics*.
- [49] Wang, X., Zhu, X., & Zhang, Y. (2018). An image encryption algorithm based on Josephus traversing and mixed chaotic map. *IEEE Access*.
- [50] Shah, T., Hussain, I., Gondal, M. A., & Mahmood, H. (2011). Statistical analysis of S-box in image encryption applications based on majority logic criterion. *International Journal of Physical Sciences*.
- [51] Shi, X.; Xiao, XYH; Lam, K. (2002). A method for obtaining cryptographically strong 8×8 S-boxes. *Int. Conf. Inf. Netw. Appl.*
- [52] Tran, M. T., Bui, D. K., & Duong, A. D. (2008). Gray S-box for advanced encryption standard. In *2008 international conference on computational intelligence and security*. IEEE.
- [53] Cui, J., Zhong, H., Wang, J., & Shi, R. (2014). Generation and optimization of Rijndael S-box equation system. *Information Technology Journal*.
- [54] Hussain, I., Shah, T., & Aslam, S. K. (2011). Graphical SAC analysis of S 8 APA S-box. *International Journal of Difference Equations*.

- [55] I. J. Cox, J. Kilian, F. T. Leighton, T. Shamoon. (1997). Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*.
- [56] Tran, M. T., Bui, D. K., & Duong, A. D. (2008). Gray S-box for advanced encryption standard. In 2008 International Conference on Computational Intelligence and Security. IEEE.
- [57] Cui, L., & Cao, Y. (2007). A new S-box structure named Affine-Power-Affine. *International Journal of Innovative Computing, Information and Control*.
- [58] Chang, H. K. C., & Liu, J. L. (1997). A linear quadtree compression scheme for image encryption. *Signal Processing: Image Communication*.
- [59] Adams, C., & Tavares, S. (1990). The structured design of cryptographically good S-boxes. *Journal of cryptology*.
- [60] Nyberg, K. (1991). Perfect nonlinear S-boxes. In *Workshop on the Theory and Application of Cryptographic Techniques*. Springer, Berlin, Heidelberg.
- [61] O'connor, L. (1994). An analysis of a class of algorithms for S-box construction. *Journal of Cryptology*.
- [62] Jamal, S. S., Khan, M. U., & Shah, T. (2016). A watermarking technique with chaotic fractional S-box transformation. *Wireless Personal Communications*, 90(4).
- [63] 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)*.
- [64] Liao, X., Lai, S., & Zhou, Q. (2010). A novel image encryption algorithm based on self-adaptive wave transmission. *Signal processing*.
- [65] Khan, M., Shah, T., & Batool, S. I. (2017). A new approach for image encryption and watermarking based on S-box over the classes of chain rings. *Multimedia Tools and Applications*.

- [66] Webster, A. F., & Tavares, S. E. (1985). On the design of S-boxes. In Conference on the theory and application of cryptographic techniques. Springer, Berlin, Heidelberg.
- [67] Rashid, A. (2016). Digital watermarking applications and techniques: a brief review. International Journal of Computer Applications Technology and Research.
- [68] Dabas, P., & Khanna, K. (2013). A study on spatial and transform domain watermarking techniques. International journal of computer applications.
- [69] Coppersmith, D., Johnson, D. B., & Matyas, S. M. (1996). A proposed mode for triple-DES encryption. IBM Journal of Research and Development.
- [70] Joan, D., & Vincent, R. (2002). The design of Rijndael: AES-the advanced encryption standard. In Information Security and Cryptography. springer.
- [71] Shannon, C. E. (1948). A mathematical theory of communication. The Bell system technical journal.
- [72] Shah, T., Ali, A., Khan, M., Farooq, G., & de Andrade, A. A. (2020). Galois Ring $GR(2^3, 8)$ Dependent 24×24 S-box Design: An RGB Image Encryption Application. Wireless Personal Communications.
- [73] Jahangir, S., & Shah, T. (2017). Designing S-boxes triplet over a finite chain ring and its application in RGB image encryption.
- [74] Javeed, A., & Shah, T. (2019). Cryptosystem techniques based on the improved Chebyshev map: an application in image encryption. Multimedia Tools and Applications.
- [75] Meshram, C., Obaidat, M. S., & Meshram, S. G. (2018). Chebyshev chaotic map-based ID-based cryptographic model using subtree and fuzzy-entity data sharing for public key cryptography. Security and Privacy.
- [76] Khan, M., & Asghar, Z. (2018). A novel construction of S-box for image encryption applications with Ginger breadman chaotic map and S_8 permutation. Neural Computing and Applications.

- [77] Alghafis, A., Munir, N., Khan, M., & Hussain, I. (2020). An Encryption Scheme Based on Discrete Quantum Map and Continuous Chaotic System. *International Journal of Theoretical Physics*.
- [78] Ahmad, M., Doja, M. N., & Beg, M. S. (2018). Security analysis and enhancements of an image cryptosystem based on hyperchaotic system. *Journal of King Saud University-Computer and Information Sciences*.
- [79] Ullah, A., Jamal, S. S., & Shah, T. (2018). A novel scheme for image encryption using S-box and chaotic system. *Nonlinear Dynamics*.
- [80] Naseer, Y., Shah, D., & Shah, T. (2019). A novel approach to improve multimedia security utilizing 3D mixed chaotic map. *Microprocessors and Microsystems*.
- [81] Javeed, A., & Shah, T. (2020). Lightweight secure image encryption scheme based on chaotic differential equation. *Chinese Journal of Physics*.
- [82] Javeed, A., & Shah, T. (2020). Design of an S-box using Rabinovich-Fabrikant system of differential equations perceiving third order nonlinearity. *Multimedia Tools and Applications*.
- [83] Chai, X., Chen, Y., & Broyde, L. (2017). A novel chaos-based image encryption algorithm using DNA sequence operations. *Optics and Lasers in engineering*.
- [84] Li, X., Wang, L., Yan, Y., & Liu, P. (2016). An improvement colour image encryption algorithm based on DNA operations and real and complex chaotic systems. *Optik*.
- [85] Naseer, Y., Shah, T., & Javeed, A. (2020). Advance image encryption technique utilizing compression, dynamical system and S-boxes. *Mathematics and Computers in Simulation*.
- [86] Khan, M., & Shah, T. (2014). A novel image encryption technique based on Hénon chaotic map and S_8 symmetric group. *Neural Computing and Applications*.
- [87] Paar, C., & Pelzl, J. (2009). *Understanding cryptography: a textbook for students and practitioners*. Springer Science & Business Media.

- [88] Kathleen, T., Tim, D., & James, A. (1996). CHAOS: an introduction to dynamical systems. Springer, New York, NY, USA.
- [89] Hussain, S., Jamal, S. S., Shah, T., & Hussain, I. (2020). A PA-loop Structure for the Construction of Non-Linear Components of Block Cipher. IEEE Access.
- [90] 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.
- [91] Biham, E., Anderson, R., & Knudsen, L. (1998). Serpent: A new block cipher proposal. In International workshop on fast software encryption. Springer, Berlin, Heidelberg.
- [92] Nandi, S., Roy, S., Nath, S., Chakraborty, S., Karaa, W. B. A., & Dey, N. (2014). 1-D group cellular automata-based image encryption technique. In 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT). IEEE.
- [93] Behnia, S., Akhshani, A., Mahmodi, H., & Akhavan, A. (2008). A novel algorithm for image encryption based on mixture of chaotic maps. Chaos, Solitons & Fractals, 35(2).
- [94] Zhu, C., Wang, G., & Sun, K. (2018). Cryptanalysis and improvement on an image encryption algorithm design using a novel chaos based S-box. Symmetry.
- [95] Pak, C., & Huang, L. (2017). A new color image encryption using combination of the 1D chaotic map. Signal Processing.
- [96] Chang, H. K. C., & Liu, J. L. (1997). A linear quadtree compression scheme for image encryption. Signal Processing: Image Communication.
- [97] Chen, C. S., & Chen, R. J. (2006, December). Image encryption and decryption using SCAN methodology. In 2006 Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'06). IEEE.
- [98] Ullah, A., Javeed, A., & Shah, T. (2019). A scheme based on algebraic and chaotic structures for the construction of S-box. Multimedia Tools and Applications.

- [99] Tanveer, M., Shah, T., Rehman, A., Ali, A., Siddiqui, G. F., Saba, T., & Tariq, U. (2021). Multi-Images Encryption Scheme Based on 3D Chaotic Map and S-box. IEEE Access.
- [100] Javeed, A., T. Shah, Attaullah. (2020). A color image privacy scheme established on nonlinear system of coupled differential equations. *Multimed Tools Appl.*
- [101] Ali, Y. H., & Rissan, H. A. (2016). Image encryption using block cipher based serpent algorithm. *Eng. Technol. J.*
- [102] Shah, T., Haq, T. U., & Farooq, G. (2020). Improved SERPENT Algorithm: Design to RGB Image Encryption Implementation. IEEE Access.
- [103] Shadangi, V., Choudhary, S. K., Patro, K. A. K., & Acharya, B. (2017). Novel Arnold scrambling based CBC-AES image encryption. *Int J Control Theory Appl.*
- [104] Izevbizua, P. O. (2015). Data security in the cloud using serpent encryption and distributed steganography. *European Scientific Journal, ESJ.*
- [105] Javeed, A., Shah, T. & Ullah, A. (2020). Construction of Non-linear Component of Block Cipher by Means of Chaotic Dynamical System and Symmetric Group. *Wireless Pers Communication.*
- [106] Javeed, A., & Shah, T. (2020). Lightweight secure image encryption scheme based on chaotic differential equation. *Chinese Journal of Physics.*
- [107] Y Naseer, T Shah, Attaullah, A Javeed. (2020). Advance image encryption technique utilizing compression, dynamical system and S-boxes, *Mathematics and Computers in Simulation.*
- [108] Javeed, A., T. Shah, Attaullah. (2020). Design of an S-box using Rabinovich-Fabrikant system of Differential Equations perceiving third order nonlinearity, *Multimedia Tools Appl.*
- [109] Elkamchouchi, H. M., Takieldean, A. E., & Shawky, M. A. (2018). A modified serpent based algorithm for image encryption. In 2018 35th National Radio Science Conference (NRSC). IEEE.

[110] IEEE Computer Society. Standards Committee. Working group of the Microprocessor Standards Subcommittee, & American National Standards Institute. (1985). IEEE standard for binary floating-point arithmetic. IEEE.

[111] Wang, X. Y., Yang, L., Liu, R., & Kadir, A. (2010). A chaotic image encryption algorithm based on perceptron model. *Nonlinear Dynamics*.

Turnitin Originality Report

Non-associative Structures for the Development and Application of Cryptosystems
Sadam Hussain .

by  turnitin

From CL QAU (DRSML)

- Processed on 18-Mar-2022 12:16 PKT
- ID: 1786972471
- Word Count: 26337

Similarity Index

15%

Similarity by Source

Internet Sources:

6%

Publications:

11%

Student Papers:

6%

sources:

- 1 4% match (student papers from 27-Aug-2018)
Submitted to Higher Education Commission Pakistan on 2018-08-27
- 2 1% match (Internet from 17-Dec-2021)
<https://www.techscience.com/cmcl/v71n1/45458/pdf>
- 3 < 1% match (student papers from 11-Nov-2016)
Submitted to Higher Education Commission Pakistan on 2016-11-11
- 4 < 1% match (student papers from 28-Mar-2013)
Submitted to Higher Education Commission Pakistan on 2013-03-28
- 5 < 1% match (student papers from 31-Mar-2013)
Submitted to Higher Education Commission Pakistan on 2013-03-31
- 6 < 1% match (student papers from 22-Apr-2013)
Submitted to Higher Education Commission Pakistan on 2013-04-22
- 7 < 1% match (student papers from 17-Jun-2014)
Submitted to Higher Education Commission Pakistan on 2014-06-17
- 8 < 1% match (student papers from 28-Jul-2011)
Submitted to Higher Education Commission Pakistan on 2011-07-28
- 9 < 1% match (Internet from 28-Oct-2019)
<https://link.springer.com/article/10.1007%2Fs00521-012-0914-5>
- 10 < 1% match (Internet from 09-Dec-2019)
<https://link.springer.com/article/10.1007%2Fs11761-018-0249-x>
- 11 < 1% match (Internet from 28-Oct-2021)
https://link.springer.com/article/10.1007/s11071-018-4056-x?code=b81accb2-b7c8-49d7-a4ba-d04c56e40dde&error=cookies_not_supported
- 12 < 1% match (Internet from 21-Apr-2019)
<https://link.springer.com/content/pdf/10.1007%2F3-540-36231-2.pdf>
- 13 < 1% match (Internet from 23-Oct-2019)
<https://link.springer.com/article/10.1007%2Fs11277-017-5054-x>
- 14 < 1% match (Internet from 20-Aug-2019)
<https://link.springer.com/article/10.1007%2Fs11128-018-1958-y>

Sadam Hussain
Tamir
Chairman
Focal Person (Turnitin)
Quaid-i-Azam University
Islamabad

CHAIRMAN
Department of Mathematics
Quaid-i-Azam University
Islamabad