On S-Boxes and their Grading by Soft Sets Based Decision Making Methods

By

Sadia Medhit

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

2016

On S-Boxes and their Grading by Soft Sets

Based Decision Making Methods

By

Sadia Medhit

Supervised By

Prof. Dr. Tariq Shah

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

2016

On S-Boxes and their Grading by Soft Sets Based Decision Making Methods

By

Sadia Medhit

A Thesis Submitted in the Partial Fulfillment of the requirements for the Degree of

DOCTOR OF PHILOSOPHY

IN

MATHEMATICS

Supervised By

Prof. Dr. Tariq Shah

Department of Mathematics
Quaid-i-Azam University
Islamabad, Pakistan
2016

Dedicated to the driving force of my life and carrier,

Abbu Ji & Ammi Ji

Also, to the miracle of my life, Harum Fatima!

Contents

Acknowledgment

First and foremost, I would like to praise my Lord; Allah the Almighty, who has given me the opportunity to undertake and complete this work during challenging times. In addition, endless durood on my beloved Prophet Hazrat Muhammad (PBUH), whose words are an inspiration in every step of my life.

The thesis owes its existence to the help, valuable guidance and support of many people to bring it fruition. I wish to express my infinite gratitude and sincere appreciation to my supervisor and mentor, Prof. Dr. Tariq Shah, for his help, encouragement, patience, flexibility, concern and motivation supervision to complete my thesis. It is all due to his continuous efforts that I am able to write this work. He has always been a source of inspiration for me at Quaid-i-Azam University, right from my first day of M.Sc program in this great institution. He helped and supported me when I lost confidence in myself, and enlightened me whenever I need guidance. I am still unable to find any suitable words to explain my regards for him. I am forever grateful. Thank You Sir!

I am also thankful to the Higher Education Commission (HEC) for providing me financial support through Indigeneous Fellowship Program during my whole Ph.D. period.

Finally, I am obliged to my father and mother for all the sacrifies that they have made on my behalf. Their prayers for me are what sustained me thus far. I like to express appreciation to my siblings Bilal and Sara who have been a tremendous support for me throughout. Furthermore, thanks to all my friends who encouraged me in writing and incented me to strive towards my goals.

Sadia Medhit

Introduction

The process of making precise decisions to choose the suitable factor among several available factors is all about reducing the risk factors, ambiguities, and uncertainties. Indeed, the most reasonable set of choices depends on the fact that how much the option is better from the rest, based on some pre-agreed criteria. The decision-making process is influenced by several other factors such as methods, algorithms, and perceptions. It can happen that one particular method or algorithm is much efficient in decision making as compare to other methods. In general, this process begins with the setting up goals and collecting the information about those goals and its options. It also involves evaluation of the evidence in favor/against of every option and making choice of options with the strongest evidence. Finally, executing the decision.

In the area of communication sciences, various kinds of set theories have played an important role. The security of private and confidential information, especially during the data transfer, is one of the major concerns for the communication scientists. Moreover, the communication networks are vulnerable and exposed to several threats and risks. This gave rise to the development of new efficient network security techniques, not only for highly sensitive data but also for the common processes like transfer of images and passwords etc. Theoretical foundations of securing the data from unauthorized access were laid by Shannon, through his theorems and theoretical development of logic gates.

Most of the contemporary data encryption principles and concepts were proposed by Claude Elwood Shannon (1916-2001). Shannon [94] theoretically deduced the principles of confusion and diffusion that should be both present in a secure cryptosystem. The purpose of confusion is to make the relation between the key and the ciphertext as complex as possible (obtained by nonlinear transformations in the form of S-boxes). In the modern cryptosystems, one of the successful tools for the securing of data is the Substitution-box (or S-box). The S-box have been a subject of the substantial amount of research for the fact that it introduces the randomness in the data with minimal conditions. The basic intention is to produce the strongest possible S-boxes to control randomness in the data. The ability of functions, to configures the S-boxes plays a pivotal role in cryptographic systems. One of the key characteristics of the functions involved in configuration of S-boxes is that by introducing a small variation in parameters can generate completely different sequences and hence create randomness and secure cryptosystems. The modern research is focused on the investigation of such properties of S-box which can create the cryptographically strong ciphers. Block cipher systems depend only on the kind of S-boxes which are fixed and have no relation with a cipher key. Therefore, the only changeable parameter is the cipher key. In contrast to confusion and diffusion spreads the influence of a single plaintext bit over many ciphertext bits (obtained by linear transformations). The Gray Level Co-ocurrence Matrix (GLCM) is performed on AES [31], APA [29], Gray [101], Lui J [61], residue prime [1], S_8-AES [47], SKIPJACK [108], and Xyi [95] S-boxes.

The view of the soft sets enables the representation of information under the specific set of parameters. It involves other mathematical models and the soft set theory which is defined to make precise decisions algorithms. The soft set theory is used to present a study, in the context of decision-making for choosing the S-box. The proposed techniques allow the parameters of each cipher for analyzing through the soft sets theory. Different mappings are assign to each parameter. The given techniques can provide a useful way which efficiently help to judge the encryption results of different S-boxes.

In order to attain a specific level of certainty and precision in the data, several approaches have been adopted. The central reason for the problem of uncertainty is the notion of classical logic. It was concluded that the fundamental cause of uncertainty lies in the set theory based on classical logic. Russell's paradox is one of the examples that can describe the limitation of classical set theory. Molodtsov [72] introduced a convenient and easily applicable concept of soft set theory for modeling the uncertainties. There is no limited condition to the description of the objects, so researchers can choose the form of parameters they needed, which greatly simplifies the decision-making process and make the process more efficient in the absence of partial information. The soft set theory is free from the difficulties, whereas other existing methods which can be considered as mathematical tools for dealing with uncertainties, such as, probability theory, fuzzy set theory [Zadeh [105]], intuitionistic fuzzy set theory [Atanassov [8]], rough set theory [Pawlak [77]], neutrosophic set theory [Smarandache [96]] etc. have their own limitations. In general, these theories fail to recognize the formulation stages of a decision and typically(particularly) can only be applied to problems comprising two or more measurable alternatives. In response to such limitations, numerous descriptive theories have been developed over the last two decades, intended to describe how decisions are made. This work presents a framework that classifies descriptive theories using a theme of comparison of S-boxes, involving analyzes and attributes. The substitution boxes (S-boxes) which provide the cryptosystem with the confusion property described by Shannon [94], are the core component of block cryptosystem and have been widely used in almost all conventional block cryptographic systems. In soft set theory, the parameters are chosen freely to simplify the decision-making process, which often makes the process more efficient. In order to determine the performance of S-box, several different properties are listed in literature for example statistical and algebraic properties. These properties are going to be taken as a parametric set of the soft sets. Next, we will introduce the decision-making algorithm to evaluate the performance of each S-box by taking the results of these properties collectively. The results of the algorithm enable us to optimally grade the S-box.

In [66] and [67], Maji et al., showed the significance of the soft set theory by applying it in the decision making problem. They also introduced new functions on soft sets. Chen in [25] established the notion of soft set parameterization reduction which made the soft theory more applicable. In [53] Kong et al., introduced the concept of normal parameter reduction of soft sets and its use to investigate the problem of submost favorable option and added parameter set in soft sets. Zuo and Xiao [107] discussed soft data analysis approach. While Neo [76], have developed the evaluation technique by using an imprecise soft set. Ali et al., [5] discussed new algebraic operations on soft sets. In [37] Feng et al. obtained some results of soft set theory based on his newly defined algebraic operations and proved that distributive law holds relating to new operations. Aktas and Çağman [3] applied notions of group theory on soft sets. The soft set theory has tremendous growth in the algebraic structures. However, in [2] Acar et. al., introduced the basic idea of a soft ring, which is, in fact, a parameterized family of subrings and ideals of a ring. Atagun and Sezgin [6] introduced soft subring and soft ideal, soft subfield over a field and soft sub-module over a left R-module. Celik et al., [24] a new concept of soft rings, soft ideals, and gave new operations on soft set theory. The notion of soft modules and its properties are defined in [99]. In [82], Rehman et al., came up with the some decision-making methods of choosing the best S-box using the fuzzy parameterized soft set (FPS set).

The notion of the fuzzy set was introduced by Zadeh [105] in 1965. This notion of fuzzy set attracted a number of research workers for applications in different branches of science and technology. It has been successfully applied and new notions have been introduced. Roy and Maji [85], also gave the particular application of fuzzy soft set in decision making. Further Kong et al., [54] and Feng et al., [36] improved the decision-making methods in fuzzy set theory and gave new algorithms. The [106], Zadeh introduced and used interval-valued fuzzy set. By combining the interval-valued fuzzy set and soft set, Yang et al., [104], proposed the interval-valued fuzzy soft set and then analyzed a decision-making problem in the interval-valued fuzzy soft set. The interval-valued fuzzy set contains lower and upper degree of membership of an element. The interval-valued fuzzy soft set assigns each parameter an interval to solve decision-making problem. Based on interval-valued fuzzy soft set, a flexible scheme for optimal selection of S-box, in which the applied decision criteria are judged equally by proposed scheme.

Atanassov [8], introduced the concept of intuitionistic fuzzy soft set theory to provide a power and successful approach to tackling the uncertainty. The concept of intuitionistic fuzzy soft set was introduced by Maji et al., [64]. In continuation to this, Cagman and Karatas [23] introduced decision-making methods by using intuitionistic fuzzy soft set. The intuitionistic fuzzy soft set decision making has received paramount importance in recent time. Therefore, it is meaningful to apply the approach of intuitionistic fuzzy soft set decision making for investigating the quality of different image encryption scheme. The membership and non-membership functions are defined by taking entropy, energy, correlation, homogeneity, contrast.

The words "neutrosophy" and "neutrosophic" were introduced by Smarandache in 1998. The word, "neutrosophy" (noun) is taken from French word neutral and Latin word neuter, neutral, and Greek word Sophia, skill/wisdom means knowledge of neutral thought. In [96], Smarandache introduced the notion of neutrosophic set (NS). Later, Maji in [63] established the notion of neutrosophic soft set (NSS) and defined certain operations on it. It is recent that, NSS has drawn the attention of researchers due to its interesting interactions with a spectrum of applied sciences. For instance, Broumi et al., [15], worked on algebraic properties of interval-valued NSS. Mukherjee and Sarkar in [73] introduced Similarity measures for NSS. The limitations of the intuitionistic fuzzy soft set are that it contains the membership and non-membership values, whereas in NSS along with membership and non-membership values, an intermediate value also presented. The unpredictably in the data is arise from the use of the intermediate function. So, to deal with the data where there is a possibility to work neutrally the NSS is proposed. The decision-making method based on NSS has shown strong encryption capabilities for evaluating the performance of S-boxes. In order to evaluate the performance of the proposed S-box, a comparison is going to be done by the applying the several statistical and algebraic analysis. The NSS is a useful tool to help the decision makers express efficiently the performance of S-boxes.

Chapterwise description

The thesis comprises of the eight chapters. Given below is a brief overview and highlight of each chapter.

The first chapter provides the basic concept related to S-boxes, which is helpful in the rest of the work. A brief review of the theoretical development of S-boxes and the analysis methods are introduced to check the different attributes of the S-boxes.

The second chapter focuses on the soft set theory and its applications. Moreover, the precise mathematical definitions of soft sets and its algebraic notions are defined. Operations on soft sets are, either extended or restricted, depending on the choice of parameters and this property is unique for soft sets so far. No earlier vague structure has addressed this problem of parameterization and, therefore, the soft set theory is adequate in operational use with parameters. It is important that reader must be familiar with the properties of these newly defined operations on soft sets. Properties of operations defined on soft sets are discussed in detail, and the examples are worked out. Further, we have given a brief review of soft set theory in the decision-making of soft sets with fuzzy sets, intuitionistic fuzzy sets, interval valued fuzzy sets and neutrosophic fuzzy soft sets.

In chapter **(third)**, we adopt the method of the selection of secure S-box by using interval-valued fuzzy soft set to the decision making. Each analysis parameter is transformed into the interval value fuzzy set. By giving an application in decision making which can refine our choice on the selection of most feasible S-box.

In chapter 4, the work done is taken [82] to a new level of classification, by analyzing the eight popular S-boxes on different images. The simulation results of S-boxes on standard images of Airplane and Baboon of size 512×512 (pixels) are employed. Furthermore, plugging in action our proposed intuitionistic fuzzy soft (IFS)-set based algorithm, we sort out the optimal S-box, which robust with our decision-making analysis. A novel approach is intended to classify S-boxes, by aid of intuitionistic fuzzy soft (IFS) set theory. Finally, logical operation AND-product have been applied to two different subsets of parameters to classify the strength of S-boxes on the basis of corresponding computing scores.

Chapter 5, describes in detail the proposed neutrosophic soft set based method for the decision making. The average deviation of membership, intermediate and non-membership functions, for objects (parameters) under consideration, presented. Later, comparison tables will be constructed by defined membership, intermediate and non-membership functions of the parameters. Moreover, neutrosophic soft set will be formed by computing the weight functions, along with that, the evaluation interval and evaluation score are defined. Finally, we will practically demonstrate our proposed method, by applying it to the enciphered image of Airplane and Baboon. Then we will sort out the suitable S-box for mentioned images. The results of IFS and NSS-sets decision-making algorithms has been compared.

In chapter 6, the algebraic and statistical analysis are used for the encrypted image encryption of Lena. Though, in this study, using statistical analysis, an improved NSS-decision making criterion for the selection of the most effective S-box from given set of S-boxes. Here, the NSS decision making is presented which is refined than the method presented in the previous chapter. The findings of NSS-decision making criterion are better than the output obtained in previous analysis. The result infers that this decision-making method is more efficient for sorting out the optimal S-box.

In chapter 7, the algebraic notion of the soft ring has been used to construct several algebraic notion which leads to constructing soft Galois ring. To fulfill this aim several notions like soft prime ideals, soft maximal ideals, soft primary ideals, and soft radical ideals are introduced for a soft ring over a given unitary commutative ring. Consequently, the primary decomposition of soft rings and soft modules is established. In addition, the ascending and descending chain conditions on soft ideals and soft sub-modules of soft rings and soft modules are introduced, however enabling us to develop the notions of soft Noetherian rings and soft Noetherian modules. Further, by constructing a soft $\mathbb{Z}_{2^k}-$module over Galois ring $GR\left(2^3,8\right)$ and the soft primary decomposition of soft $\mathbb{Z}_{2^k}-$Galois submodules. Then we extend this theory to the soft group to form soft subgroups and then S-boxes has been constructed over elements of the soft subgroup. Finally in the last section, by employing the decision-making algorithm over a fuzzy bipolar soft set, we choose the optimal S-box.

Chapter 1

On Substitution Boxes

We devote this chapter to provide the general concepts and details of specific algorithms related to Substitution box (in short, S-box). One of the fundamentally important components of the modern cryptographic system is the S-box. Their key task is to ensure the confidentiality and protection of data over the networks. More precisely, the S-box plays a central role in the construction of hash functions, MACs, pseudorandom number generators and stream ciphers. Furthermore, they are an essential ingredient of the message authentication techniques, data integrity mechanisms, entity authentication protocols, digital signature schemes.

There are a number of varieties of block ciphers available for action, but no block cipher is ideally suited for all applications, even if it offers a high level of data security. Why is that? The answer to this question lies in the inevitable trade-offs required in practical applications. For instance the required processing speed and memory limitations (like the size of the code and data size and available cache memory) and limitations implementation platforms (for example, hardware and software, chipcards). Moreover, the variable tolerance of applications to properties of various modes of operation can lead to choice a particular S-box. Thus, it is natural to consider a number of candidate block cipher in a situation and choose an optimal one. It turns out that, DES, APA, and AES are the most secure of all and do the job optimally in cryptosystems. The list of recently published block ciphers includes Lui J., S_8, Gray, Prime, Xyi and Skipjack S-boxes.

Let us set some terminology. We are going to call an original message as the *plaintext* and the coded message as *ciphertext* [98]. The transformation process of converting plaintext into the ciphertext is known as encryption or enciphering process. The process of retrieving the original plaintext from ciphertext is called decryption or deciphering process. The cryptography is the science of securing the information through the encryption and decryption. In general, cryptography comprises of two major types, know as *secret key cryptography* and *public key cryptography*. In the secret key cryptography (or symmetric key cryptography) both the sender and the receiver of information share a common secret code, called the key, cipher and decipher the information. While the public key cryptography, also called asymmetric key cryptography, depends on a pair of keys for encryption and decryption of messages. With public key cryptography, keys work in pairs of matched public and private keys.

By a cryptography technique, we mean a secure process of secret message transfer over a communication line. It involves a sophisticated mathematical algorithm for encryption and decryption of data. Since we live in the age of information and we share and store some of the personal and secret information on computers and transmit it over the Internet, so there is a huge need for cryptographic algorithms to secure the storage and exchange process of information. One of the parts of our information is mostly in the image form so it is important to protect the images from unauthorized access. There are so many algorithms available to protect the image from unauthorized access.

1.1 Boolean Function Theory

The study of Boolean algebra is a widespread and generalized area in itself. This section presents a small literature survey of Boolean function theory. Particularly, we have discussed some important cryptographic properties which are applicable to this work.

1.1.1 Properties of Boolean Functions

The purpose of this section is to make some preliminary definitions on Boolean functions. Let $\mathbb{Z}_2^n$ be the vector space of dimension n over the two-element Galois field $\mathbb{Z}_2$. $\mathbb{Z}_2^n$ consist of 2^n vectors written in a binary sequence of length n. The vector space is equipped with the scalar product $< .,. >: \mathbb{Z}_2^n \times \mathbb{Z}_2^n \to \mathbb{Z}_2$

$$< u, v >= \oplus_{j=1}^{m} u_j.v_j, \tag{1.1.1}$$

where the multiplication and addition $\oplus$ are over $\mathbb{Z}_2$. However, if additions are performed in the real numbers, then it is clear from the context.

Definition 1.1.1. *A Boolean function of n variables is a function h : $\mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2^n$ (or simply a function on $\mathbb{Z}_2^n$). The $(0,1)$-sequence is defined by $(h(\alpha_0), h(\alpha_1), ..., h(\alpha_{2^n-1}))$, also called the truth table of h, where*

$\alpha_0 = (0, 0, ..., 0), \alpha_1 = (0, 0, ..., 1), ..., \alpha_{2^n-1} = (1, 1, ..., 1)$, *ordered by lexicographical order.*

Definition 1.1.2. *A vector Boolean function is a function that maps a Boolean vector to another Boolean vector:*

$$\zeta : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2^m. \tag{1.1.2}$$

This vector Boolean function has n input bits and m output bits. A vector Boolean function can be specified by its definition table: an array containing the output value for each of the 2^n possible input values. Each bit of the output of a vector Boolean function is itself a Boolean function of the input vector. These are the coordinate Boolean functions of the vector Boolean function.

Definition 1.1.3. *A vector Boolean transformation is a vector Boolean function with the identical number of input bits as output bits.*

Definition 1.1.4. *A vector Boolean permutation is an invertible vector Boolean transformation and maps all input values to different output values. There are 2^{m2^n}, n bit to m bit vector Boolean functions. A random n bit to m bit vector Boolean function is a function selected at random from the set of 2^{m2^n} different n bit to m bit vector Boolean functions, where each function has the same probability of being chosen. A random vector Boolean function can be obtained by pulling its definition table with 2^n random m bit values.*

Definition 1.1.5. *The logical negation or complement of a Boolean function g is defined by $\overline{g} = g \oplus 1$.*

Definition 1.1.6. *A linear Boolean function is denoted by*

$$L_\alpha(x) = \alpha_1 x_1 \oplus \alpha_2 x_2 \oplus ... \oplus \alpha_n x_n, \tag{1.1.3}$$

where $\alpha_i x_i$ denotes the bitwise AND of the $i-th$ bits of α, x and $\oplus$ denotes bitwise XOR.

Definition 1.1.7. *The set of affine Boolean functions is the set of linear Boolean functions and their complements*

$$A_{\alpha,c} = L_\alpha(x) \oplus c, \tag{1.1.4}$$

where $x \in \mathbb{Z}_2^n$. The sequence of an affine (or linear) function is called an affine (or linear) sequence.

Definition 1.1.8. *The set of all single valued Boolean functions is denoted by*

$$G_n = \{g\,|g : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2\}. \tag{1.1.5}$$

The subset of all affine Boolean functions in the space G_n is denoted by

$$A_n = \{\beta\,|\beta : \textit{is affine and } \beta \in G_n\}. \tag{1.1.6}$$

We define the subset of all linear Boolean functions in the space $GF(2)^n$ by

$$L_n = \{\alpha|\alpha : \textit{is linear and } \alpha \in G_n\}. \tag{1.1.7}$$

Remark 1.1.9. *The set of all affine functions consist of the linear functions and their negations.*

Remark 1.1.10. *The cardinalities of the above sets are easily observed as*

$$|G_n| = 2^n,\ |A_n| = 2^{n+1},\ |L_n| = 2^n. \tag{1.1.8}$$

Definition 1.1.11. *To each Boolean function $g : \mathbb{Z}_2^n \to \mathbb{Z}_2$,we associate its sign function, or character form, denoted by $\widehat{g} : \mathbb{Z}_2^n \to \mathbb{R}^* \subseteq \mathbb{C}^*$,and defined by*

$$\widehat{g}(x) = (-1)^{g(x)}. \tag{1.1.9}$$

The $(1,-1)-$sequence is defined by $((-1)^{g(\alpha_0)}, (-1)^{g(\alpha_1)}, ..., (-1)^{g(\alpha_{2^n-1})})$, where α_j are defined in definition 1.

1.2 Avalanche and Propagation Criterion

An appropriate property of cryptography is avalanche effect. An input bit is altered than half the output bits changes. Feistel changes the idea of avalanche which is based on the concept of Shannon's diffusion. Furthermore, SAC was introduced by Webster and Tavares [103], in which SAC is defined as ; "If a function is to satisfy the strict avalanche criterion, then each of its output bits should change with a probability of one half whenever a single input bit x is complemented to x'". The SAC is a useful property for Boolean functions in cryptographic applications. This means that if a Boolean function is satisfying the SAC, a small change in the input leads to a large change in the output (an avalanche effect). This property is essential in a cryptographic context due to the fact that we cannot infer its input from its output. In addition to SAC we study the Propagation Criterion (PC for short) which was introduced by Preneel et al., [79]. The mathematical expression for avalanche and SAC is defined as follows:

Definition 1.2.1. *A function $g : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2^m$ has the avalanche effect, if an average of $1/2$ of the output bits change whenever a single input bit is complemented i.e.*

$$\frac{1}{2^n} \sum_{u \in GF(2)^n} \mathbf{wt}(g(x^i) - g(x)) = \frac{m}{2}, \quad for\ all\ i = 1, 2, ..., n. \tag{1.2.1}$$

Definition 1.2.2. *A function $g : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2^m$ of n input bits into m output bits is said to be complete, if each output bit depends on each input bits, i.e. change whenever a single input bit is complemented i.e.*

$$\forall\ i = 1, 2, ..., n,\ j = 1, 2, ..., m,\ \exists\ x \in \mathbb{Z}_2^n \ \ with \ \ (g(x^i))_j \neq (g(x))_j. \tag{1.2.2}$$

If a cryptographic transformation is complete, then each ciphertext bit must depend on all of the output bits. Thus, if it were possible to find the simplest

Boolean expression for each ciphertext bit in terms of the plaintext bits, each of those expressions would have to contain all of the plaintext bits if the function was complete. Alternatively, if there is at least one pair of n-bit plaintext vectors X and X_i that differ only in bit i, $g(X)$ and $g(X_i)$ differ at least in bit j for all $\{(i,j)|1 \leq i,j \leq n\}$ then the function g must be complete.

Definition 1.2.3. *A function $g : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2^m$ satisfies the strict avalanche criterion, if each output bit changes with a probability $1/2$ whenever a single input bit is complemented i.e.*

$$\forall\ i = 1,2,...,n,\ j = 1,2,...,m,\ Prob(g(x^i))_j \neq Prob(g(x))_j = \frac{1}{2}. \tag{1.2.3}$$

In the process of building these S-boxes, it was discovered that if an S-box is complete, or even perfect, its inverse function may not be complete. This could become important if these inverse functions are used in the decryption process, for it would be desirable for any changes in the ciphertext to affect all bits in the plaintext in a random fashion, especially if there is not much redundancy in the original plaintext. Complete cryptographic transformations with inverses which are complete are described as being two-way complete, and if the inverse is not complete the transformation is said to be only one-way complete.

Definition 1.2.4. *The dependence matrix of a function $g : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2^m$ is an $n \times m$ matrix A whose $(i,j)^{th}$ element a_{ij} denotes the number of inputs for which complementing the i^{th} input bit results in a change of the j^{th} output bit,*

$$a_{ij} = \#\{x \in \mathbb{Z}_2^n |\ \mathbf{wt}((g(x^i))_j - (g(x))_j\},\quad for\ i = 1,2,...,n,\ and\ j = 1,2,...,m. \tag{1.2.4}$$

Definition 1.2.5. *The distance matrix of a function $g : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2^m$ is an $n \times (m+1)$ matrix B whose $(i,j)^{th}$ element b_{ij} denotes the number of inputs for* *which complementing i^{th} input bit results in a change of the j^{th} output bit, i.e.*

$$b_{ij} = \#\{x \in \mathbb{Z}_2^n|\}(g(x^i) - g(x)) = j\}, \quad for\ i = 1, 2, ..., n,\ and\ j = 1, 2, ..., m. \tag{1.2.5}$$

Definition 1.2.6. *For $g : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2$ and $a \in \mathbb{Z}_2^n$, $a \neq 0$, we defined the function by*

$$g_a(x) = g(x) \oplus g(x \oplus a), \tag{1.2.6}$$

where g_a is called the directional derivative of g in the direction of a.

Now we are able to express the SAC in connection with the directional derivative.

Lemma 1.2.7. *[26, Lemma 5.3]A Boolean function $g : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2$ satisfies SAC if and only if the function $g(x) \oplus g(x \oplus a)$ is balanced for every $a \in \mathbb{Z}_2^n$ with $a \neq 0$, Hamming-weight 1.*

1.3 S-Box Theory

In this section we now turn our discussions to the area of substitution boxes (S-boxes). The basic definitions of S-box theory are provided to support the research work performed in this thesis. Also in this section, a review of relevant cryptographic properties as applied to S-boxes, is provided.

1.3.1 S-Box Definitions and Types

A natural progression from the theory of single output Boolean functions is the extension of that theory to multiple output Boolean functions, collectively referred to as an S-box. The relationship between the input and output bits in terms of dimension and uniqueness gives rise to various types of S-boxes. We list below several necessary S-box definitions, together with a brief description of some S-box types of interest to this research.

An $n \times m$ substitution box (S-box) is a mapping from n input bits to m output bits, $S : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^m$. The output vector $S(x) = (s_1, s_2, ..., s_m)$ can be decomposed into m component functions $S_i : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2,\ i = 1, 2, ..., m$. There are 2^n inputs and 2^m possible outputs for an $n \times m$ S-box. Often considered as a look-up table, an $n \times m$ S-box, S, is normally symbolized as a matrix of size $2^n \times m$, indexed as $S_{[i]}$ $(0 \leq i \leq 2^n - 1)$ each an m-bit entry. There are, generally speaking, three types of S-boxes: Straight, compressed and expansion S-boxes.

A straight $n \times m$ S-box with $n = m$ (takes in a given number of bits and puts out the same number of bits) may either contain distinct entries where each input is mapped to a distinct output or repeat S-box entries where multiple inputs may be mapped to the same output and all possible outputs are not represented in the S-box. An $n \times m$ S-box which is both injective and surjective is known as a bijective S-box. That is, each input maps to a distinct output entry and all possible outputs are present in the S-box. Bijective S-boxes may only exist when $n = m$ and are also called reversible since there must also exist a mapping from each distinct output entry to its corresponding input. This is the design approached used with the Rijndael cipher.

A compression $n \times m$ S-box $n > m$ with puts out fewer bits than it takes in. A good example of this is the S-box used in DES. In the case of DES, each S-box takes in 6 bits but only outputs 4 bits. A expansion $n \times m$ S-box with $n < m$ puts out more bits than it takes in. A regular $n \times m$ S-box is one which has each of its possible 2^m output appearing an equal number of times in the S-box. Thus, each of the possible output entries appears a total number of 2^{n-m} times in the S-box. All single output Boolean functions comprising a regular S-box are balanced, as are all linear combinations of these functions. Regular $n \times m$ S-boxes are balanced S-boxes and may only exist when $n \geq m$. An $n \times m$ S-box ($n \geq 2m$ and n is even) is said to be bent if every linear combination of its component Boolean functions is a bent function.

There are issues associated with both compression and expansion S-boxes. The first issue is reversibility, or decryption. Since either type of S-box alters the total number of bits, reversing the process is difficult. The second issue is a loss of information, particularly with compression S-boxes. In the case of DES, prior to the S-box, certain bits are replicated. Thus what is lost in the compression step are duplicate bits and no information is lost. In general working with either compression or expansion S-boxes will introduce significant complexities in your S-box design. Therefore straight S-boxes are far more common.

1.3.2 Cryptographic Properties of S-Boxes

While many of the Boolean function properties discussed in previous sections have conceptual equivalences when applied to S-boxes, there are fundamental differences in the manner by which these properties are derived. As an S-box is comprised of a number of component Boolean functions, it is important to observe that when considering the cryptographic properties of an S-box, it is not sufficient to consider the cryptographic properties of the component Boolean functions individually. Rather, it is also necessary to consider the cryptographic properties of all the linear combinations of the component functions. This is illustrated in the following selection of relevant S-box properties.

An $n \times m$ S-box which is balanced is one whose component Boolean functions and their linear combinations are all balanced. Because of this balance, there does not exist an exploitable bias in that the equally likely number of output bits over all output vector combinations ensures that an attacker is unable to trivially approximate the functions or the output.

The well-known concept of confusion due to Shannon [94] is described as a method for ensuring that in a cipher system a complex relationship exists between the ciphertext and the key material. This notion has been extrapolated to mean that a significant reliance on some form of substitution is required as a source of this confusion. The confusion in a cipher system is achieved through the use of nonlinear components. As expected, substitution boxes tend to provide the main source of nonlinearity to cryptographic cipher systems.

1.4 Criteria for evaluating block ciphers and modes of operation

The problem of security of block cipher has remained (and still is) a challenging problem for the experts for a long time. Our proposed design criteria are going to be used to estimate the security level and performance of block cipher. For the efficient and effective results, we are going to choose the size of the key in an appropriate way. The upper bound for the security depends on the entropy of the key space. Every medium of propagation of message leads to choosing a specific degree of the complexity of the cryptographic mapping. Another important factor that can impact the complexity of algorithm and security provided by it is the size of a block cipher. Moreover, the more algorithm becomes complex the more it affects the implementation costs both in terms of development and fixed resources, as well as real-time performance for fixed resources. We generally require preserving the size of plaintext data. For instance, the Homophonic substitution and randomized encryption techniques result in data expansion. If the decrypted ciphertext involves some bit errors then one can expect the propagation of errors to subsequent plaintext blocks. Different error characteristics are acceptable in various applications. Block size (above) typically affects error propagation.

Let us discuss some of the standard S-boxes which we commonly encounter and compare the result of these S-boxes with the new one.

1.4.1 Advanced Encryption Standard (AES) S-box

The Advanced Encryption Standard (AES) was published by the National Institute of Standards and Technology (NIST) in 2001. AES is a symmetric block cipher that was introduced to replace the DES as the newly approved standard for a huge spectrum of applications. Unlike the public-key algorithms like RSA, the structure of AES and most symmetric ciphers are quite complex and cannot be explained as easily as many other cryptographic algorithms.

Let us describe the some of the important points regarding the structure of AES. The AES technique processes the entire data block by treating it as a single matrix during each round using substitutions and permutation. The whole process comprises of the four phases involving one of permutation and three substitution phases described blow.

• Substitute bytes: This phase employs an S-box to perform a byte-by-byte substitution of the block.

• ShiftRows: A phase of dealing simple permutation.

• MixColumns: An arithmetic based substitution.

• AddRoundKey: A simple bit-wise XOR of the current block with a portion of the expanded key.

The structure of process is straight forward. In the both cases of encryption and decryption, the ciphering process kicks off with an AddRoundKey phase. In the next 9 rounds in which each round involves all above four phases. The next 10th round involves three phases. It is worth noticing that AddRoundKey stage makes use of the key. For this reason, the cipher begins and ends with an AddRoundKey stage. The remaining three stages combined are the source of confusion, diffusion, and nonlinearity, but since these phases do not involve the key so hence provide no security. Moreover, for these phases (i.e. Substitute Byte, ShiftRows, and MixColumns stages), an inverse function is used in the decryption algorithm. In case of the AddRoundKey stage, the inverse function is constructed by XORing the same round key to the block and using the identity $A \oplus B \oplus B = A$. Like the most of the block ciphers, the decryption technique essentially uses reverse order of the key expansion. Moreover, decryption and encryption techniques have significant differences due to the structure of AES. Once we made sure that all four phases are reversible then it is not difficult to establish that decryption successfully recovers the encrypted plaintext.

The construction of 8-bit bytes as elements in $GF(2^8)$, AES S-box is combined of a power of a function $k(x)$ and affine transformation $l(x)$, where $k(x) = x_i^{-1}$ for $x_i's \neq 0$ and $l(x) = x_i + c$ where the $x_i's$ are coefficient of x. From now onwards, AES S-box can be denoted by $S(x) = l \circ k$.

Several experts of crypto-analysis have studied several important structural characteristics of AES. Some of the well-known are given as follows;

1.4.2 Affine Power Affine (APA) S-box

In order to remove the uncertainties and vulnerabilities in the simple algebraic representation of AES S-box, Affine-Power-Affine (APA) S-box was introduced (cf. [29]) in the following manner,

$$S(x) = A \circ P \circ A,$$

where A denotes the affine surjectivity and P denotes the power permutation with "good" cryptographic characteristics in $GF(2^8)$. Since AES S-box are defined in following way,

$$S(x) = A \circ P.$$

One can observe that APA S-box offer a mature algebraic complexity, moreover other cryptographic characteristics are stationary i.e. invariable. After knowing the reason behind the simplicity of algebraic expressions of AES-like S-boxes, we can infer that their algebraic expressions in $GF(2^n)$ can involve at most $n+1$ objects. It has been show in literature that the algebraic complexity of AES S-box is boosted from 9 to 253 and that of inverse S-box remains 225, moreover, several other good cryptographic characteristics of AES S-box are inherited and preserved into APA S-box.

1.4.3 S_8-AES S-box

The group of symmetries S_8 plays central role in construction of S_8-AES (cf. [47]). The bytes are independently processed, and the transformation to the new S-box also exhibits nonlinear properties. The process of transformation leads to new 40320 S-boxes with different properties.

Mathematical transformation process can be given as,

$$f : S_8 \times AES\text{-S-box} \longrightarrow S_8\text{-}AES \text{ S-box}$$

Based on above description it is clear that there are precisely n^{40320} key options for the exchange of secret messages via an insecure line of communication. The sender of the option message can variate the keys with every message of length 16. In order to hack the message from outside communication system, the hacker has to:

Either check all n^{40320} keys, for instance, in the case of $n = 2$ then we get a huge number 2^{40320} of secret keys this means even if the millions of calculations are made per second the hacker needs thousands of years to decrypt the message or hacker has to face the same complexity as AES.

1.4.4 XYi S-box

We refer to [95] for the details. XYi cipher with block size 8 bits offers the substantial resistance to differential attack. It works through a transition probability matrix which is computed by exhaustive search and hence the i^{th} power i.e. i-transition probability matrix. Following are the key observations:

1. The lower bound on the computational complexity of differential attack to the 5-round mini cipher is

$$Comp(5) \geq \frac{2}{0.0067 - 1/255} > 2 \times 256$$

The above inequality says that the computational complexity of differential attack to the 5-round mini cipher has been greater than computational completely determining encryption function.

2. The minimum and maximum in the i-transition probability matrix of the mini cipher are almost agreed after 8 turns. This reflects that the probability distribution of i-round differentials converges to uniform distribution after sufficient round iterations.

The procedure of creating an 8×8 S-box against potential attacks, is illustrated as follows:

1. Randomly generating a series of 2-bit nonnegative integers as the sub-keys used in the “mini version” of the proposed cipher.

2. Orderly encrypting $0, 1, 2, \cdots, 255$ with enough round iterations of the mini cipher and those sub-keys randomly generated above.

3. Pair-wise arranging the plaintexts and their resulting Ciphertexts to form an S-box from 8-bits to 8-bits.

1.4.5 Gray S-box

We refer to [101] for the detailed treatment of Gray S-box. We are going to the discuss some of the details of the construction of Gray S-box through binary Gray code transformation.

Gray S-box corresponds to a polynomial with all 255 non-zero terms in comparison with a 9-term polynomial of original AES S-box, and hence enhances the security for S-box against algebraic attacks and interpolation attacks. Moreover, since Gray S-box reapplies AES S-box in totality, therefore all advantages and efficiency of any existing optimized implementation of AES S-box are also inherited. Further, Gray S-box establishes important cryptographic properties of AES S-box, including strict avalanche criterion, nonlinearity, and differential uniformity. Consider the following definition of Gray augmentation,[101, Definition 1] Gray augmentation: using Gray code encoding partially/entirely in a cryptographic component as an augmentation to improve its algebraic complexity.

With regards to AES S-box, we may create the modified S-box by replacing x by a multi-termed polynomial of x as the input of the original S-box in AES. We define Gray S-box, denoted by γ, be the combination of the binary Gray code conversion $G(x)$ and the original AES S-box.

$$\gamma = H \circ L \circ F \circ G$$

The algebraic expression of Gray S-box is as follows:

$$\gamma(x) = \sum_{0 \le i,j < 16} a_{ij} x^{16i+j}$$

The algebraic expression has the degree of 254 (the maximum value) and the entire 255 terms are non-zero (in comparison with only 9 terms in the algebraic expression of the original S-box in AES). This improves the resistance of S-box against interpolation attacks [41] and algebraic attacks [28].

The inverted Gray S-box corresponds to polynomial $\gamma^{-1}(x)$ with the degree of 254 and 254 non-zero terms:

$$\gamma^{-1}(x) = \sum_{0 \le i,j < 16} b_{ij} x^{16i+j}$$

As all but one term of the algebraic expression of the inverted Gray S-box are non-zero, it is unlikely to exploit the inverse Gray S-box in algebraic attacks or interpolation attacks.

1.4.6 Residue Prime S-box

The Residue prime algorithm was proposed by Cui and Cao [29]. The authors offer an improved S-box for AES in which the proposed affine mapping in the original AES S-box was augmented as a pre-processing step of the original S-box. By following the proposed algorithm, the implementation of the original S-box in AES can be reapplied entirely but the result S-box corresponds to the polynomial with only 253 terms [101].

Indeed, the residue of prime numbers can become a source of complexity to the implementation of S-box. The complete S-Box comprises of the 256 entries which are the residues of the prime number 257. The choice of 257 makes sense because each of residues from 1 to 255 have unique inverses. Furthermore, these residues can be used for all block sizes of the AES; that is, they can be used for the 256, 192 and 128 bits blocks.

To address the vulnerability concern of storing the S-Box table, one needs to store only some of the entries and figure out a way to determine the rest. Fortunately, a 50% reduction of table 1 is achievable due to the fact that all the double digits hexadecimal numbers and their inverses coexist on the same table. Therefore, the best possible reduction is to store only half of the numbers and their inverses and omit the other half. Obviously, such reduction will result in a miss ratio that equals the reduction percentage.

1.4.7 Lui J. S-box

For the detailed description and construction of Lui J. we refer to [61]. Liu J. algorithm boosts the complexity of AES S-box from 9 to 255 by changing the order of linear and inverse transformations. In order to overcome the sensitivities of simple algebraic expression, improvement of the AES S-box is required. The improved AES-box does not require the change in the previous irreducible polynomial, affine transformation matrix, and affine constant. The boost in the complexity of algebraic expression offers the capability to resist against differential cryptanalytic invariability. The following is outline of improved scheme:

1. $z = f(y)$,
2. $u = z^{-1}$,
3. $y = u \oplus 0x63$,

where x denotes some indeterminate.

1.4.8 SkipJack S-box

The block cipher Skipjack was introduced and studied by the U.S. National Security Agency (NSA) for securing the highly sensitive data. This algorithm provides an utmost security to a government intelligence agency data. Skipjack was first initiated as the encryption algorithm in a US government-sponsored scheme of key escrow. It was used in fastened phones. Skipjack deals with an 80-bit key, known as Crypto Variable (CV), to encrypt or decrypt 64-bit data blocks. It is a 32 revolutions based Feistel network. This algorithm is characterized with numerous operations, but most notable is its S-box.

1.5 Analyses Techniques

Most of the linear systems are easily breakable, therefore, the nonlinearity of the system is of fundamental importance. Nonlinearity describes the confusion created by Boolean function in the cryptographic transformation. Whereas, the amount of redundant information from the plaintexts and their corresponding ciphertexts is measured by the correlation coefficient. The correlation coefficient is a useful measure to judge encryption quality of any cryptosystem. Contrast measures the consistency between the cipher text and plain text. Entropy analysis measures the degree of indeterminateness in the system. It is a method for measuring uncertainty in a series of numbers or bytes [97]. In image encryption scheme, an energy of encrypted image is an acute and limited resource. The concept of energy detects the disorder in image encryption. Homogeneity measures the smoothness of an encrypted image and original image. Another important property for a secure block cipher is Strict Avalanche Criterion (SAC). Bit Independence Criterion (BIC) is most appropriate for cryptographic transformation. Mister and Adams [70] propose a number of criteria for S-box design. Among these are that the S-box should satisfy both SAC and BIC. A block cipher satisfies the strict avalanche effect if for a fixed plaintext block a small change in the key causes a large change in the resulting ciphertext block. Linear approximation Probability analysis (LP) is used to study the probability of the attacker for obtaining the secret key by considering the parity check matrix of plain text and cipher text.

One of the key objectives of the above-mentioned several cryptanalyses is to study the quality of S-boxes for image encryption, secondly, these cryptanalyses serve as parametric sets for an intuitionistic fuzzy soft sets. The majority of contributions in this area mainly focus on measuring the suitability of S-box through a specific parameter, one can rarely find a work in which all parameters are considered at the same time to determine the quality of S-boxes for image encryption.

1.5.1 Statistical Analyses

The following are mentioned statistical analyses.

Majority logic criterion (MLC)

The encrypted image produces randomness in the original image, and the sort of randomness hkis used to analyze the strength of the S-box in image encryption application. In [89], the MLC-defined a criterion based on different statistical analyzes to examine the characteristics and properties of an S-box. The correlation analysis, contrast analysis, entropy analysis, energy analysis, homogeneity analysis and mean absolute deviation analysis are performed under the umbrella of MLC. Probably, it will be a good idea to explore these mentioned analyzes in detail.

Contrast

Contrast analysis is used for showing the consistency of the encrypted image, it enables the viewers to recognize the original image. Contrast is a used to measure the local gray level difference of a contiguous set of pixels in the GLCM. The parameter can be characterized as a linear dependency of gray levels of neighboring pixels. The neighboring pixels have high and low values of the contrast. The high value of contrast is obtained when the encrypted image is entirely vague. The contrast of an image is very low, then the encrypted image is similar to the original image. The contrast value can be calculated as

$$C = \sum_i \sum_j (i - j)^2 p[i, j],$$

where i and j are the pixels in the image, and the element of gray-level co-occurrences matrices is represented by $p(i, j)$. The range of Contrast is

$$[0, (size(GLCM, 1) - 1)^2],$$

where Contrast is 0 for a constant image. Contrast weight values by the inverse of Homogeneity weight, which means lower the homogeneity, higher the Contrast.

Correlation

The correlation coefficient reflects the quality of encrypted cipher text and plain text. It is used to measure the amount of ambiguity between two adjacent pixels of the cipher text. Correlation is tested in horizontal, vertical and diagonal directions of the adjacent pixels in the image. More than one thousand groups of adjacent pixels are chosen to measure the pixel correlation in the horizontal, vertical and diagonal directions. High randomness in the encrypted image is shown when correlation coefficient had the value approximately near to or equal zero and the encrypted image is entirely different from the plain image. In addition to the partial regions of analysis, the complete image is also included in the image processing. The image analysis is based on the measurement of the correlation of a pixel to its neighboring pixel. The correlation representation is,

$$K = \sum_{i,j} \frac{(i - \mu i)(j - \mu j)p(i,j)}{\sigma_i \sigma_j}.$$

If encrypted image is completely identical to the original image, then correlation coefficient is 1, and encryption process is false. Also, if the correlation coefficient is -1, then it is negative of the original image

Energy

Energy analysis measures the uniformity, it indicates the ambiguity of the encrypted image. The gray-level co-occurrence matrix (GLCM), is used to detect how much the cipher text is homogenous. The GLCM distribute the values uniformly all over the grids. The energy analysis is good when GLCM has few entries of large magnitude. The sum of squared elements in the GLCM is used for energy. The formula of this analysis is given as

$$E = \sum_i \sum_j p^2[i,j].$$

The range of the energy is $[0,1]$. The higher value represent, , the greater the similarity of cipher text and plain text. The image of encryption is same as the constant image if the value is 1. Energy is actually local homogeneity and Entropy is the opposite of Energy [83].

Homogeneity

Homogeneity analysis is used to measure the distribution of elements in the GLCM to its diagonal. It's also called gray tone spatial dependency matrix. It combines the pixel gray levels in the set-theoretic form, greater the homogenous area darker the image. Hence, it provides how the encrypted image is speared out in the whole region. It can be calculated as

$$H = \sum_i \sum_j \frac{p(i,j)}{1+|i-j|}.$$

The homogeneity varies in interval $[0,1]$. The greater change in the gray tone, shows the lower homogeneity coefficient and hence the higher contrast. Similarly, a small variation in an encrypted refers to high homogeneity. While the low homogeneity coefficient gives high randomness in an image and their spatial arrangements.

Entropy

Entropy analysis is used to measure the amount of difficulty or the probability of independently calculating each bit of the encrypted image. The nonlinear component of the crypto-system. produced the uncertainty in the data. It gives the amount of uncertainty in the cipher text. Also, it is the main feature of the randomness in the system and defined as follows,

$$H(x) = -\sum_{i=0}^{n} p\left(x_i\right) \log_b p\left(x_i\right),$$

where $P\left(x_i\right)$ are the histogram counts. In the case when each symbol has equal probability, then the entropy $H(x) = 8$. If the image to be processed is uniform then the entropy will be large and hence much of GLCM elements will have very small values. The entropy of encrypted image obtained is 8 bits, which corresponds to an ideal encryption scheme. If the entropy is less than 8, then is a lack of randomness in the encrypted image. Complex image encryption tends to have high entropy. However, Entropy is strongly inversely correlated to energy.

MAD analysis

In order to judge the performance of encrypted image and the original image, the parameter used is mean of absolute deviation (MAD). MAD criterion is more strong to analyze than any other existing analysis. The higher value of MAD for encrypted image shows more complex and secure encryption scheme. The mathematical computations can be done through below-given formula,

$$MAD = \frac{1}{L \times L} \sum_{j=1}^{L} \sum_{i=1}^{L} |a_{ij} - b_{ij}|$$

where a_{ij} represents the pixels of plain image, b_{ij} represents the pixels of the corresponding encrypted image, and L represents the dimensions of the image.

1.5.2 Algebraic Analyses

Following is the brief explanation of these mentioned algebraic analyses. We now define the measure of nonlinearity for an $n \times m$ S-box.

Nonlinearity

The notion of nonlinearity was introduced by Meier and Staffelbach. The distance between a reference function under evaluation and group of all possible affine functions is nonlinearity. This method decides that the number of bits must be changed to make the function adjacent to an affine function as much as possible. By [28], a nonlinearity indicator of a function $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$, where $\mathbb{Z}_2 = \{0, 1\}$, is an $n \times m$ S-box S, denoted by $NL(F)$. Let $S = (s_1, s_2, ..., s_m)$ where s_i $(i = 1, ..., m)$ are n-variable Boolean functions. Let h_i be the set of linear combinations of s_i $(i = 1, ..., m)$ (which includes the functions s_i) and can be defined as;

$$NL(F) = \min_{h}\{N_{S_{n,m}}(h_j)\} \ (j = 1, ..., 2^m - 1).$$

The resistance of an S-box against linear cryptanalyses is measured by its nonlinearity [70]. In [39], the upper bound of nonlinearity for an S-box over $GF(2^n)$, is $UN = 2^n - 2^{n/2-1}$. So theoretically, in AES the upper bound of S-box based on $GF(2^8)$ is 120. While, practically, AES S-box gets a finest value equal to 112.

Bit Independence Criterion (BIC)

The Bit independence criterion (BIC) is introduced by Webster and Tavares [103] in 1985. BIC is used to numbered the degree of dependent change in a pair of output bits when an input bit is inverted. Practically, in this criteria all avalanche variables become independent pairs corresponding to a single plaintext bit. For measuring the degree between the pair of output bits, the correlation coefficient is used to calculate. A function $f : \mathbb{Z}_2^n \longrightarrow \{0,1\}^n$ satisfies BIC if for all $i, j, k \in (1, 2, \cdots, n)$ where $j \neq k$, inverting plaintext bit i gives cipher bits j and k to change independently. The bit independence corresponding to the effect of the i^{th} input bit change on the j^{th} and k^{th} bits of is B^{e_i}:

$$BIC(b_j, b_k) = \max_{1 \leq i \leq n} |\mathbf{corr}(b_j^{e_i}, b_k^{e_i})|. \tag{1.5.1}$$

The bit independent criterion (BIC) parameter for the S-box function f, is then defined as follows:

$$BIC(h) = \max_{\substack{1 \leq j,k \leq n \\ j \neq k}} BIC(b_j, b_k), \tag{1.5.2}$$

BIC varies in an interval $[0, 1]$. If the correlation coefficient is zero, then the output bits are independent to each other. For value equals 1, output bits are identical to each other.

Strict Avalanche Criterion (SAC)

Strict avalanche criterion (SAC) was introduced by Webster and Tavares [103], later Feng and Wu [39] generalized this concept. The completeness and avalanche properties are combined into strict avalanche criterion. It is an important property to resist differential crypa-analysis [11]. In SAC, a single input bit change, cause the half change in the output bit. Also, it should be interpreted as if the probability of change is different from half of the output, and then S-box doesn't satisfy SAC.

The behavior of the output bits of the cipher with respect to the changes applied to input bits, is analyzed by this criterion. Strict avalanche criterion (SAC) was introduced by Feng and Wu [39]. By SAC, it is desirable that if a single input bit change its value, half of the output bits must be changed. As the iteration progresses, a single change in input bit causes an avalanche of changes in output bits. The randomness shaped by cipher will be maximum if each of the output bit changes with a probability of 0.5, when only a single bit is changed.

An (n, m) S-box F is said to satisfy the SAC, if

$$\sum_{x \in \mathbb{Z}_2^n} F(x) \oplus F(x \oplus c_k^{(n)}) = \left(2^{n-1}, 2^{n-1}, \cdots, 2^{n-1}\right),$$

for all k $(1 \leq k \leq n)$. The $c_k^{(n)}$ is the k^{th} position of an n dimensional vector space with Hamming weight 1.

Linear approximation probability (LP)

Linear approximation is a useful method in crypa-analysis, was introduced by Matsui in 1993 as a theoretical attack on the Data Encryption Standard (DES) [70]. It is also known as probabilistic linear relations. It works on the principle of finding "high probability occurrences of linear expressions involving plaintext bits, ciphertext bits (actually we shall use bits from the 2nd last round output), and subkey bits". The analysis is used to study the imbalance in an input bits, output bits and secret key. It works with a single input bits. In this analysis the probability of sum of output bits is equal to the half of input bits. The notions, Γ_x and Γ_y are applied to the parity of the input and output bits, respectively. It can defined as,

$$LP = \max_{\Gamma_x, \Gamma_y \neq 0} \left| \frac{\#\{x \in X : x \cdot \Gamma_x = S(x) \cdot \Gamma_y\}}{2^n} - \frac{1}{2} \right|,$$

where the set X consists of all possible inputs and 2^n is its cardinality. The maximum linear approximation probability of vector Boolean function (S-boxes) are defined as $p = \max_i \max_{\Gamma_x, \Gamma_y} LP^{S_i}(\Gamma_y \to \Gamma_x)$.

Differential approximation probability (DP)

Differential approximation was first presented by Biham and Shamir in 1990 as an attack on DES [11]. The analysis is based on exploring the difference between the plain text and cipher text. This analysis works with the block of bits, it shows the high probability of certain occurrences of plain text and cipher text differences. It exhibits the uniformity, a unique input bit must mapped to unique output bit and it gives the information about the secret key. According to [11], differential uniformity is measured as;

$$DP(\Delta x \to \Delta y) = \left[\frac{\#\{x \in X : S(x) \oplus S(x \oplus \Delta x) = \Delta y\}}{2^n} \right],$$

where Δx and Δy are input and output differentials respectively. The maximum differential approximation probability of vector Boolean function (S-boxes) are defined as: $q = \max_i \max_{\Delta_x, \Delta_y} DP^{S_i}(\Delta_x \to \Delta_y)$.

Chapter 2

Soft sets and its applications

The main objective of the chapter is to introduce the theory of soft set, soft group, soft rings and soft modules. Several operations on soft sets and corresponding algebraic structures have been defined and their properties are investigated. In the vast world of data one of the biggest problem that everyone has to deal with the imprecision of data, therefore, there is always a natural need of methods to tackle the problem of inadequacy.

Let me give a brief overview of existing literature on soft sets. The Molodstov in [72] came up with the notion of soft sets as a solution of uncertainty, imprecision or inadequacy of data of various application. Moreover, Maji et al., [66, 67] came up with the operations on soft sets and investigated some basic properties. The operations (like intersection and inclusion) on soft sets were also defined independently by Pie and Miao in [78], and proposed some of the applications of soft sets into information systems. Ali et al., [5] spotted and corrected some mistakes in the definition of operations proposed by Maji in [66], moreover he defined some new operations on soft sets including extended and restricted operations of union, intersection and product. The soft set theory has been extended to its group theoretic version by Aktaş and Çagman in [3], who came up with some basic results about soft groups. The notion of normalistic soft group and properties has been introduced by Sezgin and Atagun in [88]. In Acar et al., [2], introduced the basic notions of soft rings, which are actually a parameterized family of subrings of a ring, over a ring. Atagun and Sezgin [6], contributed by coming up with the notion of the soft subring, soft ideal, soft subfield over a field and soft sub-module over a left R-module. Sun et al., [99] investigated some algebraic properties of soft modules.

This chapter consists of five sections. In the first section, the fundamental properties of soft set theory and some elementary properties are discussed that are familiar to the reader. In the second section, the basic properties of the soft group are presented. In the third section, the concept of soft rings is provided. Also, some structural properties are presented. In fourth section soft module structure is defined and its properties are discussed. Lastly,

2.1 Soft Set Theory

Throughout this section, U is the universal set and E is the set of parameters. Molodtsov [72], gives the definition of soft set in the following manner;

Definition 2.1.1. *[72, Definition 2.1] Let U be an initial universe and E be a set* *of parameters. Let $P(U)$ denotes the power set of U and A be a non-empty subset of E. A pair (F, A) is called a soft set over U, where F is a mapping given by $F : A \to P(U)$.*

In other words, a soft set over U is a parametrized family of subsets of the universe U. For $\varepsilon \in A$, $F(\varepsilon)$ may be considered as the set of ε-approximate elements of the soft set (F, A). Clearly a soft set is not a set.

Definition 2.1.2. *[67, Definition 2.3] For two soft sets (F, A) and (G, B) over a common universe U, we say that (F, A) is a soft subset of (G, B) (i.e., $(F, A)\tilde{\subset}(G, B)$) if*

(i) $A \subset B$ and

(ii) for all $e \in A$, $F(e)$ and $G(e)$ are identical approximations.

(F, A) is said to be a soft super set of (G, B), if (G, B) is a soft subset of (F, A) and it is denoted by $(F, A)\tilde{\supset}(G, B)$.

Definition 2.1.3. *[67, Definition 2.4] Two soft sets (F, A) and (G, B) over a common universe U are said to be soft equal if (F, A) is a soft subset of (G, B) and (G, B) is a soft subset of (F, A).*

Definition 2.1.4. *[67, Definition 2.5] Let $E = \{e_1, e_2, \ldots \quad , e_n\}$ be a set of parameters. The NOT set of E denoted by $\rceil E$ is defined by $\rceil E = \{_\rceil e_1,_\rceil e_2, \ldots,_\rceil e_n\}$, where $_\rceil e_i =$ not e_i for all i.*

Proposition 2.1.5. *[67, Prposition 2.1]*

(i) $\rceil(\rceil A) = A$;

(ii) $\rceil(A \cup B) = \rceil A \cup \rceil B$;

(iii) $\rceil(A \cap B) = \rceil A \cap \rceil B$.

Definition 2.1.6. *[67, Definition 2.7] A soft set (F, A) over U is said to be a $NULL$ soft set denoted by Φ if for all $\varepsilon \in A$, $F(\varepsilon) = \emptyset$ (null set).*

Definition 2.1.7. *[67, Definition 2.8] A soft set (F, A) over U is said to be absolute soft set denoted by $\widetilde{A}$ if for all $\varepsilon \in A$, $F(\varepsilon) = U$. Clearly $\widetilde{A}^c = \emptyset$ and $\emptyset^c = \widetilde{A}$.*

Definition 2.1.8. *[67, Definition 2.9] If (F, A) and (G, B) are two soft sets, then " (F, A) AND (G, B)" denoted by $(F, A) \wedge (G, B)$ is defined by $(F, A) \wedge (G, B) = (H, A \times B)$, where $H((\alpha, \beta)) = F(\alpha) \cap G(\beta)$, for all $(\alpha, \beta) \in A \times B$.*

Definition 2.1.9. *[67, Definition 2.10] If (F, A) and (G, B) are two soft sets then " (F, A) OR (G, B)" denoted by $(F, A) \vee (G, B)$ is defined by $(F, A) \vee (G, B) = (O, A \times B)$ where, $O((\alpha, \beta)) = F(\alpha) \cup G(\beta)$ for all $(\alpha, \beta) \in A \times B$.*

Definition 2.1.10. *[67, Definition 2.11] Intersection of two soft sets (F, A) and (G, B) over the common universe U is the soft set (H, C), where $C = A \cap B$ and for all $e \in C$, $H(e) = F(e)$ or $G(e)$. We write $(F, A)\tilde{\cap}(G, B) = (H, C)$.*

Definition 2.1.11. *[67, Definition 2.11] Union of two soft sets (F, A) and (G, B) over the common universe U is the soft set (H, C), where $C = A \cup B$ and for all $e \in C$,*

$$H(e) = \begin{cases} F(e) & if\ e \in A - B \\ G(e) & if\ e \in B - A \\ F(e) \cup G(e) & if\ e \in A \cap B \end{cases}$$

We write $(F, A)\tilde{\cup}(G, B) = (H, C)$.

Definition 2.1.12. *[35, Definition 2.3] Bi-intersection of two soft sets (F, A) and (G, B) over the common universe U is the soft set (H, C), where $C = A \cap B$,* *denoted by* $(F, A)\widetilde{\sqcap}(G, B)$, *is defined as* $(F, A)\widetilde{\sqcap}(G, B) = (H, C)$, *where* $C = A \cap B$, *and* $H(e) = F(e) \cap G(e)$ *for all* $e \in C$.

Definition 2.1.13. *[5, Definition 3.2] Extended intersection of two soft sets* (F, A) *and* (G, B) *over the common universe* U *is the soft set* (H, C), *where* $C = A \cup B$ *and for all* $e \in C$.

$$H(e) = \begin{cases} F(e) & if\ e \in A - B \\ G(e) & if\ e \in B - A \\ F(e) \cap G(e) & if\ e \in A \cap B \end{cases}$$

We write $(F, A) \cap_E (G, B) = (H, C)$.

Definition 2.1.14. *[5, Definition 3.3] The restricted intersection* (H, C) *of two soft sets* (F, A) *and* (G, B) *over a common universe* U, *such that* $A \cap B \neq \phi$, *denoted by* $(F, A) \Cap (G, B)$, *is defined as* $(F, A) \Cap (G, B) = (H, C)$, *where* $C = A \cap B$, *and* $H(e) = F(e) \cap G(e)$ *for all* $e \in C$.

Definition 2.1.15. *[5, Definition 3.3] The restricted difference* (H, C) *of two soft sets* (F, A) *and* (G, B) *over a common universe* U, *such that* $A \cap B \neq \phi$, *denoted by* $(F, A)\diagdown_{\mathcal{R}}(G, B)$, *is defined as* $(F, A)\diagdown_{\mathcal{R}}(G, B) = (H, C)$, *where* $C = A \cap B$, *and* $H(e) = F(e) - G(e)$ *for all* $e \in C$.

Definition 2.1.16. *[24, Definition 3.26] The extended sum of two soft sets* (F, A) *and* (G, B) *over a ring* R *is denoted by* $(F, A) \oplus_{\cup} (G, B)$, *is defined as* $(F, A) \oplus_{\cup} (G, B) = (H, C)$, *where* $C = A \cup B$ *and*

$$H(e) = \begin{cases} F(e) & if\ e \in A - B \\ G(e) & if\ e \in B - A \\ F(e) + G(e) & if\ e \in A \cap B \end{cases}$$

for all $e \in C$.

Definition 2.1.17. *[24, Definition 3.27] The restricted sum of two soft sets* (F, A) *and* (G, B) *over a ring* R *is denoted by* $(F, A) \oplus_{\cap} (G, B)$*, is defined as* $(F, A) \oplus_{\cap} (G, B) = (H, C)$*, where* $C = A \cap B$ *and* $H(e) = F(e) + G(e)$ *for all* $e \in C$*.*

Definition 2.1.18. *[24, Definition 3.28] The extended product of two soft sets* (F, A) *and* (G, B) *over a ring* R *is denoted by* $(F, A) \odot_{\cup} (G, B)$*, is defined as* $(F, A) \odot_{\cup} (G, B) = (H, C)$*, where* $C = A \cup B$ *and*

$$H(e) = \begin{cases} F(e) & if\ e \in A - B \\ G(e) & if\ e \in B - A \\ F(e) \cdot G(e) & if\ e \in A \cap B \end{cases}$$

for all $e \in C$*.*

Definition 2.1.19. *[24, Definition 3.29] The restricted product of two soft sets* (F, A) *and* (G, B) *over a ring* R *is denoted by* $(F, A) \odot_{\cap} (G, B)$*, is defined as* $(F, A) \odot_{\cap} (G, B) = (H, C)$*, where* $C = A \cap B$ *and* $H(e) = F(e) \cdot G(e)$ *for all* $e \in C$*.*

2.2 Soft Groups

Aktaş and Çağman [3], initiate the concept of a soft group. The structure of soft subgroups, normal soft subgroups, and soft homomorphism are developed. Then Aktaş and Özlü [4], defined cyclic soft groups and form a result similar to the Lagrange theorem in group theory.

Throughout this section, G is a group and A is any non-empty set.

Definition 2.2.1. *[3, Definition 13] Let* (F, A) *be a soft set over* G*. Then* (F, A) *is said to be a soft group over* G *if and only if* $F(x)$ *is a subgroup of* G *for all* $x \in A$*.*

Theorem 2.2.2. *[3, Theorem 15] Let (F, A) and (H, A) be two soft groups over G. Then their intersection $(F, A)\tilde{\cap}(H, A)$ is a soft group over G.*

Theorem 2.2.3. *[3, Theorem 16] Let (F, A) and (H, A) be two soft groups over G. If $A \cap B = \phi$, then their union $(F, A)\tilde{\cup}(H, A)$ is a soft group over G.*

Theorem 2.2.4. *[3, Theorem 17] Let (F, A) and (H, A) be two soft groups over G. Then $(F, A)\Lambda(H, A)$ is a soft group over G.*

2.2.1 Soft subgroup

In classical algebra the notion of subgroup gain much importance. In this subsection the notion of soft subgroup and their algebraic properties is mentioned as follows;

Definition 2.2.5. *[3, Definition 20] Let (F, A) and (H, K) be two soft groups over G. Then (H, K) is a soft subgroup of (F, A), written as $(H, K)\tilde{<}(F, A)$, if $K \subset A$ and $H(x)$ is subgroup of $F(x)$ for all $x \in K$.*

Theorem 2.2.6. *[3, Theorem 22] Let (F, A) be a soft group over G. If $\{(H_i, K_i) : i \in I\}$ is a non-empty of soft subgroups of (F, A) where I is an index set. Then;*
(i) $\bigcap\limits_{i\in I}(H_i, K_i)$ *is a soft subgroup of (F, A).*
(ii) $\Lambda\limits_{i\in I}(H_i, K_i)$ *is a soft subgroup of (F, A).*

Definition 2.2.7. *[3, Definition 28] Let (F, A) and (H, K) be two soft groups over G. Then (H, K) is a soft subgroup of (F, A), written as $(H, K)\tilde{\lessdot}(F, A)$ if $K \subset A$ and $H(x)$ is normal subgroup of $F(x)$ for all $x \in K$.*

Theorem 2.2.8. *[3, Theorem 29] Let (F, A) be a soft group over G. If $\{(H_i, K_i) : i \in I\}$ is a non-empty of the normal soft subgroups of (F, A) where I is an index set. Then;*

(i) $\bigcap\limits_{i\in I}(H_i, K_i)$ *is a normal soft subgroup of* (F, A).
(ii) $\bigwedge\limits_{i\in I}(H_i, K_i)$ *is a normal soft subgroup of* (F, A).
(iii)If $K_i \cap K_j = \phi$ *for all* $i, j \in I$, *then* $\bigvee\limits_{i\in I}(H_i, K_i)$ *is a normal soft subgroup of* (F, A).

2.2.2 Cyclic soft groups

Definition 2.2.9. *[4, Definition 28] Let* (F, A) *be a soft group over* G *and* X *be an element of* $P(G)$. *The set* $\{(a, \langle x\rangle) : F(a) = \langle x\rangle, x \in X\}$ *is called a soft subset of* (F, A) *generated by the set* X *and denoted by* $\langle X\rangle$. *If* $(F, A) = \langle X\rangle$, *then the soft group* (F, A) *is called the cyclic soft group generated by* X.

Theorem 2.2.10. *[4, Theorem 30] Let* (F, A) *be a finite group. If*

(i) (F, A) *is an infinite cyclic soft group generated by* X, *then* $|(F, A)| = |X|$.

(ii) (F, A) *be a soft group on* G. *If the order of* G *is prime, then* (F, A) *is a cyclic soft group.*

(iii) A soft subgroup of a cyclic soft group is cyclic soft group.

2.3 Soft Rings

From now on, R denotes a unitary commutative ring and all soft sets are considered over R.

Definition 2.3.1. *[2, Definition 2.9] Let* (F, A) *be a soft set. The set* $Supp(F, A) = \{x \in A : F(x) \neq \phi\}$ *is called the support of the soft set* (F, A). *A soft set is said to be non-null if its support is not equal to the empty set.*

Definition 2.3.2. *[2, Definition 3.1] Let* (F, A) *be a non-null soft set over a ring* R. *Then* (F, A) *is called a soft ring over* R *if* $F(x)$ *is a subring of* R *for all* $x \in A$.

Theorem 2.3.3. *[2, Theorem 3.3] Let (F, A) and (G, B) be soft rings over R. Then*

(i) $(F, A)\widetilde{\wedge}(G, B)$ is a soft ring over R if it is non-null.

(ii) The Bi-intersection $(F, A)\widetilde{\sqcap}(G, B)$ is a soft ring over R if it is non-null.

Definition 2.3.4. *[2, Definition 3.4] Let (F, A) and (G, B) be soft rings over R. Then (G, B) is called a soft subring of (F, A) if*

(i) $B \subset A$.

(ii) $G(x)$ is a subring of $F(x)$, for all $x \in Supp(G, B)$.

Theorem 2.3.5. *[2, Theorem 3.6] Let (F, A) and (G, B) be soft rings over R.*

(i) If $G(x) \subset F(x)$, for all $x \in B \subset A$, then (G, B) is a soft subring of (F, A).

(ii) $(F, A)\widetilde{\sqcap}(G, B)$ is a soft subring of both (F, A) and (G, B) if it is non-null.

Theorem 2.3.6. *[2, Theorem 3.8] Let $(F_i, A_i)_{i\in I}$ be a non-empty family of soft rings over R. Then*

(i) $\widetilde{\bigwedge}_{i\in I}(F_i, A_i)$ is a soft ring over R if it is non-null.

(ii) $\widetilde{\sqcap}_{i\in I}(F_i, A_i)$ is a soft ring over R if it is non-null.

(iii) $\widetilde{\bigcup}_{i\in I}(F_i, A_i)$ is a soft ring over R if $\{A_i : i \in I\}$ are pairwise disjoint.

2.3.1 Soft ideal

In classical algebra, the notion of ideals is very important. For this reason, in [2, Definition 4.1] there is an introduction of soft ideals of a soft ring. Note that, if I is an ideal of a ring R, we write $I \lhd R$.

Definition 2.3.7. *[2, Definition 4.1] Let (F, A) be a soft ring over R. A non-null soft set (γ, I) over R is called soft ideal of (F, A), which will be denoted by $(\gamma, I)\tilde{\lhd}(F, A)$, if it satisfies the following conditions:*

(i) $I \subset A$.

(ii) $\gamma(x)$ is an ideal of $F(x)$ for all $x \in Supp(\gamma, I)$.

Theorem 2.3.8. *[2, Theorem 4.3] Let* (γ_1, I_1) *and* (γ_2, I_2) *be soft ideals of a soft ring* (F, A) *over* R*. Then* $(\gamma_1, I_1)\widetilde{\sqcap}(\gamma_2, I_2)$ *is a soft ideal of* (F, A) *if it is non-null.*

Theorem 2.3.9. *[2, Theorem 4.4] Let* (γ_1, I_1) *and* (γ_2, I_2) *be soft ideals of soft rings* (F, A) *and* (G, B) *over* R*, respectively. Then* $(\gamma_1, I_1)\widetilde{\sqcap}(\gamma_2, I_2)$ *is a soft ideal of* $(F, A)\widetilde{\sqcap}(G, B)$ *if it is non-null.*

Theorem 2.3.10. *[2, Theorem 4.6] Let* (F, A) *be a soft ring over* R *and* (γ_1, I_1) *and* (γ_2, I_2) *are soft ideals of* (F, A) *over* R*. If* I_1 *and* I_2 *are disjoint, then* $(\gamma_1, I_1)\widetilde{\sqcup}(\gamma_2, I_2)$ *is a soft ideal of* (F, A)*.*

Theorem 2.3.11. *[2, Theorem 4.7] Let* (F, A) *be a soft ring over* R *and* $(\gamma_k, I_k)_{k\in K}$ *be a non-empty family of soft ideals of* (F, A)*. Then*

(i) $\widetilde{\sqcap}_k(\gamma_k, I_k)$ *is a soft ideal of* (F, A) *if it is non-null.*

(ii) $\widetilde{\wedge}_k(\gamma_k, I_k)$ *is a soft ideal of* (F, A) *if it is non-null.*

(iii) If $\{I_k : k \in K\}$ *are pairwise disjoint, then* $\widetilde{\cup}_k(\gamma_k, I_k)$ *is a soft ideal of* (F, A) *if it is non-null.*

2.3.2 Idealistic soft ring

Let (F, A) be a non-null soft set over R. Then (F, A) is called an idealistic soft ring over R if $F(x)$ is an ideal of R for all $x \in Supp(F, A)$. The trivial and whole soft ring is as follows;

Proposition 2.3.12. *[2, Proposition 5.3]Let* (F, A) *be an idealistic soft ring over* R *and* $B \subset A$*. Then* (F, B) *is also idealistic soft ring.*

Theorem 2.3.13. *[2, Theorem 5.4]Let* (F, A) *and* (G, B) *be an idealistic soft ring over* R*. Then* $(F, A)\,\widetilde{\sqcap}\,(G, B)$ *is an idealistic soft ring if it is non null.*

Theorem 2.3.14. *[2, Theorem 5.5] Let (F, A) and (G, B) be an idealistic soft ring over R. If $A \cap B = \phi$, then $(F, A) \widetilde{\cup} (G, B)$ is an idealistic soft ring.*

Definition 2.3.15. *[2, Definition 5.9] An idealistic soft ring (F, A) over a ring R is said to be trivial if $F(x) = \{0\}$ for all $x \in A$. An idealistic soft ring (F, A) over R is said to be whole if $F(x) = R$ for all $x \in A$.*

2.4 Soft Modules

In this section we recall some basic concepts of soft module. Sun et al., [99], gave the basic concept of soft modules which gives the practical approach to soft set theory in the direction of modules.

Definition 2.4.1. *[99, Definition 10] A soft set (G, B) over an R-module M is called a soft module if each $G(b)$ is a submodule of M, for all $b \in Supp(G, B)$.*

Proposition 2.4.2. *[99, Proposition 3] Let (G, B) and (G', B') are two soft modules over M. Then*

(i) $(G, B)\tilde{\cap}(G', B')$ is soft module over M.

(ii) $(G, B)\tilde{\cup}(G', B')$ is soft module over M if $B \cap B' = \phi$.

2.4.1 Soft submodules

Definition 2.4.3. *[99, Definition 13] Let (G, B) be a soft module over an R-module M. Then (H, C) be a soft submodule over (G, B) if*

(i) $C \subset B$

(ii) $H(c)$ is submodule of $G(c)$, for all $c \in Supp(H, C)$.

Proposition 2.4.4. *[99, Proposition 7] Let (G, B) be a soft module over M, and $\{(G_i, B_i)|i \in I\}$ be a non-empty family of soft submodules of (G, B). Then*

(i) $\sum\limits_{i\in I}(G_i, B_i)$ *is soft submodule of* (G, B).
(ii) $\bigcap\limits_{i\in I}(G_i, B_i)$ *is soft submodule of* (G, B).
(iii) $\bigcup\limits_{i\in I}(G_i, B_i)$ *is soft submodule of* (G, B), *if* $B_i \cap B_j = \phi$ *for all* $i, j \in I$.

Definition 2.4.5. *[99, Definition 13] Let* (H, C) *be a soft submodule of a soft module* (G, B) *over a module* M. *is called maximal soft submodule of* (G, B) *if* $H(b)$ *is a maximal submodule of* $G(b)$ *for all* $b \in C$.

2.4.2 Sums of soft submodules

Definition 2.4.6. *[102, Definition 9] Let* (G, B) *be a soft module over* M *and* $\{(G_i, B_i)\}_{i\in I}$ *are the collection of soft submodules of* (G, B), *where* I *is the non empty subset. The sum of submodules* $\{(G_i, B_i)\}_{i\in I}$ *is defined as* $\sum\limits_{i\in I}(G_i, B_i) = (H, \bigcup\limits_{i\in I} B_i)$ *such that* $H(b) = \sum\limits_{i\in I(b)} G_i(b)$ *for all* $b \in \bigcup\limits_{i\in I} B_i$ *and* $I(a)$ *is the set of all elements* $i \in I$ *such that* $a \in B_i$.

Theorem 2.4.7. *[102, Theorem 1] Let* (G, B) *be a soft module over* M *and* $\{(G_i, B_i)\}_{i\in I}$ *are the collection of soft submodules of* (G, B), *where* I *is the non empty subset. Then* $\sum\limits_{i\in I}(G_i, B_i)$ *is a soft submodule of* (G, B).

2.5 Decision Making Techniques based on Theory of Soft sets

The soft set has grabbed the huge attention of the experts due to its finest applications in various kind of sensitive decision-making situations. We going to provide a quick overview of such successful attempts.

Let us begin with [72], in which the Molodstov proposed an extremely efficient way of handling the information by means of the theory of Soft sets. Almost all of classical methods were not that much efficient in information handling, as compared to proposed method based on soft set theory. The classical methods were more computationally complex and less accurate, while the Molodstov's approach based on the soft set theory, turned out to be more accurate and computationaly feasible. The success story of theory of soft sets does not ends at decision making, it has shown a great deal of applications in areas like data analysis [107, 45], clustering attribute [80, 68], maximal association rules mining [46], parameterization reduction [25], texture classification [73], classification of musical instruments [59], flood alarming, game theory, operation research.

Maji and Roy [66], were the first to initiate the application of soft and rough sets to deal with the decision-making problems. The choice parameter is formulated to choose the optimal object. Chen [25] came up with the idea of the parameterization reduction of a soft set and gave its application to decision-making problems. Chen suggested that sub-optimal choice of object is redundant while the decision-making problem can be dealt by the direct method of optimal choice of an object corresponding to the respective soft reduction. Kong et al., [53] proposed the method of normal parameterization reduction, as the second step to optimal decision choice, when in the first step the Chen's method of parameter reduction is applied on soft set. With this method of normal parameterization reduction, a technique is suggested to characterize the choice objects in accordance with the results of decision method.

Çağman and Enginoğlu [20] investigated soft matrix theory and presented the classical soft sets in the form of matrices. The advantage of writing the soft sets as matrices, i.e., soft matrices is that such matrices require the less computational complexity, easily programmable and require less storage capacity. Further, Çağman and Enginoğlu in [21], proposed uni-int decision making algorithm which selects a set of optimum elements from two different decision-making processes. The optimal element is selected by using uni-int operators in the reduction of parameters. The method has its own discrepancy as it is difficult to operate for more than two soft sets. Feng et al., [38] improved and extended the technique of [21] from two soft sets to k soft sets.

Qin et al., [81], developed a new method of decision-making algorithm based on soft sets, which was less computationally complex from all other existing algorithms. Their proposed algorithm enjoys the choice value and comparative score based approach for various situations requiring the optimal decision making.

2.5.1 Decision making through fuzzy soft sets

An important class of soft sets is the fuzzy soft. The Roy and Maji [85], were the first to developed an algorithm based on decision-making problem that includes the choice value to find an optimally efficient object from the fuzzy soft sets. The Kong et al., [54] discovered some discrepancies in Roy's method and came up with correct revised version of the numerical algorithm. For the revised algorithm, they employed the Grey relational analysis on fuzzy soft sets. Çağman et al., [22] came up with an alternate definition of a fuzzy soft set (involving fuzzy aggregate operator) and their application for the process of decision making. Next, the Çağman et al., [18] introduced fuzzy parameterized (FP-) soft set whose parameters are fuzzy sets. By using these products, AND-FP-soft decision making and OR-FP-soft decision-making methods were constructed. The decision algorithm was used to select the optimal objects. Çağman et al., [17], defined the concept of fuzzy parameterized fuzzy soft set (FPFS-set). The properties of fuzzy parameterized fuzzy soft set are also discussed in detail. Kuang et al., [57, 58], developed an interesting definition of the triangular fuzzy soft set and trapezoidal fuzzy soft sets. He not only investigated the relevant operating properties of the mentioned sets but also built the corresponding decision-making model. The decision-making process became more realistic, and the decision-making results got by the integrated operation is more reliable.

To address the divergence of different opinions, Feng et al., [36] introduced level soft sets and initiated an adjustable decision-making scheme using fuzzy soft sets. Based on Feng' works, Basu et al., [9] further investigated the fuzzy soft set based decision making and introduced a more efficient fuzzy soft set based decision-making method, namely, the mean potentiality approach. Kong et al., [55] gives fuzzy soft set decision-making methods based on grey theory. In this method different decision makers has different opinion in various aspects but they should have the common goal to reach the destination. The most appropriate alternative is chosen from the set of feasible alternatives. The results of the alternative are classified according to choice values.

2.5.2 Decision making through intuitionistic fuzzy soft set

In 2004, Maji et al., [64] introduced the notion of intuitionistic fuzzy soft set theory. Different algebraic operations have also been studied in the context of the intuitionistic fuzzy soft set. Cagman et al., [19], redefined the concept of intuitionistic fuzzy soft sets and studied some of its algebraic structure on intuitionistic fuzzy soft sets. Jiang et al., [42] generalized the adjustable approach to decision-making problem based on intuitionistic fuzzy soft set. For this purpose, the level soft sets of intuitionistic fuzzy soft sets were employed. The notion of weighted intuitionistic fuzzy soft sets gave a practical framework to decision-making problem. Finally, Das and Kar in a [30], gave a method to solve group decision problem by intuitionistic fuzzy soft set. For instance, on a particular disease, several experts gave their expert opinion. Then a confident weight is assigned to each of the experts which depend on their prescribed opinions. Moreover, the concept of cardinal has been used to compute the weight for final consensus.

2.5.3 Decision making through neutrosophic soft sets

Maji [63] proposed a hybrid structure is called neutrosophic soft set, which is a combination of neutrosophic set [96] and soft sets. They defined several operations on neutrosophic soft sets and made a theoretical study on the theory of neutrosophic soft sets. After the emergence of neutrosophic soft set, many scholars have made a lot of contributions in this field, for instance see [13, 14, 32, 48, 86, 87]. In recent times, the Deli in [32] has defined the notion of neutrosophic soft set relation and application of neutrosophic soft set operations to make more functional [33]. After the introduction of relation on neutrosophic soft set Broumi et al., [15] examined relations of the interval-valued neutrosophic soft set and defined the algorithm for decision making. Many interesting applications of the neutrosophic set theory have been combined with soft sets in [16, 33].

Chapter 3

Decision making and grading of S-boxes based on interval valued fuzzy soft sets

The key aim of the chapter is put into action the method for the selection of secure S-box by using interval-valued fuzzy soft set to the decision making. Each analysis parameter is transformed into the interval value fuzzy set. By giving an application in decision making which can refine our choice on a selection of most feasible S-box.

3.1 Interval-valued fuzzy set

The interval-valued fuzzy set was firstly introduced, in [106], and further developed by Yang et al., [104]. The Yang studied the interval-valued set along with soft set theory and gave a new destination in the soft set known as an interval-valued fuzzy soft set theory. The focus on the fuzzy function provided the results which may not be clear for decisions. Therefore, we introduce the notion of an upper and lower degree of interval-valued fuzzy sets. It turns out that the interval-valued fuzzy soft set approach for comparison of data provides an efficient way to approach the decision. Finally, the decision of the best S-box has been made over the ranking of computed values.

Throughout this work, S denotes universal set, E is the set of parameters. For fundamentals of Soft set theory we refer to [72].

Definition 3.1.1. *[106] An interval-valued fuzzy set $\tilde{F}$ is defined as;*

$$\tilde{F} : E \longrightarrow Int([0,1])$$

where $Int([0,1])$ denotes the set of all closed subintervals of $[0,1]$.

For all $x \in U$, $\mu(x) = [\mu^{+}(x), \mu^{-}(x)]$ is called the degree of membership of an element $x \in U$, where $\mu^{+}(x)$ and $\mu^{-}(x)$ are the lower and upper degrees membership of x to U respectively such that

$$0 \leq \mu^{+}(x) \leq \mu^{-}(x) \leq 1.$$

Next we give a formal definition of interval-valued fuzzy soft set.

Definition 3.1.2. *[104] An interval-valued fuzzy soft set (F, E) over a universe U is a mapping that maps E into $P(U)$ i.e.*

$$F : E \longrightarrow P(U),$$

where $P(U)$ for the set of all closed subintervals fuzzy sets of U.

Cryptographic Properties of Boolean functions

The security of modern cryptographic networks relies heavily on the various kind of the algebraic structures. Our aim here is to choose the most efficient S-box, based on interval-valued fuzzy soft sets. In order to make the optimally efficient choice, we will employ the non-linearity, BIC, SAC, BIC-SAC, Differential approximation probability and linear approximation probability analysis. For the detailed description of mentioned list of analyses, we refer the reader to section 2 of chapter 1. Here in this section, we have to take these analysis results of some renowned S-boxes. The differential approximation probability for different S-boxes is given in Table $1, 2, 3$ and 4.

S-boxes	Nonlinearity			SAC		
	Max	Min	Avg.	Max	Min	Avg.
S_1	4	2	3.5	0.6250	0.3750	0.4922
S_2	4	2	3.5	0.7500	0.2500	0.5000
S_3	4	4	4	0.5000	0.5000	0.5000
S_4	4	2	3.5	0.6250	0.3750	0.4531
S_5	4	4	4	0.6250	0.2500	0.4375
S_6	4	2	3.5	0.7500	0.2500	0.4688

Table 3.1:Nonlinearity and SAC analyses for small S-boxes.

S-boxes	BIC-Nonlinearity			BIC-SAC		
	Max	Min	Avg.	Max	Min	Avg
S_1[27]	4	0	2.5	0.6250	0.4167	0.5052
S_2[74]	4	0	2.5	0.5833	0.4167	0.4688
S_3[12]	4	0	2.75	0.5833	0.4167	0.4688
S_4[71]	4	0	2.5	0.5833	0.4167	0.5000
S_5[10]	4	0	2.5	0.5417	0.4167	0.5000
S_6[34]	4	0	3.0	0.5417	0.4167	0.4739

Table 3.2 : BIC-Nonlinearity and BIC-SAC for small S-boxes

S-boxes	Differential Approximation Probability			Linear Approximation Probability		
	Max	Min	Avg.	Max	Min	Avg
S_1[27]	1	0.250	0.3672	0.375	0.375	0.375
S_2[74]	1	0.250	0.3672	0.25	0.25	0.25
S_3[12]	1	0.250	0.3281	0.25	0.25	0.25
S_4[71]	1	0.250	0.3516	0.375	0.375	0.375
S_5[10]	1	0.125	0.0305	0.375	0.375	0.375
S_6[34]	1	0.125	0.3125	0.375	0.375	0.375

Table 3.3 : Differential approximation probability and linear approximation probability.

S-boxes	N.L	SAC	BIC	B/S	DAP	LAP
S_1[27]	3.5	0.4922	2.5	0.5052	0.3672	0.375
S_2[74]	3.5	0.5000	2.5	0.4688	0.3672	0.25
S_3[12]	4	0.5000	2.75	0.4688	0.3281	0.25
S_4[71]	3.5	0.4531	2.5	0.5000	0.3516	0.375
S_5[10]	4	0.4375	2.5	0.5000	0.0305	0.375
S_6[34]	3.5	0.4688	3.0	0.4739	0.3125	0.375

Table 3.4 : The average nonlinearity, SAC, BIC-Nonlinearity, BIC-SAC, Differential approximation probability and Linear approximation probability.

Before proceeding further, let us recall the definition interval-valued fuzzy set and interval-valued fuzzy soft set with related terms.

3.2 Proposed interval valued fuzzy soft set in decision making

In this section, we are going to suggest and put in action a decision-making algorithm based on interval-valued fuzzy soft set operator. Let me provide a detailed step by step account of the algorithm.

Algorithm Assume that we have been a set of S-box and a set of parameters. Then following set of steps should be followed for an efficient optimal decision.

Step 1. Insert the data set for each object $S_i \in U$.

Step 2. Compute the lower and upper degrees of membership $e \in E$, where $0 \leq \mu_i^-(e) \leq \mu_i^+(e) \leq 1$.

Step 2. Transform an interval-valued fuzzy sets into soft set.

Step 3. Compute the sum of lower and upper degrees of membership for $e \in E$.

Step 4. Compute the result d_i. The optimal decision is $\max\limits_{1 \leq i \leq n}\{d_i\}$.

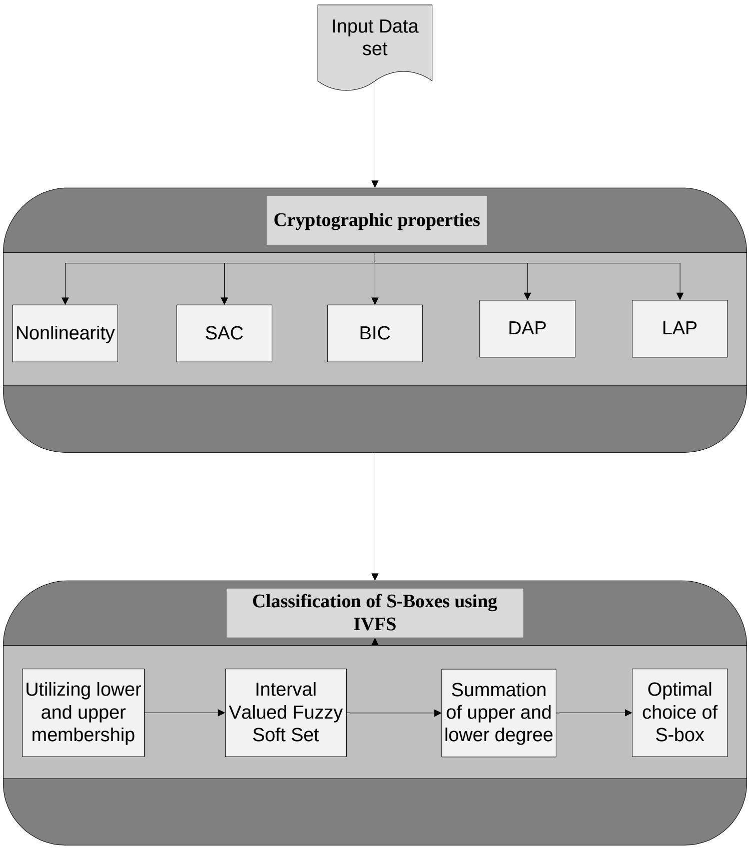

Fig. 3.1 : Flow chart of proposed selection criteria.

3.3 Interval valued fuzzy soft set for classifying the strength of S-box

Let $\{S_1, S_2, \cdots, S_6\}$ be a set of S-boxes mentioned in above section and $E = \{e_1, e_2, \cdots, e_6\}$ be the set of parameters stands for non-linearity, SAC, BIC,

BIC-SAC, DAP, LAP. Table 4 is used as a data set. Now we will give the computational formulas of computing the lower and upper grades for each analysis.

3.3.1 Formula for computing the lower and upper degrees

The interval valued fuzzy set for each analyses parameter of S-box are defined as follows;

Interval valued fuzzy set for Non-linearity

$$[\mu_1^-(S_i), \mu_1^+(S_i)] = \left[\frac{\max(e_1)}{avg(e_1)}, \frac{\min(e_1)}{6 * avg(e_1)}\right],$$

where e_1 stands for non-linearity of S-boxes.

Interval valued fuzzy set for SAC

$$[\mu_2^-(S_i), \mu_2^+(S_i)] = \left[\frac{avg(e_2)}{\max(e_2)}, (avg(e_2) - \min(e_2))\right],$$

where e_2 stands for SAC of S-boxes.

Interval valued fuzzy set for BIC

$$[\mu_3^-(S_i), \mu_3^+(S_i)] = \left[\frac{avg(e_3)}{\max(e_3)}, \frac{\max(e_3) - avg(e_3)}{4 * \min(e_3)}\right],$$

e_3 stands for BIC of S-boxes.

Interval valued fuzzy set for BIC-SAC

$$[\mu_4^-(S_i), \mu_4^+(S_i)] = \left[\frac{avg(e_4)}{\max(e_4)}, \frac{\max(e_4) - avg(e_4)}{6}\right],$$

where e_4 stands for BIC-SAC of S-boxes.

Interval valued fuzzy set for DAP

$$[\mu_5^-(S_i), \mu_5^+(S_i)] = \left[(\max(e_5) - avg(e_5)), \frac{avg(e_5) - \min(e_5)}{6}\right],$$

where e_5 stands for DAP of S-boxes.

Interval valued fuzzy set for LAP

$$[\mu_6^-(S_i), \mu_6^+(S_i)] = \left[(1 - avg(e_6)), \frac{avg(e_6)}{2}\right],$$

where e_6 stands for LAP of S-boxes.

3.3.2 Interval-valued fuzzy soft set

Consider the following set of tables based on above mentioned formulas. The interval-valued fuzzy soft set describes the analyses parameters of the candidates as follows,

S-boxes	μ_1^-	μ_1^+	μ_2^-	μ_2^+	μ_3^-	μ_3^+
S_1	0.0952	0.875	0.1172	0.7875	0.25	0.625
S_2	0.0952	0.875	0.25	0.6667	0.25	0.625
S_3	0.1667	1	0	1	0.2083	0.6875
S_4	0.0952	0.875	0.0781	0.725	0.25	0.625
S_5	0.1667	1	0.1875	0.7	0.25	0.625
S_6	0.0952	0.875	0.2188	0.6251	0.1667	0.75

Table 3.5(i) : Interval valued fuzzy soft set.

S-boxes	μ_4^-	μ_4^+	μ_5^-	μ_5^+	μ_6^-	μ_6^+
S_1	0.0148	0.8083	0.1828	0.6328	0.1875	0.625
S_2	0.0087	0.8037	0.1828	0.6328	0.125	0.75
S_3	0.0087	0.8037	0.1882	0.6719	0.125	0.75
S_4	0.0139	0.8572	0.185	0.6484	0.1875	0.625
S_5	0.0139	0.923	0.1213	0.9695	0.1875	0.625
S_6	0.0095	0.8748	0.0953	0.6875	0.1875	0.625

Table 3.5(ii) : Interval valued fuzzy soft set.

3.3.3 Summation of lower and upper degree

The lower degree sum and upper degree sum of each S-box S_i are calculated by using the following formula,

$$\rho_i^- = \sum_{i=1}^{6} \mu_i^-,$$
$$\rho_i^+ = \sum_{i=1}^{6} \mu_i^+.$$

where $i \in E$ and $1 \leq i \leq 6$.

S-boxes	ρ_i^-	ρ_i^+
S_1	0.8475	4.3536
S_2	0.9118	4.3532
S_3	0.6969	4.9131
S_4	0.8097	4.3556
S_5	0.9269	4.8425
S_6	0.7729	4.4374

Table 3.6 : Summation of lower and upper degrees

3.3.4 Analysis result

The result of an object will be given as,

$$d_i = \rho_i^+ - \rho_i^-$$

where $i \in E$ and $1 \leq i \leq 6$.

S-boxes	d_i
S_1	3.5061
S_2	3.4414
S_3	4.2162
S_4	3.5459
S_5	3.9157
S_6	3.6644

Table 3.7 : Decision result of soft set

3.3.5 Grading results

Table 3.7 results are compiling in ascending order to classify the S-boxes. The highest value represent the optimal S-box and is designed as most secure, where as the least valued gives vice versa.

S-boxes	Grading
S_3	4.2162
S_5	3.9157
S_6	3.6644
S_4	3.5459
S_1	3.5061
S_2	3.4414

Table 3.8 : Grading the S-boxes as per values

The S_3 S-box is appropriate one because it is the maximum of rest. Hence using the previously described algorithm for grading S-boxes, we have successfully classified the best S-box for further real applications. Fundamentally, a table is used for drawing the decision for the selection of good S-box.

Chapter 4

Decision making and grading of S-boxes based on intuitionistic fuzzy soft set

Our aim in this chapter is to introduce a new level of classification, by analyzing the eight popular S-boxes on different images. The simulation results of S-boxes on standard images of Airplane and Baboon of size 512×512 (pixels) are employed. Furthermore, putting in action our proposed Intuitionistic Fuzzy Soft set based algorithm, we are going to employ a modified version algorithm for the choice of optimally secure S-boxes. Finally, we have answered the question that is a single S-box can equally work for all images, or we need different S-box for different images?

The flow of the chapter is as follows. To make the work accessible to the reader, the first section has been devoted to preliminaries and necessary explanations. Moreover, in the second section decision-making approach is described in detail. Finally, in the third section, the experiment is performed on the MLC analyzes of the enciphered images of Airplane and Baboon, by different S-boxes. Moreover, the suitable S-box has been sorted out. It turns out that the Xyi S-box has been being the most appropriate in enciphering of the both image, which shows the consistency of our method. Also, we have graded the scores in descending order, to compare the image encryption quality of different S-boxes.

4.1 Intuitionistic Fuzzy Soft set

Throughout this work, S denotes universal set, E is the set of parameters. For fundamentals of Soft set theory we refer to [72]. Cagman and Karatas [23, Definition 1], defined Intuitionistic Fuzzy Soft set and their operations in following manner.

Definition 4.1.1. *Let $P(U)$ be the set of all Intuitionistic Fuzzy sets over U. An **Intuitionistic Fuzzy Soft** set (IFS-set) Γ_E over $P(U)$ is a set defined as following. A function*

$$\gamma_E : E \longrightarrow P(U),$$

*is called an **approximate function** of the IFS-set Γ_E. The value $\gamma_E(x)$, is an Intuitionistic Fuzzy set called $x-$element of Γ_E and it is defined as*

$$\gamma_E(x) = \{(u_i, \mu_{\gamma_E(x)}(u_i), \upsilon_{\gamma_E(x)}(u_i)) : u_i \in U\} \text{ for all } x \in E.$$

Here, the functions μ_E and υ_E respectively denote the membership and non membership degrees of $u_i \in U$. The μ_E and υ_E are maps from U to $[0, 1]$

satisfying,

$$0 \leq \mu_{\gamma_E(x)}(u_i) + \upsilon_{\gamma_E(x)}(u_i) \leq 1, \text{ for all } u_i \in U.$$

We denote IFS-set over $P(U)$ by,

$$\Gamma_E := \{(x, \gamma_E(x)) : x \in E\}. \tag{4.1.2}$$

We now introduce few notions which will be frequently used in our proposed IFS-set decision making method.

Definition 4.1.2. *The **Upper and Lower Evaluations** value of $u_i \in U$ are defined as;*

$$\begin{aligned} \mu^{-}_{E(ij)} &: = \mu_{\gamma_E(x_j)}(u_i), \\ \mu^{+}_{E(ij)} &: = 1 - \upsilon_{\gamma_E(x_j)}(u_i). \end{aligned} \tag{4.1.3}$$

for all $x_j \in E$ and $u_i \in U$, respectively.

Definition 4.1.3. *The **Evaluation Interval** can be given as:*

$$[\mu^{-}_{E(ij)}, \mu^{+}_{E(ij)}]. \tag{4.1.4}$$

*Furthermore, **Sum** of lower value and upper evaluations value of $u_i \in U$ can be computed as;*

$$\begin{aligned} \mu_{E(i)} &: = \sum_{j=1}^{n} \mu^{-}_{E(ij)}, \\ \upsilon_{E(i)} &: = \sum_{j=1}^{n} \mu^{+}_{E(ij)}. \end{aligned} \tag{4.1.5}$$

*Hence the individually **Evaluation Scores** for S-boxes can be given as,*

$$\begin{aligned} s_i &: = \sum_{j=1}^{n} [(\mu_{E(i)} - \mu_{E(j)}) + (\upsilon_{E(i)} - \upsilon_{E(j)})], \\ &= n\left(\mu_{E(i)} + \upsilon_{E(i)}\right) - \sum_{j=1}^{n} (\mu_{E(j)} + \upsilon_{E(j)}). \end{aligned} \tag{4.1.6}$$

Here s_i is evaluation score of each μ_i for $1 \leq i \leq n$. Therefore an optimal ***Evaluation*** *is defined as,*

$$s := \max_{1 \leq i \leq n} \{s_i\}. \tag{4.1.7}$$

4.2 Proposed intuitionistic fuzzy soft set based algorithm for optimal choice of S-box

We propose to carry out following algorithm on data of given seven S-boxes.

Step 1: Choose feasible subsets A and B of the set of parameters E.

Step 2: Construct IFS-sets Γ_A and Γ_B.

Step 3: Write the evaluation interval $[\mu^-_{A\wedge B(ij)}, \mu^+_{A\wedge B(ij)}]$.

Step 4: Compute the evaluation scores s_i.

Step 5: Obtain an evaluation s.

Thus the above five steps are used for decision making method. The best evaluation is chosen as maximum of all evaluation scores. Following is the flow chart of above mentioned algorithm,

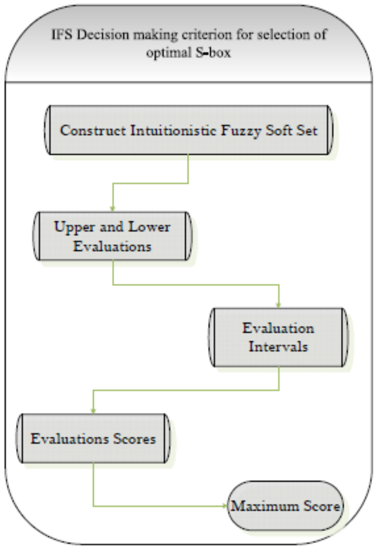

Fig. 1. Flow Chart

4.2.1 Intuitionistic fuzzy soft set for classifying the strength of S-box

Let $U = \{u_1, u_2, \cdots, u_7\}$ be the universal set, where the objects $u_1, u_2, \cdots, u_7$ respectively indicate S-boxes such as AES, APA, residue prime, S_8-AES, Gray, Xyi, and SKIPJACK S-boxes respectively. The parametric set $E = \{e_1, e_2, \cdots, e_5\}$ represents Entropy, Energy, Correlation, Homogeneity and Contrast. We consider different standard images and then classify that, which S-box is suitable in a particular image cipher.

Before tuning in to original calculations, probably, it will be worth recalling some of fundamental details of above mentioned parameters for Intuitionistic fuzzy set.

Function for Entropy The Entropy, scrutinizes the degree of occurrence among the grey level pixels. The IFS-Set for entropy can measured by following described membership and non-membership functions respectively,

$$\begin{aligned} \mu_{\tau_E(e_1)}(u_i) &= \frac{e_1(P)}{e_1(u_i)}, \\ \upsilon_{\tau_E(e_1)}(u_i) &= 2 - \frac{e_1(u_i)}{e_1(P)}. \end{aligned} \tag{4.2.1}$$

Where $e_1(P)$ is the entropy of the plain image and $e_1(u_i)$ is the entropy of ciphered image for the S-box u_i, where $1 \leq i \leq 7$.

Function of Energy It measures uniformity in an image by the amount of square elements from GLMC. The intuitionistic fuzzy set for energy is measured by following described membership and non-membership functions respectively,

$$\begin{aligned} \mu_{\tau_E(e_2)}(s_i) &= 1 - \frac{e_2(u_i)}{e_2(P)}, \\ \upsilon_{\tau_E(e_2)}(s_i) &= \frac{e_2(P) - e_1(u_i)}{e_2(P) + e_1(u_i)}. \end{aligned} \tag{4.2.2}$$

Here $e_2(P)$ is the energy of the plain image and $e_2(u_i)$ is the energy of ciphered image for the S-box u_i and $1 \leq i \leq 7$.

Functions for Correlation The *Correlation coefficient* determines the similarity between original data and coded data. The IFS set for correlation is denoted by e_3 and corresponding membership and non-membership functions, respectively, can be given as,

$$\begin{aligned} \mu_{\tau_E(e_3)}(s_i) &= e_3(P) - e_3(u_i), \\ \upsilon_{\tau_E(e_3)}(s_i) &= \frac{e_3(u_i)}{e_3(P)}. \end{aligned} \tag{4.2.3}$$

Here $e_3(P)$ is the correlation of the plain image and $e_3(u_i)$ is the correlation of ciphered image for the S-box u_i and $1 \leq i \leq 7$.

Function of Homogenity The distribution of elements in the GLMC with respect to main diagonal is used to measure the *Homogeneity.* The IFS set for homogeneity is denoted by e_4 and corresponding membership and non-membership functions, respectively, can be given as,

$$\begin{aligned}
\mu_{\tau_E(e_4)}(s_i) &= \frac{e_4(P)}{e_4(P)+e_4(u_i)}, \\
v_{\tau_E(e_4)}(s_i) &= \frac{e_4(u_i)}{e_4(P)}.
\end{aligned} \tag{4.2.4}$$

where $e_4(P)$ is the homogeneity of the plain image and $e_4(u_i)$ is the homogeneity of ciphered image for the S-box u_i and $1 \leq i \leq 7$.

Function of Contrast The parameter *Contrast* is significant because of fact that it can efficiently measure the variation in the enciphered text. The intuitionistic fuzzy set for contrast is denoted by e_5 and is defined as;

$$\begin{aligned}
\mu_{\tau_E(e_5)}(s_i) &= \frac{e_5(u_i)-e_5(P)}{e_5(u_i)+e_5(P)}, \\
v_{\tau_E(e)}(s_i) &= \frac{1}{e_5(u_i)-e_5(P)}.
\end{aligned} \tag{4.2.5}$$

Where $e_5(P)$ is the contrast of the plain image and $e_5(u_i)$ is the contrast of ciphered image for the S-box u_i and $1 \leq i \leq 7$.

4.3 Decision making algorithm in action

In this section, we have considered different standard S-boxes and used the image encryption technique to analyze them. Furthermore, the decision making steps are carried out to grade the S-boxes.

4.3.1 Decision making on performance indexes of Airplane image

Airplane First let us consider the image of airplane. The results of different S-boxes are as follow;

MLC	Entropy	Energy	Correlation	Homogeneity	Contrast
Plain Image	6.7025	0.2687	0.9429	0.9229	0.2052
AES	6.7178	0.0229	0.0887	0.4904	6.9874
APA	6.7178	0.0243	0.1553	0.5127	6.6436
Prime	6.7178	0.0231	0.1188	0.4826	7.5812
S_8-AES	6.712	0.0297	0.0862	0.4879	7.5812
Gray	6.7178	0.0215	0.1393	0.4836	6.9559
Xyi	6.7178	0.0222	0.0544	0.4698	9.005
SkipJack	6.7178	0.0209	0.0958	0.487	8.2207

Table 4.1. Characteristics of different S-boxes with respect to airplane image

Following Fig. 4.2 gives the comparison of analyses on various S-boxes corresponding to enciphered images.

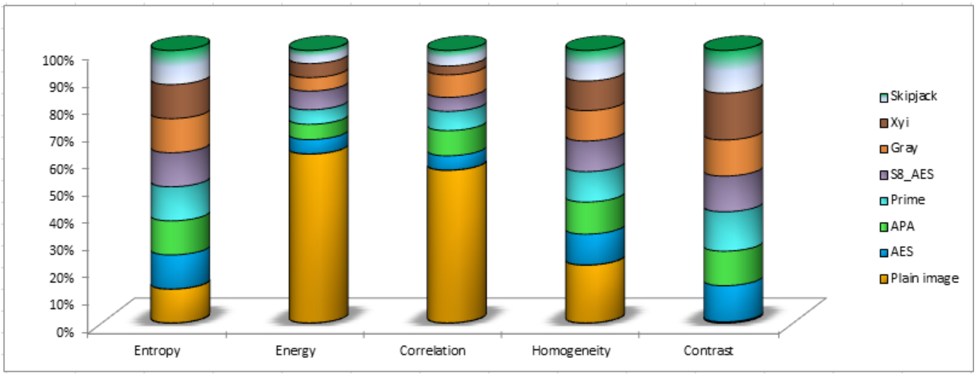

Fig. 4.2 : Comparison of analyses on various S-boxes

The figure shows that entropy and contrast of enciphered images shows the similar trend, in which the performance of Xyi S-box is comparable to that of APA S-box. The energy exhibits the highest result of AES and APA S-boxes. The energy results of S_8 and SkipJack S-boxes are comparative better than that of Xyi S-box.

The Xyi S-box is capable to measure the correlation to the highest level, whereas APA shows the low level performance. It is seen that homogeneity of Xyi S-box is better than SkipJack and Residue Prime S-boxes. The homogeneity of APA S-box is the weak reading as compare to others.

Enciphered images of airplane

A 512×512 (pixel) image of an airplane is considered for encryption and the standard S-boxes are taken for image encryption. Following are the enciphered images of airplane.

Fig. 4.3. Plain image of Airplane

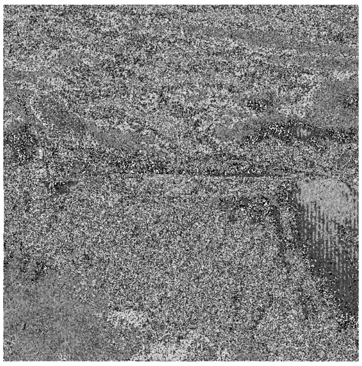

Fig. 4.4 AES transformation

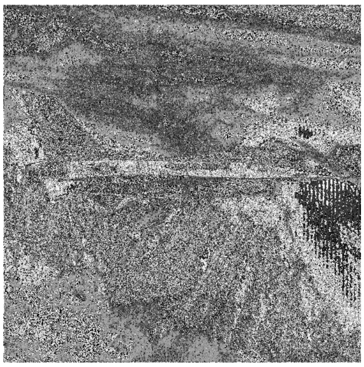

Fig. 4.5. APA transformation

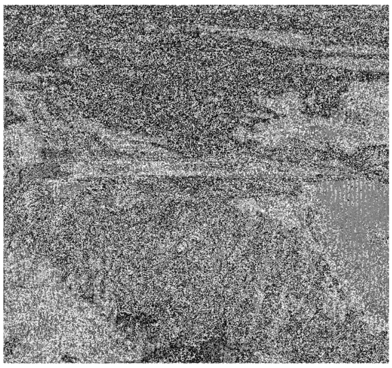

Fig. 4.6. Prime transformation

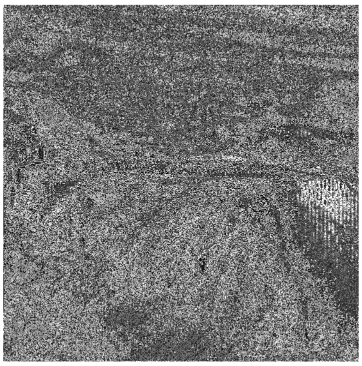

Fig. 4.7. S-8 transformation

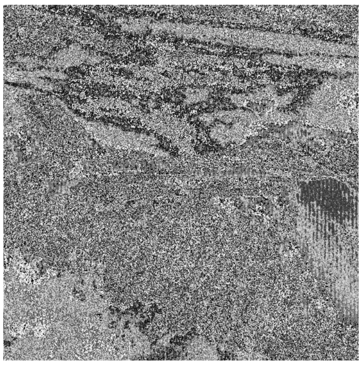

Fig. 4.8. Gray transformation

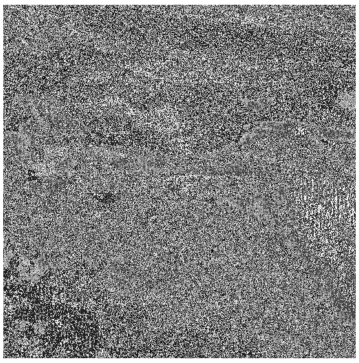

Fig. 4.9. Xyi transformation

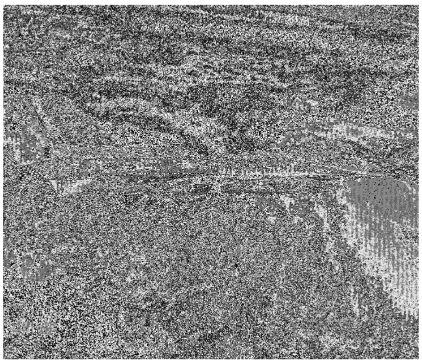

Fig. 4.10. SkipJack transformation

IFS set Choose the IFS-set Γ_E over the universe $IF(U)$. The data from the table **1** has been used for membership and non-membership functions (4.2.1)-(4.2.5). The IFS-set (4.1.2) is represented in following tabular form.

Γ_E	e_1	e_2	e_3	e_4	e_5
u_1	(0.9977,0.4977)	(0.9147,0.3429)	(0.8542,0.4059)	(0.7076,0.3060)	(0.9429,0.3483)
u_2	(0.9977,0.4977)	(0.9096,0.3341)	(0.7876,0.3353)	(0.6966,0.2857)	(0.9401,0.3557)
u_3	(0.9977,0.4977)	(0.9140,0.3417)	(0.8241,0.3740)	(0.7114,0.3132)	(0.9473,0.3371)
u_4	(0.9986,0.4986)	(0.8894,0.3009)	(0.8567,0.4086)	(0.7088,0.3083)	(0.942, 0.3507)
u_5	(0.9977,0.4977)	(0.9199,0.3518)	(0.8036,0.3523)	(0.7109,0.3123)	(0.9427, 0.349)
u_6	(0.9977,0.4977)	(0.9173,0.3474)	(0.8885,0.4423)	(0.7180,0.3253)	(0.9554,0.3162)
u_7	(0.9977,0.4977)	(0.9222,0.3557)	(0.8471,0.3984)	(0.7092,0.3091)	(0.9513,0.3268)

Table 4.2: Intuitionistic fuzzy soft set

The appropriate S-box is chosen by using the membership and non-membership functions of the IFS-set. To make the table 4.2 more clearer we consider the graphical representation of it in figure 4.11. The horizontal axis represents the membership and non-membership functions of the parametric set. The vertical axis represents the scale which vary from 0 to 1. The graph describe the inter relation between the parametric value of IFS-set and S-boxes.

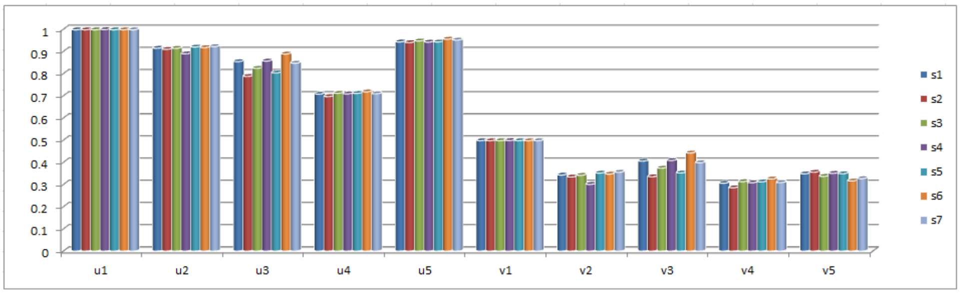

Fig. 4.11 : Relationship between the parametric value of IFS-set and S-boxes.

Evaluation interval of IFS-set The membership and non-membership functions of IFS-set from table 4.2 is apply in equation (4.1.4) and (5.2.4) for lower and upper evaluations. Then using lower and upper evaluations in equation (5.2.5) for evaluation interval. The evaluation intervals are presented in following tabular form;

$[\mu^-_{E(ij)},\mu^+_{E(ij)}]$	e_1	e_2	e_3	e_4	e_5
u_1	(0.9977,0.5023)	(0.9147,0.6570)	(0.8542,0.5941)	(0.7076,0.6940)	(0.9429,0.6517)
u_2	(0.9977,0.5023)	(0.9096,0.6658)	(0.7876,0.6647)	(0.6966,0.7143)	(0.9401,0.6443)
u_3	(0.9977,0.5023)	(0.9140,0.6583)	(0.8241,0.626)	(0.7114,0.6867)	(0.9473,0.6629)
u_4	(0.9986,0.5014)	(0.8894,0.6991)	(0.8567,0.5914)	(0.7088,0.6917)	(0.942,0.6493)
u_5	(0.9977,0.5023)	(0.9199,0.6481)	(0.8036,0.6477)	(0.7109,0.6877)	(0.9427,0.651)
u_6	(0.9977,0.5023)	(0.9173,0.6526)	(0.8885,0.5577)	(0.7180,0.6747)	(0.9554,0.6838)
u_7	(0.9977,0.5023)	(0.9222,0.6443)	(0.8471,0.6016)	(0.7092,0.6908)	(0.9513,0.6732)

Table 4.3: Evaluation intervals

The figure 4.12 shows the the evaluation interval of each S-box. The variation of lower and upper evaluation are gathered in table 4.3. The horizontal axis represents the S-boxes, the membership and non-membership values of the intervals of are graphically more clearly shown. The comparison of figure 4.11 with figure 4.12 shows that difference between membership and non-membership function are significantly less.

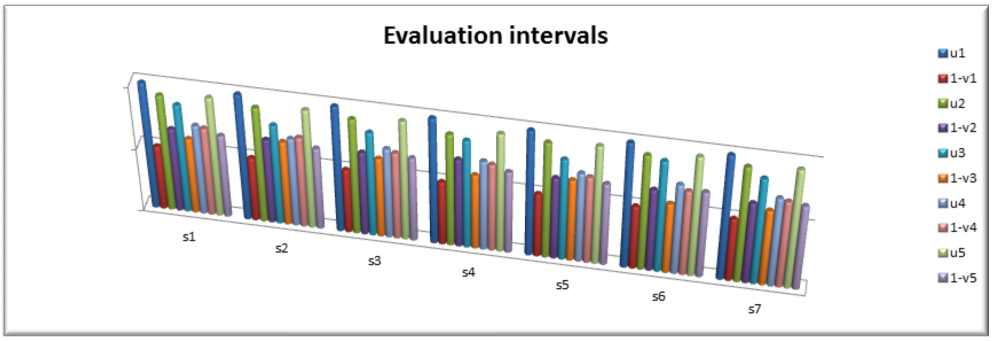

Fig.4.12 : Evaluation interval of different S-boxes

Sum of lower and upper evaluations Once again using the tables computed in table 4.3 into equation (4.1.5), we get following table of the membership and non-membership functions for each S-box,

$\mu_{E(1)}$	$=\Sigma\, \mu^-_{E(1i)}$	=0.9977+0.9148+0.8542+0.7076+0.9429	=4.4172
$\nu_{E(1)}$	$=\Sigma\, \mu^+_{E(1i)}$	=0.5023+0.6571+0.5941+0.6939+0.6517	=3.0991
$\mu_{E(2)}$	$=\Sigma\, \mu^-_{E(2i)}$	=0.9977+0.9096+0.7876+0.6966+0.9401	=4.3315
$\nu_{E(2)}$	$=\Sigma\, \mu^+_{E(2i)}$	=0.5023+0.6659+0.6647+0.7143+0.6443	=3.1913
$\mu_{E(3)}$	$=\Sigma\, \mu^-_{E(3i)}$	=0.9977+0.9140+0.8241+0.7115+0.9473	=4.3946
$\nu_{E(3)}$	$=\Sigma\, \mu^+_{E(3i)}$	=0.5023+0.6583+0.6259+0.6867+0.6629	=3.1362
$\mu_{E(4)}$	$=\Sigma\, \mu^-_{E(4i)}$	=0.9986+0.8895+0.8567+0.7088+0.9420	=4.3955
$\nu_{E(4)}$	$=\Sigma\, \mu^+_{E(4i)}$	=0.5014+0.6991+0.5914+0.6917+0.6493	=3.1328
$\mu_{E(5)}$	$=\Sigma\, \mu^-_{E(5i)}$	=0.9977+0.9199+0.8036+0.7109+0.9427	=4.3749
$\nu_{E(5)}$	$=\Sigma\, \mu^+_{E(5i)}$	=0.5023+0.6482+0.6477+0.6877+0.6510	=3.1369
$\mu_{E(6)}$	$=\Sigma\, \mu^-_{E(6i)}$	=0.9977+0.9174+0.8885+0.7181+0.9554	=4.4771
$\nu_{E(6)}$	$=\Sigma\, \mu^+_{E(6i)}$	=0.5023+0.6526+0.5577+0.6747+0.6838	=3.0710
$\mu_{E(7)}$	$=\Sigma\, \mu^-_{E(7i)}$	=0.9977+0.9222+0.8471+0.70927+0.9513	=4.4276
$\nu_{E(7)}$	$=\Sigma\, \mu^+_{E(7i)}$	=0.5023+0.6443+0.6016+0.6908+0.6732	=3.1122

Table 4.4: Sum of upper and lower evaluations

Evaluation scores The evaluation scores for each object s_i is calculated by using the sum of lower and upper evaluations of above table 4.4 with the formula (4.1.6).

$s_1 =$	-0.0843
$s_2 =$	-0.0377
$s_3 =$	0.0177
$s_4 =$	0.0006
$s_5 =$	-0.1152
$s_6 =$	0.1384
$s_7 =$	0.0804

Table 4.5: Scores of different S-boxes.

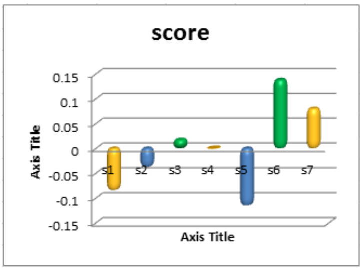

Fig 4.13:

Graphical representation of score.

In Table 4.5, the final score of each S-box given. The figure 4.13 shows the graphical representation of score. On horizontal axis S-boxes are mentioned and scale for score is mentioned on vertical axis.

4.3.2 Grading results for encrypted images of Airplane

The score of S-box represents is being sorting in descending order shows the significance of S-box.

$s_6 =$	0.1384
$s_7 =$	0.0804
$s_3 =$	0.0177
$s_4 =$	0.0006
$s_2 =$	-0.0377
$s_1 =$	-0.0843
$s_5 =$	-0.1152

Table 4.6 : Grading the scores from highest to lowest values.

Maximum Score The maximum score sort out the appropriate S-box for image encryption. It is denoted by s, and defined in equation (4.1.7) the result is;

$$s = \quad s_6 = \quad 0.1384$$

which represents the Xyi S-box as the optimal.

4.3.3 Decision making on performance indexes of Baboon image

Baboon The second image to test the decision making analysis is the image of Baboon. The results of different S-boxes are as follow;

MLC	Entropy	Energy	Correlation	Homogeneity	Contrast
Plain Image	7.3583	0.1094	0.8232	0.8098	0.5085
AES	7.7067	0.0183	0.0196	0.4267	8.4229
APA	7.7067	0.0183	0.0581	0.4327	8.081
Prime	7.7067	0.0171	0.0323	0.4211	8.9211
S_8-AES	7.6932	0.0178	0.0275	0.429	8.1915
Gray	7.7067	0.0187	0.0196	0.4301	8.3561
Xyi	7.7067	0.018	0.0069	0.4239	8.2848
SkipJack	7.7067	0.0189	0.0267	0.4318	7.8404

Table 4.7: Characteristics of different S-boxes with respect to Baboon image

Following are the comparison of parameters corresponding to different S-boxes.

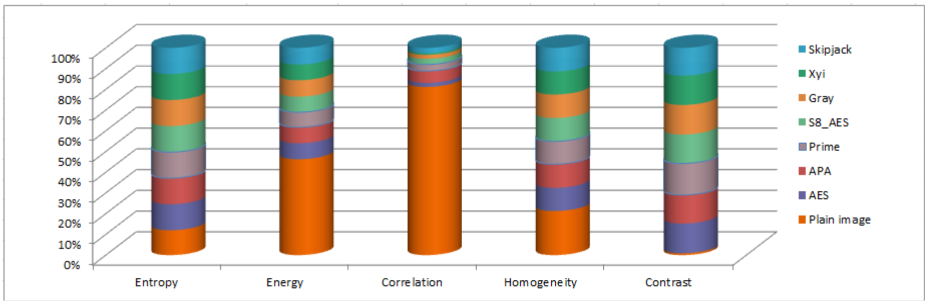

Fig 4.14: Comparison of different analyses of S-boxes.

The horizontal axis show the parametric set and its variation on different S-boxes. The variation of S-boxes on entropy and contrast are nearly same, whereas homogeneity of different S-box shows small variation with respect to plain image. The energy analysis show that Prime and Gray S-boxes are squeeze than other mentioned S-boxes. Correlation analysis of AES and Gray are better, while the APA S-box show the worse result.

Enciphered images of Baboon

A 512×512 (pixel) image of an baboon is taken for encryption. The standard S-boxes are taken for image encryption. Following are the enciphered images of Baboon.

Fig. 4.15: Plain image of Baboon

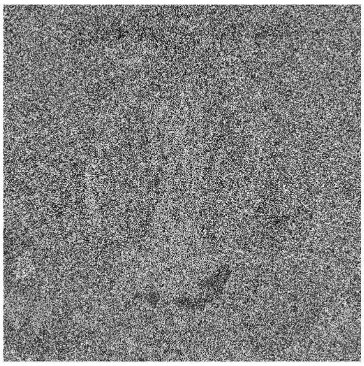

Fig. 4.16: AES transformation

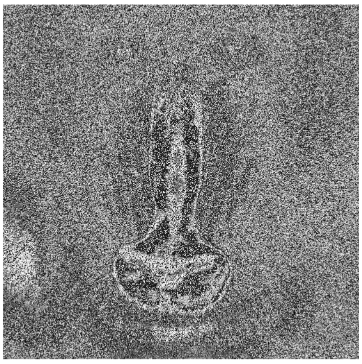

Fig. 4.17: APA transformation

Fig. 4.18: Prime transformation

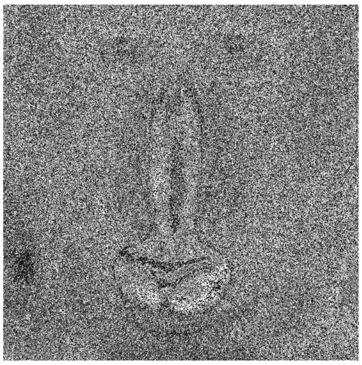

Fig. 4.19: S-8 transformation

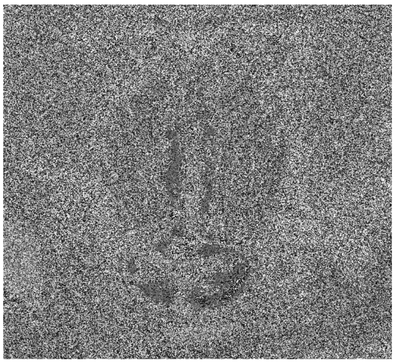

Fig. 4.20: Gray transformation

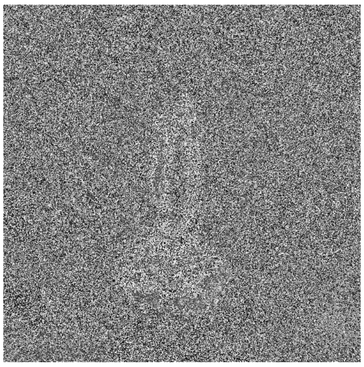

Fig. 4.21: Xyi transformation

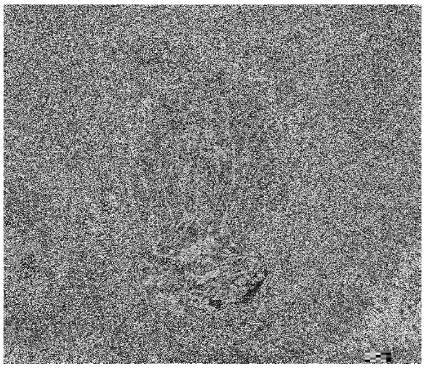

Fig. 4.22: SkipJack transformation

IFS set Choose the IFS-set Γ_E over the universe $IF(U)$. The data from the table 4.7 has been used for membership and non-membership functions

(6.2.1)-(6.2.5). The IFS-set (4.1.2) is represented in following tabular form.

Γ_E	e_1	e_2	e_3	e_4	e_5
u_1	(0.9548,0.4548)	(0.8327,0.2134)	(0.8036,0.4762)	(0.8087,0.3098)	(0.8861,0.6272)
u_2	(0.9548,0.4548)	(0.8327,0.2134)	(0.7651,0.4294)	(0.8048,0.3035)	(0.8816,0.6322)
u_3	(0.9548,0.4548)	(0.8437,0.2296)	(0.7909,0.4608)	(0.8124,0.3158)	(0.8922,0.6205)
u_4	(0.9565,0.4565)	(0.8373,0.2201)	(0.7957,0.4666)	(0.8072,0.3074)	(0.8831,0.6306)
u_5	(0.9548,0.4548)	(0.8291,0.2080)	(0.8036,0.4762)	(0.8065,0.3062)	(0.8853,0.6282)
u_6	(0.9548,0.4548)	(0.8355,0.2174)	(0.8163,0.4916)	(0.8106,0.3128)	(0.8843,0.6292)
u_7	(0.9548,0.4548)	(0.8272,0.2054)	(0.7965,0.4676)	(0.8054,0.3044)	(0.8782,0.636)

Table 4.8: Intuttionistic fuzzy soft set (IFS-set)

The appropriate S-box is chosen by using the membership and non-membership functions of the IFS-set. To make analysis more clearer consider the graphical representation of IFS-set is given figure 4.23. In this graph the membership and non-membership function of each parameter is mentioned on horizontal axis and the vertical axis gives the scale which is from 0 to 1. The graph gives the comparison of different S-boxes with respect to membership and non-membership values of parameters.

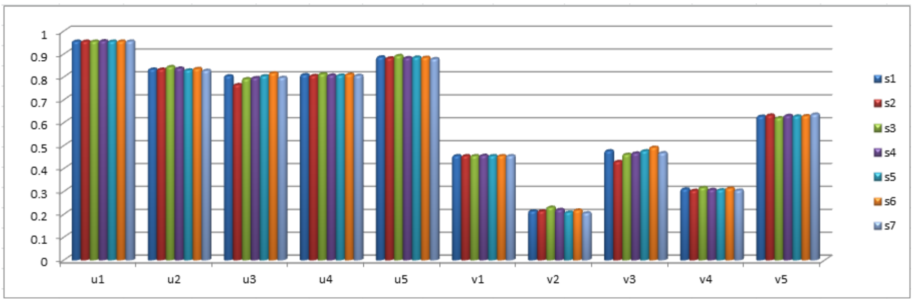

Fig. 4.23 : Comparison of different S-boxes with respect.

Evaluation interval of IFS-set The membership and non-membership functions of IFS-set from table 4.8 is apply in equation (4.1.4) and (5.2.4) for lower and upper evaluations. Then using lower and upper evaluations in equation (5.2.5) for evaluation interval.

$[\mu^{-}_{E(ij)},\mu^{+}_{E(ij)}]$	e_1	e_2	e_3	e_4	e_5
u_1	(0.9548,0.5452)	(0.8327,0.7866)	(0.8036,0.5238)	(0.8087,0.6902)	(0.8861,0.3728)
u_2	(0.9548,0.5452)	(0.8327,0.7866)	(0.7651,0.5706)	(0.8048,0.6965)	(0.8816,0.3678)
u_3	(0.9548,0.5452)	(0.8437,0.7704)	(0.7909,0.5392)	(0.8124,0.6842)	(0.8922,0.3795)
u_4	(0.9565,0.5435)	(0.8373,0.7799)	(0.7957,0.5334)	(0.8072,0.6926)	(0.8831,0.3694)
u_5	(0.9548,0.5452)	(0.8291,0.7920)	(0.8036,0.5238)	(0.8065,0.6938)	(0.8853,0.3718)
u_6	(0.9548,0.5452)	(0.8355,0.7826)	(0.8163,0.5084)	(0.8106,0.6872)	(0.8843,0.3708)
u_7	(0.9548,0.5452)	(0.8272,0.7946)	(0.7965,0.5324)	(0.8054,0.6956)	(0.8782,0.3640)

Table 4.9: Evaluation intervals.

Figure 4.24 and Table 4.9 shows the evaluation interval of each S-box with respect to the parametric membership and non-membership values. It is seen that the variation between parameters ahead to decision making.

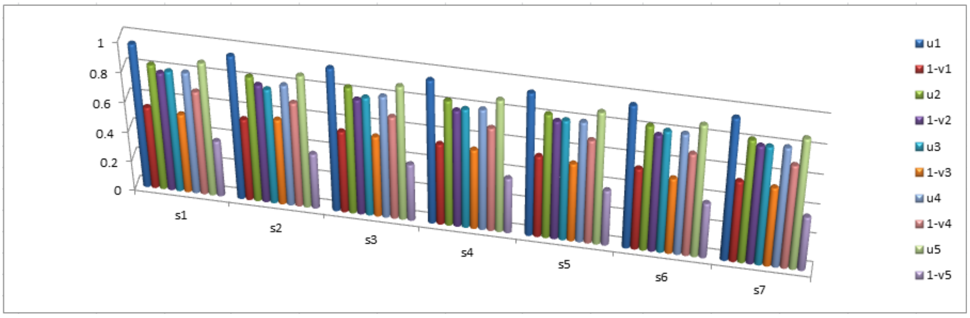

Fig.4.24 : Evaluation interval of each S-box.

Sum of lower and upper evaluations Once again using the values computed in table 4.9 into equation (4.1.5), we get following table of the membership and non-membership functions for each S-box,

$\mu_{E(1)}$	$=\Sigma\, \mu^{-}_{E(1i)}$	=0.9548+0.8327+0.8036+0.8087+0.8861	=4.2859
$\nu_{E(1)}$	$=\Sigma\, \mu^{+}_{E(1i)}$	=0.5452+0.7866+0.5238+0.6901+0.3728	=2.9185
$\mu_{E(2)}$	$=\Sigma\, \mu^{-}_{E(2i)}$	=0.9548+0.8327+0.7651+0.8048+0.8816	=4.2390
$\nu_{E(2)}$	$=\Sigma\, \mu^{+}_{E(2i)}$	=0.5452+0.7866+0.5706+0.6965+0.3678	=2.9666
$\mu_{E(3)}$	$=\Sigma\, \mu^{-}_{E(3i)}$	=0.9548+0.8437+0.7909+0.8124+0.8922	=4.2940
$\nu_{E(3)}$	$=\Sigma\, \mu^{+}_{E(3i)}$	=0.5452+0.7704+0.5392+0.6842+0.3795	=2.9185
$\mu_{E(4)}$	$=\Sigma\, \mu^{-}_{E(4i)}$	=0.9565+0.8373+0.7957+0.8072+0.8831	=4.2798
$\nu_{E(4)}$	$=\Sigma\, \mu^{+}_{E(4i)}$	=0.5435+0.7799+0.5334+0.6926+0.3694	=2.9188
$\mu_{E(5)}$	$=\Sigma\, \mu^{-}_{E(5i)}$	=0.9548+0.8291+0.8036+0.8065+0.8853	=4.2792
$\nu_{E(5)}$	$=\Sigma\, \mu^{+}_{E(5i)}$	=0.5452+0.7919+0.5238+0.6938+0.3718	=2.9266
$\mu_{E(6)}$	$=\Sigma\, \mu^{-}_{E(6i)}$	=0.9548+0.8355+0.8163+0.8106+0.8843	=4.3015
$\nu_{E(6)}$	$=\Sigma\, \mu^{+}_{E(6i)}$	=0.5452+0.7826+0.5084+0.6872+0.3708	=2.8942
$\mu_{E(7)}$	$=\Sigma\, \mu^{-}_{E(7i)}$	=0.9548+0.8272+0.7965+0.8054+0.8782	=4.2621
$\nu_{E(7)}$	$=\Sigma\, \mu^{+}_{E(7i)}$	=0.5452+0.7946+0.5324+0.6956+0.3639	=2.9318

Table 4.10: Sum of upper and lower evaluations

Evaluation scores The evaluation scores for each object s_i by using the values of table 4.10 in the formula given in equation (4.1.6).

$s_1 =$	0.01522
$s_2 =$	0.02308
$s_3 =$	0.0708
$s_4 =$	-0.02629
$s_5 =$	0.02398
$s_6 =$	-0.04732
$s_7 =$	-0.05942

Table 4.11 : Scores

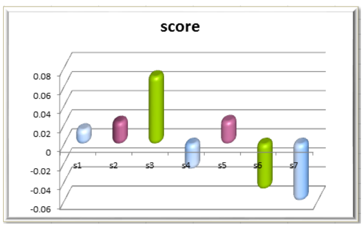

Fig. 4.25: Graphical represntation of S-boxes.

Figure 4.25 and Table 4.11 mention the score of each S-box. From the given score we select the appropriate S-box. In the graph the behavior of S-boxes in image encryption is clearly shown.

4.3.4 Grading results for encrypted images of Baboon

The score of S-box represents in descending order shows the significance of S-box.

$s_3 =$	0.0708
$s_5 =$	0.02398
$s_2 =$	0.02308
$s_1 =$	0.01522
$s_4 =$	-0.02629
$s_6 =$	-0.04732
$s_7 =$	-0.05942

Table 4.12 : Grading scores from highest to lowest.

Maximum Score The maximum score sort out the appropriate S-box for image encryption. It is denoted by s, and defined in equation (4.1.7) the result is;

$$s = \quad s_3 = \quad 0.078$$

which represents the Prime S-box as the appropriate one. It is observe from Table 4.7 that the Prime S-box have significantly better results than other S-boxes.

We have attempted to analyses the quality of S-boxes by applying a decision making algorithm based on Intuitionistic fuzzy soft set. Significant evidence have been found, when proposed methodology is applied on two different images i.e. airplane and Baboon, then it turns out that, for the airplane, the Xyi S-box is the best S-box and prime S-box for Baboon image. This also reflects the scrutiny of the methodology is quite efficient.

Chapter 5

Decision making and grading of S-boxes based on neutrosophic fuzzy soft sets

In this chapter, we are mainly concerned with the MLC-parameters which includes Entropy, Contrast, Correlation, Energy, Homogeneity. Each of the mentioned analyses can, individually, but also provides evidence of a concrete secure S-box. Moreover collective consideration the mentioned MLC parameters makes our method better and reliable than the existing methods. It is worth noticing that our algorithm is based on, Neutrosophic Soft Set (NSS) and uses the all available MLC parameters communally. The other methods suggested for examining the quality of an S-box like root mean square error (RMSE), a number of pixels change (PNCR) etc., are very time-consuming and are not user-friendly. Therefore, their is need of a method which is less time consuming and is easy to analyze the S-box.

We take the decision-making algorithm to a new level of classification, by analyzing the seven popular S-boxes on different images. Several standard images like Airplane, Pepper, Lena, Baboon etc. of size 512×512 (pixels) are employed. Furthermore, by carrying out the analyses via our proposed NSS based approach, we sort out the best S-boxes for each image. We also study that whether the results suggest a single S-box for all images, or different for different images.

The chapter comprises of two sections. The first section has been devoted to preliminaries. In section two, we describe in detail our proposed NSS based method for the decision making. The average deviation of membership, intermediate and non-membership functions, for objects (parameters) under consideration, will be presented. Later, comparison tables will be constructed by, previously, defined membership, intermediate and non-membership functions of the parameters. Moreover, Neutrosophic Soft Set will be formed by computing the weight functions, along with that, the evaluation interval and evaluation score are defined. Finally in the fourth section, we will practically demonstrate our proposed method, by applying it to the enciphered image of Airplane and Baboon. Then we will sort out the suitable S-box for mentioned images. It turns out that Xyi S-box will be the appropriate S-box, in enciphering of the both images, this also reflects the consistency of our method. We also grade the score in descending order to provide the comparison of image encryption methods. Lastly, a comprehensive study is given, in which the comparison of the results of given method with the results of IFS-method mentioned results are being discussed.

5.1 Neutrosophic Soft Set

Throughout this work, S be the universal set, E is the set of parameters. Recall that, the Soft Set theory was initiated by Molodtsov in [72]. The notions of Neutrosophic Set (NS) and Neutrosophic Soft Set (NSS) were introduced by Maji, in [63] and [16], in following manner.

Definition 5.1.1. *Let $NS(S)$ be the set of all Neutrosophic subsets of S. Then the **Neutrosophic Set** Λ over E, can be defined as:*

$$\Lambda = \{(e, \mu_E(e), \gamma_E(e), \upsilon_E(e)) : e \in E\} \tag{5.1.1}$$

where $\mu_E(e) : E \longrightarrow [0,1], \gamma_E(e) : E \longrightarrow [0,1]$ and $\upsilon_E(e) : E \longrightarrow [0,1]$, denote degree of membership, degree of indeterminacy and degree of non membership respectively.

*We denote **Neutrosophic Soft Set** (NSS) by $\Gamma_E := \Gamma_E = \{(e, \tau_E(e))\}$. Where map $\tau_E : E \longrightarrow NS(S)$ is defined as,*

$$\tau_E(e) = \left\{\left(s, \mu_{\tau_E(e)}(s), \gamma_{\tau_E(e)}(s), \upsilon_{\tau_E(e)}(s)\right) : s \in S\right\} \tag{5.1.2}$$

for all $e \in E$. Here the functions $\mu_{\tau_E(e)}(s) : S \longrightarrow [0,1], \gamma_{\tau_E(e)}(s) : S \longrightarrow [0,1]$ and $\upsilon_{\tau_E(e)}(s) : S \longrightarrow [0,1]$ denote degree of membership, degree of indeterminacy and degree of non membership respectively.

Note that in [70] instead of taking the Neutrosophic Set, with values from real standard or non-standard subset of $]^{-}0, 1^{+}[$, they considered values from the subset of $[0,1]$.

5.2 Neutrosophic soft set for decision making

In this section we will present a NSS-decision making method.

Definition 5.2.1. *If Γ_E is the NSS and $\mu_{\tau_{E(e)}}(s_i), \gamma_{\tau_{E(e)}}(s_i)$ and $\upsilon_{\tau_{E(e)}}(s_i)$ denote the membership degree, indeterminacy degree and non-membership degree for each object s_i respectively. Then the* ***average deviation*** *of membership, indeterminacy and non-membership are;*

$$\begin{aligned} \mu^*_{\tau_E}(s_i) &= \frac{1}{n}\sum |\mu_{\tau_{E(e)}}(s_i) - \bar{\mu}_{\tau_{E(e)}}(s)|, \\ \gamma^*_{\tau_E}(s_i) &= \frac{1}{n}\sum |\gamma_{\tau_{E(e)}}(s_i) - \bar{\gamma}_{\tau_{E(e)}}(s)|, \\ \upsilon^*_{\tau_E}(s_i) &= \frac{1}{n}\sum |\upsilon_{\tau_{E(e)}}(s_i) - \bar{\upsilon}_{\tau_{E(e)}}(s)|, \end{aligned} \tag{5.2.1}$$

where for each $s_i \in S$, and $\bar{\mu}_{\tau_{E(e)}}(s), \bar{\gamma}_{\tau_{E(e)}}(s)$ and $\bar{\upsilon}_{\tau_{E(e)}}(s)$ are mean of $\mu_{\tau_{E(e)}}(s_i), \gamma_{\tau_{E(e)}}(s_i)$ and $\upsilon_{\tau_{E(e)}}(s_i)$. We denote this mean by

$$< \mu^*_{\tau_E}(s_i), \gamma^*_{\tau_E}(s_i), \upsilon^*_{\tau_E}(s_i) >, \tag{5.2.2}$$

Definition 5.2.2. *A comparison table for* ***membership*** *function, denoted by Υ, is a table in which, the number of rows are equal to the number of columns, rows and columns both are labeled by the parameters $e_1, e_2, \cdots, e_n$. The entries are $x_{ij},\ i,j = 1,2,\cdots,n$, given by*

$$x_{ij} = \text{the number, for which the member degree of } e_i \text{ is important by the membership degree of } e_j \tag{5.2.3}$$

Note that $0 \le x_{ij} \le p$, $x_{ii} = p+1$ for all i,j and p is the number of objects presented.

Comparison table for ***intermediate*** *function is denoted by Φ. It is a table in which number of rows are equal to the number of columns, rows and columns both* *are labeled by he parameters $e_1, e_2, \cdots, e_n$. The entries are $y_{ij},\ i,j = 1,2,\cdots,n$, given by*

$$\begin{aligned} y_{ij} &= \text{the number, for which the intermediate degree of } e_i \text{ is} \\ &\quad \text{important by the intermediate degree of } e_j \end{aligned} \tag{5.2.4}$$

where $0 \leq y_{ij} \leq p$, and $y_{ii} = p+1$ for all i, j, here p denotes the number of objects present in the universal set.

*Finally, Ψ is a comparison table of **non-membership** function, in which number of rows are equal to the number of columns. Moreover, rows and columns both are labeled by the parameters $e_1, e_2, \cdots, e_n$. The entries are $z_{ij},\ i,j = 1,2,\cdots,n$, given by*

$$\begin{aligned} z_{ij} &= \text{the number, for which the non-membership degree of } e_i \text{ is} \\ &\quad \text{important by the non-membership degree of } e_j \end{aligned} \tag{5.2.5}$$

where $0 \leq z_{ij} \leq p$ and $z_{ii} = p+1$, for all i, j, here p is the number of objects present in the universal set.

Definition 5.2.3. *The membership function rows and columns sum of a parameter e_i, denoted by Υ_{r_i} and Υ_{c_i} respectively and defined as*

$$\begin{aligned} \Upsilon_{r_i} &= \sum_{j=1}^{n} x_{ij}, \\ \Upsilon_{c_i} &= \sum_{j=1}^{n} x_{ij}. \end{aligned} \tag{5.2.6}$$

The intermediate function rows and columns of a parameter e_i, is presented by Φ_{r_i} and Φ_{c_i} respectively and defined as

$$\begin{aligned} \Phi_{r_i} &= \sum_{j=1}^{n} y_{ij}, \\ \Phi_{c_i} &= \sum_{j=1}^{n} y_{ij}. \end{aligned} \tag{5.2.7}$$

The negative function rows and columns of a parameter e_i, is presented by Ψ_{r_i} and Ψ_{c_i} respectively and defined as

$$\Psi_{r_i} = \sum_{j=1}^{n} z_{ij}, \tag{5.2.8}$$
$$\Psi_{c_i} = \sum_{j=1}^{n} z_{ij}.$$

Definition 5.2.4. *The **Positive Weight** of each parametric set $e_i \in E$, can be computed from following formula:*

$$\mu_E(e_i) := \frac{(\Upsilon_{r_i} - \Upsilon_{c_i})}{6}. \tag{5.2.9}$$

*The **Intermediate weight** of the parametric set $e_i \in E$ can be computed as:*

$$\gamma_E(e_i) := \frac{(\Phi_{r_i} - \Phi_{c_i})}{6}. \tag{5.2.10}$$

*Similarly, the **Negative weight** of the parametric set $e_i \in E$ can be given as,*

$$\upsilon_E(e_i) := \frac{(\Psi_{r_i} - \Psi_{c_i})}{6}. \tag{5.2.11}$$

*Finally, for all $e_i \in E$, the **Neutrosophic Set (NS)** over E, is as follows;*

$$\Lambda := \{(e, \mu_E(e_i), \gamma_E(e_i), \upsilon_E(e_i)) : e_i \in E\}. \tag{5.2.12}$$

Definition 5.2.5. *If Γ_E be the **NSS** over S and Λ is **NS** over E, then the evaluation value of s_i can be calculated from,*

$$\begin{aligned} \mu_{E(i)}(s_i) &: = \max\{\mu^*_{\tau_E(e_j)}(s_i) \cdot \mu_E(e_j) : e_j \in E\}, \\ \gamma_{E(i)}(s_i) &: = median\{\gamma^*_{\tau_E(e_j)}(s_i) \cdot \gamma_E(e_j) : e_j \in E\}, \\ \upsilon_{E(i)}(s_i) &: = \min\{\upsilon^*_{\tau_E(e_j)}(s_i) \cdot \upsilon_E(e_i) : e_j \in E\}, \end{aligned} \tag{5.2.13}$$

*where $1 \leq i \leq n$ and $1 \leq j \leq m$. Once we obtained the evaluation value, then we can write the **evaluation set** in following manner,*

$$\left[\mu_{E(i)}, \gamma_{E(i)}, \upsilon_{E(i)}\right], \tag{5.2.14}$$

for all $s_i \in S$ *and* $e_j \in E$.

Definition 5.2.6. *Let* Γ_E *be the NSS over* S. *The* ***evaluation score*** *for each object* $s_i \in S$, *can be computed from the evaluation interval in following manner:*

$$\hat{s}_i = \mu_{E(i)} + \gamma_{E(i)} - \upsilon_{E(i)}, \tag{5.2.15}$$

for $1 \leq i \leq n$. *Moreover the* ***final evaluation score*** *can be obtained from following,*

$$s = \max_{1 \leq i \leq n} \{\hat{s}_i\}. \tag{5.2.16}$$

We will further proceed by describing the algorithm for decision making criterion. We propose following NSS based algorithm for the selection of appropriate S-box:

1. Choose the NSS Γ_E over the universe $NS(U)$.
2. Compute average deviation of NSS for each $s_i \in S$.
3. Compute the comparison tables Υ, Φ and Ψ.
4. Compute positive, intermediary and negative weight value for each parameter.
5. Construct the NS-set Λ over the parametric set E.
6. Construct the evaluation set for each object s_i.
7. Compute the evaluation scores $\hat{s}_i$.
8. Find s, for which $s = \max_{1 \leq i \leq n} \{\hat{s}_i\}$.

5.2.1 Neutrosophic soft set for classifying the strength S-box

Treat the S as Universal set consisting of the S-boxes for enciphering

$$S = \{u_1, u_2, \cdots, u_7\},$$

where $u_1, u_2, \cdots, u_7$, respectively represents AES, APA, residue prime, S_8-AES, Gray, Xyi, and SKIPJACK S-boxes.

Assume that E denotes the set of parameters i.e.

$$E = \{e_1, e_2, \cdots, e_5\},$$

where $e_1, e_2, \cdots, e_5$ respectively denote the entropy, energy, correlation, homogeneity and contrast parameters. We consider different standard images and classify that, which of S-box is suitable for a particular image encryption.

These parameters for Neutrosophic sets are formulized in following manner.

Neutrosophic set for each Parameter

To work on decision making, we have to find Neutrosophic value for each of the parameter. We begin by providing brief descriptions of each of the parameters and then we are going use them for the neutrosophic soft set (NSS).

Function for Entropy The entropy coefficient measures the uncertainty in the data. Corresponding neutrosophic set for soft set can be given by the following formulas,

$$\begin{aligned}
\mu_{\tau_E(e_1)}(s_i) &= 2 - \frac{e_{1(s_i)}}{e_{1(P)}}, \\
\gamma_{\tau_E(e_1)}(s_i) &= e_{1(s_i)}(\mathrm{mod}\, 1), \\
v_{\tau_E(e_1)}(s_i) &= \frac{e_{1(s_i)}}{e_{1(s_i)} + e_{1(P)}},
\end{aligned} \tag{5.3.1}$$

where $e_{1(P)}$ is the entropy of the plain image and $e_{1(s_i)}$ is the entropy of ciphered image for the S-box s_i and $1 \leq i \leq 7$.

Function of Energy The amount of square elements from GLMC is used to assess the energy coefficient. The neutrosophic set for energy can be obtain in the following manner,

$$\begin{aligned}
\mu_{\tau_E(e_2)}(s_i) &= \frac{e_{2(s_i)}}{e_{2(P)}} + e_{2(P)}, \\
\gamma_{\tau_E(e_2)}(s_i) &= \frac{e_{2(s_i)} + e_{2(P)}}{2}, \\
v_{\tau_E(e_2)}(s_i) &= \frac{e_{2(s_i)}}{e_{2(P)}},
\end{aligned} \tag{5.3.2}$$

where $e_{2(P)}$ denotes the energy of the plain image and $e_{2(s_i)}$ is the energy of ciphered image for the S-box s_i and $1 \leq i \leq 7$.

Functions for Correlation The correlation coefficient is sort of source to specify the amount of similarity between two neighboring pixels. The neutrosophic set for correlation can be described by in below given manner;

$$\begin{aligned} \mu_{\tau_E(e_3)}(s_i) &= e_{3(P)} - e_{3(s_i)}, \\ \gamma_{\tau_E(e_3)}(s_i) &= \frac{e_{3(P)} - e_{3(s_i)}}{e_{3(P)} + e_{3(s_i)}}, \\ v_{\tau_E(e_3)}(s_i) &= \frac{e_{3(s_i)}}{e_{3(P)}}, \end{aligned} \tag{5.3.3}$$

where $e_{3(P)}$ represents the correlation of the plain image and $e_{3(s_i)}$ is the correlation of ciphered image for the S-box s_i and $1 \leq i \leq 7$.

Function of Homogenity The analysis determines the natural event of established structure within the cipher text. The neutrosophic set for homogeneity is denoted by e_4 and is as follow;

$$\begin{aligned} \mu_{\tau_E(e_4)}(s_i) &= \frac{e_{4(s_i)}}{e_{4(P)}}, \\ \gamma_{\tau_E(e_4)}(s_i) &= \frac{e_{4(P)} - e_{4(s_i)}}{e_{4(P)} + e_{4(s_i)}}, \\ v_{\tau_E(e_4)}(s_i) &= \frac{e_{4(P)}}{e_{4(P)} + e_{4(s_i)}}, \end{aligned} \tag{5.3.4}$$

where $e_{4(P)}$ is the homogeneity of the plain image and $e_{4(s_i)}$ is the homogeneity of ciphered image for the S-box s_i and $1 \leq i \leq 7$.

Function of Contrast Local variation in the encrypted image is measured by contrast. The neutrosophic set for contrast is denoted by e_5 and is defined as;

$$\begin{aligned}
\mu_{\tau_E(e_5)}(s_i) &= \frac{e_{5(s_i)} - e_{5(P)}}{e_{5(s_i)} + e_{5(P)}}, \\
\gamma_{\tau_E(e_5)}(s_i) &= e_{5(s_i)}(\mathrm{mod}\,1), \\
v_{\tau_E(e)}(s_i) &= \frac{e_{5(P)}}{e_{5(s_i)}},
\end{aligned} \tag{5.3.5}$$

where $e_{5(P)}$ is the contrast of the plain image and $e_{5(s_i)}$ is the contrast of ciphered image for the S-box s_i and $1 \leq i \leq 7$.

5.3 Decision making algorithm in action

In this section, we considered different standard S-boxes and use the image encryption technique to analyze them. We perform this experiment on different images to see the result of our image encryption works or not. Furthermore, the decision-making steps of NSS is applied to grade the S-boxes.

5.3.1 Decision making on performance indexes of Airplane image

Airplane First let us consider the image of Airplane. The results encrypted image of different S-boxes are as follow;

MLC	Entropy	Energy	Correlation	Homogeneity	Contrast
Plain Image	6.7025	0.2687	0.9429	0.9229	0.2052
AES	6.7178	0.0229	0.0887	0.4904	6.9874
APA	6.7178	0.0243	0.1553	0.5127	6.6436
Prime	6.7178	0.0231	0.1188	0.4826	7.5812
S_8-AES	6.712	0.0297	0.0862	0.4879	7.5812
Gray	6.7178	0.0215	0.1393	0.4836	6.9559
Xyi	6.7178	0.0222	0.0544	0.4698	9.005
SkipJack	6.7178	0.0209	0.0958	0.487	8.2207

Table 5.1: Analyses results of Airplane

Following are the graphical self-explaining comparison of parameters on different S-boxes corresponding to enciphered images.

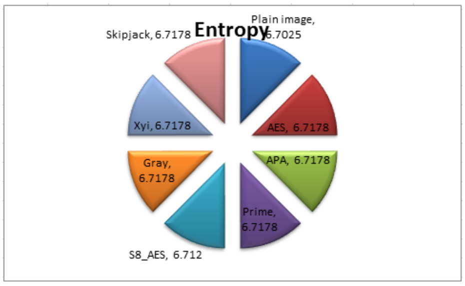

Fig. 5.1.

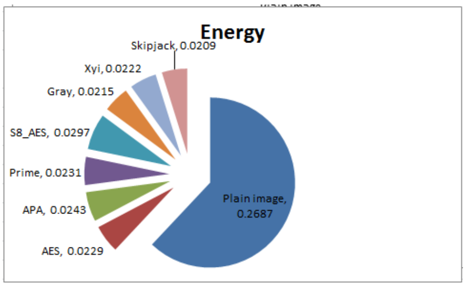

Fig. 5.2.

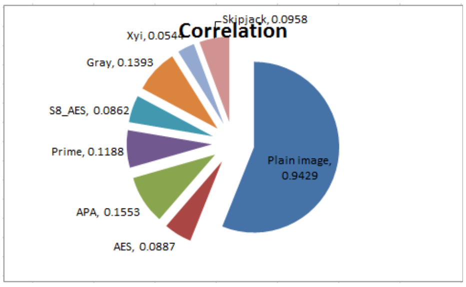

Fig. 5.3.

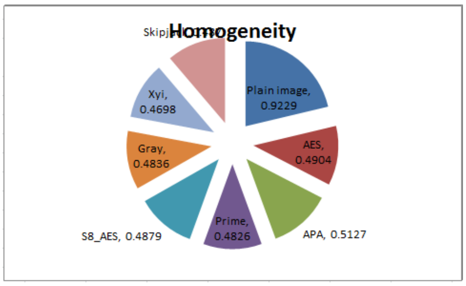

Fig. 5.4.

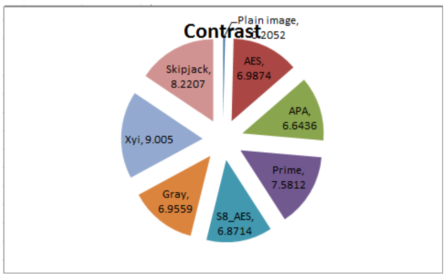

Fig. 5.5.

Enciphered images of airplane

A 512×512 (pixel) image of an airplane is taken for encryption. The standard S-boxes are taken for image encryption. Following are the enciphered images of airplane.

Fig 5.6: Plain image of airplane

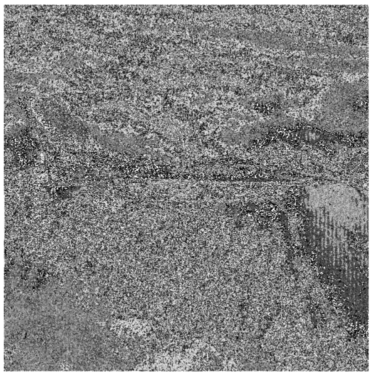

Fig 5.7: AES S-box transformation

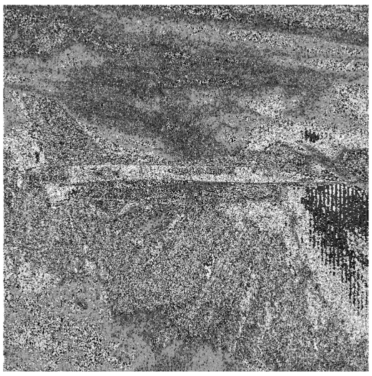

Fig. 5.8: APA S-box transformation

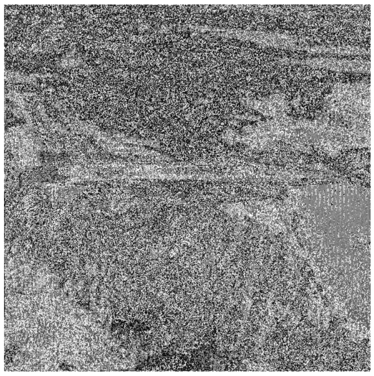

Fig. 5.9: Prime S-box transformation

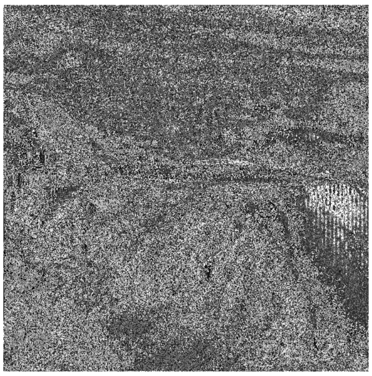

Fig. 5.10: S-8 S-box transformation

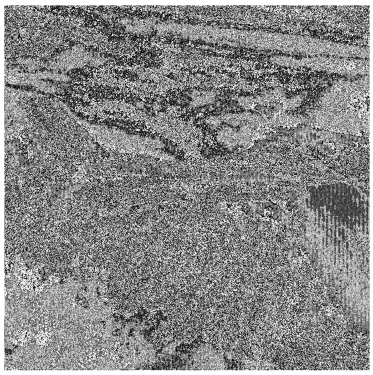

Fig. 5.11: Gray S-box transformation

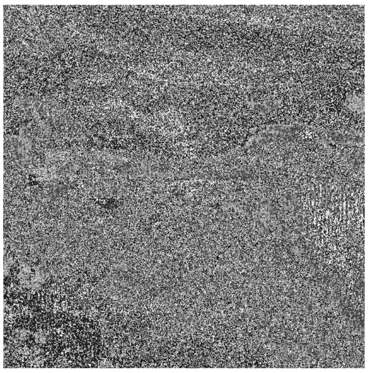

Fig. 5.12: Xyi S-box transformation

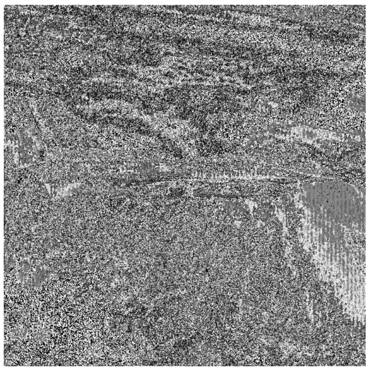

Fig. 5.13: SkipJack S-box transformation

can observe that Xyi S-box, Skip jack S-box, S-8 S-box and gray S-box quite ambiguous and protected encipher images

Neutrosophic soft set (NSS) Choose the NSS Γ_E over the universe $NS(U)$. The data from the table 5.1 has been used to transform in membership, indeterminacy and non-membership functions (6.4.1)-(6.4.5). The NSS in table 5.2 can be represented in following tabular form.

Γ_E	$\tau_E(e_1)$	$\tau_E(e_2)$	$\tau_E(e_3)$	$\tau_E(e_4)$	$\tau_E(e_5)$
s_1	<0.9977,0.7178,0.5006>	<0.3539,0.1458,0.0852>	<0.8542, 0.828,0.0941>	<0.5314,0.3060,0.6530>	<0.9429,0.9874,0.0294>
s_2	<0.9977,0.7178,0.5006>	<0.3591,0.1465,0.0904>	<0.7876,0.7172,0.1647>	<0.5555,0.2857,0.64287>	<0.9401,0.6436,0.0309>
s_3	<0.9977,0.7178,0.5006>	<0.3547,0.1459, 0.086>	<0.8241,0.7762,0.1260>	<0.5229,0.3133,0.6566>	<0.9473,0.5812,0.0271>
s_4	<0.9986,0.712,0.5004>	<0.3792,0.1492,0.1105>	<0.8567,0.8325,0.0914>	<0.5287,0.3083,0.6542>	<0.9420,0.8714,0.0299>
s_5	<0.9977,0.7178,0.5006>	<0.3487,0.1451,0.0800>	<0.8036,0.7426,0.1477>	<0.5240,0.3123,0.6562>	<0.9427,0.9559,0.0295>
s_6	<0.9977,0.7178,0.5006>	<0.3513,0.1455,0.0826>	<0.8885,0.8909,0.0577>	<0.5090,0.3253,0.6627>	<0.9554,0.0050,0.0228>
s_7	<0.9977,0.7178,0.5006>	<0.3465,0.1448,0.07779>	<0.8471,0.8155,0.1016>	<0.5277,0.3092,0.6546>	<0.9513,0.2207,0.0250>

Table 5.2: Neutrosophic soft set

The graphical representation of NSS is as follow;

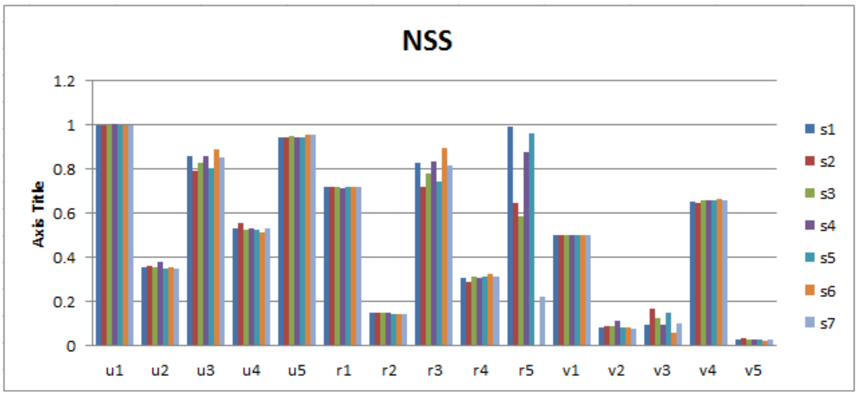

Fig. 5.14: Graphical representation.

The membership, intermediate and non-membership functions of the seven S-boxes are separately presented. This show the variation of each function according to their image encryption result.

Average deviation The NSS Γ_E from previous table is used to calculate the average deviation. The formula of average deviation is given in equation (5.2.2), and average deviation of the membership, intermediate and non-membership functions are represented as follows;

Avgdev(Γ_E)	$\langle \mu^*_{\tau_E}, \gamma^*_{\tau_E}, \nu^*_{\tau_E} \rangle$
s_1	$\langle 0.2347, 0.2969, 0.2435 \rangle$
s_2	$\langle 0.2165, 0.2288, 0.2287 \rangle$
s_3	$\langle 0.2324, 0.2218, 0.2395 \rangle$
s_4	$\langle 0.2297, 0.2767, 0.2300 \rangle$
s_5	$\langle 0.2296, 0.2768, 0.2365 \rangle$
s_6	$\langle 0.2482, 0.3091, 0.2531 \rangle$
s_7	$\langle 0.2376, 0.2601, 0.2445 \rangle$

Table 5.3: Average deviation.

Comparision tables Let us now compute the, comparison table, for membership, intermediate and non-membership functions Υ, Φ and Ψ by using the method given in (5.2.3),(5.2.4) and (5.2.5).

Υ	e_1	e_2	e_3	e_4	e_5
e_1	8	16	16	16	16
e_2	8	8	8	8	8
e_3	8	16	8	16	8
e_4	8	16	8	8	8
e_5	8	16	16	16	8

Table 5.4: Membership comparison.

Φ	e_1	e_2	e_3	e_4	e_5
e_1	8	16	9	16	11
e_2	8	8	8	8	9
e_3	15	16	8	16	11
e_4	8	16	8	8	9
e_5	10	15	10	15	8

Table 5.5: Indeterminacy comparison.

Ψ	e_1	e_2	e_3	e_4	e_5
e_1	8	16	16	8	8
e_2	16	8	8	8	16
e_3	8	12	8	16	16
e_4	16	16	16	8	16
e_5	8	8	8	8	8

Table 5.6: Non-membership comparison.

Weight Parameters The positive, intermediate and negative weight values are calculated by using equations (5.2.8)-(5.2.11) by using equation (5.2.6) to (5.2.8).

	Υ_{r_i}	Υ_{c_i}	$\Upsilon_{r_i} - \Upsilon_{c_i}$	μ_E
e_1	72	40	32	5.333
e_2	40	72	-32	-5.333
e_3	56	56	0	0
e_4	48	64	-16	-2.667
e_5	64	48	16	2.667

Table 5.7: Membership weight parameters.

	Φ_{r_i}	Φ_{c_i}	$\Phi_{r_i} - \Phi_{c_i}$	γ_E
e_1	60	49	11	1.833
e_2	41	71	-30	-5
e_3	66	43	23	3.833
e_4	49	63	-14	-2.333
e_5	58	48	10	1.667

Table 5.8: Intermediate weight parameters.

	Ψ_{r_i}	Ψ_{c_i}	$\Psi_{r_i} - \Psi_{c_i}$	ν_E
e_1	56	56	0	0
e_2	56	60	-4	-0.667
e_3	60	56	4	0.667
e_4	72	48	24	4
e_5	40	64	-24	-4

Table 5.9: Non-membership weight parameters.

NS-set The NS-set Λ over the parametric set E is constructed by as given in equation (5.2.12). The results of tables 5.7, 5.8 and 5.9 are used to build

NS-set.

Λ	(μ_E, γ_E, ν_E)
e_1	$(5.333, 1.8333, 0)$
e_2	$(-5.333, -5, -0.6667)$
e_3	$(0, 3.8333, 0.6667)$
e_4	$(-2.6667, -2.3333, 4)$
e_5	$(2.6667, 1.6667, -4)$

Table 5.10: NS-set.

Evaluation sets Next the evaluation set for each object s_i by using the formula given in equation (5.2.13) and represent in the form of (5.2.14).

Γ_E	$[\mu_{E(i)}, \gamma_{E(i)}, \nu_{E(i)}]$
s_1	$[1.2518, 0.4948, -0.9739]$
s_2	$[1.1549, 0.3814, -0.9146]$
s_3	$[1.2397, 0.3697, -0.9579]$
s_4	$[1.2249, 0.4612, -0.9599]$
s_5	$[1.2245, 0.4614, -0.9458]$
s_6	$[1.3236, 0.5166, -1.0123]$
s_7	$[1.2671, 0.4334, -0.9782]$

Table 5.11: Evaluation set.

Evaluation scores To compute the evaluation scores $\hat{s}_i$ equation (5.2.15) has been used.

	Score
$\hat{s}_1$	2.7205
$\hat{s}_2$	2.4509
$\hat{s}_3$	2.5673
$\hat{s}_4$	2.6461
$\hat{s}_5$	2.6317
$\hat{s}_6$	2.8525
$\hat{s}_7$	2.6787

Table 5.12: Evaluation score.

Maximum Score The maximum score sort out the appropriate S-box for image encryption. It is denoted by s, and defined in equation (5.2.16) the result is;

$$\boxed{s =} \boxed{\hat{s}_6 =} \boxed{2.8525}$$

which represents the **Xyi S-box**.

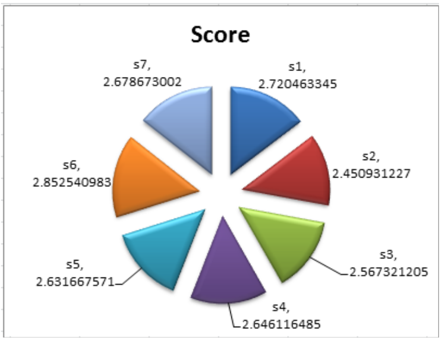

Fig. 5.15: Score of different S-boxes

5.3.2 Grading results for encrypted images of Airplane

The scores of S-boxes, are sorted in descending order, to show their performance accordingly.

	Score
$\hat{s}_6$	2.8525
$\hat{s}_1$	2.7205
$\hat{s}_7$	2.6787
$\hat{s}_4$	2.6461
$\hat{s}_5$	2.6317
$\hat{s}_3$	2.5673
$\hat{s}_2$	2.4509

Table 5.13: Grading score in descending order.

Comparison Now we compare the results obtained NSS-based algorithm with intuitionistic fuzzy soft set from table 4.6. (4.3.1). The score of both methods are as follow;

	Score
$\hat{s}_6$	0.1384
$\hat{s}_1$	0.0804
$\hat{s}_7$	0.0177
$\hat{s}_4$	0.0006
$\hat{s}_5$	-0.0377
$\hat{s}_3$	-0.0843
$\hat{s}_2$	-0.1152

Table 4.6: IFS-score

	Score
$\hat{s}_6$	2.8525
$\hat{s}_1$	2.7205
$\hat{s}_7$	2.6787
$\hat{s}_4$	2.6461
$\hat{s}_5$	2.6317
$\hat{s}_3$	2.5673
$\hat{s}_2$	2.4509

Table 5.13: NSS-score

Here we see that the Xyi S-box and S_8 S-box are lead in both decision making methods. As Xyi S-box turns out to be the best S-box so it consistent with IFS based algorithm. While other S-boxes are graded differently. One drawback in IFS based approach was that it does not involve indeterminacy function while here one can clearly observe that, in our proposed NSS decision making method, which involves indeterminacy function, has put a significant impact on score.

5.3.3 Decision making on performance indexes of Baboon image

Baboon Now we repeat the same procedure with another image of Baboon, to observe that whether the results are consistent with the previously carried out analysis on airplane image. The results of different S-boxes are as follow;

MLC	Entropy	Energy	Correlation	Homogeneity	Contrast
Plain Image	7.3583	0.1094	0.8232	0.8098	0.5085
AES	7.7067	0.0183	0.0196	0.4267	8.4229
APA	7.7067	0.0183	0.0581	0.4327	8.081
Prime	7.7067	0.0171	0.0323	0.4211	8.9211
S_8-AES	7.6932	0.0178	0.0275	0.429	8.1915
Gray	7.7067	0.0187	0.0196	0.4301	8.3561
Xyi	7.7067	0.018	0.0069	0.4239	8.2848
SkipJack	7.7067	0.0189	0.0267	0.4318	7.8404

Table 5.14: Image encryption analyses of Baboon.

Enciphered images of Baboon

A 512 × 512 (pixel) image of Baboon is taken for encryption. The standard S-boxes are taken for image encryption. Following are the enciphered images of baboon.

Fig. 5.16: Plain image of Baboon.

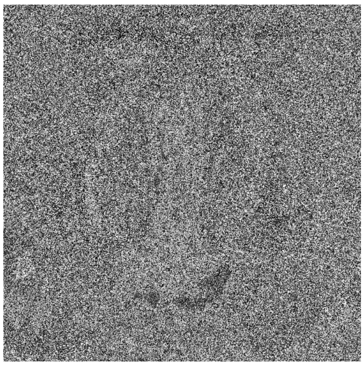

Fig.. 5.17: AES transformation of Baboon.

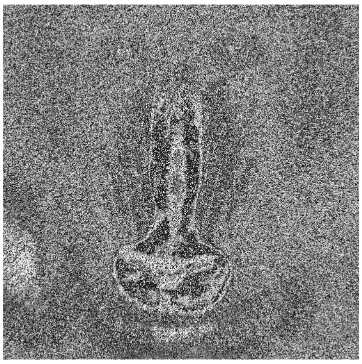

Fig. 5.18: APA transformation of Baboon.

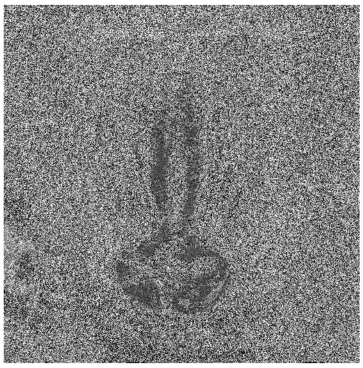

Fig. 5.19: PRIME transformation of Baboon.

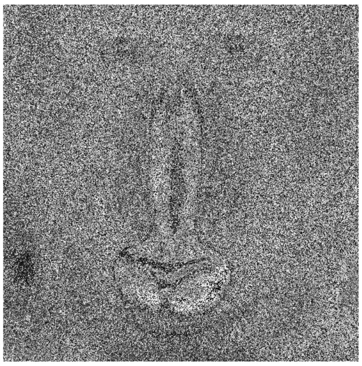

Fig. 5.20: S_8 transformation of Baboon.

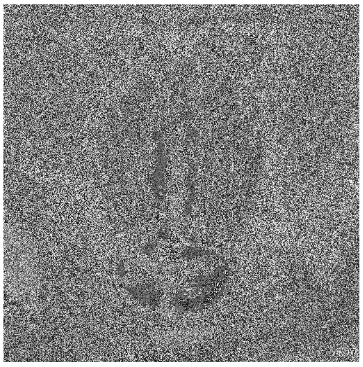

Fig. 5.21: Gray transformation of Baboon.

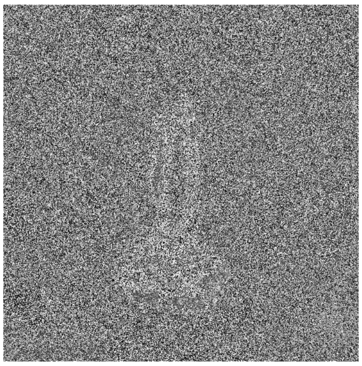

Fig. 5.22: Xyi transformation of Baboon.

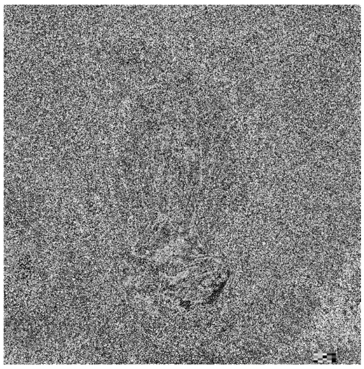

Fig. 5.23: SKIPJACK transformation of Baboon.

One can clearly observe that results of enciphered images are almost similar to the results in case of airplane image. Again Xyi S-box, Skip jack S-box, S-8 S-box and gray S-box did well by providing secure images.

The data from the table **16** has been used to for finding membership, indeterminacy and non-membership functions (6.4.1)-(6.4.5).

Neutrosophic soft set (NSS) Choose the NSS Γ_E over the universe $NS(U)$.

The data from the table **16** has been used to for membership, indeterminacy and non-membership functions (6.4.1)-(6.4.5). The NSS is representing in following tabular form.

Γ_E	e_1	e_2	e_3	e_4	e_5
u_1	(0.9548,0.4548)	(0.8327,0.2134)	(0.8036,0.4762)	(0.8087,0.3098)	(0.8861,0.6272)
u_2	(0.9548,0.4548)	(0.8327,0.2134)	(0.7651,0.4294)	(0.8048,0.3035)	(0.8816,0.6322)
u_3	(0.9548,0.4548)	(0.8437,0.2296)	(0.7909,0.4608)	(0.8124,0.3158)	(0.8922,0.6205)
u_4	(0.9565,0.4565)	(0.8373,0.2201)	(0.7957,0.4666)	(0.8072,0.3074)	(0.8831,0.6306)
u_5	(0.9548,0.4548)	(0.8291,0.2080)	(0.8036,0.4762)	(0.8065,0.3062)	(0.8853,0.6282)
u_6	(0.9548,0.4548)	(0.8355,0.2174)	(0.8163,0.4916)	(0.8106,0.3128)	(0.8843,0.6292)
u_7	(0.9548,0.4548)	(0.8272,0.2054)	(0.7965,0.4676)	(0.8054,0.3044)	(0.8782,0.636)

Table 5.15. NSS

The graphical representation of NSS is as follow;

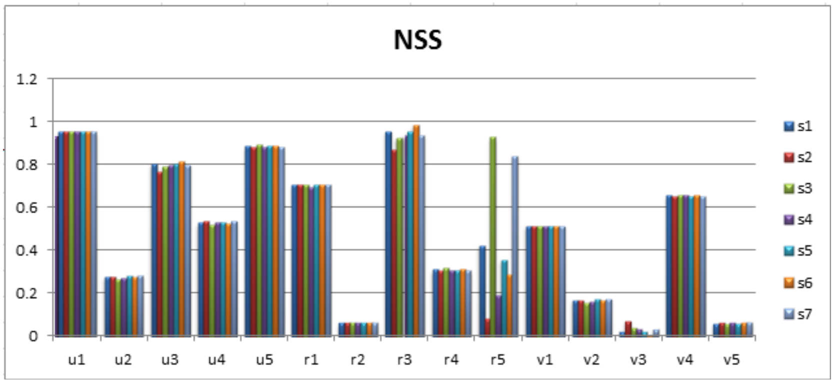

Fig. 5.24.

This show the membership, intermediate and non-membership function of each S-box and will lead to scoring the appropriate one.

Average deviation The NSS Γ_E from previous table is used to calculate the average deviation. The formula of average deviation is given in equation (5.2.2), and average deviation of the membership, intermediate and non-membership functions are as follows;

Avgdev(Γ_E)	$\langle \mu^*_{\tau_E}, \gamma^*_{\tau_E}, \nu^*_{\tau_E} \rangle$
u_1	$\langle 0.2299, 0.2709, 0.2397 \rangle$
u_2	$\langle 0.2213, 0.3062, 0.2311 \rangle$
u_3	$\langle 0.2332, 0.3184, 0.2403 \rangle$
u_4	$\langle 0.2289, 0.3009, 0.2382 \rangle$
u_5	$\langle 0.2296, 0.2768, 0.2365 \rangle$
u_6	$\langle 0.2332, 0.3091, 0.2428 \rangle$
u_7	$\langle 0.2247, 0.2601, 0.2361 \rangle$

Table 5.16. Average deviation

Comparision tables Compute the comparison table for membership, intermediate and non-membership functions Υ, Φ and Ψ by using the method given in (5.2.3),(5.2.4) and (5.2.5).

Υ	e_1	e_2	e_3	e_4	e_5
e_1	8	16	16	16	16
e_2	8	8	8	8	8
e_3	8	16	8	8	8
e_4	8	8	8	8	8
e_5	8	16	16	16	8

Table 5.17. Membership comparison

Φ	e_1	e_2	e_3	e_4	e_5
e_1	8	16	8	16	16
e_2	8	8	8	8	8
e_3	16	16	8	16	16
e_4	8	16	8	8	12
e_5	8	16	8	13	8

Table 5.18. Intermediate comparison

Ψ	e_1	e_2	e_3	e_4	e_5
e_1	8	16	16	8	16
e_2	8	8	16	8	16
e_3	8	8	8	8	8
e_4	16	16	16	8	16
e_5	8	8	16	8	8

Table 5.19. Non-membership comparison

Weight Parameters The positive, intermediate and negative weight values are calculated by using equations (5.2.8)-(5.2.11) by using equation (5.2.6) to (5.2.8).

	Υ_{r_i}	Υ_{c_i}	$\Upsilon_{r_i} - \Upsilon_{c_i}$	μ_E
e_1	72	40	32	5.333
e_2	40	64	-24	-4
e_3	48	56	-8	-1.333
e_4	40	56	-16	-2.667
e_5	64	48	16	2.667

Table 5.20. Membership weight parameters

	Φ_{r_i}	Φ_{c_i}	$\Phi_{r_i} - \Phi_{c_i}$	γ_E
e_1	64	48	16	2.667
e_2	40	72	-32	-5.333
e_3	72	40	32	5.333
e_4	52	61	-9	-1.5
e_5	53	60	-7	1.167

Table 5.21. Intermediate weight parameters

	Ψ_{r_i}	Ψ_{c_i}	$\Psi_{r_i} - \Psi_{c_i}$	ν_E
e_1	64	48	16	2.667
e_2	56	56	0	0
e_3	40	72	-32	-5.333
e_4	72	40	32	5.333
e_5	48	64	-16	-2.667

Table 5.22. Non-membership weight parameters

NS-set The NS-set Λ over the parametric set E is constructed as given in equation (5.2.12). The results of table 5.20, 5.21 and 5.22 are used.

Λ	$(\mu_{_E}, \gamma_{_E}, \nu_{_E})$
e_1	$(5.333, 2.6667, 2.6667)$
e_2	$(-4, -5.333, 0)$
e_3	$(-1.333, 5.333, -5.333)$
e_4	$(-2.6667, -1.5, 5.3333)$
e_5	$(2.6667, -1.1667, -2.6667)$

Table 5.23. NS-set

Evaluation set The evaluation set for each object s_i by using the formula given in equation (5.2.13) and represent in the form of (5.2.14).

Γ_E	$[\mu_{E(i)}, \gamma_{E(i)}, \nu_{E(i)}]$
s_1	$[1.2262, -0.3162, -1.2785]$
s_2	$[1.1800, -0.3573, -1.2324]$
s_3	$[1.2435, -0.3714, -1.2814]$
s_4	$[1.2207, -0.3509, -1.2707]$
s_5	$[1.2154, -0.3293, -1.2726]$
s_6	$[1.2435, -0.3498, -1.2951]$
s_7	$[1.1983, -0.3605, -1.2592]$

Table 5.24. Evaluation set

Evaluation scores To compute the evaluation scores $\hat{s}_i$ equation (5.2.15) is taken.

	Score
$\hat{s}_1$	2.1886
$\hat{s}_2$	2.0552
$\hat{s}_3$	2.1535
$\hat{s}_4$	2.1403
$\hat{s}_5$	2.1589
$\hat{s}_6$	2.1888
$\hat{s}_7$	2.0969

Table 5.25. Evaluation score

Maximum Score The maximum score sort out the appropriate S-box for image encryption. It is denoted by s, and defined in equation (5.2.16) the result is;

$s =$	$\hat{s}_6 =$	2.1888

which represents the Xyi S-box.

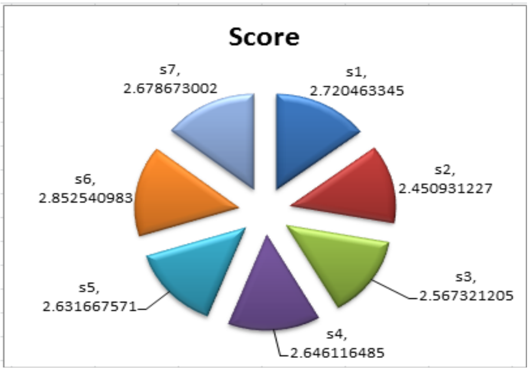

Fig. 5.25

5.3.4 Grading results for encrypted images of Baboon

The scores of S-box, sorted out in descending order, show the performance of S-boxes.

	Score
$\hat{s}_6$	2.1888
$\hat{s}_1$	2.1886
$\hat{s}_5$	2.1589
$\hat{s}_3$	2.1535
$\hat{s}_4$	2.1403
$\hat{s}_7$	2.0969
$\hat{s}_2$	2.0551

Table 5.26. Grading the score

We end by providing is a comparison of NSS-decision making method with IFS-decision making method provided in table 4.12 (4.3.3) for the image of Baboon.

The score from upper to lower order of both the method is given as;

	Score
$\hat{s}_3$	0.0708
$\hat{s}_5$	0.0239
$\hat{s}_2$	0.0231
$\hat{s}_1$	0.0152
$\hat{s}_4$	-0.0263
$\hat{s}_6$	-0.0473
$\hat{s}_7$	-0.0594

Table 4.12. IFS-score

	Score
$\hat{s}_6$	2.1886
$\hat{s}_1$	2.0552
$\hat{s}_5$	2.1535
$\hat{s}_3$	2.1403
$\hat{s}_4$	2.1589
$\hat{s}_7$	2.1888
$\hat{s}_2$	2.0969

Table 5.26. NSS-score

Here we see that the score of both are significantly different. Here the results show that NSS decision making algorithm is better than IFS-decision making algorithm.

5.3.5 Decision making on performance indexes of Pepper image

Pepper The standard S-boxes results for the image of Pepper are as follows;

MLC	Entropy	Energy	Correlation	Homogeneity	Contrast
Plain Image	5.8597	0.2140	0.9768	0.1763	0.9388
AES	7.3388	7.9274	0.0241	0.0191	0.4377
APA	7.3388	7.3363	0.0577	0.0204	0.4552
Prime	7.3388	9.1005	0.0364	0.0172	0.4202
S_8-AES	7.3318	7.5407	0.0344	0.0210	0.4441
Gray	7.3388	7.9515	0.0310	0.0193	0.4348
Xyi	7.3388	8.5151	0.0138	0.0187	0.4321
SkipJack	7.3388	8.1139	0.0584	0.0184	0.4372

Table 5.27. Image encryption analyses of Pepper

Enciphered Image of Pepper Following are the enciphered image of the Pepper.

Fig. 5.26. Plain image Pepper

Fig. 5.27. AES transformation of Pepper

Fig. 5.28. APA transformation of Pepper

Fig. 5.29. Prime transformation of Pepper

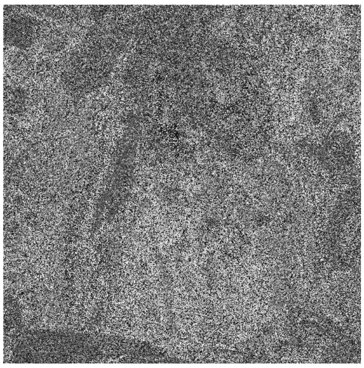

Fig. 5.30. S_8 transformation of Pepper

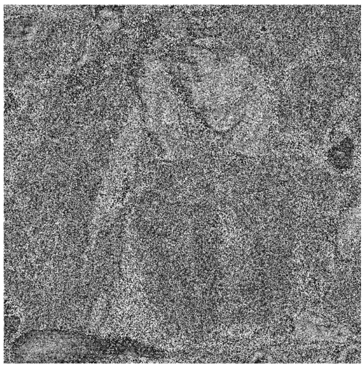

Fig. 5.31. Gray transformation of Pepper

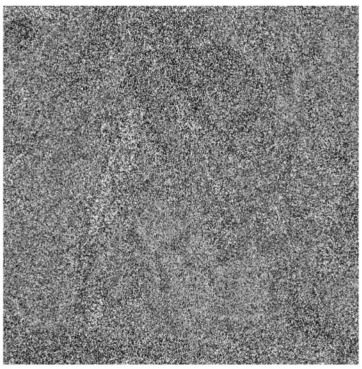

Fig. 5.32. Xyi transformation of Pepper

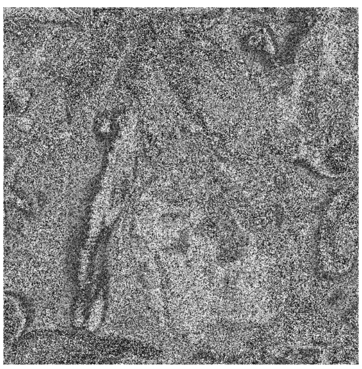

Fig. 5.33. Skipjack transformation of Pepper

Evaluation scores Repeating the same steps from (5.1.1) to (5.2.16) for the image of Pepper. We get the score;

	Score
$\hat{s}_1$	109.0637
$\hat{s}_2$	100.8376
$\hat{s}_3$	125.4098
$\hat{s}_4$	103.6748
$\hat{s}_5$	109.3957
$\hat{s}_6$	117.2579
$\hat{s}_7$	111.6658

Table 5.28. Evaluation score

5.3.6 Grading results for encrypted images of Pepper

The scores of S-box, sorted out in descending order, show the performance of S-boxes.

	Score
$\hat{s}_3$	125.4098
$\hat{s}_6$	117.2579
$\hat{s}_7$	111.6658
$\hat{s}_5$	109.3957
$\hat{s}_1$	109.0637
$\hat{s}_4$	103.6748
$\hat{s}_2$	100.8376

Table 5.29: Grading the score

Here we see that the Prime S-box is the appropriate S-box.

5.3.7 Decision making on performance indexes of Lena image

Lena The standard S-boxes results for the image of Lena are as follows;

MLC	Entropy	Energy	Correlation	Homogeneity	Contrast
Plain Image	5.0902	0.1017	0.9881	0.2505	0.9388
AES	7.2531	7.5509	0.0554	0.0202	0.4377
APA	7.2531	8.1195	0.1473	0.0183	0.4552
Prime	7.2531	7.6236	0.0855	0.0202	0.4202
S_8-AES	7.2357	7.4852	0.1235	0.0208	0.4441
Gray	7.2531	7.5283	0.0586	0.0193	0.4348
Xyi	7.2531	8.3108	0.0417	0.0187	0.4321
SkipJack	7.2531	7.7058	0.1025	0.0184	0.4372

Table 5.30. Image encryption analyses of Lena

Enciphered images of Lena Following are the Plain image and enciphered images of standard S-boxes.

Fig. 5.34. Plain image of Lena

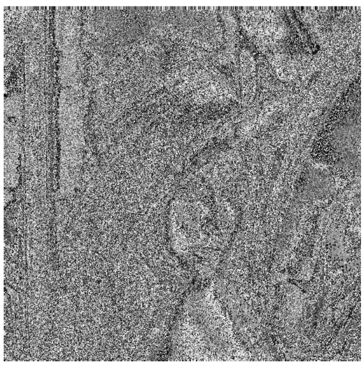

Fig. 5.35. AES transformation of Lena

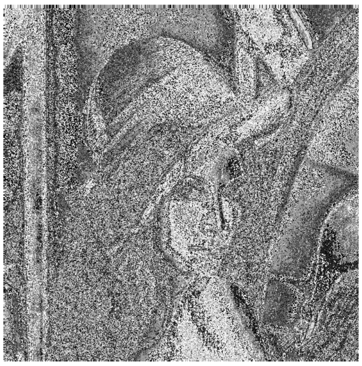

Fig. 5.36. APA transformation of Lena

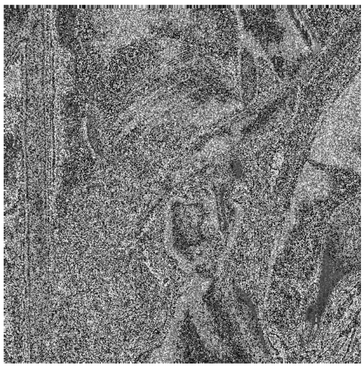

Fig. 5.37. Prime transformation of Lena

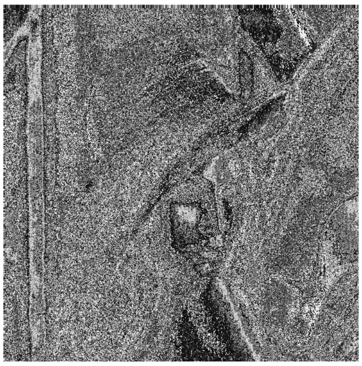

Fig. 5.38. S_8 transformation of Lena

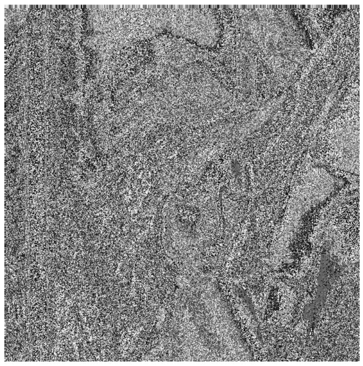

Fig. 5.39. Gray transformation of Lena

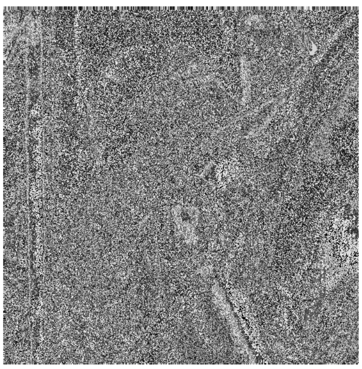

Fig. 5.40. Xyi transformation of Lena

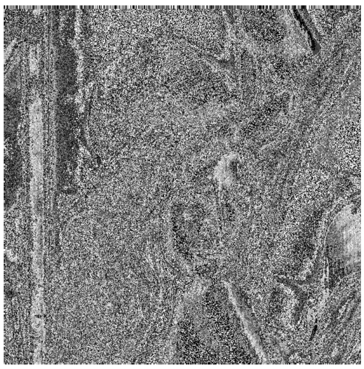

Fig. 5.41. SkipJack transformation of Lena

Evaluation scores Repeating the same steps from (5.1.1) to (5.2.16) for the image of Pepper. We get the score;

	Score
$\hat{s}_1$	221.1078
$\hat{s}_2$	237.9101
$\hat{s}_3$	223.2559
$\hat{s}_4$	219.1829
$\hat{s}_5$	220.4362
$\hat{s}_6$	243.5272
$\hat{s}_7$	225.6909

Table 5.32. Evaluation score

5.3.8 Grading results for encrypted images of Lena

The scores of S-box, sorted out in descending order, show the performance of S-boxes.

	Score
$\hat{s}_6$	243.5272
$\hat{s}_2$	237.9101
$\hat{s}_7$	225.6909
$\hat{s}_3$	223.2559
$\hat{s}_1$	221.1078
$\hat{s}_5$	220.4362
$\hat{s}_4$	219.1829

Table 5.33. Grading the score

The Xyi S-box is the appropriate one.

Chapter 6

A new decision making and grading of S-boxes based on neutrosophic fuzzy soft sets

In the previous chapter, the NSS decision-making concept is used in for selecting the appropriate S-box. In this chapter, we intend to use an improved version of decision-making on neutrosophic fuzzy soft set (NFSS), for the selection of the optimally secure S-box. The inconsistency can be efficiently measured. by NFSS, whereas fuzzy and intuitionistic fuzzy soft set cannot handle the indeterminate information.

The idea of this chapter is mainly to securitize optimal S-box among the huge list of S-boxes For the sake of completeness, the next section is devoted to preliminaries and necessary explanations. In [92], construction of S-boxes is based on the action of the projective general linear group $PGL\left(2, GF\left(2^{8}\right)\right)$ on Galois field $GF(2^{8})$,which gives us an algorithm to generates a huge number of S-boxes. These S-boxes applied on an image which gives us the table of MLC analysis. The we create a new decision-making method on NFSS. Then the steps are proposed to apply decision-making method on the table of MLC analysis of S-boxes. In the end, the scores are the grade in descending order, to compare the image encryption quality of different S-boxes.

6.1 Chaotic S-boxes generation algorithm

The construction of S-boxes is based on the idea of linear fractional transformations of the projective general linear group. The initial seed for the configuration of S-boxes in the algorithm is derived from the two-dimensional chaotic maps, that is, the Tinkerbell map, the Baker's map, and the Duffing map.

Four values are generated through Tinkerbell map which is used as seed values of the Baker's map and the Duffing map. Random values are generated by these two maps and are allocated to the parameters a, b, c and d which used by linear fractional transformations. The linear fractional transformation used in the configuration of S-boxes is:

$$PGL\left(2, GF\left(2^{8}\right)\right) \times GF\left(2^{8}\right) \rightarrow GF\left(2^{8}\right)$$

The algebraic construction used here is; $g\left(z\right) = \frac{az+b}{cz+d}$ such $a, b, c, d \in GF\left(2^{8}\right)$ and $g \in PGL\left(2, GF\left(2^{8}\right)\right)$ with $ad - bc$ is non square. The algorithm proposed for the synthesis of chaotic S-boxes for this action is given in detail [92].

Tinkerbell Map

The *Tinkerbell map* [43], is a two dimensional chaotic map whose iterations give rise to a complex pattern. It is a discrete-time dynamical system given by the equations

$$\begin{aligned} x_{n+1} &= x_n^2 - y_n^2 + ax_n + by_n, \\ y_{n+1} &= 2x_n y_n + cx_n + dy_n, \end{aligned}$$

where $a = 0.9$, $b = -0.6013$, $c = 2.0$ and $d = 0.5$. The are the Tinkerbell map iterate for $n = 4h$, where $h \in \mathbb{Z}^+$.

Let H_1 contains all values for $n = 4h'$, H_2 for $n = 4h' + 1$, H_3 for $n = 4h' + 2$ and H_4 for $n = 4h' + 3$, while $h' \leq h$.

RSA algorithm aids in the generation of initial seed for Tinkerbell map.

The computational steps of RSA algorithm for seed generation are:

1. Generation of two large primes p and q.
2. Calculation of n, where $n = p \times q$.
3. Calculation of totient function $\phi(n) = (p - 1) \times (q - 1)$.
4. Selection of encryption exponent e such that $\gcd(\phi(n), e) = 1$.
5. Calculation of decryption exponent d such that $d = (e^{-1}) \pmod{\phi(n)}$.

Let M represents our message. Then we can transform M into another integer C which will represent our ciphertext by the following modular exponent:

$$C = M^e (\operatorname{mod} n),$$

where C can be expressed as

$$C = c_1 c_2 ... c_k, \text{ where } c_i \in \mathbb{Z}^+.$$

If

$$t = c_1 + c_2 + ... + c_k,$$

then

$$C_1 = CCC...C_t.$$

Now convert C_1 into binary form

$$C_{1_{Binary}} = b_1 b_2 b_3 ... b_j, \text{ with } b_1, b_2, ... b_j \in \mathbb{Z}_2.$$

Taking

$$k_1 = \frac{\sum_{l=1}^{j} b_l}{j}, \text{ where } b_l \text{ are the } 1's \text{ in } C_{1_{Binary}},$$

and

$$k_2 = 1 - k_1.$$

If

$$k_1 = 1,$$

then put

$$C_1 = CCC...C_t C_{t+1}.$$

Consequently, the initial value for Tinkerbell map would be

$$x_0 = k_1, \; y_0 = k_2$$

Baker's Map

The *Baker's map* in [84] is defined as:

$$x'_{n+1} = \begin{cases} \lambda_a x'_n & \text{if } y'_n < \alpha \\ 1 - \lambda_a + \lambda_b x'_n & \text{if } y'_n > \alpha \end{cases},$$

$$y'_{n+1} = \begin{cases} \frac{y'_n}{\alpha} & \text{if } y'_n < \alpha \\ \frac{y'_n - \alpha}{\beta} & \text{if } y'_n > \alpha \end{cases}.$$

Here we have, $\beta = 1 - \alpha$, $\lambda_a + \lambda_b \leq 1$, $0 \leq x' \leq \lambda_a$ and $(1 - \lambda_a) \leq x' \leq 1$.

The initial seed for Baker's map is calculated as:

$$x'_0 = \left(\frac{\sum_{i=0}^{4h'} h_{1_i}}{h} \right) \pmod 1, \text{where } h_{1_i} \in H_1,$$

$$y'_0 = \left(\frac{\sum_{i=0}^{4h'+1} h_{2_i}}{h} \right) \pmod 1, \text{where } h_{2_i} \in H_2.$$

Duffing Map (Holme's Map)

The *Duffing map* is defined as:

$$\begin{aligned} x''_{n+1} &= y''_n, \\ y''_{n+1} &= -\rho x''_n + \nu y''_n - y''^3_n, \end{aligned}$$

where $\rho = 2.75$ and $\nu = 0.15$.

The initial seed values for Duffing map are calculated as

$$x''_0 = \left(\frac{\sum_{i=0}^{4h'+2} h_{3_i}}{h} \right) \pmod 1, \ \text{where } h_{3_i} \in H_3,$$

$$y''_0 = \left(\frac{\sum_{i=0}^{4h'+3} h_{4_i}}{h} \right) \pmod 1, \ \text{where } h_{4_i} \in H_4.$$

6.1.1 Algorithm for checking the nonlinearity of S-boxes

In the proposed algorithm, a proficient way for the collection of better S-boxes is being introduced. Here a nonlinearity check is induced in the algorithm which yields S-boxes along with their nonlinearity value. Now we are able to collect processed S-boxes with respect to nonlinearity. The purpose of this work is:

1. To analyze the strength of S-boxes with respect to nonlinearity.

2. To collect S-boxes having desired traits of nonlinearity.

3. To check whether the value of nonlinearity criterion affects the values of other criteria or not.

4. To calculate the number of S-boxes having particular nonlinearity, from the huge number of S-boxes gained through the algorithm obtained by Tinkerbell map, Baker's map and the Duffing map.

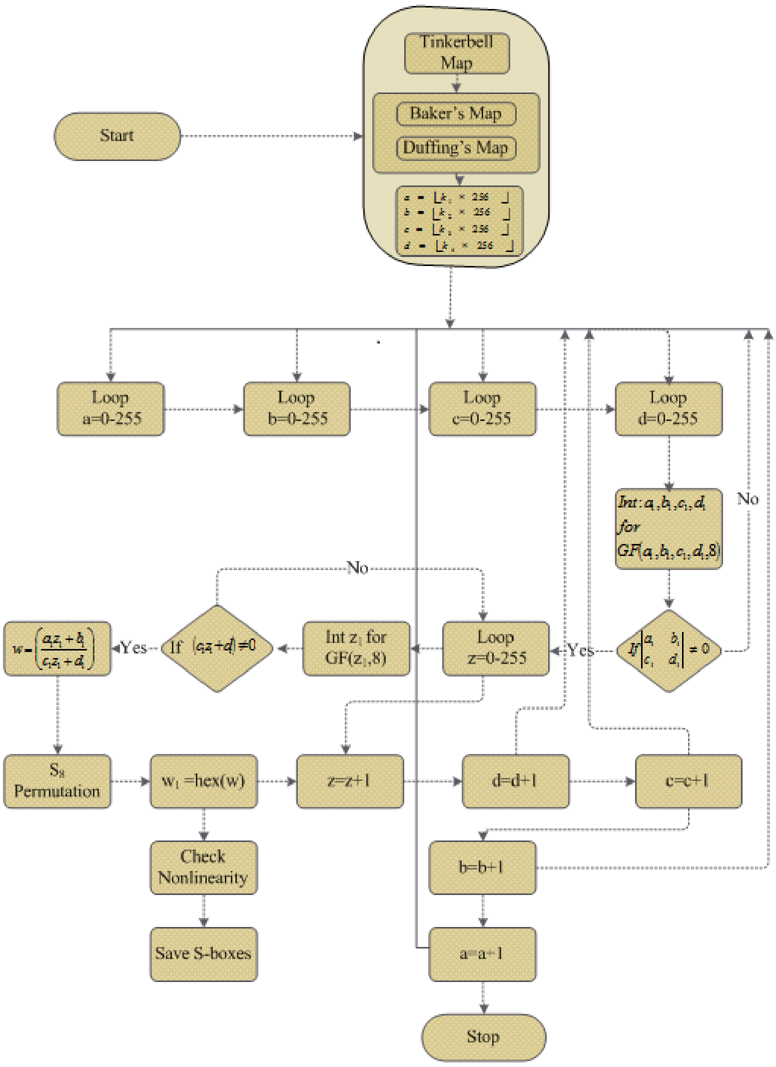

Fig. 6.1: Flow chart of Algorithm

6.1.2 S-boxes and enciphering

By using the previous algorithm we select different S-boxes, which are presenred as follows:

038	058	171	191	014	148	140	103	215	129	222	131	006	137	203	047
039	201	063	057	120	200	119	020	111	168	065	107	138	231	060	102
196	104	159	097	160	070	059	044	041	172	139	010	126	251	229	037
001	166	112	156	017	115	252	182	117	134	224	072	091	008	195	181
232	197	066	141	136	043	254	000	003	178	240	046	110	173	237	033
155	228	040	078	242	011	076	036	050	096	069	051	245	114	026	130
023	002	241	158	106	074	077	167	164	233	094	179	189	230	099	007
056	132	018	098	146	236	239	174	145	116	085	217	154	081	188	083
199	220	052	223	219	177	004	244	147	100	209	029	055	030	093	208
143	089	125	061	064	150	124	162	013	086	095	249	113	194	204	192
080	005	248	087	207	121	118	142	151	186	027	210	101	035	082	071
009	206	024	170	221	157	193	247	122	169	028	238	045	213	165	184
180	216	016	067	088	226	225	128	053	108	034	202	062	123	205	012
211	218	068	190	054	152	048	149	042	163	227	183	090	161	049	235
073	092	127	187	198	133	031	135	105	243	015	022	019	255	109	253
079	084	214	176	025	234	075	153	032	250	175	021	212	144	185	246

S-box 1

111	240	031	114	010	074	072	098	021	128	183	056	029	045	120	150
214	236	077	189	246	191	138	102	053	252	192	227	095	253	038	125
104	216	161	109	215	121	136	110	047	235	158	096	232	204	039	093
148	101	122	090	217	181	152	147	173	233	089	067	085	178	135	027
132	242	070	115	087	205	083	244	012	075	230	100	160	051	037	190
175	059	220	028	196	174	108	229	091	210	134	105	020	005	001	088
041	164	003	201	254	057	186	142	002	099	019	225	209	129	124	006
218	044	026	084	222	064	018	206	200	208	211	249	203	015	184	103
023	245	042	151	143	224	197	243	226	202	163	167	063	169	071	034
185	213	234	146	250	080	061	065	188	092	166	004	141	055	212	231
187	052	199	000	097	079	176	162	107	068	195	094	140	137	040	011
043	130	113	009	133	076	119	016	198	030	117	239	062	156	036	022
035	182	081	154	194	112	014	238	048	054	058	237	172	060	180	066
153	078	131	024	123	082	207	228	221	149	165	193	017	241	177	139
118	251	255	013	126	170	116	106	219	033	179	168	171	159	248	046
144	050	247	157	086	032	049	223	145	073	127	155	007	025	069	008

S-box 2

099	080	241	090	057	141	134	155	183	104	123	092	031	136	210	060
220	227	206	069	114	007	070	182	234	094	164	017	002	236	064	103
023	119	110	065	133	228	077	245	230	112	006	122	014	137	038	250
089	217	194	242	184	186	170	124	095	081	160	221	214	255	189	207
030	045	054	213	088	024	248	202	042	142	059	100	047	010	218	072
253	222	116	226	176	016	172	130	073	027	074	071	107	150	026	025
254	001	013	232	193	021	028	105	199	246	018	135	096	040	196	219
005	158	165	181	050	131	068	056	249	200	208	012	097	048	037	223
157	191	022	075	235	169	125	251	203	039	163	086	146	101	132	118
224	076	062	046	229	216	190	085	147	079	198	098	113	174	120	177
233	067	162	154	188	011	168	121	238	087	195	020	058	152	139	053
106	128	127	171	144	032	252	159	231	008	111	178	019	078	185	117
149	197	239	237	035	173	115	205	244	082	029	063	201	052	247	034
033	102	126	240	093	212	156	083	140	108	129	179	084	204	049	143
043	180	041	004	138	166	036	055	243	015	153	009	175	044	000	192
061	187	215	109	151	003	148	225	161	051	209	091	145	211	066	167

S-box 3

045	121	034	077	000	202	109	074	120	241	023	242	140	212	060	027
003	225	030	171	176	157	154	255	104	106	048	219	117	205	092	155
018	081	013	220	005	139	174	097	193	011	085	197	059	061	226	178
054	069	215	251	163	204	160	119	179	101	201	152	001	142	118	158
134	165	135	072	156	094	021	181	093	008	056	040	091	247	189	133
250	012	206	248	115	086	020	231	127	016	089	043	147	063	209	099
105	070	129	141	055	090	228	194	230	190	131	136	051	022	067	082
175	039	233	111	057	128	138	019	024	029	148	167	026	130	126	249
088	235	110	210	065	002	025	246	038	146	103	253	177	068	173	245
123	224	083	107	031	216	044	227	073	052	004	221	032	162	076	234
028	078	017	062	229	238	050	007	185	153	084	102	100	144	170	223
114	186	232	188	159	208	014	137	184	169	096	049	071	015	150	172
132	112	196	192	066	113	151	200	010	053	098	006	191	211	080	182
252	164	042	217	161	064	183	213	207	009	187	087	214	254	037	199
035	095	033	180	122	041	143	222	218	239	244	108	195	168	046	240
236	124	166	058	149	075	145	237	198	125	047	243	203	116	036	079

S-box 4

214	167	012	038	194	024	191	202	132	190	016	233	200	242	196	245
204	143	227	044	065	027	070	201	031	208	183	218	019	023	254	121
039	047	064	207	248	172	178	228	126	010	088	216	105	058	061	062
136	226	219	116	097	051	005	033	046	067	083	163	187	085	235	030
043	008	055	230	036	154	057	146	159	185	018	122	133	107	161	095
014	081	029	100	137	140	224	113	127	237	153	247	139	028	189	040
035	198	169	197	004	098	151	094	144	231	034	053	221	079	255	021
251	032	084	092	181	215	042	109	068	120	240	179	000	117	112	119
229	246	253	195	243	150	239	006	149	054	003	182	102	056	099	115
011	238	186	096	076	173	157	090	225	001	128	111	160	073	118	244
211	110	082	129	074	060	203	177	050	052	015	009	013	164	212	125
170	072	142	069	176	220	078	156	048	101	223	093	077	168	184	234
155	124	241	063	174	152	232	158	049	166	026	193	209	106	213	250
066	171	130	002	205	104	086	162	089	135	131	180	059	114	080	037
192	199	108	222	188	087	145	206	147	091	020	210	148	017	075	141
236	123	007	138	252	025	249	022	071	175	134	041	103	217	045	165

S-box 5

081	042	231	078	200	007	205	046	109	003	036	225	102	070	059	149
144	034	131	117	217	161	082	095	067	066	201	167	031	136	107	125
237	190	213	160	140	015	186	039	179	216	020	035	143	048	005	045
203	240	212	164	108	098	135	175	233	157	032	013	072	228	189	110
178	234	065	154	155	163	006	084	224	219	043	000	004	249	235	226
119	092	130	152	047	146	080	076	090	172	120	121	074	044	176	040
009	086	075	019	118	011	057	050	252	038	220	202	156	018	027	207
204	142	194	150	241	248	054	116	022	184	227	087	139	174	196	193
247	169	106	071	056	168	254	239	085	010	030	236	182	089	060	191
214	063	162	023	113	166	079	073	104	243	134	195	088	148	124	122
210	177	029	197	238	114	246	250	229	014	253	208	016	041	123	055
221	173	061	111	028	192	058	002	242	185	008	206	138	012	026	051
141	052	183	093	112	033	244	049	127	101	126	180	129	133	255	223
137	021	251	171	222	024	096	147	068	064	170	211	230	103	115	232
245	158	077	153	188	025	159	181	091	218	053	198	132	083	062	100
105	099	209	165	215	097	094	199	001	069	187	145	128	017	151	037

S-box 6

214	139	230	040	123	072	069	014	027	104	042	120	110	095	238	023
188	169	070	068	093	047	216	029	018	153	025	155	117	142	236	210
010	137	004	113	249	205	092	195	187	156	101	140	084	231	087	173
005	159	252	179	085	163	052	065	086	209	007	114	028	203	232	103
044	197	017	024	075	046	150	038	141	078	060	021	226	178	143	016
194	239	000	090	217	045	162	063	213	012	218	102	136	118	177	168
107	161	126	148	081	022	013	165	235	254	058	036	057	237	176	134
006	212	200	041	146	223	056	158	112	132	243	100	088	166	206	054
003	109	233	193	079	082	225	128	053	157	026	220	033	160	199	183
240	251	116	186	111	002	001	164	039	099	250	035	234	201	059	077
145	096	119	151	108	175	242	061	011	073	228	149	124	074	207	048
255	167	208	030	037	080	121	020	091	227	215	170	244	094	152	224
219	097	055	204	192	009	144	106	131	182	051	129	147	067	185	221
174	247	184	049	083	198	034	127	248	191	125	171	253	189	031	196
222	154	064	190	133	066	135	015	229	105	071	076	115	241	050	062
019	043	245	130	122	202	098	246	172	211	008	180	032	181	089	138

S-box 7

113	204	106	038	194	130	225	182	005	027	121	202	151	072	025	191
165	070	020	207	024	000	167	004	230	246	236	145	142	248	220	164
083	177	001	118	238	197	196	245	098	185	132	146	206	023	150	208
174	179	101	085	082	237	068	186	229	200	034	031	013	044	137	157
232	192	091	094	114	105	009	175	124	060	017	049	147	215	022	019
006	168	243	095	074	233	129	090	029	126	021	138	002	071	221	089
047	052	211	040	110	030	026	012	210	014	055	067	092	058	042	156
148	116	170	135	169	242	063	250	252	056	166	115	119	093	219	231
254	088	033	117	218	099	043	255	143	193	065	154	224	171	079	159
036	077	081	178	181	084	018	234	189	057	226	128	039	008	241	249
235	131	103	253	173	051	160	247	123	107	176	205	078	240	076	125
016	172	133	045	201	048	162	184	140	109	104	190	153	239	217	096
059	139	244	028	251	212	180	080	163	222	203	188	010	046	069	054
227	152	087	228	086	149	062	158	112	003	195	050	102	136	134	120
011	032	223	035	108	007	183	041	073	199	141	214	097	066	075	100
216	122	155	213	053	144	015	111	127	209	161	198	187	037	064	061

S-box 8

006	023	079	183	050	015	009	067	040	213	195	088	254	008	180	074
174	087	001	202	250	166	103	068	035	212	136	124	082	243	081	071
153	133	159	168	018	253	137	140	165	179	123	063	116	227	129	218
185	176	219	229	154	117	064	042	228	085	070	090	110	061	207	121
146	164	155	065	120	178	013	197	148	118	039	149	235	224	053	086
150	211	203	111	233	189	186	204	094	147	223	201	172	231	214	246
095	028	096	073	208	181	151	242	226	128	127	209	030	143	062	248
084	047	038	245	105	016	200	027	177	240	069	238	033	190	052	130
114	144	097	247	191	058	066	046	056	196	216	221	093	217	255	206
170	194	156	007	122	012	036	107	083	139	010	029	182	100	169	034
198	044	230	188	142	055	098	004	161	125	251	011	145	134	215	043
173	113	076	119	045	239	022	109	225	158	032	108	232	205	091	017
175	019	171	157	193	078	021	249	026	141	244	210	037	014	048	077
020	162	101	184	005	220	126	192	132	072	163	234	099	059	049	002
057	131	054	187	237	092	051	089	104	080	199	152	024	031	075	025
041	252	060	112	138	236	160	167	003	222	000	115	106	135	102	241

S-box 9

116	007	083	186	225	035	005	151	065	088	112	099	039	084	068	205
049	139	154	176	252	029	087	075	122	230	162	036	060	003	178	016
208	012	128	066	164	109	189	030	254	144	086	080	234	146	021	103
061	027	002	213	210	059	024	028	110	241	017	228	025	248	124	053
142	247	198	141	242	211	236	250	253	137	023	069	130	123	161	000
134	183	095	245	227	202	064	104	220	217	090	126	014	160	129	221
114	224	133	235	038	194	136	184	031	155	182	111	089	107	092	125
159	032	056	048	037	015	010	091	050	240	199	132	001	047	214	051
077	226	193	117	158	019	206	072	150	046	096	009	082	170	181	013
229	218	222	165	018	223	196	071	131	219	054	062	246	073	200	040
191	100	052	238	185	171	167	145	120	093	098	058	195	121	026	192
041	163	113	022	127	081	079	034	057	175	231	174	138	140	172	033
042	006	004	244	063	201	143	203	067	152	157	102	020	168	074	156
188	179	094	197	105	118	237	212	180	078	070	233	216	076	243	119
085	045	115	008	173	148	249	043	055	251	255	106	101	135	177	204
147	169	153	190	166	044	207	187	209	149	011	239	097	215	108	232

S-box 10

200	157	156	109	231	205	143	183	223	046	042	158	251	020	120	121
003	079	000	117	053	139	112	159	025	056	194	019	108	085	254	054
225	093	040	082	243	179	193	033	036	248	059	048	212	095	021	078
102	028	196	013	031	034	182	131	201	023	134	024	161	026	063	029
192	197	065	066	163	070	215	047	247	222	094	162	168	081	149	018
098	128	167	001	027	038	232	039	113	184	229	246	198	219	236	140
032	180	213	216	068	148	175	096	136	203	058	195	075	211	002	015
250	189	084	057	187	099	005	090	228	061	049	088	199	214	153	111
166	233	035	073	239	190	252	173	145	234	006	007	037	151	074	242
150	241	106	080	206	017	172	185	132	076	146	041	255	114	253	100
009	014	122	238	110	104	083	116	052	045	123	154	012	087	101	220
091	165	044	086	050	170	118	011	221	176	137	062	210	164	186	130
181	141	051	089	115	144	218	125	224	067	004	072	160	016	142	152
240	204	105	077	127	097	126	022	178	138	030	010	129	055	249	188
226	147	103	207	107	060	092	043	008	209	155	169	171	208	230	064
191	177	124	174	237	133	235	244	202	071	135	217	227	069	119	245

S-box 11

172	104	010	046	078	056	070	062	238	224	137	052	228	072	076	150
181	232	080	230	200	018	085	236	111	229	169	021	132	158	092	142
087	180	227	051	014	182	086	123	025	054	047	193	089	146	094	098
118	242	155	219	064	157	190	161	203	212	069	233	031	162	136	226
170	114	028	128	216	106	012	002	144	017	250	185	008	038	130	231
004	068	213	249	154	032	246	001	171	000	149	026	153	019	040	119
015	109	113	107	053	115	178	202	035	254	183	127	083	205	125	030
140	168	022	174	061	131	011	239	090	237	133	197	073	034	152	066
173	048	097	234	116	206	067	049	145	210	005	027	077	126	167	148
138	024	057	100	088	179	099	198	235	241	006	251	217	105	063	074
175	029	189	065	201	121	211	160	095	208	147	248	110	120	039	151
187	009	164	003	204	060	194	143	223	122	166	050	188	195	177	244
186	192	243	207	013	209	245	222	220	218	196	023	016	093	084	221
044	033	247	191	101	037	007	075	055	043	159	156	036	081	252	139
071	117	225	103	045	042	096	240	020	082	108	141	255	176	184	215
124	253	214	058	079	199	129	091	163	059	165	134	102	135	112	041

S-box 12

222	042	051	103	203	200	244	240	046	143	198	009	125	034	136	155
079	092	028	122	251	039	096	026	169	167	104	191	212	208	115	011
084	237	239	182	117	177	194	068	031	141	053	232	050	004	048	249
144	023	196	130	070	036	110	179	040	082	218	095	252	010	017	190
164	163	128	132	243	160	186	231	230	189	016	146	127	108	205	003
216	126	014	201	100	111	035	223	066	180	030	006	094	007	102	073
134	087	058	105	142	008	174	063	089	116	147	197	071	000	029	181
199	061	253	235	133	088	171	168	145	245	172	138	021	065	076	057
225	192	119	151	248	013	238	224	064	120	246	187	121	233	060	254
204	178	015	118	001	150	090	019	226	166	140	022	074	113	152	195
185	211	131	149	083	219	154	086	025	059	229	250	002	173	032	206
242	210	091	107	241	227	217	148	114	038	247	099	020	049	012	005
162	027	085	184	176	024	161	033	054	109	159	157	214	056	156	093
139	077	078	193	045	037	018	158	069	135	124	175	129	165	209	075
080	207	044	041	137	052	220	228	072	101	123	170	188	097	202	236
221	067	098	234	055	047	106	213	183	081	215	153	043	062	255	112

S-box 13

125	076	194	195	236	251	106	009	130	157	082	155	213	083	142	164
226	120	041	253	004	219	075	006	231	239	159	063	121	111	221	230
124	250	138	073	135	065	237	171	247	208	062	055	052	204	149	044
150	071	184	119	196	179	144	072	254	112	139	167	046	091	136	224
182	176	207	201	051	140	122	029	175	191	200	049	026	244	080	094
117	011	012	068	001	081	203	098	178	093	016	215	220	010	079	034
090	161	115	255	243	042	110	002	152	058	053	104	234	108	031	132
133	028	143	169	222	128	141	205	232	252	249	172	146	197	177	017
217	096	084	212	048	008	103	088	057	227	206	160	100	245	134	107
027	248	105	154	190	126	173	210	060	158	229	025	235	020	118	066
187	192	007	039	036	225	202	129	037	183	054	102	045	199	095	033
156	000	145	193	003	181	018	013	077	085	114	056	087	064	242	162
209	153	097	174	043	240	137	163	035	214	030	241	021	188	189	023
074	059	038	022	061	186	047	015	223	019	165	131	180	151	005	218
113	216	211	246	089	228	185	070	101	050	116	078	086	123	168	067
127	040	238	148	109	024	147	166	170	099	069	032	233	092	014	198

S-box 14

067	234	092	006	186	192	060	099	090	221	028	002	202	059	217	214
220	104	054	031	064	182	128	227	242	235	070	142	117	055	014	094
088	228	133	206	252	134	198	017	071	210	049	112	105	189	213	130
023	069	119	047	080	208	164	012	137	038	123	129	057	025	065	224
058	140	024	122	253	091	126	111	081	114	042	008	125	154	062	121
086	056	254	107	079	240	100	113	226	229	076	178	160	146	237	009
068	032	089	013	249	082	179	115	101	148	041	072	239	246	194	215
084	153	007	004	225	036	248	048	097	177	078	027	207	155	247	011
033	196	255	174	000	204	184	016	222	144	158	236	074	180	152	245
209	035	183	156	132	201	166	243	187	233	037	211	162	015	168	110
127	045	010	073	203	034	231	003	223	195	181	020	169	250	190	139
176	219	040	039	199	063	212	241	018	118	157	238	145	093	136	106
135	051	151	083	244	173	108	171	022	050	200	216	218	163	197	191
087	193	095	019	170	185	109	044	232	159	005	230	021	096	103	131
120	205	188	147	075	124	030	001	102	116	150	098	046	061	167	149
026	251	138	143	043	085	165	141	161	029	172	053	175	077	066	052

S-box 15

6.2 Neutrosophic soft set for decision making

In this section, we elaborate the NSS-decision making method for this we propose a few important definitions.

Definition 6.2.1. *If Γ_E is the NSS and $\mu_{\tau_E(e)}(s_i), \gamma_{\tau_E(e)}(s_i)$ and $\upsilon_{\tau_E(e)}(s_i)$ denote the membership degree, indeterminacy degree and non-membership degree of object s_i respectively. Then the average deviation of membership, indeterminacy and non-membership are;*

$$\begin{aligned} \mu^*_{\tau_E}(s_i) &= \frac{1}{n}\sum |\mu_{\tau_E(e)}(s_i) - \bar{\mu}_{\tau_E(e)}(s)|, \\ \gamma^*_{\tau_E}(s_i) &= \frac{1}{n}\sum |\gamma_{\tau_E(e)}(s_i) - \bar{\gamma}_{\tau_E(e)}(s)|, \\ \upsilon^*_{\tau_E}(s_i) &= \frac{1}{n}\sum |\upsilon_{\tau_E(e)}(s_i) - \bar{\upsilon}_{\tau_E(e)}(s)|, \end{aligned} \tag{6.2.1}$$

Then for each $s_i \in S$, and $\bar{\mu}_{\tau_E(e)}(s), \bar{\gamma}_{\tau_E(e)}(s)$ and $\bar{\upsilon}_{\tau_E(e)}(s)$ are mean of $\mu_{\tau_E(e)}(s_i), \gamma_{\tau_E(e)}(s_i)$ and $\upsilon_{\tau_E(e)}(s_i)$. It is presented as follows;

$$< \mu^*_{\tau_E}(s_i), \gamma^*_{\tau_E}(s_i), \upsilon^*_{\tau_E}(s_i) > . \tag{6.2.2}$$

Definition 6.2.2. *A comparison table for **membership** function, denoted by Υ, is a table in which, the number of rows are equal to the number of columns, rows and columns both are labeled by the parameters $e_1, e_2, \cdots, e_n$. The entries are $x_{ij},\ i, j = 1, 2, \cdots, n$, given by*

$$\begin{aligned} x_{ij} &= \text{the number, for which the member degree of } e_i \text{ is} \\ &\quad \text{important by the membership degree of } e_j \\ &= \begin{cases} 2 & \text{if } e_i > e_j, \\ 1 & \text{if } e_i < e_j. \end{cases} \end{aligned} \tag{6.2.3}$$

(6.2.1)

Note that $0 \leq x_{ij} \leq p$, $x_{ii} = p$ for all i, j and p is the number of objects presented.

*Comparison table for **intermediate** function is denoted by Φ. It is a table in which number of rows are equal to the number of columns, rows and columns both are labeled by he parameters $e_1, e_2, \cdots, e_n$. The entries are $y_{ij},\ i, j = 1, 2, \cdots, n$, given by*

$$\begin{aligned} y_{ij} &= \text{the number, for which the intermediate degree of } e_i \text{ is} \quad (6.2.4) \\ &\quad \text{important by the intermediate degree of } e_j \\ &= \begin{cases} 2 & \text{if } e_i > e_j, \\ 1 & \text{if } e_i < e_j. \end{cases} \quad (6.2.2) \end{aligned}$$

where $0 \leq y_{ij} \leq p$, $y_{ii} = p$ for all i, j and p is the number of objects present in the universal set.

*Finally, Ψ is a comparison table of **non-membership** function, in which number of rows are equal to the number of columns. Moreover, rows and columns both are labeled by the parameters $e_1, e_2, \cdots, e_n$. The entries are $z_{ij},\ i, j = 1, 2, \cdots, n$, given by*

$$\begin{aligned} z_{ij} &= \text{the number, for which the non-membership degree of } e_i \text{ is} \quad (6.2.5) \\ &\quad \text{important by the non-membership degree of } e_j \\ &= \begin{cases} 2 & \text{if } e_i > e_j, \\ 1 & \text{if } e_i < e_j. \end{cases} \quad (6.2.3) \end{aligned}$$

where $0 \leq z_{ij} \leq p$ and $z_{ii} = p$, for all i, j and p is the number of objects present in the universal set.

Definition 6.2.3. *The membership function row and column sum of a parameter e_i, denoted by Υ_{r_i} and Υ_{c_i} respectively and defined as*

$$\begin{aligned} \Upsilon_{r_i} &:= \sum_{j=1}^{n} x_{ij}, \\ \Upsilon_{c_i} &:= \sum_{j=1}^{n} x_{ij}. \end{aligned} \quad (6.2.6)$$

The intermediate function row and column of a parameter e_i, is presented by Φ_{r_i} and Φ_{c_i} respectively and defined as

$$\begin{aligned}\Phi_{r_i} &:= \sum_{j=1}^{n} y_{ij}, \\ \Phi_{c_i} &:= \sum_{j=1}^{n} y_{ij}. \end{aligned} \tag{6.2.7}$$

The negative function row and column of a parameter e_i, is presented by Ψ_{r_i} and Ψ_{c_i} respectively and defined as

$$\begin{aligned}\Psi_{r_i} &:= \sum_{i=1}^{n} z_{ij}, \\ \Psi_{c_i} &:= \sum_{j=1}^{n} z_{ij}. \end{aligned} \tag{6.2.8}$$

Definition 6.2.4. *The **Positive Weight** of each parametric set $e_i \in E$, can be computed from following formula:*

$$\mu_E(e_i) := \frac{(\Upsilon_{r_i} - \Upsilon_{c_i})}{6}. \tag{6.2.9}$$

*The **Intermediate weight** of the parametric set $e_i \in E$ can be computed as:*

$$\gamma_E(e_i) := \frac{(\Phi_{r_i} - \Phi_{c_i})}{6}. \tag{6.2.10}$$

*Similarly, the **Negative weight** of the parametric set $e_i \in E$ can be given as,*

$$\upsilon_E(e_i) := \frac{(\Psi_{r_i} - \Psi_{c_i})}{6}. \tag{6.2.11}$$

Finally, for all $e_i \in E$, the Neutrosophic Set (NS) over E, is as below;

$$\Lambda := \{(e, \mu_E(e_i), \gamma_E(e_i), \upsilon_E(e_i)) : e_i \in E\}. \tag{6.2.12}$$

Definition 6.2.5. *If* Γ_E *be the* ***NSS*** *over* S *and* Λ *is* ***NS*** *over* E*, then the evaluation value of* s_i *can be calculated from,*

$$\begin{aligned} \mu_{E(i)}(s_i) &: = \max\{\mu^*_{\tau_E(e_j)}(s_i) \cdot \mu_E(e_j) : e_j \in E\}, \\ \gamma_{E(i)}(s_i) &: = median\{\gamma^*_{\tau_E(e_j)}(s_i) \cdot \gamma_E(e_j) : e_j \in E\}, \\ v_{E(i)}(s_i)L &= \min\{v^*_{\tau_E(e_j)}(s_i) \cdot v_E(e_i) : e_j \in E\}, \end{aligned} \tag{6.2.13}$$

where $1 \leq i \leq n$ *and* $1 \leq j \leq m$*. The evaluation set is defined as follows;*

$$\left[\mu_{E(i)}, \gamma_{E(i)}, v_{E(i)}\right], \tag{6.2.14}$$

for all $s_i \in S$ *and* $e_j \in E$*.*

Definition 6.2.6. *Let* Γ_E *be the* ***NSS*** *over* S*. The evaluation score of* $s_i \in S$*, is calculated from the evaluation set as;*

$$\hat{s}_i = \mu_{E(i)} + \gamma_{E(i)} - v_{E(i)}, \tag{6.2.15}$$

for $1 \leq i \leq n$*. Moreover the final evaluation score can be obtained from following,*

$$s = \max_{1 \leq i \leq n} \{\hat{s}_i\}. \tag{6.2.16}$$

6.3 A new decision making procedure based on neutrosophic soft set

Decision making is the process of choosing the best among the available alternatives. We will proceed further by defining the algorithm for the decision-making criterion. The steps for the decision of selecting an appropriate choice are:

1. Choose the NSS Γ_E over the universe $NS(U)$.
2. Compute average deviation of NSS for each $s_i \in S$.

3. Compute the comparison tables Υ, Φ and Ψ.
4. Compute positive, intermediary and negative weight value for each parameter.
5. Construct the NS-set Λ over the parametric set E.
6. Construct the evaluation intervals for each object s_i.
7. Compute the evaluation scores $\hat{s}_i$.
8. Find s, for which $s = \max_{1 \leq i \leq n} \{\hat{s}_i\}$.

Flow chart of new decision making using NSS

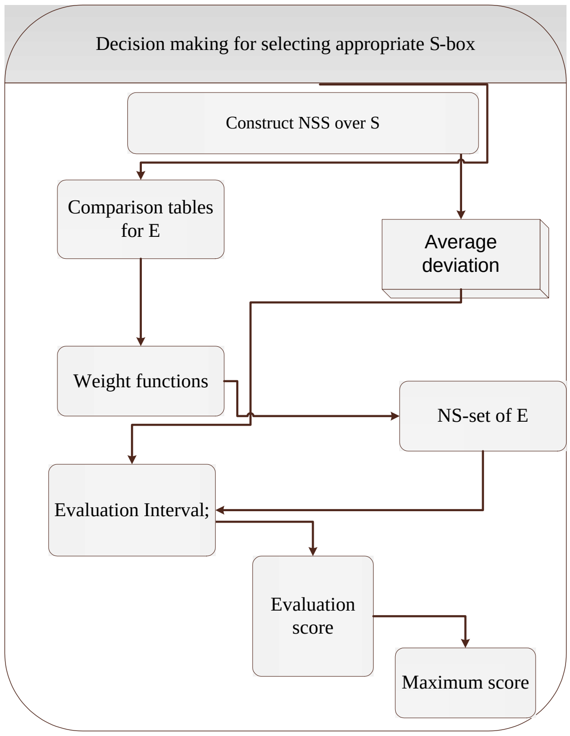

Fig. 6.2: Flow chart of new decision making by using neutrosophic soft set

6.4 A new decision making on neutrosophic soft set for selecting the suitable S-box

The decision-making process is one which involves various objects along with certain analyses parameters, followed by choosing the best one among them. The S-box has a particular importance in crypto-system, without it, attackers would compromise the system with ease. The fundamental objective of S-box is to construct a nonlinear mapping between the original text and encrypted text. The effectiveness of the S-box is investigated by using various parameters used in the literature. In [92], the algebraic and statistical analysis are used for the encrypted image of Lena. Though, in this study by using statistical analysis, an NSS-decision making criterion is constructed for the selection of the most effective S-box from a given set of S-boxes. The findings of NSS-decision making criterion are better than the output obtained by IFS (that is, Intuitionistic Fuzzy Sets) analysis.

The following table presents some image encryption analysis such as entropy, energy, correlation, homogeneity and contrast for fifteen S-boxes formed in section 6.1.2.

S-box	Entropy	Energy	Correlation	Homogeneity	Contrast
Plain Image	7.246	0.1615	0.9073	0.8995	0.2805
S-box 1	7.5841	0.0207	0.1444	0.4897	6.9398
S-box 2	7.5841	0.0203	0.0971	0.4776	7.5808
S-box 3	7.5841	0.0199	0.1301	0.4827	7.2333
S-box 4	7.5841	0.0191	0.1348	0.4778	7.5838
S-box 5	7.5841	0.0203	0.133	0.4845	7.0992
S-box 6	7.5841	0.0187	0.1305	0.4766	8.0428
S-box 7	7.5841	0.0193	0.1098	0.4753	7.7116
S-box 8	7.5841	0.0193	0.141	0.4788	7.3847
S-box 9	7.5841	0.0204	0.1432	0.485	7.1097
S-box 10	7.5841	0.0205	0.1271	0.489	7.595
S-box 11	7.5841	0.0197	0.1409	0.4844	7.4919
S-box 12	7.5841	0.0198	0.1338	0.485	7.4289
S-box 13	7.5841	0.0193	0.1224	0.4764	7.6968
S-box 14	7.5841	0.0208	0.1306	0.4867	7.1906
S-box 15	7.5841	0.0196	0.1267	0.4825	7.7758

Table 6.1: Image encryption analyses of S-box

Following are the graphical representation of various S-boxes corresponding to different image encryption analysis obtained by table 6.1.

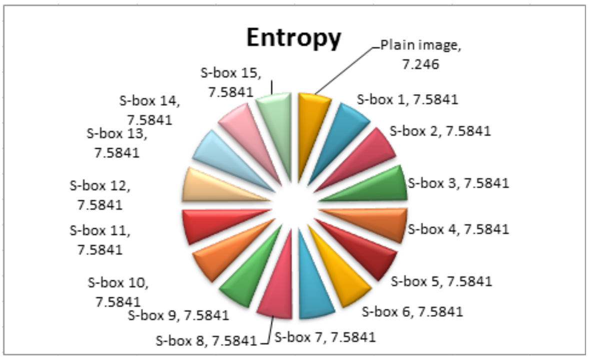

Fig. 6.3: Entropy analyses of tested S-boxes.

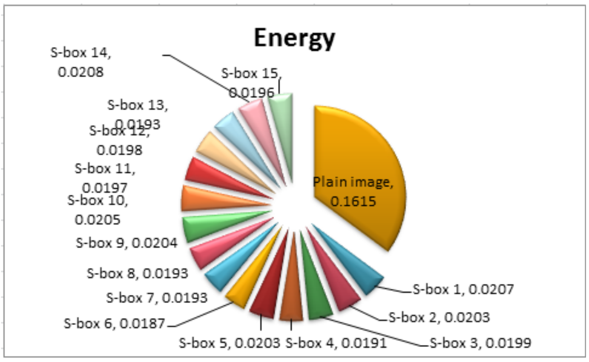

Fig. 6.4: Energy analyses of tested S-boxes.

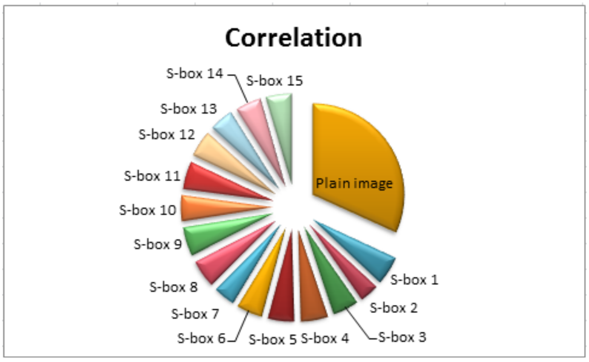

Fig. 6.5: Correlation analyses of tested S-boxes.

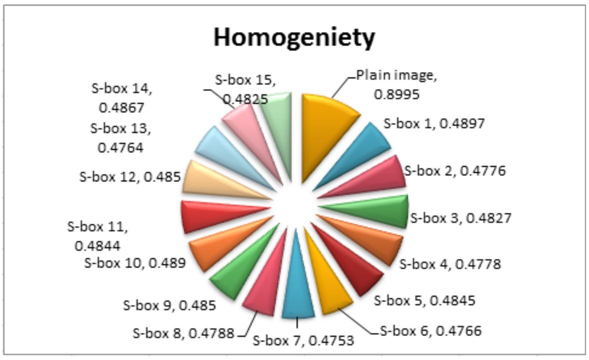

Fig. 6.5. Homogenity analyses of tested S-boxes.

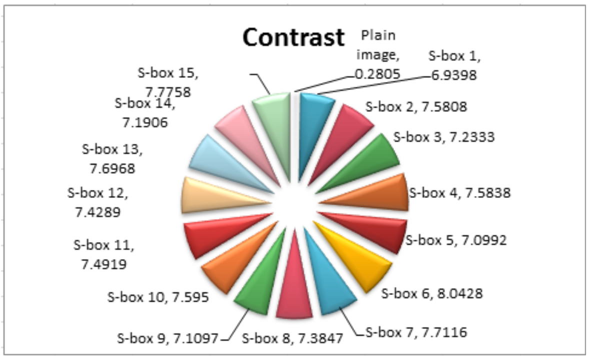

Fig. 6.6: Contrast analyses of tested S-boxes.

Enciphered images

In this work, we have used the simulation results for fifteen S-boxes for the analysis. The Fig 6.8, shows the original image and others are enciphered images. The effects of the nonlinear substitution can be observed by visually examining the transformed images resulting from the original image.

Fig 6.7: Plain image of Lena

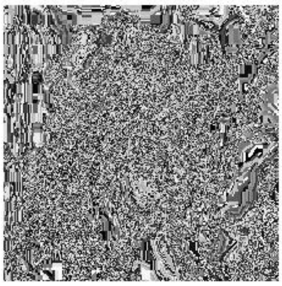

Fig 6.8: Enciphered S-box 1

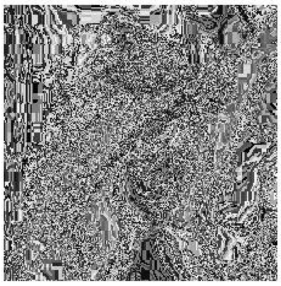

Fig 6.9: Enciphered S-box 2

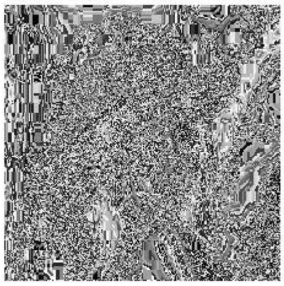

Fig 6.10: Enciphered S-box 3

Fig 6.11: Enciphered S-box 4

Fig 6.12: Enciphered S-box 5

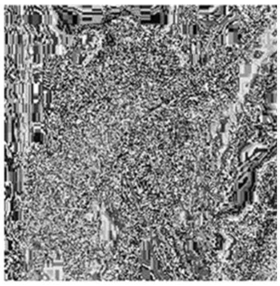

Fig 6.13: Enciphered S-box 6

Fig 6.14: Enciphered S-box 7

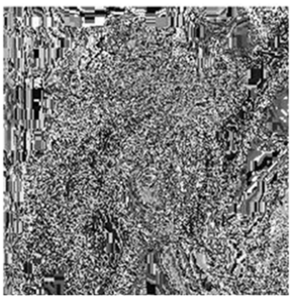

Fig 6.15: Enciphered S-box 8

Fig 6.16: Enciphered S-box 9

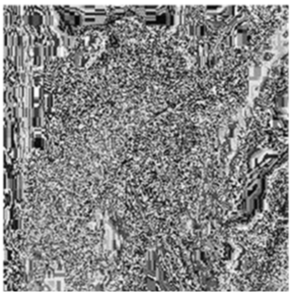

Fig 6.17: Enciphered S-box 10

Fig 6.18: Enciphered S-box 11

Fig 6.19: Enciphered S-box 12

Fig 6.20: Enciphered S-box 13

Fig 6.21: Enciphered S-box 14

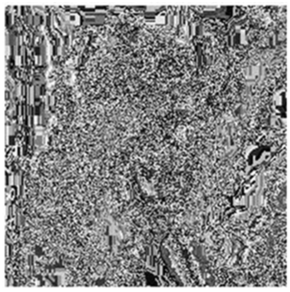

Fig 6.22: Enciphered S-box 15

We treat $S = \{s_1, s_2, s_3, \cdots, s_{15}\}$ as the universal set of S-boxes, where $s_i \in U$; $1 \leq i \leq 15$, represents fifteen different S-boxes. The S-boxes are characterized by the set of parameters $E = \{e_1, e_2, e_3, e_4, e_5\}$, where the parameters e_j, $1 \leq j \leq 5$, stands for the evaluation criteria of entropy, energy, correlation, homogeneity and contrast respectively. By using Neutrosophic set, we define the membership, intermediate and non-membership value of each S-box. Subsequently, we use a method based on NSS, for making a decision to choose an S-box of proficient nature.

6.4.1 Formula for computing the neutrosophic set (NS)

In this section, we begin by providing the reader, the details of the techniques to analyze the properties of S-boxes and their Neutrosophic set.

Neutrosophic set (NS) for Entropy

The entropy coefficient measures the uncertainty in the data. This coefficient scrutinizes the encrypted process. The neutrosophic set for soft set is measured by the following method:

$$\begin{aligned} \mu_{\tau_E(e_1)}(s_i) &= 2 - \frac{e_{1(s_i)}}{e_{1(P)}}, \\ \gamma_{\tau_E(e_1)}(s_i) &= e_{1(s_i)} (\bmod 1), \\ \upsilon_{\tau_E(e_1)}(s_i) &= \frac{e_{1(s_i)}}{e_{1(s_i)} + e_{1(P)}}, \end{aligned} \tag{6.4.1}$$

where $e_{1(P)}$ is the entropy of the plain image and $e_{1(s_i)}$ is the entropy of ciphered image for the S-box s_i and $1 \leq i \leq 7$.

Neutrosophic set (NS) for Energy The amount of square elements from GLMC has been used to assess the energy coefficient. The neutrosophic set for energy is measured by the following method:

$$\begin{aligned} \mu_{\tau_E(e_2)}(s_i) &= \frac{e_{2(s_i)}}{e_{2(P)}} + e_{2(P)}, \\ \gamma_{\tau_E(e_2)}(s_i) &= \frac{e_{2(s_i)} + e_{2(P)}}{2}, \\ \upsilon_{\tau_E(e_2)}(s_i) &= \frac{e_{2(s_i)}}{e_{2(P)}}, \end{aligned} \tag{6.4.2}$$

where $e_{2(P)}$ is the energy of the plain image and $e_{2(s_i)}$ is the energy of ciphered image for the S-box s_i and $1 \leq i \leq 7$.

Neutrosophic set (NS) for Correlation

The correlation coefficient is applied to specify the amount of similarity between two neighboring pixels. The correlation coefficient tells us the similarity between the original and coded information are identical. The neutrosophic set for correlation is denoted by e_3 and is defined as:

$$\begin{aligned} \mu_{\tau_E(e_3)}(s_i) &= e_{3(P)} - e_{3(s_i)}, \\ \gamma_{\tau_E(e_3)}(s_i) &= \frac{e_{3(P)} - e_{3(s_i)}}{e_{3(P)} + e_{3(s_i)}}, \\ v_{\tau_E(e_3)}(s_i) &= \frac{e_{3(s_i)}}{e_{3(P)}}, \end{aligned} \tag{6.3.3}$$

where $e_{3(P)}$ is the correlation of the plain image and $e_{3(s_i)}$ is the correlation of ciphered image for the S-box s_i and $1 \leq i \leq 7$.

Neutrosophic set (NS) for Homogenity

The analysis determines the evenness of established structure within the ciphertext. The neutrosophic set for homogeneity is denoted by e_4 and is as follows:

$$\begin{aligned} \mu_{\tau_E(e_4)}(s_i) &= \frac{e_{4(s_i)}}{e_{4(P)}}, \\ \gamma_{\tau_E(e_4)}(s_i) &= \frac{e_{4(P)} - e_{4(s_i)}}{e_{4(P)} + e_{4(s_i)}}, \\ v_{\tau_E(e_4)}(s_i) &= \frac{e_{4(P)}}{e_{4(P)} + e_{4(s_i)}}, \end{aligned} \tag{6.4.4}$$

where $e_{4(P)}$ is the homogeneity of the plain image and $e_{4(s_i)}$ is the homogeneity of ciphered image for the S-box s_i and $1 \leq i \leq 7$.

Neutrosophic set (NS) for Contrast

Local variation in the encrypted image is measured by contrast. The neutrosophic set for contrast is denoted by e_5 and is defined as:

$$\begin{aligned} \mu_{\tau_E(e_5)}(s_i) &= \frac{e_{5(s_i)} - e_{5(P)}}{e_{5(s_i)} + e_{5(P)}}, \\ \gamma_{\tau_E(e_5)}(s_i) &= e_{5(s_i)} (\mathrm{mod}\, 1), \\ v_{\tau_E(e)}(s_i) &= \frac{e_{5(P)}}{e_{5(s_i)}}, \end{aligned} \tag{6.4.5}$$

where $e_{5(P)}$ is the contrast of the plain image and $e_{5(s_i)}$ is the contrast of ciphered image for the S-box s_i and $1 \leq i \leq 7$.

6.4.2 Neutrosophic soft set (NSS)

The equations from (6.4.1-6.4.5) are used to define the NS of each parameters by taking the data from table 6.1. Using these NS, we form NSS and represent it in the following tabular form;

S-boxes	$(\mu_{\tau_E(e_1)}, \gamma_{\tau_E(e_1)}, \nu_{\tau_E(e_1)})$	$(\mu_{\tau_E(e_2)}, \gamma_{\tau_E(e_2)}, \nu_{\tau_E(e_2)})$	$(\mu_{\tau_E(e_3)}, \gamma_{\tau_E(e_3)}, \nu_{\tau_E(e_3)})$	$(\mu_{\tau_E(e_4)}, \gamma_{\tau_E(e_4)}, \nu_{\tau_E(e_4)})$	$(\mu_{\tau_E(e_5)}, \gamma_{\tau_E(e_5)}, \nu_{\tau_E(e_5)})$
s_1	(0.9533,0.5841,0.511)	(0.2896,0.0911,0.1281)	(0.7629,0.7253,0.1591)	(0.5444,0.2949,0.6474)	(0.9223,0.9398,0.0404)
s_2	(0.9533,0.5841,0.511)	(0.2872,0.0909,0.1256)	(0.8102,0.8066,0.1070)	(0.5309,0.3063,0.6531)	(0.9286,0.5808,0.0370)
s_3	(0.9533,0.5841,0.511)	(0.2847,0.0907,0.1232)	(0.7772,0.7492,0.1433)	(0.5366,0.3015,0.6507)	(0.9253,0.2333,0.0387)
s_4	(0.9533,0.5841,0.511)	(0.2797,0.0903,0.1182)	(0.7725,0.7412,0.1485)	(0.5311,0.3061,0.6530)	(0.9286,0.5838,0.0369)
s_5	(0.9533,0.5841,0.511)	(0.2871,0.0909,0.1256)	(0.7743,0.7443,0.1465)	(0.5386,0.2998,0.6499)	(0.9239,0.0992,0.0395)
s_6	(0.9533,0.5841,0.511)	(0.2773,0.0901,0.1158)	(0.7768,0.7485,0.1438)	(0.5298,0.3073,0.6536)	(0.9325,0.0428,0.0348)
s_7	(0.9533,0.5841,0.511)	(0.2810,0.0904,0.1195)	(0.7975,0.7840,0.1210)	(0.5284,0.3085,0.6542)	(0.9298,0.7116,0.0363)
s_8	(0.9533,0.5841,0.511)	(0.2810,0.0904,0.1195)	(0.7663,0.7309,0.1554)	(0.5322,0.3052,0.6526)	(0.9268,0.3847,0.0379)
s_9	(0.9533,0.5841,0.511)	(0.2878,0.0909,0.1263)	(0.7641,0.7273,0.1578)	(0.5391,0.2993,0.6496)	(0.9241,0.1097,0.0394)
s_{10}	(0.9533,0.5841,0.511)	(0.2884,0.091,0.1269)	(0.7802,0.7542,0.1400)	(0.5436,0.2956,0.6478)	(0.9287,0.595,0.0369)
s_{11}	(0.9533,0.5841,0.511)	(0.2834,0.0906,0.1219)	(0.7664,0.7311,0.1552)	(0.5385,0.2999,0.6499)	(0.9278,0.4919,0.0374)
s_{12}	(0.9533,0.5841,0.511)	(0.2841,0.0906,0.1226)	(0.7735,0.7429,0.1474)	(0.5391,0.2993,0.6496)	(0.9272,0.4289,0.0377)
s_{13}	(0.9533,0.5841,0.511)	(0.2810,0.0904,0.1195)	(0.7849,0.7622,0.1349)	(0.5296,0.3075,0.6537)	(0.9296,0.6968,0.0364)
s_{14}	(0.9533,0.5841,0.511)	(0.2903,0.0912,0.1287)	(0.7767,0.7483,0.1439)	(0.5410,0.2977,0.6488)	(0.9249,0.1906,0.0390)
s_{15}	(0.9533,0.5841,0.511)	(0.2828,0.0905,0.1213)	(0.7806,0.7549,0.1396)	(0.5364,0.3017,0.6508)	(0.9303,0.7758,0.0360)

Table 6.2: Neutrosophic soft set

6.4.3 Average deviation

By using the data from previous table 6.2, into equation (6.2.1), the average deviation is calculated. The computed values are expressed in (6.2.2) and average deviation is represent in the following table;

Avgdev(Γ_E)	$\left\langle \mu^*_{\tau_E}, \gamma^*_{\tau_E}, \nu^*_{\tau_E} \right\rangle$
s_1	$\langle 0.2273, 0.2672, 0.2256 \rangle$
s_2	$\langle 0.2429, 0.2201, 0.2363 \rangle$
s_3	$\langle 0.2338, 0.2199, 0.2301 \rangle$
s_4	$\langle 0.2350, 0.2103, 0.2308 \rangle$
s_5	$\langle 0.2320, 0.2404, 0.2288 \rangle$
s_6	$\langle 0.2369, 0.2493, 0.2324 \rangle$
s_7	$\langle 0.2417, 0.2370, 0.2354 \rangle$
s_8	$\langle 0.2330, 0.1907, 0.2293 \rangle$
s_9	$\langle 0.2294, 0.2347, 0.2268 \rangle$
s_{10}	$\langle 0.2318, 0.2165, 0.2295 \rangle$
s_{11}	$\langle 0.2308, 0.1954, 0.2283 \rangle$
s_{12}	$\langle 0.2322, 0.1875, 0.2294 \rangle$
s_{13}	$\langle 0.2383, 0.2314, 0.2331 \rangle$
s_{14}	$\langle 0.2214, 0.2271, 0.2285 \rangle$
s_{15}	$\langle 0.2349, 0.2442, 0.2314 \rangle$

Table 6.3: Average deviation.

6.4.4 Comparison tables

The comparison table 6.2 of NSS is computed by the method given in equations (6.2.3-6.2.5), we get following tables of interval;

Υ	e_1	e_2	e_3	e_4	e_5
e_1	15	30	30	30	30
e_2	15	15	15	15	15
e_3	15	30	15	30	30
e_4	15	30	15	15	30
e_5	15	30	15	15	15

Table 6.4: Membership comparison parameters.

Φ	e_1	e_2	e_3	e_4	e_5
e_1	15	30	15	30	24
e_2	15	15	15	15	29
e_3	30	30	15	30	28
e_4	15	30	15	15	20
e_5	20	29	17	23	15

Table 6.5: Intermediate comparison parameters.

Ψ	e_1	e_2	e_3	e_4	e_5
e_1	15	30	30	15	30
e_2	30	15	30	15	30
e_3	15	30	15	15	30
e_4	30	30	30	15	30
e_5	15	15	15	15	15

Table 6.6: Non-membership comparison parameters.

6.4.5 Weight function

Once again using the tables 6.4−6.6 into equations (6.2.6-6.2.11) we get values of weight functions of the membership, intermediate and non-membership functions for each parameter,

	Υ_{r_i}	Υ_{c_i}	$\Upsilon_{r_i} - \Upsilon_{c_i}$	μ_E
e_1	135	75	60	10
e_2	75	135	-60	-10
e_3	120	90	30	5
e_4	105	105	0	0
e_5	90	120	-30	-5

Table 6.7: Positive weight.

	Φ_{r_i}	Φ_{c_i}	$\Phi_{r_i} - \Phi_{c_i}$	γ_E
e_1	114	95	19	3.1667
e_2	89	134	-45	-7.5
e_3	133	77	56	9.3333
e_4	95	113	-18	-3
e_5	104	116	-12	-2

Table 6.8: Intermediate weight.

	Ψ_{r_i}	Ψ_{c_i}	$\Psi_{r_i} - \Psi_{c_i}$	ν_E
e_1	120	105	15	2.5
e_2	120	120	0	0
e_3	105	120	-15	-2.5
e_4	135	75	60	10
e_5	75	135	-60	-10

Table 6.9: Negative weight.

6.4.6 Neutrosophic set (NS)

The NS of tables computed from above tables 6.7−6.9, are arranged in the form given in (6.2.12) and represent NS in following table;

Λ	(μ_E, γ_E, ν_E)
e_1	$(10, 3.1667, 2.5)$
e_2	$(-10, -7.5, 0)$
e_3	$(5, 9.333, -2.5)$
e_4	$(0, -3, 10)$
e_5	$(-5, -2, -10)$

Table 6.10: NS-set.

6.4.7 Evaluation set

Using the values of table 6.3 and previous table 6.10 into equation (6.2.13) to calculate evaluation values. These values are further put into equation (6.2.14) and represent as follows;

Γ_E	$[\mu_{E(i)}, \gamma_{E(i)}, \nu_{E(i)}]$
s_1	$[2.2725, -0.5345, -2.2569]$
s_2	$[2.4295, -0.4402, -2.3635]$
s_3	$[2.3376, -0.4398, -2.3006]$
s_4	$[2.3503, -0.4206, -2.3087]$
s_5	$[2.3208, -0.4808, -2.2883]$
s_6	$[2.3685, -0.4988, -2.3249]$
s_7	$[2.4166, -0.4740, -2.3546]$
s_8	$[2.3301, -0.3815, -2.2930]$
s_9	$[2.2936, -0.4695, -2.2688]$
s_{10}	$[2.3183, -0.4331, -2.2958]$
s_{11}	$[2.3081, -0.3908, -2.2837]$
s_{12}	$[2.3222, -0.3749, -2.2941]$
s_{13}	$[2.3828, -0.4628, -2.3310]$
s_{14}	$[2.3144, -0.4541, -2.2859]$
s_{15}	$[2.3494, -0.4885, -2.3141]$

Table 6.11: Evaluation set.

6.4.8 Evaluation score

Next using the above table 6.11 into equation (6.2.15) we get the final evaluation score each of objects s_i, given as in form of following table;

	Score
$\hat{s}_1$	3.9951
$\hat{s}_2$	4.3528
$\hat{s}_3$	4.1984
$\hat{s}_4$	4.2384
$\hat{s}_5$	4.1283
$\hat{s}_6$	4.1947
$\hat{s}_7$	4.2972
$\hat{s}_8$	4.2417
$\hat{s}_9$	4.0931
$\hat{s}_{10}$	4.1810
$\hat{s}_{11}$	4.2010
$\hat{s}_{12}$	4.2414
$\hat{s}_{13}$	4.2509
$\hat{s}_{14}$	4.1462
$\hat{s}_{15}$	4.1751

Table 6.12: Evaluation score.

The graphical representation of score is as follows;

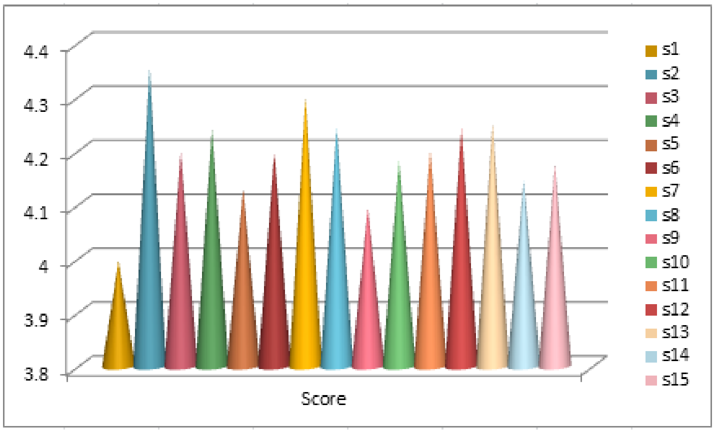

Fig. 6.23: Score of each S-box.

We can analyze from the graph that, since S-box 2 has the highest evaluation score so it turns out to be the best S-box for secure communication. Similarly, S-box 1 having the least evaluation score of all, reflects that it had performed poorly as compared to rest of S-boxes. The second best S-box is turns out to be S-box 7. The group of consisting of S-boxes 13, 8, 12 and 4 have almost similar values, consequently their performance is almost similar. We can also say that group consisting of S-boxes $11, 3, 6$ have similar performances.

6.4.9 Maximum score

Thus, the maximum score gives us the appropriate S-box. Using equation (6.2.15) we get;

$$s = \quad \hat{s}_2 = \quad 4.3528$$

Hence, the best result is achieved in the evaluation for s_2. Thus S-box 2 is an appropriate one.

6.4.10 Grading result

	Score
$\hat{s}_2$	4.3528
$\hat{s}_7$	4.2972
$\hat{s}_{13}$	4.2509
$\hat{s}_8$	4.2417
$\hat{s}_{12}$	4.2414
$\hat{s}_4$	4.2384
$\hat{s}_{11}$	4.2010
$\hat{s}_3$	4.1984
$\hat{s}_6$	4.1947
$\hat{s}_{10}$	4.1810
$\hat{s}_{15}$	4.1751
$\hat{s}_{14}$	4.1462
$\hat{s}_5$	4.1283
$\hat{s}_9$	4.0931
$\hat{s}_1$	3.9951

Table 6.13; Grading the S-boxes

The above table finally ranks the S-boxes as per their evaluation scores and hence their performance. The score justifies the fact that, when we apply our proposed algorithm, we don0t need lengthy manual work which reflects that less computational complexity is required to choose the best quality of S-box.

Chapter 7

Application of soft rings and soft modules in decision making problems of cryptography

The motivation for this chapter comes from the notion of the soft ring. The main objective is to construct a technique of the soft Galois ring and going to provide a cryptographic application of the constructed example. More precisely, we intend to employ a fuzzy bipolar soft decision-making algorithm based on soft Galois ring on selecting a secure S-box. Substitution boxes (S-boxes) is the simple yet critical component of substitution-permutation network (S-P network) to hide information while sending data. S-box is a technique that maps n bits to m bits. There are several techniques to construct an S-box [49, 50, 51, 52]. Shah et al.„ in [90] gave a technique of construction of S-boxes by maximal cyclic subgroup G_s of the group of units in Galois ring extension $GR(2^2, 2)$ and $GR(2^2, 2^2)$. These S-boxes increase the intricacy of image encryption. Further Shah et al., [91] presents the methodology to obtain maximal cyclic subgroups of the groups of units of finite Galois rings $GR(2^k, h)$. In this chapter, initially, we extend the concepts of soft ideals in a soft ring to soft irreducible ideals, soft prime ideals, soft maximal ideals, soft primary ideals and soft radical ideals. Ultimately the primary decomposition of soft rings and soft modules is proven. Furthermore, the ascending and descending chain conditions on soft ideals and soft sub-modules of soft rings and soft modules are presented. Accordingly, we are enabled to cultivate the notions of soft Noetherian rings and soft Noetherian modules. Next, we had constructed some examples of soft primary ideal and sub-module using the defined soft Galois rings and soft modules, respectively. By constructing a soft $\mathbb{Z}_{2^k}$-module over Galois ring $(GR\,(2^3, 8))$ and the soft primary decomposition of soft $\mathbb{Z}_{2^k}$-sub-modules. This theory has been extended to the soft group to form soft subgroups and then S-boxes has been constructed over elements of the soft subgroup. This process gives rise to two S-boxes of 4×4 bit S-box has been deal in this paper and 8×8 bits S-box. The optimal S-box is chosen by using the fuzzy bipolar soft set decision making algorithm given in [75]. We define a method of membership and non-membership functions for each parameter. By employing the decision-making algorithm, we choose the best S-box.

7.1 Soft prime ideal, soft maximal ideal, soft primary ideal, soft radical ideal

The notion of soft ring and soft ideal are defined by [2]. Here we defined the concept of soft prime ideal, soft maximal ideal, soft primary ideal, soft radical and further the notion of primary decomposition soft rings and its operation are defined.

Definition 7.1.1. *Let (F, A) be a soft ring over the ring R. A non-null soft set (γ, I) over R is called soft prime ideal of (F, A), which will be denoted by $(\gamma, I) \rhd^p (F, A)$ if it satisfies the following conditions:*

(a) $I \subset A$.

(b) $\gamma(x)$ is an ideal of $F(x)$ $\forall$ $x \in Supp(\gamma, I)$.

(c) For $F(a)$, $F(b) \in (F, A)$, $F(a) \cdot F(b) \in (\gamma, I) \Rightarrow$ either $F(a) \in (\gamma, I)$ or $F(b) \in (\gamma, I)$.

Definition 7.1.2. *Let (F, A) be a soft ring over a ring R. A non-null soft set (γ, I) over the ring R is called soft maximal ideal of (F, A) which will be denoted by $(\gamma, I) \rhd^m (F, A)$ if it satisfies the following conditions;*

(a) $I \subset A$.

(b) $\gamma(x)$ is maximal ideal of $F(x)$ $\forall$ $x \in Supp(\gamma, I)$.

Definition 7.1.3. *Let (F, A) be a soft ring over the ring R. A non-null soft set (γ, I) over R is called soft primary ideal of (F, A), which will be denoted by $(\gamma, I) \rhd^{p'} (F, A)$ if it satisfies the following conditions:*

(a) $I \subset A$.

(b) $\gamma(x)$ is an ideal of $F(x)$ for all $x \in Supp(\gamma, I)$.

(c) $\forall$ $F(a)$, $F(b) \in (F, A)$, $F(a) \cdot F(b) \in (\gamma, I) \Rightarrow$ either $F(a) \in (\gamma, I)$ or $(F(b))^n \in (\gamma, I)$, for some $n \in \mathbb{Z}^+$.

Definition 7.1.4. *Let* (γ, I) *be a soft ideal of* (F, A) *over the ring* R*. Then radical of the soft ideal* (γ, I) *is denoted by* $rad((\gamma, I))$ *and is defined as*

$$rad((\gamma, I)) = \{F(a) \in (F, A) : (F(a))^n \in (\gamma, I)\}.$$

Proposition 7.1.5. *The radical of soft primary ideal is soft prime ideal.*

7.2 Primary decomposition of soft rings

We initiate in this section the notion of primary decomposition of soft rings and establish some relevant results. Furthermore, ascending and descending chain conditions on a soft ring are investigated, which are used to define the notion of soft Notherian rings.

Definition 7.2.1. *A soft ring* $(F,\ A)$ *over* R *is said to have a primary decomposition (resp. a Laskerian soft ring) if each soft ideal of* $(F,\ A)$ *has a primary decomposition (resp. finite primary decomposition).*

Definition 7.2.2. *A primary decomposition of a soft ring* (F, A) *is said to be reduced or irredundant if* $(\gamma, I) = \Cap_{i\in\mathbb{N}} (\gamma_i, I_i)$, *where* (γ_i, I_i) *are soft primary ideals,*

(a) $rad\ ((\gamma_i, I_i)) \neq rad\big((\gamma_j, I_j)\big)$, *for all* $i,\ j \in \mathbb{N},\ i \neq j$;

(b) $(\gamma_i, I_i) \not\supseteq \Cap_{j\in\mathbb{N}\setminus i} \left(\gamma_j, I_j\right)$, *for all* $i,\ j \in \mathbb{N}$.

Definition 7.2.3. *Let* $(F,\ A)$ *be a soft ring over* R *and* (γ, I) *be soft ideal of* (F, A) *then* (γ, I) *is soft irreducible if* $(\gamma, I) = (\gamma_1, I_1) \Cap (\gamma_2, I_2)$, *where* (γ_1, I_1) *and* (γ_2, I_2) *be a soft ideals of* (F, A), *and either* $(\gamma,\ I) = (\gamma_1, I_1)$ *or* $(\gamma, I) = (\gamma_2, I_2)$.

Definition 7.2.4. *Let* (γ, I) *and* (γ, J) *be two soft ideals of a soft ring* (F, A) *then* (γ, I) *is said to be* (γ, J)*-primary if:*

(a) (γ, I) *is soft primary.*

(b) $rad\left((\gamma, I)\right) = (\gamma, J)$.

Definition 7.2.5. *Let* $(\gamma_1,\ I_1)$ *and* $(\gamma_2,\ I_2)$ *be two soft ideals of* $(F,\ A)$ *over* R. *Denote soft ideal quotient by the set* $((\gamma_1, I_1) : (\gamma_2, I_2)) = \{F(a) : F(a)(\gamma_2, I_2) \subseteq (\gamma_1, I_1)\}$, *where the product* $F(a) \cdot \gamma_2(b) \in (\gamma_1, I_1)$ *for all* $\gamma_2(b) \in (\gamma_2, I_2)$, *implies that* $((\gamma_1, I_1) : (\gamma_2, I_2))$ *is a soft ideal of* (F, A).

Theorem 7.2.6. *Let* $(F,\ A)$ *be a soft ring over* R *and* $(\gamma_i,\ I_i)_{i\in\mathbb{N}}$ *be soft ideals of* $(F,\ A)$. *The following conditions are equivalent:*

1. *Every ascending chain of soft ideals is stationary, i.e.*

   (a) *The set of subsets* I_i *of a given set* A *are ordered by inclusion.*

   (b) $\gamma_1(x) \subseteq \gamma_2(x) \subseteq \gamma_3(x) \subseteq \cdots$ *such that* $\gamma_n(x) = \gamma_{n+1}(x)$, *for all* $x \in Supp(\cap_{i\in\mathbb{N}}(\gamma_i, I_i))$

   and $(\gamma_1, I_1) \subseteq (\gamma_2, I_2) \subseteq (\gamma_3, I_3) \subseteq \cdots \subseteq (\gamma_n, I_n) \subseteq (F,\ A)$.

2. *Every non empty set of ideals in* (F, A) *has a maximal element.*

Proof. Let S be a set of proper soft ideals in a soft ring (F, A) over a ring R. (a) implies that every ascending chain of soft ideal in S has an upper bound in S. By Zorn's lemma, S contains a soft maximal element. The soft maximal element is a proper soft ideal of (F, A), that is, soft maximal ideal for inclusion among all proper soft ideals.

Conversely, assume that $(\gamma_1,\ I_1) \subseteq (\gamma_2,\ I_2) \subseteq (\gamma_3,\ I_3) \subseteq \cdots$ be an ascending chain of soft ideals. Suppose $(\gamma, I) = \tilde{\cup}_{i\in\mathbb{N}}(\gamma_i, I_i)$, S is a set of soft ideals contained in (γ, I). Therefore, it contains a maximal element. For some $n \in \mathbb{N}$, each (γ_i, I_i) belongs to $(\gamma_n,\ I_n)$.

$$(\gamma_n,\ I_n) = \left(\gamma_{n+1},\ I_{n+1}\right) = \left(\gamma_{n+2},\ I_{n+2}\right) = \cdots = (\gamma,\ I).$$

■

Remark 7.2.7. Let $(F,\ A)$ be a soft ring over a ring R called soft Noetherian and which $(\gamma_i, I_i)_{i\in\mathbb{N}}$ be soft ideals of (F, A).

1.If every ascending chain condition on soft ideals is stationary, that is,

(a) $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ there exist a positive integer n such that $I_n = I_{n+1}$.

(b) $\gamma_1(x) \subseteq \gamma_2(x) \subseteq \gamma_3(x) \subseteq \cdots$ such that $\gamma_n(x) = \gamma_{n+1}(x)$, for all $x \in Supp\left(\cap_{i\in\mathbb{N}}(\gamma_i, I_i)\right)$

and it can be represented as $(\gamma_1, I_1) \subseteq (\gamma_2, I_2) \subseteq (\gamma_3, I_3) \subseteq \cdots \subseteq (\gamma_n,\ I_n) \subseteq (F,\ A)$.

2. Every non-empty set of soft ideals of $(F,\ A)$ is contained in soft maximal ideal.

Example 7.2.8. Let (γ_1, I_1) and (γ_2, I_2) be soft ideals of a soft ring (F, A) over a ring R. Consider the ring $R = A = \mathbb{Z}$, and $I_1 = I_2 = I_3 = \mathbb{Z} - \{0\}$. Let us consider the set-valued function $F : A \longrightarrow P(R)$ given by $F(x) = x\mathbb{Z}$. (F, A) is a soft ring over R. Now consider the functions $\gamma_i : I_i \rightarrow P(R)$, for $1 \leq i \leq 3$, given by $\gamma_1(x) = 8x\mathbb{Z}$, $\gamma_2(x) = 4x\mathbb{Z}$, $\gamma_3(x) = 2x\mathbb{Z}$ where $x \in Supp\left(\gamma_i,\ I_i\right)$.Thus $(\gamma_1,\ I_1) \subseteq (\gamma_2,\ I_2) \subseteq (\gamma_3,\ I_3) \subseteq (F, A)$ and $(\gamma_3,\ I_3)$ is a soft maximal ideal of (F, A).

Remark 7.2.9. *Ascending chain of soft ideals need not to be stationary. For instance consider the ring* $R = \mathbb{Z} + X\mathbb{Q}\left[X\right]$, $A = \mathbb{Q}$ *and* $I_i = \frac{1}{2^i}\mathbb{Z}$. *Consider the set valued function* $F : A \longrightarrow P(R)$ *such that* $F\left(a\right) = \left\{\left(\frac{X}{a}\right),\ a \in Supp\left(F,\ A\right)\right\}$. *Consider the function* $\gamma_i : I_i \rightarrow P(R)$ *given* $\gamma_i(a) = \left\{\left(\frac{X}{a}\right),\ a \in Supp\left(\gamma_i,\ I_i\right)\right\}$. *This gives* $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ *and* $\gamma_1(x) \subseteq \gamma_2(x) \subseteq \gamma_3(x) \subseteq \cdots$. *So,* $(\gamma_1,\ I_1) \subseteq (\gamma_2,\ I_2) \subseteq (\gamma_3,\ I_3) \subseteq (\gamma_4,\ I_4) \subseteq \cdots$. *Hence, we get a non-terminating* *ascending chain of soft ideals. This is a non Noetherian ring. Here the soft maximal ideal of the soft ring is* $(F,\ A)$ *itself.*

Definition 7.2.10. *Let* (F, A) *be a soft ring over a ring* R *and* (γ, I) *be soft prime ideal of* (F, A). (γ, I) *is minimal soft prime ideal if it is minimal in* $Spec\,(F, A)$ *with respect to inclusion.*

Remark 7.2.11. *The following conditions hold for conductor ideals.*
(a) $(\gamma, I) \subseteq ((\gamma, I) : (\zeta, J))$.
(b) $((\gamma, I) : (\zeta, J)) \odot_{\cap} (\zeta, J) \subseteq (\gamma, I)$.
(c) $((\gamma, I) : (\zeta, J)) : (\eta, L) = ((\gamma, I) : (\zeta, J)) \odot_{\cup} (\eta, L)$.
(d) $((\gamma, I) : (\zeta, J)) = \Cap_{n=1}^{\infty} ((\gamma_n, I_n) : (\zeta, J))$ *where* $(\gamma, I) = \Cap_{n=1}^{\infty} (\gamma_n, I_n)$.
(e) $((\gamma, I) : (\zeta, J)) = \Cap_{n=1}^{\infty} ((\gamma, I) : (\zeta_n, J_n))$ *where* $(\zeta, J) = \oplus_{\cap} (\zeta_n, J_n)$ *for* $n \in \mathbb{N}$.

Theorem 7.2.12. *Let* $(F,\ A)$ *be a soft Noetherian ring over* R*. Each soft ideal of* $(\gamma,\ I)$ *of* $(F,\ A)$ *over* R *is finite intersection of soft irreducible ideals.*

Proof. Suppose, on contrary, that the soft ideal $(\gamma,\ I)$ can't be written as a finite intersection of soft irreducible ideals. Set $\tilde{N} = \{(\gamma,\ I) \mid (\gamma,\ I)$ cannot be written as finite product of soft irreducible ideals$\}$. Since $(F,\ A)$ is a soft Noetherian, $\exists$ a maximal ideal $\left(\gamma',\ I'\right) \in \tilde{N}$, such that $\left(\gamma',\ I'\right)$ can't be written as a finite product of soft irreducible ideals.

Also $\left(\gamma',\ I'\right)$ is not a soft irreducible ideal, there exists $(\gamma_1,\ I_1)$ and $(\gamma_2,\ I_2)$ such that the restricted intersection of $(\gamma_1,\ I_1) \Cap (\gamma_2,\ I_2) = \left(\gamma',\ I'\right)$ implies either $\left(\gamma',\ I'\right) \subseteq (\gamma_1,\ I_1)$ or $\left(\gamma',\ I'\right) \subseteq (\gamma_2,\ I_2)$. The maximality of $\left(\gamma',\ I'\right)$ implies that $(\gamma_1,\ I_1) \notin \tilde{N}$ and $(\gamma_2,\ I_2) \notin \tilde{N}$. This implies $(\gamma_1,\ I_1)$ and $(\gamma_2,\ I_2)$ can be written as the finite intersection of soft irreducible ideals i.e. $\left(\gamma',\ I'\right)$ can be written as the finite intersection of soft irreducible ideals which is a contradiction. Hence, proved. ∎

Theorem 7.2.13. *Let $(F,\ A)$ be a soft noetherian ring over a ring R. Every soft irreducible ideal of $(F,\ A)$ is a soft primary ideal of $(F,\ A)$.*

Proof. Let (γ, I) be a soft irreducible ideal over (F, A), then for $F(a)$, $F(b) \in (F, A)$, such that $F(a)F(b) \in (\gamma, I)$ but $F(b) \notin (\gamma, I)$. Moreover,
$((\gamma, I) : F(a)) \subseteq ((\gamma, I) : F(a)^2) \subseteq ((\gamma, I) : F(a)^3 \subseteq \cdots$ is an ascending chain of soft ideals of $(F,\ A)$ over R. Since $(F,\ A)$ is Noetherian, there exist $n \in \mathbb{N}$, such that
$((\gamma, I) : F(a)^n) = ((\gamma, I) : F(a)^{n+1})$, for all $n \in \mathbb{N}$. We have to show that

$$(\gamma, I) = ((\gamma, I) \oplus_{\cap} F(a)^n \cdot (F,\ A)) \Cap ((\gamma, I) \oplus_{\cap} F(b) \cdot (F,\ A)),\ for\ all\ n \in N.$$

Consider an element $\gamma(a) \in (\gamma, I)$, $\gamma(a) \subseteq \gamma(a) + \ F(a)^n F(c)$ and

$$\gamma(a) \subseteq \gamma(a) + F(b)^n F(d);\ F(c), F(d) \in (F,\ A).$$

This implies

$$(\gamma, I) \subseteq ((\gamma, I) \oplus_{\cap} F(a)^n \cdot (F,\ A)) \Cap ((\gamma, I) \oplus_{\cap} F(b) \cdot (F, A)).$$

Conversely, assume that

$$\gamma(c) \in ((\gamma, I) \oplus_{\cap} F(a)^n \cdot (F, A)) \Cap ((\gamma, I) \oplus_{\cap} F(b) \cdot (F, A))$$

and

$$\gamma(c) = \gamma(b_i) + F(a)^n F(c) = \gamma(b_j) + F(b)F(d).$$

For $c \in Supp(\gamma, I)$

$$\gamma(c) \cdot F(a) = \gamma(b_i) \cdot F(a) + F(a)^{n+1} F(c) = \gamma(b_j) \cdot F(a) + F(a)F(b)F(d).$$

Since $F(a)F(b) \in (\gamma, I)$, so, $F(a)^{n+1}F(c) \in (\gamma, I)$. Also, $F(c) \in ((\gamma, I) \oplus_{\cap} F(a)^n \cdot (F, A))$ and $\gamma(c) \in (\gamma, I)$, therefore,

$$((\gamma, I) \oplus_{\cap} F(a)^n \cdot (F, A)) \Cap ((\gamma, I) \oplus_{\cap} F(b) \cdot (F, A)) \subseteq (\gamma, I).$$

Since (γ, I) is irreducible and $(\gamma, I) \subset (\gamma, I) \oplus_{\cap} F(b) \cdot (F, A)$, due to the fact that $F(b) \notin (\gamma, I)$. So,

$$(\gamma, I) = ((\gamma, I) \oplus_{\cap} F(a)^n \cdot (F, A)).$$

This proves that $F(a)^n \in (\gamma, I)$ is primary. ■

Theorem 7.2.14. *Every soft noetherian ring is a soft Laskerian ring.*

Proof. Follows directly from Theorems 7.2.12 and 7.2.13. ■

Theorem 7.2.15. *If (γ_1, I_1) and (γ_2, I_2) be primary decomposition ideals of a soft ring (F, A) over a ring R. $(\gamma_1, I_1) \oplus_{\cup} (\gamma_2, I_2)$ is a primary decomposition soft ideal of (F, A) if $I_1 \cap I_2 = \Phi$.*

Proof. Obvious. ■

Theorem 7.2.16. *Let (γ_1, I_1) and (γ_2, I_2) be primary decomposition ideals of a soft ring (F, A) over R. $(\gamma_1, I_1)\widetilde{\wedge}(\gamma_2, I_2)$ need not to be a primary decomposition ideal of (F, A).*

Proof. Obvious. ■

Remark 7.2.17. *Let (γ_1, I_1) and (γ_2, I_2) be primary decomposition of soft ideals of a soft ring (F, A) over R. Then*

(a) $(\gamma_1, I_1) \oplus_{\cap} (\gamma_2, I_2)$ needs not be a primary decomposition soft ideal of (F, A).

(b) $(\gamma_1, I_1) \odot_{\cap} (\gamma_2, I_2)$ needs not be a primary decomposition soft ideal of (F, A).

(c) $(\gamma_1, I_1) \Cap (\gamma_2, I_2)$ needs not be a primary decomposition soft ideal of (F, A).

Theorem 7.2.18. *Every soft ideal of a soft noetherian ring contains the power of its soft radical.*

Proof. Let (γ, I) be a soft ideal of a soft ring $(F,\ A)$. Take $F(a_i) \in\ rad(\gamma, I)$, where $a_i \in Supp(F,\ A)$. Then $F(a_i)^{n_i} \in (\gamma, I)$, for some $n_i \in \mathbb{N}$. Put $n = 1 + \sum(n_i - 1)$, then $(\gamma, I)^n$ is generated by $F(a_1)^{m_1} \cdot F(a_2)^{m_2} \cdot F(a_3)^{m_3} \cdot \cdots \cdot F(a_i)^{m_i}$ where $\sum m_i = n$. At least one of $m_i \geq n_i$ making each $F(a_i)^{m_i}$ an element of (γ, I). Hence $(\gamma, I)^n \subseteq (\gamma, I)$. ∎

Theorem 7.2.19. *Restricted product of two soft ideals is contained in their restricted intersection.*

Proof. Let (γ_1, I_1) and (γ_2, I_2) be two soft ideals of soft ring (F, A) over a ring R. Take $\gamma_1(a)\gamma_2(a) \in (\gamma_1, I_1) \odot_{\cap} (\gamma_2, I_2)$ where $\gamma_1(a) \in (\gamma_1, I_1)$, $\gamma_2(a) \in (\gamma_2, I_2)$ and $a \in Supp((\gamma_1, I_1) \odot_{\cap} (\gamma_2, I_2))$. Since $a \in I_1 \cap I_2$, hence $\gamma_1(a)\gamma_2(a) \in (\gamma_1, I_1)$ and $\gamma_1(a)\gamma_2(a) \in (\gamma_2, I_2)$. Thus $\gamma_1(a)\gamma_2(a) \in (\gamma_1, I_1) \Cap (\gamma_2, I_2)$.
Hence,

$$(\gamma_1, I_1) \odot_{\cap} (\gamma_2, I_2) \subseteq (\gamma_1, I_1) \Cap (\gamma_2, I_2).$$

∎

Proposition 7.2.20. *Let (γ, I) be a soft prime ideal and $(\gamma_1, I_1),\ (\gamma_2, I_2), \cdots, (\gamma_n, I_n)$ any n soft ideals of (F, A). The following statements are equivalent:*
(a) (γ, I) contains (γ_j, I_j), for some j,
(b) $\Cap_{i=1}^{n}(\gamma_i, I_i) \subseteq (\gamma, I)$,
(c) $\odot_{\cap}(\gamma_i, I_i) \subseteq (\gamma, I)$ for $1 \leq i \leq n$.

Proof. Obvious. ∎

Theorem 7.2.21. *Let (γ, I) and (σ, P) be soft ideals of soft ring (F, A) over a ring R. (γ, I) is a soft primary for (σ, P) if and only if*

(a) $(\gamma, I) \subseteq (\sigma, P) \subseteq rad\ \ (\gamma, I)$

(b) If $F(a) F(b) \in (\gamma, I)$ and $F(a) \notin (\gamma, I)$, then $F(b) \in (\sigma, P)$.

Proof. Suppose (a) and (b) holds. If $F(a) F(b) \in (\gamma, I)$ and $F(a) \notin (\gamma, I)$, then $F(b) \in (\sigma, P) \subseteq rad\ \ (\gamma, I)$. Thus $F(b)^n \in (\gamma, I)$ for some $n > 0$. Therefore, (γ, I) is soft primary. To show (γ, I) is soft primary for (σ, P). We need only to show that $(\sigma, P) = rad\ \ (\gamma, I)$. By (a), $(\sigma, P) \subseteq rad\,(\gamma, I)$. If $F(b) \in rad\ \ (\gamma, I)$, then for some positive integer n such that $F(b)^n \in (\gamma, I)$. If $n = 1$, then $F(b) \in (\gamma, I) \subseteq (\sigma, P)$. If $n > 1$, then $F(b)^{n-1} F(b) \in (\gamma, I)$ with $F(b)^{n-1} \notin (\gamma, I)$ by the minimality of n, by (b), $F(b) \in (\sigma, P)$. Thus $F(b) \in rad\,(\gamma, I)$ gives $F(b) \in (\sigma, P)$. The converse implication is obvious. ■

Theorem 7.2.22. *If $(\gamma,\ I), (\gamma_1,\ I_1), (\gamma_2,\ I_2), \cdots, (\gamma_n,\ I_n)$, are soft ideals of a soft ring (F, A). Then,*

(a) $rad(rad\,(\gamma,\ I)) = rad(\gamma,\ I)$

(b) $rad((\gamma_1,\ I_1) \odot_\cap (\gamma_2,\ I_2) \odot_\cap \cdots \odot_\cap (\gamma_n,\ I_n)) = \Cap_{i=1}^{n} rad\,(\gamma_i,\ I_i)$.

Proof. (a) Let $F(a) \in rad(rad\,(\gamma,\ I))$. Then $F(a)^n \in rad\,(\gamma, I)$. Hence, $(F(a)^n)^m \in (\gamma,\ I)$ for $n, m \in \mathbb{N}$. Therefore $F(a) \in rad\,(\gamma, I)$.

Conversely Let $F(a) \in rad\,(\gamma, I)$. This implies $F(a)^1 \in rad\,(\gamma, I)$. Hence $F(a) \in rad(rad\,(\gamma, I))$.

(b) Let $F(a) \in \Cap_{i=1}^{n} Rad\,(\gamma_i, I_i)$. Then there are $m_1, m_2, \cdots, m_n > 0$ such that $F(a)^{m_i} \in (\gamma_i,\ I_i)$, for each j. If $m = m_1 + m_2 + \cdots + m_n$, then

$$F(a) = F(a)^{m_1} F(a)^{m_2} \cdots F(a)^{m_n} \in (\gamma_1, I_1) \odot_\cap (\gamma_2, I_2) \odot_\cap \cdots \odot_\cap (\gamma_n, I_n).$$

Hence

$$\Cap_{i=1}^{n} rad\,(\gamma_i, I_i) \subseteq rad((\gamma_1, I_1) \odot_\cap (\gamma_2, I_2) \odot_\cap \cdots \odot_\cap (\gamma_n, I_n)).$$

Since

$$(\gamma_1, I_1) \odot_\cap (\gamma_2, I_2) \odot_\cap \cdots \odot_\cap (\gamma_n, I_n)) \subseteq \Cap_{i=1}^{n} (\gamma_i, I_i)\,,$$

we have

$$rad((\gamma_1,\ I_1) \odot_\cap (\gamma_2,\ I_2) \odot_\cap \cdots \odot_\cap (\gamma_n,\ I_n)) \subseteq \Cap_{i=1}^{n} rad\,(\gamma_i,\ I_i)\,.$$

■

Theorem 7.2.23. *Let (F, A) be a soft ring over a ring R. If $(\gamma_i, I_i)_{1\leq i\leq n}$ are soft primary ideals for the soft prime ideal (σ, P), then $\Cap_{i=1}^{n} (\gamma_i, I_i)$ is also a soft primary ideal belonging to (σ, P).*

Proof. Let $(\gamma, I) = \Cap_{i=1}^{n} (\gamma_i, I_i)$. According to [Theorem 7.2.22]

$$rad\,(\gamma, I) = rad \Cap_{i=1}^{n} (\gamma_i, I_i) = \Cap_{i=1}^{n} rad\,(\gamma_i, I_i) = \Cap_{i=1}^{n} (\sigma, P) = (\sigma, P)\,;$$

Using [Theorem 7.2.21], $(\gamma, I) \subseteq (\sigma, P) \subseteq rad\ \ (\gamma, I)$. If $F(a)\,F(b) \in (\gamma, I)$ and $F(a) \notin (\gamma, I)$, then $F(a)\,F(b) \in (\gamma_i, I_i)$ for some i. Since (γ_i, I_i) is (σ, P)-soft primary, $F(b) \in (\sigma, P)$. Consequently, (γ, I) itself is (σ, P)-soft primary. ■

Theorem 7.2.24. *Let (γ, I) be a soft ideal of a soft ring (F, A) over a ring R. If (γ, I) has a primary decomposition of soft rings, then (γ, I) has a reduced primary decomposition.*

Proof. Let $(\gamma, I) = (\gamma_1, I_1) \Cap (\gamma_2, I_2) \Cap \cdots \Cap (\gamma_n, I_n)$ be intersection of soft primary ideals and some (γ_i, I_i) contains
$(\gamma_1, I_1) \Cap (\gamma_2, I_2) \Cap \cdots \Cap \left(\gamma_{i-1}, I_{i-1}\right) \Cap \left(\gamma_{i+1}, I_{i+1}\right) \Cap \cdots \Cap (\gamma_n, I_n)$
so $(\gamma, I) = (\gamma_1, I_1) \Cap (\gamma_2, I_2) \Cap \cdots \Cap \left(\gamma_{i-1}, I_{i-1}\right) \Cap \left(\gamma_{i+1}, I_{i+1}\right) \Cap \cdots \Cap (\gamma_n, I_n)$ is also a primary decomposition. By eliminating the superfluous (γ_i, I_i) and reindexing we have $(\gamma, I) = (\gamma_1, I_1) \Cap (\gamma_2, I_2) \Cap \cdots \Cap (\gamma_k, I_k)$ with no (γ_i, I_i) containing the intersection of others $\left(\gamma_j, I_j\right)$. Let $(\sigma_1, P_1)\ (\sigma_2, P_2) \cdots (\sigma_h, P_h)$ be distinct prime

ideals in the set $\{rad\,(\gamma_1, I_1),\, rad\,(\gamma_2, I_2)\,, \cdots, rad\,(\gamma_k, I_k)\}$. Let $\left(\gamma_i^{'}, I_i^{'}\right)$ $(1 \leq i \leq h)$ be the intersection of all the (γ_i, I_i) that belong to the prime (σ_i, P_i). Each $\left(\gamma_i^{'}, I_i^{'}\right)$ is soft primary for (σ_i, P_i). Clearly no $\left(\gamma_i^{'}, I_i^{'}\right)$ contains the intersection of all soft primary ideals. Therefore, $(\gamma, I) = \Cap_{i=1}^{k} (\gamma_i, I_i) = \Cap_{i=1}^{h} \left(\gamma_i^{'}, I_i^{'}\right)$. Hence (γ, I) has a reduced primary decomposition of soft rings. ■

7.3 Primary decomposition of soft modules

In this section we introduce the algebraic notions such as soft noetherian module, soft primary module and primary decomposition of soft modules. Throughout this section all rings are commutative with identity and all modules are unitary.

Recall that a module M is said to be noetherian (resp. artinan) if every ascending chain (resp. descending chain) of sub-modules of M is stationary. A proper sub-module C of a R-module M is said to be a primary sub-module if $r \in R,\ b \notin M$ and $rb \in C$ this gives $r^n M \in C$ for some positive integer n. A soft set (G, B) over a $R-$module M is called a soft module if each $G\,(b)$ is a sub-module of M, for all $b \in Supp\,(G, B)$ (see [99, Definition 10]).

Definition 7.3.1. Let (G, B) be a soft module over an R-module M. It is said to be soft noetherian module, if the following conditions are equivalent,

1. Every ascending chain of soft sub-modules is stationary, that is,

(a) The set of subsets of B_i of a given set B are ordered by inclusion.

$B_1 \subseteq B_2 \subseteq B_3 \subseteq \cdots$ such that $B_n = B_N$, for $n \geq N$.

(b) $(G_1, B_1) \subseteq (G_2, B_2) \subseteq (G_3, B_3) \subseteq \cdots$.. there exist a positive integer n such that $(G_n, B_n) = (G_N, B_N)$, for $n \geq N$ and chain takes form

$(G_1, B_1) \subseteq (G_2, B_2) \subseteq (G_3, B_3) \subseteq \cdots \subseteq (G_n, B_n)$.

2.Every non-empty set of soft sub-modules of (G, B) is contained in soft maximal sub-module.

Definition 7.3.2. A soft module (F, A) satisfies the maximal condition [resp. minimum condition] on soft sub-modules if every non-empty set of soft sub-modules of (F, A) contains a maximal [resp. minimal] element (with respect to set theoretic inclusion).

Definition 7.3.3. Let (F, A) be a soft ring over a ring R and (G, B) be a soft module over an R-module M.If (γ, I) is a soft prime ideal of (F, A), $(\gamma, I) \odot (G, B) = \{\gamma(a) G(b) : a \in Supp(\gamma, I), \ b \in Supp(G, B)\}$ is a soft sub-module of (G, B).

Example 7.3.4. For $R = M = \mathbb{Z}$, $A = B = \mathbb{N}$ and $I = 2\mathbb{N}$, let us consider the set value function $F : A \longrightarrow P(R)$ given by $F(x) = \{x\mathbb{Z} : x \in A\}$. (F, A) is a soft ring over R. Also consider an R-module M and $G : B \longrightarrow P(M)$ given by $G(b) = M$, for all $b \in B$. (G, B) be a soft module over an R-module M. Now again consider $\gamma : I \longrightarrow P(R)$ given by $\gamma(x) = 3x\mathbb{Z}$. (γ, I) is a soft ideal of (F, A). As $(\gamma, I) \odot (G, B) = 3x\mathbb{Z} \cdot \mathbb{Z} = 3x\mathbb{Z}$, for $x \in Supp(\gamma, I)$ is a soft sub-module of (G, B).

Theorem 7.3.5. *A soft module (F, A) satisfies the ascending [resp. descending] chain condition on soft sub-modules if and only if (F, A) satisfies the maximal [resp. minimal] condition on soft sub-modules.*

Proof. Suppose (F, A) satisfies the minimal condition on soft sub-modules and

$$(G_1, B_1) \tilde{\supseteq} (G_2, B_2) \tilde{\supseteq} (G_3, B_3) \tilde{\supseteq} \cdots$$

is a chain of soft sub-modules. Then the set $\{(G_i, B_i) \,|\, i \geq 1\}$ has a minimal element, say (G_n, B_n). Consequently, for $i \geq n$ we have $(G_n, B_n) \tilde{\supseteq} (G_i, B_i)$ by hypothesis and $(G_n, B_n) \tilde{\subseteq} (G_i, B_i)$ by minimality. Hence $(G_n, B_n) = (G_i, B_i)$ for each $i \geq n$. Therefore, (F, A) satisfies the descending chain condition. Conversely suppose (F, A) satisfies the descending chain condition and S is a non-empty set of soft sub-modules of (F, A). Then there exists $(G_o, B_o) \in S$. If S has no minimal element, then for each soft sub-module (G, B) in S there exists at least one soft sub-module $\left(G', B'\right)$ in S such that $(G, B) \tilde{\supseteq} \left(G', B'\right)$. For each (G, B) in S, choose one such $\left(G', B'\right)$. This choice then defines a function $f : S \longrightarrow S$ by $B \longmapsto B'$. There is a function $\varphi : \mathbb{N} \longrightarrow S$ such that $\varphi(0) = (G_o, B_o)$ and $\varphi(n+1) = f(\varphi(n)) = \varphi\left(n'\right)$. Thus if $(G_n, B_n) \in S$ denotes $\varphi(n)$, then there is a sequence $(G_o, B_o) \tilde{\supseteq} (G_1, B_1) \tilde{\supseteq} (G_2, B_2) \tilde{\supseteq} (G_3, B_3) \tilde{\supseteq} \cdots$ This contradicts the descending chain condition. Therefore, S must have a minimal element. Hence (F, A) satisfies minimum condition.

The proof for ascending chain condition and maximum conditions is analogous. ■

Definition 7.3.6. Let (F, A) be a soft ring over a ring R and (G, B) be a soft module over an R-module M. A non-null soft subset of (H, C) of soft module (G, B) is said to be soft primary sub-module, if it satisfies the following conditions:

(a) $C \subseteq B$

(b) $H(c)$ is sub-module of $G(c)$ for all $c \in Supp(H, C)$

(c) $F(a) \in (F, A)$ such that $F(a)^n G(b) \in (H, C)$ for all $G(b) \in (G, B)$ and $n \in \mathbb{N}$.

Theorem 7.3.7. *Let (F, A) be a soft ring over a ring R and (G, B) be a soft module over an R-module M. (H, C) be a soft primary sub-module (G, B) such that, $(\xi, Q) = \{F(a) \in (F, A) : F(a)(G, B) \subseteq (H, C)\}$ is soft primary ideal in (F, A).*

Proof. Let $F(a_1) F(a_2) \in (\xi, Q)$ and $F(a_2) \notin (\xi, Q)$, then $F(a_2)(G, B) \notin (H, C)$ for all $b \in Supp(G, B)$. Consequently, there exist $G(b) \in (G, b)$, $F(a_2) G(b) \notin (H, C)$ but $F(a_1)(F(a_2) G(b)) \in (H, C)$. Since (H, C) is a soft primary sub-module $F(a_1)(G, B) \subseteq (H, C)$ for some n; that is, $F(a_1)^n \in (\xi, Q)$. Therefore, (ξ, Q) is soft primary. ■

Example 7.3.8. For $R = M = \mathbb{Z}$, $A = B = \mathbb{N}$ and $C = 3\mathbb{N}$, let us consider the set value function $F : A \longrightarrow P(R)$ given by $F(x) = \{x\mathbb{Z} : x \in A\}$ then (F, A) is a soft ring over R. Also consider a R-module M and $G : B \longrightarrow P(M)$ given by $G(b) = M$ for all $b \in B$. (G, B) be a soft module over a R-module M. Now again consider $H : C \longrightarrow P(M)$ given by $H(m) = 2m\mathbb{Z}$ is soft sub-module of (G, B). It is observe that $(\xi, Q) = \{F(2),\ F(4), \cdots, F(2n) : for\ n \in \mathbb{N}\}$ is a soft primary sub-module of (G, B).

Definition 7.3.9. Let (F, A) be a soft ring over a ring R and (G, B) be a soft module over an R-module M. A soft primary sub-module(H, C) of a soft module (G, B), is said to be a (σ, P)-soft primary sub-module of (G, B) if
$(\sigma, P) = rad\ \ (\xi, Q) = \{F(a) \in (F, A) : F(a)^n (G, B) \subseteq (H, C)\ \ for\ n > 0\}$ where $(\xi, Q) = \{F(a) \in (F, A) : F(a)(G, B) \subseteq (H, C)\}$ is soft primary ideal in (F, A).

Definition 7.3.10. Let (F, A) be soft ring over a ring R and (G, B) be soft module over an R-module M. A soft sub-module (H, C) of (G, B) has a primary decomposition if $(H, C) = \Cap_{i=1}^{n} (H_i, C_i)$ with each (H_i, C_i) is a (σ_i, P_i)-soft primary sub-module of (G, B), for some soft prime ideal (σ_i, P_i) of (F, A).

If no $(H_i, C_i) \subseteq \Cap_{j=1}^{n} (H_j, C_j)$ for $i \neq j$ and if the soft ideals (σ_i, P_i) are all distinct then the soft primary decomposition is said to be reduced primary decomposition.

Theorem 7.3.11. *Let (F, A) be a soft ring over a ring R and (G, B) be a soft module over an R-module M. If a soft sub-module (H, C) of (G, B) has a primary decomposition, then (H, C) has a reduced primary decomposition.*

Proof. Obvious ∎

Theorem 7.3.12. *Let (F, A) be a soft ring over a ring R and (G, B) be a soft module over an R-module M satisfying ascending chain condition on soft* *sub-modules. Every soft sub-module (H, C) of (G, B) has a reduced soft primary decomposition.*

Proof. Let S be the set of all soft sub-modules of (G, B) that doesn't have a primary decomposition. Clearly no soft primary sub-module in S. We show S is in fact empty. Assume that S is nonempty, then S contains a soft maximal element say (H, C). Since (H, C) is not soft primary, there exist $F(a) \in (F, A)$ and $G(b) \in (G, B) \setminus (H, C)$ such that $F(a) G(b) \in (H, C)$ but $F(a)^n G(b) \notin (H, C)$ for all $n > 0$. Consider $(G_n, B_n) = \{G(b) \in (G, B) : F(a)^n G(b) \in (H, C)\}$. Then each (G_n, B_n) is soft sub-module of (G, B) and $(G_1, B_1) \subseteq (G_2, B_2) \subseteq \cdots$ By hypothesis there exists $k > 0$ such that $(G_i, B_i) = (G_k, B_k)$ for $i \geq k$. Let $(K, D) = \{G(b) : G(b) = F(a)^k G(b') + H(c) : b' \in Supp(G, B),\ c \in Supp(H, C)\}$ be soft sub-module of (G, B). Clearly $(H, C) \subseteq (G_k, B_k) \Cap (K, D)$. Conversely, if $G(b) \in (G_k, B_k) \Cap (K, D)$ then $G(b) = G_k(b') + K(d)$ and $F(a)^k G(b) = F(a)^k G_k(b') + F(a)^k K(d) \in (H, C)$. Therefore, $(H, C) = (G_k, B_k) \Cap (K, D)$. Now by maximality of (H, C) in S, (G_k, B_k) and (K, D) must have primary decomposition. Thus S is empty and every soft sub-module has a primary decomposition. ■

Lemma 7.3.13. *Let (F, A) be a soft ring over a ring R and (G, B) be a soft module over an R-module M. Let (γ, I) be a soft prime ideal of (F, A) and (H, C) is (γ, I)-soft primary sub-module of soft noetherian module (G, B), then there exist a smallest integer m such that $(\gamma, I)^m \odot (G, B) \subset (H, C)$.*

Proof. Recall that there exist primary ideal (σ, Q) such that $rad(\sigma, Q) = (\gamma, I)$, for some soft primary sub-module (H, C). Suppose $\gamma(a) \in (\gamma, I)$ such that $\gamma(a)^{n_i} G(b) \in (H, C)$, for all $b \in Supp(G, B)$ and $n_i \geq 1$. Take $m = \max(n_1, n_2, \cdots, n_i)$, hence for all $a \in Supp(\gamma, I)$ we get

$\gamma(a)^m G(b) \in (H,C)$, for all $b \in Supp(G,B)$. Thus $(\gamma,I)^m \odot (G,B) \subset (H,C)$. ∎

Now we present the Krull intersection theorem in soft sense.

Theorem 7.3.14. *Let (F,A) be a soft ring over a ring R, (γ,I) be a soft ideal of (F,A) and (G,B) be a soft module over a $R-$module M. If $(H,C) = \Cap_{n=1}^{\infty} (\gamma,I)^n \odot (G,B)$, then $(\gamma,I) \odot (H,C) = (H,C)$.*

Proof. If $(\gamma,I) \odot (H,C) = (G,B)$, then $(\gamma,I) \odot (H,C) \subseteq (H,C)$.
Hence $(H,C) = (G,B)$.

If $(\gamma,I) \odot (H,C) \neq (G,B)$, then by lemma 7.3.13 $(\gamma,I) \odot (H,C)$ has a soft primary decomposition, that is, $(\gamma,I) \odot_{\cap} (H,C) = \Cap_{i=1}^{n} (H_i,C_i)$,where each (H_i,C_i) is (σ_i,P_i) soft primary sub-module of (G,B), for some soft prime ideal (σ_i,P_i) of (F,A). Since $(\gamma,I) \odot (H,C) \subseteq (H,C)$, we need to show that $(H,C) \subset (\gamma,I) \odot (H,C)$ for every i.

Let i $(1 \leq i \leq n)$ be fixed. Suppose that $(\gamma,I) \subset (\sigma_i,P_i)$. By Lemma 7.3.13, there is an integer m such that, $(\sigma_i,P_i)^m \odot (G,B) \subset (H_i,C_i)$. Hence

$$(H,C) = \Cap_{n=1}^{\infty} (\gamma,I)^n \odot (G,B) \subset (\gamma,I)^m \odot (G,B) \subset (\sigma_i,P_i)^m \odot (G,B) \subset (H_i,C_i).$$

If $(H,C) \subset (H_i,C_i)$, then there exists $c \in Supp(H,C)$ and $a \in Supp(\gamma,I)$ such that $\gamma(a) H(c) \in (\gamma,I) \odot (H,C) \subset (H_i,C_i)$ and (H_i,C_i) is soft primary, $\gamma(a)(G,B) \subset (H_i,C_i)$ for some $n > 0$. Thus $(H,C) \subset (H_i,C_i)$, this gives,

$$(H,C) \subset (\gamma,I) \odot (H,C).$$

∎

Definition 7.3.15. *Let (F,A) be a soft ring over the ring R and (G,B) be a soft module over an R-module M. If (γ,I) be a soft prime ideal of (F,A), then*

$$(\gamma,I) \odot (G,B) = \{\gamma(a) G(b) : a \in Supp(\gamma,I) \wedge b \in Supp(G,B)\}$$

is a soft sub-module of (G, B).

Definition 7.3.16. *Let* (F, A) *be a soft ring over a ring* R *and* (G, B) *be a soft module over an* R*-module* M. *A soft primary sub-module* (H, C) *is said to be* (σ, P)*-soft primary sub-module of* (G, B). *If*

$$(\sigma, P) = rad\,(\xi, Q) = \{F\,(a) : F\,(a) \in (F, A) \wedge F\,(a)^n\,(G, B) \subseteq (H, B) \ \textit{for}\ n \geq 0\}$$

where

$$(\xi, Q) = \{F\,(a) : F\,(a) \in (F, A) \wedge F\,(a)\,(G, B) \subseteq (H, B)\}$$

Definition 7.3.17. *Let* (F, A) *be soft ring over a ring* R *and* (G, B) *be a soft module over an* R*-module* M. *A soft sub-module* (H, C) *of* (G, B) *has a primary decomposition if* $(H, C) = \Cap\,(H_i, C_i)$ *is a* (σ_i, P_i)*-soft primary sub-module of* (G, B), *where* (σ_i, P_i) *is a soft prime ideal of* (F, A).

7.4 Soft Galois rings and modules

Let us consider p be a prime number and k be a positive integer, $\mathbb{Z}_{p^k}$ is a finite local ring corresponding to residue field $\mathbb{Z}_p$. The polynomial extension of $\mathbb{Z}_{p^k}$ is $\mathbb{Z}_{p^k}[X] = \{a_0 + a_1X + a_2X^2 + \cdots + a_nX^n : a_i \in \mathbb{Z}_{p^k}, n \in \mathbb{Z}^+\}$. Let $f\,(x)$ is basic irreducible polynomial of degree r in $\mathbb{Z}_{p^k}[X]$ and $\frac{\mathbb{Z}_{p^k}[X]}{\langle f(x) \rangle} = \{a_0 + a_1X + a_2X^2 + \cdots + a_{h-1}X^{h-1} : a_i \in \mathbb{Z}_{p^k}[X]\}$ be the set of residue classes of polynomial X over $\mathbb{Z}_{p^k}$ modulo $f(X)$. The ring is denoted by $GR(p^k, r)$ and is known as Galois ring. The Galois ring $GR(p^k, 1)$ is isomorphic to $\mathbb{Z}_{p^k}$ and $GR(p, r)$ is isomorphic to $GF(p^r)$ a Galois field. If s divides r, then $GR(p^k, s)$ is subring of $GR(p^k, r)$ which is also a Galois ring. This ascending chain of Galois subrings becomes $\mathbb{Z}_{p^k} \subseteq GR(p^k, s_1) \subseteq GR(p^k, s_2) \subseteq \cdots \subseteq GR(p^k, r)$, while the ascending chain of Galois field is $\mathbb{Z}_p \subseteq GF(p^{s_1}) \subseteq GF(p^{s_2}) \subseteq \cdots \subseteq GF(p^r)$, where

s_i divides r. If we study the following structure on module over commutative rings, then the ascending chain of $\mathbb{Z}_{p^k}$-sub-modules is $\mathbb{Z}_{p^k} \subseteq GR(p^k, s_1) \subseteq GR(p^k, s_2) \subseteq \cdots \subseteq GR(p^k, r)$. The ascending chain of $\mathbb{Z}_p$-Galois subspaces $\mathbb{Z}_p \subseteq GF(p^{s_1}) \subseteq GF(p^{s_2}) \subseteq \cdots \subseteq GF(p^r)$.

In this section the soft rings and soft modules are being specified to soft Galois rings and soft modules. Further, their properties are studied, which are useful in the forthcoming discussion.

Definition 7.4.1. *Let $R = GR(p^k, r)$ be the Galois ring. The soft ring over the Galois ring R is map $F : A \longrightarrow P(R)$, defined as; $F(a_i) = GR(p^k, a_i)$, where A is the parametrized set and $A = \{a_i : a_i \text{ divides } r\}$. Each $F(a_i)$ is subrings of R and we call the soft ring (F, A) as the soft Galois ring.*

Definition 7.4.2. *Let (F, A) be soft Galois ring defined over R. The soft ideal of (F, A) is the mapping $\gamma : I \longrightarrow P(R)$, where $I \subseteq A$, $\gamma(a_i)$ is an ideal of $F(a_i)$ for $a_i \in I$ and $\gamma(a_i) = 0$ for $a_i \notin I$. Then soft ideal of (F, A) is denoted by (γ, I).*

Example 7.4.3. *Take the Galois ring $R = GR(2^4, 8)$. The soft ring (F, A) is $F : A \longrightarrow P(R)$ is defined as $F(a_i) = GR(2^4, a_i)$, where $A = \{a_i : a_i \text{ divides } 8\}$. The soft ideal (γ, I) with $I = A$ is defined as $\gamma(a_i) = pF(a_i) = pGR(2^4, a_i)$.*

We now construct the example of soft primary ideal and the definition of soft primary ideal is given in 7.1.3.

Example 7.4.4. *Take $R = A = \mathbb{Z}_8$. The soft ring (F, A) is defined as $F : A \longrightarrow P(R)$, $F(a_i) = a_i\mathbb{Z}_8$, where $a_i \in A$. Consider (γ, I) with $I = A\backslash\{0\}$ and is defined as $\gamma(a_i) = a_i\mathbb{Z}_8$ is a soft primary ideal of (F, A).*

From the definition of [99, Definition 10], the soft module is defined as follows;

Definition 7.4.5. *Let us consider the module (resp. algebra) $M = GR(p^k, r)$ over the ring $R = \mathbb{Z}_{p^k}$. The soft module (resp. soft algebra) is the mapping $G : B \longrightarrow P(M)$ where M is R.*

We now construct the example of soft sub-module over soft module and the definition of soft sub-module is given in (7.3.3).

Example 7.4.6. *Take the ring $R = \mathbb{Z}_8$. The $M = GR(2^3, 8)$ is an R-module. The soft ring (F, A) is given by $F : A \longrightarrow P(R)$ and is defined as $F(a_i) = a_i\mathbb{Z}_8$, where $A = \{a_i : a_i \text{ divides } 8\}$. A soft prime ideal (γ, I) in the soft ring (F, A) such that for given mapping $\gamma : I \longrightarrow P(R)$, where $I = \{q : q = 2, 4\} \subseteq A$, $\gamma(q) = q\mathbb{Z}_8$. Now consider the R-module M and the mapping $G : B \longrightarrow P(G)$ is defined as $G(b_i) = GR(2^3, b_i)$, where $B = \{b_i : b_i \text{ divides } 8\}$, (G, B) becomes a soft module over an R-module M. Then the soft sub-module of (G, B) is $(\gamma, I) \odot (G, B) = \gamma(q) \cdot G(b) = q\mathbb{Z}_8 \cdot GR(2^3, b_i)$.*

7.5 A connection between S-Boxes and soft $\mathbb{Z}_{2^k}-$module

In this section we develop a connection between the S-box and the soft ring and studied their properties. The construction of S-box over $GR(2^3, 4)$ and analyze statistical such as contrast, homogeneity, entropy, correlation and energy.

In particular, the ring $R = \mathbb{Z}_{2^3}$ is considered. The soft ring is the mapping $\mathcal{F} : A \longrightarrow P(R)$ and is defined as $\mathcal{F}(a_i) = (a_i)$. The soft ring becomes $(\mathcal{F}, A) = \{(0), (2), (4)\}$, where the set of attributes $A = \{0, 2, 4\}$. Soft primary ideal (ξ, I) over the ring R is defined as $\xi(a) = (a)$. Thus $(\xi, I) = \{(2)\}$, where

$a \in I = \{2\} \subseteq A$. Now consider a new set of parameters $B = \{2, 4, 8\}$ for $\mathbb{Z}_{2^k}-$module $GR(2^3, 8)$. The soft $\mathbb{Z}_{2^k}-$module $(\mathcal{G}, B)$ becomes $(\mathcal{G}, B) = \{GR(2^3, 2), GR(2^3, 4), GR(2^3, 8)\}$. The soft $\mathbb{Z}_{2^k}-$sub-module is $(\mathcal{H}, C) = \{GR(2^3, 4), GR(2^3, 8)\}$, where $C = \{4, 8\} \subset B$. The $(\mathcal{H}, C)$ is soft primary $\mathbb{Z}_{2^3}-$sub-module; indeed

$$\begin{aligned}
(\sigma, P) &= \{\mathcal{F}(a) : \mathcal{F}(a) \cdot (\mathcal{G}, B) \subseteq (\mathcal{H}, C)\} = \{\mathcal{F}(2), \mathcal{F}(4)\}, \\
\text{where } F(a) \cdot (\mathcal{G}, B) &= \left\{ \begin{array}{c} \mathcal{F}(2)\,\mathcal{G}(2), \mathcal{F}(2)\,\mathcal{G}(4), \mathcal{F}(2)\,\mathcal{G}(8), \\ \mathcal{F}(4)\,\mathcal{G}(2), \mathcal{F}(4)\,\mathcal{G}(4), \mathcal{F}(4)\,\mathcal{G}(8) \end{array} \right\}, \\
&= \left\{ \begin{array}{c} 2GR(2^3, 2), 2GR(2^3, 4), 2GR(2^3, 8), \\ 4GR(2^3, 2), 4GR(2^3, 4), 4GR(2^3, 8) \end{array} \right\}, \\
&\subseteq \{\mathcal{H}(4), \mathcal{H}(8)\} = (\mathcal{H}, C). \\
(\xi, I) &= rad(\sigma, P), \\
&= \{\mathcal{F}(a) : \mathcal{F}(a)^n \cdot (\mathcal{G}, B) \subseteq (\mathcal{H}, C)\}, \\
&= \{\mathcal{F}(2)\}.
\end{aligned}$$

Thus $(\xi, I) = \{\mathcal{F}(2)\}$ is soft primary ideal and $(\mathcal{H}, C)$ is $(\xi, I)-$soft primary $\mathbb{Z}_{2^3}-$sub-module.

Now we define the another soft $\mathbb{Z}_{2^3}-$sub-module $(\mathcal{K}, C) = \{2GR(2^3, 4), 2GR(2^3, 8)\}$. Also, $(\mathcal{K}, C)$ is soft $\mathbb{Z}_{2^3}-$sub-module of $(\mathcal{H}, C)$ and it is $(\xi, I)-$soft primary $\mathbb{Z}_{2^k}-$sub-module. Therefore using the definition of soft primary decomposition of soft modules (definition 7.3.10), we have $(\mathcal{K}, C) = (\mathcal{H}, C) \Cap (\mathcal{K}, C)$. Further, by applying the soft compliment operation (2.1.15) and is denoted by(γ, C);

$$\begin{aligned}
(\mathcal{H}, C) \setminus_C (\mathcal{K}, C) &= \{\mathcal{H}(4) - \mathcal{K}(4), \mathcal{H}(8) - \mathcal{K}(8)\}, \\
(\gamma, C) &= \{R_4^*, R_8^*\}.
\end{aligned}$$

Whereas R_4^*, R_8^* are respectively the set of units of the Galois rings $GR(2^3,4)$ and $GR(2^3,8)$. Here it is notice that (γ, C) soft group based on multiplicative groups R_4^*, R_8^*.

Further we extend our study to soft groups. Let (λ, D) be a soft group over a group R_8^*, where $D = \{i : i \text{ is order of subgroups of } R_8^*\}$. Each element $\lambda(i) \in P(R_8^*)$ is a subgroup of R_8^* of order i. The soft subgroup (λ_1, D_1) of soft group (λ, D), where $D_1 = \{j : j \text{ is order of cyclic subgroups of } R_8^*\} \subset D$. Therefore, each $\lambda_1(j)$ is cyclic subgroup of R_8^*. Let us consider another soft subgroup (λ_2, D_2) and $D_2 = \{j \in D_1 : j = 15, 255\} \subset D_1$. Then $(\lambda_2, D_2) = \{G_{15}, G_{255}\}$ is soft subgroup of soft group (γ, C). The maximal cyclic subgroups of R_4^* and R_8^* are respectively G_{15} and G_{255}. The order of maximal cyclic subgroup G_{15} is $2^4 - 1$, however the maximal cyclic subgroup G_{255} has order $2^8 - 1$.

We consider (λ_2, D_2) to construct S-boxes. An 8×8 S-box by using the maximal cyclic subgroup G_{255} of the Galois ring $GR(2^3, 8)$ is given in [93]. However for the sake of this work, we construct 4×4 S-box by the maximal cyclic subgroup G_{15} of the group of units of Galois ring $GR(2^3, 4)$.

Statistical analysis of 8×8 S-box:

Consider the maximal cyclic subgroup G_{255} contained in soft subgroup (λ_2, D_2). The S-box in G_{255} is constructed by defined the mappings from $G_{255} \cup \{0\}$ to $G_{255} \cup \{0\}$ [93]. The result of these analyses of proposed S-box for color components of original and encrypted images are given in following tables.

color components of original and encrypted images are given in following tables.

Texture features	Gray scale image
Contrast	0.36394
Homogeneity	0.881055
Entropy	7.76601
Correlation	0.920316
Energy	0.122742

Table 7.1 : Texture features of original image

Texture features	Gray scale image
Contrast	4.98983
Homogeneity	0.499004
Entropy	7.8011
Correlation	0.0867383
Energy	0.0285312

Table 7.2 : Texture features of encrypted image

Statistical analysis of S-box over G_{15} :

Let us consider the maximal cyclic subgroup G_{15} of soft subgroup (λ_2, D_2).The idea of construction of S-box based on G_{15} is the composition of linear functions. The following mappings from $G_{15} \cup \{0\}$ to $G_{15} \cup \{0\}$.

1. The inverse map I is defined as $I(a) = a^{-1}$.

2. The scalar multiplication function f is defined as $f(a) = ca$, where c is the scalar taken from G_{15}.

The concept of S-box is basically by taking the composition of these two functions as $I \circ f(a) = (ca)^{-1}$. This implies that by taking different scalars from G_{15}, we can construct 15 different S-boxes because 15 distinct scalar multiples are taken from

G_{15}. The following table of 4×4 S-box is constructed by taking one particular scalar.

0000	7005	3712	0433
4414	1075	2103	4176
0364	7557	1210	7700
1000	0171	5725	6603

Table 7.3 : S-boxes based on Galois ring

The analysis result of following S-box is as follows:

Contrast	0.3939
Homogeneity	0.8811
Entropy	7.7660
Correlation	0.9203
Energy	0.1227

Table 7.4 : Texture features of original image

Contrast	2.8294
Homogeneity	0.7974
Entropy	5.7005
Correlation	0.0417
Energy	0.4829

Table 7.5 : Texture features of encrypted image

The plain and encrypted image is as follows;


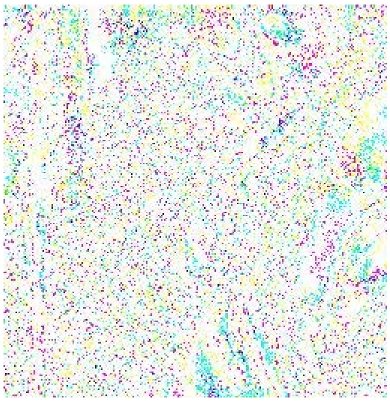

Fig. 7.1. Original image Fig 7.2. Encrypted image

In the following an approach is given, which integrate the soft subgroup (λ_2, D_2) and decision making technique for the selection of an appropriate S-box. Consider the soft subgroup $(\lambda_2, D_2) \subseteq (\lambda, D)$. The 4×4 and 8×8 S-boxes respectively constructed through the maximal cyclic subgroups G_{15} and G_{255}. Statistical analyses are performed over these S-boxes which show the reboutness of the encryption scheme. The decision making problem consider in this study is to select the most appropriate S-box which has better tendency to hide the image in transmission of data.

7.6 Proposed decision making method

In our proposed approach, we consider the statistical analyses as set of parameters and S-boxes as object. The decision is decompose into the following steps;

i. Select the desired number of S-boxes for input and statistical analyses for parametric set.

ii. Construct a fuzzy bipolar formula for each of the parameter.

iii. Structure the fuzzy bipolar soft set (Γ, E).

iv. Compute the comparison table for the bipolar functions.

v. Compute the positive and negative score for each object.

vi. Compute the final score.

The input set are the S-boxes constructed over the soft subgroup (λ_2, D_2), that is $\{S_4, S_8\}$. Whereas the set of parameters $E = \{e_1, e_2, e_3, e_4, e_5\}$ are contrast, homogeneity, entropy, correlation and energy. Before tuning into decision making steps it is worth recalling some details about the above mention parameters for bipolar soft set.

Function for contrast The bipolar fuzzy set for contrast is defined as;

$$\begin{aligned} \mu_{\Gamma_E(e_1)}(s_i) &= e_1(P_{s_i}) \cdot e_1(O_{s_i}) \pmod 1, \\ \mu_{\Gamma_{\neg E}(\neg e_1)}(s_i) &= \frac{e_1(P_{s_i})}{e_1(O_{s_i})} \pmod 1, \end{aligned}$$

where $e_1(P_{s_i})$ is value of encrypted image of contrast and $e_1(O_{s_i})$ is value of original image of contrast.

Function for homogenity The bipolar fuzzy set for homogeneity is defined as;

$$\begin{aligned} \mu_{\Gamma_E(e_2)}(s_i) &= e_2(P_{s_i}) \cdot e_2(O_{s_i}), \\ \mu_{\Gamma_{\neg E}(\neg e_2)}(s_i) &= \frac{e_2(P_{s_i})}{e_2(O_{s_i})}, \end{aligned}$$

where $e_2(P_{s_i})$ is value of encrypted image of homogeneity and $e_2(O_{s_i})$ is value of original image of homogeneity.

Function for entropy The bipolar fuzzy set for entropy is defined as;

$$\begin{aligned} \mu_{\Gamma_E(e_3)}(s_i) &= (e_3(P_{s_i}) - e_3(O_{s_i})) \bmod 1, \\ \mu_{\Gamma_{\neg E}(\neg e_3)}(s_i) &= \frac{e_3(P_{s_i})}{e_3(O_{s_i})}, \end{aligned}$$

where $e_3(P_{s_i})$ is value of encrypted image of entropy and $e_3(O_{s_i})$ is value of original image of entropy.

Function for correlation The bipolar fuzzy set for correlation is defined as;

$$\begin{aligned}\mu_{\Gamma_E(e_4)}(s_i) &= e_4(O_{s_i}) - e_4(P_{s_i}),\\ \mu_{\Gamma_{\neg E}(\neg e_4)}(s_i) &= 1 - \left(e_4(O_{s_i}) + e_4(P_{s_i})\right),\end{aligned}$$

where $e_4(P_{s_i})$ is value of encrypted image of correlation and $e_4(O_{s_i})$ is value of original image of correlation.

Function for energy The bipolar fuzzy set for energy is defined as;

$$\begin{aligned}\mu_{\Gamma_E(e_1)}(s_i) &= 1 - \left(e_5(O_{s_i}) + e_5(P_{s_i})\right),\\ \mu_{\Gamma_{\neg E}(\neg e_1)}(s_i) &= \frac{e_5(P_{s_i})}{e_5(O_{s_i})},\end{aligned}$$

where $e_5(P_{s_i})$ is value of encrypted image of energy and $e_5(O_{s_i})$ is value of original image of energy.

7.6.1 Fuzzy bipolar soft set

[75]A fuzzy bipolar soft set $(\Gamma_E, \Gamma_{\neg E}, E)$ over U, where Γ_E and $\Gamma_{\neg E}$ are mappings such that $\Gamma_E : E \longrightarrow FP(U)$ and $\Gamma_{\neg E} : \neg E \longrightarrow FP(U)$ such that $0 \leq \Gamma_E(x) + \Gamma_{\neg E}(x) \leq 1$ for all $e \in E$.

Γ_E	e_1	e_2	e_3	e_4	e_5
S_4	0.1145	0.7026	0.0655	0.8786	0.3944
S_8	0.8159	0.4397	0.0351	0.8336	0.8488

Table 7.6 : Positive fuzzy bipolar soft set

$\neg\Gamma_E$	$\neg e_1$	$\neg e_2$	$\neg e_3$	$\neg e_4$	$\neg e_5$
S_4	0.1042	0.5591	0.1776	0.0261	0.8821
S_8	0.3712	0.1821	0.9978	0.0339	0.5897

Table 7.7 : Negative fuzzy bipolar soft set

Comparision Table

[75, Definition 20] Let $(\Gamma_E, \Gamma_{\neg E}, E)$ be a fuzzy bipolar soft set defined over the set U. A comparison table for Γ_E is a square table in which the numbers of rows and numbers of columns are equal, rows and columns both are labeled by the object names S_4, S_8 of the initial universe U, and the entries are $x_{ij},\ i, j = 1, 2$ given by

$$x_{ij} = \text{the number, for which the positive membership function of } e_i \text{ is important by the membership degree of } e_j \quad (7.6.1)$$

$$= \begin{cases} 1 & \text{if } e_i > e_j, \\ 0 & \text{if } e_i < e_j, \end{cases} \quad (7.6.2)$$

Note that $0 \leq x_{ij} \leq 5$, $x_{ii} = 5$ for all i, j and 5 is the number of parameters presented in E.

Ψ	S_4	S_8
S_4	5	3
S_8	2	5

Table 7.8. Comparison positive.

Comparison table for negative membership function is denoted by Φ. It is a table in which number of rows are equal to the number of columns, rows and columns both are labeled by he parameters $e_1, e_2, \cdots, e_5$. The entries are $y_{ij},\ i,j = 1,2.$ given by

$$\begin{aligned} y_{ij} &= \text{the number, for which the negative membership function of } e_i \text{ is} \\ &\quad \text{important by membership function of } e_j \\ &= \begin{cases} 1 & \text{if } e_i > e_j, \\ 0 & \text{if } e_i < e_j, \end{cases} \end{aligned} \tag{7.6.3}$$

(3.4)

where $0 \leq y_{ij} \leq p$, $y_{ii} = 5$ for all i, j and 5 is the number of parameters present in E.

Φ	S_4	S_8
S_4	5	2
S_8	3	5

Table 7.9 : Comparison negative.

Score [75, Definition 21] The positive row sum is denoted by r_i and positive column sum is denoted by c_i. The formula for calculating positive row and column sum is $r_i = \sum_{i=1}^{5} x_{ij}, c_i = \sum_{i=1}^{5} x_{ij}$. The positive score x_i of S-box S_i is calculated $x_i = r_i - c_i$.

In the following table positive score is calculated as;

$+$	r_i	c_i	x_i
S_4	8	7	1
S_8	7	8	-1

Table 7.10 : Positive score.

The negative row sum is denoted by r_i' and negative column sum is denoted by c_i'. The formula for calculating negative row and column sum is $r_i = \sum_{i=1}^{5} y_{ij}, c_i = \sum_{i=1}^{5} y_{ij}$. The negative score y_i of S-box S_i is calculated $y_i = r_i' - c_i'$. In the following table negative score is calculated as;

-	r'_i	c'_i	y_i
S_4	7	8	-1
S_8	8	7	1

Table 7.11 : Negative score.

7.6.2 Grading and final result

[75, Definition 22] The final score z_i of S-box S_i will be given by $z_i = x_i - y_i$. The maximum value represents the optimal one.

z_i	$x_i - y_i$
S_4	2
S_8	-2

Table 7.12 : score.

We find out the S_4 is the best. The evaluation method based on fuzzy bipolar soft set theory is being presented which sort out the appropriate S-box constructed over soft subgroup (β, C).

Chapter 8

Conclusion

In literature and lifespan, we untimely pursue, not the conclusion but beginnings. Therefore, to conclude thesis, a summary of research performed is presented in the first section of this chapter which is followed by discussions of possible future directions that could explain this research as mentioned in the final section of this chapter.

The construction of the secure S-boxes with complete cryptographic features is extremely important for constructing dominant encryption systems. There is list of available algorithms to construct the efficient S-boxes but the major aim of S-box is to construct the nonlinear component of block ciphers. To measure the encryption quality of the S-box different decision-making algorithms have been devised. In this work, we used the soft set along with the different already soft set theories to deal with uncertainty.

Initially, we have investigated the characterization of S-boxes by using interval-valued fuzzy soft sets. A decision-making scheme is constructed by using the technique to separately deal with lower and upper approximation. The interval-valued fuzzy soft set approaches for comparison of data and easy way to approach the decision. The ranking of S-boxes by interval-valued fuzzy decision-making result is an alternative way to judge the quality of S-box.

The decision-making process is related to construct more accurate intuitionistic fuzzy soft set decision benchmarks which are used to deals with computing and measuring the performance of S-boxes. Different images are used to judge the quality and consistency of S-boxes in the digital medium. The formulation of membership and non-membership function for each parameter is used to determine the performance of analyses parameters. Some significant evidence is found, when we have applied our proposed testing standards on available images in literature.

The intuitionistic fuzzy soft set fundamentally based on membership and non-membership utilities. The work is refined by using the neutrosophic fuzzy soft set which not only deals with membership and non-membership functions but also there is an intermediate function in between these both functions. The neutrosophic fuzzy soft set decision-making method is introduced to characterize the S-boxes. The enciphered results of four different images are taken and by carrying out our proposed analysis, the optimal S-box for each image is chosen. The comparison of the results of the already available algorithm with the outcomes of the intuitionistic fuzzy soft set method is being discussed.

Further, we introduced an improved decision-making technique. The average deviation was used to gauge the neutrosophic soft set. We have used the property of basic operation of central tendency. The property of basic operation of central tendency is applied. These operations enabled us to classify the S-boxes. The method for the construction of S-boxes was based on the action of the projective general linear group over Galois field. This method generates a huge number of S-boxes which is refined by inducing a non-linearity check in the proposed algorithm to collect the desired S-boxes. For the assessment of the strength of the generated S-boxes, we analyzed their characteristics through statistical analyses. The new decision-making method for the neutrosophic fuzzy soft set, with functions defined in the proposed analysis, are accustomed to the statistical analysis for the selection of the nonlinear component of block cipher which is not vulnerable and ability to provide confusion in security systems. With this work, we established novel results in the field of intuitionistic fuzzy soft set and information security.

The notion of soft prime ideal, soft primary ideal, soft radical ideal and primary decomposition of soft rings is introduced. Further, the idea of soft modules is used to define the primary decomposition of soft modules. This indication of soft rings and soft modules is further developed and defined the particular soft Galois ring and soft Galois modules. Then by using the theory of soft Galois modules to define the S-box which is used in decision-making algorithm. The projected procedure for selecting best S-box permits us to classify the best S-box which definitely reduces the cost and time of execution of our machine. These sorts of selection criteria can be embedded in systems in order to protect cost which is a growing issue of existing green world ideology.

To the best of our knowledge and deep findings, our proposed methodologies contribute efficiently to the selection of the optimal S-box. Our proposed idea essentially provides a bridge between fuzzy soft set theory and information security namely cryptographic algorithm. Through this classification, one can easily classify the central component of block ciphers which is surely S-boxes. This work provides a new area of research for the oncoming researcher and entered the fuzzy soft idea into a completely new era.

Future work will entail refining our model by exploiting data on the different model which gives more accurate results. The research is continuing in this direction, in future the work can be extended to the technique for order preferences by similarity to ideal solution (TOPSIS) model along with soft set theory and its generalized form. We do believe that present findings based on applying decision-making algorithm, will surely support us, to efficiently handle diverse problems of cryptology, watermarking and steganography.

Bibliography

[1] E. S. Abuelyman, A. A. S. Alsehibani, An optimized implementation of the S-Box using residue of prime numbers, *Int. J. Comput. Sci. & Netw. Secur.*, 8(4): (2008), 304-309.

[2] U. Acar, F. Koyuncu, B. Tanay, Soft sets and soft rings, *Comput. Math. Appl.*, 59(11): (2010), 3458-3463.

[3] H. Aktaş, N. Caĝman, Soft sets and soft groups, *Inform. Sciences*, 177(13): (2007), 2726-2735.

[4] H. Aktaş, S. Özlü, Cyclic soft groups and their applications on groups, *The Scientific World J.*, 2014: (2014), 1-5.

[5] M. I. Ali, F. Feng, X. Y. Liu, W.K. Min, M. Shabir, On some new operations in soft set theory, *Comput. Math. Appl.*, 57(9): (2009) 1547–1553.

[6] A. O. AtagÄun, A. Sezgin, Soft substructures of rings, Fields and modules, *Comput. Math. Appl.*, 61(3): (2011), 592-601.

[7] K. Atanassov, Intuitionistic fuzzy sets, *Fuzzy Set Syst.,* 20: (1986) 87-96.

[8] K. Atanassov, Intuitionistic Fuzzy Sets–Theory and Applications, *Stud. Fuzziness Soft Comput.*, 35: (1999).

[9] T. M. Basu, N. K. Mahapatra, S. K. Mondal, A balanced solution of a fuzzy soft set based decision making problem in medical science, *Appl. Soft Comput.*, 12(10): (2012), 3260–3275.

[10] S. I. Batool, T. Shah, M. Khan, A color image watermarking scheme based on affine transformation and S_4 permutation, *Neural Comput. Appl.*, 25(7): (2014), 2037-2045.

[11] E. Biham, A. Shamir, Differential cryptanalysis of DES-like cryptosystems, In: Advances in Cryptology-CRYPT0' 90, *Lect. Notes. Comput. Sc.,* 537: pp. 2-21, (1991).

[12] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, C. Vikkelsoe, PRESENT: An Ultra-Lightweight Block Cipher. In: Cryptographic Hardware and Embedded Systems, *Lect. Notes. Comput. Sc.*, 4727: pp. 450-466, (2007).

[13] S. Broumi, F. Smarandache, Intuitionistic Neutrosophic Soft Set, *Journal of Information and Computing Science*, 8(2): (2013), 130-140.

[14] S. Broumi, Generalized Neutrosophic Soft Set, *Int. J. Comput. Sci. Eng. Inf. Tech.*, 3(2): (2013), 17-30.

[15] S. Broumi, I. Deli, and F. Smarandache, Relations on Interval Valued Neutrosophic Soft Sets, *Journal of New Results in Science*, 5: (2014), 1-20.

[16] S. Broumi, I. Deli, F. Smarandache, Neutrosophic Parametrized Soft Set theory and its decision making problem, *International Frontier Science Letters*, 1(1): (2014), 01-11.

[17] N. Cagman, F. Citak, S. Enginoglu, Fuzzy parameterized fuzzy soft set theory and its applications, *Turkish Journal of Fuzzy Systems,* 1: (2010), 21–35.

[18] N. Cagman, F. Citak, S. Enginoglu, FP-soft set theory and its applications, *Ann. Fuzzy Math. Inform.,* 2(2): (2011), 219-226.

[19] N. Cagman, I. Deli, Intuitionistic fuzzy parametrized soft set theory and its decision making, *Appl. Soft Comput.*, 28: (2012), 109–113.

[20] N. Cagman, S. Enginoglu, Soft matrix theory and its decision making, *Comput. Math Appl.,* 59: (2010), 3308–3314.

[21] N. Cagman, S. Enginoglu, Soft set theory and uni-int decision making, *European J. Oper. Res.*, 207(2): (2010), 848–855.

[22] N. Cagman, S. Enginoglu, F. Citak, Fuzzy soft set theory and its applications, *Iran. J. Fuzzy Syst.,* 8(3): (2011), 137–147.

[23] N. Cagman, S. Karatas, Intuitionistic fuzzy soft set theory and its decision making, *J. Intell. Fuzzy Syst.*, 24: (2013), 829-836.

[24] Y. Celik, C. Ekiz and S. Yamak, A new view on soft rings, *Hacet. J. Math. Stat.*, 40(2): (2011), 273-286.

[25] D. Chen, The parametrization reduction of soft sets and its Applications, *Comput. Math. Appl.,* 49: (2005), 757-763.

[26] J. Christian, M. Hortmann, G. Leander, Boolean Functions, *PhD thesis*, (2012).

[27] C. Cid, S. Murphy, M. J. B. Robshaw, Small Scale Variants of the AES, In: Fast Software Encryption, *Lect. Notes. Comput. Sc.*, 3557: pp. 145-162, (2005).

[28] N. T. Courtois, J. Pieprzyk, Cryptanalysis of block ciphers with overdefined systems of equations, In: 8th International Conference on the Theory and Application of Cryptology and Information Security Queenstown, *Lecture Notes in Comput. Sci.,* 2501: pp 267-287, (2002).

[29] L. Cui, Y. Cao, A new S-box structure named Affine- Power-Affine, Int. J. Innov. Comput. I. *International Journal of Innovative Computing, Information and Control*, 3(3): (2007), 45-53.

[30] S. Das, S. Kar, Group decision making in medical system: An intuitionistic fuzzy soft set approach, *Appl. Soft Comput.*, 24: (2014), 196–211.

[31] J. Daemen, V. Rijmen, AES Proposal: Rijndael. AES Algorithm Submission, Available: http://csrc.nist.gov/archive/aes/rijndael/ Rijndael-ammended.pdf. (1999).

[32] İ. Deli, S. Broumi, Neutrosophic soft relations and some properties, *Ann. Fuzzy Math. Inform.*, 9(1): (2015), 169-182.

[33] I. Deli, Y. Toktas, S. Broumi, Neutrosophic Parameterized Soft Relations and Their Applications, *Neutrosophic Sets and Systems,* 4: (2014), 25-34.

[34] H. M. El-Sheikh, O. A. El-Mohsen, T. Elgarf, A. Zekry, A new approach for designing key-dependent S-Box defined over $GF(2^4)$ in AES, *Int. J. Comput. Theory Eng.*, 4(2): (2012), 158-164.

[35] F. Feng, Y. B. Jun, X. Zhao, Soft semirings, *Comput. Math. Appl.,* 56: (2008), 2621-2628.

[36] F. Feng, Y. B. Jun, X. Liu, L. Li, An adjustable approach to fuzzy soft set based decision making, *J. Comput. Appl. Math.*, 234: (2010), 10–20.

[37] F. Feng, C. Li, B. Davvaz, M.I. Ali, Soft sets combined with fuzzy sets and rough sets: a tentative approach, *Soft Comput.,* 14(9): (2010), 899–911.

[38] F. Feng, Y. Li, N. Çağman, Generalized uni-int decision making schemes based on choice value soft sets, *Eur. J. Oper. Res.*, 220(1): (2012), 162–170.

[39] D. Feng and W. Wu, Design and analysis of block ciphers, *Tsinghua University Press (* 2000).

[40] R. Forre, The strict avalanche criterion: Spectral properties of boolean functions and an extended definition, In: Advances in Cryptology - CRYPTO' 88, *Lect. Notes. Comput. Sc.*, 403: pp. 450-468, (1990).

[41] T. Jakobsen and L. R. Knudsen, The interpolation attack on block ciphers, In: Fast Software Encryption, *Lect. Notes. Comput. Sc.*, 1267: (1997), 28–40.

[42] Y. Jiang, Y. Tang, Q. Chen, An adjustable approach to intuitionistic fuzzy soft sets based decision making, *Appl. Math. Model.,* 35: (2011), 824–836.

[43] A. Goldsztejn, W. Hayes, P. Collins, Tinkerbell is Chaotic, *SIAM J. Appl. Dyn. Syst.,* 10(4): (2011), 1480-1501.

[44] R. M. Haralick, K. Shanmugam, I. Dinstein, Texture features for image classification, *IEEE T. Syst. Man Cy-S*, 3(6): (1973), 610–621.

[45] T. Herawan, M. M. Deris, Soft decision making for patients suspected influenza, In: Computational Science and Its Applications - ICCSA 2010, *Lect. Notes. Comput. Sc.*, 6018: pp.405-418, (2010).

[46] T. Herawan, M. M. Deris, A soft set approach for association rules mining, *Knowl.-Based Syst.*, 24: (2011). 186–195.

[47] I. Hussain, T. Shah, H. Mehmood, A New Algorithm to Construct Secure Keys for AES, *Int. J. Contemp. Math. Sci.,* 5(26): (2010), 1263-1270.

[48] F. Karaaslan, Neutrosophic soft set with applications in decision making, *International Journal of Information Science and Intelligent System*, 4(2): (2015), 1-20.

[49] M. Khan, T. Shah, A novel construction of substitution box with Zaslavskii chaotic map and symmetric group, *J. Intell. Fuzzy Syst.,* 28: (2015), 1509–1517.

[50] M. Khan, T. Shah, A construction of novel chaos base nonlinear component of block cipher, Nonlinear Dynamics, *Nonlinear Dynam.,* 76: (2014), 377–382.

[51] M. Khan, T. Shah, A novel image encryption technique based on Hénon chaotic map and S8 symmetric group, *Neural Comput. Appl.*, 25: (2014), 1717-1722.

[52] M. Khan, T. Shah, A construction of novel chaos base nonlinear component of block cipher, *Nonlinear Dynam.,* 76: (2014), 377–382.

[53] Z. Kong, L. Gao, L. Wang, The normal parameter reduction of soft sets and its algorithm, *Comput. Math. Appl.*, 56(12): (2008) 3029–3037.

[54] Z. Kong, L. Gao, L. Wang, Comment on 'A fuzzy soft set theoretic approach to decision making problems', *J. Comput. Appl. Math.,* 223(2): (2009), 540–542.

[55] Z. Kong, L. Wang, Z. Wu, Application of fuzzy soft set in decision making problems based on grey theory, *J. Comput. Appl. Math.,* 236: (2011), 1521–1530.

[56] D. V. Kovkov, V. M. Kolbanov, D. A. Molodtsov, Soft sets theory-based optimization, *J. Comput. Sys. Sc. Int.*, 46(6): (2007), 872-880.

[57] T. L. Kuang, Z. Xiao. A Multi-Criteria Decision Making Approach based on Triangle-valued Fuzzy Soft Sets, *Journal of Convergence Information Technology*, 7(15): (2012), 17-25.

[58] T. L. Kuang, Trapezoid-valued Fuzzy Soft Sets and its Applications, Adv. Inf. Sci. Serv. Sci., 4(15): (2012), 310-316.

[59] S. A. Lashari, R. Ibrahim, N. Senan, Performance comparison of musical instrument family classification using soft set, *International Journal of Artificial Intelligence and Expert Systems*, 3(4): (2012), 100-110.

[60] R. Lechner, Harmonic analysis of switching functions. In: Recent developments in switching theory, *Academic Press, New York*, (1971).

[61] J. Lui, B. Wai, X. Cheng, X. Wang, An AES S-box to increase complexity and cryptographic analysis, In 19th International Conference on Advanced Information Networking and Applications, *AINA 2005,* 1: pp.724-728, (2005).

[62] P. K. Maji, More on intuitionistic fuzzy soft sets, In: Rough sets, Fuzzy sets, Data mining and granular computing, *Lecture Notes in Artificial Intelligence,* 5908: pp.231-240, (2009).

[63] P. K. Maji, Neutrosophic soft set, *Ann. Fuzzy Math. Inform.*, 5(1): (2013), 157-168.

[64] P. K. Maji, R. Biswas, R. Roy, Fuzzy soft sets, *J. Fuzzy Math.,* 9(3): (2001), 589–602.

[65] P. K. Maji, R. Biswas, R. Roy, Intuitionistic fuzzy soft sets, *J. Fuzzy Math.,* 9(3): (2001), 677-692.

[66] P. K. Maji, R. Roy, An application of soft sets in a decision making problem, *Comput. Math. Appl.*, 44: (2002), 1077-1083.

[67] P. K. Maji, R. Biswas, R. Roy, Soft set theory, *Comput. Math Appl.*, 45: (2003), 555-562.

[68] R. Mamat, T. Herawan, M. M. Deris, MAR: Maximum Attribute Relative of soft set for clustering attribute selection, *Knowl.-Based Syst.*, 52: (2013), 11–20.

[69] P. P. Mar, K. M. Latt, New Analysis Methods on Strict Avalanche Criterion of S-Boxes, *World Acad. Sci. Eng. Technol.,* 48: (2008).

[70] S. Mister and C. Adams, Practical S-Box Design, Proceedings, *Workshop in Selected Areas of Cryptography*, SAC' 96: (1996).

[71] H. Mihajloska, D. Gligoroski, Construction of Optimal 4-bit S-boxes by Quasigroups of Order 4. In: The Sixth International Conference on Emerging Security Information, Systems and Technologies, *SECURWARE 2012*, (2012).

[72] D. Molodtsov, Soft set theory first results, *Comput. Math. Appl.*, 37: (1999), 19-31.

[73] M. M. Mushrif, S. Sengupta, A. K. Ray, Texture Classification Using a Novel soft Set Theory Based Classification Algorithm, In: 7th Asian Conference on Computer Vision, 3851: pp. 246-254, (2006).

[74] J. Nakahara Jr., D. S. Freitas, Mini-ciphers: a reliable testbed for cryptanalysis?, In Symmetric Cryptography, Seminar, Dagstuhl Seminar Proceedings. *Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik*, 09031: pp. 1862-4405, (2009).

[75] M. Naz, M. Shabir, On fuzzy bipolar soft sets, their algebraic structures and applications, *J. Intell. Fuzzy Syst.*, 26(4): (2014), 1645-1656.

[76] T. J. Neon, An application of imprecise soft sets in teaching evaluation, *International Journal for Basic Sciences and Social Sciences,* 1(2): (2012), 25-29.

[77] Z. Pawlak, Rough sets, *Int. J. Parallel Prog.*, 11(5): (1982), 341-356.

[78] D. Pie, D. Miao, From soft sets to information systems, *IEEE Conference on Granular Computing*, 2: (2005), 617-621.

[79] V. Preneel, V. Leekwijk, V. Linden, G. Vandewalle, Propagation characteristics of boolean functions, *Lect. Notes. Comput. Sc.*, 473: pp. 161-173, (1991).

[80] H. Qin, X. Ma, J. M. Zain, T. Herawan, A novel soft set approach in selecting clustering attribute, Knowl.-Based Syst. 36: (2012), 139–145.

[81] K. Qin, J. Yang, X. Zhang, Soft set approaches to decision making problems, In: 7th International Conference, *RSKT 2012*, 7414: pp. 456–464, (2012).

[82] I. Rehman, T. Shah, I. Hussain, Analyses of S-box in image encryption applications based on fuzzy decision making criterion, *Z. Naturforsch. A,* 69a: (2014), 207-214.

[83] F. R. Renzetti, L. Zortea, Use of a gray level co-occurrence matrix to characterize duplex stainless steel phases microstructure, *Fracture and Structural Integrity*, 16: (2011), 43-51.

[84] F. J. Ronald, Construction of the Jordan basis for the Baker map, *Chaos*, 7: (1997), 254-255.

[85] R. Roy, P. Maji, A fuzzy soft set theoretic approach to decision making problems, *J. Comput. Appl. Math.*, 203(2): (2007), 540-542.

[86] R. Şahin, A. Kücük, Generalised Neutrosophic Soft Set and its Integration to Decision Making Problem, *Appl. Math. Inf. Sci.*, 8(6): (2014), 2751-2759.

[87] R. Şahin, A. Küçük, On Similarity and Entropy of Neutrosophic Soft Sets, *J. Intell. Fuzzy Systems*, 27(5): (2014), 2417-2430.

[88] A. Sezgin and A. O. AtagÄun, Soft groups and normalistic soft groups, *Comput. Math. Appl.,* 62(2): (2011), 685-698.

[89] T. Shah, I. Hussain, M. A. Gondal, A. Mahmood, Statistical analysis of S-box in image encryption applications based on majority logic criterion, *Int. J. Phys. Sci.,* 6(16): (2011), 4110-4127.

[90] T. Shah, A. Qamar and I. Hussain, Substitution Box on Maximal Cyclic Subgroup of Units of a Galois Ring, *Z. Naturforsch. A*, 68a: (2013), $567-572$.

[91] T. Shah, N. Mehmood, A. A. Andrade and R. Palazzo, Maximal cyclic subgrougs of the groups of units of Galois rings: a computational approach, *Comput. Appl. Math.,* (2015), 25-50.

[92] T. Shah, M. Zafar, S. Medhit, N. Mehmood, Chaotic S-boxes generation algorithm and IFS-Decision making, (submitted).

[93] T. Shah, M. Khan, R. Parveen, A. Ali, A novel S-box consturction over $GR(2^3, 8)$ and its application in image encryption, (Submitted).

[94] C. E. Shannon, Communication system of secrecy system, *Bell Systems Technical Journal,* 28(4): (1949), 656-715.

[95] X. Y. Shi, H. U. Xiao, X. C. You, K. Y. Lam, A Method for obtaining cryptographically strong 8×8 S-boxes, *IEEE Global Telecommunications Conference, 1997*, 2(3): (1997), 689-693.

[96] F. Smarandache, A Unifying Field in Logics. Neutrosophic Logic. Neutrosophy, Neutrosophic Set, Neutrosophic Probability (fourth ed.), *Multimedia Larga*, (2005).

[97] R. L. Sparta and J. H. Bradley, Using Entropy Analysis to Find Encrypted and Packed Malware, *IEEE Secur. Priv.*, 5(2): (2007), 40-45.

[98] W. Stallings, Cryptography and Network Security: Principles & Practices, sixth ed. *Pearson Education Limited*, (2014).

[99] Q. M. Sun, Z. L. Zhang, J. Liu, Soft Sets and Soft Module: Proceedings of the third international conference on rough sets and knowledge technology, *Lect. Notes Comput. Sc.*, 5009: pp. 403-409, (2008).

[100] T. W. Cusick, P. Stanica. Cryptographic Boolean functions and applications, *Elsevier/Academic Press*, Amsterdam, (2009).

[101] M. T. Tran, D. K. Bui, A. D. Doung, Gray S-box for advanced encryption standard, In: International Conference on Computational Intelligence and Security, 2008. 1: pp. 253-258, (2008).

[102] E. Türkmen, A. Pancar, On some new operations in soft module theory, *Neural Comput. Appl.*, 22(6): (2012), 1233-1237.

[103] A. F. Webster, S. E. Tavares, On the design of S-boxes, In Advances in Cryptology- CRYPTO'85 Proceedings, *Lect. Notes. Comput. Sc.*, 218: pp. 523-534, (1986).

[104] X. B. Yang, T. Y. Lin, J. Y. Yang, Y. Li, D. J. Yu, Combination of interval-valued fuzzy set and soft set, *Comput. Math. Appl.*, 58(3): (2009), 521-527.

[105] L. A. Zadeh, Fuzzy sets, *Inform. Control*, 8: (1965), 338 - 353.

[106] L.A. Zadeh, The concept of a linguistic variable and its application to approximate reasoning - I, *Inform. Sciences*, 8: (1975), 199 - 249.

[107] Y. Zou, Z. Xiao, Data analysis approaches of soft sets under incomplete information, *Knowl.-Based Syst.*, 21: (2008), 941-945.

[108] SKIPJACK and KEA Algorithm. Specifications version. 2(29): (1998), 1-23.