A Cryptosystem Technique based on DNA Operations from a Non-Associative LA-Field

By

Khadija Tariq

(770-FBAS/MSMA/F21)

Department of Mathematics and Statistics

Faculty of Sciences

International Islamic University, Islamabad

Pakistan

2023

Nonassociative rings.

Algebra, Nonassociative

Cryptography - Mathematics.

Mathematical models.

A Cryptosystem Technique based on DNA Operations from a Non-Associative LA-Field

By

Khadija Tariq

(770-FBAS/MSMA/F21)

Supervised by

Dr. Nazli Sanam

Department of Mathematics and Statistics

Faculty of Sciences

International Islamic University, Islamabad

Pakistan

2023

A Cryptosystem Technique based on DNA Operations from a Non-Associative LA-Field

By

Khadija Tariq

(770-FBAS/MSMA/F21)

A Thesis
Submitted in the Partial Fulfillment of the
Requirement of the Degree of
MASTER OF SCIENCE
In
MATHEMATICS

Supervised by

Dr. Nazli Sanam

Department of Mathematics and Statistics
Faculty of Sciences
International Islamic University, Islamabad
Pakistan
2023

Certificate

A Cryptosystem Technique based on DNA Operations from a Non-Associative LA-Field

By

Khadija Tariq

A DISSERTATION SUBMITTED IN THE PARTIAL FULFILLMENT OF THE

REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE IN MATHEMATICS

We accept this dissertation as confirming to the required standard.

1. ____________________
Dr. Naveed Yaqoob
(External Examiner)

2. ____________________
Dr. Tahir Mehmood
(Internal Examiner)

3. ____________________
Dr. Nazli Sanam
(Supervisor)

4. ____________________
Prof. Dr. Nasir Ali
(Chairperson)

Department of Mathematics and Statistics
Faculty of Sciences
International Islamic University, Islamabad
Pakistan
2023

Declaration

I, Khadija Tariq hereby declare that the work presented in this thesis, titled "**A Cryptosystem Technique based on DNA Operations from a Non-Associative LA-Field**" is solely the result of my original research and intellectual endeavors. I confirm that all sources used have been duly acknowledged and cited. This work has not been submitted for any other degree or qualification at any other institution. I take full responsibility for the content and authenticity of this work, and I understand that any dishonesty or plagiarism will have serious consequences.
The work was done under the supervision of **Dr. Nazli Sanam** at International Islamic University, Islamabad.

Khadija Tariq
MS (Mathematics)
Reg.no.770-FBAS/MSMA/F21
Department of Mathematics and Statistics
Faculty of Sciences,
International Islamic University Islamabad, Pakistan.

Forwarding Sheet by Research Supervisor

The thesis entitled "**A Cryptosystem Technique based on DNA Operations from a Non-Associative LA-Field**" submitted by "**Khadija Tariq, 770-FBAS/MSMA/F21**" in partial fulfillment of MS Degree in Mathematics has been completed under my guidance and supervision. I am satisfied with the quality of her research work and allow her to submit this thesis for further process to graduate with a Master of Science degree from the Department of Mathematics & Statistics, as per IIUI rules and regulations.

Date ....

Signatures: ______________

(Dr. Nazli Sanam)
Lecturer
Department of Maths & Stats,
International Islamic University, Islamabad,
Pakistan.

Acknowledgement

All praise and thanksgiving are due to Allah (SWT), the Merciful Lord, the Creator, Who leads me in the dark, helps me in difficulties, and gives me the ability to bravely achieve the final stage. Gratitude in particular for the last Prophet Muhammad (PBUH).

Foremost, appreciation goes to my loving parents, whose unwavering support, encouragement, and unconditional love have been my constant motivation, I am forever grateful. My heartiest thanks to my siblings, who have always stood by my side and provided invaluable support, words of encouragement, and a sense of belonging, I am truly thankful.

A special appreciation goes to my husband Muhammad Sajjad Shad, whose unwavering belief in my abilities and continuous support have been instrumental in my success. His love and encouragement have been my pillar of strength. I would like to express my heartfelt appreciation to my dear friends and fellow researchers for their unwavering support and invaluable discussions throughout the journey of my thesis.

I extend my sincere appreciation to my dedicated supervisor, Dr. Nazli Sanam. Her guidance, expertise, and unwavering support have shaped this work and elevated it to new heights. Her invaluable insights and encouragement have been invaluable throughout the research process.

Furthermore, I would like to acknowledge the assistance and expertise of Dr. Tanveer ul Haq. His collaboration and assistance in conducting the Lyapunov exponent and bifurcation diagrams of the Novel chaotic map have been indispensable in enriching this research.

Khadija Tariq

Dedicated

to

My Family

and

My Supervisor Dr. Nazli Sanam

Preface

In an era, where information security is of paramount importance, the field of cryptography has emerged as a powerful tool for protecting sensitive data from unauthorized access. Traditional cryptographic techniques rely on mathematical algorithms and computational complexity to ensure the confidentiality and integrity of information. However, with the ever-increasing computational power of modern computers, there is a constant need for innovative approaches that can withstand the relentless advances in technology. Cryptography involves securing information through mathematical algorithms. It can be categorized into symmetric key cryptography (using a shared key) and asymmetric key cryptography (using public and private keys). DNA, the extraordinary molecule that encodes the essence of life, follows a set of profound coding rules. Discovered by Watson and Crick, these rules follow the pairing of nucleotides in the DNA double helix: adenine (A) with thymine (T) and cytosine (C) with guanine (G). Leveraging the power of these coding rules, along with operations such as addition, subtraction, and XOR, DNA based encryption unveils a new frontier in image security. By exploiting the unique properties of DNA, images can be transformed into intricate genetic codes, safeguarding their confidentiality through the ingenious fusion of biology and cryptography. This amalgamation of science and art promises to unlock novel possibilities in the realm of image encryption, where the language of life becomes a shield for digital secrecy. DNA based cryptography explores the use of DNA molecules for encryption, leveraging their unique properties for secure information storage and transmission. Due to the complexity of operations and peculiar properties, algebraic structures play a vital role in data security. Conventionally, algebra based schemes use finite Galois fields $(GF(2^n)$ for $2 \leq i \leq 8)$, symmetric groups and chain rings. Recently, non-associative algebraic structures have got attention for the applications in cryptography. Non-associative structures such as loops, LA-semigroups, LA-groups and

LA-rings have been used in developing robust cryptosystems. These non-associative algebraic structures possess some attractive properties such as; the complexity of their operation, invertibility of zero element, diversity in Cayley tables, and existence of various options.

Chaos, a non-linear dynamical system, has received a lot of attention and plays a crucial role from the point of view of application in a number of academic fields, including physics, engineering, and technology, etc. The ergodicity, unpredictability, strong sensitivity and dependence on the initial values and parameters make chaotic systems an ideal choice for a secure cryptosystem. Chaos, in the context of DNA, refers to the phenomenon of unpredictable behavior observed in certain DNA sequences. The intricate nature of DNA sequences, coupled with non-linear dynamics and feedback loops, can lead to chaotic patterns. Understanding and analyzing chaos in DNA sequences has implications in various fields, including bioinformatics and evolutionary biology. By studying chaotic behavior in DNA, researchers can gain insights into the complexity and dynamics of genetic information.

This study amalgamates the above mentioned three significant areas of cryptography to present a robust image encryption scheme that not only has a huge key space but also it can withstand many well-known attacks. The thesis comprises of three chapters.

Chapter 1 lays the foundation by providing a comprehensive overview of the fundamental concepts in cryptography, DNA, algebraic structures of LA-ring & LA-field, chaos theory, as well as image and image encryption. This chapter establishes the necessary background knowledge required to grasp the subsequent chapters and sets the stage for understanding the intricacies of DNA based encryption.

Chapter 2 presents the core of the research, an innovative encryption scheme tailored to the specific requirements and challenges posed by the chosen topic. Building upon the knowledge acquired in the previous chapter, a comprehensive encryption scheme is proposed that leverages the unique characteristics of DNA operations based on a non-associative LA-field. In this chapter, first a novel DNA affine transformation is defined, where the DNA operations coincide with the operations of a non-associative LA-field. A 3D-chaotic map with a strong chaotic behavior is introduced. Finally both the DNA affine transformation and the 3D-chaotic map are employed to construct a robust image cryptosystem, where both are responsible for the desirable properties of confusion and diffusion.

Chapter 3 is dedicated to the critical task of security analysis. Here, the newly suggested encryption scheme is subjected to a rigorous scrutiny, assessing its strengths, weaknesses, and vulnerabilities. Through a comprehensive security analysis, including differential attack analysis, histogram analysis, key space analysis, quality measure analysis, image quality measure analysis and texture analysis, the robustness and reliability of the proposed scheme is evaluated.

Lastly, the thesis offers a glimpse into some concluding remarks and some future directions are suggested.

Contents

Chapter 1

Introduction and Basic Definitions

An overview of the basic terms and concepts which are crucial to our research is given in this chapter. It not only aims to establish a common understanding of these terms but also discusses their historical context and theoretical frameworks with examples for clarification. The major focus is on basics of cryptography, DNA and DNA based cryptography, LA-ring, and LA-field. Chaos theory, image and image encryption are also included.

1.1 Cryptography

Greek etymology gives the word "cryptology," which means "secret word" . Cryptography and cryptanalysis are part of it. Ancient Egypt seems to be where cryptology's documented history first began (approximately 4500 years ago). Governments

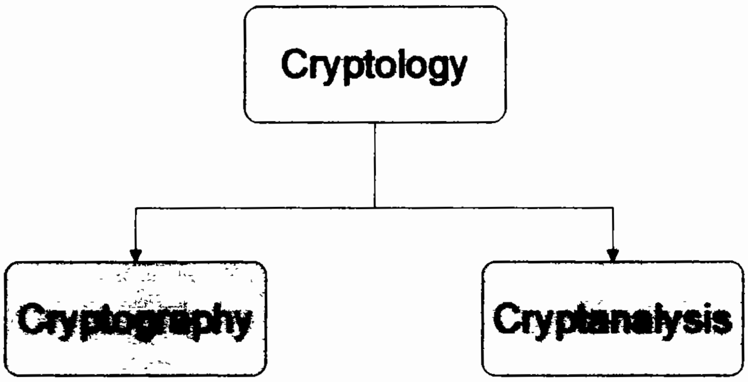


Figure 1.1: Cryptology

and the military mostly employ this art to protect sensitive information. Shannon's 1948 work [1] turned this practise into a science. It can be stated that this marks the beginning of modern cryptology, where maintaining the message's confidentiality is just as crucial as assuring its integrity and confirming the sender's identity. The rise of wireless communications in the 1920s may have accelerated the transition of cryptology from an art to a science. Yet, the advent of the computer era opened up regarding the study of cryptology. Cryptanalysis refers to the study of mathematical methods for attempting to undermine cryptographic algorithms.

The origins of the term "cryptography" are Kryptos, which means hidden in Greek, and Graphein, which means to write. Cryptography is the study of methods for altering a secret message such that only a designated recipient who has been given a secret key for deciphering may understand it. The message shouldn't be understandable if it is intercepted by an unauthorised recipient (let's call him the Enemy). A crucial technique that is used in electronic key systems for access control, document digital signatures, and data secrecy is cryptography [2]. It is the practice of securing communication from an unauthorized access or interception. Through encryption, decryption, and key management it is ensured that the information to be transmitted is only accessible by authorised parties. Cryptography has not only been used for centuries to protect sensitive information, but it also continues to be an essential tool in the modern digital age. The significance of cryptography is rising rapidly as the internet and electronic communication become more widely used. The major applications, include online banking, e-commerce, and secure messaging etc. Cryptography's evolution is ongoing, where new algorithms and methods are developed to stay ahead of potential threats.

1.1.1 Core Concepts in Cryptography

A scientific study must be based on precise definitions derived from fundamental ideas. The terms and basic principles that are utilized throughout the text of cryptography are listed here.

1. Plain Text

The plaintext refers to the original message. It is an original, logical communication or information.

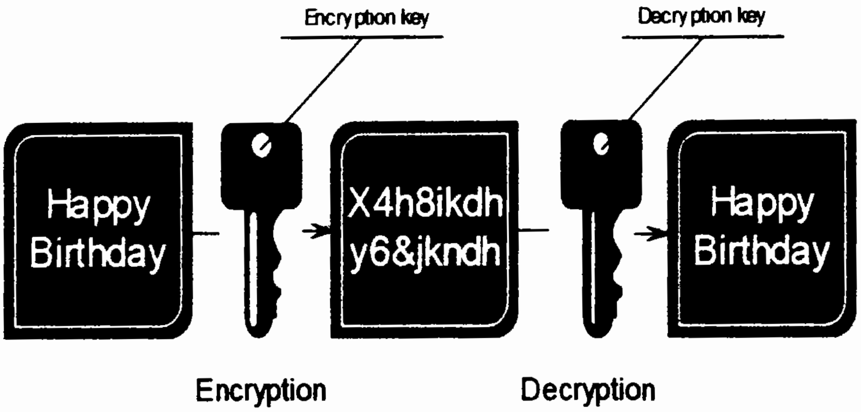


Figure 1.2: Encryption and Decryption

2. Cipher Text

The ciphertext refers to the message that has been altered and cannot be read.

3. Key

A key can be words, numbers, phrase or any combination of numbers or symbols, which encrypt or decrypt the plaintext. It regulates the process of encryption and decryption.

4. Encryption

The process of converting original text to enciphered text is called encryption or enciphering.

5. Decryption

Decryption or decoding refers to the process of converting ciphertext back into plaintext, which is carried out by the recipient with the necessary knowledge to reveal the disguised information.

6. Cipher or Cryptosystem

A cryptosystem or a cipher is a plan or method that uses a set of instructions to convert plaintext into ciphertext (and vice versa) so that data can be encrypted (decrypted). It refers to a cryptographic algorithm used to encode or decode data.

1.1.2 Branches of Cryptography

Asymmetric key cryptography and symmetric key cryptography are the two fundamental categories of cryptography [3].

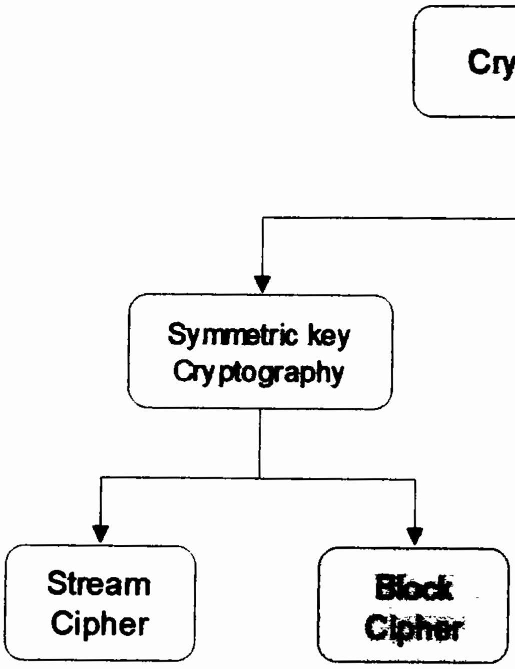


Figure 1.3: Branches of Cryptography

1. Asymmetric key cryptography

Asymmetric key cryptography, also known as the public key cryptography, is a cryptographic technique that uses a pair of mathematically related keys for encryption and decryption, which are respectively called the public key and private key. Although the two keys are mathematically interconnected, but it is computationally impossible to derive the private key from the public key. Hence the public key is freely distributed and can be used by anyone to encrypt messages. The private key is confidential, and only the recipient can know about it. RSA [4], Diffie Hellman [5], ECC [6], El Gamal [7], and DSA [8] are some asymmetric encryption algorithms. However, asymmetric encryption algorithms are computationally more expensive than symmetric algorithms, making them less suitable for encrypting large volumes of data.

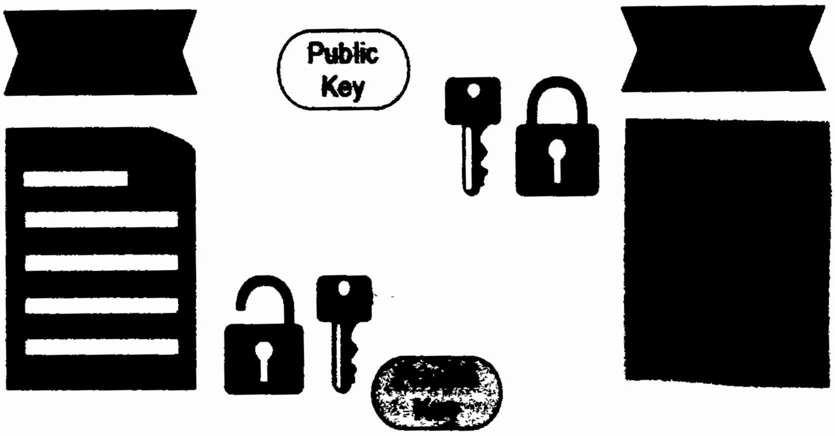


Figure 1.4: Asymmetric Key Cryptography

2. Symmetric Key Cryptography

A cryptographic technique that uses a single key for both encryption and decryption of data is the symmetric key cryptography, also known as secret key cryptography. In it, a secret key is generated by a trusted entity and shared securely between the communicating parties. The key must be kept confidential, as the encrypted data may be decrypted by anyone with access to the key. Key distribution, storage, and rotation should be carefully handled to prevent unauthorized access or compromise. This type of cryptography is computationally efficient, making it suitable for encrypting large volumes of data. The symmetric encryption and decryption algorithms are typically fast and require fewer computational resources compared to asymmetric key cryptography. It's commonly used in a wide variety of applications, including secure communication channels, encryption of data, file and disk encryption, secured network protocols, and securing data at rest.
Stream cipher and block cipher are two types of symmetric algorithms.

i) Stream Cipher

A stream cipher is characterized as a symmetric encryption algorithm that encrypts plaintext in a sequential manner with one bit at a time is being processed. They are designed to be fast and efficient, making them suitable for real-time encryption and communication systems. Ceaser cipher and vigenere cipher are examples of the stream cipher [9].

ii) Block Cipher

A block cipher is another type of symmetric encryption algorithm that oper-

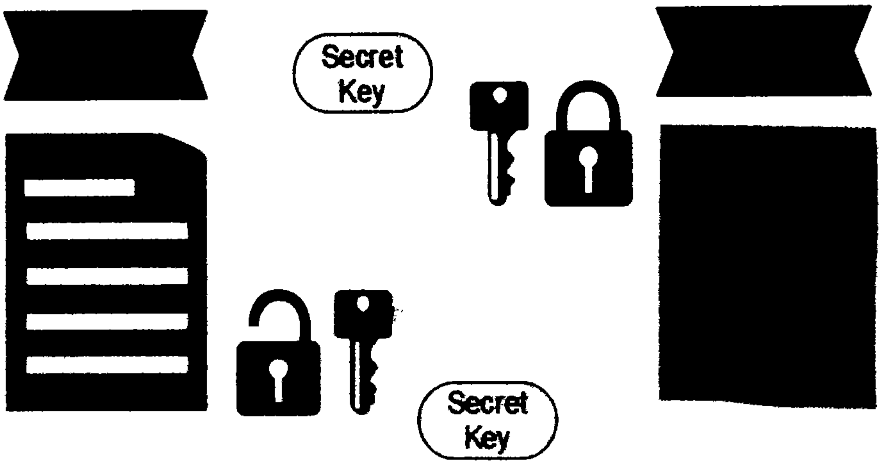


Figure 1.5: Symmetric Key Cryptography

ates on fixed-length blocks of the original text, typically consisting of multiple bytes. It breaks the plaintext into blocks of equal size and encrypts each block independently. Block ciphers are widely used in various encryption standards and protocols. Common block sizes include 64 bits (as in DES) and 128 bits (as in AES). The security and performance of the cipher are influenced by the choice of block size. The size and strength of the encryption keys are decisive to the security of a block cipher. Block ciphers usually require longer keys compared to stream ciphers. They are designed to be resistant to various cryptanalysis techniques, including brute-force attacks and differential or linear cryptanalysis. Data encryption standard DES, triple DES (3DES or TDEA), and advanced data encryption standard AES are some examples of block ciphers. AES (Advanced Encryption Standard) and DES (Data Encryption Standard) are two extensively used symmetric block ciphers. They are encryption algorithms that work only on fixed size blocks of data.

a) DES (Data Encryption Standard)

DES [10] is a symmetric block cipher that was widely used as a standard encryption algorithm in the 1970s and 1980s. It was developed by IBM and the U.S. government adopted it as a standard for encryption. However, due to advances in computing abilities and the increased vulnerability to brute-force attacks, DES is now considered relatively weak and has been largely replaced by AES. DES uses a 56-bit encryption key. It operates on fixed-size blocks of 64 bits, and uses 16 rounds of encryption steps. A Feistel network structure is employed in DES, which involves splitting the plaintext into two halves and multiple rounds of substitution and permutation operations are carried out.

b) AES (Advanced Encryption Standard)

The National Institute of Standards and Technology (NIST) chose the symmetric block cipher AES [11] as the standard encryption algorithm for securing sensitive information in 2001. Three key sizes are supported by AES: 128 bits, 192 bits, and 256 bits. The encryption strength and algorithmic security increases with the size of the key. Depending on the size of keys, it uses a different number of encryption rounds: 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys, and operates on fixed-size blocks of 128 bits. AES employs a substitution-permutation network (SPN) that combines substitution and permutation operations to achieve confusion and diffusion in the encrypted text.

1.1.3 Properties of a Secure Cryptosystem

The two properties of a secure cryptosystem identified by Claude Elwood Shannon [1] are confusion and diffusion. These two properties work together to counter many cryptanalytic attacks.

2. Confusion

Confusion is a technique which aims to make the relationship of plaintext and encrypted text as complicated as possible. In confusing a message, the goal is to make it challenging for an attacker to extract information about the plaintext from the ciphertext. The majority or all of the bits in the encrypted text will change if even one bit in the key is altered. Confusion is usually achieved by substitution.

1. Diffusion

Diffusion is a technique used to spread the information of the plaintext as widely as possible throughout the ciphertext. In diffusion, each ciphertext symbol is typically influenced by multiple plaintext symbols. Thus, altering a single bit in the plaintext will lead to multiple changes in the encrypted text to conceal the message's contents. Permutation is a source of diffusion in a cryptosystem.

1.1.4 Objectives of Cryptography

Cryptography is the science of making communications secure by encoding messages so that only the intended recipient is able to understand them. The objectives of cryptography are to provide confidentiality, integrity, non repudiation and authentication to data and communications.

1. Confidentiality

Confidentiality means that information is kept secret from individuals who are not authorized to view or access it. It is one of the primary objectives of cryptography, which enables the protection of sensitive information during transmission across a network and is achieved through encryption.

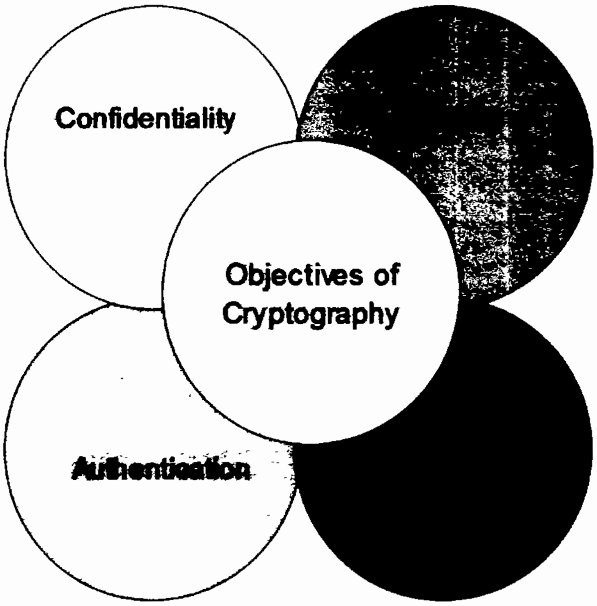


Figure 1.6: Objectives of Cryptography

2. Integrity

Integrity means that data is protected against unauthorized modification, adding, or deleting by using techniques such as message digests and digital signatures. A message digest is a hash code created by applying a mathematical transformation to the original message. Thus, if someone alters the message, the hash code will be different, and the receiver will know that it has been tampered with. Similarly, a digital signature is a method used to verify the sender's identity and the integrity of the message.

3. Authentication

Authentication means verifying that the individual or entity is who they claim to be. In cryptography, authentication is achieved through the use of digital certificates, public and private keys, and digital signatures.

4. Non-repudiation

Non-repudiation is the ability to ensure that the senders of a message cannot deny sending the message. Digital signatures provide non-repudiation because they provide a unique identifier of the sender, and once the message is sent, the sender cannot deny sending it.

1.2 Deoxyribonucleic Acid (DNA)

DNA is an organic compound that has a unique molecular structure. DNA is a set of molecules that is in charge of transporting and transferring hereditary elements or genetic instructions from parents to their offspring's. DNA has instructions for how to put cells together. A human cell contains the entire DNA sequence and each person has a different DNA. The DNA structure defines the basic genetic makeup of a living being.

1.2.1 Structure of DNA

In 1869, while studying white blood cells, a Swiss researcher named Johannes Friedrich Miescher [12] discovered and identified DNA. Nucleic acids in all organisms that take the form of DNA or RNA are organic molecules. These nucleic acids consist of nitrogenous bases, sugar molecules and phosphate groups that are bound together by a series of linkages. The arrangement of nitrogenous bases determines the genetic code or DNA instructions. Deoxyribo nucleotides are the monomers

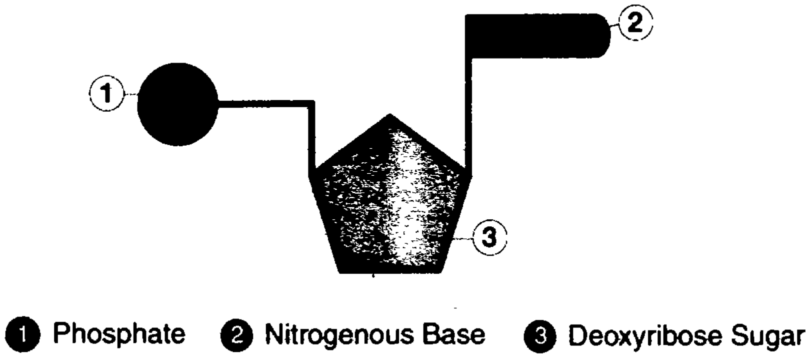


Figure 1.7: Basic Components of DNA

that make up the polymer DNA. Each nucleotide is made up of three fundamental components: a nitrogenous base, a phosphate group, and deoxyribose sugar. There are two different kinds of nitrogenous bases: pyrimidines and purines (Adenine and Guanine), (Cytosine and Thymine). They are denoted by the letters A, G, C, and T. T binds to A, while G binds to C. For the DNA double helix structure, which resembles a twisted ladder, these base pairs are crucial. The two DNA strands run in opposing directions and the hydrogen connection that exists between the two complimentary bases holds these strands together.

1.2.2 DNA based Cryptography

DNA cryptography is a relatively new field that merges the disciplines of cryptography and molecular biology. It is a promising and rapidly developing topic in data security. In order to encode information, standard binary data uses two numbers '0' and '1'. However, data is encoded by four bases viz: Adenine(A), Guanine(G), Cytosine(C) and Thymine(T) in DNA molecules, which are the natural transporter of information. This approach use DNA sequences as cryptographic keys and employs encoding and decoding algorithms to transform plaintext into DNA sequences and vice versa. Various research projects are being carried out around the world to either improve existing DNA cryptography procedures or to offer innovative and novel approaches in this domain. DNA substitution and One-Time Pad, steganography using DNA microdots, DNA cryptography using binary strands, symmetric key, asymmetric key DNA cryptosystem and signature method, triple stage DNA cryptography, and chaos with DNA are the emerging topics in DNA based cryptography. It offers advantages such as high information density, potential resistance to quan-

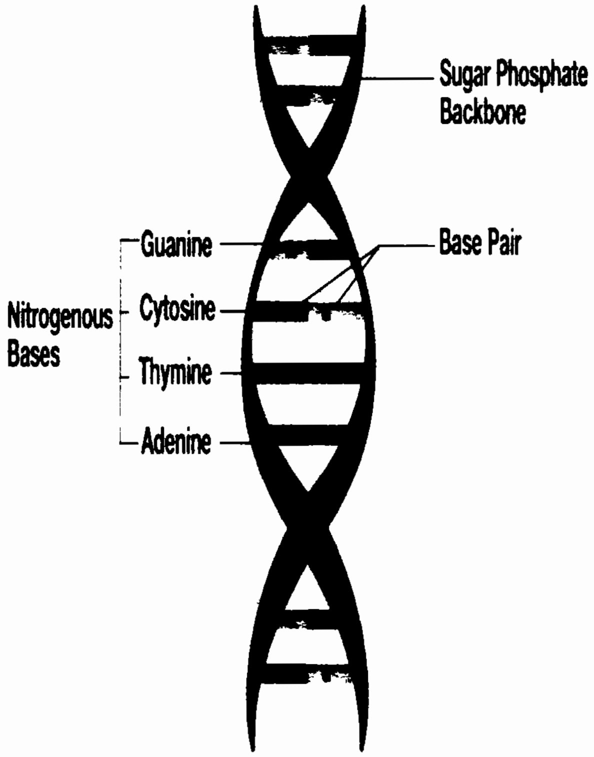


Figure 1.8: Double Helix Structure of DNA

tum computing attacks, and the ability to store large amounts of data efficiently. This field of study has potential applications in secure communication, data storage, authentication, and cryptographic key management systems. It can be further studied from [13–15].

1.2.3 Encoding and Decoding using DNA Principles

During DNA formation '*A*' has to join '*T*' and '*G*' has to be paired with a '*C*'. They are considered to complement of each other, and this is called Watson Crick Complement model [16]. In binary numbers, '0' and '1' are complements of each other. Accordingly '11' and '00' , '10' and '01' are complements. There are 4! = 24 bijective mappings of the four bases '*C*', '*G*', '*A*' and '*T*' to '01', '10', '00' and '11'. These are called DNA encoding rules and out of these 24 rules, only 8 satisfy the Watson-Crick complement model. These rules are listed in Table 1.1.

In digital communications, data is transmitted in form of bytes. Bytes have decimal

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

Table 1.1: DNA Rules

values between 0 and 255. It is not difficult to encode and decode a byte to transform it. For instance 185 has the binary representation '10111001'. As per Rule 5, the corresponding DNA sequence is '*GAGC*'. Now from Table 1.1, according to rule 7, '*GAGC*' is equal to '11011100' in binary having decimal value 220, the transformed byte. While decoding, the DNA rules are used in reverse to get the pixel values.

1.2.4 DNA Operations

DNA operations based on those of Z_4 (also known as the 4-bit DNA system) are used in DNA computing to perform computations using DNA sequences. The DNA nucleotides are usually considered to represent elements of the modular ring $Z_4 = \{ 0, 1, 2, 3 \}$ and follow the operations modulo 4. '*C*', '*T*', '*A*', and '*G*' are usually mapped onto '0', '1', '2', and '3' respectively. Basic DNA operations are DNA addition, DNA subtraction and DNA XOR.

1. DNA Addition

DNA addition follows the addition modulo 4 operation. Table 1.2 is the DNA addition table.

+	C	T	A	G
C	C	T	A	G
T	T	A	G	C
A	A	G	T	C
G	G	C	T	A

Table 1.2: DNA Addition

2. DNA Subtraction

DNA subtraction follows the subtraction modulo 4 operation is described by the Table 1.3.

-	C	T	A	G
C	C	G	A	T
T	T	C	G	A
A	A	T	C	G
G	G	A	T	C

Table 1.3: DNA Subtraction

3. DNA XOR

For the DNA XOR operation, two DNA bases are converted into binary using DNA encoding and then bit wise XOR operation is performed. Table 1.4 depicts the XOR operation when *C*, *T*, *A*, and *G* are encoded to 00, 01, 10 and 11 respectively.

⊕	**C = 00**	**T = 01**	**A = 10**	**G = 11**
C = 00	C	T	A	G
T = 01	T	C	G	A
A = 10	A	G	C	T
G = 11	G	A	T	C

Table 1.4: DNA XOR

1.3 Algebraic Structure of Non-Associative LA-Field

Prior to the middle of the 19^{th} century, associative and commutative structures, were the only ones to be considered in the study of rings and algebras and some times the study limited to associative structures only. Numerous non-associative variants have been used since the middle of the 19^{th} century. Octonions, Lie structures, Jordan algebras, Lie algebras, alternative rings, loops, and loop rings are a few examples.

With connections to other branches of Mathematics and some areas of sciences, such as Biology, Physics, and Computer science etc, non-associative ring theory has thrived as a flourished area of algebra.

In 1972 Kazim and Naseeruddin [17] were the first to introduce the left almost semigroup (LA-semigroup), also known as an Abel Grassman-groupoid (AG-groupoid), which is a groupoid with the left invertive law $(st)u = (ut)s$. Left almost groups (also known as LA-groups or AG-groups) were first presented by Mushtaq and Kamran in 1996 [18] as an LA-semigroup with left identity and all elements invertible. The left identity would be referred to as the left zero element in the case of an additive LA-group. Furthermore, Shah and Rehman [19] generalized the notion of an LA-group to establish a non-associative and non-commutative ring called a left almost ring (LA-ring). An LA-ring $(R, +, \cdot)$ is an additive LA-group and a multiplicative LA-semigroup. The two operations are combined via distributive laws. Shah and Shah in their article [20], introduced an LA-field as an LA-ring whose nonzero elements form a multiplicative LA-group. In [21], Rehman et al. proved the existence of a non-associative LA-ring and provided examples of some finite LA-rings and LA-fields. They also introduced special LA-rings as an LA-rings which are additive abelian groups. Thus a special LA-field can be defined as a special LA-ring that is an LA-field.

1.4 Chaos

The two meanings of chaos that are most frequently used are: a condition of nature that is absolutely devoid of order, and severe confusion or disorder connected to unpredictable action. The latter, the dynamic as opposed to the static, is the more well-liked and appropriate of the two of the chaos theory in mathematics. Chaos refers to a branch in mathematics and physics that deals with the deterministic behaviour of complex systems which exhibit unpredictable behaviour, characterised by delicate reliance on initial conditions and non linear dynamics.

1.4.1 Characteristics of Chaotic Maps

When evaluating and designing chaotic maps, there are several parameters or characteristics that are considered desirable for good chaotic behavior. Here are some important parameters to be considered.

1. Sensitivity to Initial Conditions

A good chaotic map should exhibit sensitivity to initial conditions, i.e, small changes in the initial state or input values should lead to significantly different trajectories or outputs. Sensitivity to initial conditions is a fundamental aspect of chaos and contributes to the unpredictability and complexity of the system.

2. Mixing and Ergodicity

Mixing refers to the property of a chaotic map where nearby points in the phase space become widely separated over time, ensuring that the system explores the entire phase space. Ergodicity implies that the system explores all possible states with equal probability, ensuring that the chaotic behavior covers the entire range of possible values.

3. Chaotic Attractors

Chaotic maps often exhibit attractors, such as strange attractors or fractal structures, which represent the long-term behavior of the system. Good chaotic maps may possess attractors with desirable properties, such as complexity, a large number of points, and sensitivity to initial conditions.

4. Nonlinearity

Nonlinear dynamics are a key characteristic of chaotic maps. Nonlinear equations capture the complex interactions and feedback loops that lead to chaotic behavior. Good chaotic maps should have sufficiently nonlinear equations or iterative rules to produce intricate and unpredictable behavior.

1.4.2 Chaos Evaluation Tools

Bifurcation diagrams and Lyapunov exponents serve as crucial evaluation tools for analyzing chaotic systems.

1. Bifurcation Diagram

A bifurcation diagram [22] is a graphical representation that illustrates how the behavior of a dynamic system changes as a control parameter is varied. It represents transitions and bifurcations within the system. The horizontal axis represents the parameter being adjusted, which could be a physical or numerical value. The vertical axis represents system behavior, often shown through a specific variable or an indicator like stability or chaos. Bifurcation points on the diagram indicate qualitative shifts in system behavior, such as stability, periodicity, or chaos. Multiple branches on the diagram depict different stable or unstable states of the system, which can undergo splitting, merging, or complex patterns as the parameter is modified. Bifurcation diagrams offer insights into dynamic system behavior, revealing phenomena like chaotic behavior and periodic windows.

2. Lyapunov Exponent

Lyapunov exponents [23] are a quantitative measure of the sensitivity to initial conditions, providing a way to quantify the chaotic behavior of a system. They quantify the average rate of time dependent divergence or convergence of neighbouring phase space trajectories. Positive Lyapunov exponents indicate exponential divergence of nearby trajectories, indicating chaotic behavior. Negative or zero Lyapunov exponents indicate convergence or stability, respectively. The largest Lyapunov exponent is of particular interest as it characterizes the overall rate of divergence of nearby trajectories and provides a measure of the system's predictability or unpredictability. The computation of Lyapunov exponents involves analyzing the evolution of infinitesimally close trajectories and calculating the growth rates of their separations. They provide a numerical measure of chaos, helping to quantify the inherently unpredictable and sensitive nature of initial conditions in chaotic systems.

1.4.3 Chaotic Systems

Chaotic systems are classified into two categories.

1. Discrete

Discrete chaotic maps describe systems that evolve in discrete time steps. Examples of discrete chaotic maps include the logistic map [24], the tent map [25], Arnold's cat map [26], Baker's map [27], and the Henon map [28]. These maps exhibit chaotic behavior through processes such as period doubling, bifurcations, and strange attractors.

2. Continuous

Continuous chaotic maps describe systems that evolve continuously over time. Examples of continuous chaotic maps include the Lorenz system [29], the Rossler system [30], and the Chua circuit [31]. These maps often involve differential equations and exhibit complex behaviors such as the presence of strange attractors and sensitivity to initial conditions.

1.4.4 Chaos in Cryptography

Chaos theory has been employed in various cryptographic applications to enhance security and randomness. Chaotic systems produce pseudo-random numbers crucial for encryption keys and other cryptographic parameters. They can be utilized in stream ciphers, combining chaotic dynamics with other techniques for secure encryption algorithms. The sensitivity to initial conditions and complex dynamics of chaos contribute to the robustness and unpredictability of chaos-based cryptographic schemes. It's important to note that research is ongoing in chaos theory's applications in cryptography and image encryption, with constant advancements and algorithms being developed to improve security and performance. The articles [32–35] are recommended to delve deeper into chaos theory and its applications in cryptography and image encryption.

1.5 Image and Image Encryption

The Latin word imitari, meaning "to copy or imitate", is the origin of the image; the image is judged by how realistic it is of the person or object it shows. An image is a depiction in art of the outer appearance of an object. It's an array or a matrix of pixels that are placed in columns and rows; each pixel contains either colour or grayscale information. Some of the types of image are given below.

1. Binary Image

It consists of pixels that can take only two possible values: black and white. Each pixel represents a single bit of information. It is Widely used in image analysis, object recognition, and computer vision tasks.

2. Grayscale Image

It is an image using varying shades of gray ranging between 0 - 255. Each pixel typically contains a single intensity value representing brightness. These images are used in scenarios where color information is not required, such as medical imaging or certain types of document processing.

3. RGB Image

An RGB image is a digital image representation composed of red, green and blue color channels. Each pixel is defined by the intensity values of these color channels ranging between 0 - 255. Several combinations of red, green and blue gives a wide range of colors so it is commonly used in digital displays and photography.

4. Indexed Color Image

This type of image use a limited set of colors defined in a color palette. Each pixel contains an index value that refers to a specific color in the palette. These are Often used in computer graphics, icon creation, and web design.

5. Multispectral / Hyperspectral Image

It is an image that captures information across multiple spectral bands or wavelengths. Each pixel contains data from multiple bands, providing detailed spectral information. It is Used in remote sensing, environmental monitoring, and scientific research.

Image encryption [36] is a process that uses a secret key to transform a plain image into a distorted image to protect its confidentiality and integrity. It ensures that unauthorized individuals cannot access or comprehend the original content of the image. The process of decryption converts the cipher image back into the original form. Image encryption techniques are based on a variety of concepts, including the Substitution box, Chaos, and DNA. Image encryption can be further studied from [37–39].

1.5.1 Chaos based Image Encryption

For the encryption of images, chaos theory has been widely applied to provide a secure and robust encryption algorithm [40]. In order to achieve a higher level of security, the chaotic properties of nonlinear dynamic systems are used to encrypt images. Encryption keys or masks are generated by some chaotic systems and are used to transform the image pixels. Image pixels are scrambled in such a way that the image appears random.

1.5.2 DNA based Image Encryption

DNA-based image encryption [41] is an emerging field of cryptography that utilizes the properties of DNA molecules for encryption purposes. It takes advantage of the four nucleotide bases (adenine, thymine, cytosine, and guanine) present in DNA to represent binary information. Encryption techniques which are based on DNA offer advantages such as massive data storage capacity, parallel processing capability, and robustness against attacks. These techniques involve encoding image pixels or encryption keys into DNA sequences and leveraging DNA operations for encryption and decryption processes.

1.5.3 DNA and Chaos based Image Encryption

Combination of DNA coding and some chaotic systems in image encryption is a rapidly developing field [42]. DNA coding is used to create diffusion, whereas chaotic systems performs confusion in encryption process. This approach utilizes DNA computing principles and chaotic dynamics to ensure the security of digital images. This innovative approach leverages the inherent complexity and randomness of DNA sequences and chaotic dynamics to achieve robust encryption and decryption algorithms.

Chapter 2

RGB Image Encryption Scheme

This chapter provides a detailed literature survey on existing encryption schemes focusing on DNA based cryptography. A novel 3D - chaotic map is proposed. Furthermore an LA-field based DNA affine transformation is defined and secure image encryption scheme utilizing the chaotic map and affine transformation is presented.

2.1 Literature review

In this section, a comprehensive literature review focusing on DNA based cryptography. By critically analyzing the literature, key trends, challenges, and potential areas for further exploration are aimed to be identified. This review serves as a foundation for novel approach in utilizing DNA based techniques for the encryption purpose. DNA based cryptography, a cutting-edge field at the intersection of biology and cryptography, utilizes DNA molecules' exceptional characteristics for developing novel encryption techniques and enhancing data security. In recent years, this technique has gained significant attention due to its potential advantages over traditional cryptographic methods. Research in DNA based cryptography is a relatively new field, and the first studies in this area began to emerge in the late 1990s. Since then, there has been a growing interest in this field, and a significant amount of research has been conducted by various scientists and research groups worldwide.
Adleman [43] the pioneer of DNA computing in 1994, proposed the first ever DNA based encoding and decoding. Since then, several studies have been conducted to develop more robust and secure DNA based encryption methods. In recent years, with the advancement of technologies such as next generation sequencing and syn-

thetic biology, there has been a renewed interest in this field, and several research groups are exploring the potential applications of DNA based cryptography in various fields such as secure communication, data storage, and biometric authentication. In 1999, Gehani et al. [44] presented a potential cryptosystem utilising DNA molecules, by creating a one-time pad encryption approach. Later in the year 2000, Gehani et al. [45] and Leier et al. [46], performed some more experiments utilizing the properties of DNA molecules to offer more resillient cryptosystems. Risca [47] in the year 2001 presented an implementation of steganography using DNA molecules. Yang [48] proposed a simple generalized group-oriented cryptosystems using ElGamal cryptosystem in 2003. In 2007 MingXin et al. [49], suggested a DNA cryptosystem based on micro array technology. Furthermore G. Cui et al. [50] and Wang et al.[51] proposed an image encryption approach based on the DNA sequence addition operation in the year 2008 and 2009. In the study [52] in 2010 Borda presented DNA secret writing techniques using One-Time-Pad (OTP), DNA XOR OTP and DNA chromosomes indexing technologies. Lai et al. [53], in the year 2010 developed an asymmetric-key DNA cryptosystem and signature mechanism, using DNA micro array technology, the scientists created DNA-PKC. In the year 2012, Zhang and Xue, [54] introduced a unique image encryption technique based on the operation of DNA sub sequences. In order to scramble the position and values of pixel points in an image, these operations have been combined by them with a logistic chaotic map. Later in 2013, Soni et al. [55] developed a novel DNA cryptography technique based on the Moore machine notion from automata theory. Zhang and Fang, [56] in the year 2014 introduced a technique for the encryption of images using both chaotic maps as well as DNA sequences. Ibrahim FE [57] in the year 2015 proposed a method for using double DNA sequences to make data hiding more secure. In the year 2017 Zhang et al. [58] proposed a DNA based cryptographic scheme for information security. The scheme used DNA sequences to encode and decode messages and a set of specific enzymes for the decoding process. Furthermore in the year 2018 Wu and Liao [59] presented 2D Hénon-Sine map and DNA approach based image encryption. Later, Zhang et al. [15] in 2019, developed DNA origami cryptography (DOC) which secures communication by folding an M13 viral scaffold into nanometer-scale self-assembled braille-like patterns. In the year 2020, Tanveer and Shah [60] presented a novel colour multiple image encryption approach based on a algebra-chaos amalgamated 256-length-12-bit random sequence and the DNA transform. Later in 2020, Kumar et al. [38] provided a comprehensive overview of DNA-based steganography and cryptography. They discussed the various approaches used for encoding and decoding information using DNA sequences and their applications. Furthermore, In 2021 Firdousi et al. [61] presented Parent daughter confusion component. He used deoxyribonucleic acid (DNA) sequences to build S boxes which was a new method for creating nonlinear confusion components. In the year 2021, a new four dimensional memristive hyperchaotic system based on the Liu chaotic framework was developed with the introduction of a fluxcontrolled memristor model by Yang, et al. [62]. Aljazaery [63], in 2022 provided a novel way for encoding 2D and 3D colour pictures. The approach was structured using the DNA strand building as a foundation. Recently in 2023 Ahmed et al. [64] presented a DNA based colour image encryption scheme using a convolutional auto encoder. In the same year Das and Sanyal [65] proposed a colour medical image encryption approach based on DNA coding.

In our proposed work, LA-field based DNA affine transformation is suggested, also novel chaotic map is introduced which named as 3D - NK chaotic map. An efficient algorithm is described utilizing the non-associative structure of LA-field and sequences generated from newly design chaotic map. both the chaotic map and affine transformation create confusion as well as diffusion. The combination of algebra chaos and DNA ensures that the encrypted image is highly resistant to unauthorized access and decryption attempts. Due to non-associative behaviour of the algebraic structure used along with chaotic behaviour shown by NK map, significant results are achieved. The novel image encryption scheme offers remarkable advancements in image security and holds the potential for the various benefits in the field of image encryption.

2.2 Core Components of the Encryption Scheme

This section highlights the integration of three significant components within our encryption scheme: a non-associative LA-field, a novel LA- field based DNA affine transformation, and a novel 3D chaotic map. These elements are strategically combined to enhance the security and efficiency of the encryption process.

2.2.1 Non-Associative LA-Field under Consideration

In this section the particular example of LA field R is presented. A software MACE 4 [66] is used to obtain some examples of non-associative special LA-rings and found that the smallest possible order of a special LA-ring is 4. In particular, an example of a non-associative LA-field $R = \{0,1,2,3\}$ of order 4 is obtained. Which is shown in Table 2.1. From the Table 2.1 it is clear that all the properties of LA-field are being satisfied, 1 is the zero element and 2 is the left identity. It is not difficult to see that R is non-associative, as $0 \cdot (0 \cdot 0) \neq (0 \cdot 0) \cdot 0$.

+	0	1	2	3
0	1	0	3	2
1	0	1	2	3
2	3	2	1	0
3	2	3	0	1

(a) Addition

·	0	1	2	3
0	2	1	3	0
1	1	1	1	1
2	0	1	2	3
3	3	1	0	2

(b) Multiplication

Table 2.1: Operations of Non associative LA-Field

2.2.2 Proposed LA-Field based DNA Affine Transformation

In this section, a novel technique to use DNA encoding and decoding for image encryption is introduced. Conventionally, DNA encryption depends on the DNA operations from the modular ring Z_4 or DNA XOR operation. Here a DNA affine transformation is defined that utilizes the operations of addition and multiplication from the non-associative LA-field of order 4. When an RGB image is considered, its pixel values for each layer range with in '0' and '255', that is a byte. DNA encoding is used to convert each pixel into a sequence of 4 characters from the set $\{A, C, G, T\}$. A bijection from the set $\{A, C, G, T\}$ onto the LA-field $R = \{0,1,2,3\}$ converts the sequence of nucleotides into a sequence of elements in R. Now it becomes possible to add or multiply any two pixel values using the operations of LA-field component wise. Let 'a' and 'b' be fixed integers between '0' and '255'. For any pixel value x, $x \mapsto xa + b$ is a bijection on the set $\{0,..,255\}$ with inverse, $x \mapsto xa^{-1} - b$. Here 'a^{-1}' is the component wise multiplicative inverse of 'a' and '-b' is the component wise additive inverse of 'b'. Finally, the resulting sequences of elements in R are converted to DNA sequences and then to bytes using some bijection and a DNA rule respectively. Bytes are then converted into integer values of the pixels.

2.2.3 Novel 3D Chaotic Map

This section proposes a discrete chaotic map for an image encryption system which is more efficient. Chaos refers to a complex and unpredictable behavior that arises in certain dynamical systems. It is characterized by extreme sensitivity to initial conditions, non-linear dynamics, and a lack of long-term predictability.
The subsequent equations represent the suggested NK chaotic map.

$$\begin{aligned} x_{(i+1)} &= u^m cos(x_i) + y_i - v^m sin(z_i) \\ y_{(i+1)} &= cos(x_i).sin(y_i + x_i + tan(z_i)) \\ z_{(i+1)} &= y_i^m sin(i) + x_i cos(i) - f^m tan^{-1}(z_i) - c \end{aligned}$$

In the above equations; the variables are x, y, and z, control parameters are u, v, f and c, and i, m are non negative integers being m represents the exponent. For a specific set of initial values and control parameters, every chaotic system shows chaotic behaviour. Figure 2.1 shows the bifurcation diagram of the NK chaotic map, which clearly indicates a strong chaotic behaviour. The Lyapunov exponent is a key factor in determining whether the chaotic map is practical for cryptography.

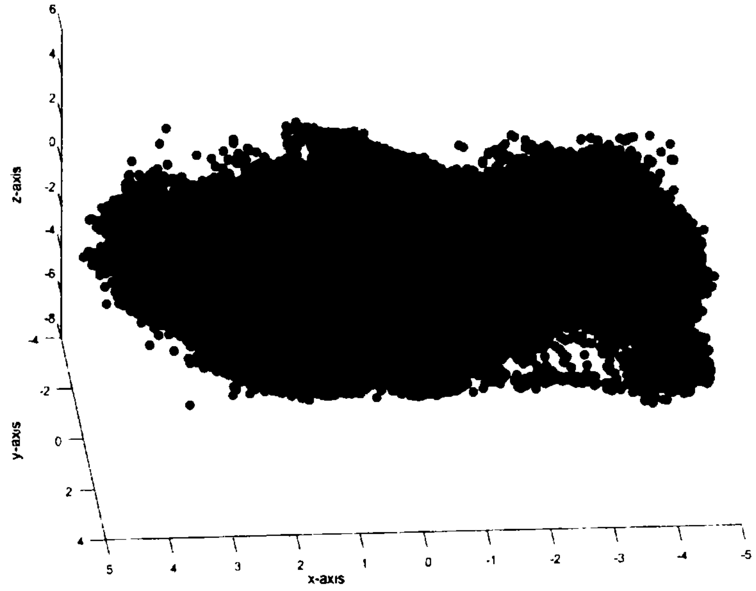


Figure 2.1: Bifurcation diagram of NK chaotic map

The seed parameters, such as the control parameters and initial conditions , exhibit significant sensitivity for this exponent. The values of Lyapunov exponent for the NK map are given in Table 2.2. It is obvious that Lyapunov exponent values are positive , so the behaviour of the system is chaotic.

Figure 2.2 , Figure 2.3 and Figure 2.4 shows 1D , 2D & 3D plots for the chaotic attractor of the NK map respectively.

Variables	Lyapunov exponent values
X	17.923250
Y	18.274127
Z	18.323939

Table 2.2: The Lyapunov exponent values of variables of NK chaotic map

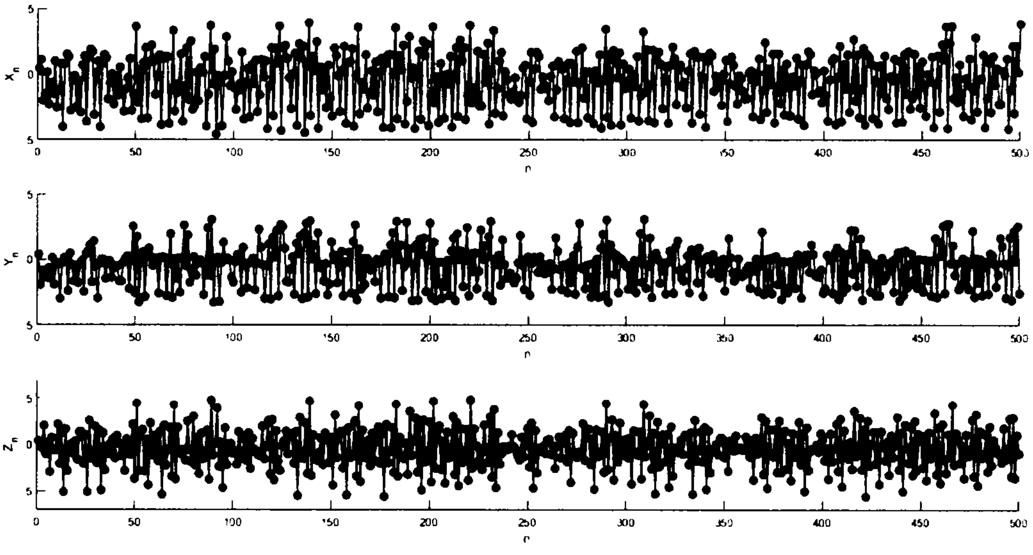
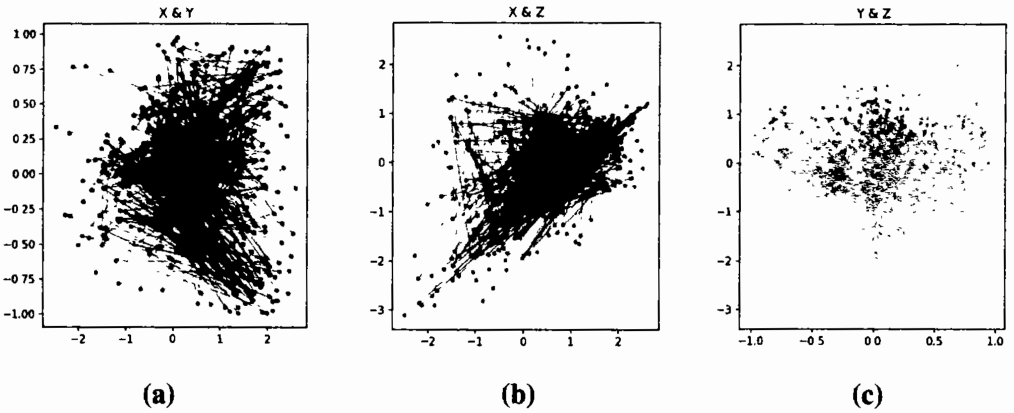


Figure 2.2: 1D attractors of NK chaotic map

The 0 – 1 Randomness Test

The 0 – 1 test is one way for determining a dynamical system's chaotic behaviour. This test can also be used instead of the Lyapunov exponent. To determine the unpredictability of a chaotic system, phase space reconstruction is required for calculating the Lyapunov exponent. Whereas, The time series $\gamma(d)$ for $d = 1, 2, 3,....$ is



(a) (b) (c)

Figure 2.3: 2D attractors of the NK chaotic map

required for the $0-1$ test to determine the chaotic behaviour of a dynamical system. The two dimensional system is derived from the $0-1$ test to measure the unpredictability of a chaotic system by using $\gamma(d)$ for $d = 1, 2, 3, \ldots.$

$$t(d+1) = p(d){+}\gamma(d+1)cos(sd)$$
$$q(d+1) = q(d)+\gamma(d+1)sin(sd)$$

where s is fixed and is in $(0, 2\pi)$. The system's mean square displacement is:

$$R(d) = \lim_{D\to\infty} \frac{1}{D} \sum_{k=1}^{D} ([t(k+d)-t(k)]^2 + [q(k+d)-q(k)]^2), d = 1, 2, 3, \ldots.$$

Whereas its rate of growth can be calculated as:

$$S = \lim_{d\to\infty} \frac{\log(R(d))}{\log(d)}$$

If the value of S is close to zero, the system is consistent, and the system is chaotic, if it is close to one. The findings of the x, y, and z components of the NK chaotic system are shown in the Table 2.3. Its demonstrates that all three series have $0-1$ test values close to 1. It follows that the NK system exhibits chaotic behaviour.

2.3 The Encryption Procedure

To avoid the insecurities in DNA based image encryption schemes, a novel encryption technique is proposed using a proposed DNA affine transformation based on

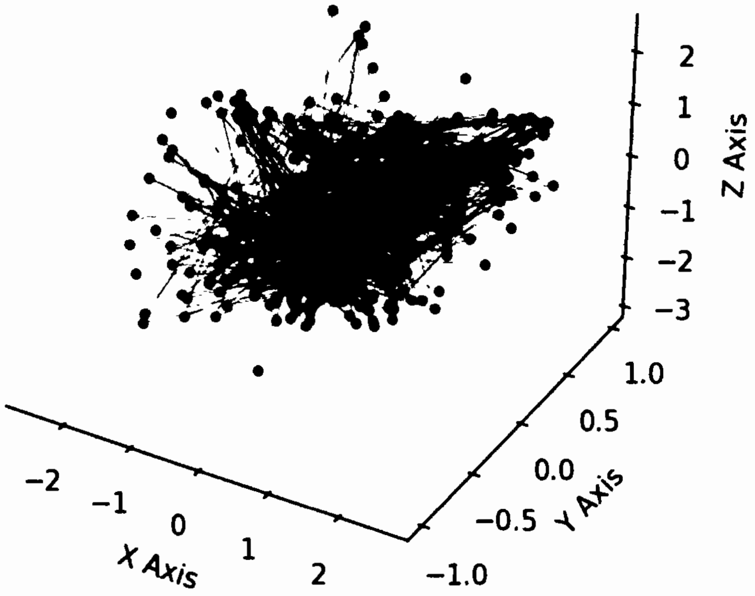


Figure 2.4: 3D attractor of the NK chaotic map

Sequences	values
X	0.9977
Y	0.9975
Z	0.9989

Table 2.3: 0-1 test of the NK chaotic map

the operations from non-associative LA-field and the newly introduced 3D chaotic system. The scheme encompasses only few steps and hence ensures efficiently the secure transformation of images.

Algorithm

Step 1 : Consider an RGB image of size $M \times M$ and split it into red, green and blue layers.

Step 2 : Generate three sequences x_1, x_2, x_3 of size $M \times M$ from the NK chaotic map. Extend and enfold the values of x_1, x_2, x_3 with in the range 0-255 by using the equation given below. Arrange these values in three $M \times M$ matrices and name them C_1 , C_2 and C_3 respectively.

$$s_i = round((ceil(abs((q_j \times 10^{15})))mod\ 256)\ \ \forall q_j \in x_i,\ \ j = 1,2,3,..........M \times M,\ i = 1,2,3$$

Step 3 : Define three LA-field based DNA affine transformations as:

$$\begin{aligned} \alpha_1 : x &\longrightarrow x a_1 + b_1 \ , \ where\ a_1 = 205\ ,\ b_1 = 117 \\ \alpha_2 : x &\longrightarrow x a_2 + b_2 \ , \ where\ a_2 = 247,\ b_2 = 216 \\ \alpha_3 : x &\longrightarrow x a_3 + b_3 \ , \ where\ a_3 = 69,\ \ b_3 = 27 \end{aligned}$$

Step 4 : Apply transformation α_1 from step 3 on the pixels of red matrix. Repeat this step for green and blue layers using α_2 and α_3 respectively.

Step 5 : Multiply the transformed matrix of red layer by matrix C_1 from step 2 to get encrypted red layer. Repeat this step for the green and blue layers using the matrices C_2 and C_3 respectively to get there encrypted layers.

Step 6 : Combine the encrypted red, green and blue channels to get the encrypted color image.

The technique can be used to encrypt any image of size $M \times M$. To execute the encryption process images of Lena, Fruits, House, Number, and Dragon are considered. Their original and encrypted images are given in Figure 2.6.

Chapter 3

Security Analysis

This chapter examines the security of the encryption scheme introduced in Chapter 2. It evaluates the scheme's robustness against potential threats and vulnerabilities. The analysis includes theoretical examination and practical experimentation to validate its security claims. The results affirm the scheme's reliability and suitability for real world applications. Detailed findings and limitations of some security analyses are discussed in subsequent sections.

3.1 Differential Attack Analysis

It analyzes the differences between pairs of actual text and encrypted text to identify patterns and weaknesses in the cryptographic system. By comparing the outputs of different inputs, an attacker can determine the key used to encrypt the data. UACI and NPCR [67] are two commonly used metrics for evaluating the effectiveness of image encryption algorithms.

3.1.1 Unified Average Changing Intensity (UACI)

It measures the average change intensity of difference between the original image and the encrypted image. The UACI values should be close to 33%. 'Z_1' and 'Z_2' are considered as an encrypted image and plain image. 'Z_1' is of dimension K × L, which differs only by one pixel from 'Z_2'. UACI can be calculated as:

$$UACI = \frac{1}{K \times L} \sum_{h,w} \frac{|Z_1(h,w) - Z_2(h,w)|}{255} \times 100\%,$$

Where, $Z_1(h,w)$ and $Z_2(h,w)$ are pixel values of Z_1 and Z_2 at (h,w) position respectively. Table 3.1 shows the UACI values of some RGB images.

UACI			
Images	**Red layer**	**Green layer**	**Blue layer**
Lena	33.6194	33.6855	33.5540
Fruits	33.6922	33.4760	33.4725
House	33.6584	33.3683	33.4992
Number	33.5818	33.6421	33.6192
Dragon	34.8970	33.1729	33.2368

Table 3.1: UACI values of some enciphered images

3.1.2 Number of Pixel Change Rate (NPCR)

NPCR measures the percentage of pixels that change between two encrypted images generated from slightly different plain images. NPCR considers the impact of a single pixel change on the entire image that is being encrypted using the proposed technique. For potent cryptosystem NPCR values should be closer to 99%. NPCR can be calculated as:

$$NPCR = \frac{\sum_{h,w} N(h,w)}{K \times L} \times 100\%,$$

where

$$N(h,w) = \begin{cases} 0, & if\, Z_1(h,w) = Z_2(h,w), \\ 1, & if\, Z_1(h,w) \neq Z_2(h,w) \end{cases}$$

Table 3.2 shows the NPCR values of some RGB images. Table 3.3 gives the comparison of distorted image of the Lena's standard 256 × 256 image obtained using the proposed scheme with some existing DNA and chaos based schemes.

3.2 Key Space Analysis

It analyzes the size and complexity of the key space, which is the total number of possible keys that can be used to encrypt the data [72]. Only cryptosystems with key space sizes smaller than 2^{100} are susceptible to the brute force attack. A larger

NPCR			
Images	**Red layer**	**Green layer**	**Blue layer**
Lena	99.9954	99.6109	99.6078
Fruits	99.9954	99.6124	99.6094
House	99.9985	99.6078	99.6063
Number	99.9924	99.6048	99.6078
Dragon	99.9985	99.6094	99.6109

Table 3.2: NPCR values of some enciphered images

Lena	**NPCR**			**UACI**		
Methods	**R**	**G**	**B**	**R**	**G**	**B**
Proposed	99.9954	99.6109	99.6078	33.6194	33.6855	33.5540
Ref[60]	99.6600	99.6300	99.6200	33.4000	33.4000	33.3800
Ref[68]	99.5900	99.6000	99.6000	33.2100	33.3100	33.3100
Ref[69]	99.6800	99.6600	99.7500	33.5500	33.5200	33.5300
Ref[70]	99.5900	99.5900	99.5900	33.0300	33.3100	33.0300
Ref[71]	99.5712	99.5758	99.6094	33.1056	30.5178	27.5385

Table 3.3: Comparison of NPCR & UACI values of standard Lena image

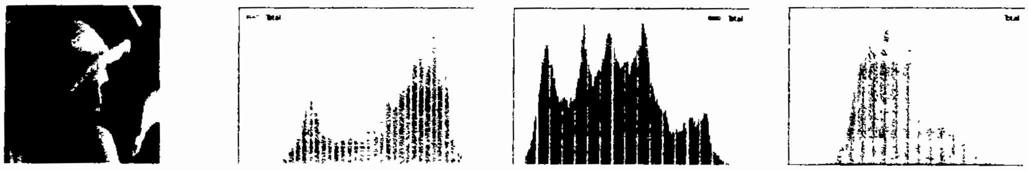
key space makes it more difficult for an attacker to guess or brute force the key. Furthermore, to resist a brute force attack, an encryption algorithm must be sensitive to even little changes. The secret keys in the proposed scheme are the 4 parameters b, c, f and d and 3 initial values x_1, y_1 and z_1 of 3D NK chaotic map and parameters of LA-field based DNA affine transformation. If each parameter of NK map has a precision of 10^{15}, the key space for it is $(10^{15})^7 = 10^{105} \approx 2^{349}$. Furthermore, 8 DNA rules used for encoding and decoding , 256 × 256 options for the choice of 'a' and 'b' and 24 bijections between $\{A, C, G, T\}$ and R. As a result, the total key space size of the proposed encryption technique is $(10^{15})^7 \times 65536 \times 8^2 \times 24^2 \approx 2^{381}$. So It is obvious that the suggested scheme's key space is adequate in size that can withstand a brute force attack.

3.3 Time Execution Analysis

In order to assess the worth of a cryptosystem, the time required to execute the algorithm is crucial. The suggested approach is evaluated on a machine with the following specifications: Intel(R) Core (TM) *i*5-7300U CPU @ 2.7GHz (4 CPUs); 8.00 GB RAM; and Windows 10 pro operating system. For the encryption procedure, computerised simulations are carried out in Python 3.9.12. In 11.64 seconds, the RGB test image is encrypted.

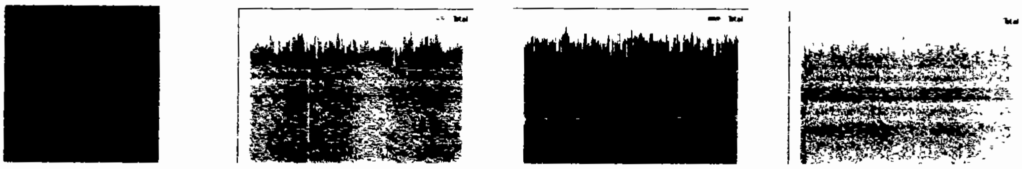
3.4 Histogram Analysis

Histograms are used to analyze the frequency distribution of values in the ciphertext to identify patterns or anomalies [73]. It can reveal any existing bias in the encryption algorithm or if certain values are more likely to occur than others, indicating a weakness in the system. Here, some RGB images taken to encrypt them using the suggested method, and then analyze their 3D histograms. Figures 3.1, 3.3, 3.5, 3.7, 3.9 (a-d) show the original Lena, Fruits, House, Number and Dragon image alongwith the histograms of their three channels. On the other hand, Figures 3.2, 3.4. 3.6, 3.8, 3.10 depict the encrypted Lena, Fruits, House, Number and Dragon images together with their three channels histograms.



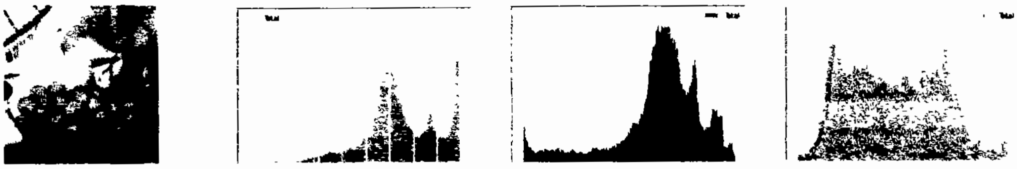
(a) (b) (c) (d)

Figure 3.1: Histogram plots of three colour channels of plain Lena image



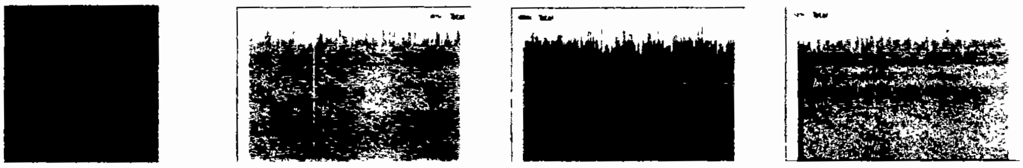
(a) (b) (c) (d)

Figure 3.2: Histogram plots of three colour channels of enciphered Lena image



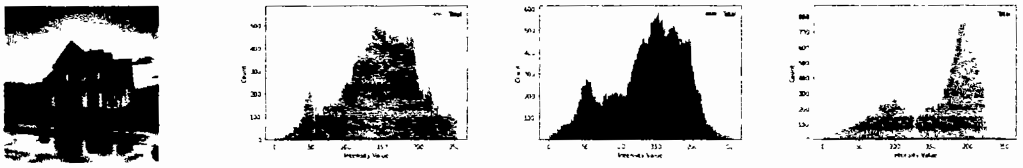
(a) (b) (c) (d)

Figure 3.3: Histogram plots of three colour channels of plain Fruits image



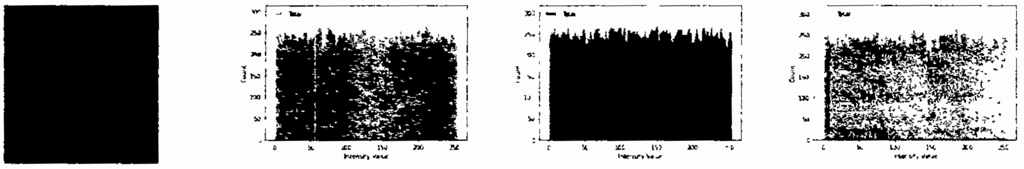
(a) (b) (c) (d)

Figure 3.4: Histogram plots of three colour channels of enciphered Fruits image



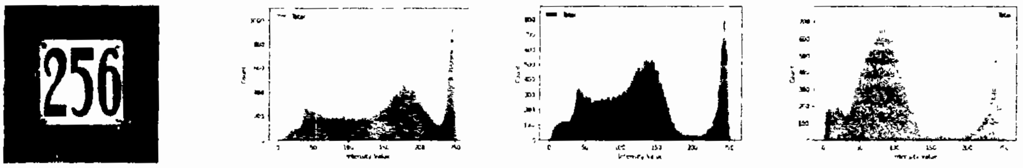
(a) (b) (c) (d)

Figure 3.5: Histogram plots of three colour channel of original House image



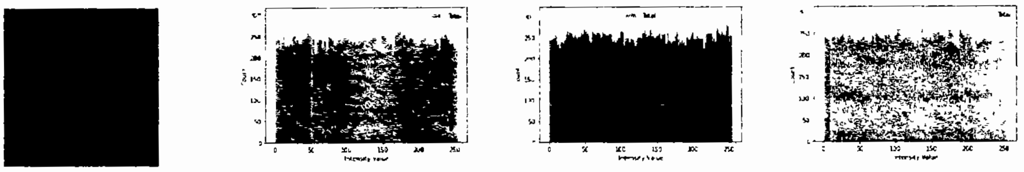
(a) (b) (c) (d)

Figure 3.6: Histogram plots of three colour channels of encrypted House image



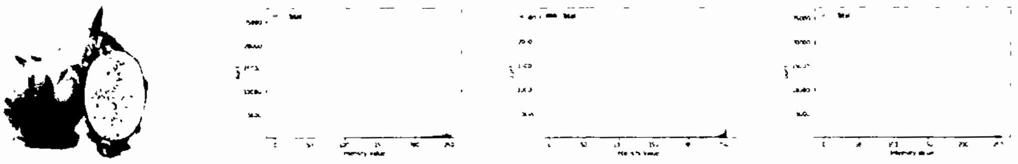
(a) (b) (c) (d)

Figure 3.7: Histogram plots of three colour channels of original Number image



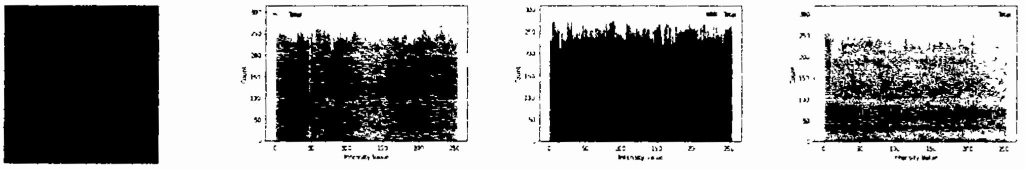
(a) (b) (c) (d)

Figure 3.8: Histogram plots of three colour channels of enciphered Number image



(a) (b) (c) (d)

Figure 3.9: Histogram plots of three colour layers of plain Dragon image



(a) (b) (c) (d)

Figure 3.10: Histogram plots of three colour channels of enciphered Dragon image

3.5 Texture Analysis

Texture is a visual attribute that refers to the surface properties and repetitive patterns present in an image. It provides important cues for understanding and interpreting the content of an image. It focuses on extracting information about the spatial arrangement of pixels or the statistical properties of local neighborhoods in an image. By characterizing and quantifying the texture patterns in an image, texture analysis enables more advanced and robust interpretation of images. There are various methods for examining texture, but the Fourier methodology is the most efficient [74]. Following are the few common features of the texture analysis.

3.5.1 Information Entropy

Entropy analysis focuses on measuring the amount of randomness or uncertainty present in an image. It quantifies the distribution and complexity of pixel values within the image. Various measures can be employed to determine the entropy of an image. Shannon's entropy, a method to calculate the average size of information needed for each pixel in an image, is the more commonly used measure. The maximum information entropy for a standard image with a data range of $0-255$ is 8. In general, the information entropy is closer to 8, the more random the distribution of the image pixels is, unlikely it is to crack the ciphertext image using an entropy attack. The formula to calculate the entropy B(ζ) is given as:

$$B(\zeta) = -\sum_{i=1}^{p} h(\zeta_i) log_c h(\zeta_i)$$

where ζ_i shows the histogram computations. Table 3.4 shows the entropy values for some RGB images. While Table 3.5 shows comparison of entropy values of standard Lena's distorted 256 × 256 image.

Entropy	**Plain Image**				**Encrypted Image**			
Images	**R**	**G**	**B**	**RGB**	**R**	**G**	**B**	**RGB**
Lena	7.3106	7.6088	7.0825	7.7789	7.9971	7.9973	7.9971	7.9990
Fruits	7.2330	7.4469	7.7412	7.7173	7.9976	7.9976	7.9974	7.9992
House	7.6866	7.6196	7.5162	7.6946	7.9973	7.9972	7.9971	7.9991
Number	7.7312	7.6142	7.4362	7.8204	7.9967	7.9973	7.9971	7.9990
Dragon	4.8429	5.5101	5.5225	5.3701	7.9971	7.9972	7.9970	7.9990

Table 3.4: Entropy analysis of three layers of some plain and enciphered color images

3.5.2 Correlation

It analyzes the correlation between different parts of the plaintext and ciphertext to identify patterns or weaknesses in the system. Correlations can reveal if certain bits of the plaintext are more likely to result in certain bits of the encrypted text, making it easier for an attacker to guess the key. By utilizing correlation analysis in image

Lena	Entropy			
Methods	R	G	B	RGB
Proposed	7.9971	7.9973	7.9971	7.9990
Ref[75]	7.9961	7.9940	7.9968	7.9956
Ref[76]	7.9901	7.9912	7.9921	7.9113
Ref[77]	7.99171	7.99121	7.99177	7.9916
Ref[78]	7.9972	7.9965	7.9962	7.9987
Ref[79]	7.9980	7.9980	7.9981	7.9970

Table 3.5: Comparison of Entropy for Lena image

encryption, one can assess the quality, strength, and vulnerabilities of scheme. It inspects the closeness of neighboring pixels in plain and encrypted image. The estimated coefficient values for the highly correlated pixels are close to 1 or -1, whereas the estimated coefficient values for the uncorrelated pixels are closer to zero. The test is segmented into three sections. These are correlations along the diagonal, vertical, and horizontal axes. Correlation can be calculated using the equation:

$$CC = \frac{Co(S,K)}{Sd(S) \times Sd(K)}$$

$$Co(S,K) = \frac{1}{M}\sum_{i=1}^{M}(S_i - E(S))(K_i - E(K))$$

$$Sd(S) = \sqrt{\frac{1}{M}\sum_{i=1}^{M}(S_i - E(S))^2}$$

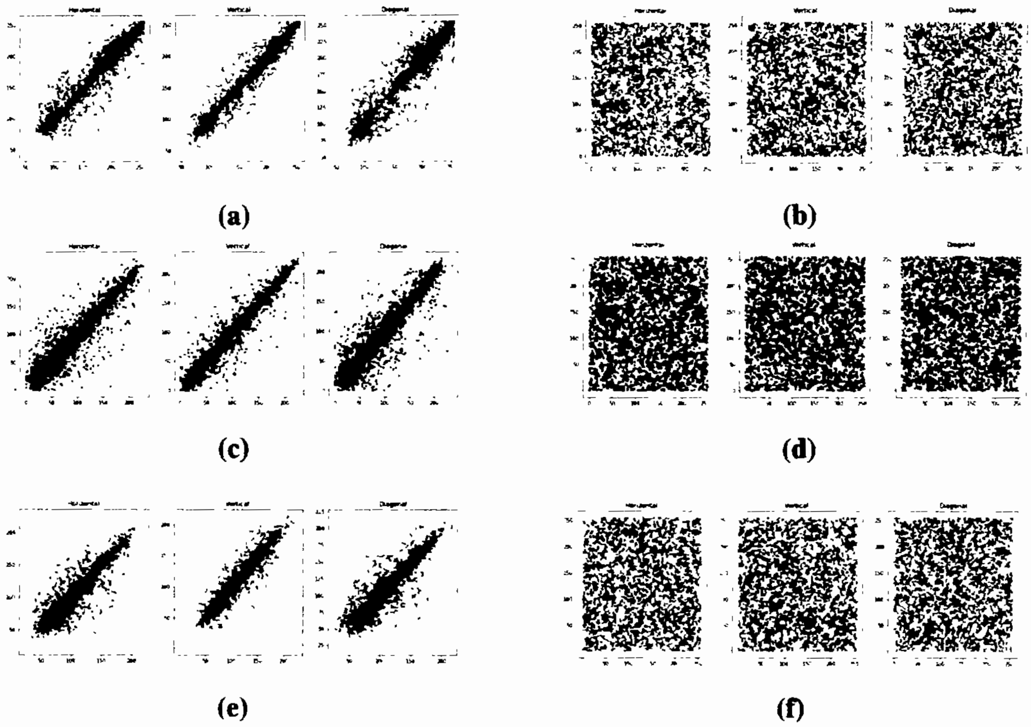
$$Sd(K) = \sqrt{\frac{1}{M}\sum_{i=1}^{M}(K_i - E(K))^2}$$

$$E(S) = \frac{1}{M}\sum_{i=1}^{M} S_i$$

$$E(K) = \frac{1}{M}\sum_{i=1}^{M} K_i$$

Table 3.6 depicts the correlation analysis of original and enciphered RGB images in horizontal, vertical and diagonal directions. Figure 3.11 - 3.15 (a-c) present the correlations horizontal, vertical and diagonal plots of the pixels correlation of original

Lena, Fruits, House, Number and Dragon, three channels. While Figure 3.11 - 3.15 (d-f) show the horizontal, vertical and diagonal plots of the pixel correlation in the three layers of the corresponding distorted images.



(a)

(b)

(c)

(d)

(e)

(f)

Figure 3.11: Correlation plots of pixels for original and enciphered images of Lena for horizontal, vertical and diagonal lines of three colour channels.

3.5.3 Homogeneity

Homogeneity analysis focuses on quantifying the uniformity and regularity of pixel values or texture patterns within an image. It aims to identify regions of the image that exhibit similar pixel values or have consistent texture characteristics and enables to calculate the proximity of the scattered pixels of the "Gray Level co-occurrence Matrix (GLCM)". It is defined as:

$$H=\sum_{w}\sum_{r}\frac{t(w,r)}{1-|w-r|}$$

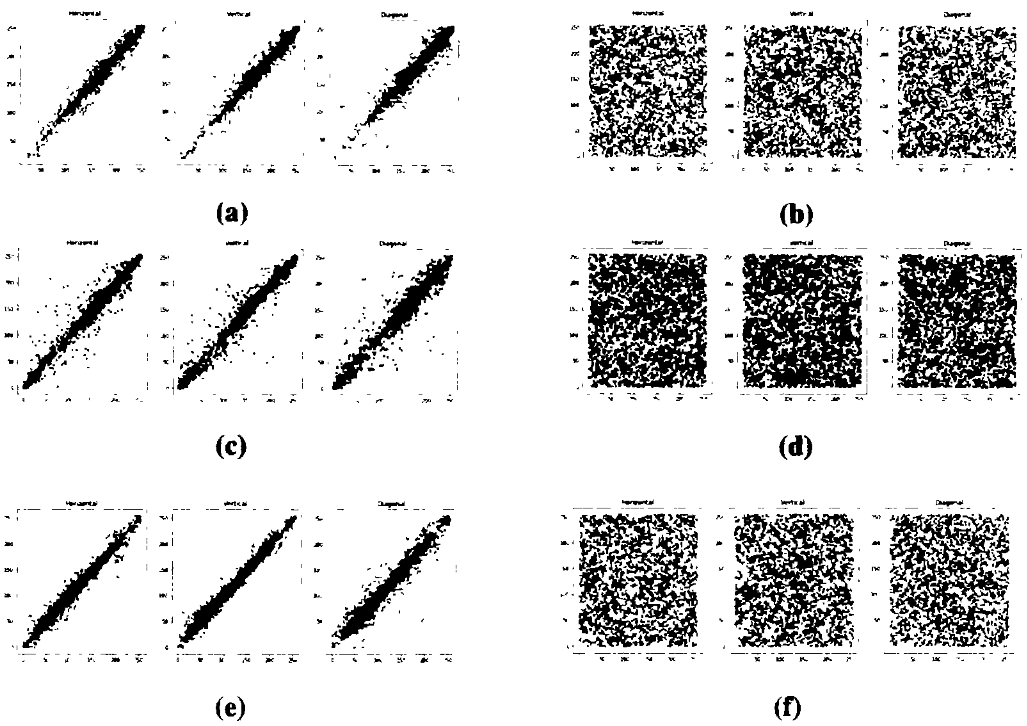
where 'w' and 'r' represent the pixels in an image, and $t(w,r)$ represents the number of Gray Level co-occurrence Matrices (GLCM). The values for homogeneity should be closer to 0.3. Table 3.7 depicts the results for homogeneity analysis for some RGB images.

Correlation		**Plain Image**			**Encrypted Image**		
Images	**Lines**	**R**	**G**	**B**	**R**	**G**	**B**
Lena	**Horizontal**	0.9294	0.9333	0.8651	0.0074	-0.0021	0.0219
	Vertical	0.9616	0.9633	0.9311	-0.0068	-0.0048	-0.0148
	Diagonal	0.9132	0.9157	0.8360	0.0132	-0.0136	0.0042
Fruits	**Horizontal**	0.9680	0.9721	0.9740	-0.0048	0.0032	0.0027
	Vertical	0.9598	0.9753	0.9803	-0.0136	-0.0031	-0.0329
	Diagonal	0.9311	0.9598	0.9530	0.0119	-0.0176	0.0059
House	**Horizontal**	0.9533	0.9496	0.9518	-0.0191	0.0334	-0.0000
	Vertical	0.9314	0.9160	0.9238	0.0041	0.0112	-0.0182
	Diagonal	0.9018	0.8936	0.8993	0.0077	-0.0176	-0.0144
Number	**Horizontal**	0.9456	0.9479	0.9542	0.0035	-0.0088	0.0115
	Vertical	0.9454	0.9460	0.9514	-0.0200	0.0065	0.0033
	Diagonal	0.9046	0.9152	0.9212	0.0377	0.0093	-0.0023
Dragon	**Horizontal**	0.8875	0.9544	0.9469	0.0034	-0.0076	0.0128
	Vertical	0.8965	0.9710	0.9616	-0.0268	-0.0063	0.0026
	Diagonal	0.8581	0.9414	0.9126	0.0369	-0.0161	-0.0265

Table 3.6: Pixel correlation analysis of three color layers of some plain and enciphered RGB images

Homogeneity	**Original Image**			**Enciphered Image**		
Images	**R**	**G**	**B**	**R**	**G**	**B**
Lena	0.8444	0.8463	0.8451	0.3893	0.3883	0.3917
Fruits	0.8824	0.8771	0.8615	0.3905	0.3892	0.3897
House	0.8211	0.8235	0.8156	0.3885	0.3896	0.3890
Number	0.7484	0.7663	0.7501	0.3880	0.3899	0.3875
Dragon	0.9057	0.8743	0.8629	0.3901	0.3904	0.3877

Table 3.7: Homogeneity analysis of three colour layers of some original and enciphered RGB images



(a) (b) (c) (d) (e) (f)

Figure 3.12: Correlation plots of pixels for original and enciphered images of Fruit for horizontal, vertical and diagonal lines of three colour channels.

3.5.4 Contrast

The spectator must contrast an image in order to perceive its various components. When the value of the contrast approaches a significant level during an encryption procedure, the unpredictability of an image increases. Contrast analysis focuses on quantifying the variation in pixel intensity or color values within an image and measures the difference between its lightest and darkest regions. A higher contrast value indicates strong encryption. Formula to calculate contrast is given below:

$$C = \sum_{w}\sum_{r}(w-r)^{2}t(w,r)$$

For constant images contrast value is zero. For good encryption the values for contrast analysis should be closer to 10. Table 3.8 depicts the outcomes of the contrast analysis.

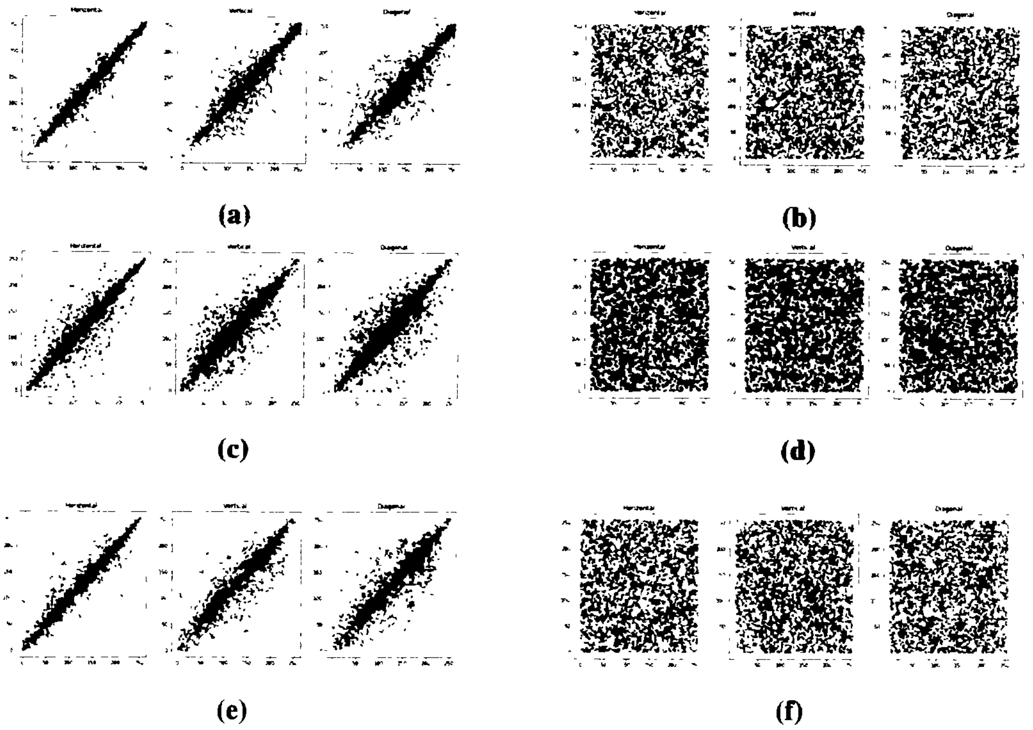


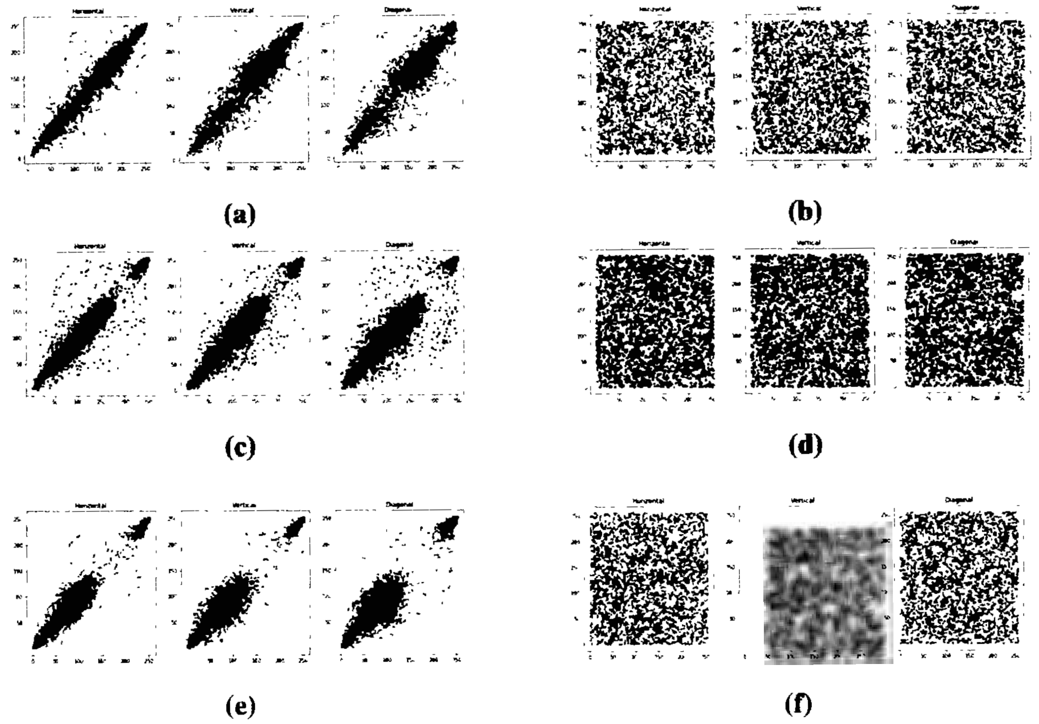
Figure 3.13: Correlation plots of pixels for original and enciphered images of House for horizontal, vertical, and diagonal lines of three color channels.

Contrast	**Original Image**			**Enciphered Image**		
Images	**R**	**G**	**B**	**R**	**G**	**B**
Lena	0.5512	0.5835	0.5449	10.5239	10.5519	10.4725
Fruits	0.4802	0.5038	0.5145	10.5148	10.5586	10.4864
House	1.0054	0.9717	1.1585	10.5249	10.4287	10.4600
Number	1.3023	1.1043	1.0805	10.6197	10.5675	10.5467
Dragon	0.5992	0.8766	0.9494	10.5531	10.3809	10.5458

Table 3.8: Contrast analysis of three colours channels of some plain and enciphered RGB images

3.5.5 Energy

Energy, also known as the sum of squared pixel intensities, measure the overall strength or magnitude of texture patterns in an image. Energy refers to the concentration or strength of pixel values, highlighting regions of high activity or significant



(a) (b)

(c) (d)

(e) (f)

Figure 3.14: Correlation plots of pixels for original and enciphered images of Number for horizontal, vertical, and diagonal lines of three color channels.

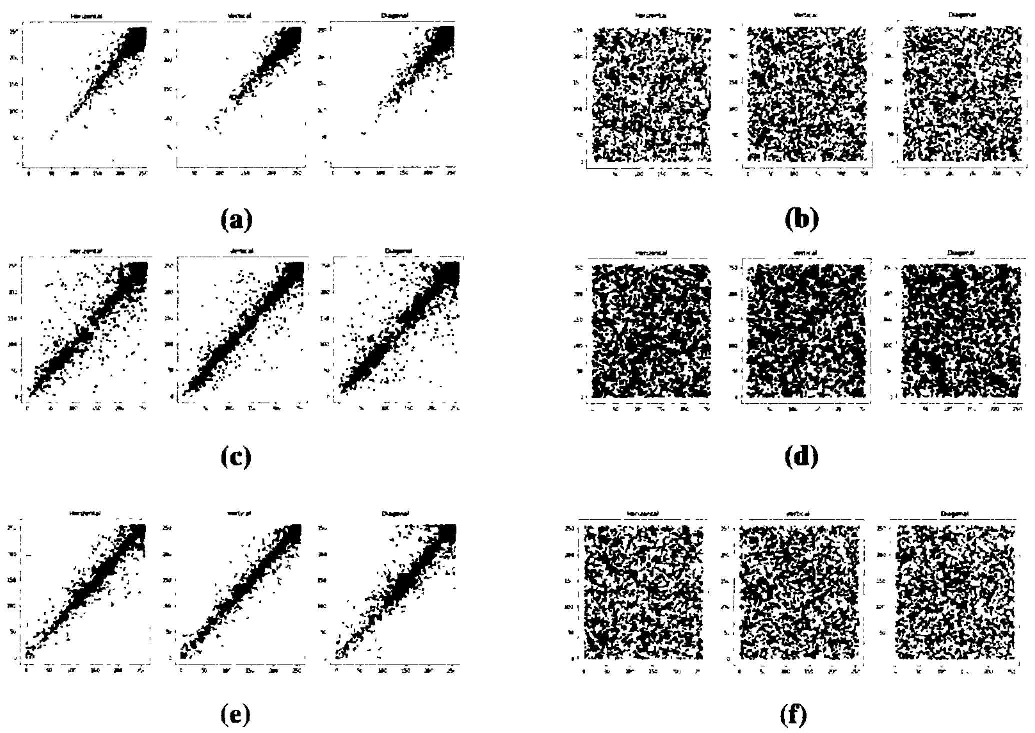
information.

$$E = \sum_{w} \sum_{r} t^2(w, r)$$

Constant images have 1 energy value. The optimal value for energy analysis is 0.0156 which is highly resistant to the different attacks. Table 3.9 depicts the values for energy analysis of RGB images.

3.6 Image Quality Measures

It measures the quality of the encryption algorithm based on various criteria such as speed, security, and efficiency. A high quality encryption algorithm should be fast, secure, and efficient. There are several quality measuring techniques [80], some of them are given below:



(a)

(b)

(c)

(d)

(e)

(f)

Figure 3.15: Correlation plots of pixels for original and enciphered images of Dragon for horizontal, vertical and diagonal lines of three colour channels.

Energy	Original Image			Enciphered Image		
Images	**R**	**G**	**B**	**R**	**G**	**B**
Lena	0.1234	0.0902	0.1528	0.0156	0.0156	0.0156
Fruits	0.1634	0.1454	0.0930	0.0156	0.0156	0.0156
House	0.0890	0.0966	0.1222	0.0156	0.0156	0.0156
Number	0.0652	0.0742	0.0831	0.0156	0.0156	0.0156
Dragon	0.5496	0.3514	0.3224	0.0156	0.0156	0.0156

Table 3.9: Energy analysis of three colours channels of some plain and enciphered RGB images

3.6.1 Mean Square Error (MSE)

The mean square error is a metric for measuring the difference between two images. It calculates the average of the squared differences between each pixel in the original image and its corresponding pixel in the compressed or distorted image. Formula to calculate MSE is given below.

$$MSE = \frac{1}{G \times H}\sum_{s=1}^{G}\sum_{t=1}^{H}[L(s,t) - N(s,t)]^2$$

where $G \times H$ is the size of image. $L(s,t)$ and $N(s,t)$ indicate the pixels of original and enciphered image located at (s,t) position. For safe encryption scheme, MSE value must be higher.

3.6.2 Peak Signal to Noise Ratio (PSNR)

Peak signal to noise ratio is a measure used to calculate the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the accuracy of its representation. The formula for PSNR is given by:

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

where J_{max} represents the maximum value of an image pixel. A higher PSNR value depicts better image quality. A lower PSNR value indicates a secure encryption scheme.

3.6.3 Structural Similarity Index Metric (SSIM)

Structural similarity index (SSIM) is a measure that is used to calculate the similarity between two images. It anticipate the luminance, contrast, and structure of the images. When the SSIM value is 1 it shows that two images are more similar or identical. Formula to calculate SSIM is given below:

$$SSIM(A,E) = \frac{(2\beta_A\beta_E + E_1)(2\eta_{AE} + E_2)}{({\beta_A}^2 + {\beta_E}^2 + E_1)({\eta_A}^2 + {\eta_E}^2 + E_2)}$$

where$\beta_A, \beta_E, {\eta_A}^2, {\eta_E}^2, \eta_{AE}$ are the average variance and covariance of A and E respectively. Furthermore, $E_1 = (q_1, r)^2$ and $E_2 = (q_2, r)^2$ are the variables used to stabilize the division with a low denominator, the fluctuating range of the pixel values is r, and $r_1 = 0.01$ and $r_2 = 0.03$ are the values by default.

Table 3.10 depicts the results for Quality measure analysis of some RGB images. Now in the succeeding sections some other analyses done for standard 256 × 256 RGB Lena image are presented.

	MSE			PSNR			SSIM		
Images	**R**	**G**	**B**	**R**	**G**	**B**	**R**	**G**	**B**
Lena	10633.17	8908.89	7119.16	7.8641	8.6325	9.6065	0.0119	0.0127	0.0095
Fruits	10759.24	9626.40	8846.78	7.8129	8.2961	8.6629	0.0084	0.0106	0.0078
House	8511.62	8172.12	9259.68	8.8306	9.0074	8.4648	0.0096	0.0107	0.0088
Number	10592.43	9871.27	10669.30	7.8808	8.1870	7.8494	0.0096	0.0073	0.0048
Dragon	17882.63	16368.13	15986.56	5.6064	5.9908	6.0932	0.0091	0.0087	0.0064

Table 3.10: Quality measure analysis of some RGB images

3.7 Maximum Deviation

Maximum deviation is a criterion used to assess an encryption scheme's statistical security. It calculates the disparity in pixel values between the encrypted image and the original image. A higher maximum deviation value indicates that the encryption system is more safe.

The formula for calculating the maximum deviation is as follows:

$$MD = \frac{K_o + K_{255}}{2} + \sum_{j=1}^{254} K_j$$

In this case, the histogram difference between the original and encrypted versions of the image at value j is represented by K_j. K_o and K_{255} are difference values at j = 0 & j = 255, respectively. Table 3.11 shows the maximum deviation of standard 256 × 256 RGB Lena image.

Image	Red	Green	Blue	RGB
Lena	50210	37069	61118	83780

Table 3.11: Maximum deviation of standard RGB Lena 256 × 256 image

3.8 Irregular Deviation

In light of the maximum deviation, ensuring the randomness of an enciphered image is insufficient. For the cipher to be effective against statistical attacks, the pixel values should fluctuate at random. A high randomness is produced in statistically insecure algorithm for certain images whereas in others, it generates modest randomness. This consequence can be investigated via irregular deviation. The following formula is used to calculate the irregular deviation ID:

$$ID = \sum_{j=0}^{255} |g_j - M_g|$$

g_j is the histogram of the absolute difference between the original and encrypted images. The mean value of g_j is denoted by M_g. A lower ID value indicates the closeness of the histogram pins values to regularity and resistance to statistical attacks. Table 3.12 depicts the irregular deviation of standard RGB 256×256 image.

Image	Red	Green	Blue	RGB
Lena	27366	19064	28028	52654

Table 3.12: ID of standard 256 × 256 RGB Lena image

3.9 3D Intensity Histograms of RGB Plain and Encrypted Image

The pixel intensity of an image's many layers is used to evaluate the appearance of a digital image. It offers pixel information about the image. The colour depth of an image stabilises the appearance of a digital medium in pixels. It ensures an algorithm's resistance to numerous attacks. Figures 3.16 depicts the intensity histogram of the plain and encrypted images of Lena. From Figure 3.16 it can be seen that the intensity histogram of the plain image and its red, green, and blue channels has sharp edges. In contrast, the enciphered image and its three channels exhibit a uniform pattern. As a result, breaking into plain image data might be difficult. Hence the algorithm's robustness is ensured by the intensity histogram.

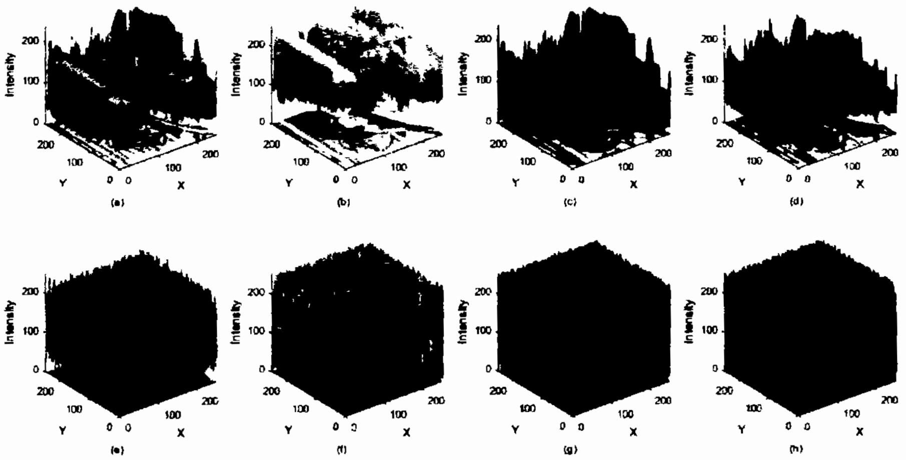


Figure 3.16: The intensity histograms of the original and ciphered images of Lena are shown in (a) and (e), while the intensity histograms of Lena's original and ciphered R, G, B layers are shown in (b), (c), (d), and (f), (g), (h), respectively

Conclusion and Future Directions

This chapter summarises the entire research work which is presented in this thesis. The potential of utilizing DNA operations from a non-associative LA field and a novel chaotic map to develop a cryptosystem technique has been explored in this thesis. The research presented in each chapter contributes to the overall strength of the proposed work. Chapter 1 provided an introductory overview of the key concepts, including cryptography, DNA based cryptography, non-associative LA-field, chaos, and image & image encryption. This chapter laid the foundation for a comprehensive exploration of the research topic, ensuring a solid understanding of the underlying principles. In chapter two the findings of the research work are described and the entire encryption scheme with the algorithm is presented carefully. The highlight of this chapter is the development of a unique LA-field based DNA affine transformation, never before utilized in existing research. An LA-field R of order 4 is obtained using MACE 4. The operation of addition and multiplication utilized in constructing the proposed LA-field based DNA affine transformation. Furthermore, the 3D chaotic NK map was proposed. The LA-field based DNA affine transformation combined with the three-dimensional chaotic NK map, to establishes a robust encryption scheme with enhanced security features. The non-associative structure of the transformation ensures stronger encryption, making the proposed work a notable contribution to the field of image encryption. Chapter 3 focused on conducting various security analyses to assess the resilience and robustness of the proposed encryption scheme. Through meticulous assessments, including texture analysis, differential attack analysis, image quality measures, histogram analysis, key space analysis, and time execution analysis the effectiveness of the presented scheme has been evaluated. The results of these analyses provided compelling evidence of the scheme's ability to withstand potential attacks, confirming its strength and reliability as a secure data encryption method.

Future Directions

The contributions made in this research pave the way for advancements in DNA-based cryptography, offering a promising avenue for future research and development. These are listed here:

1. Modifying the proposed encryption scheme for different formats of images.

2. Explore more associative and non-associative structures.

3. Design enhanced encryption schemes combining the non associative structure of LA-field and DNA cryptography.

4. Investigate the potential integration of the proposed NK chaotic map into the emerging encryption methodologies, enhancing security and efficiency for novel schemes.

5. Embark on demanding pursuits by extending the application of the LA-field based DNA affine transformation, leading to the exploration of new research horizons.

Bibliography

[1] C. E. Shannon, "A Mathematical Theory of Communication," *The Bell system technical journal*, vol. 27, no. 3, pp. 379–423, 1948.

[2] J. Buchmann, *Introduction to Cryptography*, vol. 335. Springer, 2004.

[3] N. Bisht and S. Singh, "A comparative Study of some Symmetric and Asymmetric Key Cryptography Algorithms," *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 4, no. 3, pp. 1028–1031, 2015.

[4] S. Burnett and S. Paine, *RSA Security's official guide to Cryptography*. McGraw-Hill, Inc., 2001.

[5] M. Ahmed, B. Sanjabi, D. Aldiaz, A. Rezaei, and H. Omotunde, "Diffie-Hellman and its Application in Security Protocols," *International Journal of Engineering Science and Innovative Technology (IJESIT)*, vol. 1, no. 2, pp. 69–73, 2012.

[6] S. U. Nimbhorkar and L. Malik, "A Survey on Elliptic Curve Cryptography (ECC)," *International Journal of Advanced Studies in Computers, Science and Engineering*, vol. 1, no. 1, pp. 1–5, 2012.

[7] T. ElGamal, "A public key Cryptosystem and a Signature Scheme based on Discrete Logarithms," *IEEE transactions on information theory*, vol. 31, no. 4, pp. 469–472, 1985.

[8] C. N. Mathur and K. Subbalakshmi, "Digital Signatures for Centralized DSA Networks," in *2007 4th IEEE Consumer Communications and Networking Conference*, pp. 1037–1041, Citeseer, 2007.

[9] S. R. Nagpaul, *Topics in Applied Abstract Algebra*, vol. 15. American Mathematical Soc., 2005.

[10] F. Pub, "Data Encryption Standard (DES)," *FIPS PUB*, pp. 46–3, 1999.

[11] M. J. Dworkin, E. B. Barker, J. R. Nechvatal, J. Foti, L. E. Bassham, E. Roback, J. F. Dray Jr, *et al.*, "Advanced Encryption Standard (AES)," 2001.

[12] R. Dahm, "Discovering DNA: Friedrich Miescher and the Early Years of Nucleic Acid Research," *Human genetics*, vol. 122, pp. 565–581, 2008.

[13] M. Mondal and K. S. Ray, "Review on DNA Cryptography," *arXiv preprint arXiv:1904.05528*, 2019.

[14] G. Jacob, "DNA based Cryptography: An Overview and Analysis," *International Journal of Emerging Sciences*, vol. 3, no. 1, p. 36, 2013.

[15] Y. Zhang, F. Wang, J. Chao, M. Xie, H. Liu, M. Pan, E. Kopperger, X. Liu, Q. Li, J. Shi, *et al.*, "DNA Origami Cryptography for Secure Communication," *Nature Communications*, vol. 10, no. 1, pp. 1–8, 2019.

[16] J. D. Watson and F. H. Crick, "The Structure of DNA," in *Cold Spring Harbor symposia on quantitative biology*, vol. 18, pp. 123–131, Cold Spring Harbor Laboratory Press, 1953.

[17] M. Kazim and M. Naseeruddin, "On Almost Semigroups," *Portugaliae mathematica*, vol. 36, no. 1, pp. 41–47, 1977.

[18] Q. Mushtaq and M. Kamran, "On Left Almost Groups," *Proceedings-Pakistan Academy of Sciences*, vol. 33, pp. 53–56, 1996.

[19] T. Shah and I. Rehman, "On LA-Rings of Finitely Non-Zero Functions," *Int. J. Contemp. Math. Sciences*, vol. 5, no. 5, pp. 209–222, 2010.

[20] M. Shah and T. Shah, "Some basic Properties of LA-Rings," in *Int. Math. Forum*, vol. 6, pp. 2195–2199, 2011.

[21] I. Rehman, M. Shah, T. Shah, and A. Razzaque, "On Existence of Non-Associative LA-Rings," *Analele Stiintfice ale Universitatii Ovidius Constanta*, vol. 21, no. 3, pp. 223–228, 2013.

[22] A. Jafari, I. Hussain, F. Nazarimehr, S. M. R. H. Golpayegani, and S. Jafari, "A Simple Guide for Plotting a Proper Bifurcation Diagram," *International Journal of Bifurcation and Chaos*, vol. 31, no. 01, p. 2150011, 2021.

[23] J. B. Dingwell, "Lyapunov exponents," *Wiley encyclopedia of biomedical engineering*, 2006.

[24] Y. Wu, G. Yang, H. Jin, and J. P. Noonan, "Image Encryption using the Two-Dimensional Logistic Chaotic Map," *Journal of Electronic Imaging*, vol. 21, no. 1, pp. 013014–013014, 2012.

[25] T. Yoshida, H. Mori, and H. Shigematsu, "Analytic study of Chaos of the Tent Map: band structures, power spectra, and critical behaviors," *Journal of statistical physics*, vol. 31, pp. 279–308, 1983.

[26] G. Peterson, "Arnold's Cat Map," *Math Linear Algebra*, vol. 45, pp. 1–7, 1997.

[27] G. Alvarez and S. Li, "Breaking an Encryption Scheme based on Chaotic Baker Map," *Physics Letters A*, vol. 352, no. 1-2, pp. 78–82, 2006.

[28] F. R. Marotto, "Chaotic Behavior in the Hénon Mapping," *Communications in Mathematical Physics*, vol. 68, pp. 187–194, 1979.

[29] O. M. Al-Hazaimeh, M. F. Al-Jamal, N. Alhindawi, and A. Omari, "Image Encryption Algorithm based on Lorenz Chaotic Map with Dynamic Secret Keys," *Neural Computing and Applications*, vol. 31, pp. 2395–2405, 2019.

[30] S. Yanchuk and T. Kapitaniak, "Chaos–Hyperchaos Transition in Coupled Rössler systems," *Physics Letters A*, vol. 290, no. 3-4, pp. 139–144, 2001.

[31] R. N. Madan, *Chua's circuit: A Paradigm for Chaos*, vol. 1. World Scientific, 1993.

[32] L. Kocarev, "Chaos-based Cryptography: A Brief Overview," *IEEE Circuits and Systems Magazine*, vol. 1, no. 3, pp. 6–21, 2001.

[33] Z. Hong and D. Ji-xue, "Chaos Theory and its Application in Modern Cryptography," in *2010 International Conference on Computer Application and System Modeling (ICCASM 2010)*, vol. 7, pp. V7–332, IEEE, 2010.

[34] M. K. Mandal, G. D. Banik, D. Chattopadhyay, and D. Nandi, “An Image Encryption Process based on Chaotic Logistic Map,” *IETE Technical Review*, vol. 29, no. 5, pp. 395–404, 2012.

[35] H. Wang and X. Li, “New Route of Chaotic Behavior in a 3D Chaotic System,” *Optik*, vol. 126, no. 20, pp. 2354–2361, 2015.

[36] A. Belazi, A. A. Abd El-Latif, and S. Belghith, “A Novel Image Encryption Scheme based on Substitution-Permutation Network and Chaos,” *Signal Processing*, vol. 128, pp. 155–170, 2016.

[37] S. Liu, C. Guo, and J. T. Sheridan, “A Review of Optical Image Encryption Techniques,” *Optics & Laser Technology*, vol. 57, pp. 327–342, 2014.

[38] M. Kaur and V. Kumar, “A Comprehensive Review on Image Encryption Techniques,” *Archives of Computational Methods in Engineering*, vol. 27, no. 1, pp. 15–43, 2020.

[39] K. D. Patel and S. Belani, “Image Encryption using Different Techniques: A Review,” *International Journal of Emerging Technology and Advanced Engineering*, vol. 1, no. 1, pp. 30–34, 2011.

[40] J. Fridrich, “Image Encryption based on Chaotic Maps,” in *1997 IEEE international conference on systems, man, and cybernetics. Computational cybernetics and simulation*, vol. 2, pp. 1105–1110, IEEE, 1997.

[41] G. K. Shraida and H. A. Younis, “A Review of DNA-Based Color Image Encryption Algorithms,” *Iraqi Journal of Intelligent Computing and Informatics (IJICI)*, vol. 1, pp. 56–65, 2022.

[42] X. Wang and C. Liu, “A Novel and Effective Image Encryption Algorithm based on Chaos and DNA Encoding,” *Multimedia Tools and Applications*, vol. 76, pp. 6229–6245, 2017.

[43] L. M. Adleman, “Molecular Computation of Solutions to Combinatorial Problems,” *science*, vol. 266, no. 5187, pp. 1021–1024, 1994.

[44] A. Gehani, T. LaBean, and J. Reif, “DNA-based Cryptography, 5th DIMACS Workshop on DNA based Computers,” 1999.

[45] A. Gehani, T. LaBean, and J. Reif, "DNA-based cryptography. DIMACS DNA based Computers V," *American Mathematical Society*, 2000.

[46] A. Leier, C. Richter, W. Banzhaf, and H. Rauhe, "Cryptography with DNA Binary Strands," *Biosystems*, vol. 57, no. 1, pp. 13–22, 2000.

[47] V. I. Risca, "DNA-based Steganography," *Cryptologia*, vol. 25, no. 1, pp. 37–49, 2001.

[48] C.-C. Yang, T.-Y. Chang, J.-W. Li, and M.-S. Hwang, "Simple Generalized Group-Oriented Cryptosystems Using ElGamal Cryptosystem," *Informatica*, vol. 14, no. 1, pp. 111–120, 2003.

[49] M. Lu, X. Lai, G. Xiao, and L. Qin, "Symmetric-key Cryptosystem with DNA Technology," *Science in China Series F: Information Sciences*, vol. 50, pp. 324–333, 2007.

[50] G. Cui, L. Qin, Y. Wang, and X. Zhang, "An Encryption Scheme using DNA Technology," in *2008 3rd International Conference on Bio-Inspired Computing: Theories and Applications*, pp. 37–42, IEEE, 2008.

[51] Q. Zhang, L. Guo, X. Xue, and X. Wei, "An Image Encryption Algorithm based on DNA Sequence Addition Operation," in *2009 Fourth International on Conference on Bio-Inspired Computing*, pp. 1–5, Ieee, 2009.

[52] M. Borda and O. Tornea, "DNA Secret Writing Techniques," in *2010 8th International Conference on Communications*, pp. 451–456, IEEE, 2010.

[53] X. Lai, M. Lu, L. Qin, J. Han, and X. Fang, "Asymmetric Encryption and Signature Method with DNA Technology," *Science China Information Sciences*, vol. 53, pp. 506–514, 2010.

[54] Q. Zhang, X. Xue, and X. Wei, "A Novel Image Encryption Algorithm based on DNA Subsequence Operation," *The Scientific World Journal*, vol. 2012, 2012.

[55] R. Soni, G. Prajapati, A. Khan, and D. Kulhare, "Triple Stage DNA Cryptography using Sequential Machine," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 8, pp. 859–867, 2013.

[56] J. Zhang, D. Fang, and H. Ren, "Image Encryption Algorithm based on DNA Encoding and Chaotic Maps," *Mathematical Problems in Engineering*, vol. 2014, pp. 1–10, 2014.

[57] F. E. Ibrahim, H. Abdalkader, and M. Moussa, "Enhancing the Security of Data Hiding using Double DNA Sequences," in *Industry Academia Collaboration Conference (IAC)*, pp. 6–8, 2015.

[58] Y. Zhang, X. Liu, and M. Sun, "DNA based Random key Generation and Management for OTP Encryption," *Biosystems*, vol. 159, pp. 51–63, 2017.

[59] J. Wu, X. Liao, and B. Yang, "Image Encryption using 2D Hénon-Sine Map and DNA Approach," *Signal processing*, vol. 153, pp. 11–23, 2018.

[60] T. ul Haq and T. Shah, "Algebra-Chaos Amalgam and DNA Transform based Multiple Digital Image Encryption," *Journal of Information Security and Applications*, vol. 54, p. 102592, 2020.

[61] F. Firdousi, M. Khan, S. S. Jamal, and N. Faraz, "Parent-Daughter Confusion Component: A New Approach for the Construction of Nonlinear Confusion Component," *Wireless Personal Communications*, vol. 120, no. 4, pp. 3095–3115, 2021.

[62] Y. Yang, L. Wang, S. Duan, and L. Luo, "Dynamical Analysis and Image Encryption Application of a Novel Memristive Hyperchaotic System," *Optics & Laser Technology*, vol. 133, p. 106553, 2021.

[63] I. A. Aljazaery, H. T. Salim ALRikabi, and A. H. M. Alaidi, "Encryption of Color Image Based on DNA Strand and Exponential Factor," *International Journal of Online & Biomedical Engineering*, vol. 18, no. 3, 2022.

[64] F. Ahmed, M. U. Rehman, J. Ahmad, M. S. Khan, W. Boulila, G. Srivastava, J. C.-W. Lin, and W. J. Buchanan, "A DNA based Colour Image Encryption Scheme using a Convolutional Autoencoder," *ACM Transactions on Multimedia Computing, Communications and Applications*, vol. 19, no. 3s, pp. 1–21, 2023.

[65] S. Das and M. K. Sanyal, "Dynamic Key Generator based Colour Medical Image Protection Algorithm using 3D Unified Chaotic System and Dynamic

DNA Coding," *International Journal of Information Technology*, vol. 15, no. 2, pp. 1015–1033, 2023.

[66] W. McCune, "Mace4 Reference Manual and Guide," *arXiv preprint cs/0310055*, 2003.

[67] Y. W. NPCR, "UACI Randomness Tests for Image Encryption," *Cyber JJ Selected Areas Telecommun*, 2011.

[68] P. N. Lone, D. Singh, and U. H. Mir, "Image Encryption using DNA Coding and Three-Dimensional Chaotic Systems," *Multimedia Tools and Applications*, vol. 81, no. 4, pp. 5669–5693, 2022.

[69] D. S. Malik and T. Shah, "Color Multiple Image Encryption Scheme based on 3D-Chaotic Maps," *Mathematics and Computers in Simulation*, vol. 178, pp. 646–666, 2020.

[70] M. Tanveer, T. Shah, A. Rehman, A. Ali, G. F. Siddiqui, T. Saba, and U. Tariq, "Multi-Images Encryption Scheme based on 3d Chaotic Map and Substitution Box," *IEEE Access*, vol. 9, pp. 73924–73937, 2021.

[71] W. Alexan, N. Alexan, and M. Gabr, "Multiple-Layer Image Encryption Utilizing Fractional-Order Chen Hyperchaotic Map and Cryptographically Secure PRNGs," *Fractal and Fractional*, vol. 7, no. 4, p. 287, 2023.

[72] D. S. Monaghan, U. Gopinathan, T. J. Naughton, and J. T. Sheridan, "Key-Space Analysis of Double Random Phase Encryption Technique," *Applied optics*, vol. 46, no. 26, pp. 6641–6647, 2007.

[73] O. Holub and S. T. Ferreira, "Quantitative Histogram Analysis of Images," *Computer Physics Communications*, vol. 175, no. 9, pp. 620–623, 2006.

[74] A. Baraldi and F. Panniggiani, "An Investigation of the Textural Characteristics Associated with Gray Level Cooccurrence Matrix Statistical Parameters," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 33, no. 2, pp. 293–304, 1995.

[75] T. ul Haq and T. Shah, "12× 12 S-box Design and its Application to RGB Image Encryption," *Optik*, vol. 217, p. 164922, 2020.

[76] J. Wu, X. Liao, and B. Yang, "Color Image Encryption based on Chaotic Systems and Elliptic Curve ElGamal Scheme," *Signal Processing*, vol. 141, pp. 109–124, 2017.

[77] Y.-Q. Zhang, Y. He, P. Li, and X.-Y. Wang, "A New Color Image Encryption Scheme based on 2DNLCML System and Genetic Operations," *Optics and Lasers in Engineering*, vol. 128, p. 106040, 2020.

[78] W. Alexan, M. Elkandoz, M. Mashaly, E. Azab, and A. Aboshousha, "Color Image Encryption Through Chaos and kaa Map," *IEEE Access*, vol. 11, pp. 11541–11554, 2023.

[79] A. T. Hashim, A. H. Jassem, and S. A. Ali, "A Novel Design of Blowfish Algorithm for Image Security," in *Journal of Physics: Conference Series*, vol. 1818, p. 012085, IOP Publishing, 2021.

[80] A. Hore and D. Ziou, "Image Quality Metrics: PSNR vs. SSIM," in *2010 20th International Conference on Pattern Recognition*, pp. 2366–2369, IEEE, 2010.