

A Digital Image Enciphering based on Amalgamation of a Non-associative Algebra and Chaos Theory



By

Tanzeela Anwar

(823-FBAS/MSMA/F21)

Department of Mathematics and Statistics

Faculty of Sciences

International Islamic University, Islamabad

Pakistan

2023

✓ TH-27073

MS
512.54
TAD

Nonassociative rings

Algebra, Nonassociative

Chaotic behavior in systems

Image processing - Digital techniques

Image encryption, mathematical models

A Digital Image Enciphering based on Amalgamation of a Non-associative Algebra and Chaos Theory



By

Tanzeela Anwar

(823-FBAS/MSMA/F21)

Supervised by

Dr. Nazli Sanam

Department of Mathematics and Statistics

Faculty of Sciences

International Islamic University, Islamabad

Pakistan

2023

A Digital Image Enciphering based on Amalgamation of a Non-associative Algebra and Chaos Theory

By

Tanzeela Anwar
(823-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

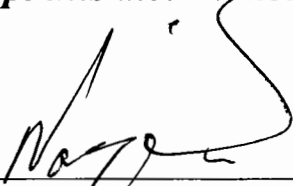
A Digital Image Enciphering based on Amalgamation of a Non-associative Algebra and Chaos Theory

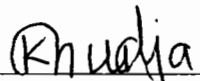
By

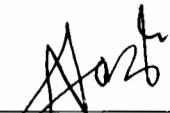
Tanzeela Anwar


*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. Nasir Siddiqui
(External Examiner)

2. 
Dr. Khudija Bibi
(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*

Author's Declaration

I hereby declare that this thesis is my original work. I have not copied from any other student's work or from any other source except where due reference or acknowledgement is made explicitly in the text, nor has any part been written for me by another person.

The work was done under the supervision of **Dr. Nazli Sanam** at International Islamic University, Islamabad.

Tanzeela Anwar

MS (Mathematics)

Reg.no.823-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 Digital Image Enciphering based on Amalgamation of a Non-associative Algebra and Chaos Theory**” submitted by “**Tanzeela Anwar, 823-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

First and foremost, I am deeply grateful to Allah, the Almighty, for granting me the strength and guidance throughout this research journey. I am humbled by the countless blessings bestowed upon me by Allah, which have facilitated my academic growth and the successful completion of this thesis and recognize that this achievement would not have been possible without His divine support.

I would like to express my heartfelt gratitude and extend my warmest thanks to my supervisor, Dr. Nazli Sanam, for her invaluable guidance, mentorship, and expertise. Her insightful feedback and dedication have played a crucial role in shaping this research work. I am appreciative of the time and effort invested in my development as a researcher. Her patience, encouragement, and belief in my potential, which have inspired me to overcome challenges and strive for excellence.

I am deeply indebted to my parents, whose unconditional love, unwavering support, and continuous encouragement have been my greatest source of inspiration. Their sacrifices, belief in my abilities, and prayers have fueled my determination, and I am forever grateful for their presence in my life.

Dedicated

to

My

Parents

Preface

In the modern era, with the rapid advancement of technology and the increasing reliance on digital information, securing the confidentiality of sensitive information has become crucial. Ensuring the secrecy and authenticity of digital images, which serve as a medium for capturing and conveying our visual experiences, emerges as a crucial imperative. Consequently, numerous researchers have embarked on developing diverse security techniques. While some methods for data security exist, there is still a room for improvement to ensure robust protection of data.

Data hiding or concealment plays a crucial role in the present times, providing techniques for encoding data in a manner that makes it intricate for unintended users to comprehend. Three primary methods of data hiding include watermarking, cryptography, and steganography. Cryptography is the skill of transforming information into an encrypted form which ensures data confidentiality, integrity, authentication, providing a comprehensive range of benefits for secure information exchange. Current cryptographic approaches primarily focus on block-based encryption techniques, such as "AES" and "DES". While these approaches have proven effective for securing textual information, they face limitations when it comes to the massive transmission of data in the form of images.

Image encryption techniques play a crucial role in the domain of data hiding by concealing sensitive information within images. This ensures that neither hackers nor eavesdroppers, including server administrators and other unauthorized entities, can access the original content of transmitted data over open networks like the internet. In the last few years, numerous techniques for encrypting images have been presented, and it has been discovered that encryption methods based on chaos and algebra exhibit particularly high effectiveness.

The central focus of the proposed thesis is to design a cryptosystem that utilizes the memristive chaotic system and a non-associative algebraic structure (LA-group). This combination aims to create a robust encryption technique capable of generating

ciphered images with exceptional resistance against various attacks. By leveraging the behavior of the memristive system and the unique properties of non-associative algebra, the cryptosystem aims to offer robust security measures and protect sensitive image data from unauthorized access. The scheme described in this dissertation comprises of two phases. In the first phase, the proposal introduces the generation of four algebraic-chaotic sequences. These sequences are derived by the sequences obtained from memristive system in combination with non-associative LA-group. In the second phase, a proposed scheme for encrypting color images is introduced, utilizing the generated algebraic-chaotic sequences. By incorporating the algebraic-chaotic sequences into the encryption process, the scheme aims to ensure the security and protect the confidentiality of data representing images with color information. This encryption algorithm stands out for its remarkable balance between ease of implementation and a high level of security. Despite its simplicity in implementation, this algorithm offer robust protection, making it resistant to brute force attacks.

A comprehensive evaluation of this encryption scheme is conducted through various analyses to assess its robustness. These analyses include entropy, correlation, histogram, key space and key sensitivity. Also occlusion and noise attacks are done that illustrates the high security level of proposed scheme.

Contents

Author's Declaration	i
Forwarding Sheet by Research Supervisor	ii
Acknowledgement	iii
Preface	vi
1 Preliminaries	1
1.1 Cryptography	1
1.1.1 Fundamentals of Cryptography	2
1.1.2 Objectives of Cryptography	3
1.1.3 Types of Cryptography	4
1.1.4 Confusion and Diffusion	6
1.2 LA-semigroup and LA-group	7
1.2.1 LA-semigroups (Left Almost Semigroups)	7
1.2.2 LA-groups (Left Almost Groups)	8
1.3 Chaos Theory	9
1.3.1 Chaos and Cryptography	10
1.3.2 Chaotic Systems	11
1.4 Digital Image	13
1.4.1 Types of Digital Image	13
1.5 Image Encryption	14
1.6 Aims and Objectives of the Thesis	16
1.7 Thesis Layout	17
2 A Non-associative LA-group and Memristive Chaotic System based RGB Image Encryption Scheme	18
2.1 Literature Review	18
2.2 The Memristive Chaotic System	21
2.2.1 Background	21

2.2.2	Mathematical Model and its Dynamical Analyses	22
2.3	Construction of Algebraic-Chaotic Sequences over LA-group with Memristive System	25
2.3.1	Generating Algorithm for the Proposed Algebraic-Chaotic Sequences	25
2.4	RGB Image Encryption and Decryption schemes	30
2.4.1	Proposed Encryption Algorithm	30
2.4.2	Decryption Scheme	31
3	Security Analysis of Proposed Encryption Algorithm	33
3.1	Differential Attack Analysis	33
3.1.1	Number of Pixels Change Rate (NPCR)	34
3.1.2	Unified Average Changing Intensity (UACI)	34
3.2	Statistical Analysis	35
3.2.1	Histogram Analysis	35
3.2.2	Correlation Analysis	36
3.2.3	Key-space Analysis	40
3.2.4	Key Sensitivity Analysis	41
3.3	Texture Analysis	42
3.3.1	Entropy	44
3.3.2	Contrast	44
3.3.3	Homogeneity	45
3.3.4	Energy	45
3.4	Image Quality Measures	46
3.4.1	Mean Square Error (MSE)	47
3.4.2	Peak Signal-to-Noise Ratio (PSNR)	47
3.4.3	Average Difference (AD)	47
3.4.4	Structural Content (SC)	47
3.4.5	Normalized Absolute Error (NAE)	48
3.4.6	Normalized Cross Correlation (NCC)	48
3.4.7	Root Mean Square Error (RMSE)	48
3.4.8	Maximum Difference (MD)	49
3.4.9	Universal Quality Index (UQI)	49
3.4.10	Structural Similarity Index Metric (SSIM)	49
3.5	Occlusion Attack Analysis	51

3.6	Noise Attack Analysis	53
3.7	Time Execution Analysis	55
4	Conclusion and Future Directions	56
4.1	Conclusions	56
4.2	Future work	57

Chapter 1

Preliminaries

The aim of this introductory chapter is to provide some fundamental concepts, definitions and background information to lay the groundwork for the content presented in the rest of the thesis. The chapter covers the fundamentals of cryptography, basics of LA-groups and a study of chaos, digital image and image encryption.

1.1 Cryptography

Since the beginning of confidential communications, it has always been a top priority for both states and individuals to secure the sensitive information. People have continually looked for ways to preserve sensitive data since the time of ancient Egypt. Evidence indicates that the ancient Egyptians utilised coded symbols to maintain the confidentiality of their communications. There were very advanced ancient civilizations that utilised pictorial-like symbols in their encrypted data to deceive unauthorized reader.

In the current era of advanced technologies, significant amount of crucial and sensitive information cruises in daily life between people through sharing and open networking. The development of digital content has opened up a number of new opportunities that have been seized to boost the efficiency of numerous processes and grow its influence on everyday life. At present, digital contents are employed in every arena of life, such as medicine, electronic advertising, web designing, business, banking and numerous other fields. However the distribution of digital data over the internet has produced plausible scenarios that put their integrity and confidentiality at risk and make them particularly vulnerable to widespread abuse. Cryptography is the platform that provides the methods capable to secure data integrity, anonymity,

authenticity, and confidentiality. Since the 1950s, cryptography has been regarded as a legitimate scientific field. However, in comparison to others, it is a completely new and rapidly expanding field of research, and each day brings fresh advancements. In cryptography, the methods for protecting data of any kind (text, audio, images, videos) generally include an encryption algorithm and a key. In our dissertation, we'll concentrate on digital image encryption techniques and how to improve their effectiveness and security.

1.1.1 Fundamentals of Cryptography

Cryptology is the study of science which deals with the storage and transmission of data in secret and secure form. The term "cryptology" originates from two Greek words "Kryptos," meaning "hidden," and "logos," meaning "word". Cryptography and cryptanalysis are the two primary branches into which cryptology can be further categorized. Cryptography is the process of protecting data, information, or information systems by converting them into an incomprehensible form or secret codes so that they can be preserved from unauthorized access or manipulation. It is derived from the Greek words "kryptos" and "graphein" which combine to mean "secret writing". On the contrary, cryptanalysis refers to the procedure of cracking or recovering a concealed message or code to its original form, without being authorized.

Cryptography plays an important role for protection of data or information in current era. In earlier cryptography, encryption had been done using synonymously words in place of different words but current cryptographic techniques depend on computer science, mathematical models and electrical engineering which makes it more secure to resist different attacks. This covers the three essentials areas authentication, integrity and confidentiality which will be discuss later. Cryptography has significant applications in computer science, financial transactions, e-commerce transactions, and many more.

Here is a list of some basic concepts and terminologies that are used through the contents of cryptography [1–3].

Plaintext The original form of message, data or information within the language that can be easily understood by anyone.

Ciphertext Unreadable or coded form of data or information that has undergone some encryption process which cannot be understood by an unauthorized person.

Key An essential element that is shared between the encryption and decryption processes, enabling them to effectively encode and decode the information. The key must be kept secret in the process because the whole communication depends on it. A key can be words, numbers, phrase or any combination of numbers or symbols etc.

Encryption It is the procedure used to convert plaintext (readable message) into ciphertext (unreadable message). Enciphering process depends on key and strong algorithm to protect confidential data from the person you want to hide it.

Decryption The term used to describe the reverse procedure of encryption. In other words, it refers to the process of transforming ciphertext back into plaintext by utilizing a secret key.

Cryptosystem It is the structure or a plan comprising of a set of algorithms and instructions to convert plaintext into ciphertext or vice versa. Cryptosystem consist of finite numbers of plaintexts, ciphertexts, possible numbers of finite keys and instructions for both encryption and decryption.

1.1.2 Objectives of Cryptography

The fundamental objectives of cryptography that ensures the security of a system are as follows:

Confidentiality Confidentiality means protecting a data or information from an unapproved individual. It ensures that only the intended receiver or authorized recipient decoded the encrypted message by using the key. It is the main and commonly addressed goal of cryptography.

Integrity Integrity ensures that data or information cannot be altered or modified from transmitting to receiving end by any unauthorized person intentionally or accidentally.

Authenticity Authenticity makes sure that data comes from a trusted origin or source. It identifies the source of a message from receiver or sender. In short, authenticity means that the sender and receiver both can verify each other identities to avoid from being deceived or tricked.

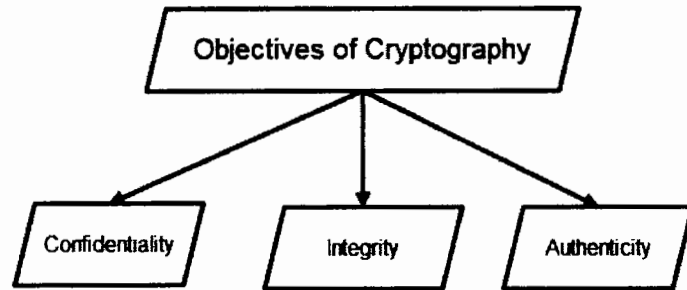


Figure 1.1: Objectives of Cryptography

1.1.3 Types of Cryptography

For encryption and decryption there is a choice of having the keys (private or public). This fact divides the cryptography into two types

- Asymmetric (Public) Key Cryptography
- Symmetric (Private) Key Cryptography

Asymmetric Key Cryptography

Asymmetric key cryptography, also known as public-key cryptography utilises a pair of keys to facilitate secure communication and data protection. One key is used for encryption called as "public (shared) key" that can be shared over insecure channel or can be known to every one while for decryption second key is used which is called "private (secret) key" and it must be kept secret by its holder. Anyone can encrypt data or information who knows public key but cannot decrypt the data. On the other hand, only that person can decrypt it who has a private key. Moreover, the mathematical relationship between the respective keys ensure that deriving the secret key from the associated shared key is considered computationally intractable,

providing an additional layer of security. RSA [4], ECC, and Rabin are some examples of asymmetric key based cryptographic scheme.

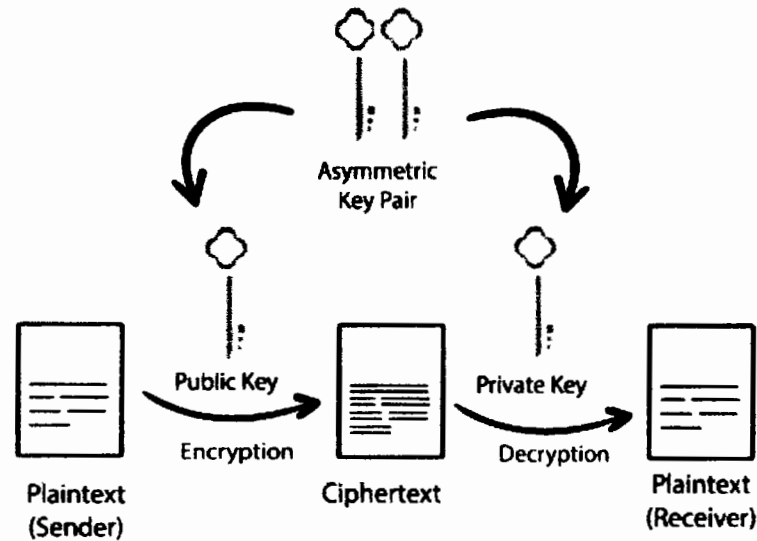


Figure 1.2: Asymmetric Encryption

Symmetric Key Cryptography

In symmetric key cryptographic algorithms, encryption and decryption are performed using the same key. Secret key, single key or private key cryptography are some other names for the symmetric key cryptography. The original message is encrypted by the sender using a secret key, and the resulting encrypted message is then transmitted to the receiver. On the other hand, the receiver decrypts this message by using the same key and recovers the original message. Data Encryption Standard (DES) [5], Triple DES [6], Advanced Encryption Standard (AES) [7], and RC4 [8] are some examples of symmetric key based cryptographic scheme.

Stream cipher and block cipher are two types of symmetric key cryptography, each offering distinct approaches to secure data encryption.

Stream Cipher

Stream cipher is a symmetric key cryptosystem that encrypts data by examining and processing individual binary digits one at a time. In programming techniques stream cipher is relatively quicker and comparatively simple enciphering process. Vigenere

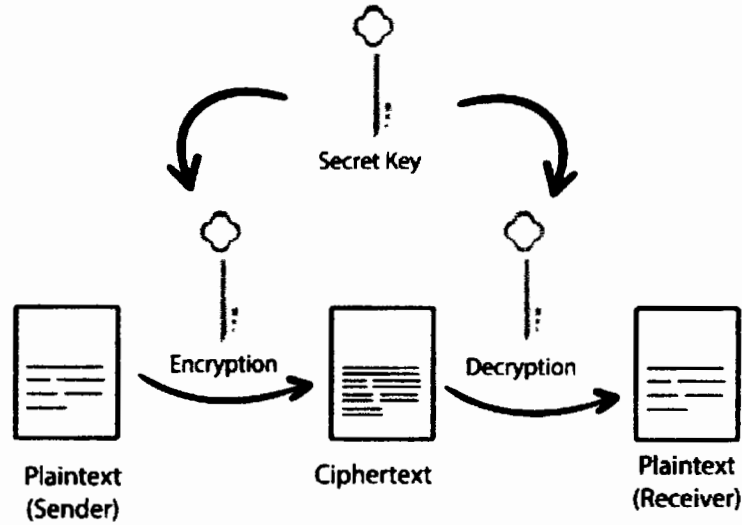


Figure 1.3: Symmetric Encryption

cipher and Caesar cipher [9] are examples of stream cipher in standard cryptography whereas RC4 is an example in modern cryptography.

Block Cipher

In a block cipher, data is segmented into fixed-length groups of bit sequences called blocks. Each block is encrypted separately using a secret key and an encryption algorithm, resulting in cipher blocks of the same fixed length. The security and effectiveness of the cipher are influenced by the length of the key utilized. AES [7] and DES [5] are examples of block cipher.

1.1.4 Confusion and Diffusion

Claude Elwood Shannon introduced the concepts of confusion and diffusion in 1949 as fundamental elements for constructing a robust cryptosystem [10]. The basic purpose of these concepts is to create irregularity in data to make cryptosystem more secure.

The technique which incept or establish a complicated relation between ciphertext and secret key is known as Confusion. In other words, confusion refers to the phenomenon where modifying a single bit in a key results in significant or widespread alterations in the ciphertext, affecting multiple or most of its bits. This property of confusion adds difficulty for attackers to derive the key from the ciphertext, thus

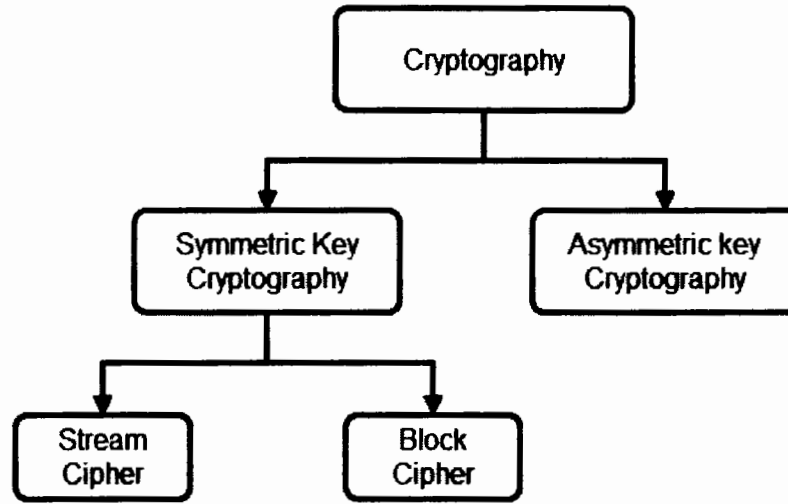


Figure 1.4: Types of Cryptography

enhancing the overall security of the system and providing robust protection against a wide range of attacks.

Diffusion is a technique in which if we change a single plaintext bit then it creates alteration about fifty percent of bits in ciphertext. Similarly, alteration in single ciphertext bit creates alteration in half of bits of plaintext. Infact, the purpose of diffusion is to maximize the complexity of the relationship between the plaintext and ciphertext.

1.2 LA-semigroup and LA-group

A general review of LA-groups and their properties are elaborated in this section. Furthermore, concept of LA-semigroups is also provided for better understanding of LA-groups.

1.2.1 LA-semigroups (Left Almost Semigroups)

An LA-semigroup is a term used to describe a magma G that satisfies the left invertive law $(uv)w = (wv)u$. Naseeruddin and Kazim [11] were the first ones to introduce the concept of LA-semigroups in 1972. Some other names that are referred to LA-semigroups are left invertive groupoid [12], right modular groupoid

[13], AG-groupoid or Abel Grassmann's groupoid [14]. It is a non commutative and non associative algebraic structure. An LA-semigroup structure can be regarded as an intermediate concept between a commutative semigroup and a groupoid. The medial law is satisfied by an LA-semigroup : $(uv)(wx) = (uw)(vx)$.

It is not necessary for an LA-semigroup to contain a left identity. An LA-semigroup that possesses a left identity is referred to as an LA-monoid. If there is a left identity element in an LA-semigroup, it is guaranteed to be unique. In an LA-semigroup, the presence of left identity does not imply the existence of right identity [15]. The structure of an LA-semigroup is somehow connected to a commutative semigroup, as an LA-semigroup becomes a commutative semigroup if it contains right identity.

1.2.2 LA-groups (Left Almost Groups)

Left Almost group or LA-group is an extension of LA-semigroup, introduced by Mushtaq and Kamran in 1996 [16]. If an LA-semigroup G satisfies the existence of a left identity element e such that $eu = u$ for all $u \in G$ and there exist $u^{-1} \in G$ for all $u \in G$ such that $u^{-1}u = uu^{-1} = e$, then G is called an LA-group. The medial law: $(uv)(wx) = (uw)(vx)$ also holds naturally in LA-groups. An LA-group is a generalization of an abelian group. The structure of an LA-group is non-associative and non-commutative but if one of them holds in LA-group, the other will automatically hold. In other words, we can say that commutativity and associativity imply each other in an LA-group. In literature, the name like Abel Grassmann's group abbreviated as AG-group has been used by different authors for the said structure. Some significant results and properties of LA-groups can be found in [16–18].

1. An LA-group is cancellative.
2. There is no other idempotent element in an LA-group except the left identity.
3. Let G be an LA-group and let $u, v, w, x \in G$ with left identity e in G , then following conditions hold:

- $uv = wx \implies vu = xw$
- $u \cdot vw = v \cdot ux$
- $(uv)(wx) = (xv)(wu)$ (para-medial law)

- $uv = e \implies vu = e$
- The element e becomes the left identity in an LA-group G if it is the right identity element in G i.e, $ue = u \implies eu = u$
- $(uv)^{-1} = u^{-1}v^{-1}$

Example[19] Let $A = \{(u, v) | u \in R, v = -1 \text{ or } 1\}$, where R denotes the set of real numbers. The symbol " \cdot " represents a binary operation defined in the following manner:

$$(u, v) \cdot (w, x) = (uw, v/x); \quad \forall (u, v), (w, x) \in A$$

Then,

$$[(u, v) \cdot (w, x)] \cdot (y, z) = (uw, v/x) \cdot (y, z) = (uwy, v/xz);$$

$$[(y, z) \cdot (w, x)] \cdot (u, v) = (yw, z/x) \cdot (u, v) = (uwy, z/vx).$$

because $v, x \in \{1, -1\}$, $v^2 = x^2$, and $v/x = x/v$. We can get $v/xz = z/vx$.

Therefore,

$$[(u, v) \cdot (w, x)] \cdot (y, z) = [(y, z) \cdot (w, x)] \cdot (u, v),$$

the left invertive law is satisfied. Also $(1, 1)$ is left identity element in A and $(1/u, \pm 1)$ is the inverse of $(u, \pm 1)$.

$$(1, 1) \cdot (u, v) = (u, 1/v) = (u, v); \quad (\text{because } v = 1 \text{ or } -1)$$

$$(1/u, 1) \cdot (u, 1) = (1, 1) \quad \text{and} \quad (1/u, -1) \cdot (u, -1) = (1, 1).$$

Therefore, (A, \cdot) is an LA-group.

1.3 Chaos Theory

The term "Chaos" originates from the Greek word "Xaos," which conveys the idea of unpredictability or a state of disorder. Chaos theory enables us to be prepared for unexpected as different strategies can be employed to tackle or handle the predictable behaviour like electricity, chemical reactions, gravity. Chaos theory provides us framework for understanding and managing the unpredictable aspects found in various phenomenon, including the stock market, human brain states, weather patterns etc.

Chaotic systems are considered as deterministic, simple and non-linear. These systems show their unpredictable nature by having irregular or random appearance. They exhibit high sensitivity to initial values, implying that even a slight alteration in the input parameters can result in substantial variations in the output results. This phenomenon is also named as butterfly effect. This underlying principle of chaos explains that even a slight modification in the initial state of a non-linear deterministic system can cause a large difference in its subsequent states. This butterfly effect can be explained by a metaphor such that "flipping of butterfly wings in Brazil can cause a tornado in Texas".

Chaos theory enables us to have a new insight, strength and idea to understand the chaotic nature of our world. In many natural systems chaotic behavior can be observed including weather, laser, electronic structures, fluid flows, heartbeats irregularities etc. Additionally, chaotic dynamics can also manifest in systems incorporating artificial components, such as road traffic. We can study these behaviours through the analyses of mathematical models. Applications of chaos theory can be found in many areas including anthropology, meteorology, computer science, economics, environmental science and engineering etc.

1.3.1 Chaos and Cryptography

Over the past few decades, chaos theory is the focus of many researchers in many different fields like fluid dynamics, electronic structures, climate and cryptography etc. Cryptographers used dynamical chaotic systems extensively in the development of numerous cryptographic primitives. These algorithms include watermarking, steganography, secure pseudo-random number generators and image encryption algorithms etc. Typically, these algorithms rely on the utilisation of single modal chaotic maps. The main incentive behind the creation of chaos-based cryptographic algorithms is similarity between certain characteristics of chaotic maps and cryptographic systems. These similarities serve as a key motivation for leveraging chaos theory in the design of secure cryptographic algorithms. The sensitivity to initial conditions and the inherent randomness displayed by chaotic systems make them valuable in cryptographic techniques for introducing confusion as well as diffusion in encryption processes. In the 1990s, numerous algorithms based on chaos were introduced, which employed chaotic maps for security purposes. Text and other various data formats can be encrypted using chaos based encryption schemes in

communication systems.

Chaos theory was first developed by Yorke and Li in 1975 [20]. In 1890 Poincare presented the dynamical equations and problem of three body in his article [21]. Later Hadamard [22] observed random behaviour and the sensitivity of initial values of special system in 1898. After this, Poincare monitored in 1908 that sensitivity of systems depends of its initial conditions which provides unpredictable results. Edward Lorenz conducted the initial analysis of chaos theory in 1963, where he presented the mathematical structure for weather prediction. Lorenz concluded in [23] that equations have random and complex behaviour because of initial conditions. Mathews [24] introduced the chaotic encryption technique that encrypt text based data in 1989. In 1998, Fridrich introduced the first image encryption technique based on chaotic maps, marking a significant milestone in the field of cryptography [25]. After that numerous image encryption techniques based on chaotic maps have been introduced, aiming to provide protection to confidential images. The fusion of DNA computing and chaotic systems has been employed to enhance the security of information encryption. There are many types of cryptosystems based on chaos theory including watermarking scheme [26], audio encryption [27, 28], video encryption [29] etc. Utilising the chaos theory in cryptosystem enhance the security to a higher level.

1.3.2 Chaotic Systems

Chaotic system is considered as a set of dynamical equations that exhibit some sort of chaotic behaviour based on the initial seed values. These chaotic systems which vary with time are categorized as discrete and continuous chaotic systems. In a discrete chaotic system, time and state variables are defined in discrete steps or intervals. While in a continuous chaotic system, time and state variables are defined continuously, without any discrete steps or intervals. Discrete chaotic systems are often described by difference equations or iterated functions, whereas differential equations are used to describe the continuous systems. Random sequences are generated by chaotic systems that exhibit a strong dependence on both initial conditions and control parameters. These sequences possess properties of unpredictability and sensitivity to small variations, making them valuable in various applications requiring secure and robust randomization. When chaotic systems are utilized in cryptography, the base values and parameters can be treated as keys. Chaotic behaviour

of the chaotic systems are based on specific region of control parameters. Chaotic systems are an excellent option for building cryptosystems because of their distinctive qualities or features including determinacy, ergodicity, and sensitivity to initial conditions. Some fundamental tools that are used to evaluate and analyze chaotic systems are Bifurcation diagram and Lyapunov exponent.

Bifurcation

A bifurcation is a period doubling, the splitting of a trajectory into two during iteration which occurs when the control parameter is varied. As the period doubling increases, chaotic behaviour of a system can be observed. This is because the trajectory's route is mixed up and inseparable at a particular point, causing the system to become chaotic. The bifurcation diagram is produced by plotting the equilibrium values against each parameter value. Bifurcation appears when a small change to the bifurcation parameter value causes a sudden change in the system behaviour. This transition is usually sudden and might be "qualitative" or "topological". Bifurcation can happen in both types of chaotic systems (Discrete and Continuous).

Lyapunov Exponent (LE)

The term Lyapunov exponent [30], represents the average rate of divergence between two neighboring trajectories within a dynamical system. The Lyapunov exponent can therefore be used to measure the initial value sensitivity of the chaotic system to identify whether the system is chaotic or not. The better initial parameter choice of chaotic maps occurring in chaotic regions is made possible by the Lyapunov exponent. Lyapunov exponent is defined as follows:

$$\lambda(x_0) = \lim_{m \rightarrow \infty} \frac{1}{m} \sum_{i=0}^{m-1} \ln |f'(x_i)|$$

The Lyapunov exponent is critical in describing the behavior of a dynamical system such as positive value indicates that the system exhibits the chaotic dynamics. Where the negative value signifies that the system is non-chaotic in nature. The system is in the steady state mode when it is zero. As the Lyapunov exponent increases, the system exhibits a higher degree of chaotic behavior.

1.4 Digital Image

A numeric representation of an image that can be stored and processed by a digital computer is known as "Digital Image". In other words an image can be precisely defined as a two-dimensional array that is organized in rows and columns. It is composed of finite numbers of elements, each of which have a specific value at a certain position. These elements are named as picture elements or pixels. A pixel is a commonly used term to represent the elements of digital image. The imaging device note a numbers or a set of numbers for each pixel that identify pixel's characteristics like its colour or brightness (Intensity).

1.4.1 Types of Digital Image

Binary Image: A black and white image that contains only two pixel values either 0 or 1 is known as a binary image. The value 0 represent Black and the value 1 represents White. These types of images are commonly used in applications like optical character recognition (OCR) or for reading text on a computer etc, where only a basic shape or outline is required.

Gray-Scale Image: It is a black and white image that contains 8 bit pixels and it has 256 different shades of colour in it. The range of available gray levels is determined by the number of bits employed for each pixel. 0 refers to black, 255 refers to white and 127 refers to gray. Gray scale image is also referred to as a monochrome (one color) image.

Color Image: A color image refers to an image that contains multiple colors, as opposed to a grayscale or black-and-white image. The most common representation of color images is through the RGB (Red, Green, Blue) color model. In this model, each pixel's color is defined by red, green, and blue channels. A color image contains 24-bits with 8 bits allocated to each of the three color channels (Red, Green, and Blue) and $(256)^3 = 16,777,216$ different colors in it.

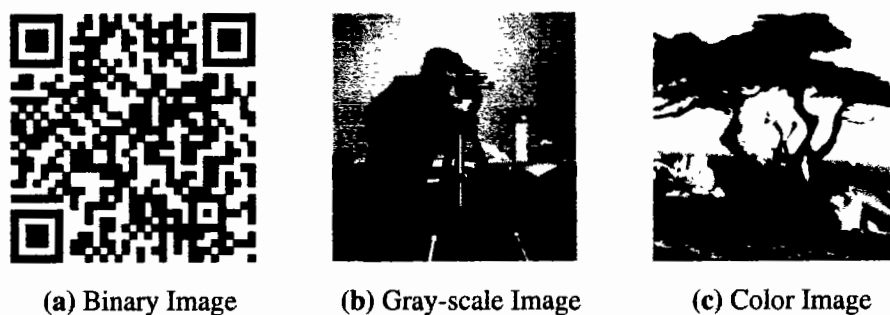


Figure 1.5: Types of digital Images

1.5 Image Encryption

Image encryption involves converting an original image into a coded or encrypted image using a secret key in order to shield the image from outside sources while it is being transmitted over a public network. A digital image is altered in such a way that it becomes unrecognizable and entirely different from its original form. When the image is to be viewed, the decryption process is employed to return it to its original state. Whereas decryption is a reversed encryption process which restores an encrypted image to its original state when the key is known. In this process, the coded image can only be decrypted by an authorized person who has the access of the key. By utilizing the decryption algorithm and the key, they can retrieve the original image.

Due to the advancement in technologies, digital images have become integral to various aspects of modern culture and find applications in diverse fields such as advertising, military branches and video conferencing etc. These images may contain highly confidential and sensitive information and their leakage can result a great loss. The transmission of these images over the insecure channels of the network can cause a threat to the information on the internet exposed and unsafe. Therefore the security of digital images transmitted over open networks has progressively gained importance and attracted significant attention from researchers. Many encryption methods for encoding and decoding of the image have been proposed to ensure the privacy of the image from unauthorized access. In general, many efforts have been made to develop text data encryption techniques. The majority of the standard encryption scheme, including DES and AES are typically designed for text encryption. However, the high redundancy, strong correlation among neighboring pixels, and large data capacity of digital images make encryption techniques de-

signed for text data less suitable for securing images. Although typical encryption techniques can be used to directly encrypt images but this may not be a good idea for some reasons as it will have a long encryption time because the text size is usually smaller than the image size and the low security it offers as the data originally has strong correlation. Different schemes for encrypting images have been developed so far using chaos theory, s-boxes, optical transform, random grids, DNA coding, compressive sensing etc. If an algorithm meets the following criteria, it is considered to be secure and ideal for an image encryption.

- The encryption scheme must exhibit robust security measures and effectively withstand various known attacks.
- The implementation of the process should prioritize simplicity, aiming for a straightforward and uncomplicated approach.
- Another important factor for good encryption is the speed in which an image is being encrypted. The computational time of an encryption scheme should be less without compromising the security.
- Ciphred image pixels must be less correlated. Encryption algorithm to be considered secure, the correlation values should be near to zero.
- The size of the encryption key must be large because it is difficult for an attacker to identify the specific key if the key size is large.
- Entropy value of algorithm should approaches 8. If an encrypted image has an entropy value under 8 then this could leads to consistency and a risk to anticipated security.
- Key sensitivity is also necessary. To put it another way, a minor alteration in the key would render the image decryption infeasible.

There have been a number of suggested image encrypting techniques that ranges in terms of effectiveness and robustness. Chai et al. [31] introduced an image encryption method utilizing DNA sequence operations and chaotic systems. The color image undergoes an initial encoding process based on DNA rules. After that, the encoded image is encrypted using a chaotic system. This technique not only produces outstanding encryption results but also demonstrates remarkable resilience against

common attacks. An encryption scheme utilizing matrix semi-tensor product theory was introduced by Wang and Gao [32]. Random sequences are obtained from hyperchaotic Lorenz map and then these chaotic sequences are utilized for generating two fixed scrambling matrices. Chen et al.[33] used Chebyshev map and sine map to encode an image. To enhance the cryptosystem, this technique introduces a novel two-dimensional chaotic system that combines the Sine map, the Chebyshev map, and a linear function. The results indicate that this technique achieves a high security level and improved resilience against common attacks. Simiao Wang [34] developed a color image encryption algorithm that integrates a 4D chaotic system with DNA technology. The rules for DNA encoding, decoding, and calculation are determined by generating four chaotic sequences from a 4D chaotic system.

1.6 Aims and Objectives of the Thesis

The aims and objectives of this dissertation can be summarized as follows:

- To use the LA-group (a non-associative algebraic structure) of order 16 and four-dimensional memristive chaotic system to increase the complexity in algorithm for secure cryptosystem. The main purpose of using LA-group and memristive system is to enlarge the key space which is the main component of encryption schemes because the efficiency and security lie upon it.
- To obtain the robust four algebraic-chaotic sequences for enhancing the security level of the encryption algorithm. In this thesis, algebraic-chaotic sequences are obtained by the amalgamation of LA-group with four-dimensional memristive chaotic system.
- To propose an image encryption method that uses traditional confusion and diffusion phase depending on the algebraic-chaotic sequences and chaotic sequences generated from memristive chaotic system.
- To examine the potency of the proposed encryption technique, various simulation analyses such as statistical analysis (Histogram, key space, key sensitivity and correlation analyses), differential analysis (UACI and NPCR), image quality measures, occlusion attack analysis, noise attack analysis and some well-known texture analysis are conducted.

The objective of the proposed work is to develop a technique that combines high complexity, large key size, randomness, and fast processing speed for encryption in order to enhance performance and to minimize encryption time.

1.7 Thesis Layout

The structure of this dissertation consists of four chapters.

- **Chapter 1** briefly discusses the fundamentals of non-associative algebraic structure (LA-group) and basic definitions and concepts of cryptography. Detailed explanation of chaos theory and image encryption as well as current research in image encryption is also highlighted in the chapter that provides a foundation for the upcoming chapters.
- **Chapter 2** introduces an image encryption techniques for an RGB image based on algebraic-chaotic sequences. This chapter has three detailed parts. In the first part of the chapter, an overview of the considered memristive chaotic system is given. In the second part, an efficient and simple scheme to design the algebraic-chaotic sequences (utilising combination of memristive system with the non-associative operation of an LA-group) is discussed. Whereas an encryption algorithm is presented in the third part of the chapter.
- **Chapter 3** is dedicated to implementing security measures that aim to guarantee both the strength and efficiency of the proposed image encryption algorithm. These security measures includes statistical, texture and differential attack analysis, analysis of noise and occlusion attacks and image quality analysis.
- **Chapter 4** gives the conclusion to the presented work and few suggestions for possible future work.

Chapter 2

A Non-associative LA-group and Memristive Chaotic System based RGB Image Encryption Scheme

This chapter introduces a novel color image encryption technique that utilises the combination of an LA-group and a four-dimensional memristive chaotic system. The principal objective of proposed encryption scheme is to offer a secure method for transmitting digital images. In this chapter, various topics are covered, including the introduction and analysis of a four-dimensional memristive system and its dynamical properties, the development of an algorithm for constructing algebraic chaotic sequences, and the implementation of color image encryption and decryption algorithms utilizing the algebraic-chaotic sequences.

2.1 Literature Review

When the secret information is transmitted, the key challenge is preventing unauthorised access to the information. As the digital images are the most prevalent way for people to transmit information, therefore, it has become essential to protect image data against unauthorised intrusion. For that purpose the most efficient strategy is image encryption. Several encryption techniques have been developed, incorporating cryptographic principles into their algorithms that ensures the security of digital images over the insecure channels of network. Classical encryption techniques, such as mono-alphabetical and poly-alphabetic cyphers, typically use substitution

or permutation to create a cryptosystem. Any encryption scheme that relies only on substitution or permutation is vulnerable to various types of cryptographic attacks. As a result of technological advancements the cryptosystems are becoming weaker day by day. Following the groundbreaking work of Claude Shannon, the concept of confusion and diffusion got the attention of many researchers and was widely used in secure communications which led to the concurrent utilization of substitution and permutation techniques in modern block ciphers [35].

Image encryption techniques that are currently state of arts use algebraic structures, DNA transforms and chaotic systems. Various algebraic structures such as groups, rings, Galois fields, Galois rings, as well as other commutative and associative structures, have been employed for the development of image encryption algorithms. In modern cryptography most of the cryptosystem algorithms are designed using finite Galois fields ($GF(2^n)$ for $2 \leq n \leq 8$). For the last three decades associative algebras of Galois fields have served as the foundation for the majority of encryption schemes. To increase the complexity in algorithm for secure cryptosystem it was quite legitimate and appropriate to replace the associative algebraic structures with non-associative algebraic structures. The intriguing characteristics of these structures, including non-associativity and the existence of an inverse for the zero element, contribute to enhancing the security levels of cryptosystem algorithms. In [36, 37] the novel designs for image encryption are introduced over the non-associative ring with a cardinality of 512 and the elements of inverse property loop respectively. In their article [38] the authors used inverse LA-semigroup and a modified non-linear chaotic map to design the encryption scheme for color image.

Over the past few years, the concept of chaos has discovered numerous applications in image security. Chaotic maps have been used to construct several cryptosystems [39, 40] offering more secure encryption methods. The use of chaotic systems for designing the secure image processing cryptographic systems is an ideal choice because of its several characteristics like it exhibits random behavior, extreme initial conditions and parameters sensitivity and high randomness. The Lyapunov exponent, the bifurcation diagram and chaotic attractors demonstrate the intricate dynamics exhibited by chaotic maps. In recent years, many researchers have proposed various chaos theory based encryption schemes using different methodologies [41, 42]. Uni-dimensional [43] and multi-dimensional [44] chaotic systems are two basic categories into which chaotic systems are often divided. Uni-dimensional

chaotic systems are characterized by their simplicity and ease of use due to their straightforward structures. Most of the algorithms for gray-scale images uses one dimensional chaotic systems [45] but the only drawbacks of these systems are their limited key space, which compromises the overall security of the encryption algorithm. In [46] a new algorithm is designed for image encryption using multichaotic maps. Some researchers suggested image enciphering techniques based on hyper-chaotic maps [47, 48]. In [49], a commutative chain ring and one dimensional mixed chaotic map were combined and DNA transformation was incorporated to present an RGB image encryption scheme. Furthermore, a 4D mixed chaotic map was introduced and utilized for the purpose of image encryption in [50]. The utilization of multiple systems and hyper-chaotic systems in image cryptographic schemes serves the purpose of increasing the key space in order to enhance resistance against various attacks.

In recent years, memristor has been introduced into chaotic systems widely because of their special nonlinear characteristics which aroused renewed studies in many fields such as secure communication [51], artificial neural network [52, 53] and computing in-memory etc. Based on the above application prospects, the application research of various kinds of chaotic circuit systems including memristor element has recently gained a lot of attention. Itoh and Chua [54] proposed first memristor based chaotic circuits in 2008 and analyzed its dynamic characteristics. Memristive chaotic systems exhibit multistability (i.e., multiple coexisting attractors) due to remarkable nonlinearity, it greatly enhances the flexibility and robustness of the system. The memristive chaotic system has high security performance for image encryption then general chaotic systems because it has more complex topology, higher unpredictability and greater randomness. Many interesting images encryption methods were reported as well, which relayed on memristive chaotic systems [55–58]. A five-dimensional memristive chaotic system was depicted and used for image encryption in Ref.[59]. The results showed that the memristive chaotic system possesses good security capabilities for image encryption. then the security of the ciphered image was tested and the encryption effect was very well. Ref.[60] proposed a novel image encryption algorithm based on the Chua's memristive circuit system and the proposed encryption technique has stronger anti-crack ability as compared to the other existing algorithms. [58] applied the memristive chaotic system for image encryption with DNA variation and gained satisfactory expectation

in performance testing.

Utilising the non-associative operation of an LA-group and the chaotic sequences produced from the memristive system, an efficient algorithm is first created to build algebraic-chaotic sequences. Furthermore, a strategy for the encryption of RGB images is developed, where the chaotic sequences from the four-dimensional memristive chaotic system and the algebraic-chaotic sequences are utilised in the confusion and diffusion phase of the encryption. The underlying concept behind the design of this technique is to enhance both robustness and the size of the key space due to the non-associative behavior of algebraic structure and the hyperchaotic properties of 4D memristive system. The designed encryption scheme has high confusion/diffusion creating capabilities due to the structural properties of the memristive system and LA-group and fulfills the necessary requirements for the secure encryption scheme. The proposed encryption scheme demonstrates high efficiency in terms of robustness, security and computational speed, making it a promising solution for secure data transmission and protection.

2.2 The Memristive Chaotic System

2.2.1 Background

Chua's circuit, the famous third-order autonomous system was designed by Leon O. Chua in 1983. This simple non-linear electronic circuit can exhibit a variety of dynamical behaviours including chaos or chaotic phenomena and bifurcations depending on different circuit parameters. This classical Chua's circuit comprised of two capacitors, an inductor, one active resistor and one non-linear resistor also referred to as Chua's diode. There are numerous ways in which the classical Chua's circuit can be changed to create a more complex system with chaotic behaviour. In 1971, "Memristor-The Missing Circuit Element" paper was published by Leon O. Chua [61]. In this paper, the original theoretical framework for memristors (a contraction for memory resistor) were provided. It is the fourth basic non-linear circuit element which took place along side the other well-known circuit components such as the resistor, capacitor, and inductor. Through this paper, it was revealed that this element exhibits unusual behaviour that differs from the other circuit elements. These characteristics enable a variety of novel applications that are not possible with RLC

networks alone.

For over thirty years, the memristor did not have much of an impact on circuit theory as a result, academics have not given memristor research enough attention. In 2008, the research team led by Strukov at Hewlett-Packard (HP) laboratory published a paper titled as "The missing memristor found" [62] in which they claimed to have produced a nano-sized TiO_2 solid-state memristor and cemented its position as the fourth circuit component. This paper validates Chua's theory on memristors and highlights the transition of relevant research from the theoretical phase to practical implementation. Since then it has drawn the interest of researchers from a variety of fields and a dynamic development process has begun in the investigation and application research on the memristor principle [63–65]. Memristors have excellent features such as lower power consumption, nano-size, and non-volatility as a result the applications based on memristors have been studied in a variety of fields including artificial neural network [52, 66], secure communication [51, 67] etc. It is a highly effective nonlinear circuit component for creating chaotic circuits and the generation of chaotic dynamics. The memristive chaotic circuit serves a crucial role not only to analyze the nonlinear dynamical characteristics of memristors but also holding significant application value in various fields related to chaos. When employed in image encryption, the memristive chaotic systems provide excellent security due to their high unpredictability and randomness compared to the general chaotic systems.

2.2.2 Mathematical Model and its Dynamical Analyses

The classical Chua's circuit was modified to obtain the new four-dimensional memristive system [58]. The mathematical expression of the utilized system based on memristor is described by the following differential equations:

$$\begin{aligned}\dot{x} &= ay + bx - cW(w)x \\ \dot{y} &= z - (y - x) \\ \dot{z} &= -(\alpha y + \beta z) \\ \dot{w} &= x\end{aligned}\tag{2.1}$$

Where $W(w) = s + 3t(w^2)$ is the memristor and parameters 's' and 't' are constants. By selecting parameters values such as $s = 0.2$, $t = 0.4$, $c = 16.4$, $\alpha = 15$, $a \in [15.2, 16.6]$, $b \in [6.3, 7.3]$, $\beta \in [0.52, 0.62]$ the memristive system exhibits chaotic

behavior. Fig.2.1 and Fig.2.2 show 2D and 3D chaotic attractors respectively, portraying the behavior of the memristive system with $a = 16.4$, $b = 6.56$, $\beta = 0.5$ and base values (0.2, 0.1, 0.1, 0.1). The Lyapunov exponents of the memristive system are obtained as 0.3329, 0.0001, - 0.0066, - 7.8613 which indicates that the system can be used for image encryption and has good chaotic dynamical properties.

The bifurcation diagram and the Lyapunov exponent are employed as the standard analysis tools to investigate the performance and characteristics of the memristive chaotic system. In Fig.2.3 bifurcation diagrams are presented while Fig.2.4 illustrates the Lyapunov exponents when the parameter values are chosen as $z \in [15.2, 16.6]$, $b \in [6.3, 7.3]$, $\beta \in [0.52, 0.62]$ and keeping other values fixed. As can be seen from Fig.2.3 the chaotic states of the system are the colour ranges with colour depths larger than 5 while other ranges correspond to periodic states. In conclusion, the memristive system have a significantly wide range of parameters, indicating its exceptional suitability for image encryption purposes.

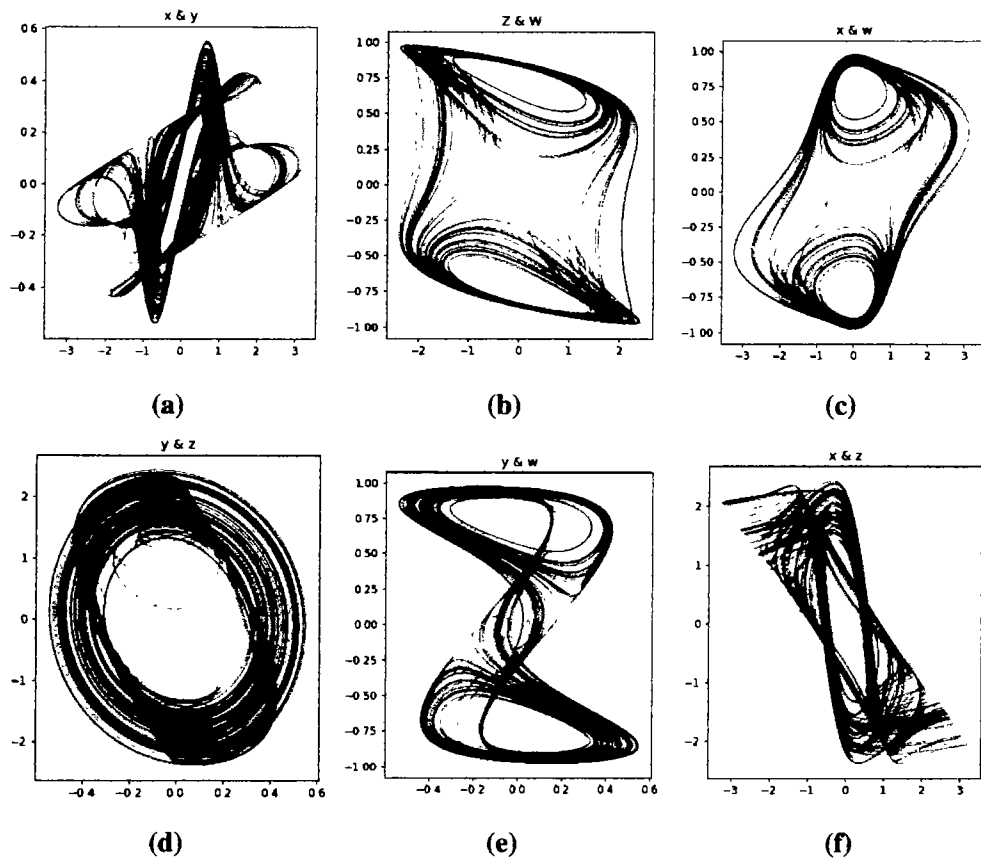


Figure 2.1: 2D chaotic attractors of the 4D memristive chaotic system

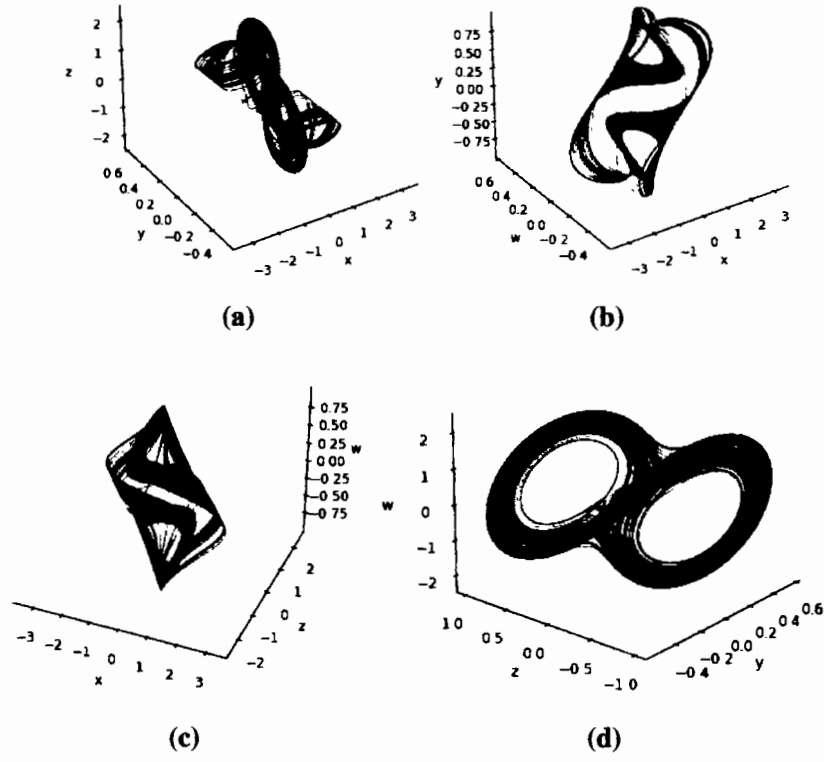


Figure 2.2: 3D chaotic attractors of the 4D memristive chaotic system

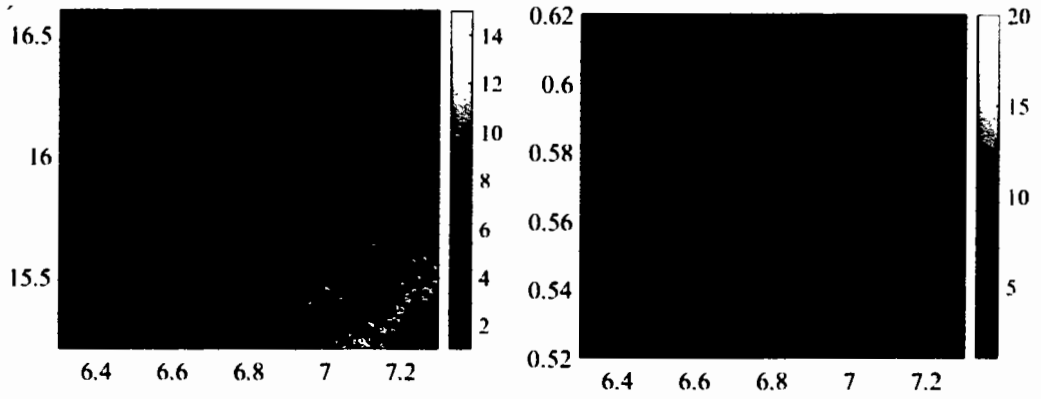


Figure 2.3: Bifurcation diagrams (a) $a \in [15.2, 16.6]$ and $b \in [6.3, 7.3]$ (b) $a \in [15.2, 16.6]$ and $\beta \in [0.52, 0.62]$

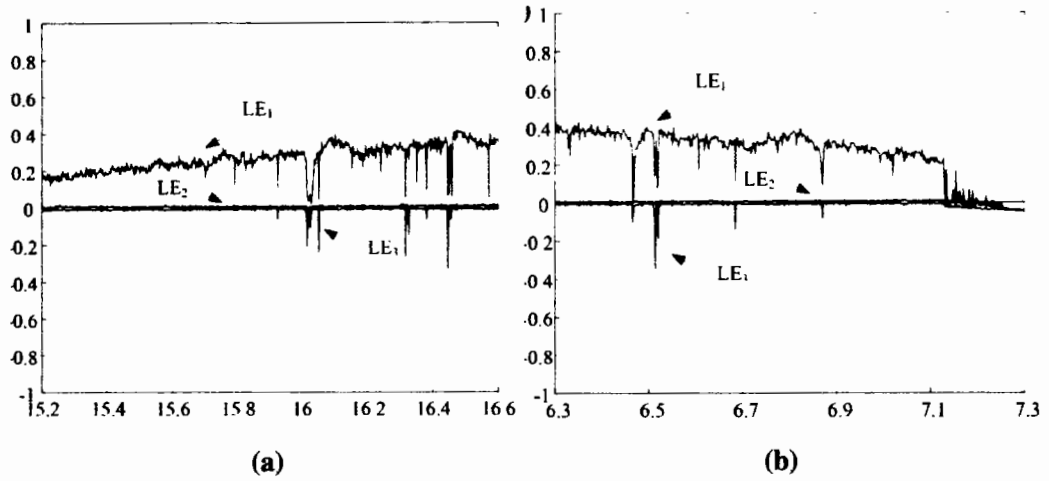


Figure 2.4: Lyapunov exponents (a) $a \in [15.2, 16.6]$ (b) $b \in [6.3, 7.3]$

2.3 Construction of Algebraic-Chaotic Sequences over LA-group with Memristive System

The method for the formation of algebraic-chaotic sequences using an LA-group and four-dimensional memristive chaotic system is presented in this section.

2.3.1 Generating Algorithm for the Proposed Algebraic-Chaotic Sequences

By employing four random sequences obtained from a memristive chaotic system and the operation of a non-associative algebraic structure LA-group, the algorithm is designed. These four chaotic sequences are then subsequently employed in the encryption process of RGB images. The execution of the algorithm involves a series of sequential steps as described below:

Step 1 Obtaining an LA-group of order 256 In this step, first a software MACE 4 [68] is used to obtain an LA-group of order 16 $L = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15\}$ with the operation given by the Table 2.1. Then the Cartesian product of L with itself, denoted as $P = L \times L$ is considered. P is again an LA-group consisting of 256 elements which are ordered pairs of elements in L . The operation and inverses in P are defined component wise.

Step 2 Generating chaotic sequences using a memristive system In this step of algorithm, a 4D memristive system is utilized. This step is completed in following sub-steps:

- i The proposed 4D memristive chaotic system 2.1 is iterated 65,536 times using the fourth-order Runge-kutta method. Four chaotic sequences X_1, X_2, X_3 and X_4 are obtained with the system parameters $a = 16.4$, $b = 6.56$, $c = 16.4$, $\alpha = 15$, $\beta = 0.5$, $s = 0.2$, $t = 0.4$ and $(x(0) = 0.2, y(0) = 0.1, z(0) = 0.1, w(0) = 0.1)$ initial values.
- ii The following formulas are used to restrict the values of chaotic sequences X_1, X_2, X_3, X_4 obtained from the preceding step in the range 0 – 255:

$$X'_1 = \text{round}((\text{floor}(X_1 \times K_1) \bmod 256))$$

$$X'_2 = \text{round}((\text{floor}(X_2 \times K_2) \bmod 256))$$

$$X'_3 = \text{round}((\text{floor}(X_3 \times K_3) \bmod 256))$$

$$X'_4 = \text{round}((\text{floor}(X_4 \times K_4) \bmod 256))$$

where, K_1, K_2, K_3 and K_4 are random numbers generally greater than 10000. Here in this case $K_1, K_2, K_3, K_4 = 65,536$.

- iii Four chaotic sequences are designed from the results of above step in such a way that each sequence contains the unique integers between 0-255. we name these sequences as R_1, R_2, R_3 and R_4 where each sequence is of length 256.

Step 3 Constructing algebraic-chaotic sequences The procedure of constructing algebraic-chaotic sequences based on the outcomes of Step 1 and Step 2, is described step by step in the following:

- i Firstly, the four bijective mappings are defined as

$$\psi_i : R_i \longrightarrow P$$

for all $1 \leq i \leq 4$.

- ii Now consider the linear scalar multiple mapping $\phi : P \longrightarrow P$ given by $\phi(x) = xu \oplus v$ for all $x \in P$ and define the composition mappings $\delta_i =$

$\psi_i^{-1}\phi\psi_i$ such that:

$$\delta_1(x_j) = x_j u \oplus v \quad \forall x_j \in R_1$$

$$\delta_2(y_j) = y_j u \oplus v \quad \forall y_j \in R_2$$

$$\delta_3(z_j) = z_j u \oplus v \quad \forall z_j \in R_3$$

$$\delta_4(w_j) = w_j u \oplus v \quad \forall w_j \in R_4$$

for all $0 \leq j \leq 255$. Where u and v are fixed elements of P and \oplus is indication of bitwise "Exculsive OR" operation.

Four algebraic-chaotic Sequences S_1, S_2, S_3 and S_4 , each of length 256 are obtained as the output of this step. These sequences are displayed as 16×16 matrices in the Table 2.2 - Table 2.5 respectively.

Table 2.1: Operation table for 16 order LA-group

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

Table 2.2: Algebraic-chaotic sequence S_1

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

Table 2.3: Algebraic-chaotic sequence S_2

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

TH-27073

Table 2.4: Algebraic-chaotic sequence S_3

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

Table 2.5: Algebraic-chaotic sequence S_4

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

2.4 RGB Image Encryption and Decryption schemes

This section presents the proposed scheme for encrypting RGB images. The encryption process achieves the property of confusion by utilizing a 4D memristive chaotic system. While the obtained algebraic-chaotic sequences are used for the purpose of diffusion. The consolidation of a 4D memristive system and a non-associative LA-group results in a remarkable encryption technique that enhances the randomness in original data and exhibits strong resistance to a wide range of attacks.

2.4.1 Proposed Encryption Algorithm

- 1 Consider an RGB image of size $M \times M$.
- 2 Split the image into three layers red, green and blue.
- 3 Construct four algebraic-chaotic sequences S_1, S_2, S_3 and S_4 through the proposed algorithm from the section 2.3.1.
- 4 Using the memristive chaotic system, generate four chaotic sequence M_1, M_2, M_3 and M_4 , each of length $M \times M$. Arrange these sequences into $M \times M$ matrices. Multiply each of M_1, M_2 and M_3 by M_4 from left to get the matrices N_1, N_2 and N_3 .
- 5 Permute the pixels in red layer through the sequences S_1 and S_2 row-wise and column-wise respectively. Repeat this step for the green and blue layers using the sequences S_2, S_3 and S_3, S_4 respectively.
- 6 Multiply the permuted red, green and blue matrices by N_1, N_2, N_3 respectively from left to get encrypted red, green and blue channels.
- 7 At last the concatenation of all three encrypted layers obtained in the preceding step yields the encrypted RGB image.

Fig.2.5 shows the flow chart of the proposed scheme.

A 256×256 standard Lena image, Baboon image, Peppers image and House image with same dimensions have been encrypted for the experiment simulation. Fig.2.6 (a-d) display the original Lena, Baboon, Peppers and House image where Fig.2.6 (e-h) show the encrypted images resulting from the application of the proposed algorithm to the original images. On comparing the images before and after

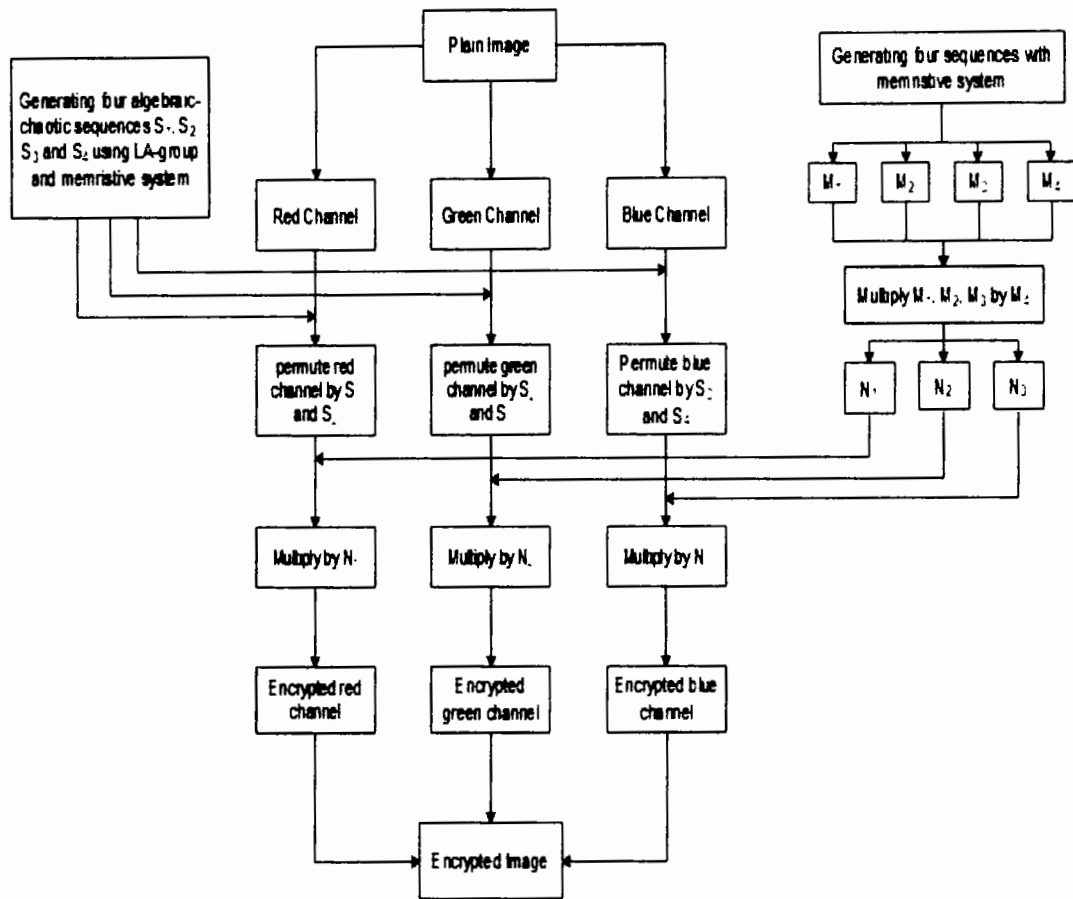


Figure 2.5: Flow chart

encryption, it becomes clear that the presented encryption algorithm has strong encryption effects. Since once the original images are encrypted, all of their original feature information is lost.

2.4.2 Decryption Scheme

The decryption method serves as the similar but reverse process of the encryption procedure. It enables us to restore the ciphered image to its original form. This decryption process requires using the same key as that employed in the encryption process. Fig.2.6 (i-l) displays the decrypted images of the images in Fig.2.6 (c-h) respectively.

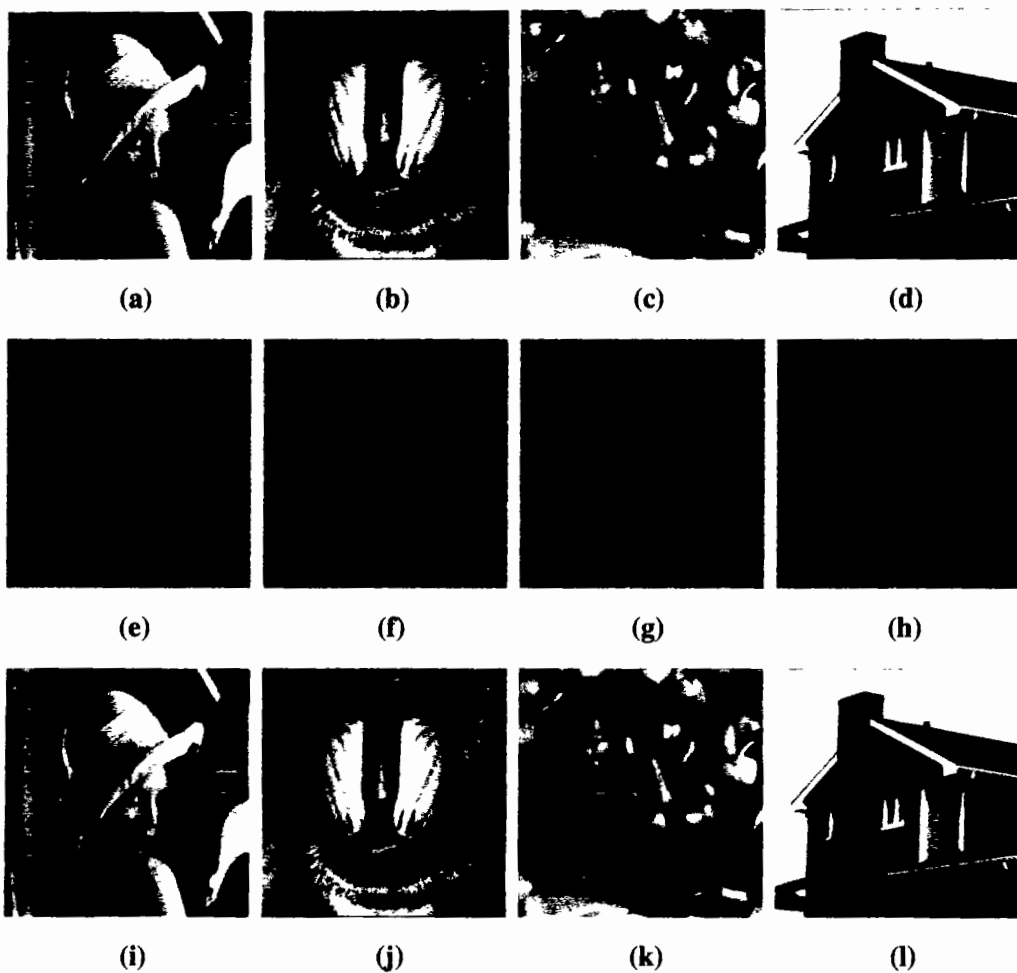


Figure 2.6: (a-d) represents Lena Image, Baboon Image, Peppers Image and House Image respectively, (e-h) display encrypted images, while (i-l) show decrypted images

Chapter 3

Security Analysis of Proposed Encryption Algorithm

This chapter focuses on conducting critical security analyses that examine the quality of the encryption. Security analysis is crucial in order to assess the resilience and effectiveness of a cryptographic scheme. An efficient encryption scheme should possess the ability to withstand various standard attacks or assaults, including occlusion and noise attacks, statistical and differential attacks etc. The strength of the suggested encryption scheme is tested by various security measures such as differential, statistical and textual analyses, occlusion and noise attack analyses and quality measures whereas experiments are performed on $256 \times 256 \times 3$ sized "Lena", "Baboon", "Peppers" and "House" images.

3.1 Differential Attack Analysis

One of the major strategy adopted by cryptanalyst to retrieve the original image is the differential attack. An essential characteristic of a cipher is the degree of sensitivity of an encrypted image to even minor modifications in the original image. As a result, it could be impossible for cryptanalyst to determine the encryption scheme by distinguishing the difference between cipher images resulting from changes in plain images. NPCR and UACI are two most common quantities that are used to estimate the strength of an encryption against the differential attack.

3.1.1 Number of Pixels Change Rate (NPCR)

NPCR is a metric used to quantify the rate of pixel variation in an encrypted image when a little disturbance is introduced to the pixel value of the original image [69]. When the NPCR value exceeds 99%, the sensitivity of the cryptosystem to variations in the original image increases significantly. This high sensitivity enhances the resistance of the cryptosystem against potential attacks from hackers, making it more robust and secure.

Consider two encrypted images, denoted as S_1 and S_2 which only differ by a single pixel. The NPCR is calculated by the following equation :

$$NPCR(S_1, S_2) = \frac{\sum_{l,m} D(l, m)}{T} \times 100\%,$$

The values $S_1(l, m)$ and $S_2(l, m)$ represent the pixel values at the grid position (l, m) in the encrypted images S_1 and S_2 respectively. The symbol T represents the total number of pixels and the difference function $D(l, m)$ at grid position (l, m) is described as follows:

$$D(l, m) = \begin{cases} 0, & \text{if } S_1(l, m) = S_2(l, m), \\ 1, & \text{if } S_1(l, m) \neq S_2(l, m) \end{cases}$$

3.1.2 Unified Average Changing Intensity (UACI)

UACI measures the average intensity change in the encrypted image compared to the original image [69]. When the UACI value approaches 33% the cryptosystem is considered more secure and provides enhanced protection against differential attacks. The value of UACI can be calculated by the following equation :

$$UACI = \frac{1}{T} \sum_{l,m} \frac{|S_1(l, m) - S_2(l, m)|}{P} \times 100\%,$$

Symbol P represents the largest allowed pixel intensity.

In Table 3.2, the UACI and NPCR measures are presented for the three color channels of the encrypted images. The analysis result shows that the NPCR and UACI values achieved by our proposed scheme are optimal. Table ?? also compares the differential analysis results of the standard Lena colour image with some recent Chaos, DNA and memristive system based encryption schemes.

Table 3.1: Differential analysis for the color components of some digital images

Image	UACI			NPCR		
	R	G	B	R	G	B
Lena	33.6228	33.4629	33.5972	99.609	99.223	99.6109
Baboon	33.6121	33.4861	33.4488	99.606	99.651	99.608
Peppers	33.4515	33.5406	33.3151	99.611	99.223	99.609
House	33.4436	33.5697	33.5278	99.640	99.602	99.632

Table 3.2: A comparison of differential analysis of Lena image

Schemes	UACI			NPCR		
	R	G	B	R	G	B
Proposed	99.609	99.223	99.611	33.622	33.463	33.597
Ref.[34]	99.63	99.62	99.62	33.51	33.32	33.46
Ref.[70]	99.59	99.59	99.59	33.03	33.31	33.03
Ref.[49]	99.66	99.63	99.62	33.4	33.4	33.4
Ref.[71]	98.5	98.5	98.5	32.1	32.1	32.1
Ref.[72]	99.60	99.60	99.60	33.48	33.48	33.48
Ref.[73]	99.602	99.620	99.609	33.248	33.497	33.387

3.2 Statistical Analysis

For an encryption scheme to be considered secure, its algorithm's ability to resist statistical analysis must be guaranteed. If a scheme survives every statistical assault, it is considered to be resilient. This section presents the statistical analysis of the suggested technique, which includes the study of the histogram, correlation, key-space and key sensitivity analyses.

3.2.1 Histogram Analysis

Histogram analysis is employed to analyze the distribution of pixel intensity values in a certain image. If the histogram of the encrypted image exhibits uniformity, it indicates that the scheme is considered good, making it resilient against various statistical attacks. In a uniform histogram, all pixel values have an equal probability of

occurrence.

In this study, 256×256 dimensional RGB Lena, Baboon, Peppers and House images are analyzed. Fig.3.1-Fig.3.4 display the histograms of the original and ciphered images. Red, green and blue layers of original images are represented by sharp edges histograms in Fig.3.1-Fig.3.4 (b-d). Whereas Fig.3.1-3.4 (f-h) show the flat histograms of three layers of ciphered images under the proposed scheme. The figures clearly demonstrate that the histograms of the encrypted images exhibit uniformity and are totally different from those of the original images. This observation provides compelling evidence that the proposed algorithm ensures sufficient security for image encryption and possesses the ability to withstand various well-known attacks.

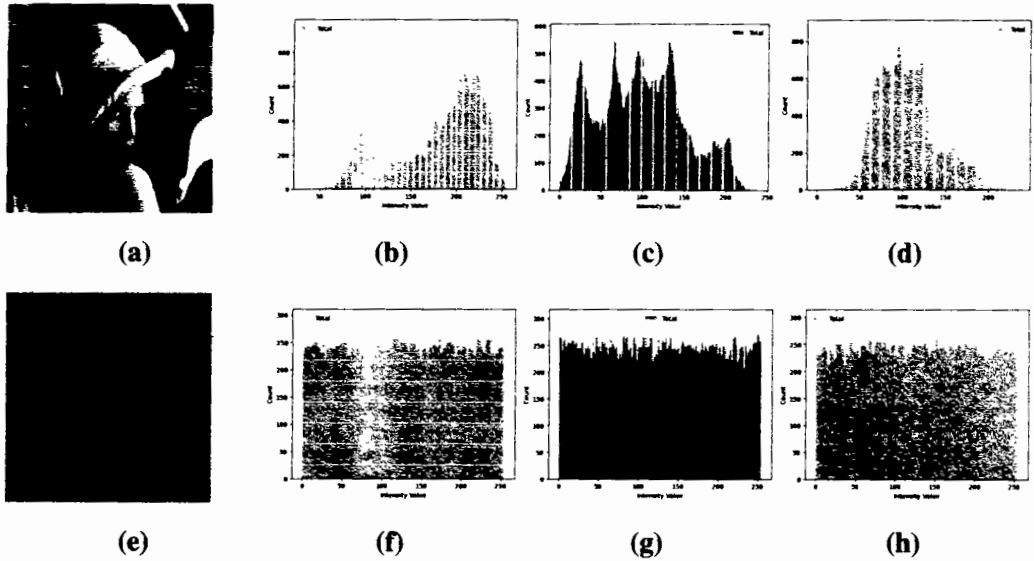


Figure 3.1: (b-d): Original Lena image color component histograms, (f-h): Encrypted Lena image color component histograms

3.2.2 Correlation Analysis

Correlation analysis is a statistical technique used to measure the closeness of adjacent pixels in an image. The correlation is determined through the use of the following equation:

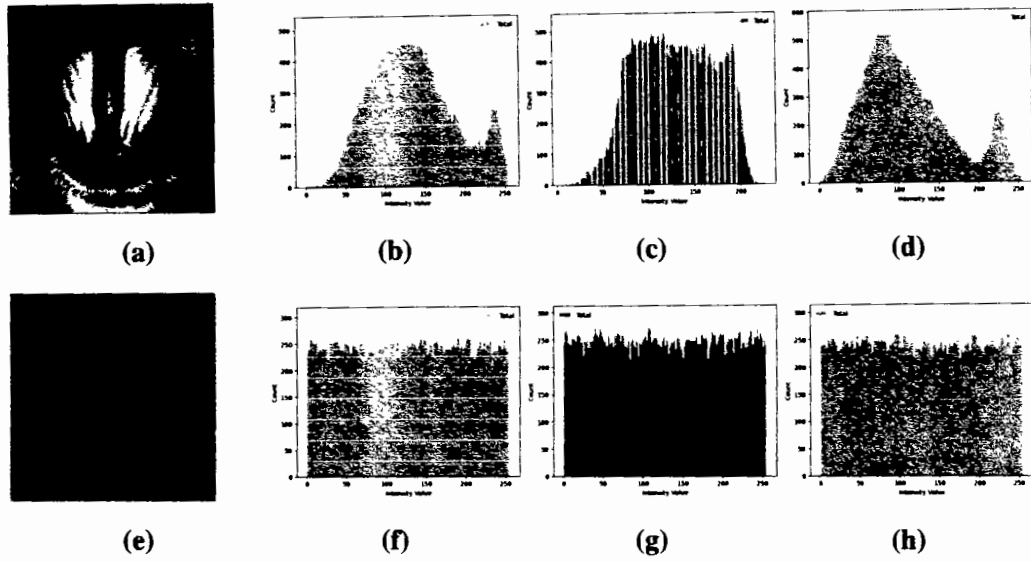


Figure 3.2: (b-d): Original Baboon image color component histograms, (f-h): Encrypted baboon image color component histograms

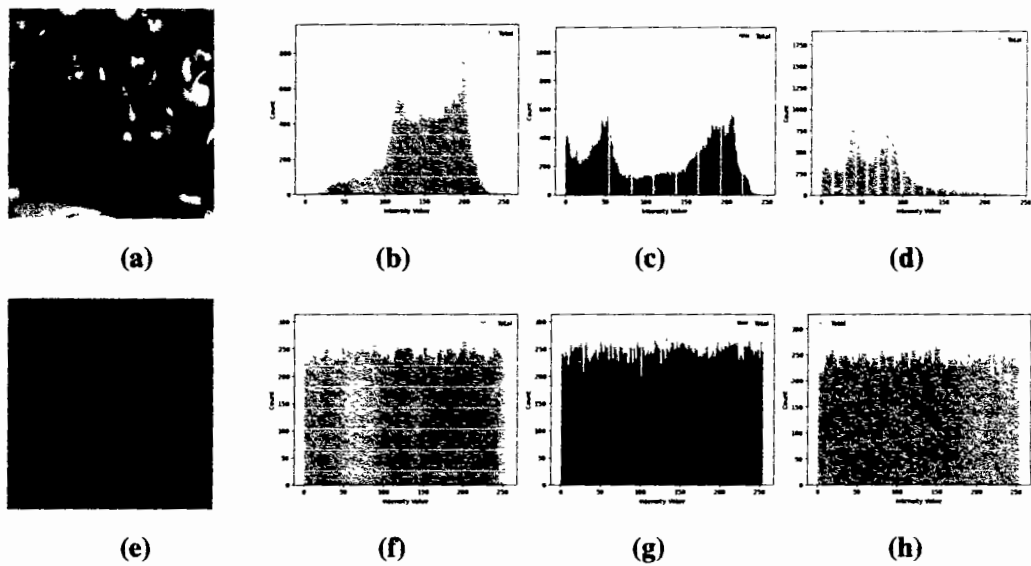


Figure 3.3: (b-d): Original Peppers image color component histograms, (f-h): Encrypted Peppers image color component histograms

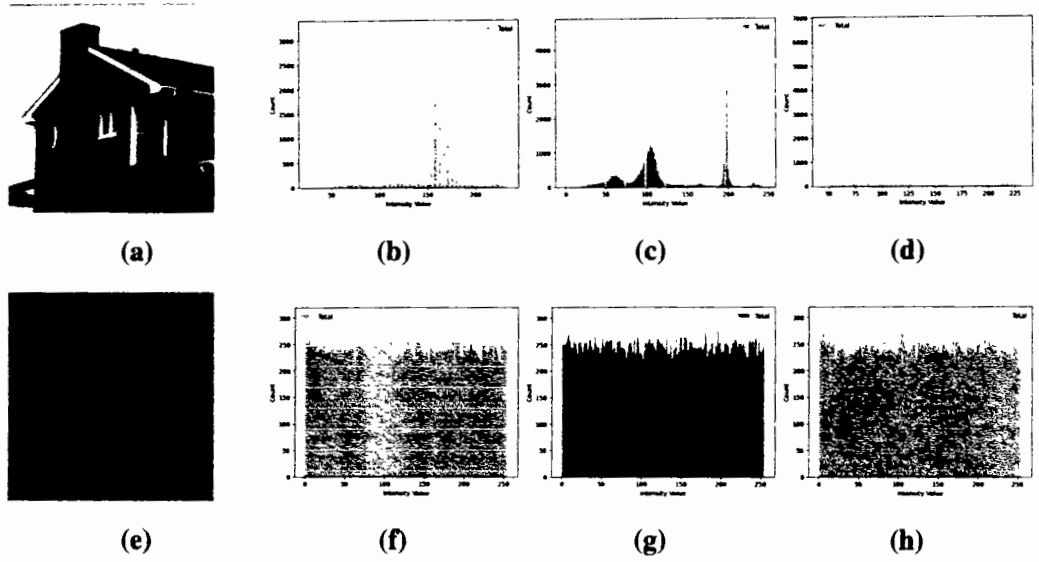


Figure 3.4: (b-d): Original House image color component histograms, (f-h): Encrypted House image color component histograms

$$K = \frac{\sum_{p,q} (p - \mu_p)(q - \mu_q) f(p, q)}{\sigma_p \sigma_q}$$

Here $f(p, q)$ represents the number of gray-level co-occurrence matrices, while μ and σ denotes the mean and standard deviation respectively. One parameter use to analyze the encryption system's resistance to various outbreaks is correlation. A cipher is considered weak against attacks if the highly correlated pixels have coefficient values in near 1 or -1, whereas for the strong encryption the coefficient values of non-correlated pixels must be close to '0'. The outcomes of correlation analysis of proposed original and encrypted RGB images in vertical, diagonal and horizontal directions are displayed in Table 3.3. The results of Table 3.3 show that the correlation values of encrypted images are close to '0', while the correlation values of plain images are almost close to '1'.

Table 3.3: Correlation analysis for RGB images

Image	Layer	Original Image			Encrypted Image		
		Horizontal	Vertical	Diagonal	Horizontal	vertical	Diagonal
Lena	R	0.9294	0.9616	0.9132	0.0091	0.0028	-0.0077
	G	0.9333	0.9633	0.9157	-0.0177	0.0059	0.0029
	B	0.8651	0.9311	0.8360	-0.0146	-0.0013	0.0104
Baboon	R	0.9813	0.9786	0.9757	0.0079	0.0230	0.0143
	G	0.9740	0.9746	0.9607	-0.0215	0.0141	0.0165
	B	0.9784	0.9706	0.9661	0.0056	-0.0055	0.0311
Peppers	R	0.9667	0.9747	0.9433	-0.0322	-0.0167	0.0064
	G	0.9803	0.9849	0.9628	-0.0177	0.0211	-0.0106
	B	0.9545	0.9694	0.9270	-0.0157	-0.0073	0.0314
House	R	0.9665	0.9272	0.9030	0.0048	-0.0336	-0.0029
	G	0.9803	0.9463	0.9227	0.0252	-0.0101	0.0184
	B	0.9809	0.9749	0.9630	0.0115	-0.0225	-0.0033

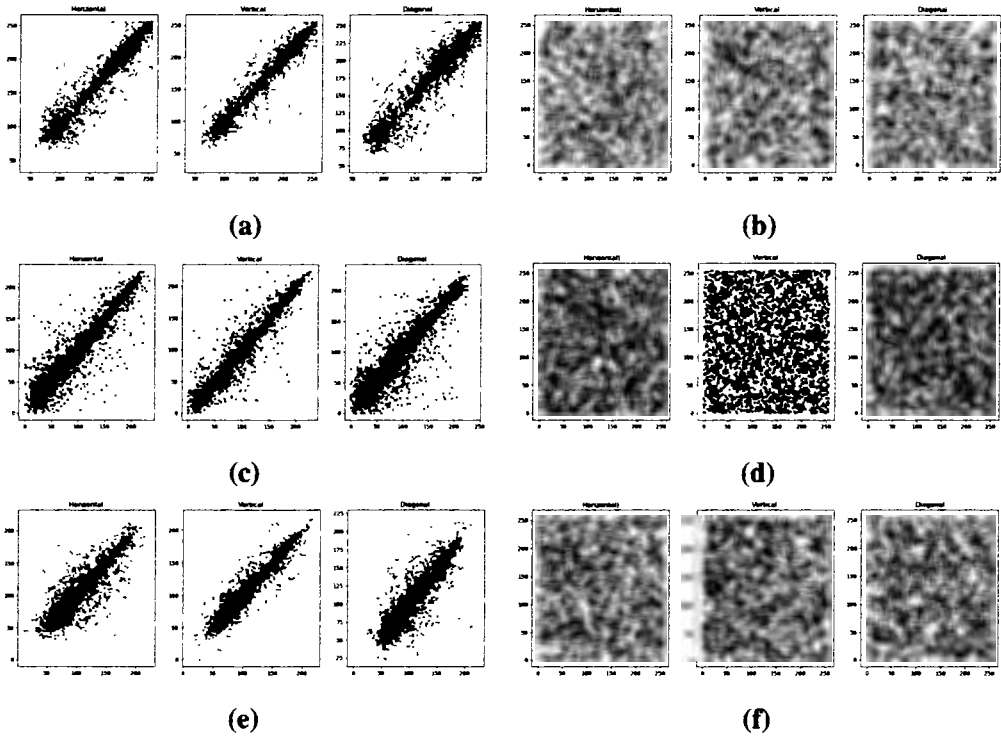


Figure 3.5: Lena Image; (a-b): Correlation of red layer of plain and encrypted image, (c-d): Correlation of green layer of plain and encrypted image, (e-f): Correlation of blue layer of original and encrypted image

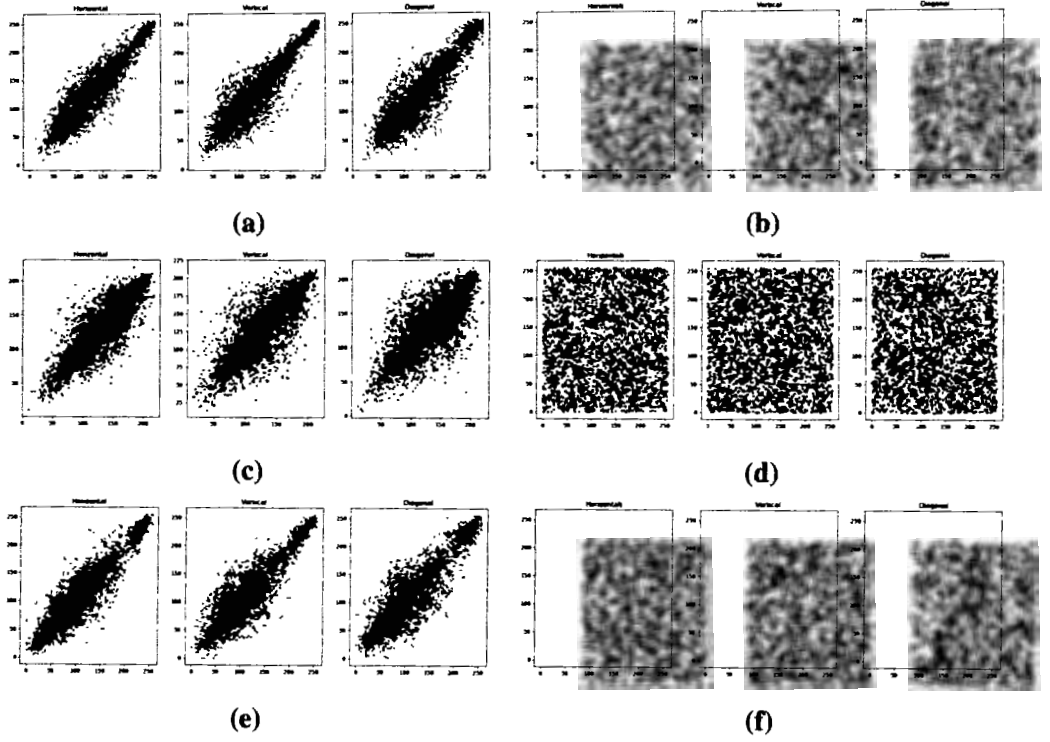


Figure 3.6: Baboon Image; (a-b): Correlation of red layer of plain and encrypted image, (c-d): Correlation of green layer of plain and encrypted image, (e-f): Correlation of blue layer of original and encrypted image

3.2.3 Key-space Analysis

The collection or set of all valid keys that can be used to encrypt data during a certain encryption technique is known as the key-space of that method. In order to effectively withstand brute-force attacks, it is crucial for the key-space of an image encryption technique to be sufficiently large i.e. greater than 2^{100} . The proposed encryption scheme involves the utilisation of parameters and base values of the memristive system, along with the parameters of the affine transformation, which relies on the cartesian product of LA-group and chaotic system. The 4 initial conditions and 7 control parameters of memristive system have key space size of 10^{15} . By considering the memristive system one for the generation of algebraic-chaotic sequences and then for the generation of chaotic matrices, the total size of the key-space becomes $((10^{15})^{11})^2 = (10^{165})^2 \approx (2^{548})^2 = 2^{1096}$. Within the set P , there are a total of 256 choices for both the fixed elements u and v . These choices collectively

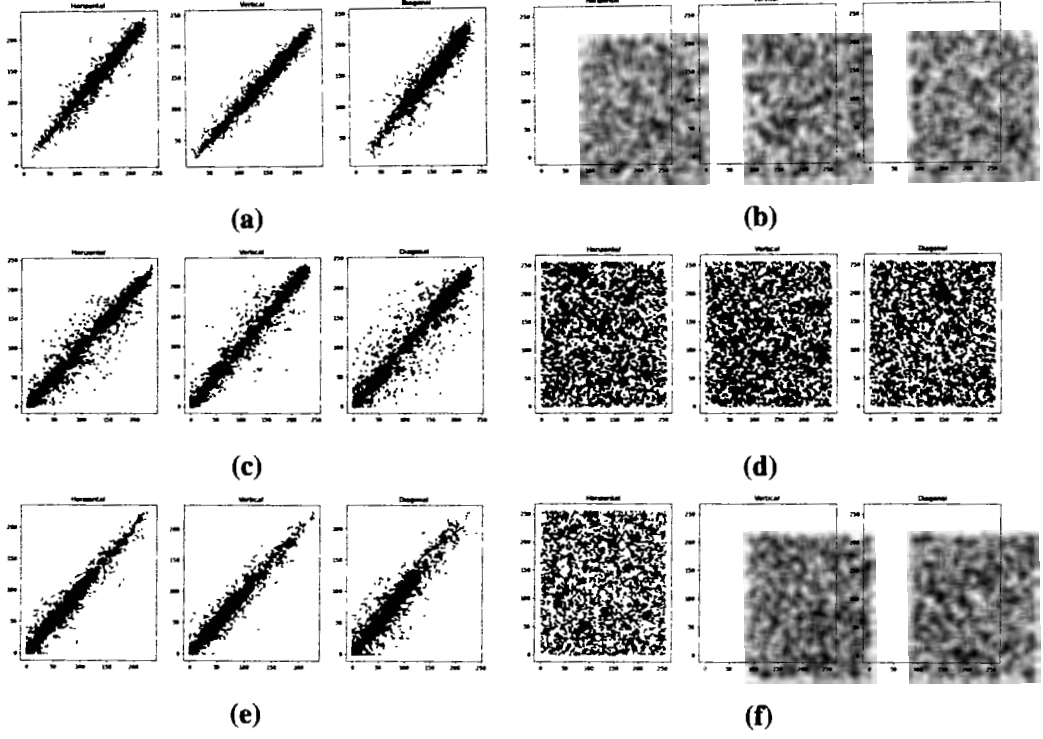


Figure 3.7: Peppers Image; (a-b): Correlation of red layer of plain and encrypted image, (c-d): Correlation of green layer of plain and encrypted image, (e-f): Correlation of blue layer of original and encrypted image

give rise to a total of 65536 possible affine mappings. Thus the encryption scheme presented in this study has a total key space size $2^{1096} \times 65536 \approx 2^{1112}$ which is much bigger than 2^{100} . So it follows that proposed encryption scheme has excellent resistance to brute force attacks.

3.2.4 Key Sensitivity Analysis

The encryption algorithm shows a remarkable level of security and sensitivity to key variations, as even a slight deviation in the key yields a completely different restored image compared to the original image. First, we used a key labelled as k_1 to encrypt given colour digital images of Lena, Baboon, Peppers and House. Where k_1 has parameters $a = 16.4$, $b = 6.56$, $c = 16.4$, $\alpha = 15$, $\beta = 0.5$, $s = 0.2$, $t = 0.4$, and initial values $(0.2, 0.1, 0.1, 0.1)$. To decrypt the encrypted images k_2 key is used which is slightly different from key k_1 . In key k_2 , the parameter a is changed 10^{15} such that $a = 16.400000000000001$ while the other parameters and initial conditions remain

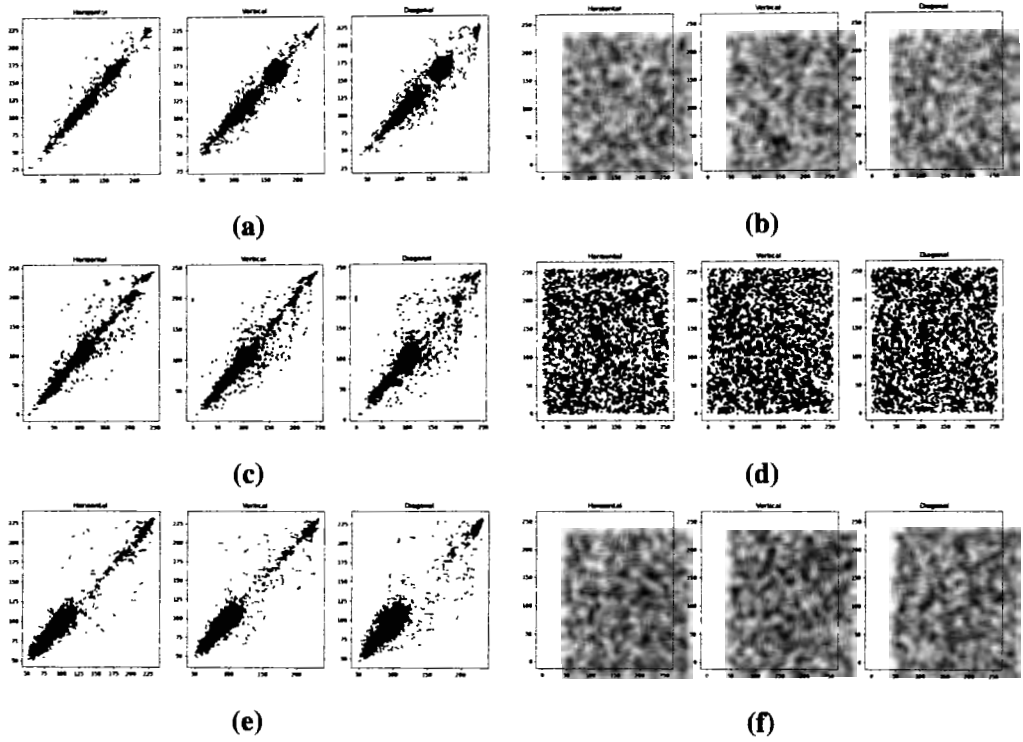


Figure 3.8: House Image; (a-b): Correlation of red layer of plain and encrypted image, (c-d): Correlation of green layer of plain and encrypted image, (e-f): Correlation of blue layer of original and encrypted image

unchanged. From Fig.3.9 it is clear that even a slight modification in the value of k_1 makes it impossible to decrypt the original image. Whereas using the key k_1 , one can retrieve the original color images. This observation emphasizes the encryption algorithm's exceptional sensitivity to the secret key.

3.3 Texture Analysis

One of the most valued features of a digital image is texture. It enlightens the outer appearance of digital image along with chromatic character. Texture analysis can be done in variety of ways. Two such ways are Fourier approach and Wavelet approach. The analysis of texture holds a captivating interest, particularly in its connection to the human visual system's perception, a very important first step in understanding the texture created by Haralick [74], and it has a wide range of application in image dissection. By this method various characteristics of an image are employed to define its texture, including contrast, homogeneity, energy, and entropy.

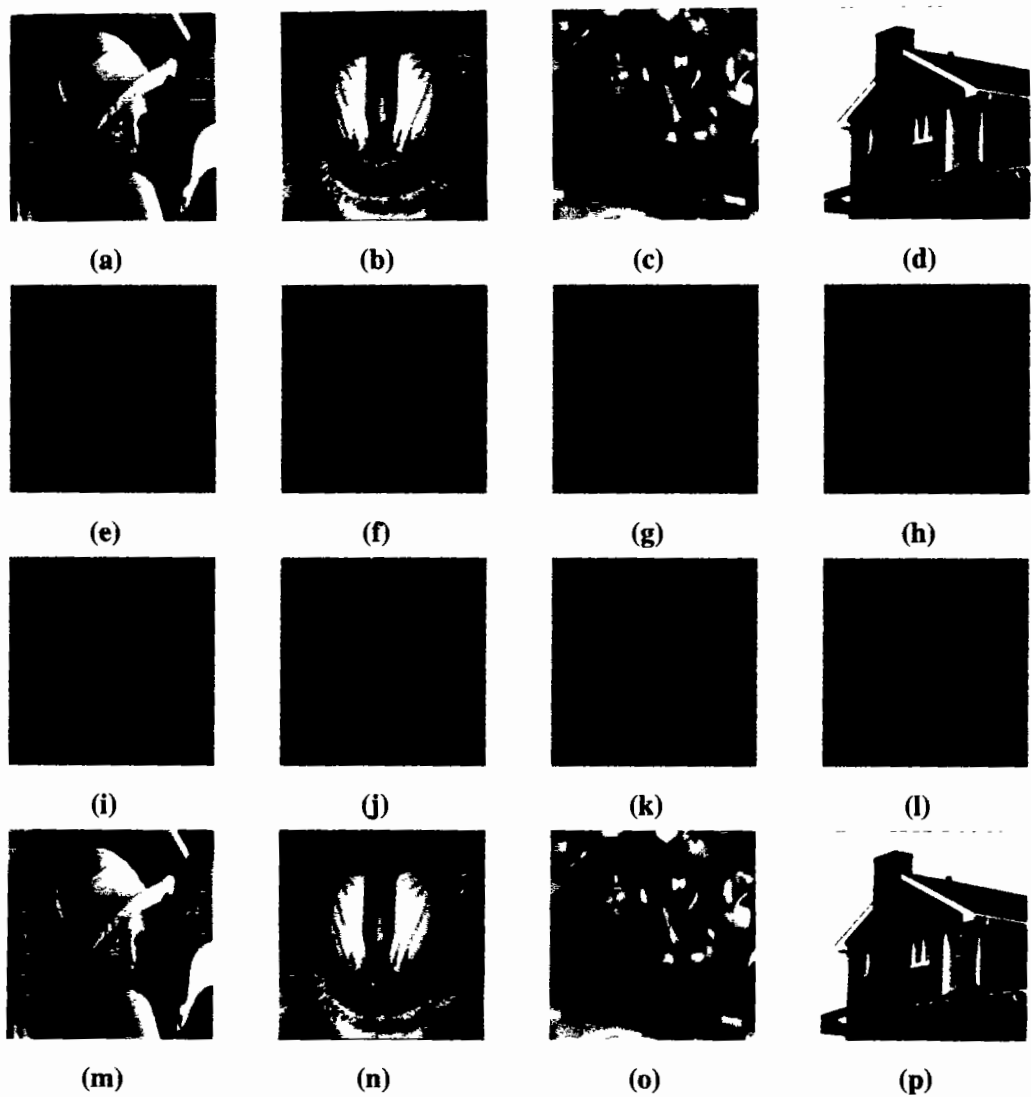


Figure 3.9: (a-d): Original images, (e-h): Encrypted images, (i-l): Decrypted images after using k_2 , (m-p): Decrypted images after using k_1

3.3.1 Entropy

Entropy is a quantitative evaluation of randomness and disorder in a system. It serves as an indicator of disturbance and utter randomness or unpredictability in the dispersion of image pixel values. As the image becomes coarser, the entropy increases proportionally. It is difficult to distinguish the image with higher entropy value due to their greater randomness which makes the encryption scheme the best opposer to various attacks. Mathematically, the entropy is represented by the following formula:

$$H(z) = - \sum_{k=1}^l p(z_k) \log_b p(z_k)$$

where z_k indicates the histogram calculations.

The entropy value approaches '8' for an ideal random image. If an encrypted image has an entropy value under '8' then this could leads to consistency and a risk to anticipated security. The results listed in Table 3.4 shows the values of entropy analysis of each layer of enciphered color images. Table 3.5 demonstrate that the entropy values obtained from the proposed scheme are significantly closer to the optimal value in comparison to other referenced schemes. This observation signifies that the novel encryption scheme exhibits a high level of robustness against entropy attacks.

Table 3.4: Entropy analysis for RGB images

Image	Original Image				Encrypted Image			
	R	G	B	RGB	R	G	B	RGB
Lena	7.3106	7.6088	7.0825	7.7789	7.9972	7.9969	7.9974	7.9991
Baboon	7.6778	7.3683	7.7061	7.7040	7.9971	7.9972	7.9971	7.9990
Peppers	7.3649	7.6587	7.1746	7.7642	7.9973	7.9969	7.9970	7.9990
House	6.4311	6.5389	6.2320	7.0686	7.9972	7.9973	7.9971	7.9992

3.3.2 Contrast

Contrast analysis involves the evaluation of the variations in pixel intensity values within an image, particularly focusing on the difference between light and dark areas. During the encryption of an image the amount of disorderness increases

Table 3.5: Entropy comparison for Lena image

Algorithms	R	G	B	RGB
Proposed	7.9972	7.9969	7.9974	7.9991
Ref.[75]	7.9972	7.9965	7.9962	7.9987
Ref.[70]	7.9977	7.9945	7.9943	7.9955
Ref.[50]	7.9967	7.9973	7.9970	7.9991
Ref.[76]	7.9917	7.9912	7.9917	7.9915
Ref.[77]	7.9913	7.9914	7.9916	7.9914

which rises the level of the contrast to an extremely high level. A robust encryption is indicated when the contrast reaches its maximum value. That is why, there is a direct relation between the value of contrast and uncertainty of ciphered image. The value of this factor is directly correlated with the level of confusion in the data, as it increase when the confusion in data increases. The contrast is obtained by the following equation:

$$C = \sum_l \sum_m (l - m)^2 f(l, m)$$

Here ' l ' and ' m ' represent the pixels of image, while $f(l, m)$ is representation of the numbers of grey-scale co-occurrences matrices. When applied to a constant image, the resulting contrast value is '0'.

3.3.3 Homogeneity

The data of an image is distributed naturally in relation to the contents of the associated image. Homogeneity analysis in image encryption involves quantifying the degree of proximity or closeness between elements within GLCM to its diagonal. The tabular form of the GLCM illustrates the combinations of pixel brightness values or gray-levels. The encryption scheme works better when homogeneity drops near to zero. The mathematical form of this analysis is given as:

$$H = \sum_l \sum_m \frac{f(l, m)}{1 - |l - m|}$$

3.3.4 Energy

The gray-level co-occurrence matrix (GLCM) is utilized in the process of energy analysis. Energy is obtained by adding the squared components of the GLCM. The

Table 3.6: Texture analyses of RGB Images

Image	Layer	Plain Image			Encrypted Image		
		Contrast	Energy	Homogeneity	Contrast	Energy	Homogeneity
Lena	R	0.5512	0.1234	0.8444	10.3531	0.0156	0.3917
	G	0.5835	0.0902	0.8463	10.4822	0.0156	0.3892
	B	0.5449	0.1528	0.8451	10.5093	0.0156	0.3886
Baboon	R	1.0237	0.0572	0.8198	10.5020	0.0156	0.3907
	G	1.0460	0.0652	0.7207	10.5059	0.0156	0.3897
	B	1.1013	0.0533	0.7118	10.6007	0.0156	0.3880
Peppers	R	0.4200	0.1229	0.8681	10.4500	0.0156	0.3901
	G	0.5395	0.1032	0.8608	10.5118	0.0156	0.3893
	B	0.3945	0.1568	0.8697	10.4714	0.0156	0.3903
House	R	0.4598	0.1589	0.8454	10.4489	0.0156	0.3907
	G	0.6579	0.1915	0.8797	10.5005	0.0156	0.3892
	B	0.5810	0.1649	0.8468	10.4457	0.0156	0.3882

mathematical representation of energy is:

$$E = \sum_l \sum_m f^2(l, m)$$

For a constant or uniform image, the energy value is equal to '1'.

Table 3.7 shows the texture assessment of the plain and encrypted RGB images which reveals that the energy is low, the value of contrast is quite high and the homogeneity is also decreasing. We may conclude from these results that the proposed encryption scheme that uses amalgamation of non-associative algebra and memristive system is effective.

3.4 Image Quality Measures

Researchers pay more attention to security analyses rather than the quality of the original and enciphered images. The user may face the enciphered images with some distortion resulting from the image encryption algorithm. Therefore, ensuring the quality of images is also an important issue. For this purpose, some image quality metrics [78] are performed. These are calculated by MSE, PSNR, AD, SC,

NAE, NCC, RMSE, MD, UQI and SSIM.

3.4.1 Mean Square Error (MSE)

The mean square error is characterized as the squared average difference between the original image and the cipher image. The higher value of MSE is an evidence of excellent encryption scheme. The mathematical formulation of MSE is:

$$MSE = \frac{1}{h \times w} \sum_{s=1}^h \sum_{t=1}^w [O(s, t) - C(s, t)]^2$$

Where $O(s, t)$ and $C(s, t)$ are the location of pixel at s^{th} row and t^{th} column of original and ciphered image and $h \times w$ is the size of image. 0

3.4.2 Peak Signal-to-Noise Ratio (PSNR)

Corrupting noise may comprise the reliability of the signal representation. Peak signal-to-noise ratio is a measure of how strong a signal is compared to corrupting noise [79]. Original image serves as the signal, while noise refers to the distortion that arises as a result of the encryption process. Mathematically PSNR is defined as:

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

Where I_{max} denotes a pixel's highest possible value in an image.

3.4.3 Average Difference (AD)

The average difference [79] is calculated as the mean of the deviations between the plain image and ciphered image. The larger value of the AD represents the excellent image encryption scheme, while the zero value of AD shows that both images are identical. Mathematically, the average difference is represented by the following expression:

$$AD = \frac{1}{h \times w} \sum_{s=1}^h \sum_{t=1}^w [O(s, t) - C(s, t)]$$

3.4.4 Structural Content (SC)

The structural content [79] is one of the correlation based measure that computes the the resemblance between any two images. It deals with the structural position

of pixels in the images to show the close connection between them. The quality of the image decreases as the value of SC increases. When two nearly identical images are taken into account, its value approaches '1'. Formula to calculate SC is given below:

$$SC = \frac{\sum_{s=1}^h \sum_{t=1}^w [O(s, t)]^2}{\sum_{s=1}^h \sum_{t=1}^w [C(s, t)]^2}$$

3.4.5 Normalized Absolute Error (NAE)

The Normalized absolute error [78] is a metric used to assess the dissimilarity or discrepancy between two images (original and ciphered) and is calculated by the following equation:

$$NAE = \frac{\sum_{s=1}^h \sum_{t=1}^w |O(s, t) - C(s, t)|}{\sum_{s=1}^h \sum_{t=1}^w |O(s, t)|}$$

A higher NAE value indicates a lower quality of the image obtained after the encryption process.

3.4.6 Normalized Cross Correlation (NCC)

The normalized cross-correlation [80] measure quantifies the similarity between two signals or images and is mathematically defined as:

$$NCC = \frac{\sum_{s=1}^h \sum_{t=1}^w \frac{O(s, t) \times C(s, t)}{\sum_{s=1}^h \sum_{t=1}^w [O(s, t)]^2}}$$

The value of NCC ranges between '-1' and '1'.

3.4.7 Root Mean Square Error (RMSE)

RMSE computes the square root of the average of the squared errors. It is frequently used method to evaluate the variation of an encrypted image compared to the plain image. The equation for obtaining the RMSE is as follows:

$$RMSE = \sqrt{\frac{1}{h \times w} \sum_{s=1}^h \sum_{t=1}^w [O(s, t) - C(s, t)]^2}$$

3.4.8 Maximum Difference (MD)

The extreme value of the error signal, which represents the differentiation between the plain and the ciphered images, is assessed through the utilisation of the maximum difference. [78]. MD is obtained by the following mathematical formula:

$$MD = \max |O(s, t) - C(s, t)|$$

3.4.9 Universal Quality Index (UQI)

UQI is a metric that measures the similarity between the plain and encrypted images based on factors such as structural information, luminance, and contrast [81]. The formula for calculating the Universal Image Quality Index is as follows:

$$UQI = \frac{4\sigma_{PQ}\mu_P\mu_Q}{(\sigma_P^2 + \sigma_Q^2)(\mu_P^2 + \mu_Q^2)}$$

Where μ_P, μ_Q are the means of plain and the encrypted images while σ_P^2, σ_Q^2 are their variances. The UQI value falls within the range of [-1, 1]. In the case of identical images, the maximum UQI value attainable is '1'.

3.4.10 Structural Similarity Index Metric (SSIM)

A more advanced variant of UQI is the SSIM [69]. This technique quantifies the resemblance between two images. If an image maintains a flawless quality, then SSIM acts as the standard by which subsequent images's quality is measured. The structural similarity index makes estimations on various frames P and Q of equal size $h \times w$:

$$SSIM(P, Q) = \frac{(2\mu_P\mu_Q + e_1)(2\sigma_{PQ} + e_2)}{(\mu_P^2 + \mu_Q^2 + e_1)(\sigma_P^2 + \sigma_Q^2 + e_2)}$$

Where μ_P and μ_Q are the averages and σ_P^2 and σ_Q^2 are variances of P and Q respectively, while σ_{PQ} indicates the covariance. Two variable quantities $e_1 = (r_1 S)^2$ and $e_2 = (r_2 S)^2$ are utilised to soothe the division with the low denominator. S represents the dynamic range of the pixel values, while r_1 and r_2 default to 0.01 and 0.03, respectively. The SSIM index is bounded within the range of [-1, 1], where a value of '1' signifies identical images.

Table 3.7 presents a compilation of the image quality measures, demonstrating that the proposed scheme achieves optimal values.

Table 3.7: Quality Analyses for RGB Images

Image	Layer	Image Quality Measures									
		MSE	PSNR	AD	SC	NAE	NCC	RMSE	MD	UQI	SSIM
Lena	R	7881.4386	7.866247	52.05177	1.60336	0.46944	0.65849	103.0927	255	0.00231928	0.01038284
	G	8883.7614	8.64483	-27.8316	0.58054	0.78403	1.00498	94.2537	254	0.00804133	0.00867432
	B	7106.5788	9.61419	-22.15744	0.56649	0.67005	1.09212	84.3005	248	-0.00520932	0.01123198
Baboon	R	8333.8522	8.92235	9.5979	0.9987	0.55079	0.80661	91.2899	255	-0.00251514	0.01100109
	G	7284.5535	9.50677	1.62434	0.85290	0.55172	0.88853	85.3496	255	-0.00260106	0.00765116
	B	9014.5345	8.58137	-14.10697	0.74469	0.69131	0.88992	94.9449	255	0.00030038	0.00565732
Peppers	R	7881.4386	9.16475	22.07784	1.12527	0.49173	0.78173	88.7775	240	-0.00244739	0.01042050
	G	10741.4335	7.82018	-11.98575	0.85596	0.73421	0.79377	103.6409	255	0.00248359	0.00823595
	B	10835.0625	7.78249	-59.89987	0.29152	1.26873	1.35293	104.0916	255	-0.00371107	0.00639351
House	R	6817.5701	9.79451	19.06799	1.03723	0.47377	0.82947	82.5686	226	0.00093093	0.00801144
	G	8559.2290	8.80646	5.84549	0.96365	0.57358	0.81226	92.5161	255	0.00264022	0.00786989
	B	9517.7206	8.34547	14.72746	1.11460	0.56320	0.74998	97.5588	230	-0.00450747	0.00917247

3.5 Occlusion Attack Analysis

During the transmission of encrypted images through a communication channel, there is a possibility of information loss due to network congestion or damage, which can complicate the deciphering process of plain images. The occlusion attack analysis is employed to assess the limitations of restoring the original images from encrypted images when some portion of it have been dropped. Different occlusion patterns are applied to the cypher images during an occlusion attack, and the decryption procedure is carried out on the occluded images. This analysis helps in determining the strength and resilience of the image encrypting scheme. Fig.3.10-Fig.3.13 (a-c) show the ciphered images with occlusion attack and Fig.3.10-Fig.3.13 (d-f) give the corresponding recovered images. The analysis indicate that the designed algorithm is remarkably efficient in countering or resisting occlusion attacks, displaying excellent robustness.

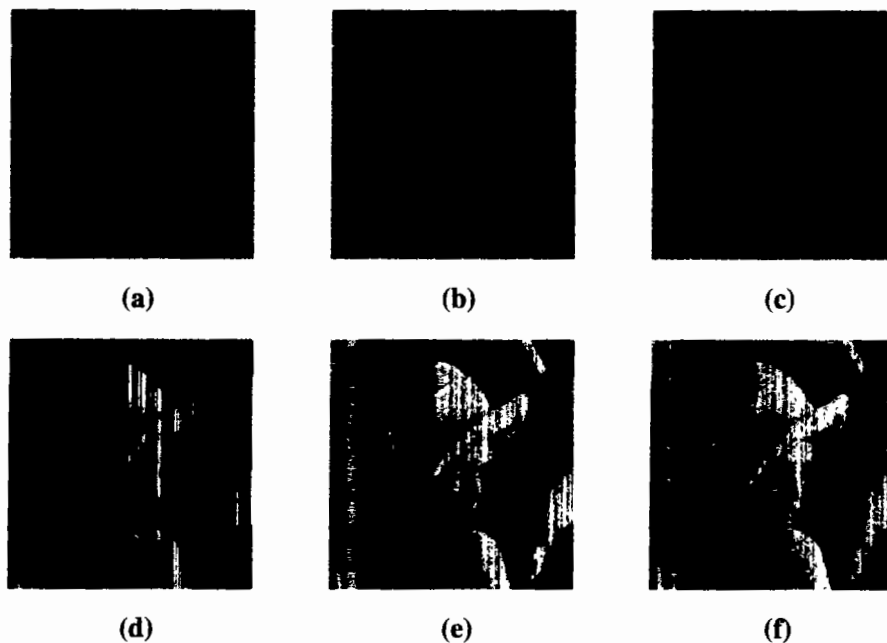


Figure 3.10: (a-c) represent encrypted Lena images with 23.44%, 5.49% and 7.34% occlusion, while (d-f) represent their decrypted images respectively

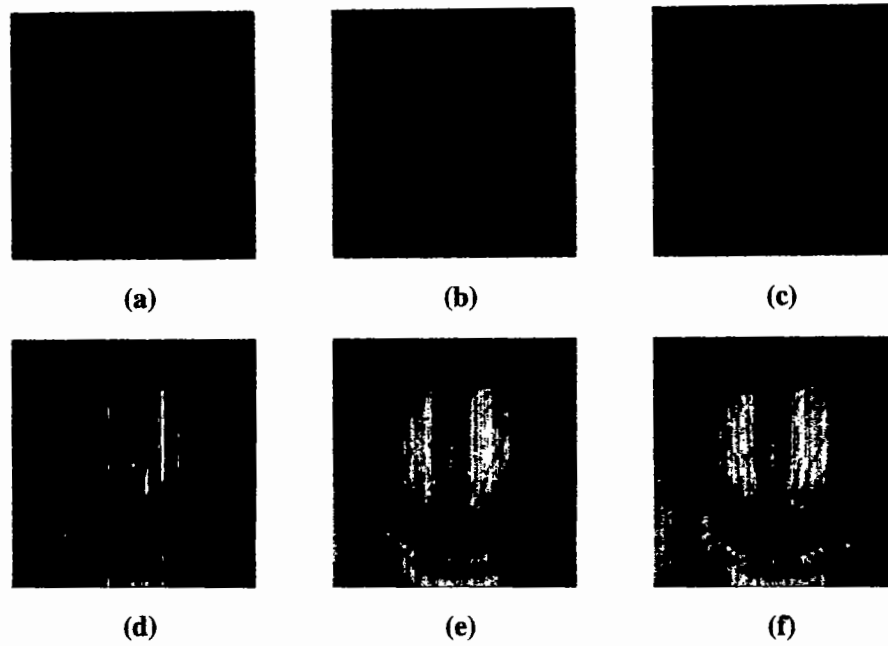


Figure 3.11: (a-c) represent encrypted Baboon images with 23.44%, 5.49% and 7.34% occlusion, while (d-f) represent their decrypted images respectively

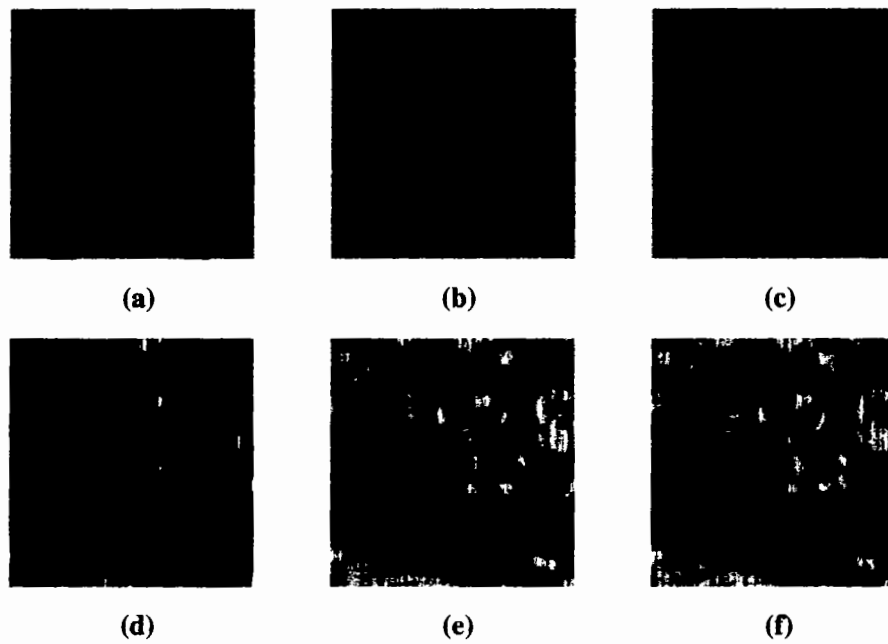


Figure 3.12: (a-c) represent encrypted Peppers image with 23.44%, 5.49% and 7.34% occlusion, while (d-f) represent their decrypted images respectively

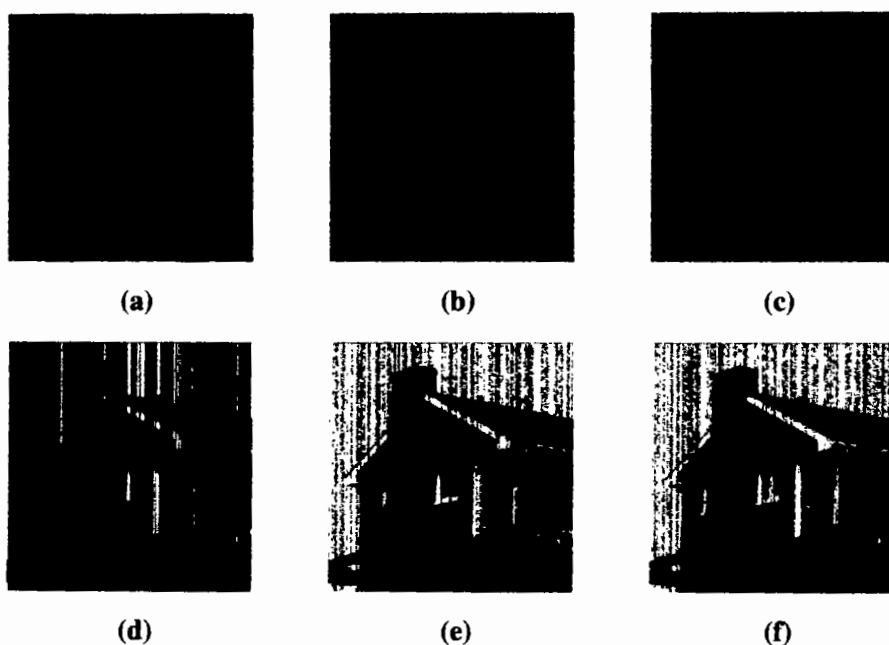


Figure 3.13: (a-c) represent encrypted House image with 23.44%, 5.49% and 7.34% occlusion, while (d-f) represent their decrypted images respectively

3.6 Noise Attack Analysis

During the transmission of cipher images, various types of noise can be induced, which can pose challenges in accurately recovering the original plain images. When encrypted images are transmitted over a channel, noise can be produced due to various factors such as communication errors, electromagnetic interference, compression artifacts, or environmental disturbances. The noise attack evaluates the algorithm's ability to withstand the addition of noise in the ciphered image. An effective encryption technique should make sure that the inclusion of noise does not compromise the comprehensibility of the decrypted image.

Salt and pepper noise is a commonly encountered form of noise that primarily arises from incorrect alterations during the transmission or analog-to-digital (A/D) conversion of elements. It appears in the form of scattered random white and black pixels within an image, creating a visual effect similar to the presence of salt and pepper grains. The occurrence of salt and pepper noise can result in a deterioration of image quality and visual appearance making it challenging to interpret or process. The ciphered images (shown in Fig.2.6(e-h)) have salt and pepper noise added to them with varying densities of 0.1% and 5% in order to assess the resilience of the algo-

rithm against noise. By applying the decryption algorithm to the ciphered images, decrypted images are obtained and are depicted in Fig.3.14-3.17. The experimental result demonstrate that when salt and pepper noise is introduced to the encrypted images, the decrypted images may suffer from some degree of damage. However, despite this, it is still possible to distinguish the essential elements of the original images.

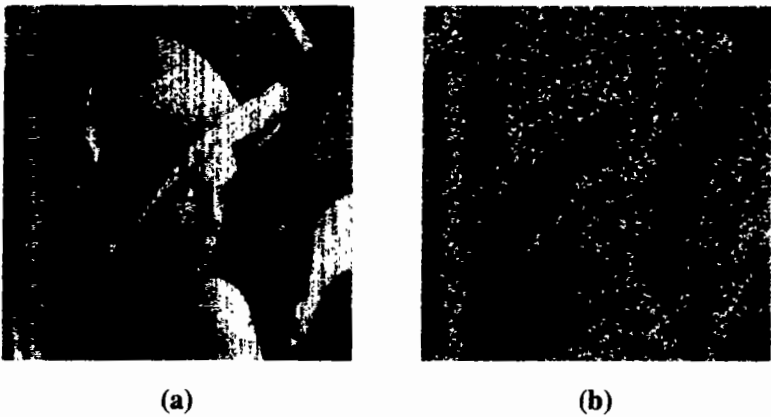


Figure 3.14: The noise attack analysis: (a) and (b) represent decrypted images of Lena with salt and pepper noise level of 0.1% and 5% respectively

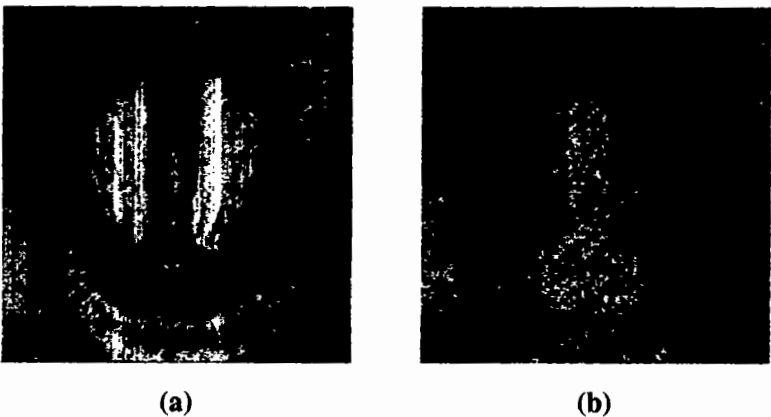


Figure 3.15: The noise attack analysis: (a) and (b) represent decrypted images of Baboon with salt and pepper noise level of 0.1% and 5% respectively

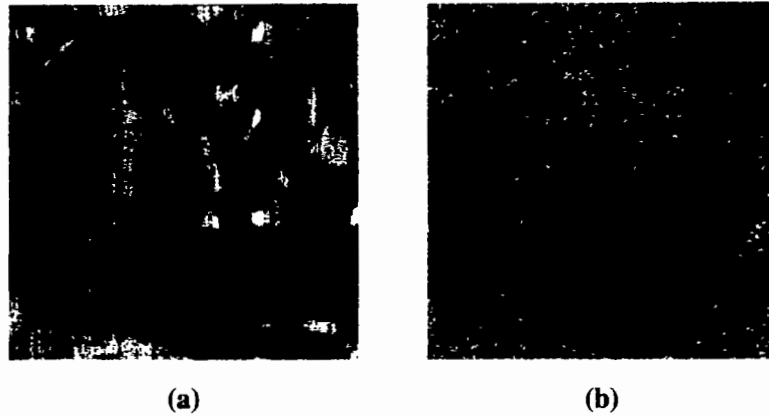


Figure 3.16: The noise attack analysis: (a) and (b) represent decrypted images of Peppers with salt and pepper noise level of 0.1% and 5% respectively

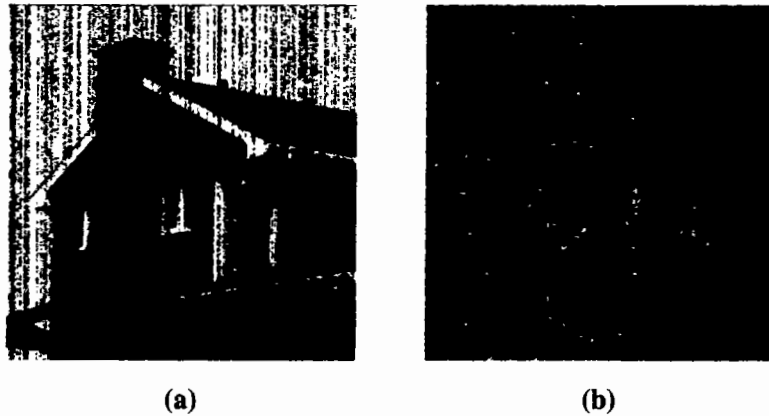


Figure 3.17: The noise attack analysis: (a) and (b) represent decrypted images of House with salt and pepper noise level of 0.1% and 5% respectively

3.7 Time Execution Analysis

The execution time of an algorithm is a key factor in evaluating the efficiency of a cryptosystem, as it directly impacts the system's overall performance and effectiveness. The experimental evaluation of the proposed algorithm was conducted on a machine equipped with an Intel(R) Core(TM) i3-5010U processor running at 2.10GHz, 8.00 GB RAM, and operating on Windows 10 Enterprise. The encryption process was simulated using Python version 3.9.12, with the RGB Test image taking approximately 11.6160 seconds to encrypt.

Chapter 4

Conclusion and Future Directions

This chapter provides a concise summary of the complete work presented in the thesis. Additionally, it outlines important future directions and guidelines for further experimentation and development.

4.1 Conclusions

The dissertation introduces an innovative RGB encryption scheme that utilises a non-associative algebraic structure and a four-dimensional memristive system. By utilising this unique combination, the aim is to establish a robust and efficient method for achieving confidentiality in image transmission.

Chapter 1 provides a comprehensive review of the foundational concepts and background knowledge required to grasp the subsequent chapters and the research conducted in this thesis. It covers a range of important topics including background, definitions and terminologies of cryptography, chaos theory and its role in cryptography, digital images, image encryption and a literature survey of existing encryption schemes. An overview of LA-group, non-associative and non-commutative algebraic structure is also addressed. Furthermore the contributions and the layout of the thesis are also outlined.

In chapter 2, first an algorithm is designed to generate algebraic-chaotic sequences over the amalgamation of non-associative LA-group with the memristive chaotic system. Further, a colored image encryption scheme is presented, utilizing the sequences derived from a 4D memristive system and the algebraic-chaotic sequences. The designed algorithm possess the significant properties of confusion and diffusion. Sequences from the memristive system is responsible for adding the

confusion, While pixel permutation through algebraic-chaotic sequences is used for purpose of diffusion. The involvement of memristive system with an LA-group in the scheme, not only developed diffusion but also provided more security and robustness in the scheme.

In chapter 3, the resilience and robustness of the cryptosystem is judged by conducting the simulation experiments which validated the encryption technique. The performance of the proposed RGB image encryption method is found to be comparable to that of the standard prime level, indicating its high level of effectiveness and security.

4.2 Future work

Some proposed directions for future research are listed as follows:

- Design more encryption schemes combining non associative structure of LA-group and memristive system.
- Construction of image encryption schemes based on different non-associative algebraic structures like LA-rings and LA-fields.
- Utilising the hyper-chaotic memristive systems to increase the robustness of encryption scheme.
- Exploration of different non-commutative and non-associative algebraic structures to obtain their application in cryptography.
- Modifying the proposed technique to make it suitable for other image formats.

Bibliography

- [1] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC press, 2018.
- [2] M. E. Whitman and H. J. Mattord, *Principles of Information Security*. Cengage learning, 2021.
- [3] D. E. R. Denning, *Cryptography and Data Security*, vol. 112. Addison-Wesley Reading, 1982.
- [4] R. L. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.
- [5] R. Davis, “The Data Encryption Standard in Perspective,” *IEEE Communications Society Magazine*, vol. 16, no. 6, pp. 5–9, 1978.
- [6] D. Coppersmith, “The Data Encryption Standard (DES) and Its Strength Against Attacks,” *IBM journal of research and development*, vol. 38, no. 3, pp. 243–250, 1994.
- [7] F. P. Miller, A. F. Vandome, and J. McBrewster, *Advanced Encryption Standard*. Alpha Press, 2009.
- [8] A. Mousa and A. Hamad, “Evaluation of the RC4 Algorithm for Data Encryption,” *Int. J. Comput. Sci. Appl.*, vol. 3, no. 2, pp. 44–56, 2006.
- [9] S. R. Nagpaul, *Topics in Applied Abstract Algebra*, vol. 15. American Mathematical Soc., 2005.
- [10] C. E. Shannon, “Communication Theory of Secrecy Systems,” *The Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

- [11] M. Kazim and M. Naseeruddin, "On Almost Semigroups," *Portugaliae mathematica*, vol. 36, no. 1, pp. 41–47, 1977.
- [12] P. Holgate, "Groupoids Satisfying a Simple Invertive Law," *Math. Stud.*, vol. 61, no. 1–4, pp. 101–106, 1992.
- [13] J. Cho, J. J. Pusan, and T. Kepka, "Praha, Paramedial Groupoids," *Czechoslovak Mathematical Journal*, vol. 49, p. 124, 1996.
- [14] P. Protic and M. Bozinovic, "AG-test and Some Genaral Properties of Abel-Grassmann's Discrete Mathematics," *Nis*, vol. 3, pp. 879–886, 1995.
- [15] I. Younas, *On Structure, Symmetry and Graphs of Inverse LA-semigroups*. PhD thesis, PhD Thesis, 2019.
- [16] Q. Mushtaq and M. Kamran, "On Left Almost Groups," *Proceedings-Pakistan Academy of Sciences*, vol. 33, pp. 53–56, 1996.
- [17] P. Protic, "Some Remarks on Abel-Grassmann's Groups," *Quasigroups and Related Systems*, vol. 20, no. 2, pp. 267–274, 2012.
- [18] M. Shah and A. Ali, "Some Structural Properties of AG-Groups," in *Int. Math. Forum*, vol. 6, pp. 1661–1667, 2011.
- [19] X. Zhang and X. Wu, "Involution Abel–Grassmann's Groups and Filter Theory of Abel–Grassmann's Groups," *Symmetry*, vol. 11, no. 4, p. 553, 2019.
- [20] G. Alvarez and S. Li, "Some Basic Cryptographic Requirements for Chaos-based Cryptosystems," *International journal of bifurcation and chaos*, vol. 16, no. 08, pp. 2129–2151, 2006.
- [21] J. Pietraszek, M. Kołomycki, A. Szczotok, and R. Dwornicka, "The Fuzzy Approach to Assessment of ANOVA Results," in *Computational Collective Intelligence: 8th International Conference, ICCCI 2016, Halkidiki, Greece, September 28–30, 2016. Proceedings, Part I* 8, pp. 260–268, Springer, 2016.
- [22] X. Zeng, R. A. Pielke, and R. Eykholt, "Chaos Theory and Its Applications to the Atmosphere," *Bulletin of the American Meteorological Society*, vol. 74, no. 4, pp. 631–644, 1993.

- [23] E. N. Lorenz, "Deterministic Nonperiodic Flow," *Journal of atmospheric sciences*, vol. 20, no. 2, pp. 130–141, 1963.
- [24] R. Matthews, "On the Derivation of a "Chaotic" Encryption Algorithm," *Cryptologia*, vol. 8, no. 1, pp. 29–41, 1984.
- [25] J. Fridrich, "Symmetric Ciphers Based on Two-Dimensional Chaotic Maps," *International Journal of Bifurcation and chaos*, vol. 8, no. 06, pp. 1259–1284, 1998.
- [26] L. Chen, J. Chen, G. Zhao, and S. Wang, "Cryptanalysis and Improvement of a Chaos-Based Watermarking Scheme," *IEEE Access*, vol. 7, pp. 97549–97565, 2019.
- [27] R. Gnanajeyaraman, K. Prasad, *et al.*, "Audio Encryption Using Higher Dimensional Chaotic Map," *International Journal of Recent Trends in Engineering*, vol. 1, no. 2, p. 103, 2009.
- [28] R. I. Abdelfatah, "Audio Encryption Scheme Using Self-Adaptive Bit Scrambling and Two Multi Chaotic-Based Dynamic DNA Computations," *IEEE Access*, vol. 8, pp. 69894–69907, 2020.
- [29] Z. Su, S. Lian, G. Zhang, and J. Jiang, "Chaos-Based Video Encryption Algorithms," *Chaos-Based Cryptography: Theory, Algorithms and Applications*, pp. 205–226, 2011.
- [30] R. Stoop and P. Meier, "Evaluation of Lyapunov Exponents and Scaling Functions from Time Series," *JOSA B*, vol. 5, no. 5, pp. 1037–1045, 1988.
- [31] X. Chai, Y. Chen, and L. Broyde, "A Novel Chaos-Based Image Encryption Algorithm Using DNA Sequence Operations," *Optics and Lasers in engineering*, vol. 88, pp. 197–213, 2017.
- [32] X. Wang and S. Gao, "Application of Matrix Semi-Tensor Product in Chaotic Image Encryption," *Journal of the Franklin Institute*, vol. 356, no. 18, pp. 11638–11667, 2019.
- [33] C. Chen, K. Sun, and S. He, "An Improved Image Encryption Algorithm with Finite Computing Precision," *Signal Processing*, vol. 168, p. 107340, 2020.

- [34] S. Wang, Q. Peng, and B. Du, "Chaotic Color Image Encryption Based on 4D Chaotic Maps and DNA Sequence," *Optics & Laser Technology*, vol. 148, p. 107753, 2022.
- [35] C. Li, D. Lin, and J. Lü, "Cryptanalyzing an Image-Scrambling Encryption Algorithm of Pixel Bits," *IEEE MultiMedia*, vol. 24, no. 3, pp. 64–71, 2017.
- [36] N. Sanam, A. Ali, T. Shah, and G. Farooq, "Non-Associative Algebra Redesigning Block Cipher with Color Image Encryption," *Comput. Mater. Continua*, vol. 67, no. 1, pp. 1–21, 2021.
- [37] Y. Naseer, T. Shah, S. Hussain, and A. Ali, "Steps Towards Redesigning Cryptosystems by a Non-associative Algebra of IP-Loops," *Wireless Personal Communications*, vol. 108, pp. 1379–1392, 2019.
- [38] I. Younas and M. Khan, "A New Efficient Digital Image Encryption Based on Inverse Left Almost Semi Group and Lorenz Chaotic System," *Entropy*, vol. 20, no. 12, p. 913, 2018.
- [39] A. Anees and A. M. Siddiqui, "A Technique for Digital Watermarking in Combined Spatial and Transform Domains Using Chaotic Maps," in *2013 2nd national conference on information assurance (NCIA)*, pp. 119–124, IEEE, 2013.
- [40] F. Cairone, P. Anandan, and M. Bucolo, "Nonlinear Systems Synchronization for Modeling Two-Phase Microfluidics Flows," *Nonlinear Dynamics*, vol. 92, pp. 75–84, 2018.
- [41] S. Wang, C. Wang, and C. Xu, "An Image Encryption Algorithm Based on a Hidden Attractor Chaos System and the Knuth–Durstensfeld Algorithm," *Optics and Lasers in Engineering*, vol. 128, p. 105995, 2020.
- [42] X.-Y. Wang and Z.-M. Li, "A Color Image Encryption Algorithm Based on Hopfield Chaotic Neural Network," *Optics and Lasers in Engineering*, vol. 115, pp. 107–118, 2019.
- [43] L. Liu and S. Miao, "A New Simple One-Dimensional Chaotic Map and Its Application for Image Encryption," *Multimedia Tools and Applications*, vol. 77, pp. 21445–21462, 2018.

- [44] A. Kanso and M. Ghebleh, "A Novel Image Encryption Algorithm based on a 3D Chaotic Map," *Communications in Nonlinear Science and Numerical Simulation*, vol. 17, no. 7, pp. 2943–2959, 2012.
- [45] F. Belkhouche and U. Qidwai, "Binary Image Encoding Using 1D Chaotic Maps," in *Annual Technical Conference IEEE Region 5, 2003*, pp. 39–43, IEEE, 2003.
- [46] J. mei Liu, S. Qiu, F. Xiang, and H. Xiao, "A Cryptosystem Based on Multiple Chaotic Maps," *2008 International Symposiums on Information Processing*, pp. 740–743, 2008.
- [47] T. Gao and Z. Chen, "A New Image Encryption Algorithm Based on Hyper-Chaos," *Physics letters A*, vol. 372, no. 4, pp. 394–400, 2008.
- [48] C. Zhu, "A Novel Image Encryption Scheme Based on Improved Hyperchaotic Sequences," *Optics communications*, vol. 285, no. 1, pp. 29–37, 2012.
- [49] 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.
- [50] T. ul Haq and T. Shah, "4D Mixed Chaotic system and Its Application to RGB Image Encryption Using Substitution-Diffusion," *Journal of Information Security and Applications*, vol. 61, p. 102931, 2021.
- [51] S. Kannan, N. Karimi, O. Sinanoglu, and R. Karri, "Security Vulnerabilities of Emerging Nonvolatile Main Memories and Countermeasures," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 34, no. 1, pp. 2–15, 2014.
- [52] M. Lv, C. Wang, G. Ren, J. Ma, and X. Song, "Model of Electrical Activity in a Neuron Under Magnetic Flow Effect," *Nonlinear Dynamics*, vol. 85, pp. 1479–1490, 2016.
- [53] H. Bao, J. H. Park, and J. Cao, "Adaptive Synchronization of Fractional-Order Memristor-Based Neural Networks with Time Delay," *Nonlinear Dynamics*, vol. 82, pp. 1343–1354, 2015.

- [54] M. Itoh and L. O. Chua, "Memristor Oscillators," *International journal of bifurcation and chaos*, vol. 18, no. 11, pp. 3183–3206, 2008.
- [55] M.-H. Qin and Q. Lai, "Extreme Multistability and Amplitude Modulation in Memristive Chaotic System and Application to Image Encryption," *Optik*, vol. 272, p. 170407, 2023.
- [56] X. Ye, X. Wang, S. Gao, J. Mou, Z. Wang, and F. Yang, "A New Chaotic Circuit with Multiple Memristors and Its Application in Image Encryption," *Nonlinear Dynamics*, vol. 99, pp. 1489–1506, 2020.
- [57] J. Sun, C. Li, T. Lu, A. Akgul, and F. Min, "A Memristive Chaotic System With Hypermultistability and Its Application in Image Encryption," *IEEE Access*, vol. 8, pp. 139289–139298, 2020.
- [58] L. Xiong, F. Yang, J. Mou, X. An, and X. Zhang, "A Memristive System and Its Applications in Red–Blue 3D Glasses and Image Encryption Algorithm with DNA Variation," *Nonlinear Dynamics*, vol. 107, no. 3, pp. 2911–2933, 2022.
- [59] Z. Wang, F. Min, and E. Wang, "A New Hyperchaotic Circuit with Two Memristors and Its Application in Image Encryption," *Aip Advances*, vol. 6, no. 9, p. 095316, 2016.
- [60] G. Peng and F. Min, "Multistability Analysis, Circuit Implementations and Application in Image Encryption of a Novel Memristive Chaotic Circuit," *Nonlinear Dynamics*, vol. 90, no. 3, pp. 1607–1625, 2017.
- [61] L. Chua, "Memristor-The Missing Circuit Element," *IEEE Transactions on circuit theory*, vol. 18, no. 5, pp. 507–519, 1971.
- [62] D. B. Strukov, G. S. Snider, D. R. Stewart, and R. S. Williams, "The Missing Memristor Found," *nature*, vol. 453, no. 7191, pp. 80–83, 2008.
- [63] A. Buscarino, L. Fortuna, M. Frasca, and L. V. Gambuzza, "A Gallery of Chaotic Oscillators Based on HP Memristor," *International Journal of Bifurcation and Chaos*, vol. 23, no. 05, p. 1330015, 2013.

- [64] B. Muthuswamy, "Implementing Memristor Based Chaotic Circuits," *International Journal of Bifurcation and Chaos*, vol. 20, no. 05, pp. 1335–1350, 2010.
- [65] F. Corinto, A. Ascoli, and M. Gilli, "Nonlinear Dynamics of Memristor Oscillators," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 58, no. 6, pp. 1323–1336, 2011.
- [66] S. P. Adhikari, C. Yang, H. Kim, and L. O. Chua, "Memristor Bridge Synapse-Based Neural Network and Its Learning," *IEEE Transactions on neural networks and learning systems*, vol. 23, no. 9, pp. 1426–1435, 2012.
- [67] A. Mazady, M. T. Rahman, D. Forte, and M. Anwar, "Memristor PUF—A Security Primitive: Theory and Experiment," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 5, no. 2, pp. 222–229, 2015.
- [68] W. McCune, "Prover9 and Mace4, software available online at <http://www.cs.unm.edu/~mccune>," 2005.
- [69] Y. Wu, J. P. Noonan, S. Agaian, *et al.*, "NPCR and UACI Randomness Tests for Image Encryption," *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)*, vol. 1, no. 2, pp. 31–38, 2011.
- [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] R. Enayatifar, F. G. Guimarães, and P. Siarry, "Index-Based Permutation-Diffusion in Multiple-Image Encryption Using DNA sequence," *Optics and Lasers in Engineering*, vol. 115, pp. 131–140, 2019.
- [72] Y. Naseer, D. Shah, and T. Shah, "A Novel Approach to Improve Multimedia Security Utilizing 3D Mixed Chaotic Map," *Microprocessors and Microsystems*, vol. 65, pp. 1–6, 2019.
- [73] P. Li, J. Xu, J. Mou, and F. Yang, "Fractional-Order 4D Hyperchaotic Memristive System and Application in Color Image Encryption," *EURASIP Journal on Image and Video Processing*, vol. 2019, no. 1, pp. 1–11, 2019.

- [74] R. M. Haralick, K. Shanmugam, and I. H. Dinstein, "Textural Features for Image Classification," *IEEE Transactions on systems, man, and cybernetics*, no. 6, pp. 610–621, 1973.
- [75] 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.
- [76] X. Liu, D. Xiao, and C. Liu, "Quantum Image Encryption Algorithm Based on Bit-Plane Permutation and Sine Logistic Map," *Quantum Information Processing*, vol. 19, pp. 1–23, 2020.
- [77] H. Liu, A. Kadir, X. Sun, and Y. Li, "Chaos Based Adaptive Double-Image Encryption Scheme Using Hash Function and S-Boxes," *Multimedia Tools and Applications*, vol. 77, pp. 1391–1407, 2018.
- [78] A. M. Eskicioglu and P. S. Fisher, "Image Quality Measures and their Performance," *IEEE Transactions on communications*, vol. 43, no. 12, pp. 2959–2965, 1995.
- [79] Q. Huynh-Thu and M. Ghanbari, "Scope of Validity of PSNR in Image/Video Quality Assessment," *Electronics letters*, vol. 44, no. 13, pp. 800–801, 2008.
- [80] Z. Wang and A. C. Bovik, "A Universal Image Quality Index," *IEEE signal processing letters*, vol. 9, no. 3, pp. 81–84, 2002.
- [81] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image Quality Assessment: From Error Measurement to Structural Similarity," *IEEE transactions on image processing*, vol. 13, no. 1, 2004.