CAPITAL UNIVERSITY OF SCIENCE AND TECHNOLOGY, ISLAMABAD

A Modified Image Encryption Scheme Based on Henon Chaotic Map and Brownian Motion

by

Asad Ur Rehman

A thesis submitted in partial fulfillment for the degree of Master of Philosophy

in the

Faculty of Computing
Department of Mathematics

2022

My Parents

without their effort and prayers, I would never have reached so far

CERTIFICATE OF APPROVAL

A Modified Image Encryption Scheme Based on Henon Chaotic Map and Brownian Motion

by

Asad Ur Rehman

(MMT 193013)

THESIS EXAMINING COMMITTEE

S.No.	Examiner	Name	Organization
(a)	External Examiner	Dr. Waqas Mehmood	QAU, Islamabad
(b)	Internal Examiner	Dr. Muhammad Afzal	CUST, Islamabad
(c)	Supervisor	Dr. Rashid Ali	CUST, Islamabad

Dr. Rashid Ali
Thesis Supervisor
December, 2022

Dr. Muhammad Sagheer
Head
Dept.of Mathematics
December, 2022

Dr. Muhammad Abdul Qadir
Dean
Faculty of Computing
December, 2022

Author's Declaration

I **Asad Ur Rehman** hereby state that my MPhil thesis titled "**A Modified Image Encryption Scheme Based on Henon Chaotic Map and Brownian Motion**" is my own work and has not been submitted previously by me for taking any degree from Capital University of Science and Technology, Islamabad or anywhere else in the country/abroad.

At any time if my statement is found to be incorrect even after my graduation, the University has the right to withdraw my MPhil Degree.

(Asad Ur Rehman)
Registration No: MMT193013

Plagiarism Undertaking

I solemnly declare that research work presented in this thesis titled "**A Modified Image Encryption Scheme Based on Henon Chaotic Map and Brownian Motion**" is solely my research work with no significant contribution from any other person.Small contribution/help wherever taken has been duly acknowledged and that complete thesis has been written by me.

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

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even after award of MS Degree, the University reserves the right to withdraw/revoke my MPhil degree and that HEC and the University have the right to publish my name on the HEC/University website on which names of students are placed who submitted plagiarized work.

Asad Ur Rehman
Registration No: MMT193013

Acknowledgement

First and foremost I would like to thank Almighty **Allah** the most merciful for all his blessings throughout my life, and for always being my strength and peace. I could not have achieved this much without the grace of Almighty Allah.

I am profoundly grateful to my generous supervisor **Dr. Rashid Ali** for his encouragement. He was always there whenever I found any problem. I really appreciate his efforts and guidance throughout my thesis and proud to be a student of such kind supervisor.

I am especially indebted to **Dr. Muhammad Sagheer**, Head of the Department of Mathematics, who have been supportive of my career goals and detailed feedback have been very important to me.

I am thankful to all of my **family members** for becoming a bulwark of patience and support during my research work. However, my deepest gratitude is reserved for my Parents for their earnest prayers, unconditional love and unflinching support in completing my degree program. They supported and encouraged me throughout.

I am grateful for my uncle MR. Muhammad Naseer whose constant love and support keep me motivated and confident. Deepest thanks to my siblings, who keep me grounded, remind me of what is important in life, and are always supportive of my adventures. Finally, I owe my deepest gratitude to my wife. I am forever thankful for the unconditional and support .

I would like to thank all of my friends for motivating me during my degree program. Mostly, I would like to thank **Tahir Ali Sajad**, **Iqrar Raza**, **Muhammad Awais** and **Hassan Raza** also helped me a lot and guided me whenever I needed it.

(Asad Ur Rehman)

Abstract

A detailed review of the work of M. Xu "A new chaos based image encryption algorithm" is presented in this thesis. The work focuses on an image encryption scheme based on Chen chaotic system and Chebyshev map. In this work the encryption of a grey scale image is performed. This encryption uses three steps. In the first step permutation of rows is carried out by using circular shift operation, then in second step XOR operation is used for diffusion purpose finally columns are scrambled by using circular shift utilizing Chebyshev chaotic map. The scheme is implemented by developing a code for the encryption and decryption of algorithm. The implementation is then used to create various cipher images. The review work is further extended by introducing a new scheme which is based on Henon Chaotic map and Brownian motion. The initial keys used in the permutation and diffusion stages interact with each other. The extended scheme is also implemented on MATLAB and the security anaylsis is performed on various cipherimages obtained by the implementation of modified scheme. Security anaylsis results depict that newly developed scheme is not much different from scheme of Ming. However the running time of the new scheme is less than the original one. The improvement solution is novel and transplantable, it can also be used to enhance the ability of resisting differential attack on image encryption algorithms.

Contents

List of Figures

List of Tables

Abbreviations

AES	Advanced Encryption Standard
BM	Brownian Motion
DES	Data Encryption Standard
IDEA	International data encryption algorithm
JPEG	Joint Photographic Experts Group
NPCR	Number of Pixel Changing Rate
PCC	Pearson Correlation Coefficient
PNG	Portable Network Graphic
RSA	Rivest - Shamir - Adleman
TIFF	Tagged Image File Format
UACI	Unified Averaged Changed Intensity

Symbols

C	Ciphertext
C	Cipherimage
D	Decryption algorithm
E	Encryption algorithm
t, u	Control parameter of Henon chaotic map
a_1, b_1, c_1	Control parameter of Chen chaotic system
A	Number of rowns
B	Number of column
v	Key
P	Plaintext
t	Step length
Greek letters	
λ	Lyapunove exponent
δ_{st}	Pearson correlation coefficient
y	Control parameter of Brownian motion
z	Control parameter of Brownian motion

Chapter 1

Introduction

Cryptography is the study of ciphers and codes, which is important in safeguarding and protecting data. Its traces can also be seen in the ancient Egyptian civilization. It is not an exaggeration to say that the present encryption method is the outcome of a lengthy and unparalleled history of evolution [1]. Cryptography has a long history that dates back thousands of years.

The first known evidence of the use of cryptography, as stated in [2] was discovered in an inscription carved around the central chamber of the tomb of the nobleman Khnumhotep 2 in Egypt . To a large degree, the organizer relied on a few unusual pictogram images rather than more typical ones. The objective was not to cover the message, but rather to alter its structure in such a way that it appeared ethical.

Julius Caesar was reported to use a sort of crypto to convey secret communications to his military men stationed on the battlefield circa 100 BC [3]. The substitition cipher, the Caesar cipher, are the most cited notable codes in literature. In a substitution cipher, each plaintext character is substituted by another character to form the ciphertext.

At the beginning of the 19th century when everything got to be electric, Hebern planned an electro-mechanical contraption which was called the Hebron rotor machine, detailed is given in [4]. It employments a single rotor, in which the secret key is inserted in a pivoting circle. The key encoded a substitution table and each

keypress from the console comes about within the yield of cipher content. This was once broken by utilizing letter frequencies.

Up to the World War II, most of the work on cryptography was for military purposes, as a rule, utilized to cover up important military data. In any case, cryptography pulled in commercial consideration post-war, with businesses attempting to secure their information from competitors. In the early 1970s, IBM realized that their clients were requesting a few shapes of encryption, so they shaped "crypto bunch" headed by Horst-Feistel. They outlined a cipher called Lucifer [5].

In 1973, the Country Bureau of Standards (now called NIST) within the US put out and ask for recommendations for a square cipher that would end up a national standard. They had realized that they were buying a part of commercial items without any great crypto back. Lucifer was inevitably acknowledged and was called DES or the data encryption Standard. In 1997, DES was broken by a cryptanalyst . The most issue with DES was the shorter of the encryption key.

1.1 Image Encryption

The internet and digital technology are expanding at a rapid pace. As a result, individuals are increasingly relying on digital media for communication. For example, image, audio, and video. Images provide a sizable portion of multimedia. Images are used extensively in Military, National-Security, and Diplomatic communications. Because these photographs may contain very personal information. They require considerable caution when users accumulate them anywhere on an untrustworthy site. Furthermore, when users want to share photographs via a secure network, is critical to guarantee complete security. In summary, a image must be protected against numerous security threats [6]. To accomplish this goal, encryption is one of the most effective means of information concealment. Many image encryption techniques have been developed by researchers over the past decade. To boost security, they employ several image encryption methods. These methods [7] are classified according to several principles such as Chaotic Maps , DNA, Compressive Sensing, and Optical-Image Encryption.

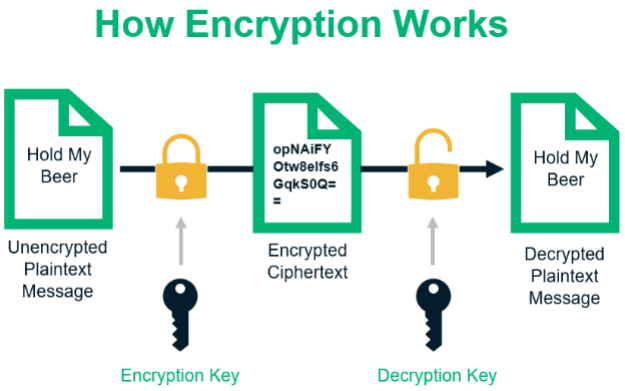


FIGURE 1.1: Image encryption

Image encryption is a process that uses a secret key to turn a plain image into an encrypted image [7]. Using the secret key, the decryption procedure converts the cypher image into the original image [8, 9]. Decryption is similar to encryption, however, it is performed in opposite order. Encryption relies heavily on secret keys. Because the encryption approach's security is primarily based on it. There are two sorts of keys are used, private keys and public keys [10, 11].

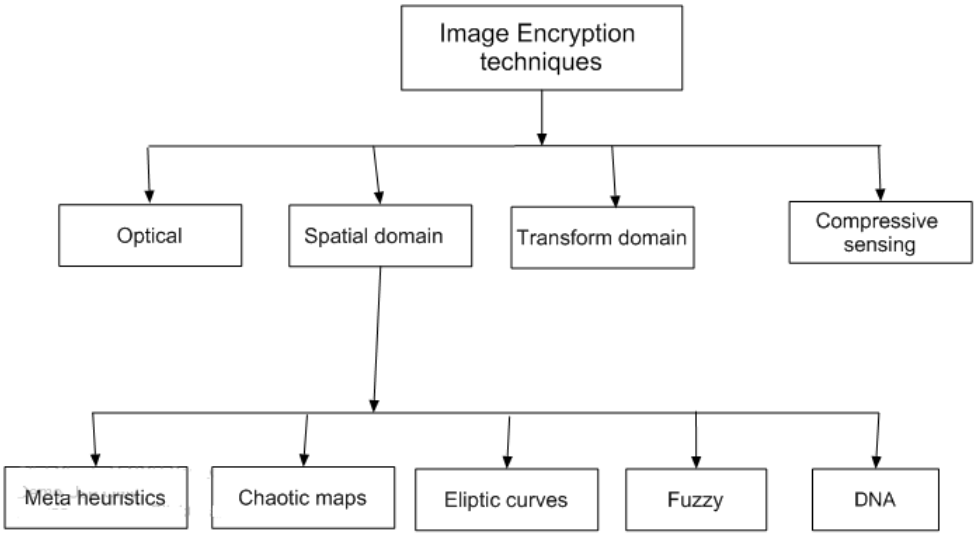


FIGURE 1.2: Flow chart of image encryption techniques

1.1.1 Encryption of Images in the Spatial Domain

Spatial domain techniques are those that involve directly changing the pixels of a image [7]. There are several space domain-based image encryption methods

described in the literature [7], such as chaotic elliptic curve, fuzzy, DNA, and metaheuristics-based approaches. However, in this research, the use of chaotic mapping in the image encryption scheme is investigated.

1.2 Literature Survey

With the rapid development of the internet, digital information exchange has grown more frequent in recent decades. Most of the industries (for example, military image databases, video conferencing, medical imaging systems, web based photos and album) now demand a secure, quick, and reliable system to store and communicate digital images. The necessity to meet the security demands of digital pictures has resulted in the development of excellent encryption algorithms to manage digital image security [12]. A plethora of encryption algorithms based on various ideas have recently been presented by number of researchers. For example, chaos-based encryption algorithms that are viable for application (e.g., video streams). Furthermore, these algorithms offer an excellent balance of speed, high security, complexity, appropriate computational overheads, and computing power [12–14] . In general, digital pictures contain properties such as redundant data, significant correlation among neighbouring pixels, being less sensitive than text data, i.e., a slight change in the characteristic of any pixel of the image does not dramatically damage the image's quality, and bulk capacity of data. As a result, standard ciphers such as IDEA (International Data Encryption Algorithm), AES (Advanced Encryption Standard), DES (Data Encryption Standard), and RSA (Rivest, Shamir-Adleman) are unsuitable for real-time image encryption since they need a long calculation time and a lot of computer resources [13]. Only those ciphers are suitable for real-time image encryption since they need less time while maintaining security. Any encryption technique that operates very slowly, on the other hand, may offer a higher level of security. As a result, this type of method would have limited practical application in real-time procedures [14].

However, in open networks, it is critical to protect confidential material including military and medical images from unauthorized access [15]. By maintaining the

security of sensitive information only beneficary may access , particularly multimedia data, has been the principal impediment to the wider adoption of digital image services.

In order to create safe cryptosystems, Claude Shannon invented a technique of confusion and dispersion in 1949, the scheme is given in [16]. It is known as the substitution-permutation network in current information security systems (SP-network) [17]. Traditional symmetric ciphers, such as advanced encryption standard (AES) [18], and data encryption standard (DES) [19], as well as all versions of these cryptosystems, are designed to have low confusion and diffusion. Several encryption techniques have been developed to ensure the privacy of digital data. Many parts of current cypher systems are based on SP-network to increase confusion and dispersal.

Chaos is a strangely nonlinear physical phenomena that appears in the ordinary world. Li and York [20] presented the first mathematical definition of chaos which is widely used for one-dimensional iterative maps. Following that, a few alternative chaotic definitions were given for various types of frameworks.

The most commonly used definitions are Devaney's chaos [21], Wiggins' chaos [22], and Smale's chaos [23]. All of these definitions focus on the many performances of chaos for example, Li-chaos York's is concerned with the dissemination of chaotic directions, whereas Devaney's chaos is concerned with topological features. There is currently no accurate numerical description that can encompass all manifestations of chaos. Regardless, the lack of a single definition does not exclude the use of chaos. On the contrary, chaos has been widely used in practically all sectors of science, architecture, and even the humanities.

The chaos hypothesis is inextricably linked with cryptography. Chaotic systems have qualities with encryption, such as high entropy, sensitive to chaotic parameters, beginning circumstances, its undeterministic character, pseudo-randomness and ergodicity, and so on. All of which are essential considerations for constructing any modern cryptosystem [24].

The link between chaotic and encryption provided a new concept. In digital information systems, a new system has emerged. As a result, after the 1990s, chaos

theory was widely used to construct resilient cryptosystems.

In recent years, research on bifurcation and chaotic behaviour in nonlinear dynamical frameworks has become extremely important. Bifurcation and chaos have been seen in a large number of experiments, and some writers have advanced the idea that computer simulations play an important role in the search for current chaotic attractors [6, 25]. Chaos is often defined by a sensitive dependency on the initial circumstances of the constituents.

There are various families of maps in mathematics, and they commonly occur in pairs. Fibonacci maps, Lucas maps, logistic maps, cat maps, tent maps, Henon maps [26] etc. They are generated via the same repeat connection but with different initial values, and multiple families connect the two families [25].

Pixels are the essential components of an image. To protect an image, we must secure the material hidden in each pixel. The location values of pixels can also be utilized for encryption [15].

The image encryption technique ought to be sufficiently powerful. It is necessary to ensure that the encrypted image is suitable for testing and data file retrieval. Transformation is the act of converting data to another form by removing any redundancy. Using this type of encoding would render the data illegible.

Chaos-based image encryption [27] systems offer various benefits over standard encryption techniques due to the chaotic underlying maps and the associated initial key sensitivity.

Edward Lorenz a mathematician and meteorologist, discovered chaos theory during a weather prediction experiment in the early 1960s, the detailed of this theory is given in [15]. The above theory is concerned with uncovering hidden patterns in seemingly random data. It offers a handy method for solving non-linear issues in both natural and artificial systems with unexpected behaviors.

Traffic, financial markets, earthquakes, healthy heart rhythms, DNA coding sequences, weather and climatic conditions are such kind of behaviors included [15].

1.3 Thesis Contribution

A detailed review of the work of M. Xu [28] "A New Chaos- Based Image Encryption Algorithm" is presented in this thesis. The work focuses on an image encryption scheme based on Chen chaotic system and Chebyshev map. The scheme is implemented by developing a MATLAB code for the encryption and decryption of algorithm. The implementation is then used to create various cipher images. Following the smooth execution of the previously discussed technique for the grayscale image on MATLAB, some security analysis, such as key sensitivity and statistical analysis, are also evaluated. In this scheme the algorithm is slightly changed which proved beneficial for good cryptosystem.
In the last part of thesis a new scheme is introduced. Because the initial procedure of the previous scheme requires more time to run. We have used Brownian Motion to enhance the randomness in our new scheme as well. Henon chaotic map has been used instead of Chen chaotic map. Most of the properties of cryptographic are found in this map. However, there is no change in algorithm for some reasons. The encryption and decryption algorithm are again implemented using the palteform MATLAB. Our new program also execute very nicely and finally some security analysis of this game was done.

1.4 Thesis Arrangement

This thesis reviews grayscale image encryption with various techniques.

- **Chapter 2**: It is a basic introduction to cryptology, including basic ideas of cryptography and various cryptographic properties. The Chaos theory is also described in detail and then in the same chapter the Compound chaotic map based image encryption scheme is critically examined.
- **Chapter 3**: The analysis of the article "A New Chaos-Based Image Encryption Algorithm" by M. Xu is presented. Some merits and some demerits of the above scheme are dicussed. Apart from this, the security of the scheme has also been reviewed.

- **Chapter 4**: In this chapter, Henon chaotic map and Brownian motion are explained in detail. In the same chapter image encryption and decryption is done under the same scheme. There is the security review of our new scheme.

- **chapter 5**: In this chapter, the conclusion of previously discussed work is given and some future directions are suggested.

Chapter 2

Preliminaries and Basic Concepts

In this chapter the basic introduction to cryptology, including basic ideas of cryptography and various cryptographic properties are presented. The chaos theory is then described in great detail. The compound chaotic scheme is also critically examined in the same chapter. In this chapter, we discussed a recent approach for image encryption [28] in detail.

2.1 Cryptography

Cryptography is such a technique through which we can convert plaintext to ciphertext and ciphertext is converted to plaintext again. The plaintext is a normal message that anyone can read and understand. Whereas, the ciphertext is a kind of secret message that everyone can read but only few can understand. We use cryptography to achieve confidentiality.

When it comes to compassion security there is an important concept in network security, which is known as C. I. A (Confidentiality, Integrity, and Availability). For example, I have to send a message to my friend which is far away from me. I can send this message through the internet. Now someone is taking my message on the way. He/she is trying to hack my message in an unauthorized way. But it does not mean that either confidentiality is breached or confidentiality becomes zero. No, anyone can take the message because all the devices are connected in a

vulnerable manner on the internet. The word Vulnerable means that any person with some knowledge can get the message but it does not mean he/she can also can understand that message because the sended message is not in understandable form. Any unauthorized person cannot understand the message.

For securing any message we use cryptography. Before sending the plaintext, sender use the encryption method. In encryption, we use many algorithms to encrypt the plaintext. In encryption the important part is key. The sender will lock the message with a key. After applying the lock it becomes ciphertext. when the sender sends the message on the receiver side receiver receives ciphertext nor plaintext. The receiver will decrypt the message. Decryption means converting ciphertext to plaintext. It means the sender does encryption and the receiver does decryption. Now-a-days network security and cyber security are very popular. We use cryptography in two ways symmetric key and Asymmetric key. Symmetric key implies the same key utilized for encryption and the same key utilized for decryption.

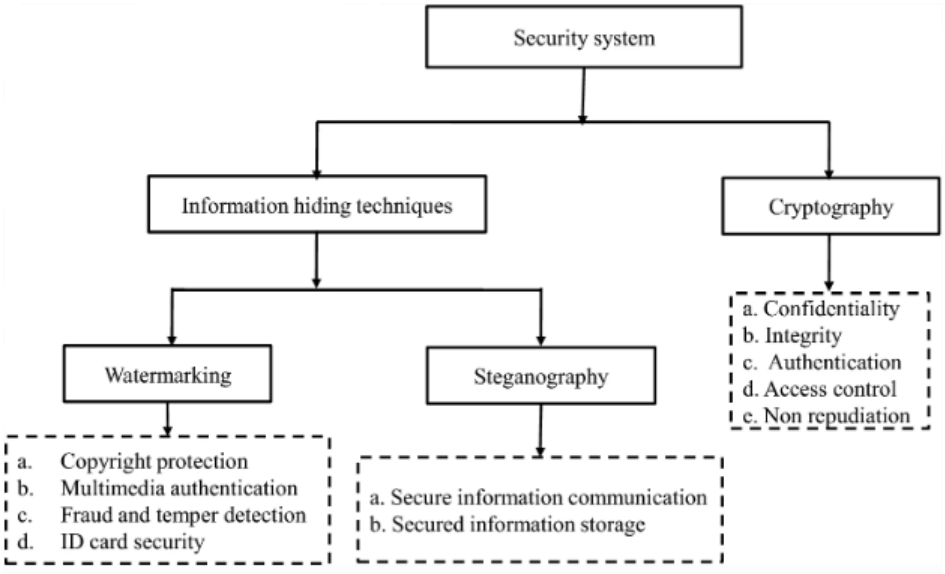


FIGURE 2.1: Flow chart of security system

Asymmetric key implies diverse keys utilized for encryption and decryption. There are many cryptographic techniques such as Ceaser cipher [29], hill cipher [5], AES [18], DES [19], RSA [30] etc.

2.2 Cryptosystem

A cryptosystem is a framework or scheme that consists of a series of algorithms that convert plaintext to ciphertext in order to securely encode or decode communications. The phrase cryptosystem is shorthand for cryptographic system and it pertains to a computer system that uses cryptography. Cryptosystem is a system through which we secure the data and conversation via the use of codes. Only those who intended to read and interpret the information may do so.
A cipher system is another name for a cryptosystem. Symmetric key encryption and asymmetric key encryption are two different types of cryptosystems.

2.2.1 Cryptosystem Components

Let's have a look at a few components of cryptosystem in more detail.

1. **Plaintext** is a term used to describe any piece of writing. It can be a message or image that everyone can understand.

2. **Ciphertext** often known as encrypted text, is a set of completely random characters and numerals that people cannot understand. The ciphertext can be a message or information that is not clear. Decryption can be used to reverse the ciphertext and recover the original plaintext.

3. **Encryption Algorithm** is a term used to describe a method of encrypting data. It could be a program for converting ordinary text to ciphertext using an encryption key. We need two types of inputs to generate the ciphertext. The first one is plain text and the second is encryption key.

4. **Decryption Algorithm** is the inverse of an encryption algorithm. Decryption is the process of transforming encoded or encrypted text or data back into its original form.

5. **Encryption Key** is such a key that sender of the message uses when converting a plaintext message into an encrypted message.

6. **Decryption Key** is such a key that recipient of the message uses when converting the encrypted message into a plaintext.

2.2.2 Types of Cryptosystems

Cryptosystems are divided into two categories.

- **Symmetric Key Encryption** (SKE)
- **Asymmetric Key Encryption** (AKE)

1. **Symmetric Key Encryption**

   SKE is a type of encryption that uses two keys to encrypt data. Both the sender and recipient use the same secret key, or encryption key, to encrypt and decrypt data. Symmetric cryptography is another name for symmetric key encryption. Many programs are SKE designed to achieve security. There are many examples such as DES (Data Encryption Standard) [19], IDEA (International Data Encryption Algorithm) [31], 3D-ES (Triple Data Encryption Standard) [32], Blowfish [32] and similar ones that use SKE techniques. It would not be wrong to say that almost all cryptosystems use this technique.

   Both the sender and receiver of the message use the same key in symmetric-key encryption. The sender of the message transmits some data to the recipient of the message through encryption, which is called plaintext. This encryption is done using a key that converts plaintext to ciphertext After receiving the data, the receiver converts this ciphertext back to plaintext. But the special thing is that the receiver uses the key that was used by the sender of the content.

   Advantages of Symmetric Key Encryption

   The main advantage of this scheme is that it has a small key and simple algorithm, due to which it does encryption and decryption very quickly.

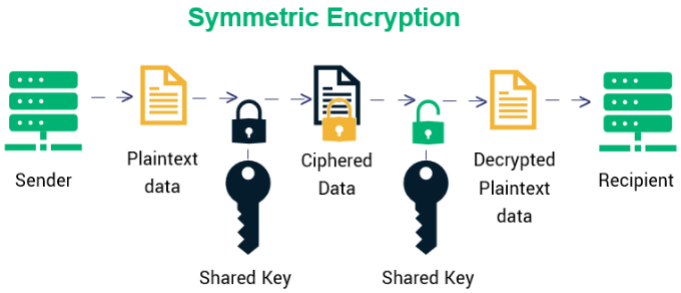


FIGURE 2.2: Symmetric key

Some important points to remember when using SKE are stated below.

- Both groups (senders and receivers) must share the key. Because both have to make plaintext and ciphertext using the same key.
- The key should be updated time to time to avoid any type of attack.
- There must be a secure channel that allows the sender and recipient to communicate a secret key.

SKE Disadvantages

- It is quite difficult for both(sender and recipient) to agree that they will use the SKE method, which necessitates the use of a key generation process.
- In SKE the sender and recipient have to share the symmetric key, therefore they must have mutual trust. For example, imagine the receiver's secret key is stolen by attackers and he fails to alert the sender.

2. **Asymmetric Key Encryption**

Two keys are employed in AKE. One is the public key and the other one is private key.

- **Public Key**: This is a key that anyone can use to encrypt any message, but the receiver decrypts the message using his own private key
- **Private Key**: This type of key is also called a secret or personal key.

In a mathematical relationship, these two keys are related to one another. Generally private keys held in a secure location, whilst public keys are kept

in a public location.

Sender encrypts the private data and sends it to the recipient using the recipient's public key. As soon as the receiver receives his message (encrypted form) he decrypts this message using his own private key.

AKE Disadvantages

- In AKE the key is very long due to which encryption and decryption procedure become very difficult. Here the key is long thats why the encryption and decryption forms in AKE have grown difficult.
- Due to the big key the speed of encryption process slows down considerably.

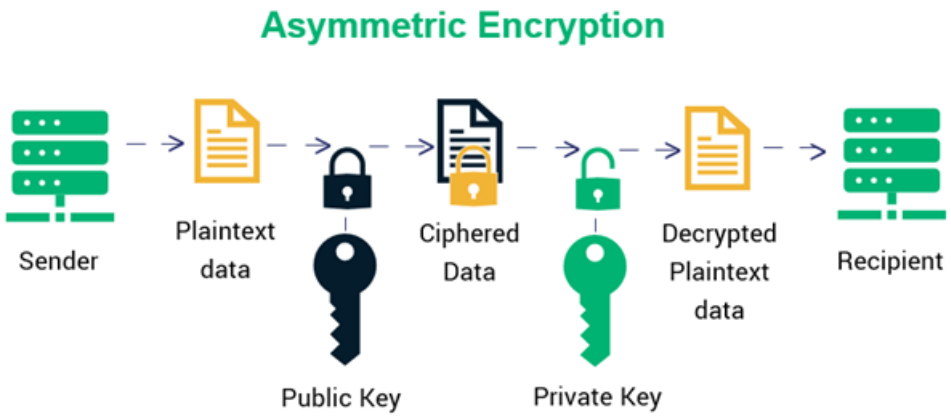


FIGURE 2.3: Asymmetric key

- The computation of the private key using the public key is not simple.
- Since public keys must be shared, they are huge in size and difficult to remember, thus they are stored on digital certificates for secure transmission and distribution. private keys, on the other hand, don't need to be shared they are held in the cloud computer programme or operating system you're using, or on equipment devices.

Advantages of Asymmetric Key Encryption

AKE has many advantages which are listed below.

- Since the private key is not shared with anyone, therefore it does not need to be updated again and again.

- There is a major problem in a cryptosystem of sharing the key in a secure way. In this technique there is no need to share the key with anyone this is why it is considered a secure method.

Hash Function

Any function that may be used to map data of self-assertive measures to fixed-size values is referred to be a hash function. Hash values, hash codes, digests, or generally hashes are the values returned by a hash operation. The values are frequently used to list a hash table, which is a fixed-size table.

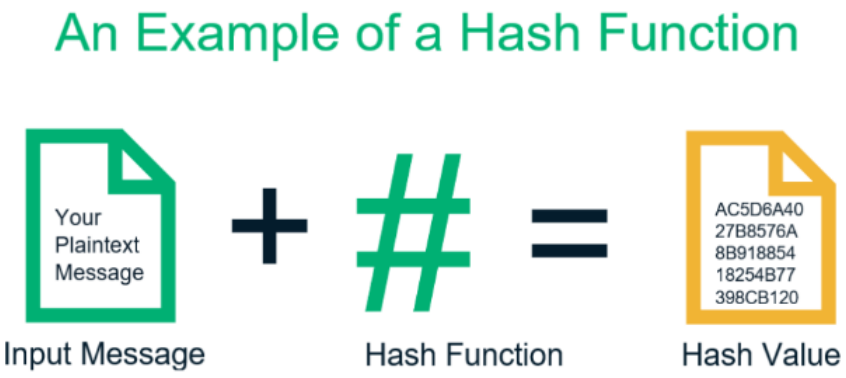


FIGURE 2.4: Hash function

It is easier to discover the shorter hash value than the larger string, for sorting and locating objects in databases. Hash functions are one-way, irreversible functions that ensure the information while preventing the recovery of the initial message. The following are some of the most well-known hashing algorithms: MD5, SHA-1, SHA-2, SHA-3, Whirlpool, Blake 2, and Blake 3 [33] are all examples of Hashing Algorithms.

2.3 Cryptanalysis

Cryptology is divided into two parts: cryptography (the creation of secret codes) and cryptanalysis (the study of cryptographic algorithms and the breaking of those secret codes). A cryptanalyst is someone who practises cryptanalysis. It assists us

in better understanding of cryptosystems and in improving the system by identifying any flaws and working to enhance the algorithm to generate a more secure secret code. A cryptanalyst tries to decipher the ciphertext by any means and he gets the plaintext or somehow he get the encryption key.

Cryptanalysis is practiced by a wide extend of organizations, counting governments pointing to decode other nations' private communications, companies creating security items that utilize cryptanalysts to test their security highlights, and programmers, saltines, autonomous researchers and academicians who rummage around for shortcomings in cryptographic conventions and algorithms.

2.3.1 Cryptanalysis Techniques and Attacks

It is important to attack the cryptographic system in order to attack th check the security of a crypto system. So that we can understand the flaws of this crypto system and then we can make our system more secure. These attacks require the cryptanalyst to have some information for example, the nature of the program should be known. The cryptanalyst should know in which language the information he wants to get, that is either in english or computer language. The attacks are based on the algorithmic nature as well as knowledge of the plaintext's general features, such as whether it is a conventional document written in english or a java code. As a result, before trying to employ the attacks, the plaintext's nature should be understood. For detailed on cryptanlysis see [34]

2.4 Chaos Theory

Henri Poincare proposed chaos theory in 1890 and he was the first person to introduce the system of determining Chaos. He believed that if the initial state of any system is changed even slightly, the final results can change completely. Accordingly, if we cannot correctly detect the initial changes of any system, we will not be able to create any good system, as discussed in [35]. Ray Bradbury a famous American science fiction novelist, wrote in one of his novels "A Sound of

Thunder" in 1952 that a huge storm can occur due to the butterfly flutter once [1]. Lorenz started the use of a computer model in 1961 to make weather forecasts. He put 0.506 as a shortcut rather than the full decimal figure of 0.506127, and he realized that all the weather had changed. Complete model of this experiment is discussed in [36].

Chaos is the science of unexpected of the nonlinear and unpredictable events. It teaches us to be prepared for the unexpected situation. However much conventional science is concerned with allegedly predictable phenomena such as gravity, electricity, or chemical reactions. On the other hand chaos theory is concerned with nonlinear and unpredictable phenomena that are virtually hard to anticipate or regulate, such as turbulence, weather, stock market, our mental states etc. Fractal mathematics, which represents nature's infinite complexity, is frequently used to describe these events. Many natural objects such as landscapes, clouds, trees, organs, rivers, etc, display fractal qualities as do many of the systems in which humans exist.

- A dynamic system is a system that evolves with time. To determine the state for all future times, it requires iterations of the relation by a number of times. If the system can be solved with a given initial point it is possible to determine all its future positions.
- The stability of the dynamical system implies that there is a class of initial conditions for which the trajectories would be equivalent.

2.5 Some Importants Chaotic Maps

Chaos is defined by the properties of deterministic, nonlinear, sensitive dependence. These are the fundamental properties of chaos. There are many other examples of a chaotic system, such as Sine map, Tent map, Arnold map, Roses system, Henon chaotic map and Chens system etc.

In this section brief discription of some well known chaotic maps and their properties are dissused.

2.5.1 Logistic Map

The two-dimensional logistic map is researched for its complicated behaviors of the evolution of basins and attractors. It has more complex chaotic behaviors than any one-dimensional Logistic map [37].

Logistic Map:

$$x_{n+1} = rx_n(1 - x_n). \tag{2.1}$$

1. **Deterministic:** Chaos is deterministic. A chaotic process can be defined by a mathematical model. A mathematical model can be expressed as a simple equation. It can be written in two ways, discrete equation and differential equation. A discrete equation is an example of a logistic map. It is also an example of a chaotic map. Secondly, the Lorenz system 2.4 can be expressed as a differential equation and is known as the chaotic system.

2. **Nonlinearity**: The next important property of chaos theory nonlinearity. Nonlinearity is a mathematical term that describes a situation in which there is no straight-line or direct relationship between variables. Nonlinear systems are those in which the change in output is not proportional to the change in input. Nonlinear dynamical systems, describing change in variables over time, may appear chaotic or unpredictable. The logistic map is an example of a nonlinear recurrence relation.

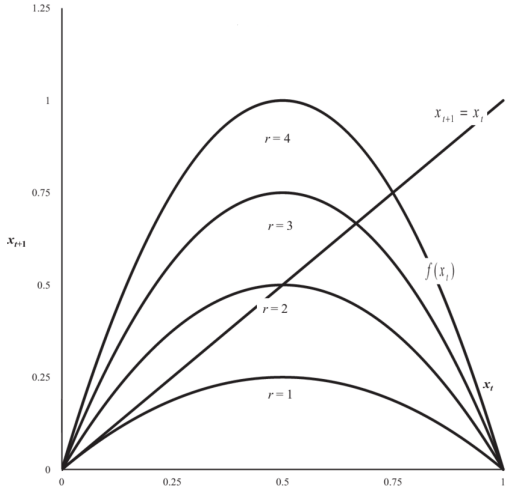


FIGURE 2.5: Logistic map

The logistic map is an example of a nonlinear recurrence relation.

3. **Bifurcation**

   One of the key concepts in understanding chaos theory is bifurcation. Mitchel. Jf [38] an American mathematical physicist, found the bifurcation process in a nonlinear dynamic system in 1975. He used a basic mathematical model to characterise the system's disorderly behaviour. In specific situations, a model's behaviour evolves from stability to periodicity, and subsequently from periodicity to randomness. Small disruption in a system's guiding rules causes it to bifurcate and change state.

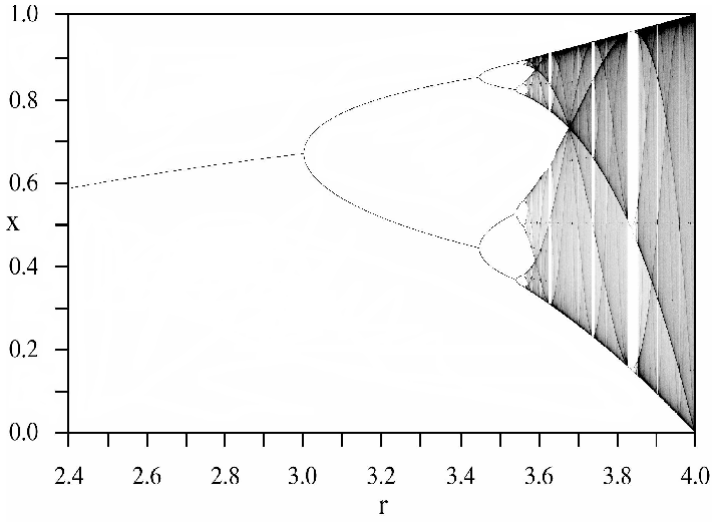


FIGURE 2.6: Bifurcation diagram of logistic map

2.5.2 Henon Chaotic Map

The Henon map is a 2-D invertible iterated map wich have chaotic solutions.The Henon map, developed by Henon in 1976, is a simplified form of the Poincare map for the Lorenz equation as discussed in [39, 40]. It is represented by state equations with a chaotic attractor. As a method for creating pseudorandom sequences, the chaotic Henon mapping has been suggested [41]. The following equation represents the 2-D Henon map [42].The Henon chaotic map lies between $[-1.5, 1.5]$ on the Y-axis and $[-0.4, 0.4]$ on the X-axis. If $u = 0.3$ is fixed and t varies in the range of $[0, 1.5]$ the henon map behave chaoticaly.

$$\begin{aligned} x_{m+1} &= 1 + y_m - t x_m^2, \\ y_{m+1} &= u x_m \end{aligned} \tag{2.2}$$

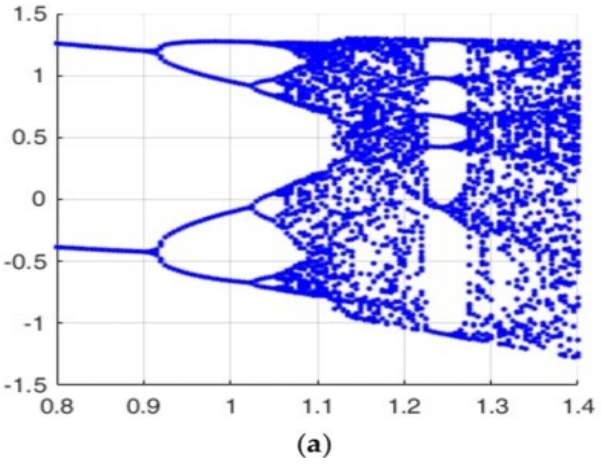


FIGURE 2.7: Bifurication diagram of Henon chaotic map

1. **Lyapunov Exponent**

   Lyapunov [43] was a Russian mathematician scientist who published his article in 1892 in which stability and non-periodic motions were well described in it. This theory of Lyapunov played a fundamental role in non-linear system. Through this we can find out

   i. How much a system is chaotic.

   ii. Measures of small dependance on initials conditions.

   iii. The rate of seperation or convergance of infinitesmely close tracjectories because it is ane exponential function.

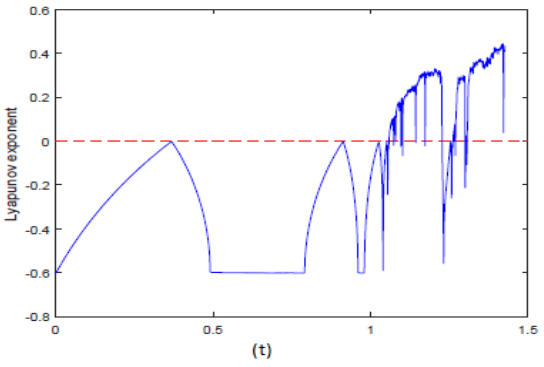


FIGURE 2.8: LE of Henon chaotic map

Lyapunove exponent can be defined as:

$$\lambda = \lim_{m\to\infty} \frac{1}{m} \sum_{t=1}^{m-1} \ln |g^{'}(x_t)| \tag{2.3}$$

Lyapunove exponent has three dynamic cases which are as follows:

- $\lambda = 0$ shows the system is neutrally stable.
- $\lambda < 0$ shows orbit is directed to a fixed or stable point.
- $\lambda > 0$ shows system is chaotic and unstable.

2.5.3 Chebyshev Maps

The same holds true for Chebyshev polynomials of the first and second kinds. There are two less well-known advanced polynomial families, the Chebyshev polynomials of the third and fourth kinds. Each of the four types is an example of an orthogonal polynomial family $P_n(x)$.

There are too many associations between these four sorts, so first we recall a description and certain features of the first and second kind univariate Chebyshev polynomials.

The Chebyshev polynomials are two polynomial sequences linked to the cosine and sine functions, denoted as $T_t(y)$ and $U_t(y)$. They can be defined in numerous methods.

The Chebyshev polynomials of the first kind T_t are given by

$T_t(\cos\theta) = \cos(t\theta)$

Similarly, define the second-order Chebyshev polynomials U_t as

$U_t(\cos\theta)\sin\theta = \sin((t+1)\theta)$.

First Kind: The first few Chebyshev polynomials of the first kind are

$T_0(y) = 1$

$T_1(y) = y$

$T_2(y) = 2y^2 - 1$

$T_3(y) = 4y^3 - 3y$

$T_4(y) = 8y^4 - 8y^2 + 1$

$T_5(y) = 16y^5 - 20y^3 + 5y$

$T_6(y) = 32y^6 - 48y^4 + 18y^2 - 1$

Second Kind: The first few Chebyshev polynomials of the second kind are

$$U_0(y) = 1$$
$$U_1(y) = y$$
$$U_2(y) = 2y^2 - 1$$
$$U_3(y) = 4y^3 - 3y$$
$$U_4(y) = 8y^4 - 8y^2 + 1$$
$$U_5(y) = 16y^5 - 20y^3 + 5y$$
$$U_6(y) = 32y^6 - 48y^4 + 18y^2 - 1$$

2.5.4 Chen Chaotic System

The equations representing the Chen Chaotic system given by

$$\begin{aligned} \frac{dx}{dt} &= a_1(y - x), \\ \frac{dy}{dt} &= (c_1 - a_1)x - xz + c_1 y, \\ \frac{dz}{dt} &= xy - b_1 z. \end{aligned} \tag{2.4}$$

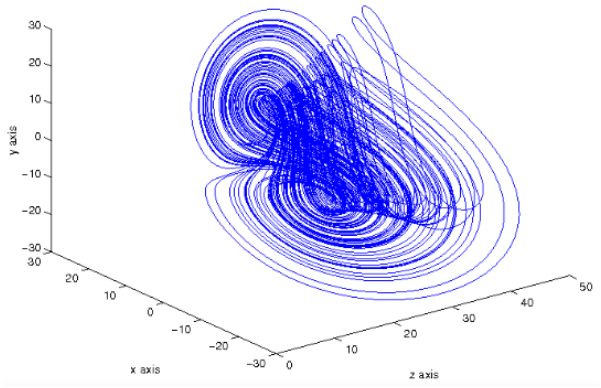


FIGURE 2.9: The Chen chaotic attractor ($a_1 = 35$, $b_1 = 3$, $c_1 = 28$).

The coupled Equations (2.4) are transformed into a one-dimensional circle by the chaotic strategy. The chaotic mixing techniques in [28] are clearly more secure

than the established blending strategies. In above equations a_1, b_1, and $c_1$are control parameters. With a few suitable settings, above system will be chaotic. figure 2.9 shows the chaotic attractor of this system when a_1= 35, b_1= 3, and c_1= 28. Chen chaotic framework has a high dynamical complexity. The Lyapunov exponent of Chen framework is around 2.168, which is larger than the most often used chaotic systems. Regardless, the complexity of each dimensional variable is or may be considerable. In this study, a chaotic technique for generating one-dimensional sequence with great complexity from the Chen system is described. Actually, chaotic number sequences are utilised to mix the three-dimensional state variables of Chen's chaotic system.

2.5.5 Unpredictability

Chaos theory tells us that the future world is always uncertain. Every future event is connected with the probability of occurrence. Rather, we cannot even say with 100% certainty that the sun will rise tomorrow. The future of any complex system is always uncertain. The way of behaving of complicated frameworks is flawlessly delicate to conditions, so that little changes towards the beginning can bring about ever bigger changes over the long run. On the other hand in words that have been ascribed to both physicist Niels Bohr and baseball supervisor Yogi Berra, "Expectation is truly challenging, particularly about what's to come".

Butterfly Effect

Edward Lorenz [44] presented a question during the $139th$ meeting of American Association for the Advancement of Science. "Can a butterfly flapping its wings in Brazil cause a tornado in Texas?"

The answer may be different than what you are thinking right now. However the correct answer is that a butterfly's wings in Brazil can cause a tornado in Texas. It might require a truly lengthy investment, yet the association is certifiable. In the event that the butterfly had not fluttered its wings at fair the right point in space/time, the typhoon could not have possibly occurred. In short, it happens many times that little changes inside the basic circumstances lead to outrageous

changes inside the outcomes. The image is taken from IS STOCK photos which represents small distrbance in system can lead to large-scale and unpredictable variation in the future state of the system. This trend can be tested through some linear equations of mathematics.

FIGURE 2.10: Buttrtfly effect

2.5.6 Order / Disorder

Chaos is not simply disordered. Chaos explores the transitions between order and disorder, which often occurs in surprising ways.

2.5.7 Feedback

When there is feedback, systems frequently become chaotic. The stock market's behavior is an excellent example of it. Individuals are influenced to buy or sell a stock when its value grows or decreases. This, in turn, effects the stock's price, leading it to fluctuate erratically.

2.5.8 Fractals

A fractal is an infinite pattern. Fractals are geometric models of chaotic functions that are related to the study of science and mathematics. Fractals are designs that

never end through any scale [15]. Things that appeared unconnected at first yet had a very close link with each other $\phi_g(g)$. If g is the domain of some function g, then the following sequence is the orbit of y for $\phi_g(g)$ is given as [15].

$$\phi_g(g) = y, g(y), g(g(y)) \dots \tag{2.5}$$

2.6 Image Encryption

Within the modern-day trends, the technologies are advanced. Almost everyone uses the internet to send information from one location to another. There are many feasible ways to transmit information using the net like: via e-mails, sending textual content and images, and so forth. In the present communication world, images are widely in use. However, one of the important issues with sending information over the net is the security and authenticity. Encryption is one of the technique for information protection. Image encryption is a method that converts the original image to any other shape that is difficult to recognize. Without a decryption key, no one can view the material. Furthermore, unique and dependable protection in the storage and transmission of virtual images is desired in many packages, which include cable television, online non-public image album, scientific imaging structures, military image communications and personal video conferences, and many others. So one can fulfill this kind of challenge. Encryption is the manner of encoding simple text messages into ciphertext message whereas the opposite method of remodeling ciphertextual content to straight forward text is referred to as decryption. Many image encryption methods were proposed in literature. The image encryption calculations can be ordered into three significant groups.

i) **Position stage based algorithm**.

ii) **Esteem change based algorithm**.

iii) **Visual change based algorithm** .

2.6.1 Terminologies Related to Image Encryption

These are some basic terms that are commonly used in image encryption schemes.

i) **Encryption** is the process from converting cipherimage to cipherimage.

ii) **Decryption** is the restoring cipherimage from cipherimage.

iii) **Key** is a numeric or alphanumeric text or might be a special image. The Key is utilized at the time of encryption process on the Plainimage and at the time of decoding process on the Codedimage. The choice of a key in cryptography is vital since the security of an encryption scheme relies straight forwardly upon it.

iv) **Digital image** is an image composed of image elements, moreover known as pixels, each with limited, discrete amounts of numeric representation for its concentrated or gray level that's a yield from its two-dimensional functions encouraged as input by its spatial arranges denoted on the $x, y - axis$ respectively.

v) **Pixels** is the smallest piece of data in an image. Pixels are organized in a 2-dimensional grid. Each pixel may be a sample of an original image, where more samples regularly give more-accurate representations of the first. The intensity of each pixel is variable in color frameworks, each pixel has regularly three or four components such as ruddy, green, and blue, or cyan, fuchsia, yellow, and black.

Chapter 3

A Chaos Based Image Encryption and its Implementation

3.1 Introduction

In this chapter, the first section contains a brief description and shortcomings of the original encryption algorithm [45] comprises the compound chaotic sequence. Second section consists of the implementation of chaos based image encryption. Third section comprises the security analysis of the scheme presented in the pervious section.

3.2 Cryptantlsis on the Original Algorithm Using a Differential Chosen-Plaintext

1. X.Tong et al. [45] presented an image encryption technique based on a compound chaotic sequence. Later on, Li et al. [46] did the security anaylsis of compound based chaotic seheme and found some drawbacks in this scheme. They revealed that the scheme would be broken by using differential choosen plaintext attacks. In response of this cryptanalysis Ming.Xu [28] proposed a new scheme to counter the attack mounted by Li et al. Additionally, they presented the figure's 3.2 and histogram of the previous Algorithm's image.

2. They also calculated the variance 609.2568 which was large enough, causing the procedure vulnerable to statistical examination. According to [46] the analogous conclusion in [45] was incorrect and inadequate. Li et al. [46] gave observations thats why the compound based chaotic scheme was not secure.

   - Pixel substitution and permutation were unaffected by the plainimage.
   - As a random-number generator, the Compound chaotic sequence used for difusionis inadequate.

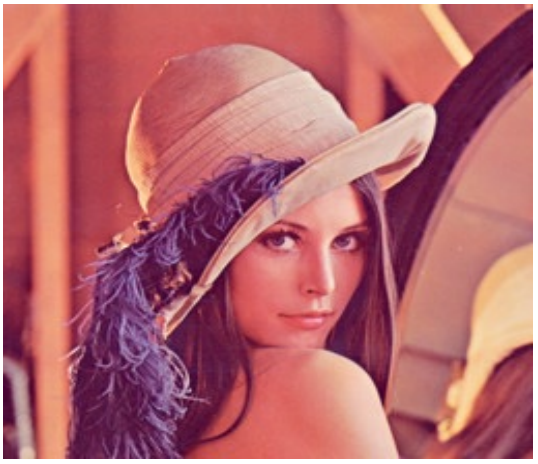


FIGURE 3.1: Plain image.

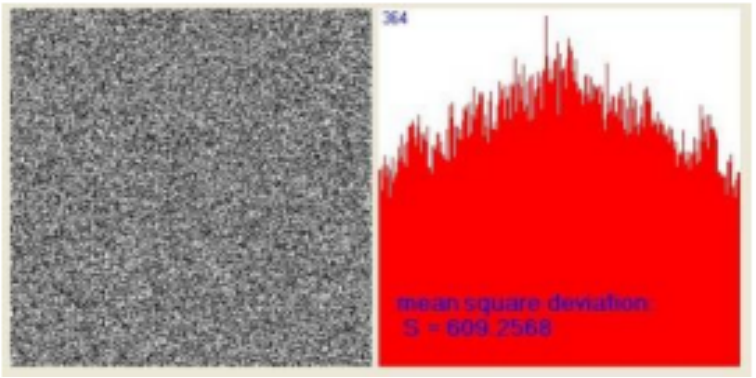


FIGURE 3.2: Encrypted image and its histogram.

3. However, the approach of X.Tong et al. [45] has various advantages, for example, it makes use of Chebyshev map for confusion and diffusion, as well as the permutation is made from of horizontal shifts and vertical shifts, dynamical shifts, all of them are worthy of our reference.

3.3 The Modified Image Cryptoystem

The new encryption algorithm depends on the plainimage and Chen chaotic sequence is used to generate the substitution instead of the compound chaotic sequence.

3.3.1 The Secret keys

The secret keys are two random real numbers of the modified encryption scheme of precision 10^{-14} y_1, $z_1 \in [-1, 1]$.

$$\begin{aligned} L_0 &: y_{n+1} = 8y_n^4 - 8y_n^2 + 1, \\ L_1 &: z_{n+1} = 4z_n^3 - 3z_n \qquad n = 0, 1, 2, \ldots \end{aligned} \tag{3.1}$$

These values of y_1, z_1 will be taken into account as the rst values for both of the Chebyshev polynomials as given in [28] y_1=0.32145645647836, z_1=0.48124356788345. Moreover another set of three secret values will be taken into account as the rst values of Chen's chaotic system are, X_1=-10.058, Y_1=0.368, Z_1=37.368 as given in Equation (2.4). In Equation (2.4) a_1, b_1 and c_1 are the control parameters. If these parmeters are replaced by 35, 3, 28 respectively [47] the system will behave chaotically.

3.3.2 The Initial Phase

Three pseudo-random integer sequences are generated as part of the startup phase.

1. Pseudo-random sequence, $\{\mathbf{T}_1(t)\}_{t=1}^{AB}$ for XOR substitution of pixel values. $A = 256; B = 256$; $R_o = \frac{A*B}{3}$, $1 \leq m \leq R_o$, h=0.0001

$$\begin{aligned} T_1(3(m-1)+1) &= |X_m - \lfloor X_m \rfloor| * 10^{14} \mod 256 \\ T_1(3(m-1)+2) &= |Y_m - \lfloor Y_m \rfloor| * 10^{14} \mod 256 \\ T_1(3(m-1)+3) &= |Z_m - \lfloor Z_m \rfloor| * 10^{14} \mod 256 \end{aligned} \tag{3.2}$$

In Equation (3.2), $\lfloor X \rfloor$ represents floor function. To obtain the real values of X_m, Y_m, Z_m RK 4 Method is applied.

$$\begin{aligned} \frac{dX}{dt} &= a_1(Y - X) = F, \\ \frac{dY}{dt} &= (c_1 - a_1)X - Xr + c_1 Y = G, \\ \frac{dZ}{dt} &= XY - b_1 Z = H \end{aligned} \tag{3.3}$$

In Equation (3.3) a_1, b_1,and c_1 are the the control parameters and some fixed values considered as t_1=0, h=0.0001. The complete scheme of RK-4 is given as.

$$\begin{aligned} k_1 &= h * F(t(i), X(i), Y(i), Z(i)), \\ l_1 &= h * G(t(i), X(i), Y(i), Z(i)), \\ m_1 &= h * H(t(i), X(i), Y(i), Z(i)). \end{aligned}$$

$$\begin{aligned} k_2 &= h * F(t(i) + \frac{h}{2}, X(i) + \frac{k_1}{2}, Y(i) + \frac{l_1}{2}, Z(i) + \frac{m_1}{2}), \\ l_2 &= h * G(t(i) + \frac{h}{2}, X(i) + \frac{k_1}{2}, Y(i) + \frac{l_1}{2}, Z(i) + \frac{m_1}{2}), \\ m_2 &= h * H(t(i) + \frac{h}{2}, X(i) + \frac{k_1}{2}, Y(i) + \frac{l_1}{2}, Z(i) + \frac{m_1}{2}). \end{aligned}$$

$$\begin{aligned} k_3 &= h * F(t(i) + \frac{h}{2}, X(i) + \frac{k_2}{2}, Y(i) + \frac{l_2}{2}, Z(i) + \frac{m_2}{2}), \\ l_3 &= h * G(t(i) + \frac{h}{2}, X(i) + \frac{k_2}{2}, Y(i) + \frac{l_2}{2}, Z(i) + \frac{m_2}{2}), \\ m_3 &= h * H(t(i) + \frac{h}{2}, X(i) + \frac{k_2}{2}, Y(i) + \frac{l_2}{2}, Z(i) + \frac{m_2}{2}). \end{aligned}$$

$$\begin{aligned} k_4 &= h * F(t(i) + h, X(i) + k_3, Y(i) + l_3, Z(i) + m_3), \\ l_4 &= h * G(t(i) + h, X(i) + k_3, Y(i) + l_3, Z(i) + m_3), \\ m_4 &= h * H(t(i) + h, X(i) + k_3, Y(i) + l_3, Z(i) + m_3). \end{aligned}$$

$$\begin{aligned} X(i+1) &= X(i) + \frac{(k_1 + 2k_2 + 2k_3 + k_4)}{6}, \\ Y(i+1) &= Y(i) + \frac{(l_1 + 2l_2 + 2l_3 + l_4)}{6}, \end{aligned}$$

$$Z(i+1) = Z(i) + \frac{(m_1 + 2m_2 + 2m_3 + m_4)}{6},$$
$$t(i+1) = t(1) + ih.$$

Having obtained the values of X_i, Y_i and Z_i from above system and using these values in Equation (3.3), Table 3.1 can be generated.

2. Horizontal permutation $\{T_2(m)\}_{m=1}^{A}$ for row shifting.

$$\begin{aligned} L_0 &: y_{n+1} = 8y_n^4 - 8y_n^2 + 1, \\ L_1 &: z_{n+1} = 4z_n^3 - 3z_n \qquad n = 1, 2, \ldots \end{aligned} \tag{3.4}$$

$$T_2(m) = \begin{cases} \lfloor \frac{1+y_m}{2} B \rfloor, & -1 \leq y_m < 1. \\ B - 1, & \text{if } y_m = 1. \end{cases} \tag{3.5}$$

TABLE 3.1: Some iterative values of Chen chaotic system.

t_i	X_i	Y_i	Z_i	$T_1(m)$
0	-10.058000000	0.3680000000	37.3680000000	0
0.001000000	-9.6915314816	0.8222343737	37.2502049356	0
0.0020000000	-9.3221265374	1.2716789579	37.1286921833	128
0.0030000000	-8.9500544887	1.7161291661	37.0038537260	128
0.0040000000	-8.5755821758	2.1553950508	36.87607989727	0
0.0050000000	-8.1989735471	2.589300904	36.74575842450	0
0.0060000000	-7.820489275	3.017684809	36.6132735235	0
0.00700000000	-7.4403864072	3.4403981536	36.4790050429	0
0.00710000000	-7.4503864072	3.4403990536	36.4790050430	0
0.00700000000	-7.4503864072	3.4403985536	36.4790050430	0

TABLE 3.2: Some iterative values of Chebyshev map for column shifting.

z	$L_1(z)$	$T_3(n)$
0.481244	0.997915667292101	245
0.997915667292101	-0.981293102721896	47
-0.981293102721896	0.835811114800762	226
0.835811114800762	0.171908895833851	144
0.171908895833851	-0.495405221081258	21
-0.495405221081258	0.999873716059895	184
0.999873716059895	0.998863635902597	220
0.998863635902597	0.989788213134064	52
0.998863635902500	0.989788213134165	51
0.998863635902596	0.989788213134063	51

TABLE 3.3: Some iterative values of Chebyshev map for row shifting.

y_1	$L_1(y)$	$T_2(m)$
0.321456	0.258751578720439	242
0.258751578720439	0.500241933032771	136
0.500241933032771	-0.500967497778115	68
-0.500967497778115	-0.503866232407596	54
-0.503866232407596	0.515404212166988	127
0.515404212166988	0.560608755019518	28
0.560608755019518	0.724071119397409	141
0.724071119397409	0.995284246731698	25
0.724071119397410	0.995284246731700	26

3. Vertical permutation $\{T_3(n)\}_{n=1}^{B}$ for column shifting dynamically (the specific process is available in) [45].

$$T_3(n) = \begin{cases} \lfloor \frac{1+z_n}{2} A \rfloor, & -1 \leq z_n < 1. \\ A-1, & \text{if } z_n = 1. \end{cases} \tag{3.6}$$

To obtain a chaotic sequence the Equations given in (3.5) and (3.6) are solved by using the initial values of parametes y_1 and z_1 from Section 3.3.1. The values of $L_0(y)$ and $L_1(z)$ are presented in Tables 3.2 and 3.3 from these Tables one can clearly observe that these values represent a chaotic behavior. The values of $T_2(m)$ and $T_3(n)$ are calculated from Equation (3.5) and (3.6). The values of $T_2(m)$ and $T_3(n)$ are tabulated in Table 3.2 and Table 3.3.

3.3.3 The Encryption Algorithm

As in the original algorithm of X.Tong et al. [45], the encryption technique is performed in three parts: that is an XOR operation based substitution part and two permutation parts, however the order of these three parts has been changed and the newly obtained sequence is more resistive and secure.

1. **Permutation Part, Horizontal Circular Shift Operation** use a simple image $p = \{P_{mn} | \mathbf{1} \leq m \leq A, 1 \leq n \leq B, \}$ as source, where p_{mn} signifies the pixel of P placed at the m_{th} row and n_{th} column. At first, 1 equals to n and use the mod operation to replace the starting key v_0 into an unmarked integer v between 0 and 255, then assign $T_2(1)$ to variation L (L represents the horizontal-shift step length) then carry out the aforementioned steps to every row in the image P $(1 \leq n \leq m)$.

   i) Create the sequence $Q_1 = \{Q_1(n)\}\ _{n=1}^{B+1}$ where $Q_1(1) = v$ and $Q_1(n+1) = P_{mn}$, $1 \leq n \leq B$ after that, perform a horizontal shift of $Q1$ to L pixels. And then obtain a new sequence $Q_2 = \{Q_2(n)\}\ _{n=1}^{B+1}$ as $Q_2(n) = Q_1((n-l) \bmod (B+1))$.

ii) Get the n_{th} row of intermediate image $P^{\star} = \{p^{\star}_{mn} | 1 \leq m \leq A, 1 \leq n \leq B\}$ as $p^{\star}_{mn}$=$Q_2(n)$ $1 \leq n \leq B$, while assigned the final pixel of $Q_2(B+1)$ to $\mathbf{v}$, at last step of 1 replace $p^{\star}_{mB} \bigoplus T_2(m+1)$ to L.

iii) $m = m + 1$, if $m \leq A$, go back to 1, if $m > A$ jump out of the loop.

2. **XOR Based Substitution Part**

   Taking $P^{\star}$ as input. another intermediate image

$$P^{\star\star} = \{P^{\star\star}_{mn} | 1 \leq m \leq A, 1 \leq n \leq B\} \tag{3.7}$$

   is obtained as $P^{\star\star}_{mn}$= $p^{\star}_{mn} \bigoplus T_1((m-1)A+n)$. where $\{1 \leq m \leq A, 1 \leq n \leq B\}$.

3. **Permutation Part-Vertical Circular Shift Operations** Taking $P^{\star\star}$ as input, at first, assign 1 to n and assign $p^{\star\star}_{AB} \bigoplus T_3(1)$ to L.
   to variation L (L represents the vertical-shift step length), and then repeat the following procedures for each column image $P^{\star\star}$ (from $m = 1$ to $n = B$).

   i) Create the sequence $D_1 = \{D_1(j)\}\ {}^{A+1}_{m=1}$ where $D_1(1)$= $\mathbf{v}$ ($\mathbf{v}$ is the variation which is appeared in (1), at present the value of $\mathbf{v}$is that in the last step of (1)) and $D_1(m+1)$=$p^{\star\star}_{mn}$ $1 \leq m \leq A$, then do vertical shift at D_1 by L pixels, we can obtain a new sequence D_2= $\{D_2(n)\}\ {}^{A+1}_{m=1}$ as $D_2(m)$= $D_1((m-L)\mathrm{mod}(A+1))$.

   ii) The n_{th} column of the final cipher image
   $P^{'} = \{a_{mn} | 1 \leq m \leq A, 1 \leq n \leq B\}$ as d_{mn}=$D_2(m)$ $1 \leq m \leq A$, Meanwhile assign the last pixel of $D_2(A+1)$ to $\mathbf{v}$, assign $c_{An} \bigoplus T_3(n+1)$ to L.

   iii) $n = n + 1$, if $n \leq B$, go back to 1, if $n > B$ jump out of the loop. At the end of encryption process cipher image $P^{'}$ is obtained.

3.3.4 The Decryption Algorithm

The decryption of the cipher image can be obtained by adopting the reverse procedure of previous steps. but inintilization process is same.

1. **Permutation part-vertical circular shift operations**

   Taking cipher image $P^{'} = \{d_{mn} | 1 \leq m \leq A, 1 \leq n \leq B\}$ and ciphertext v as input, at first, assign B to n and then for each column of the cipher image $P^{'}$ from (from $n = B$ to $n = 2$);

   repeat the following operations.

   i) Create the sequence $D_2 = \{D_2(m)\}\ {}_{m=1}^{A+1}$, $D_2(m) = d_{mn}\ 1 \leq m \leq A$ Meanwhile assign the last pixel $D_2(A+1)$ to v, compute $L = d_{A(n-1)} \bigoplus T_3(j)$,

   and then do vertical shift at D_2 by L pixel in the direction opposite to the encryption process, we can obtain a new sequence $D_1 = \{D_1(m)\}\ {}_{m=1}^{A+1}$ as $D_1(i) = D_2((m+d) \bmod (A+1))$.

   ii) The n_{th} column of the final intermediate image $P^{\star\star} = \{p_{mn}^{\star\star} | 1 \leq m \leq A, 1 \leq n \leq B\}$ as $p_{mn}^{\star\star} = D_1(m+1)$, $1 \leq m \leq A$, Meanwhile assign the first $D_1(1)$ to v.

   iii) $n = n - 1$, if $n < B$, go back to 1, if $n = 1$ jump out of the loop and go to 4.

   iv) Create the sequence ; $D_2 = \{D_2(m)\}\ {}_{m=1}^{A+1}$, $D_2(m) = d_{m1}\ 1 \leq m \leq A$ Meanwhile assign the last pixel $D_2(M+1)$ to $\mathbf{v}$, compute $d = p_{AB}^{\star\star} \bigoplus T_3(1)$, and then do vertical shift at D_2 by L pixel in the direction opposite to the encryption process, we can obtain a new sequence $D_1 = \{D_1(n)\}\ {}_{m=1}^{A+1}$ as $D_1(m) = D_2((m+L) \bmod (A+1))$.

   Then we get the first column of the intermediate image $P^{\star\star}$ as

$$p_{m1}^{\star\star} = D_1(m+1) 1 \leq m \leq A \tag{3.8}$$

   meanwhile assign the first pixel $D_1(1)$ to v.

2. **XOR substitution part**

   Taking $P^{\star\star}$ as input and another intermediate image $P^{\star} = \{p_{mn}^{\star} | 1 \leq m \leq A, 1 \leq n \leq B\}$ is obtained as

$$p_{mn}^{\star} = p_{mn}^{\star\star} \bigoplus \mathbf{T}_1((m-1)B + n) \tag{3.9}$$

where $\{1 \leq m \leq A, 1 \leq n \leq B\}$.

3. **Permutation part-horizontal circular shift operations**

   Taking image $\mathbf{P}^{\star} = \{p^{\star}_{mn} | 1 \leq m \leq A, 1 \leq n \leq B\}$ and variation $\mathbf{v}$ as input, ($\mathbf{v}$ is the variation which is appeared in (1), at present the value of $\mathbf{v}$is that in the last step of (1)) At first, assign $\mathbf{A}$ to $\mathbf{m}$ and then for each row of the image $\mathbf{P}^{\star}$ (from $m = A$ to $m = 2$);

   repeat the following operations.

   i) Create the sequence $\mathbf{Q}_2 = \{\mathbf{Q}_2(n)\}\ {}^{B+1}_{n=1}$, $\mathbf{Q}_2(n) = p^{\star}_{mn}$, $1 \leq n \leq B$, Meanwhile assign the last pixel $\mathbf{Q}_2(B+1)$ to v, compute $\mathbf{d} = p^{\star}_{(m-1)B} \bigoplus \mathbf{T}_2(m)$,

   and then do vertical shift at Q_2 by L pixel in the direction opposite to the encryption process, we can obtain a new sequence $Q_1 = \{\mathbf{Q}_1(n)\}^{B+1}_{n=1}$ as $Q_1(n) = Q_2((m+L)\mathrm{mod}(B+1))$.

   ii) Get the m_{th} row of the final image $\mathbf{P} = \{p_{mn} | 1 \leq m \leq A, 1 \leq n \leq B\}$ as $p_{mn} = \mathbf{Q}_1(n+1)$ $1 \leq n \leq B$, Meanwhile assign the first $Q_1(1)$ to v.

   iii) $m = m - 1$, if $m \geq 1$, go back to 1, if $m = 1$ jump out of the loop and go to 4.

   iv) create the sequence $\mathbf{Q}_2 = \{\mathbf{Q}_2(n)\}\ {}^{B+1}_{n=1}$, $\mathbf{Q}_2(n) = p_{1n}$ $1 \leq n \leq B$ Meanwhile assign the last pixel $\mathbf{Q}_2(B+1)$ to $\mathbf{v}$, and then do vertical shift at $\mathbf{Q}_2$ by $\mathbf{T}_2(1)$ pixel in the direction opposite to the encryption process, we can obtain a new sequence $Q_1 = \{\mathbf{Q}_1(n)\}\ {}^{B+1}_{n=1}$ as $Q_1(m) = Q_2((m+L)\mathrm{mod}(A+1))$.

   Then we get the first row of the plain image $\mathbf{P}$ as $\mathbf{p}_{mn} = Q_1(n+1)$ $1 \leq n \leq B$, meanwhile assign the first pixel $Q_1(1)$ to $\mathbf{v}$.

3.4 An Implementation of Chaos based Image Encryption

The above encryption and decryption algorithm are implemented on the MATLAB. The working of these algorithms is illustrated here with the following toy

example. **The initilization procedure**

$$T_1(i) = \begin{bmatrix} 1 & 0 & 2 & 2 & 1 \\ 2 & 1 & 3 & 2 & 0 \\ 1 & 3 & 2 & 3 & 3 \\ 4 & 3 & 0 & 4 & 3 \\ 0 & 1 & 1 & 3 & 4 \end{bmatrix} T_2(i) = \begin{bmatrix} 3 \\ 4 \\ 3 \\ 1 \\ 2 \end{bmatrix} T_3(j) = \begin{bmatrix} 4 \\ 2 \\ 1 \\ 2 \\ 3 \end{bmatrix} \tag{3.10}$$

$T_1(i)$ represents a matrix values of chen chaotic system. These values are using RK-4 Method. $T_2(i)$ and $T_3(j)$ two matrices are drawn by using chebyshev maps.

3.4.1 The Encryption Algorithm

$$P = \begin{bmatrix} ② & 3 & 4 & 1 & 3 \\ 4 & 1 & 3 & 2 & 2 \\ 2 & 2 & 3 & 4 & 1 \\ 0 & 1 & 2 & 4 & 3 \\ 4 & 3 & 1 & 3 & 2 \end{bmatrix} \tag{3.11}$$

$\mathbf{p} = \{P_{mn} | \mathbf{1} \leq m \leq A, 1 \leq n \leq B\}$

A =5 ;B=5 at start m=1 v_0 =2; L=$T_2(1)$ =3; (L represents the horizontal-shift step length), and then repeat the following procedures for each row of the image P (from $m = 1$ to $m = A$):

1. create the sequence $\mathbf{Q}_1 = \{\mathbf{Q}_1(n)\}\ _{n=1}^{B+1}$ where $Q_1(1) = v$ and $Q_1(n+1) = \mathbf{p}_{mn}$, $1 \leq n \leq B$ then do horizontal shift at Q_1 by L pixels.

we can obtain a new sequence Q_2= $\{\mathbf{Q}_2(n)\}\ _{n=1}^{B+1}$ as $Q_2(n)$=$Q_1((n-L)\text{mod}(B+1))$. Here we assume $Q_3(m,n)$=$(n-L)\text{mod}(B+1)$.

if $Q_3(m,n)$=0 then $Q_3(m,n)$=6; Q_2=$Q_1(Q_3)$

$$Q_1 = \begin{bmatrix} 2 & 2 & 3 & 4 & 1 & 3 \\ 3 & 4 & 1 & 3 & 2 & 2 \\ 2 & 2 & 2 & 3 & 4 & 1 \\ 4 & 0 & 1 & 2 & 4 & 3 \\ 2 & 4 & 3 & 1 & 3 & 2 \end{bmatrix} Q_3 = \begin{bmatrix} 4 & 5 & 6 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 3 & 4 & 5 \\ 5 & 6 & 1 & 2 & 3 & 4 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{bmatrix} Q_2 = \begin{bmatrix} 4 & 1 & 3 & 2 & 2 & 3 \\ 3 & 4 & 1 & 3 & 2 & 2 \\ 1 & 2 & 2 & 2 & 3 & 4 \\ 4 & 3 & 4 & 0 & 1 & 2 \\ 1 & 3 & 2 & 2 & 4 & 3 \end{bmatrix} \tag{3.12}$$

2. Get the m_{th} row of intermediate image $\mathbf{P}^{\star} = \{p^{\star}_{mn} | 1 \leq m \leq A, 1 \leq n \leq B\}$ as $p^{\star}_{mn}$=$\mathbf{Q}_2(n)$ $1 \leq n \leq B$,Meanwhile assign the last pixel of $\mathbf{Q}_2(B+1)$ to $\mathbf{v}$,Assign $\mathbf{p}^{\star}_{mB} \bigoplus \mathbf{T}_2(m+1)$ to $\mathbf{L}$.

$$\mathbf{P}^{\star} = \begin{bmatrix} 4 & 1 & 3 & 2 & 2 \\ 3 & 4 & 1 & 3 & 2 \\ 1 & 2 & 2 & 2 & 3 \\ 4 & 3 & 4 & 0 & 1 \\ 1 & 3 & 2 & 2 & 4 \end{bmatrix} \tag{3.13}$$

v= $\mathbf{Q}_2(m, B+1)$, $\mathbf{L}$= $\mathbf{p}^{\star}_{mB} \bigoplus \mathbf{T}_2(m+1)$

v= $\mathbf{Q}_2(1,6)$=3; , $\mathbf{L}$= $\mathbf{p}^{\star}_{1,5} \bigoplus \mathbf{T}_2(2)$ =2 $\bigoplus$ 4=6

v= $\mathbf{Q}_2(2,6)$=2; , $\mathbf{L}$= $\mathbf{p}^{\star}_{2,5} \bigoplus \mathbf{T}_2(3)$ =2 $\bigoplus$ 3=1

v= $\mathbf{Q}_2(3,6)$=4; , $\mathbf{L}$= $\mathbf{p}^{\star}_{3,5} \bigoplus \mathbf{T}_2(4)$ =3 $\bigoplus$ 1=2

v= $\mathbf{Q}_2(4,6)$=2; , $\mathbf{L}$= $\mathbf{p}^{\star}_{4,5} \bigoplus \mathbf{T}_2(5)$ =1 $\bigoplus$ 2=3

v= $\mathbf{Q}_2(5,6)$=3; next to be used

2. Xor substitution part.

Taking $\mathbf{P}^{\star}$ as input.another intermediate image $\mathbf{P}^{\star\star}$= $\{P^{\star\star}_{mn} | 1 \leq m \leq A, 1 \leq n \leq B\}$ is obtained as $P^{\star\star}_{mn}$= $p^{\star}_{mn} \bigoplus \mathbf{T}_1((m-1)B+n)$. where $\{1 \leq m \leq A, 1 \leq n \leq B\}$.

$$\mathbf{P}^{\star\star} = \begin{bmatrix} 4 & 1 & 3 & 2 & 2 \\ 3 & 4 & 1 & 3 & 2 \\ 1 & 2 & 2 & 2 & 3 \\ 4 & 3 & 4 & 0 & 1 \\ 1 & 3 & 2 & 2 & 4 \end{bmatrix} \bigoplus \begin{bmatrix} 1 & 0 & 2 & 2 & 1 \\ 2 & 1 & 3 & 2 & 0 \\ 1 & 3 & 2 & 3 & 3 \\ 4 & 3 & 0 & 4 & 3 \\ 0 & 1 & 1 & 3 & 4 \end{bmatrix} = \begin{bmatrix} 5 & 1 & 1 & 0 & 3 \\ 1 & 5 & 2 & 1 & 2 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 4 & 4 & 2 \\ 1 & 2 & 3 & 1 & 0 \end{bmatrix} \tag{3.14}$$

3.Permutation part-vertical circular shift operations

Taking $\mathbf{P}^{\star\star}$ as input, At first, assign **1** to **n** and Assign $p^{\star\star}_{AB} \bigoplus \mathbf{T}_3(1)$ to $\mathbf{L}$. $\mathbf{v}$ =3, $\mathbf{L}$ =4, Here we assume $A_3(m,n)$=$(m-L)\mathrm{mod}(B+1)$.

if $D_3(m,n)$=0 then $D_3(m,n)$=6;

D_2=$D_1(D_3)$

$$D_1 = \begin{bmatrix} 3 & 5 & 0 & 3 & 1 \\ 5 & 1 & 1 & 0 & 3 \\ 1 & 5 & 2 & 1 & 2 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 4 & 4 & 2 \\ 1 & 2 & 3 & 1 & 0 \end{bmatrix} D_3 = \begin{bmatrix} 3 & 6 & 1 & 1 & 6 \\ 4 & 1 & 2 & 2 & 1 \\ 5 & 2 & 3 & 3 & 2 \\ 6 & 3 & 4 & 4 & 3 \\ 1 & 4 & 5 & 5 & 4 \\ 2 & 5 & 6 & 6 & 5 \end{bmatrix} D_2 = \begin{bmatrix} 1 & 2 & 0 & 3 & 0 \\ 0 & 5 & 1 & 0 & 1 \\ 0 & 1 & 2 & 1 & 3 \\ 1 & 5 & 0 & 1 & 2 \\ 3 & 1 & 4 & 4 & 0 \\ 5 & 0 & 3 & 1 & 2 \end{bmatrix} \tag{3.15}$$

2. Get the n_{th} column of the final cipher image $\mathbf{P}^{'} = \{d_{ij} | \mathbf{1} \leq m \leq A, 1 \leq n \leq B\}$ as d_{mn}=$\mathbf{D}_2(m)$ $1 \leq m \leq A$, Meanwhile assign the last pixel of $\mathbf{D}_2(B+1)$ to $\mathbf{v}$,Assign d_{An} $\bigoplus$ $\mathbf{T}_3(n+1)$ to $\mathbf{L}$.

3. $n = n+1$, if $n \leq B$, go back to 1, if $n > B$ jump out of the loop.

$$\mathbf{P}^{'} = \begin{bmatrix} 1 & 2 & 0 & 3 & 0 \\ 0 & 5 & 1 & 0 & 1 \\ 0 & 1 & 2 & 1 & 3 \\ 1 & 5 & 0 & 1 & 2 \\ 3 & 1 & 4 & 4 & 0 \end{bmatrix} \tag{3.16}$$

v= $\mathbf{D}_2(M+1, j)$, $\mathbf{L}$= $\mathbf{p}^{'}_{An} \bigoplus \mathbf{T}_3(j+1)$

v= $\mathbf{D}_2(6,1)$=5 , $\mathbf{L}$= $\mathbf{p}^{'}_{5,1} \bigoplus \mathbf{T}_3(2)$ =3 $\bigoplus$ 2=1

v= $\mathbf{D}_2(6,2)$=0 , $\mathbf{L}$= $\mathbf{p}^{'}_{5,2} \bigoplus \mathbf{T}_3(3)$ =1 $\bigoplus$ 1=0

v= $\mathbf{D}_2(6,3)$=3 , $\mathbf{L}$= $\mathbf{p}^{'}_{5,3} \bigoplus \mathbf{T}_3(4)$ =4 $\bigoplus$ 2=6

v= $\mathbf{D}_2(6,4)$=1 , $\mathbf{L}$= $\mathbf{p}^{'}_{5,4} \bigoplus \mathbf{T}_3(5)$ =4 $\bigoplus$ 3=7

3.4.2 The Decryption Algorithm

$\mathbf{L}$=$d^{'}_{A(n-1)} \bigoplus T_3$(n); $D_3(m,n)$=$(m+L)$mod$(B+1)$.

if $D_3(m,n)$=0 then $D_3(m,n)$=6;

D_1=$D_2(D_3)$

L=7,6,0,1,4

$$\mathbf{P}^{'} = \begin{bmatrix} 1 & 2 & 0 & 3 & 0 \\ 0 & 5 & 1 & 0 & 1 \\ 0 & 1 & 2 & 1 & 3 \\ 1 & 5 & 0 & 1 & 2 \\ 3 & 1 & 4 & 4 & 0 \end{bmatrix} \tag{3.17}$$

$$D_2 = \begin{bmatrix} 1 & 2 & 0 & 3 & 0 \\ 0 & 5 & 1 & 0 & 1 \\ 0 & 1 & 2 & 1 & 3 \\ 1 & 5 & 0 & 1 & 2 \\ 3 & 1 & 4 & 4 & 0 \\ 5 & 0 & 3 & 1 & 2 \end{bmatrix} D_3 = \begin{bmatrix} 5 & 2 & 1 & 1 & 2 \\ 6 & 3 & 2 & 2 & 3 \\ 1 & 4 & 3 & 3 & 4 \\ 2 & 5 & 4 & 4 & 5 \\ 3 & 6 & 5 & 5 & 6 \\ 4 & 1 & 6 & 6 & 1 \end{bmatrix} \mathbf{D}_1 = \begin{bmatrix} 3 & 5 & 0 & 3 & 1 \\ 5 & 1 & 1 & 0 & 3 \\ 1 & 5 & 2 & 1 & 2 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 4 & 4 & 2 \\ 1 & 2 & 3 & 1 & 0 \end{bmatrix} \tag{3.18}$$

Substitution Part

$$\mathbf{P}^{\star\star} = \begin{bmatrix} 5 & 1 & 1 & 0 & 3 \\ 1 & 5 & 2 & 1 & 2 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 4 & 4 & 2 \\ 1 & 2 & 3 & 1 & 0 \end{bmatrix} \bigoplus \begin{bmatrix} 1 & 0 & 2 & 2 & 1 \\ 2 & 1 & 3 & 2 & 0 \\ 1 & 3 & 2 & 3 & 3 \\ 4 & 3 & 0 & 4 & 3 \\ 0 & 1 & 1 & 3 & 4 \end{bmatrix} = \begin{bmatrix} 4 & 1 & 3 & 2 & 2 \\ 3 & 4 & 1 & 3 & 2 \\ 1 & 2 & 2 & 2 & 3 \\ 4 & 3 & 4 & 0 & 1 \\ 1 & 3 & 2 & 2 & 4 \end{bmatrix} \tag{3.19}$$

$L{=}p'_{(m-1)B} \bigoplus T_3(\mathrm{n})$, $Q_3(m,n){=}(n+L)\mathrm{mod}(B+1)$

$$Q_2 = \begin{bmatrix} 4 & 1 & 3 & 2 & 2 & 3 \\ 3 & 4 & 1 & 3 & 2 & 2 \\ 1 & 2 & 2 & 2 & 3 & 4 \\ 4 & 3 & 4 & 0 & 1 & 2 \\ 1 & 3 & 2 & 2 & 4 & 3 \end{bmatrix} Q_3 = \begin{bmatrix} 4 & 5 & 6 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \\ 3 & 4 & 5 & 6 & 1 & 2 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{bmatrix} Q_1 = \begin{bmatrix} 2 & 2 & 3 & 4 & 1 & 3 \\ 3 & 4 & 1 & 3 & 2 & 2 \\ 2 & 2 & 2 & 3 & 4 & 1 \\ 4 & 0 & 1 & 2 & 4 & 3 \\ 2 & 4 & 3 & 1 & 3 & 2 \end{bmatrix} \tag{3.20}$$

$$P = \begin{bmatrix} 2 & 3 & 4 & 1 & 3 \\ 4 & 1 & 3 & 2 & 2 \\ 2 & 2 & 3 & 4 & 1 \\ 0 & 1 & 2 & 4 & 3 \\ 4 & 3 & 1 & 3 & 2 \end{bmatrix} \tag{3.21}$$

3.5 Results and Discussion

There are several tests conducted and results have proved their efficiency as well as accuracy of suggested approach. The images utilised (Lena, Barbera, Baboon) are gray-scale images from the USC SIPI public media library. The image encryption strategy is implemented on a PC running MATLAB R2017a with the O.S Windows 8.0 64bit, a Core i5-4300M with a 2.60 GHz CPU, and 8 G of RAM. Initial keys are randomly

selected as $y_1 = 0.321456$, $z_1 = 0.481244$ and the initial values of Chen's chaotic system are X_1=-10.058, Y_1=0.368, Z_1=37.368. Figure 3.3 depicts that outcome of our described algorithm's encryption and decryption.

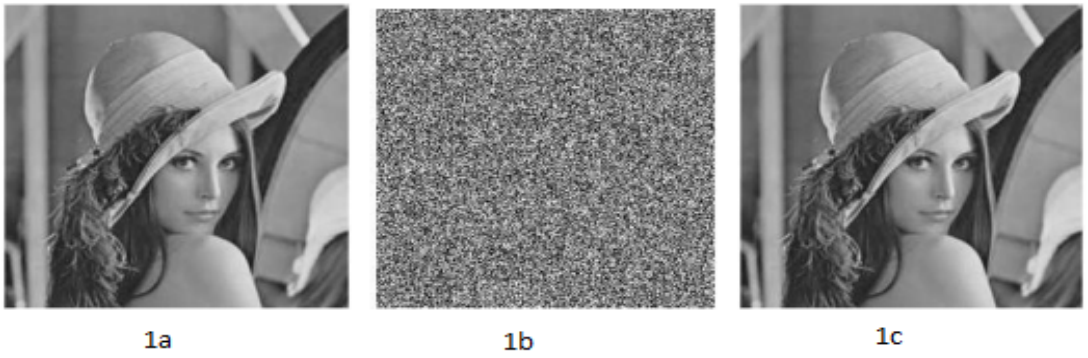


FIGURE 3.3: Experimental results: (1a) Plain image of Lena,(1b) Cipher image of Lena and (1c) Decrypted image of Lena.

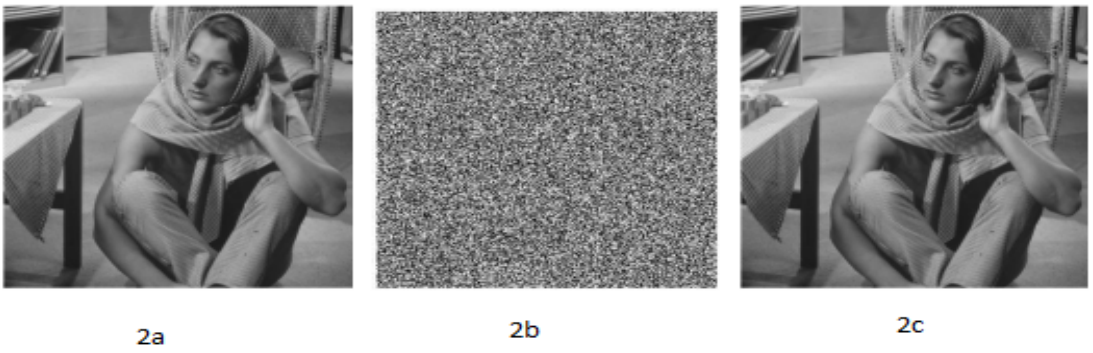


FIGURE 3.4: Experimental results: (2a) Plain image of Barbera, (2b) Cipher image of Barbera and (2c) Decrypted image of Barbera.

FIGURE 3.5: Experimental results: (3a) Plain image of Baboon,(3b) Cipher image of Baboon and (3c) Decrypted image of Baboon.

3.5.1 Security Analysis

This part examines security assessments such as (keys-space, sensitivities, and stats) and their correlations.

1. **Key-Space Analysis**

   Minimum key space of 10^{30} is suggested to bothstrong security and resilience to brute-force attacks [48]. The suggested technique makes use of the keys x_1, y_1, X_1, Y_1 and Z_1. The number of possible key combinations is 10^{70} when the precision is set to 10^{-14}. As a result, the brute force attack is difficult to execute successfully.

2. **Key sensitivity**

   A decent image encryption technique should be key sensitive in order to avoid unauthorised preliminary attacks. As an example, Figure 3.6 (a) displays the plainimage of a Boat of size 256 by 256. Figure 3.6 (b) depicts the cipherimage of a boat. However, decryption is then done on $x_1^{'}$, $y_1^{'}$, $X_1^{'}$, $Y_1^{'}$ and $Z_1^{'}$. Figures 3.7 and 3.8 indicate that if a little modification of 10^{-14} is made in keys, the results are wrong (c - g). This indicates how sensitive the algorithm is to key.

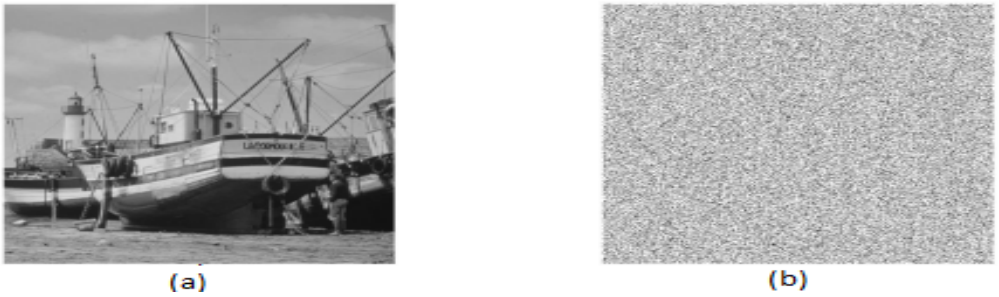


FIGURE 3.6: Key sensitivity: (a) Plain image of boat and (b) Cipher Image of a boat.

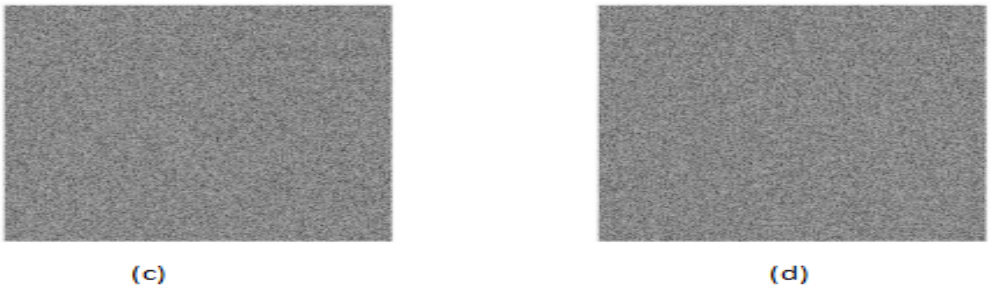


FIGURE 3.7: Incorrect decryption of (b) using first two altered keys.

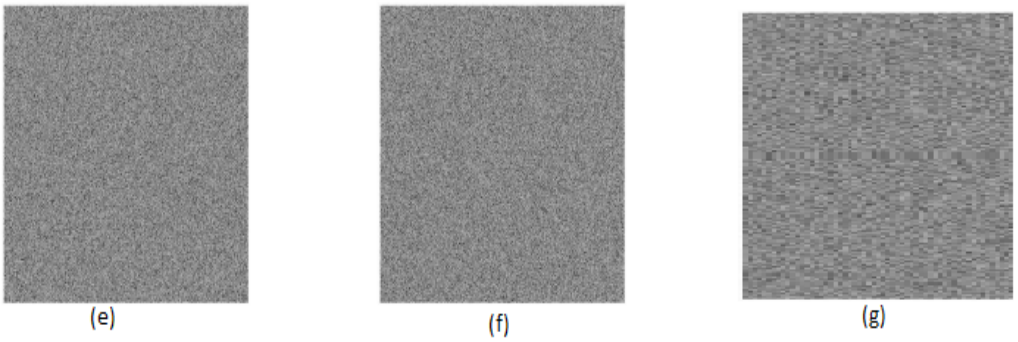


FIGURE 3.8: Incorrect decryption of (b) using last three altered keys.

3.5.2 Differential Attacks

Differential cryptanalysis is a broad term for cryptanalysis that mostly applies to block ciphers that operate on binary sequences. Differential cryptanalysis is commonly credited to Biham and Shamir [49]. They published their article on this form of attack on many ciphers. They also included theoretical vulnerability of the (DES) [50]. As a result, the differential attack has become a prevalent attack that has been be addressed during encryption design [51]. There are two types of differential attacks given below.

1. **Number of Pixels Change Rate (NPCR)**
2. **Unified Average Change Intensity (UACI)**

It is interesting to note that, NPCR and UACI was firstly introduced in 2004 [25, 52] From that era, NPCR and UACI have been two frequently utilized in security investigations in the image encryption field for diverse attacks.

- **Definition**

  The NPCR is developed to assess the number of changing pixels. The UACI is developed averaged altered intensity between ciphertext images.

  Assume we have a plainimage P_1 and its cipherimage is P_1^*. Now we change in one pixel in plainimage. The new plainimage is P_2 and its cipher image is P_2^*. Now the pixel esteem of cipherimages at that network is (m, n) indicated by $P_1^*(m, n)$ and $P_2^*(m, n)$. we can find NPCR and UACI by solving following equations.

- **Mathematical form**

$$Q_2(m,n) = \begin{cases} 0, & \text{if } P_1^*(m,n) = P_2^*(m,n), \\ 1, & \text{if } P_1^*(m,n) \neq P_2^*(m,n). \end{cases} \tag{3.22}$$

$$UACI = \frac{1}{L \times M}[\sum_{m,n} \frac{|p_1^*(m,n) - p_2^*(m,n)|}{255}] \times 100\% \tag{3.23}$$

$$NPCR = \frac{\sum_{n,m} Q_2(m,n)}{L \times M} \times 100\% \tag{3.24}$$

The greatest permitted pixels appropriate with the ciphertext image format is denoted by L . M denotes the pixels. From the above equations we can easily conclude that the NPCR concentrates on the absolute number of pixels that change value in differential attacks. The UACI concentrates on the averaged difference between two paired images [51]. The NPCR and UACI both have ranges [0,1]. Table 3.4 displays the numerical findings for UACI and NPCR [51].

TABLE 3.4: Numericals findings of UACI and NPCR .

Image	$Mean_{NPCR}$	$Mean_{UACI}$
64*by*64	99.6094000000	33.4635416667
128*by*128	99.6094000000	33.4635416667
256*by*256	99.6094000000	33.4635416667
512*by*512	99.6094000000	33.4635416667
1024*by*1024	99.6094000000	33.4635416667

The results of testing several images by altering the value of a pixels at random positions are shown in Table 3.5. As a result, even modest changes to the plain image result in a drastically different cipher image. In other words, our technique satisfies the high plaintext sensitivity criteria. Equation (3.23) is used to determine the value of UACI, and equation (3.24) is used to calculate the value of NPCR.

TABLE 3.5: Experimental Results of Different Images

Image	*lena*	*Baboon*	*Barbera*
NPCR	99.609375	99.5956	99.5956
UACI	33.36271	33.4177	33.4758

3.5.3 Statistical Analysis

Data analysis is used to discover the link between plain image and cipher image. As a result, plain imageis completely different after encryption.

1. **Histogram**

   A histogram can be used to depict the grey distribution. The histogram of the cipher image should be uniform or nearly uniform, and it should differ from the plain image after encryption to match the requirements of a successful encryption technique.

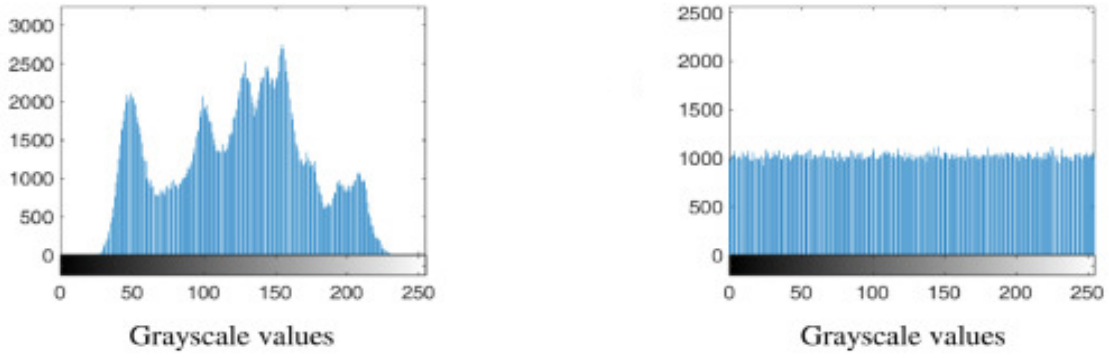


FIGURE 3.9: Histograms of encrypted image (Lena).

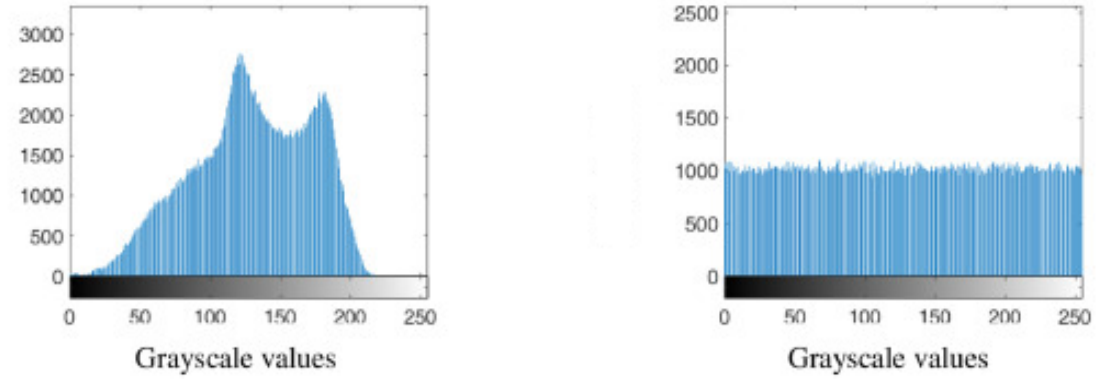


FIGURE 3.10: Histograms of encrypted image (Barbera).

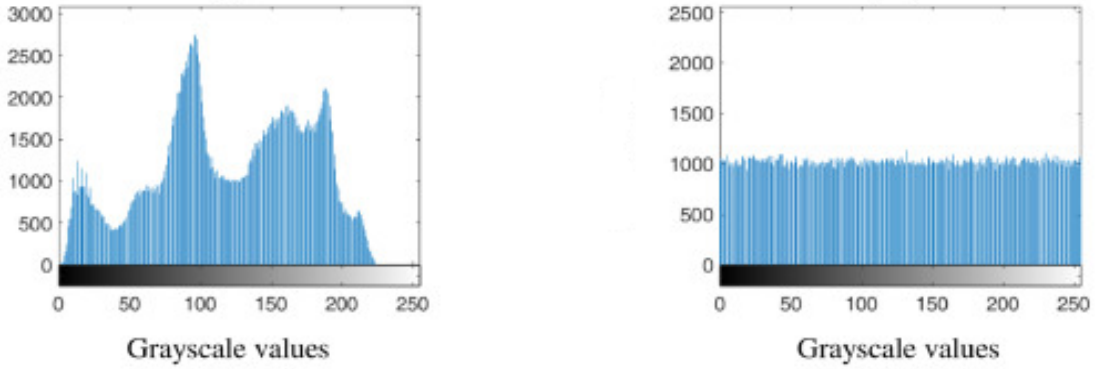


FIGURE 3.11: Histograms of encrypted image (Baboon).

2. **Correlation Coefficient**

The Pearson correlation coefficient (PCC) [53] of two neighboringpixels in a basic plain image is often high. For a successful coding technique to be employed on a basic image, there must be a weak association between nearby pixels in the corresponding coded image. When comparing the similarity of two adjacent pixels in a plain-image and a cipher-image, The PCC of all neighboringpixels (vertical, horizontal, and diagonal) in a plain -image and a cipher-image is determined using the formula below.

$$\begin{aligned} P(a) &= \frac{1}{Z}\sum_{n=1}^{Z} a_{(n)} \\ Q(a) &= \frac{1}{Z}\sum_{n=1}^{Z} (a_{(n)} - P(a))^2 \\ R(b,a) &= \frac{1}{Z}\sum_{n=1}^{Z} (b_n - P(a))(a_{(n)} - P(a)) \\ r_{ba} &= \frac{R(b,a)}{\sqrt{(Q(a))(Q(b))}} \end{aligned} \tag{3.25}$$

TABLE 3.6: Correlation Coffeicent of Cipher Image (lena).

Direction	*Plainimage*	*Cipherimage*
Vertical	0.9583243	-0.002944
Horizontel	0.9783154	0.0061854
Diagonal	0.933050	0.003079

Two nearby pixels values are a and b, the correlation coefficient is r. The test outcomes are listed in Table 3.6. The findings show that the PCC in the cipher image generated by current approach is near to zero.

3.5.4 Information Entropy

The most essential property of randomness is information entropy. The information entropy is computed using equation (3.26) which is then used to test the various images.The computation for information entropy $P(a)$ of an information is as follows.

$$P(a) = \sum_{u=0}^{2^Z-1} I(a_{(u)}) \log_2 \frac{1}{I(a_{(u)})} \tag{3.26}$$

If we choose information from an image Lena, then Z is number of bits of that source.We choose 256 by 256 image so number of bits is 8 . This means Z is 8. $I(a_u)$is probability of that source which is 1/256, then

$$P(a) = \sum_{u=0}^{255} I(a_{(u)}) \log_2 \frac{1}{I(a_{(u)})} = 8 \tag{3.27}$$

Theoretically informational entropy is equal to 8. The grey scale image Lena has an information entropy of 7.56828525761. The value of Information Entropy is highly sensitive even when the value of a one or two pixel changes, the value of Information Entropy changes as well. It is utilized to impact the generation of our algorithm as well as key stream selection, Table 3.7 displays the Information Entropy results of different images such as lena, Barbera and Baboon. This is because the suggested algorithm's information entropy values are near to the theoretical value of 8, it may withstand information entropy attacks and create an equivalent random message for the cipher-image after employing the approach.

TABLE 3.7: Information Analysis.

image	*Lena*	*Barbera*	*Baboon*
plainimage	7.5682	7.4664	7.3583
cipherimage	7.9974	7.9992	7.9769

Chapter 4

A Modified Image Encryption Scheme based on Henon Chaotic Map and Brownian Motion

4.1 Introduction

In this chapter, we present a new image encryption technique based on Henon chaotic maps to improve efficiency, provide a high degree of security, and decrease the overhead delay for real-time image encryption. A 2-D chaotic map is utilised in this study to generate the chaotic sequence and to regulate the encryption process. Henon maps, together with all of its qualities and characteristics, have been explored and employed among the many maps. The suggested technique randomly shuffles image pixels. Furthermore, to strengthen the cipherimage, pixel values are adjusted using a bitwise XOR operation between the original pixel value and a key. Table values are generated from the same chaotic map.

4.2 Brownian motion

Our goal here is to create an image encrypted based on technique using 2-D chaotic maps and Brownian motion. Brownian motion is the randomized particle movement suspended in fluid (liquid or gas) caused by the quick collision of liquid or gas molecules.

The word "Brownian motion" is a mathematical concept or model used in the creation of safe cryptosystems that describes the "random movement of particles". Wang and Xu [54] employed the Monte Carlo approach to encrypt the original test image in 2014, using a single particle from Brownian theory as a pixel. In 2015, Zhu [55] broke the technique created by then [54]. since the system designed by Wan was based on permutation and diffusion sequences that had nothing to do with plaintext images, making their approach ineffective.

It is the chaotic (zig-zag) movement of particles along three separate axes, notably the X, Y, and Z axes as shown in Figure 4.1. The particle's behaviour is named for botanist Brown, who studied microscopic particles. He discovered the notion at the first time when pollen grains dropped into a stream and he saw variations and random motion in the water, albeit he did not discover the basis for the behaviour he witnessed. Later, in 1905, one of the greatest scientist's of all time, Albert Einstein, wrote a paper in which he described the precise irregular motion of particles seen by Brown.

Our major goal is to create a strong algorithm that is resistant to cryptanalysis and has few weaknesses that may be exploited to get access to encrypted digital items. In cryptanalysis, hackers investigate potential breaches and flaws in attempt, to decipher the encryption algorithm. Certain statistical procedures that assure the strength of the suggested algorithm can be used to validate the robustness of the proposed system. The cryptosystem's strength is heavily dependent on two factors, the proposed algorithm for encryption and the confidentiality of keys used in the proposed system to encrypt information. To generate the most random sequence, we employed Brownian particle motion and henon chaotic maps. Before this we assumed and defined a particular number of particles with respect to time. These particles aided us in attaining the effect of zigzag motion of initially defined particles with regard to time and presumed particle number. The presumed particles are determined by the number of pixels in the test image, and the track varies as the influence of these particles changes. These particles are arranged in a three-dimension along the X, Y, and Z axes and the security analyst can propose their cryptosystem in any direction along the X, Y, and Z axes. The combined action of the X, Y, and Z axes can make the system more secure. To improve resistance, the zig-zag motion sequence is injected into Hanon chaotic map to produce a highly randomized pattern.

It is shown in Fig 4.2, that a point in space can be represented by the equation (4.1)

that follows spherical coordinates. where $0 \leq p \leq \infty$, $0 \leq y \leq 2\pi$, and $0 \leq z \leq 2\pi$.

$$\begin{aligned} X &= p \sin y \cos z \\ Y &= p \sin y \sin z \\ Z &= p \cos y \end{aligned} \tag{4.1}$$

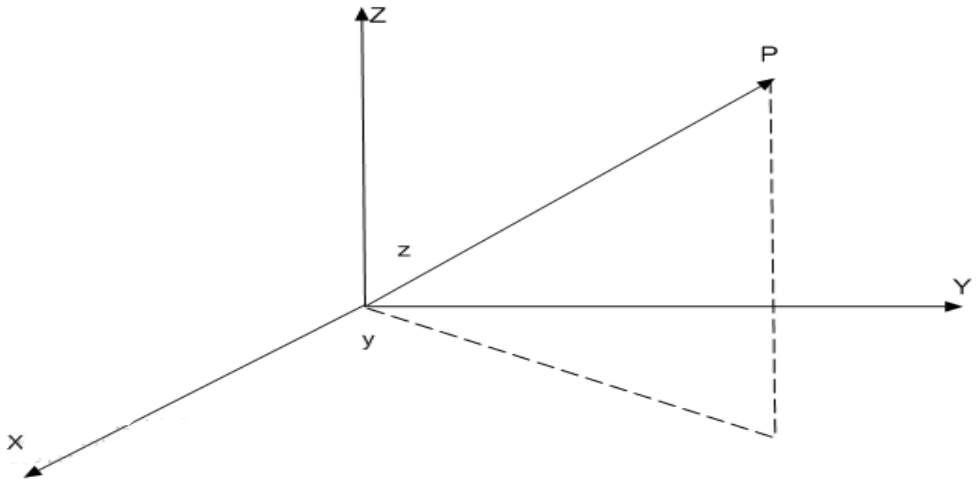


FIGURE 4.1: Brownian Motion in 3 dimension.

4.2.1 The Initial Strategy

Three pseudo-random integer sequences are generated as part of the startup phase.

1. Pseudo-random sequence . $\{\mathbf{T}_1(t)\}_{t=1}^{AB}$ for XOR substitution of pixel values is given as,

$$\begin{aligned} T_1(3(m-1)+1) &= |X_m - \lfloor X_m \rfloor| * 10^{14} \mod 256 \\ T_1(3(m-1)+2) &= |Y_m - \lfloor Y_m \rfloor| * 10^{14} \mod 256 \\ T_1(3(m-1)+3) &= |Z_m - \lfloor Z_m \rfloor| * 10^{14} \mod 256 \end{aligned} \tag{4.2}$$

In equation (4.2) $\lfloor X \rfloor$ represents floor function. To obtain the real values of X_m, Y_m, Z_m we use Brownian motion and for the iteretion of brownian motion we use Hanon chaotic map .

$A = 256, B = 256,\ R_o = \frac{A*B}{3},\ 1 \leq m \leq R_o,\ P = 2$

$$\begin{aligned} X_m &= p \sin y_a(m) \cos z_b(m) \\ Y_m &= p \sin y_a(m) \sin z_b(m) \\ Z_m &= p \cos y_a(m) \end{aligned} \tag{4.3}$$

$$\begin{aligned} y_a(m) &= y_m \pi \\ z_b(m) &= 2 z_m \pi \end{aligned} \tag{4.4}$$

$$\begin{aligned} y_{m+1} &= 1 + z_m - t y_{m^2}, \\ z_{m+1} &= u y_m \end{aligned} \tag{4.5}$$

The Henon chaotic map lies between $[-1.5, 1.5]$ on the X-axis and $[-0.4, 0.4]$ on the Y-axis. If $u = 0.3$ is fixed and t varies in the range of $[0, 1.5]$ the henon map behave chaoticaly.

2. Horizontal permutation $\{\mathbf{T}_2(m)\}_{m=1}^{A}$ for row shifting.

$$T_2(m) = \begin{cases} \lfloor \frac{1+y_m}{2} B \rfloor, & -1 \leq y_m < 1. \\ B - 1, & \text{if } y_m = 1. \end{cases} \tag{4.6}$$

3. Vertical permutation $\{\mathbf{T}_3(n)\}_{n=1}^{B}$ for column shifting dynamically.

$$T_3(n) = \begin{cases} \lfloor \frac{1+z_n}{2} A \rfloor, & -1 \leq z_n < 1. \\ A - 1, & \text{if } z_n = 1. \end{cases} \tag{4.7}$$

To obtain chaotic sequences the Equation given in (4.6) are solved by using randomly choosen values as $z_m = 0.12346545678544, y_m$=0.1284345344434 and parameters as $t = 1.4$ and $u = 0.3$.

The values of y_m and z_m can easily be calculated using matlab .Having obtained the values of X_m, Y_m and Z_m from above system and using these values in equation (4.3) one gets a sequence T_1. From calculated one can clearly observe that these values represent a chaotic behavior. In view of reported values $T_2(m)$ and $T_3(n)$ are calculated from equations (4.6) and (4.7).

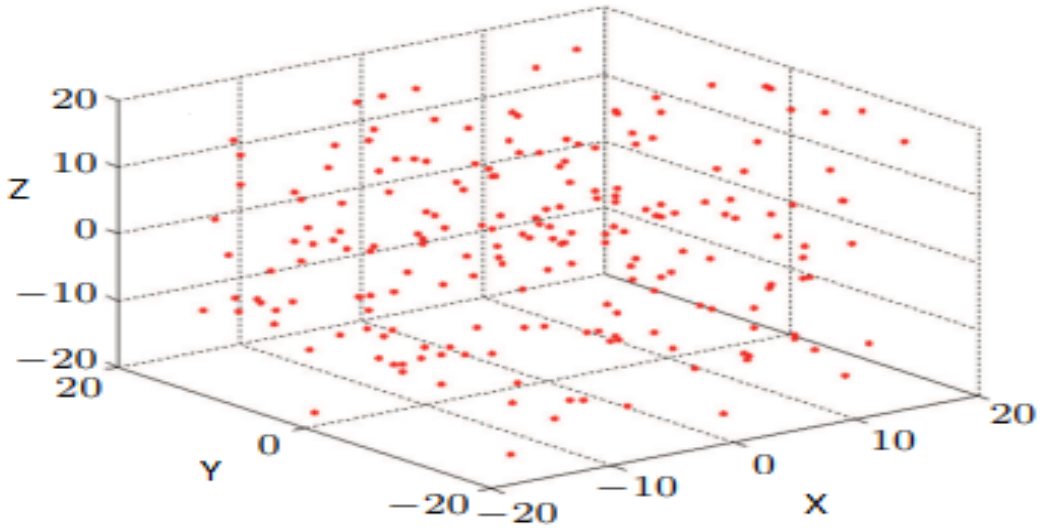


FIGURE 4.2: Brownian motion of particles.

4.3 The Encryption and Decryption Algorithm

We have not made any change in algorithm 3.3.3 because it is an efficent algorithm. There were some deficiencies in the first rendering technique that eliminated using this technique.

We have used Henon Chaotic map instead of Chebyshev map because Chebyshev map is not a coupled map and used Brownian motion instead of Chen Chaotic system. Because the Chen Chaotic system is based on the coupled differential Equations and one has to solve or iterate with RK-4 method. The Chen system with the parameters set in section 2.5.4 is chaotic [56] but it may not be chaotic for some other parameters. However on the other hand Henon chaotic map is coupled map and have only one fix parameter detail is given in section 2.5.2. In [57] one can read, "Chens attractor exists if Lorenz repulsor exist" and most of the literature on the Chen system is redundant because the results obtained can be directly derived from the corresponding results on the Lorenz system.

And also brownian motion has simple algebric equations however solution of these equation are simple. We have eliminated the first 50,000 values in our technique due to Transient effect. Due to which the effect of chaos became prominent. We have described some of the results of this new technique below.

4.4 Results and Discussion

There are several tests we have conducted and results have proved their efficiency as well as accuracy of suggested approach. The images utilised (lena, barberaera, baboon) are gray-scale images from the USC SIPI public media library. The image encryption strategy is implemented on a PC running MATLAB R2017a with the O.S Windows 8.0 64bit, a Core i5-4300M with a 2.60 GHz CPU and 8GB of RAM.

Initial keys are randomly selected as $y_1 = 0$, $z_1 = 0$ (Brownian Motion) and the initial values of Henon chaotic map are $z_1 = 0.12346545678544, y_1$=0.1284345344434, $t = 1.4$ and $u = 0.3$. Figures 4.3, 4.4, 4.5 depict the outcome of our described algorithm's encryption and decryption.

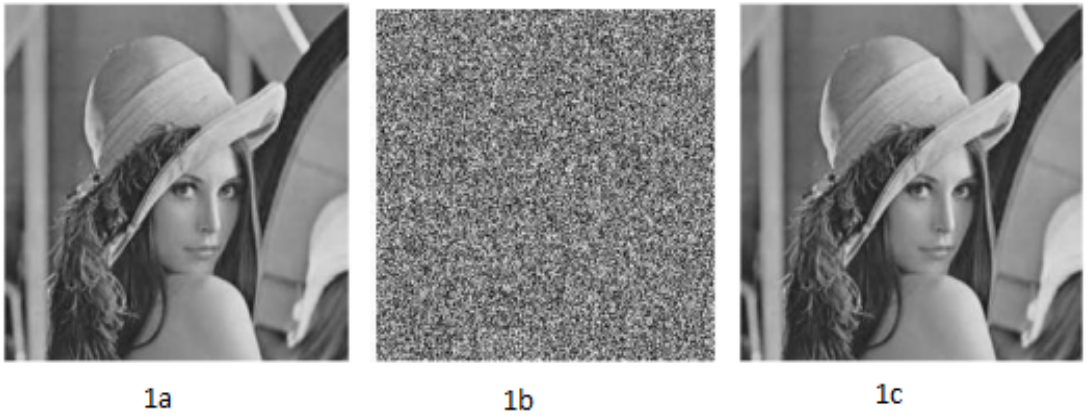


FIGURE 4.3: Experimental results: (1a) Plain image of Lena, (1b) Cipher image of Lena and (1c) Decrypted image of Lena.

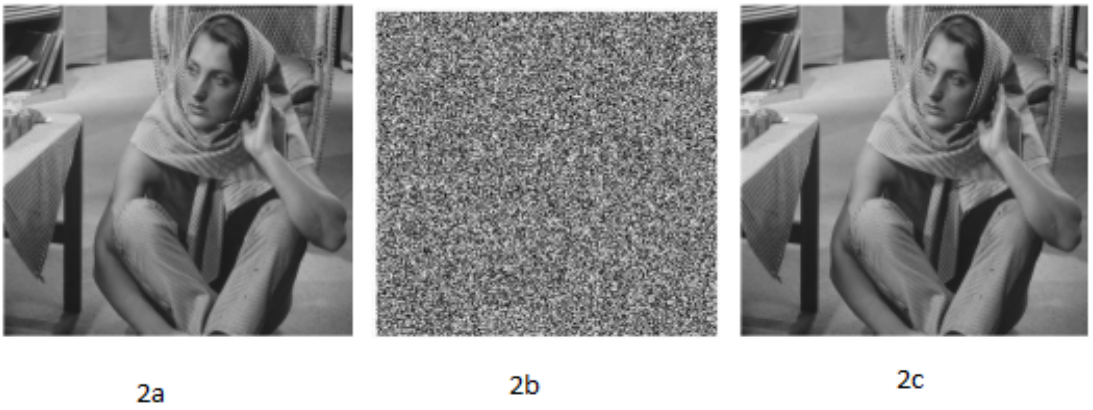


FIGURE 4.4: Experimental results: (2a) Plain image of Barbera, (2b) Cipher image of Barbera and (2c) Decrypted image of Barbera.

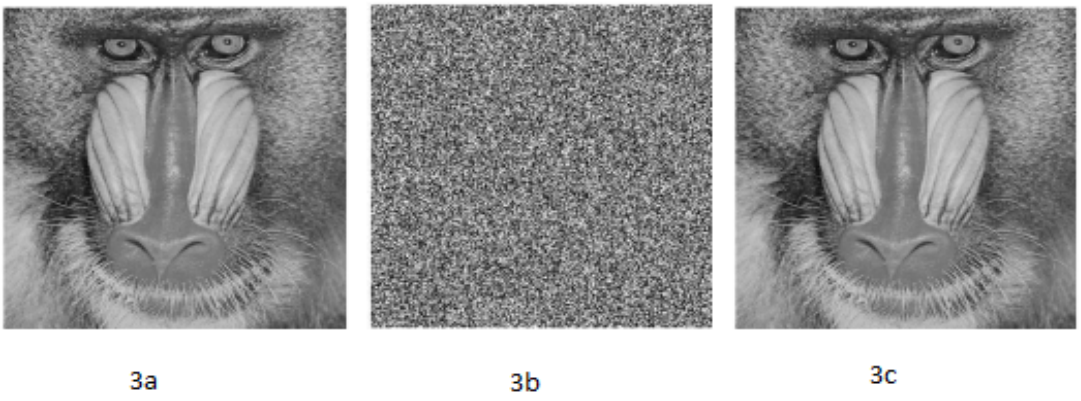


FIGURE 4.5: Experimental results: (3a) Plain image of Baboon, (3b) Cipher image of Baboon and (3c) Decrypted image of Baboon.

4.4.1 Security Analysis

This part examines security assessments such as (keys-space, Sensitivities, and Stats) and their correlations.

1. **Key-Space Analysis**

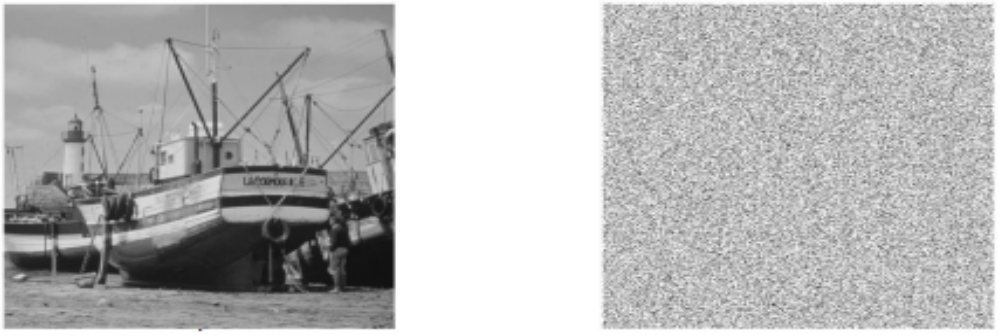
   Minimum key space of 10^{30} is suggested to bothstrong security and resilience to brute-force attacks [48]. The suggested technique makes use of the keys y_1, z_1 (Brownian Motion) and the initial values of Henon chaotic map are z_1, y_1.

   The number of possible key combinations is 10^{56} when the precision is set to 10^{-14}. As a result, the brute force attack is difficult to execute successfully.

2. **Key sensitivity**

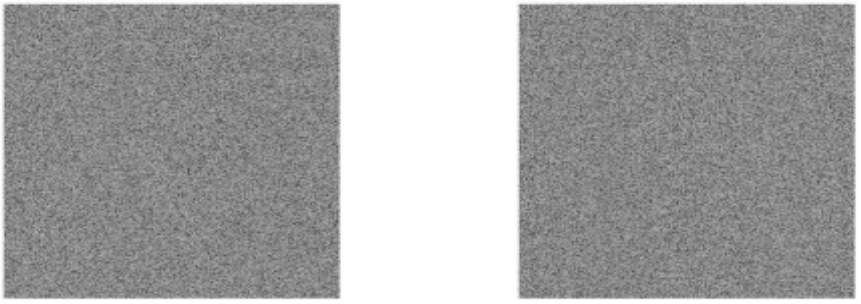
   A decent image encryption technique should be key sensitive in order to avoid unauthorised preliminary assaults. As an example, Figure 4.6(a) displays the plainimage of the boat of size 256 by 256. Figure 4.6(b) depicts the cipherimage of the boat. However, decryption is then done on $y_1^{'}$, $z_1^{'}$ (Brownian Motion) and on the initial values of Henon chaotic map $z_1^{'}, y_1^{'}$.

   Figures 4.7 and 4.8 indicate that if a little modification of 10^{-14} is made in keys, the results are wrong (c - f). This indicates how sensitive the algorithm is to key.



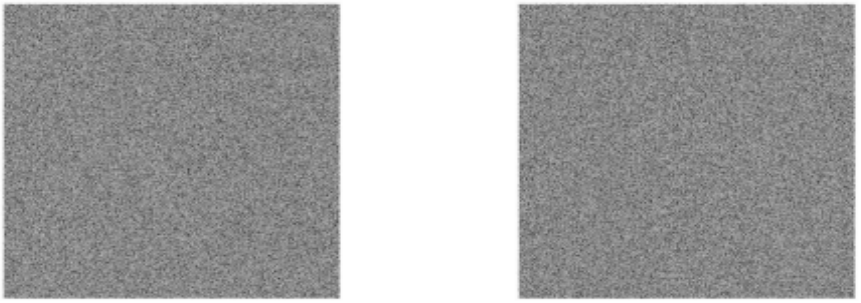
(a) (b)

FIGURE 4.6: Key Sensitivity: (a) Plain image of boat and (b) Cipher image of boat.



(c) (d)

FIGURE 4.7: Incorrect decryption of (b) using first two altered keys .



(e) (f)

FIGURE 4.8: Incorrect decryption of (b) using last two altered keys.

4.4.2 Differential Attacks

Differential cryptanalysis is a broad term for cryptanalysis that mostly applies to block ciphers that operate on binary sequences. Differential cryptanalysis is commonly credited to Biham and Shamir [49].

1. **Nnumber of Pixels Change Rate (NPCR)** .
2. **Unified Average Change Intensity (UACI)**.

The NPCR and UACI both have ranges [0,1]. Table 4.1 displays the numerical findings for UACI and NPCR [51].

TABLE 4.1: Numericals findings of UACI and NPCR.

Image	$Mean_{NPCR}$	$Mean_{UACI}$
$64by64$	99.6094000000	33.4635416667
$128by128$	99.6094000000	33.4635416667
$256by256$	99.6094000000	33.4635416667
$512by512$	99.6094000000	33.4635416667
$1024by1024$	99.6094000000	33.4635416667

The results of testing several images by altering the value of a pixels at random positions are shown in Table 4.2. As a result, even modest changes to the plain image result in a drastically different cipher image. In other words, our technique satisfies the high plaintext sensitivity criteria.

TABLE 4.2: Experimental Results of Different Images.

Image	*Lena*	*Baboon*	*Barbera*
$NPCR$	99.703454	99.453432	99.389328
$UACI$	33.43672	33.5463	33.9934

4.4.3 Statistical Analysis

Data analysis may be used to discover the link between plain image and cipher image. As a result.plain imageis completely different after encryption.

1. **Histogram** A histogram can be used to depict the grey distribution. The histogram of the cipher image should be uniform or nearly uniform, and it should differ from the plain image after encryption to match the requirements of a successful encryption technique. Using new scheme he histogram of cipherimage is uniform and different from the histograms of differents plainimages as shown in the histograms of images so it does not provide any clue to employ any statistical attack on the new encryption procedure.

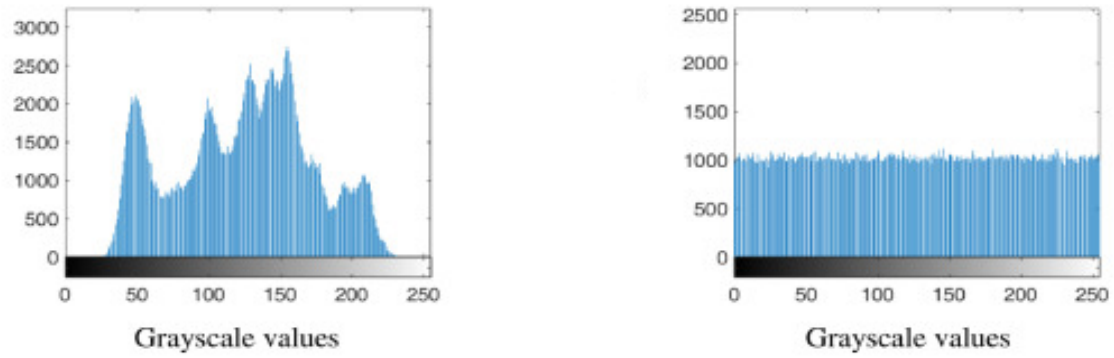


FIGURE 4.9: Histograms of encrypted image (Lena).

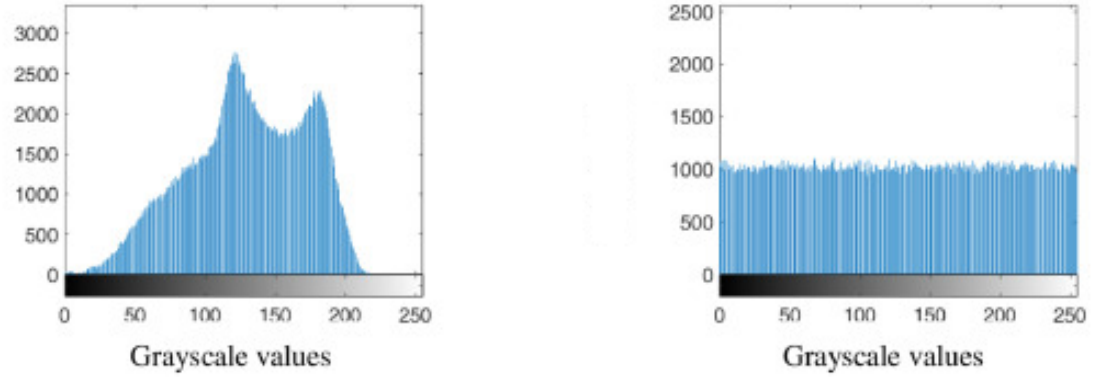


FIGURE 4.10: Histograms of encrypted image (Barbera).

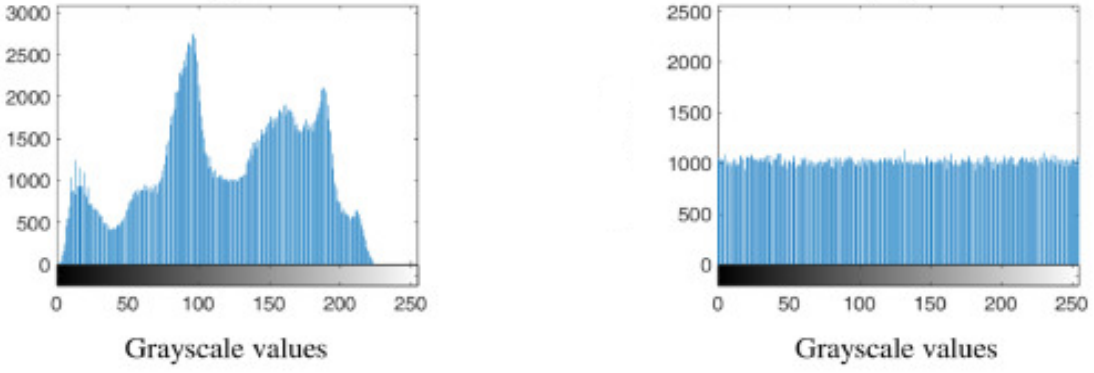


FIGURE 4.11: Histograms of encrypted image (Baboon).

2. **Correlation Coefficient.** The Pearson correlation coefficient (PCC) [53] of two neighboring pixels in a plain image is often high. For a successful coding technique to be employed on a image there must be a weak association between nearby pixels in the corresponding coded image. The test outcomes are listed in Table 4.3. The findings show that the PCC in the cipher image generated by our new approach is near to zero.

TABLE 4.3: Correlation Coffeicent of Cipher Image (lena).

Direction	*Plainimage*	*Cipherimage*
Vertical	0.912564	0.0042987
Horizontel	0.892675	-0.0045398
Diagonal	0.914754	-0.0342898

4.4.4 Information Entropy

The most essential property of randomness is information entropy. The grey scale image Lena has an information entropy of 7.56828525761. The value of Information Entropy is highly sensitive, even when the value of a one or two pixel changes the value of Information entropy changes as well. Table 4.4 displays the Information Entropy results of different images such as lena, Barbera and Baboon. This is because the suggested algorithm's information entropy values are near to the theoretical value of 8. It may withstand information entropy attacks and create an equivalent random message for the cipher-image after employing the approach.

TABLE 4.4: Information Analysis.

Image	*Lena*	*Barbera*	*Baboon*
plainimage	7.23754	7.13486	7.45326
cipherimage	7.91645	7.98345	7.94778

Chapter 5

Conclusion

In this chapter, the concluding remarks regarding the scheme [45] reviewed in Chapter 3 and extended work presented in Chapter 4.

Information security is becoming the focus of attention, how to ensure the security of digital image storage and transmission has become an important topic of information security.

1. A detailed review of the work of M. Xu [28] "A new chaos- based image encryption" is presented in this thesis. The work focuses on an image encryption scheme based on Chen chaotic system and Chebyshev map. The modulation operation is used between diffusion and permutation functions, The scheme is implemented by developing a MATLAB code 3.3.1for the encryption and decryption of algorithm .

2. At the receiver end, the cipherimage is decrypted by using decryption Algorithm 3.3.4 In decryption algorithm, the receiver will use three modules, i.e, inverse diffusion, modulation and permutation using same secret keys and updated keys. As the updated keys is generated with the help of chen chaotic system and cheby shev map of permuted image, to recover plainimage from cipherimage. The implementation is then used to create various cipher images Furthermore, security analysis provides significant results.

3. As the scheme is symmetric so the secret keys are mutually shared through a secure channel. Key is very sensitive element in the encryption scheme, the image

is encrypted using secret keys (x_1, y_1, X_1, Y_1 and Z_1). While in the decryption, if the same key is used only then the original image is obtained. If a very insignificant change of 10^{-14} in any of the key x_1, y_1, X_1, Y_1 and Z_1 is done, then the plainimage cannot be obtained.

4. In chapter 4 we propose a new image encryption scheme based on the Henon chaotic map and Brownian Motion. The extended scheme is also implemented on MATLAB and the security anaylsis is performed of the cipherimage obtained by the updated scheme. Security anaylsis results depict that newly developed scheme is not much different from scheme of Ming. However the running time of the new scheme is less then the original one.

Bibliography

[1] J. F. Dooley, *History of cryptography and cryptanalysis: Codes, Ciphers, and their algorithms*. Springer, 2018.

[2] T. M. Damico, "A brief history of cryptography," *Inquiries Journal*, vol. 1, no. 11, 2009.

[3] J. Andress, "The basics of information security," *(Second Edition), J. Andress, Ed., Second Edition, Boston: Syngress*, pp. 69–88, 2014.

[4] W. O. Mccagg, *A history of Habsburg Jews, 1670-1918*. Indiana University Press, 1992.

[5] A. Sorkin, "Lucifer, a cryptographic algorithm," *Cryptologia*, vol. 8, no. 1, pp. 22–42, 1984.

[6] M. Kumar, A. Aggarwal, and A. Garg, "A review on various digital image encryption techniques and security criteria," *International Journal of Computer Applications*, vol. 96, no. 13, 2014.

[7] M. Kaur, S. Singh, and M. Kaur, "Computational image encryption techniques: a comprehensive review," *Mathematical Problems in Engineering*, vol. 2021, 2021.

[8] M. Kaur and V. Kumar, "Adaptive differential evolution-based lorenz chaotic system for image encryption," *Arabian Journal for Science and Engineering*, vol. 43, no. 12, pp. 8127–8144, 2018.

[9] A. Belazi, A. A. Abd El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Processing*, vol. 128, pp. 155–170, 2016.

[10] M. Kaur and V. Kumar, "Beta chaotic map based image encryption using genetic algorithm," *International Journal of Bifurcation and Chaos*, vol. 28, no. 11, pp. 185–0132, 2018.

[11] M. Kaur, D. Singh, K. Sun, and U. Rawat, "Color image encryption using non-dominated sorting genetic algorithm with local chaotic search based 5d chaotic map," *Future Generation Computer Systems*, vol. 107, pp. 333–350, 2020.

[12] M. Yang, N. Bourbakis, and S. Li, "Data-image-video encryption," *IEEE potentials*, vol. 23, no. 3, pp. 28–34, 2004.

[13] X. Yi, C. H. Tan, C. K. Slew, and M. R. Syed, "Fast encryption for multimedia," *IEEE Transactions on Consumer Electronics*, vol. 47, no. 1, pp. 101–107, 2001.

[14] B. M. Macq and J.-J. Quisquater, "Cryptology for digital tv broadcasting," *Proceedings of the IEEE*, vol. 83, no. 6, pp. 944–957, 1995.

[15] M. G. Avasare and V. V. Kelkar, "Image encryption using chaos theory," in *2015 International Conference on Communication, Information & Computing Technology (ICCICT)*, pp. 1–6, IEEE, 2015.

[16] N. Koblitz, "The uneasy relationship between mathematics and cryptography," *Notices of the AMS*, vol. 54, no. 8, pp. 972–979, 2007.

[17] S. Rana, S. Hossain, H. I. Shoun, and M. A. Kashem, "An effective lightweight cryptographic algorithm to secure resource-constrained devices," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 11, 2018.

[18] D. A. Osvik, J. W. Bos, D. Stefan, and D. Canright, "Fast software aes encryption," in *International Workshop on Fast Software Encryption*, pp. 75–93, Springer, 2010.

[19] D. Coppersmith, D. B. Johnson, and S. M. Matyas, "A proposed mode for triple-des encryption," *IBM Journal of Research and Development*, vol. 40, no. 2, pp. 253–262, 1996.

[20] P. Kloeden and Z. Li, "Li–yorke chaos in higher dimensions: A review," *Journal of Difference Equations and Applications*, vol. 12, no. 3-4, pp. 247–269, 2006.

[21] J. Banks, J. Brooks, G. Cairns, G. Davis, and P. Stacey, "On devaney's definition of chaos," *The American mathematical monthly*, vol. 99, no. 4, pp. 332–334, 1992.

[22] S. Wiggins and J. M. Ottino, "Foundations of chaotic mixing," *Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, vol. 362, no. 1818, pp. 937–970, 2004.

[23] S. Smale, "Finding a horseshoe on the beaches of rio," *The Mathematical Intelligencer*, vol. 20, no. 1, pp. 39–44, 1998.

[24] M. Khan, F. Masood, A. Alghafis, M. Amin, and S. I. Batool Naqvi, "A novel image encryption technique using hybrid method of discrete dynamical chaotic maps and brownian motion," *PLoS One*, vol. 14, no. 12, pp. 225–331, 2019.

[25] Y. Mao, G. Chen, and S. Lian, "A novel fast image encryption scheme based on 3d chaotic baker maps," *International Journal of Bifurcation and chaos*, vol. 14, no. 10, pp. 3613–3624, 2004.

[26] S. Agarwal, "A review of image scrambling technique using chaotic maps," *International Journal of Engineering and Technology Innovation*, vol. 8, no. 2, p. 77, 2018.

[27] S. Shaukat, A. Arshid, A. Eleyan, S. A. Shah, J. Ahmad, *et al.*, "Chaos theory and its application: An essential framework for image encryption," *Chaos Theory and Applications*, vol. 2, no. 1, pp. 17–22, 2020.

[28] M. Xu, "A new chaos-based image encryption algorithm," *Int. Arab J. Inf. Technol.*, vol. 15, no. 3, pp. 493–498, 2018.

[29] B. Purnama and A. H. Rohayani, "A new modified caesar cipher cryptography method with legibleciphertext from a message to be encrypted," *Procedia Computer Science*, vol. 59, pp. 195–204, 2015.

[30] U. Somani, K. Lakhani, and M. Mundra, "Implementing digital signature with rsa encryption algorithm to enhance the data security of cloud in cloud computing," in *2010 First International Conference On Parallel, Distributed and Grid Computing (PDGC 2010)*, pp. 211–216, IEEE, 2010.

[31] S. Basu, "International data encryption algorithm (idea)–a typical illustration," *Journal of global research in Computer Science*, vol. 2, no. 7, pp. 116–118, 2011.

[32] R. Bhanot and R. Hans, "A review and comparative analysis of various encryption algorithms," *International Journal of Security and Its Applications*, vol. 9, no. 4, pp. 289–306, 2015.

[33] S. Kumar and D. P. Tyagi, "Comparitive analysis of crtptographic hash function for advancementof network security,"

[34] A. Biryukov, A. Shamir, and D. Wagner, "Real time cryptanalysis of a5/1 on a pc," in *International Workshop on Fast Software Encryption*, pp. 1–18, Springer, 2000.

[35] J. H. Poincaré, "Chaos and the solar system,"

[36] P. Murphy, "Chaos theory as a model for managing issues and crises," *Public relations review*, vol. 22, no. 2, pp. 95–113, 1996.

[37] Y. Wu, J. P. Noonan, G. Yang, and H. Jin, "Image encryption using the two-dimensional logistic chaotic map," *Journal of Electronic Imaging*, vol. 21, no. 1, pp. 013–014, 2012.

[38] M. J. Feigenbaum, "The transition to aperiodic behavior in turbulent systems," *Communications in mathematical physics*, vol. 77, no. 1, pp. 65–86, 1980.

[39] F. Dachselt and W. Schwarz, "Chaos and cryptography," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 48, no. 12, pp. 1498–1509, 2001.

[40] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," *Chaos, Solitons & Fractals*, vol. 35, no. 2, pp. 408–419, 2008.

[41] T. S. Parker and L. O. Chua, "Chaos: A tutorial for engineers," *Proceedings of the IEEE*, vol. 75, no. 8, pp. 982–1008, 1987.

[42] O. Al-Hazaimeh, N. Alhindawi, S. M. Hayajneh, and A. Almomani, "Hanon chaotic map-based new digital image encryption algorithm," *Magnt Research Report*, vol. 2, pp. 261–266, 2014.

[43] A. Lyapunov, "General problem of stability of motion, harkov math," *Soc, published in Collected Papers*, vol. 2, pp. 5–163, 1892.

[44] Q. Wang, "Can a butterfly in brazil control the climate of texas?," in *APS Division of Fluid Dynamics Meeting Abstracts*, pp. K07–003, 2020.

[45] X. Tong and M. Cui, "Image encryption with compound chaotic sequence cipher shifting dynamically," *Image and Vision Computing*, vol. 26, no. 6, pp. 843–850, 2008.

[46] C. Li, S. Li, G. Chen, and W. A. Halang, "Cryptanalysis of an image encryption scheme based on a compound chaotic sequence," *Image and Vision Computing*, vol. 27, no. 8, pp. 1035–1039, 2009.

[47] X. Huang, L. Liu, X. Li, M. Yu, and Z. Wu, "A new pseudorandom bit generator based on mixing three-dimensional chen chaotic system with a chaotic tactics," *Complexity*, vol. 2019, 2019.

[48] 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.

[49] E. Biham and A. Shamir, "Differential cryptanalysis of des-like cryptosystems," *Journal of cryptology*, vol. 4, no. 1, pp. 3–72, 1991.

[50] D. E. Standard *et al.*, "Data encryption standard," *Federal Information Processing Standards Publication*, vol. 112, 1999.

[51] 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.

[52] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3d chaotic cat maps," *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749–761, 2004.

[53] K. Pearson, "Notes on the history of correlation," *Biometrika*, vol. 13, no. 1, pp. 25–45, 1920.

[54] X. Wang and D. Xu, "A novel image encryption scheme based on brownian motion and pwlcm chaotic system," *Nonlinear dynamics*, vol. 75, no. 1, pp. 345–353, 2014.

[55] X.-L. Chai, Z.-H. Gan, K. Yuan, Y. Lu, and Y.-R. Chen, "An image encryption scheme based on three-dimensional brownian motion and chaotic system," *Chinese Physics B*, vol. 26, no. 2, pp. 020–504, 2017.

[56] G. A. Leonov and N. V. Kuznetsov, "On differences and similarities in the analysis of lorenz, chen, and lu systems," *Applied Mathematics and Computation*, vol. 256, pp. 334–343, 2015.

[57] A. Algaba, F. Fernández-Sánchez, M. Merino, and A. J. Rodríguez-Luis, "Chen's attractor exists if lorenz repulsor exists: The chen system is a special case of the lorenz system," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 23, pp. 033–108, 2013.