CAPITAL UNIVERSITY OF SCIENCE AND TECHNOLOGY, ISLAMABAD

Review of a Medical Image Encryption Scheme using Brownian Motion and Chaotic Mapping

by

Hassan Raza

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

in the

Faculty of Computing
Department of Mathematics

2022

Copyright © 2022 by Hassan Raza

All rights reserved. No part of this thesis may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, by any information storage and retrieval system without the prior written permission of the author.

Dedicated to

My Parents

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

CERTIFICATE OF APPROVAL

Review of a Medical Image Encryption Scheme using Brownian Motion and Chaotic Mapping

by

Hassan Raza

(MMT193015)

THESIS EXAMINING COMMITTEE

S. No.	Examiner	Name	Organization
(a)	External Examiner	Dr. Atta ullah	NUTECH, Islamabad
(b)	Internal Examiner	Dr. Dur-e-Shehwar Sagheer	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, **Hassan Raza** hereby state that my MS thesis titled "**Review of a Medical Image Encryption Scheme using Brownian Motion and Chaotic Mapping**" 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 MS Degree.

(Hassan Raza)

Registration No: MMT193015

Plagiarism Undertaking

I solemnly declare that research work presented in this thesis titled "**Review of a Medical Image Encryption Scheme using Brownian Motion and Chaotic Mapping**" 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 MS 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.

(Hassan Raza)
Registration No: MMT193015

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 very thankful to the Head of Department **Dr.Muhammad Sagheer** for the kind permission to avail this opportunity.

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 of supervisor.

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 my life.

I would like to thank all of my friends for motivating me during my degree program. Mostly, I would like to thank **Tahir Sajad Ali**, **Khuzaima Nasir** and **Asad ur Rehman** also helped me a lot and guided me whenever I needed it.

(Hassan Raza)

Abstract

In the present thesis, the article a lightweight chaos based medical image encryption scheme using random shuffling and XOR operation by Masood et al. is reviewed. The implementation of proposed scheme is done on MATLAB. The scheme includes random shuffling, modulation and XOR operations. The initial keys used in the permutation and diffusion steps interact with each other. Proposed scheme is developed by the combination of Brownian Motion (BM) and Chen's Chaotic system (CCS). It achieved the required protection in data of hospitals and medical healthcare units. The confusion is achieved through Henon Chaotic Map, although diffusion is obtained using XOR operation of Brownian motion and Chen's Chaotic System. The experimental results show that the proposed cryptosystem is a lightweight approach that can achieve the desired security level.

Contents

List of Figures

List of Tables

Abbreviations

AES	Advanced Encryption Standard
BM	Brownian Motion
CCS	Chen's Chaotic System
DES	Data Encryption Standard
DICOM	Digital Image Communication in Medicine
HIPAA	Health Insurance Portability and Accountability Act
IDEA	International Data Encryption Algorithm
ISO	International Standard Organization
IBM	International Business Machines
JPEG	Joint Photographic Experts Group
MRI	Magnetic Resonance Imaging
NPCR	Number of Pixel Changing Rate
PCC	Pearson Correlation Coefficient
PNG	Portable Network Graphic
PGP	Pretty Good Privacy
RSA	Rivest - Shamir - Adleman
TIFF	Tagged Image File Format
UACI	Unified Averaged Changed Intensity

Symbols

C	Cipherimage
D	Decryption Algorithm
E	Encryption Algorithm
h	Control parameter of henon chaotic map
K	Key
P	Plaintext
t	Step length
t_p	Specified time duration
λ	Lyapunove exponent
δ_{st}	Pearson correlation coefficient
θ	Control parameter of Brownian motion
ϕ	Control parameter of Brownian motion

Chapter 1

Introduction

Right from the beginning of the mankind, the problem which is faced by the states as well as individual is that how to secure their secret information. For the solution of this problem intellectuals gave suggestions and developed a system that protects the transmission of necessary confidential information. In the modern age, many techniques and methods are utilized for cryptography to protect the secret data or messages. These methods are used to protect sensitive information during its transmission and only the beneficiary may access, modify or utilize them. In cryptography, the original communication is referred as plaintext P, and the codded message is referred as ciphertext C. The algorithm that transforms original text into codded text with the help of keys is called encryption algorithm E. The procedure used to transform the codded message into original message with the help of secret keys is called the decryption algorithm D. Cryptography is split into two branches, one is symmetric key cryptography (also known as secret key cryptography) and other is asymmetric key cryptography based on (public key cryptography). In symmetric key cryptography, only a secret key is used for both encryption and decryption. Asymmetric key cryptography is a method of encrypting and decrypting data by using two separate keys, first is public key and the second is known as secret key.

1.1 Image Encryption

Image is an artwork of visualization for example a photo or any 2D projection. It is expressed the intensity of light at all the locations. An image has two types one is

Analog image and other is Digital image. The analog image shows a constant set of parameters that denotes the position and amount of light (i.e CRT system screen image). Digital image is made by image elements called pixels. Pixel value seems to be represented by the lightness of a fixed location. It is used in everyday life, such as satellites TV and neuroimaging, and in academics, like astrophysics and geographic systems. There are two types of system to secure the information, one is hiding the data and other is encryption of data. For hiding data two methods are used steganography [1] and watermarking [2]. Steganography is the concealing of information, it attempts to hide the presence of information while transfering. While in cryptographic effect, the encrypted private information is shared to the public, but the contents are hidden from public view. Moreover, watermarking depends on the original information being embedded with a unique identifying watermark. At the receiver ends, the watermarked signature is taken out. The purpose is to avoid the unauthorized use of copyrighted or proprietary materials. Furthermore, the idea behind encrypting data is to change original data into an unreadable format before transmitting.

1.2 Image Encryption in Medical Science

Telemedicine is a rapidly expanding phenomenon that involves giving help to patient who are not available at same place as health-care provider. Secret data of patients like; medical scans, is transmitted via Web or cellular communication channels. The telemedicine method was created for approximately 40 years around the world [3]. Now it is researched in china because they are in problem due to legislation demanding encoded image information. The work presented in this thesis proposed a modern technique that protects concealment of medical images. Digital image communication in medicine (DICOM) [4] is introduced for medical image encryption and it is acknowledged by ISO (International Standard Organization). Many methodologies are used for medical analysis, which relies on signal processing to show the inner aspect of living bodies. Furthermore, nowadays medical procedures are predominantly protected by artificial intelligence. To protect medical photographs containing delicate information about patients, a comprehensive system with genuine protection measures is generally required. In reality, just like typical cloud platforms, e-health systems are subjected to many sorts of violations/attack; as a result, keeping medical photos in their original form is comparably easy to access by simply compromising the system's security standards.

Moreover, in 2015, millions of people were affected by health data breaches in the US [5]. A lot of medical images and records have been consistently created and disseminated online among medical specialists and healthcare workers due to the appearance of COVID-19.

Another case in 2019, IBM reported that the health industry had recorded maximum cases of data breaches and that data can be misused in several ways. The high court of Bombay refused to give bail to a man who was out on temporary bail for about 10 months based on forged medical documents in 2021 [6]. Because of this, there is significant problem for different researcher societies to analyze the facts of their unauthorized use. The electronic medical record is valuable in a variety of aspects. Even though the Health Insurance Portability and Accountability Act (HIPAA) [7] established secret regulations for medical records, securing these records remain a difficulty.

Encryption method is necessary for the security of health images in hospitals/healthcare departments. By converting an actual image into a cipher image, we can ensure that only authorized users may access the data with the help of an encryption method. A technique in which a picture is encoded with different encryption schemes is called Image Encryption.

In medical science tests are performed to detect abnormal signs like CT scans and magnetic resonance imaging. Patients confront many difficulties while safe transmission of their test reports. Nowadays it is very easy way to send or receive an image due to advance technologies and the creation of cryptographic algorithms.

Cryptology is an essential element in developing a safe sharing technique for the transfer of images. So we have various techniques for image encryption due to its need and importance. Images are opposite from text in their properties like high correlation analysis and massive information stroage. Therefore sometimes, the famous techniques like AES [8] and international data encryption algorithm IDEA [9] are not suitable.

1.3 Literature Review

A safe cryptographic technique can get through many procedures like permutations and substitutions as show in Figure 1.1.

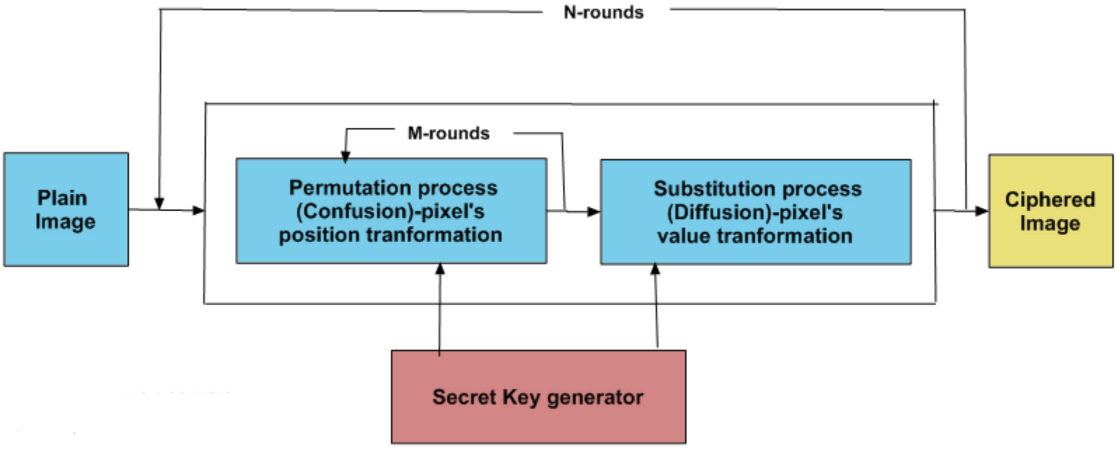

N-rounds
M-rounds
Plain Image
Permutation process (Confusion)-pixel's position tranformation
Substitution process (Diffusion)-pixel's value tranformation
Ciphered Image
Secret Key generator

FIGURE 1.1: Pixel's Confusion and diffusionn process

In 1998, Friedrich [10] suggested an image encryption scheme which depends on permutation and diffusion. He used permutation algorithm to the plainimage for pixel shuffling. Hence a permuted image is obtained which cannot be readable. The statistical features of a plainimage would not be altered during this process. Encrypted image decoded by using inverse permutation algorithm. In Fridrich's scheme, diffusion process is modified for gray levels by using random sequence. The basic goal is to produce the avalanche effect, which states that a small change in single bit of plainimage will significantly change in cipherimage.

Tiegang and Chen [11] presented a novel image encryption algorithm based on "hyper chaos". In this method position of pixel is shuffled via shuffling matrix and logistic map is used for permutation process. Then with the help of hyperchaotic system, it modifies its pixels values without loss of generality. This scheme gives high security because it has high key space, which is sufficient to defend the brute force attacks.

Pareek [12] presented image encryption scheme, in which two chaotic logistic maps and 80-bits long secret key is used. Initial keys are obtained using secret keys and is changed significantly for the encryption of each block cipher which consists of sixteen pixels. This alteration gives strong protection against any attacks. This scheme is very helpful for real time encryption scheme.

The study of chaotic dynamics made remarkable advancements in 1960 and 1970. The renowned KAM theorem was proposed by Kolmogorov, Arnold and Moser in 1960 [13]. KAM theorem, which served as the foundation for dynamic systems/chaos theory, is based on the investigation of motion stability in the integrable Hamiltonian system. Next for the simulation of climate changes, Lorenz [14] suggested a three-dimensional autonomous system. This was the well-known Lorenz system, which was the first chaos model to be described mathematically. Lorenz concluded that initial conditions had a significant impact on how the weather/climate developed.

A chaotic system is very sensitive to its initial conditions, which means that even a little variation in initial conditions will significantly affect the output. He also relates it with butterfly effect. The conceptual characteristics of chaotic system have a subject of many researchers [15]. Today, chaos theory is significant in many other domains, including mathematics, physics [16], economics [17], and biology, in addition to fields like meteorology [18] and turbulence.

Chaos theory typically serves as a foundation for security awareness when put to the test against well-known cryptanalysis methods. The chaotic theory is famous in cryptography because it has unpredictable and random behavior. It is very sensitive in its nature. It serves as a foundation for internet security when it is tested by cryptographic methods. Researchers have used dynamic chaotic systems to create new cryptographic primitives by utilizing chaotic maps such as logistic maps [19], Henon maps [20], Chen Chaotic System [21] and Tent maps [22]. There are some methods of image encryption such as chaos system [23, 24], Arnold transform [25] and Brownian motion [26]. Brownian motion can be generated using Carlo's experiment [27]. In this technique, Monte Carlo method (also called Monte Carlo's experiment) is one kind of computational process that produces numerical solutions by repeating random values. For each given course of action, Monte Carlo's simulation provides the decision-maker with a range of probable outcomes as well as the probabilities that they will occur.

Chaos based image encryption scheme is insecure under some attacks. For example, Wang and Xu [27], used the Monte Carlo technique to secure the original test image in 2014 by using one molecule from this theory as a pixel. Zhu [28] attacked Wang et al's method in 2015 because their system was dependent on permutations and diffusing sequences that were irrelevant to unencrypted images. Chosen plaintext attack is applied on encryption algorithm to get a diffusion sequence and permutation vector.

To address the aforementioned issues and to enhance the protection level, an image encryption scheme [3] is presented. Process of encryption and decryption is carried out with the help of shared keys. Henon chaotic map is used for random shuffling and permutaion process. With the help of Brownian motion and Chen chaotic system diffusion process is executed. Modulus and XOR operation is used between them. As a result this scheme gives a secure way of communication.

1.4 Thesis Contribution

In this thesis, an encryption scheme presented by Masood et al. in [3] is reviewed. Initial keys are used to iterate chaotic map. In this scheme, two chaotic maps are used, including Henon chaotic map (Section 2.5.3), Chen chaotic system (Section 2.5.4) and a technique Brownian motion (Section 3.2.1) is also included. "A Lightweight Chaos Based Medical Image Encryption Scheme Using Random Shuff-ling and XOR Operations" [3] is discussed. Firstly, Image is divided into equal number of blocks then for pixel shuffling and block shuffling a circular permutation is applied on these block images. Combining all blocks to get a new permuted image. A new technique Brownian motion is itreated to enhance the randomness in this system. Then, the modulation, absolute and round operation are applied. Multiply results with permuted Image and get a new permuted image. In the end, diffusion is applied through Chen chaotic system and takes bitwise XOR with permuted Image. As a result, the encrypted image is obtained. As the image encryption algorithm is symmetric in nature, so the decryption process is in reverse order. After applying decryption algorithm the original grayscale image is achieved. The scheme is successfully implemented on the MATLAB through initial keys and parameters to encrypt and decrypt the grayscale image, the security analysis of the scheme such as entropy analysis, histogram analysis, pixels correlation analysis (Homogeneity, Energy and contract Analysis) are determined. Differential attack analysis such as NPCR and UACI are also determined.

1.5 Thesis Layout

In this thesis, a review of chaotic image encryption scheme [3] for gray scale image is discussed. Following is a summary of the dissertation's major contributions as mentioned in the chapters:

- **Chapter 2** shows the fundamental introduction to the cryptology in which fundamental concepts of the cryptography, some properties of cryptography are presented. Then, detail on cryptosystem, its all kinds and security services of cryptography are discribed. Cryptanalysis of image encryption are discussed. Then, some basic terminolgy related to image encryption i.e. digital image and pixel etc are discussed. After that chaos theory and chaotic map such as Henon chaotic map are discussed.
- **Chapter 3** the review of article "A Lightweight ChaosBased Medical Image Encryption Scheme Using Random Shuffling and XOR Operations" [3] is presented. For that purpose, Chen chaotic System and Brownian motion is

discussed in detail. Encryption/Decryption process and its implementation is presented.

- In **Chapter 4** the security analysis of the scheme is discussed in detail.
- **Chapter 5** presented the conclusion of above work and some directions for future work are also given.

Chapter 2

Preliminaries

The role of cryptography is important in the digital world for providing services such as encryption, digital signature and key establishment etc. In this chapter, the introduction of cryptography is given in Section 2.1 , which includes somexz vspace0.1cm fundamental concepts of cryptography, properties of cryptography, cryptosystem and its types. Cryptanalysis and some common cryptographic attacks are discussed in Section 2.2 . In Section 2.3 terminologies related to image encryption are discussed. The complete description of chaos theory is presented in Section 2.4. Section 2.5 discusses the introduction of chaotic map such as Henon chaotic map. Finally, chaos and cryptography is discussed in Section 2.6.

2.1 Cryptography

Cryptography is the study of secret communication method that allows sender and recipient to read the data and access its information. Cryptography is the science of concealing information in order to introduce secrecy in data. The term “cryptography” is the combination of two Greek words i.e “Krypto and graphene” which means “hidden and writing” respectively [29]. A word ‘plain-text’ in cryptography refers to a hidden message that the sender wishes to send.

Plaintext cannot be delivered in its original form instead, it is changed into ciphertext before being sent to the target recipient. Ciphertext is a coded message that cannot be understood by the intended recipient.

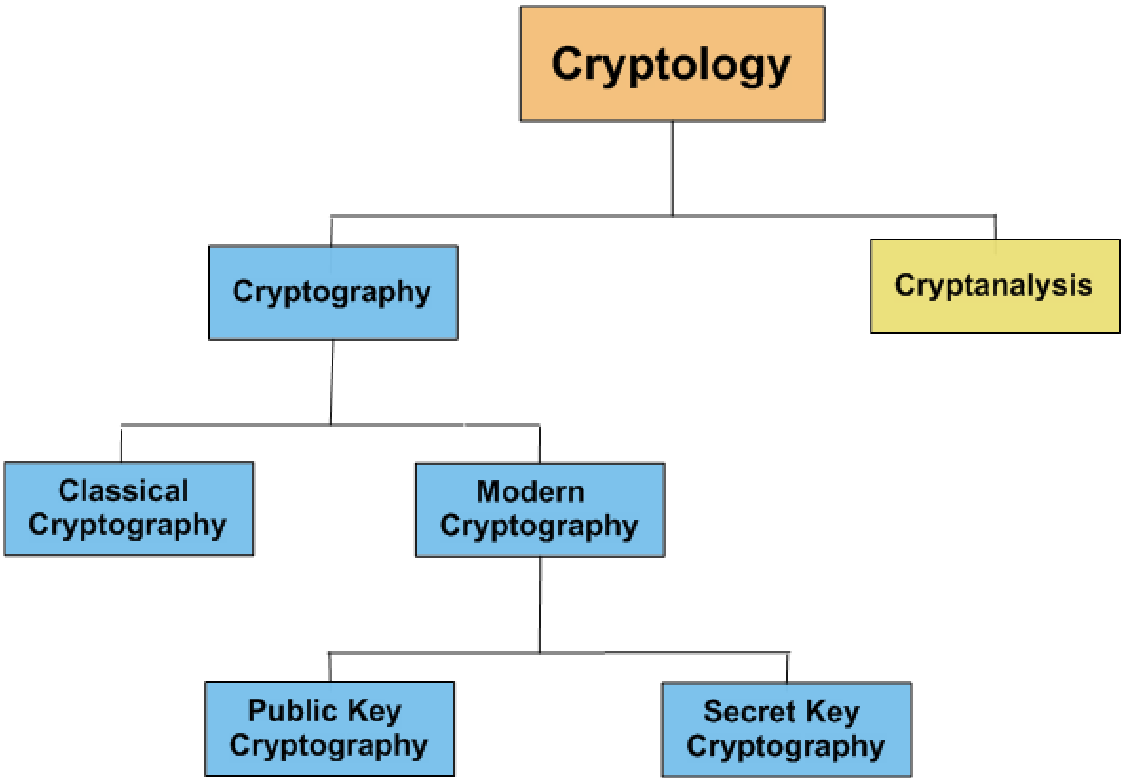


Figure 2.1: Structure diagram of cryptology

Cryptography uses encryption technique, that is the process of transforming plaintext into ciphertext and then another method that retrieves back data to its original form which is called decryption. Cryptography has two main branches. One is Symmetric key cryptography and other is Asymmetric key cryptography . Symmetric key cryptography is a type of encryption/decryption that uses a single confidential key to cipher and decipher message. Asymmetric key cryptography is a type of encryption/decryption that uses two different keys, one for encryption purpose and the other is for decryption. In encryption we convert plaintext to ciphertext, whereas In decryption turning ciphertext back to plaintext. 'Encrption algorithm' is a method for converting plaintext to ciphertext using a secret key. 'Decryption algorithm' is the algorithm that uses a secret key to retrieve the plaintext from the ciphertext. It is possible to convert plaintext to ciphertext and vice versa [30].

2.1.1 Cryptosystem

The term “cryptosystem” refers to a system that transforms plaintext into ciphertext. This conversion depends on the encryption and decryption process, which is simplified by the use of different techniques. This process has a history of 4000 years. The first known use of cryptography is writing dates and it goes back to around 1900 B.C [31]. Continuous progress of cryptography has supplied us with secure communication, money transactions, emails and many other internet services. It protects the private data of the users and at times hides the users’s data from a third party. A cryptosystem is a program that implements cryptographic algorithms. It consists of two algorithms: one for encrypting data and the other for decrypting it .

Components of Cryptosystem

Cryptosystem is represented by five tuples (P, C, K, E, D) which are listed below:

1. P is the set of plaintext data.
2. C is the set of ciphertext data.
3. K is the key space.
4. E is the set of encryption algorithms
5. D is the set of decryption algorithms

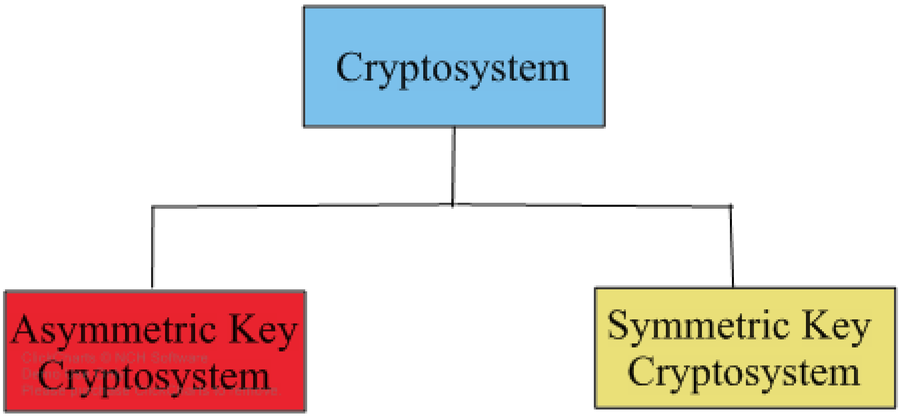
The encryption algorithm E corresponding to key k is denoted by E_k and decryption algorithm D corresponding to the key k is denoted by D_k.
Therefore

$$D_k(E_k(p)) = p \tag{2.1}$$

for all plaintext data p

Kinds of Cryptosystem

Secret key for encryption and decryption depends on type of cryptosystem and it may be the same or diferent. Usually cryptosystem has two kinds:



ClickCharts © NCH Software
Please purchase ClickCharts to remove.

Figure 2.2: Kinds of cryptosystem

1. Symmetric key (Secret key)
2. Asymmetric key (public key)

2.1.2 Symmetric Key Cryptography

When a secret key is used for both encryption and decryption, it is referred to as symmetric key cryptography or symmetric encryption. Figure 2.3 shows exact definition of symmetric key cryptography. It is also known as secret key cryptography. In this type of cryptosystem data is changed to a format that cannot be read or inspected by anyone who doesnot have the same secret key that is used to encrypt it earlier [32].

For understanding consider two parties those communicate with each other: Say, Ali and Haider. Ali wants to communicate with Haider via Internet. He uses a secret key that must be shared with Haider in encryption process.

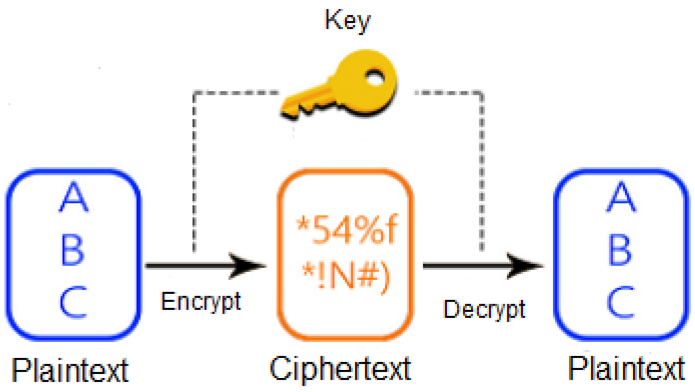


Figure 2.3: symmetric key cryptosystem

For this purpose, he sends the encrypted text to Haider via Internet and shares the key with him via a secure channel. Haider can simply decrypt the text using the decryption technique once he has both the text and the key. A secure route is required to send the key to the selected receiver. Otherwise, security will be impossible to achieve. Key management and the usage of the same key by the sender and receiver are the two fundamental concerns with symmetric key cryptosystems. AES [8] , DES [33] and 3DES [34] are examples of symmetric key. There are two main disadvantages of symmetric key which are as follows:

(a) **Key Sharing**

when 'n' people communicate with each other and if one person leaks the key then whole conversation's privacy will be distroyed. It is the main problem with this type of cryptosystem.

(b) **Authentication**

Authentication is another main problem in symmetric key cryptography. If Ali and Haider communicate and the middle man guesses the key and starts communication, the cryptosystem is unable to identify whether or not he is an authorized user.

2.1.3 Asymmetric Key Cryptography

Asymmetric key cryptography is a type of encryption (decryption) that uses two different keys, one for encryption purpose and other is for decryption. In 1976, Diffie-Hellman [35] presented an asymmetric key cryptosystem to address issues with symmetric key cryptosystems. The development of the asymmetric key cryptosystem is the most significant breakthrough in cryptographic history. Asymmetric key cryptography is also known as public key cryptosystem. Public key and private key is used for encryption and decryption algorithm. The public key is for public, who wants to send a message to sender and private key that keeps secret, is known to the sender only. A data which is encrypted by public key, can be decrypted by private key. Security of public key is not necessary because it is available publically. For information transmission, asymmetric encryption is thought to be the best option.

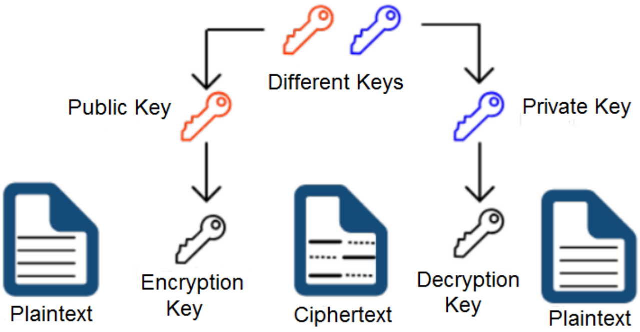


Figure 2.4: Asymmetric key cryptosystem

Figure 2.4 shows a pattern of asymmetric keys. Usually, two keys are used for asymmetric key cryptography. one is for encryption and the other is used for decryption. Key which is used for encryption process remains publicly accessible while decryption key remains secret. This key is not sent to authorized receiver through a secure medium. It means that if anyone have secret key, he can decrypt the message, therefore two keys are used to boost up the protection level. The public key is reachable for anyone who wants to communicate. Although decryption key is only known to authoriz receiver and he can retrieve the original text. So asymmetric key cryptosystem resolves the issues of symmetric key. RSA [36], which is used for encryption and authentication, Pretty Good Privacy (PGP) [37], that is used to protect emails and ElGamal [38] have capability to make the key predictions extremely tough, are examples of this system. When security is more important than speed, asymmetric encryption is utilized.

Some applications for asymmetric encryption are:

- **Digital signature** It is used to verify the identity of sender and receiver.
- **Asymmetric key infrastructure** authorized encryption keys through the issue of digital certificates. It is not necessary to share the decryption key over a secure channel. The owner of the private key assures that he has full authority to decrypt the text, which improves the security.

2.1.4 Security Services of Cryptography

There are five basic information security features of cryptography that are;

1. Confidentiality
2. Integrity
3. Authentication
4. Non-Repudiation
5. Access Control Authentication

1. **Confidentiality** It is a guarantee that any message is not made available or revealed to unauthorized person or organization during its transmission. The original data is known to sender or receiver only. No one can understand the transmitted data except authorized person. Security mechanism of cofidentiality is shown in Figure 2.5. There are some confidentiality services listed below:
   - Connection confidentiality, ensures that all users are protected in connections.

- Connectionless confidentiality, All users in a standard connectionless session are protected by connectionless confidentiality.
- Selective field confidentiality, For p users on q connections or a unique connectionless session, it protects chosen fields.
- Traffic-flow confidentiality, It protects information against wiretapping by inactive wiretap or eavesdropping by wiretappers.

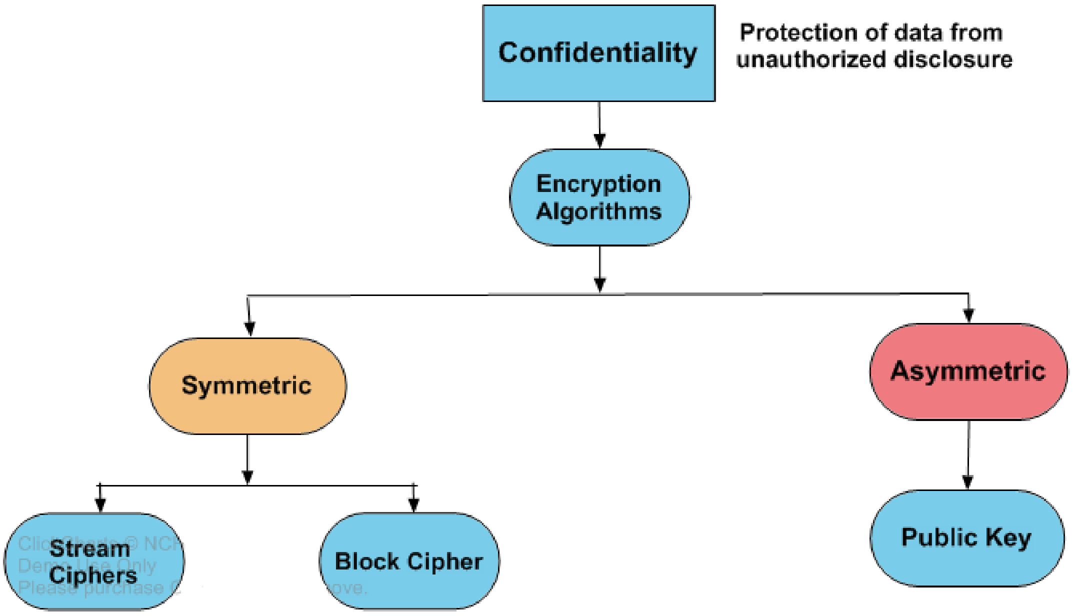


Figure 2.5: Confidentailty and its security mechanism

2. **Integrity** Data integrity refers to the assurance that message is not altered, modified or deleted in transit by accident or on purpose. Message Authentication Codes (MACs) [39] are the techniques that use a secret key to perform integrity checks. These are typically used between two involved individuals who share a private key to verify data transmitted between them. For example, if Ali sends encrypted message to Haider, integrity ensures that the message is not modified or changed during transmission or not altered during its communication and it convinces Haider to believe that the message is still in its original form. The MAC function is a one-way hash function that is key-dependent. A frequent way for generating a MAC algorithm is to use a block cypher in conjunction with the Cipher Block Chaining (CBC) [40] operating mode. Figure 2.6 shows the security mechanism of integrity.

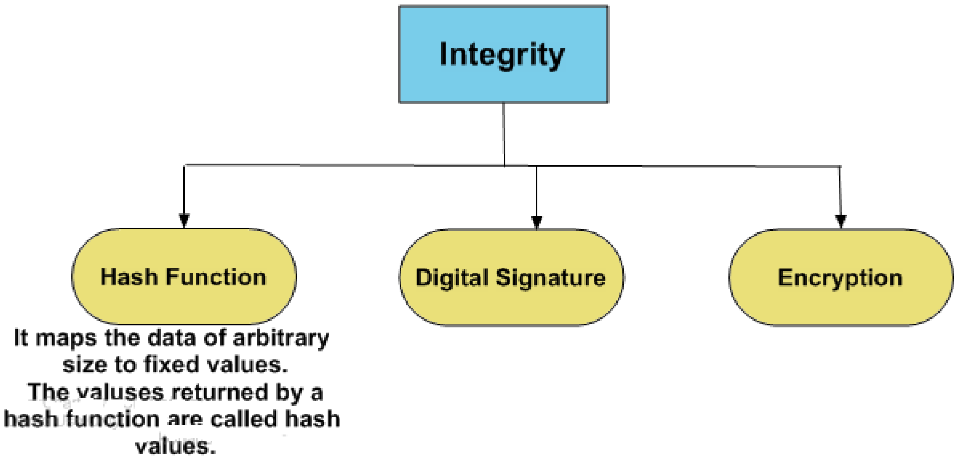

Integrity
Hash Function
Digital Signature
Encryption
It maps the data of arbitrary size to fixed values.
The valuses returned by a hash function are called hash values.

FIGURE 2.6: integrity and its security mechanism

3. **Authentication** A cryptosystem also includes authentication. It ensures that the domain of data or electronic message is truely identified, with the belief that the identity is not wrong. It permits for the verification of the sender's or recipient's identity. It assures that the information is obtained from a trustworthy source. It correctly identifies the message's source as well as the transmitter and receiver. Finally, it guarantees that the sender and receiver are both verified. Consider the scenario in which Ali and Haider adopt a secure technique to communicate. To avoid being scammed, they must be able to use an encryption algorithm to authenticate each other's identities. Participants can use the authentication attribute to make sure they are speaking with each other rather than with the attacker.

4. **Non-Repudiation** It means that neither sender nor the receiver of a data be able to refuse the transmission. If Haider sends the message, there is no way for him to refuse it later. This supports the receiver in gaining the sender's confidence in any cryptographic procedure. The non-repudiation have two forms:

   (a) **Nonrepudiation with proof of origin:** A proof of the information's origin is given to the information's receiver. This proof will shield the receiver from the sender's attempts to wrongly refuse sending the material or its original content. The author can not deny that message is sent by him or material of message is in its original form.

(b) **Nonrepudiation with proof of delivery:** It assures that the data sent has proof that it is delivered and receiver has verification that data is sent by authorized sender, so that neither party can subsequently dispute the processing data.

5. **Access Control Authentication:** Illegal usage of resources can be prevented by access control. It comprises preventing illegal use of a resource by verifying the network, originator's and single user's have ability to access certain kind of data.

2.2 Cryptanalysis

Cryptanalysis [41] is the study of principles and methods of transforming the plaintext from the ciphertext (breaking a code) without having the knowledge of the key. The information will be analyzed in order to find the system's hidden nodes. A cryptanalyst is someone who attempts to execute this task. He decrypts ciphertext using an algorithm without knowing the original sources or encryption keys. By detecting faults in a security protocol, a cryptanalyst also attempts to improve existing approaches. This can be done by discovering the key and upgrading methods that lack the four properties of confidentiality, integrity, authentication, and non-repudiation. If any of the four qualities is missing, the protection of transmission can be affected and the encrypted message can easily be decoded.

There are two types of attacks used in cryptanalysis: active and passive. To accomplish cryptanalysis, a cryptanalyst must breaks some cryptographic scheme. [42]

1. **Passive Attack**

   A cryptanalyst tries to crack the system independently based on known data while unable to engage with any of the operators. Passive attacks are those which do not affect the network's normal operation in these types of attacks. Attackers monitor the data in network traffic without modifying it. If an attacker is also able to understand data collected through monitoring, confidentiality might be compromised. Because the network's operations are unaffected, detection of these attacks is difficult [43].

2. **Active Attack**

   In this type of attack, the cryptanalyst alters the message. He tries to reveal the key through generating, fabricating, modifying, altering, deleting or diverting communication [44].

There are many attacks, some of them are discussed here.

- **Plaintext Attacks**

  In this attack, a cryptanalyst knows the encrypted message and the associated known partial plaintext. He seeks to design an efficient technique for decrypting every encrypted message as well as the key of its matching plaintext using this knowledge. This allows the attacker to analyze the relationship between the plaintext and the ciphertext.

- **Chosen Plaintext Attacks**

  Chosen-plaintext attacks provide a wide range of possibilities. i.e, an enemy compensates someone who encrypts the chosen text. A chosen-plaintext attack is a kind of active attack. Such attacks compromise the integrity and confidentiality of the data being transferred. The ciphertext $c = e(p,k)$ is given to the attacker by the user, where p is chosen text, c is encrypted text and e is the encrypted function. The goal of attacker is to determine the unecrypted text $p^{'} = p$. Since the attacker has the access to the cipher block e, he can cipher his messages p_i and analyze the obtained ciphertexts c_i = e(p_i,k). Finally, attacker found the message $p^{'}$ and transmits it to the intended recipient [45].

- **Brute Force Attack** This attack is also called exhaustive study. It is a cryptographic attack that works by assuming all possible password combinations until the correct one is found. A brute force attack can take a very long time to execute, be hard to carry out if information bafflement is used. By extending the key space, this approach can make more difficult. Tabel 2.1 have a detailed picture of all possible attacks and there features.

TABLE 2.1: Comparative study of some possible attacks and their features

Cipher	**Type**	**Bit length**	**Possible attack**
DES [33]	Symmetric Key	56 bits	Brute force Attack, Differential and Linear Cryptanalysis
AES [8]	Symmetric Key	128,192,256 bits	Known plaintext
RSA [36]	Asymmetric key	1024-2048 bits	Brute force Attack
ElGamal Encryption [38]	Asymmetric key	1024-2048 bits	Chosen Ciphertext attacks

2.3 Terminolgy Related to Image Encryption

These are some of the most basic terminology in image encryption methods.

2.3.1 Digital Image

Image is a two-dimensional light intensity function $h(u, v)$, where u and v are structural coordinate. The value of h at any point (u, v) tells the brightness of the image component at that point.

A digital image is a graphical representation of an image that has been digitally encoded. It is a two-dimensional image's numerical representation, often known as a raster image or a bit-mapped image. Pixels of a digital image are placed in a rectangular 2-dimensional grid, known as a matrix with N rows and M columns. The main method is used for the digital image protection method to encrypt the digital information included in the digital image, gives a completely distinct encrypted image by the appearance than the original digital image. When the digital image is required for showing , the corresponding decryption algorithm is used to calculate and decrypt the encrypted image in order to restore the digital image's original content which is an important method used for digital image content protection in a transmitted environment of high security protocols [46].

2.3.2 Pixel

Pixel is the combination of two words Pix and el, which means picture element. It is the basic component of an image. An image is made up of various pixels. There are three primary colors red, green and blue whose composition determines the pixel colour [47].

2.3.3 Types of Image Format

Image have many formats. Some of them are listed here:

1. Tagged Image File Format(TIFF).
2. Joint Photographic Experts Group(JPEG).
3. Portable Network Graphics(PNG).

2.3.3.1 Tagged Image File Format (TIFF)

TIFF is a popular image file format used in publishing and graphic designing. TIFF was established as a single format for scanned images. It's currently used to generate TIFF images by fax and scanning software. TIFF picture files support internal meta data tags, as its name implies. The original file remains unchanged in this format despite of how many times it is duplicated, zipped or re-saved. This format is generally used for printing, archival copies and professional publications, among other things. GeoTIFF [48] and (MDI) microsoft document image format [49] are both expanded versions of TIFF. The file extensions .tif or .tiff are used for this image format.

2.3.3.2 Joint Photographic Experts Group (JPEG)

JPEG is members of ISO and ITU [50]. It creates standards for a set of image compressive methods. In web graphics it supports various level of compressions. In jpg image, 16M different colours are created through eight bits for red, green, and blue in color scale image. This method may reduce dimension of bitmap by 10 times and it does not affect it's standard. Even, this method is called lossless because sometimes it sacrifices image standard. This disadvantage emphasis many skilled photographers to work on raw matrial becuase they can change them to good standard as much as required. The file extension .jpg or .jpeg is used for this format.

2.3.3.3 Portable Network Graphics (PNG)

This format is usually used for interactive files and documents in web sites, but it is not suitable for printing. This format is also uncompressed which implies that it can be edited without affecting the original file's quality. It displays 16 millions colours range. File extension used for this format is .png.

2.3.4 Image Resolution

The image resolutions specifies the quality of an image. It is a basic character of different types of images like; digital images, movies pictures and other sorts of images. There are many methods to quantify its resolution. The term "resolution" relates that how lines can be near to each other while it even visibles now. Sizes of lines are line per mm, line per inch and total sizes of frame are line per frame high, television line or angled substance can all be linked to resolution units. Instead of lines, line pairs are frequently employed. So there are two types of lines: dark and bright. Resoulation is often known by any picture's lenght, width and its number of pixels.

Assume a picture with m columns and n rows has a resolution of $m\times\ n$. The order $m\times\ n$ denotes the entire number of pixels in a picture. For example 2046 pixel wide by 1530 pixel height image (2046 ×1530) contains 3,130,380 pixels. Similarly, a 2048 pixel wide by 800 pixel height image (2048 ×800) comprises 1,638,400 pixels (or 1.6 Megapixels). If we compare any two resolution then image with a resolution of 3.1 Megapixel has a higher quality than the image with a resolution of 1.6 Megapixel. As a result, a high-resolution image will have greater image quality. As shown in Figure 2.7, in this figure there are six images of different sizes 2 ×2, 5 ×5, 10 ×10, 20×20,50 ×50 and 100 ×100 are shown.

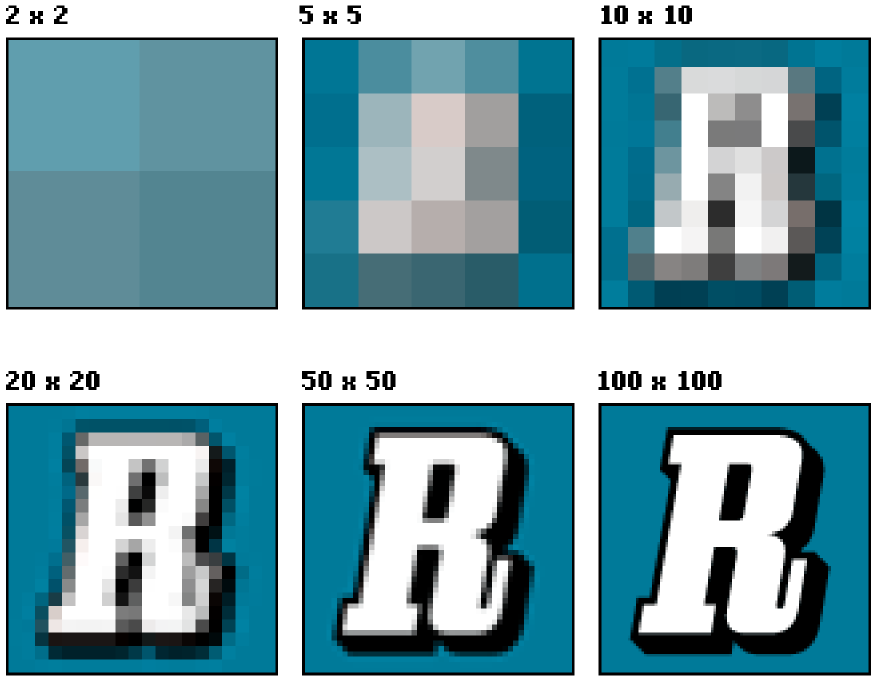
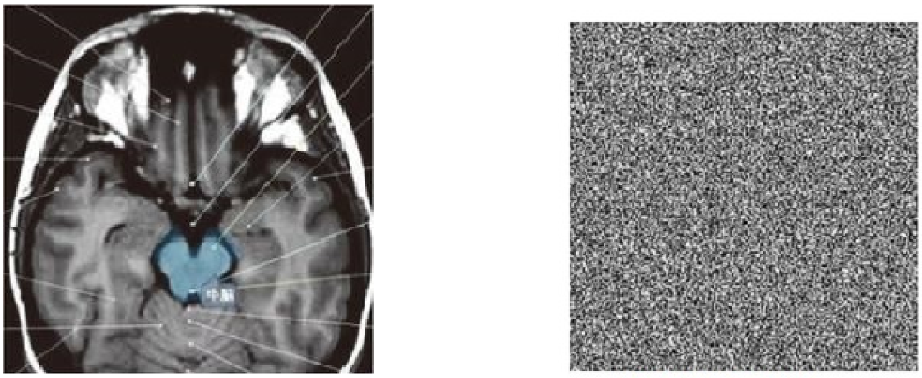


Figure 2.7: Different Image Resolution

It is clearly seen from the figure that image having size 100×100 have visually better appearance than other.

2.3.5 Image Encryption and Decryption

Image encryption is a method of tranmitting an original image into a coded image. It protects the image during transmission over a public network. There is always a need to secure the data related to the secret image in order to maintain its security, and no one can identify them other than the authorized receiver. As show in Figure 2.8 , an encrypted image is obtained by using a spcific Image encryption secheme, which will be described in Section 3.3. Permutation modulation and diffusion(PMD) based image encryption algorithm is used to encrypt the image of MRI. After that image is sent to its authorized receiver through public network.

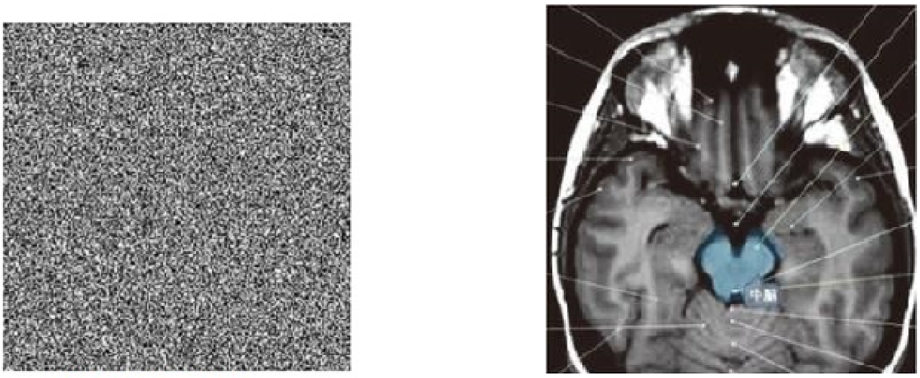


(a) MRI original image

(b) Encrypted image

Figure 2.8: Image Encryption

Decryption is reversable process in which image is converted in to its orignal form by using the secret keys and decryption technique as shown in Figure 2.9.



(a) Encrypted image

(b) Orignal image

Figure 2.9: Image Decryption

Only an authorized person can acquire the original image in this process. When the encrypted image is received, the receiver decrypts it to recover the original image. To obtain the plainimage, a receiver uses the inverse permutation modulation and diffusion secheme. The original image is then acquired at the receiver's end. [6].

2.4 Chaos Theory

It is a branch of mathematics which deals with several applications like physics, biology, philosophy and economics etc. It behaves like dynamical system which is very sensitive to initial conditions. In deterministic chaos, unpredictability comes from the fact that two very similar initial conditions often lead to two very different outcomes. Chaotic behavior lies in many natural phenomenas e.g turbulence in fluids, weather, stock exchange and mental states etc.

In chaos theory, fractal mathematics is also used. A fractal pattern is a pattern that never ends but also is self-similar at all scales. Trees, rivers, beaches, mountains, clouds, hurricanes and other natural phenomena are examples of fractals chaos. In order to illustrate the dynamic system's fractal structure, the best example to convey the full scenario is the balloon pilot [51]. When he reaches at his destination, he must consider the complex, chaotic change in the environment. Chaos theory can find a better approach to objects that are chaotic or fractal in nature. Chaos theory is also influencing the growth of fields like physics, economics [52], engineering and biology among others [53].

2.4.1 Butterfly Effect

The buttery effect is a phenomenon that helps to explain the chaotic behavior. It narrates that huge change happens as a result of a relatively minor influence or change. The butterfly effect describes how a small change in the input can have a huge impact on the output. Simply we can say that fluttering of a butterfly's wing can cause hurricane halfway around whole globe [54]. Prior to Lorenz study, many felt that having a rough grasp of the initial conditions would lead to a rough prediction of the conclusion. Lorenz system is simplified model of the earth atmosphere. In 1960s, because of large sequence and limited process strength, he divided larger data into smaller size and started the next subsequence with previous result with a lower precision. A simulation of this behavior based on Lorenz system can be found in Figure 2.10 , where y_0 is initial condition, which is taken out from [55].

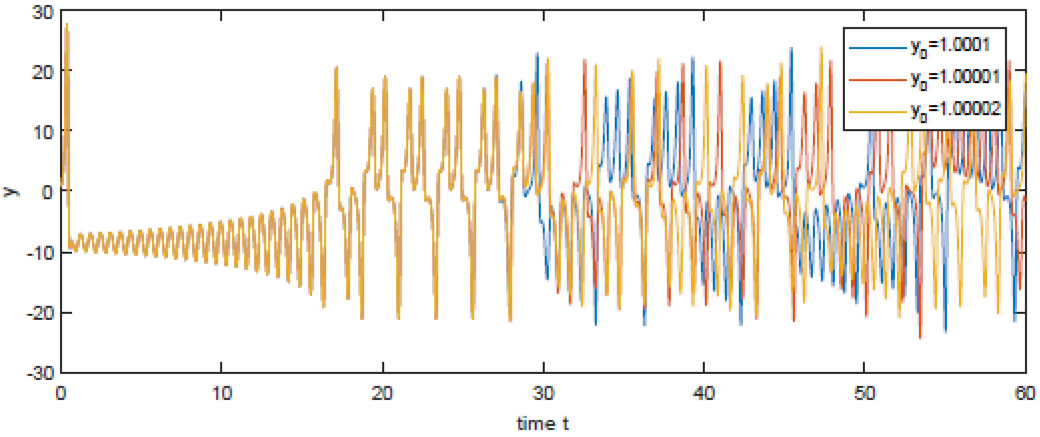


Figure 2.10: Sensitivity in Lorenz system

2.4.2 Properties of Chaotic System

Many natural structures, including a significant number of technical and industrial regions, have borne witness to chaos. Such instances point to definite possessions that are difficult to locate and forecast. Chaos is a phenomenon that occurs in practically all nonlinear deterministic systems. There are several properties that summarize the characteristics of chaotic systems [56].

1. **Self-similiarty** It indicates the appearance of a system evolving across time or space at different scales of observation.

2. **Non-periodicity** A chaotic system does have sequence of values for the evolving variable which repeat themselves resulting in periodic sequence beginning at any point in the sequence. However, such periodic sequence does

not attract but repel which means that if evolving variable is outside the sequences, it will divert from it and will not enter consequently in all initial condition. The variable evolves chaotically and non-periodically.

3. **Sensitivity to Initial Conditions** The sensitivity to initial conditions describes how each locations in a chaotic system is arbitrarily closely approximated by other locations with significantly differing future paths or trajectories. As a result, even slight changes in the current trajectory can result in significantly different future behaviour.

2.5 Chaotic Map

A chaotic system is highly sensitive to initial conditions in science. Chaotic maps and cryptographic algorithms have same characteristics like sensitive to initial conditions, pseudorandom behaviour unstable periodic orbits with lengthy periods. Chaotic systems have properties such as randomness, strange attractor, aperiodicity, ergodicity and high sensitivity, making them easy to secure cryptosystems [57]. If the initial condition's value is changed imperceptibly, system's output will change unexpectedly. Many natural systems around us are chaotic [58] . For example chaotic mapping can parameterize using a discrete-time or continuous-time parameters. Iterated functions are usually discrete maps. In the study of dynamical systems, chaotic maps are commonly encountered.

- **Control parameter** A control parameter is an essential part of any chaotic map. It actually controls the behavior of map. Many chaotic maps show chaotic behaviour in a certain control parameter region. It can be seen in Henon chaotic map (HCM) 2.5.3, Brownian motion(BM) 3.2.1 or Chen chaotic system(CCS) 2.5.4.

2.5.1 Lyapunove Exponent

An essential characteristic of chaotic map is a small instability of initial data will correspond to rapid expansion of outcomes. In a non chaotic map, paths near to one another may merge rapdily or split rapdily. The Lyapunov exponent (LE) [59] is “a quantity that characterizes the rate of separation of infinitesimally close trajectories”. It represents “the numerical characteristic of the average exponential divergence rate of adjacent trajectories in the phase space which is one of the key features used to identify the chaotic system”. A positive LE means that two trajectories diverge in each iterations and no matter how close they are each other. For a chaotic map $h(x)$, it can be expressed as

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n-1} \ln |h^{'}(x_i)| \tag{2.2}$$

The dynamical cases of the Lyapunove exponent exist and given below:

1. When $\lambda < 0$, its orbit behaves like a single point.
2. When $\lambda = 0$, system behaves stable. Such system are conservative and in steady state mode.
3. When $\lambda > 0$, then system is chaotic and unstable.

2.5.2 Bifurcation Diagram

Bifurcation arises, when initial condition is changed. It is a period doubling transition from anQ-point attractor to a 2Q-point attractor.A bifurcation diagram shows the pattern of period-doubling when the control parameter $h$rises graphically. Bifurcation diagram of Henon chaotic map is shown in Figure 2.11, with h along x-axis having range of [0, 1.5].

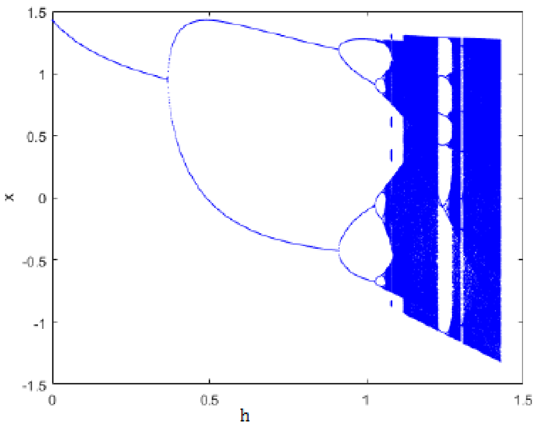


FIGURE 2.11: Bifurcation diagram

So it has been seen that from 1.05 to 1.44, has chaotic region. Although system is not chaotic for all values of $h \in [1.05,\ 1.44]$, even there are some points in which it shows three to four attractors.

2.5.3 Henon Chaotic Map

This map is dynamical and two dimensional system of the discrete time non linear chaotic map. It is well-known application of 2D dynamical form with chaotic behaviour. Henon introduced this system in 1976 [60]. The 2D injective map is proposed as,

$$\begin{aligned} x_{n+1} &= 1 - hx_n^2 + y_n \\ y_{n+1} &= kx_n \end{aligned} \tag{2.3}$$

where h and k are the control parameters, $h \in (0.54, 2)$, and $k \in (0, 1)$ with two initial parameters x_0, y_0 of this map. The value for $h = 1.4$ and $k = 0.3$ which shows chaotic behavior.

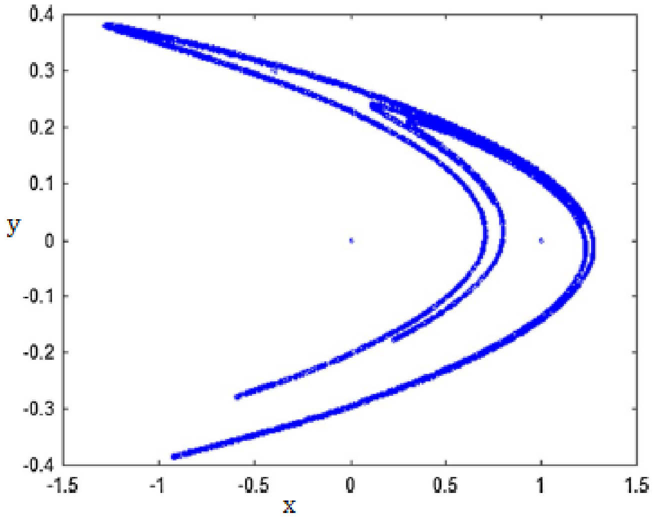


FIGURE 2.12: 2D chaotic mapping for many iterations with initial conditions h=1.4 and k=0.3

The Henon chaotic map lies in range of $[-1.5, 1.5]$ on x-axis while $[-0.4, 0.4]$ on y-axis. If $k = 0.3$ is fixed and h varies in the range of $[0, 1.5]$, the bifurcation diagram [55] of Henon Chaotic map is shown in Figure 2.13. Bifurcation shows at 0.38, 0.9, 1.08 (approximately) etc. Until reached at 1.05, where system behaves chaotic.

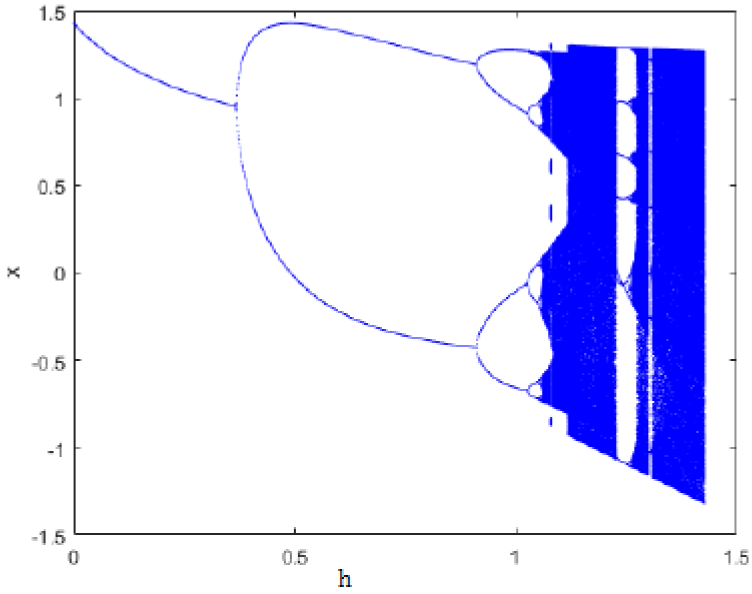


FIGURE 2.13: Bifurcation diagram of Henon chaotic map

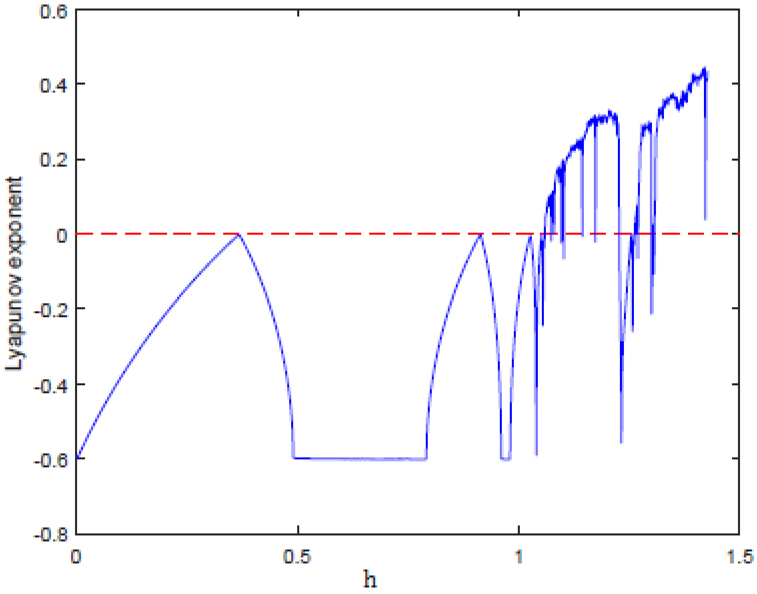


FIGURE 2.14: lyapunov exponent of Henon chaotic map

The lyapunov exponent of Henon chaotic map is shown in Figure 2.14 and shows chaotic when $\lambda > 0$.

2.5.4 Chen Chaotic System (CCS)

A chen chaotic system is three dimensional system and it is used to select different dimensional coordinates. It transforms 3D chaotic orbit into a 1D orbit. This chaotic mixing strategy is clearly more secure than the fixed mixing strategy. We demonstrate mathematically that the generated new system is still chaotic and that the sequence generated by this new system is numerically more complex than any dimensional variable of the original Chen system. We also proposed a Pseudorandom bit generator based on this new chaotic system. Both statistical and security analysis show that the generated PRBS has good statistical properties and a high resistance to attacks.

Mathematically, the chen chaotic system is given as:

$$\begin{aligned} \frac{dx}{dt} &= h(y-x), \\ \frac{dy}{dt} &= (j-h)x - xz + cy, \\ \frac{dz}{dt} &= xy - iz, \end{aligned} \tag{2.4}$$

where $(h, i \text{ and } j) \in \mathbf{R}^3$ are constant parameter. For $h = 35$, $i = 3$, $j = 28$, then the system shows chaotic attractor [62]. The attractor of chen chaotic system is shown in Figure 2.15.

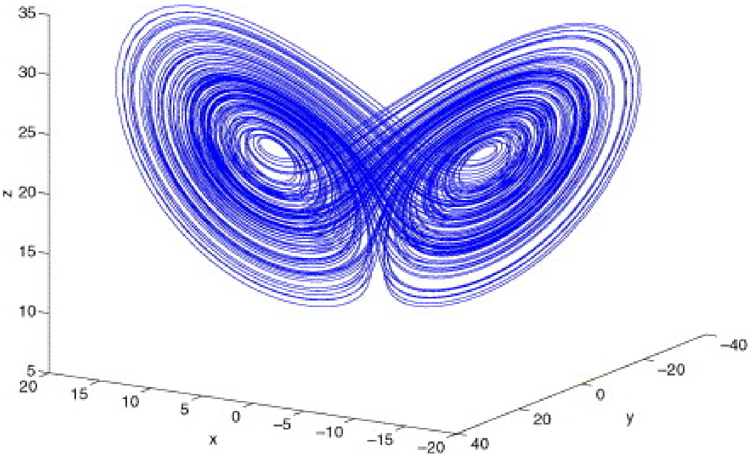


FIGURE 2.15: Three dimensional picture of chen chaotic map

Bifurcation diagram of this system is shown in Figure 2.16 with the range of h and i, when $j = 28$.

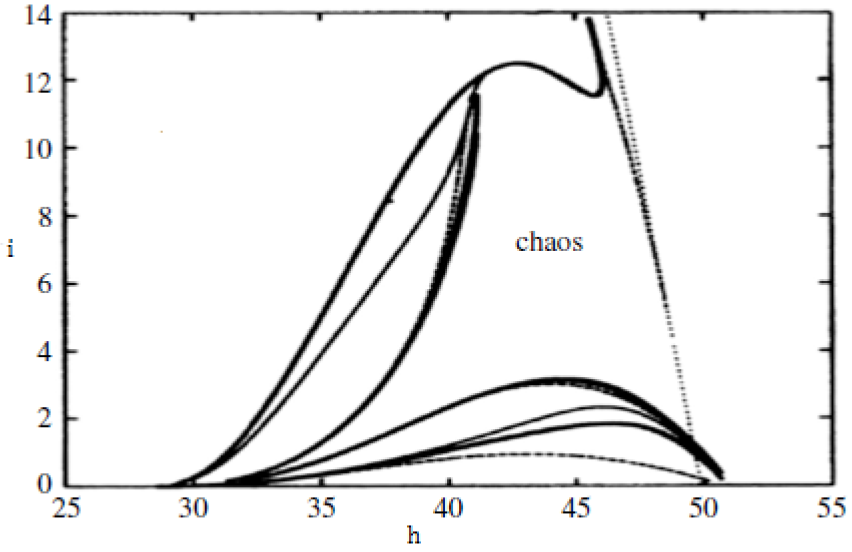


FIGURE 2.16: Bifurcation diagram of CCS

A 4th-order RK [61] techinque is used for numerical iterations of the Chen chaotic system in the numerical tests keeping the numerical outputs very probable to the actual model behaviour. PRBG(Pseudorandom bit generator) has a number of advantages. The generated sequence exhibits complicated behaviour than any of the original Chen system's dimensional variables, complicating the extraction of information from the orbits. Because we do not use any specific properties of the CCS(chen chaotic system).

2.6 Chaos and Cryptography

Chaos is generally observed in nonlinear systems and is particularly sensitive to the system's initial conditions. Understanding the output of these systems for an analyst who is aware of the initial conditions affecting the features is a key element of these systems. When the system's initial values are uncertain then the system tends to be very randomized. Unless the authorized user is aware of pseudo-random behavior.

2.6.1 Chaos Based Cryptosystem

According to this literature, majority of chaos based cryptosystems are symmetric in nature. A chaos based system used to generate the key and encryption and decryption algorithms by using chaotic values. It can be seen in Figure 2.17 from [55].

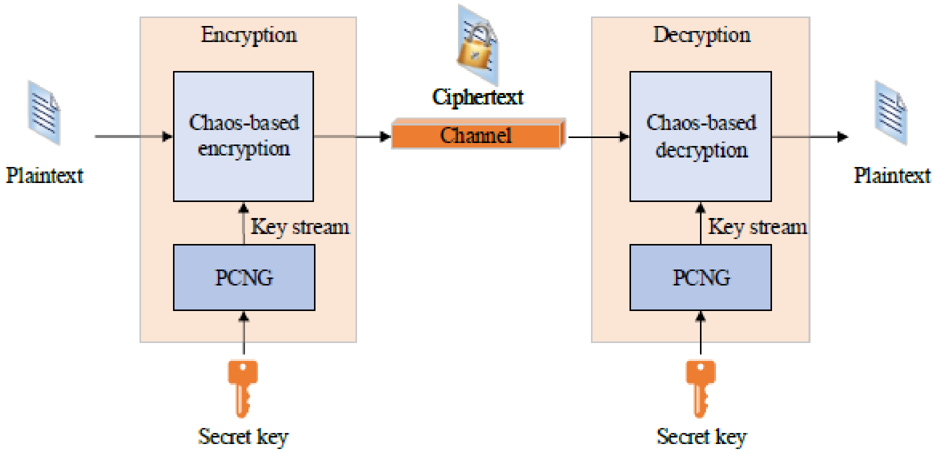


FIGURE 2.17: Chao based cryptosystem scheme

In a chaos based cryptosystem, original message in transformed into ciphertext by using chaos based encryption algorithm with private keys. The key stream for the process of encryption is provided by the pseudo chaotic number generator by using the private keys. Authorized users can obtain plaintext by decrypting the ciphertext with symmetric private keys. Chaotic components play a vital part in the encryption and decryption processes, not only in providing cryptographic key streams for encryption and decryption methods but also in attaining a satisfactory confusion and diffusion process. The pseudo chaotic number generator should be able to generate pseudo-random numbers as the key stream that are both random and sensitive to the secret key.

2.6.2 Confusion and Diffusion

Confusion and Diffusion are the two principles that are used to secure the encryption and decryption secheme. Diffusion referes to making of a plaintext effect on several ciphertext in order to obscure plaintext's statistical structure. Confusion is the process that makes it difficult to rely on plaintext for ciphertext data. In other words, the property of confusion specifies that the key and the cipher should not be linked. In the difusion property, small change in a single bit of a plain image causes the huge distrubance in cipher bytes/bits.

Chapter 3

Review of a Medical Image Encryption using XOR Operation, Brownian Motion and Chen Chaotic System

Brownian motion is zigzag motion of particles among three different directions. Particle movement is the name given by Botanist Rober Brown, whose examined very small particles. In this chapter Section 3.1 gives the detailed discussion on Brownian motion. A complete encryption algorithm of this proposed scheme is presented in Section 3.2.1 and decryption algorithm is given in 3.3. Section 3.4 gives the implementation of encryption/decryption algorithm.

3.1 Brownian Motion

Brownian motion [58] is the ostensibly random movement of items/particles suspend to a fluid (liquid or gas) as a result of bombardment by the gas or liquid's fast-moving atoms or molecules. The mathematical model used to represent such random movements, known as a particle theory, is also referred to as "Brownian motion".

Firstly, this concept came from a pollen seeds that are dropped into the water and he noticed oscillations and spontaneous motion in it. But at that time he did not identify the cause of this behavior which he noticed.

Laterly, in 1905, a nobel scientist, Albert Einstein, published an article in which he described the exact random motion of particles observed by Brown via movement of particles, so this invention was an enormous achievement in science. He found zigzag was caused by the kinetic energy of water molecules [58]. This phenomenon is used to design a secure cryptosystems.

In 2014, Wang and Xu [27] considered single particle of Brownian theory as a pixel of image and used Monte Carlo method and encrypt original test image. Zhu [28] attacked Wang et al. method [27] in 2015 because their system was dependent on permutations and diffusing sequences that were irrelevant to plaintext image thus scheme given by Wang et al. [27] was unfeasible to show resistivity against the chosen plaintext.

3.1.1 Monte Carlo Method

Brownian motion can be generated using Monte Carlo's method [27]. Monte Carlo method (also called Monte Carlo's experiment) is computational process that produces numerical solution by repeating random values. For each process, Monte Carlo simulation provides the decision-maker with a range of probable outcomes as well as the probabilities that they will occur. It gives the extreme outcomes and the most conservative decision.
Although Monte Carlo algorithms differ, they always follow a particular procedure whose steps are given below:

1. Establish a domain of possible inputs.
2. Randomly generate inputs from a probability distribution over the domain.
3. Calculate the inputs in a deterministic manner.
4. Combine the results.

3.1.2 The Simulation Process

Brownian is impulsive motion of elements in fluid (liquid or gas) substance due to interchange between freely moving molecules.

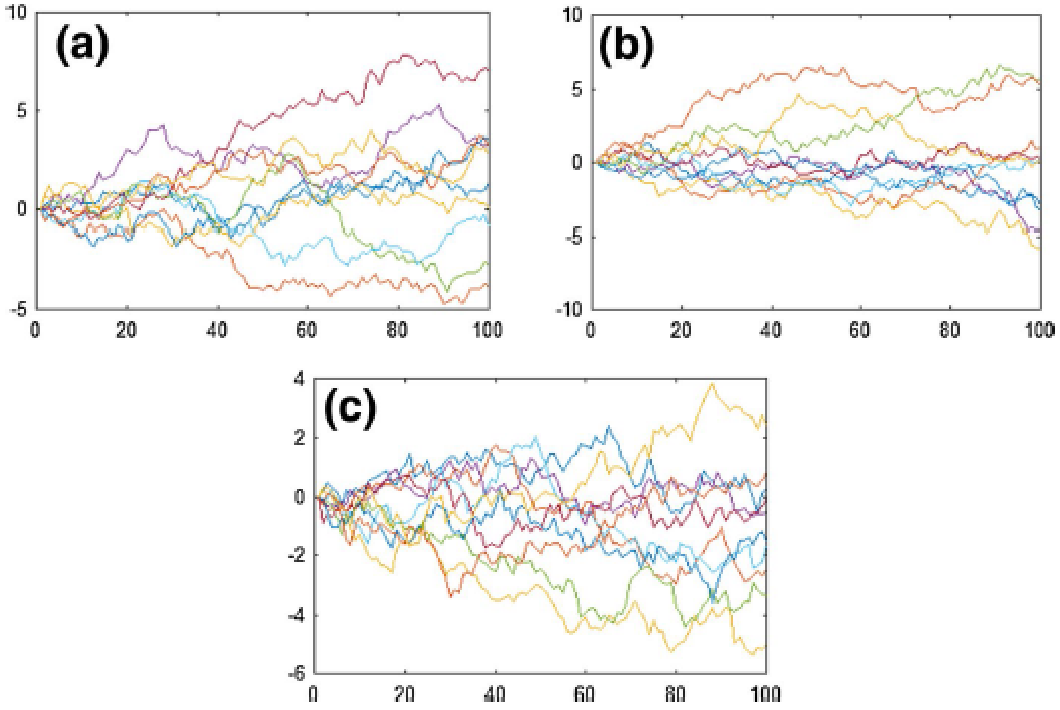


FIGURE 3.1: Brownian motion elements along three axies

The particle growth along three main axis (H, I, and J) as shown in Figure 3.1 is mathematically expressed as

$$\begin{aligned} H &= t \sin\theta \cos\phi \\ I &= t \sin\theta \sin\phi \\ J &= t \cos\theta \end{aligned} \tag{3.1}$$

whereas $0 \leq$ t $\leq +\infty$, $0 \leq \phi \leq 2\pi$ and $0 \leq \theta \leq \pi$

The following information is also required for the simulation of Brownian particles, i.e

1. Motion of particles along three axis (H, I and J)

2. A specified time duration (t_p).

3. Total number of particles (n_p).

4. Number of impulses per change in track.

5. Step length $t = 2$.

6. Use of pseduo random function to get direction of particles.

By using initial values and sequence x_n and y_n of Henon chaotic map one can iterate BM coupled equations. For any pixel $n = 1, 2, 3, \ldots, i \times j$ using the following formulas we acquire the two angles under polar coordinates system [28].

$$\begin{aligned}
\theta_n &= x_n \times \pi \\
\phi_n &= y_n \times 2\pi \\
H_n &= t \sin\theta_n \cos\phi_n \\
I_n &= t \sin\theta_n \sin\phi_n \\
J_n &= t \cos\theta_n
\end{aligned} \tag{3.2}$$

3.2 Key Setting

There are following control parameters that are playing very important role in encryption and decryption algorithm.

- This method uses Henon chaotic map, chen chaotic map and brownian motion for encryption process.

- For the iteration of Henon chaotic map use the key x_0= 0.63135448 and y_0= 0.18940634 and for permutation process l_0= 0.0056, $m_0 = 0.3678$, $l_0^{'} =$ 0.6229, $m_0^{'} = 0.7676$ are used, detailed discussed in Section 2.5.3

- Brownian motion is iterated using Henon chaotic sequence x, y, which discussed in Section 3.1.

- Key used for the iteration of Chen chaotic map 2.5.4 is $X(1)$ = -10.058, $Y(1)$ = 0.368, $Z(1)$ = 37.368.

3.2.1 Encryption Algorithm

Let F be an image with $i \times j$ as the dimensions of a gray scale image, in which i and j shows number of rows and numbers of columns respectively. Also $i \times j$ is the resolution of image (Considered here as 512×512). The complete permutation and diffusion encryption process is described as follow:

Input: Plainimage (F), Chaotic map 2.5, Brownian motion 3.1, Initial keys (l_0, m_0, $l_0^{'}$, $m_0^{'}$)

Output: Cipherimage ($V1_{encrypt}$, $V2_{encrypt}$ and $V3_{encrypt}$)

1. The image F which contains 262144 pixels, is divided into four blocks, i.e., $F = f_1, f_2, f_3, f_4$ and each block contains size of $m \times n = 256 \times 256$.

2. Iterate two dimensional Henon chaotic map (HCM) 2.5.3 to generate the random matrix A of size $m{\times}n$.

3. Use keys l_0, m_0, $l_0^{'}$, $m_0^{'}$ to find middle parameter a and b as

$$\begin{aligned} a &= \lceil (l_0 + m_0 + 1) \times 10^7 \rceil \mod m + 1 \\ b &= \lceil (l_0^{'} + m_0^{'} + 1) \times 10^7 \rceil \mod n + 1 \end{aligned} \tag{3.3}$$

   where $\lceil\ . \rceil$ is the ceiling function that gives the near largest integral value. Then choose a row and column from A. To apply the circular shift on each block of F. Suppose a^{th} row of A as a row vector h is taken and b^{th} column of A is column verctor k.

4. An alternative function is used to modify row vector h of order m and the column vector k of order n as

$$\begin{aligned} h^{'} &= \lceil h \times 10^{14} \rceil \mod m \\ k^{'} &= \lceil k \times 10^{14} \rceil \mod n \end{aligned} \tag{3.4}$$

   In each Block (f_1, f_2, f_3, f_4), $h^{'}$ is used for the circular permutation row wise and k is for column wise. After applying the permutation to the plain image A in the row and column direction, permuted block of image P1, P2, P3, P4, are obtained. Combining all the permuted blocks to get the permuted Image $P^{'}$.

5. After intra-block shuffling of image $P^{'}$, image blocks are shuffled up to third phase, then apply horizontal circularshift of blocks with respect to $h\prime$. After shuffling the Blocks a permuted image P is formed.

6. Then a 3D Brownian motion is used. This motion is started to explain the number of particles in terms of time, position of different particles and the amount of impulses per each change performed in each of three different axis $(H, IandJ)$ e.g., $H = t_1, I = t_2$, and $J = t_3$. These values are saved in each direction, here total number of particles are 256, total time $t = 60$ *second* and number of impulses per change in track (N) is 100.

7. In this step Brownian Motion is iterated for $N = 1536256$ times for each direction t_1, t_2, t_3 respectively. The first 1274112 values are discarded, $1536256 - 1274112 = 262144$ from each direction to increase the randomness. So these random values are iterated and saved as Q_1, Q_2, Q_3, respectively.

8. The values of Q_1, Q_2 and Q_3 are now multiplied by 10^{14} to get R_1, R_2 and R_3, respectively. Further R_1, R_2 and R_3 are change to order of 512×512 pixel, which helps to get random sequencing for three directions (S_1, S_2 and S_3).

9. Absolute and round function are implemented to S_1, S_2 and S_3 and the new data are saved in T_1, T_2 and T_3, respectively.

10. Modulus 256 operation is implement to T_1, T_2 and T_3 in order to get U_1, U_2 and U_3.

11. Zig-zag random sequence U_1, U_2 and U_3 are multiplied with the permuted grey image P and the new values are saved in V_1, V_2 and V_3.

12. A Chen chaotic System is introduced for an extra layer of protection, boosting the proposed program's unpredictability and entropy.

13. Lastly, CCS is generated and bitwise XOR with V_1, V_2 and V_3 to generate new encrypted layers such as $V1_{encrypt}$, $V2_{encrypt}$ and $V3_{encrypt}$.

The complete encryption procedure is illustrated by the flow-chart given in Figure 3.2.

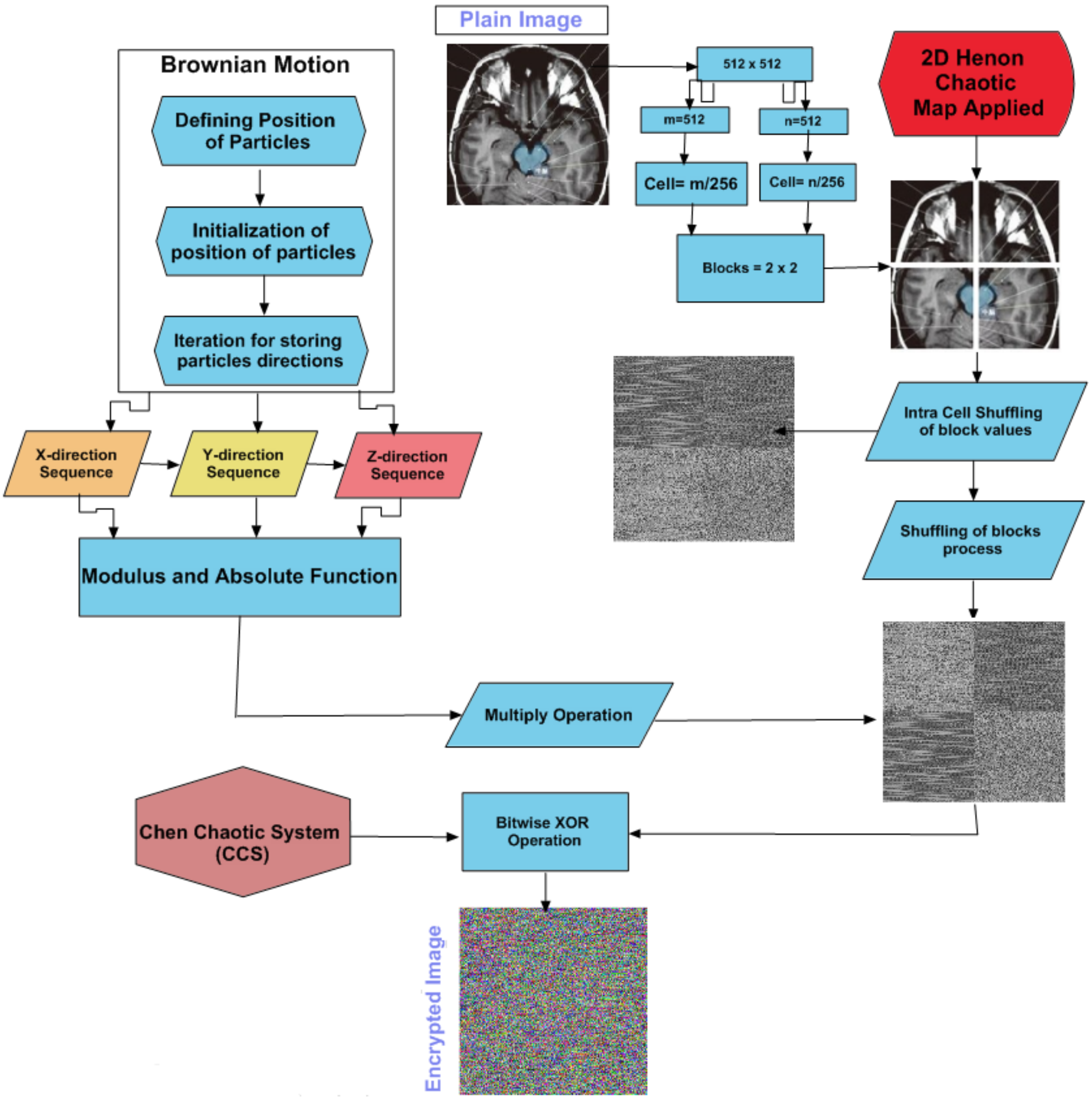

Plain Image
Brownian Motion
Defining Position of Particles
Initialization of position of particles
Iteration for storing particles directions
512 x 512
m=512
n=512
Cell= m/256
Cell= n/256
Blocks = 2 x 2
2D Henon Chaotic Map Applied
X-direction Sequence
Y-direction Sequence
Z-direction Sequence
Intra Cell Shuffling of block values
Shuffling of blocks process
Modulus and Absolute Function
Multiply Operation
Chen Chaotic System (CCS)
Bitwise XOR Operation
Encrypted Image

Figure 3.2: Complete Encryption process of a medical image

3.3 Decryption Algorithm

As the proposed image cryptosystem is symmetric in nature therefore decryption process can also be carried out by using similar steps in the opposite direction.

1. Firstly a three dimenionsal (3D) Chen chaotic System is iterated with inital keys and generate three output layers stored as CS1, CS2 and CS3.

2. CCS output layers are taken for bitwise XOR with encrypted layers $V1_{encrypt}$, $V2_{encrypt}$ and $V3_{encrypt}$.

3. New layers stored as D_1, D_2 and D_3.

4. Brownian Motion is iterated for 1536256 times through all axis t_1, t_2 and t_3.

5. Initially 1274112 entries are neglected and remaining 262144 entries will be used to increase the randomness. So these random values are iterated and saved as Q_1, Q_2, Q_3 respectively.

6. The values of Q_1, Q_2 and Q_3 are multiplied by 10^{14}.

7. New values stored as R_1, R_2 and R_3, respectively.

8. Further R_1, R_2 and R_3 are change to generate a random motion of order 512×512 pixel, which help to get random sequencing for three directions(S_1, S_2 and S_3).

9. Absolute function is implemented to S_1, S_2 and S_3.

10. Round function is also implemented to S_1, S_2 and S_3.

11. New data are saved in T_1, T_2 and T_3 respectively.

12. Modulus 256 operation is implement to T_1, T_2 and T_3.

13. New values stored as get U_1, U_2 and U_3.

14. Take the inverse of U_1, U_2, U_3.

15. U_1, U_2, U_3 is multiplied with D_1, D_2, D_3 (Which is taken from first Phase)and get another three layers of images, which all are same and stored as G.

16. The image G which contains 262144 pixels is further divided into four Block, i.e, G= g_1, g_2, g_3, g_4 ane each block has size of $m \times n = 256 \times 256$.

17. Iterate the two dimensional HCM (2.4.1) to generate the random matrix A of size $m{\times}n$.

18. Use keys l_0, m_0, $l_0^{'}$, $m_0^{'}$ to find middle parameter a and b as

$$\begin{aligned} a &= \lceil (l_0 + m_0 + 1) \times 10^7 \rceil \mod m+1 \\ b &= \lceil (l_0^{'} + m_0^{'} + 1) \times 10^7 \rceil \mod n+1 \end{aligned} \tag{3.5}$$

where $\lceil \; . \rceil$ is the ceiling function that gives the near largest integer.

19. Then choose a row and column from A. To apply the back circularshift on each block of G.

20. Suppose a^{th} row of A as a row vector h is taken and b^{th} column of A is column verctor k.

21. For saving time, an alternative function is used to modify row vector h of order m and the column vector k of order n as

$$\begin{aligned} h^{'} &= \lceil h \times 10^{14} \rceil \mod m \\ k^{'} &= \lceil k \times 10^{14} \rceil \mod n \end{aligned} \tag{3.6}$$

In each Block (g_1, g_2, g_3, g_4), $h^{'}$ is used for the back circularshift row wise and k is for column wise.

22. After applying the permutation to the image A in the row and column direction, a decrypted block image M1, M2, M3 and M4 is obtained.

23. Combining all the permuted Block to get the plainimage M .

24. After intra-block shuffling of Image M, image blocks are shuffled up to this phase with a_1= $h^{'} \mod 4$.

25. Apply horizontal back circularshift of blocks with respect to a_1.

26. After shuffling the blocks a plain image N is formed.

The complete decryption procedure is illustrated by the flow-chart given in Figure 3.3.

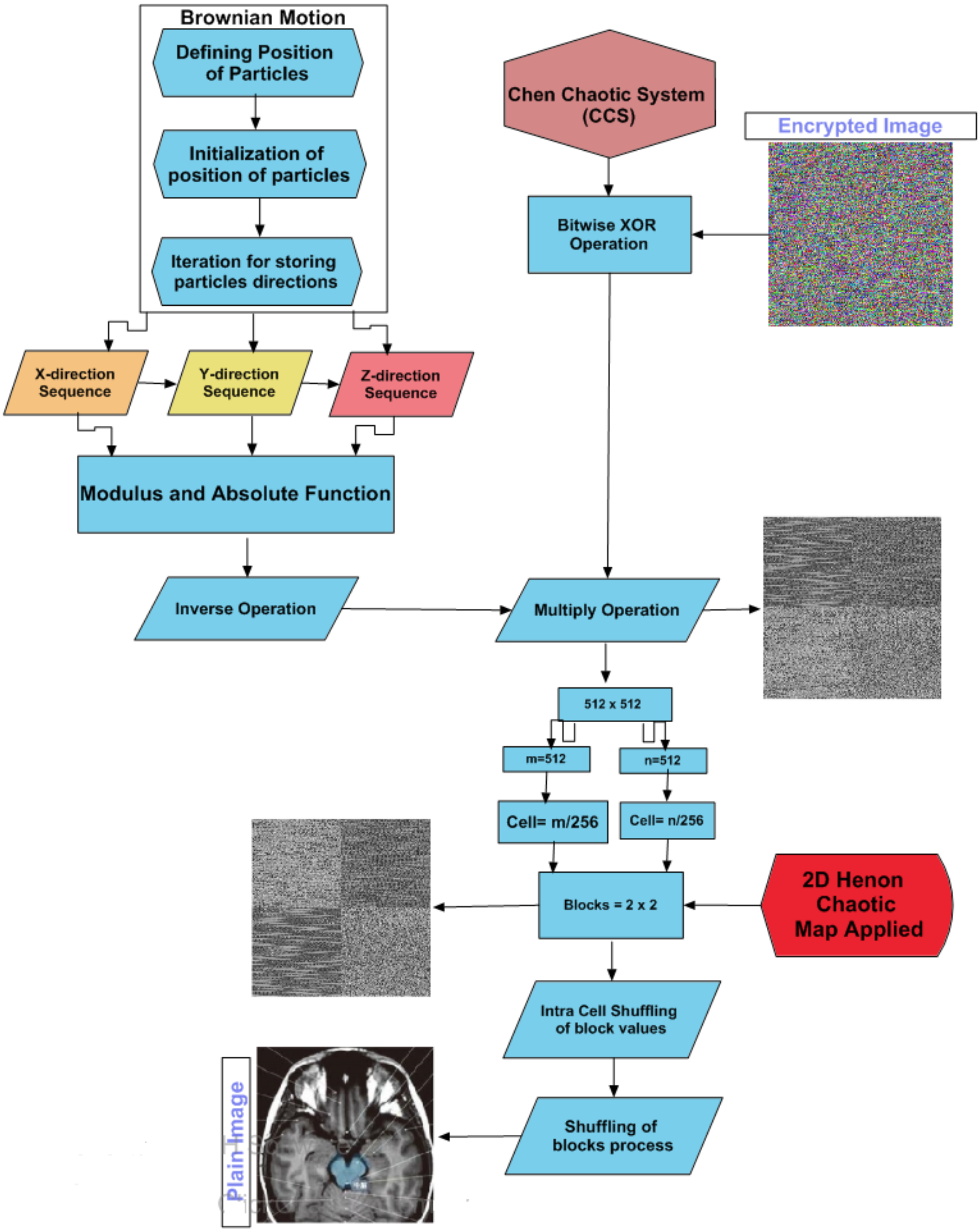

Brownian Motion
Defining Position of Particles
Initialization of position of particles
Iteration for storing particles directions
X-direction Sequence
Y-direction Sequence
Z-direction Sequence
Modulus and Absolute Function
Inverse Operation
Chen Chaotic System (CCS)
Encrypted Image
Bitwise XOR Operation
Multiply Operation
512 x 512
m=512
n=512
Cell= m/256
Cell= n/256
Blocks = 2 x 2
2D Henon Chaotic Map Applied
Intra Cell Shuffling of block values
Shuffling of blocks process
Plain Image

FIGURE 3.3: Complete Decryption process of a medical image

3.4 An Implementation of Image Encryption and Decryption Algorithm

3.4.1 Implementation of Encryption Algorithm

To understand the whole algorithm process of encryption and decryption. Firstly it is implemented on MATLAB successfully, then take a tie example and construct a matrix of size 6 × 6 with initial keys l_0 = 0.0056, m_0 =0.3678, $l_0^{'}$= 0.6229, $m_0^{'}$ = 0.7676 for encryption process.

1. Let

$$J = \begin{bmatrix} 138 & 116 & 141 & 136 & 150 & 99 \\ 118 & 116 & 154 & 180 & 141 & 110 \\ 122 & 116 & 99 & 159 & 110 & 146 \\ 117 & 88 & 104 & 138 & 102 & 174 \\ 110 & 88 & 84 & 132 & 121 & 167 \\ 116 & 67 & 96 & 159 & 150 & 102 \end{bmatrix} \tag{3.7}$$

2. Split matrix J into four blocks i.e J_1, J_2, J_3, J_4

$$J_1 = \begin{bmatrix} 138 & 116 & 141 \\ 118 & 116 & 154 \\ 122 & 116 & 99 \end{bmatrix} J_2 = \begin{bmatrix} 136 & 150 & 99 \\ 180 & 141 & 110 \\ 159 & 110 & 146 \end{bmatrix} \tag{3.8}$$

$$J_3 = \begin{bmatrix} 117 & 88 & 104 \\ 110 & 88 & 84 \\ 116 & 67 & 96 \end{bmatrix} J_4 = \begin{bmatrix} 138 & 102 & 174 \\ 132 & 121 & 167 \\ 159 & 150 & 102 \end{bmatrix} \tag{3.9}$$

3. Iterate HCM to genrate a matrix A.

$$A = \begin{bmatrix} 0 & -0.12 & 0.166296683763917 \\ 0 & 0.3228 & 0.104265484522578 \\ 0.3 & -0.22226592 & 0.299156312569778 \end{bmatrix} \tag{3.10}$$

4. Use keys l_0, m_0, $l_0^{'}$, $m_0^{'}$ to find middle parameter a and b as

$$\begin{aligned} a &= \lceil (l_0 + m_0 + 1) \times 10^7 \rceil \mod i + 1 \\ b &= \lceil (l_0^{'} + m_0^{'} + 1) \times 10^7 \rceil \mod j + 1 \end{aligned} \tag{3.11}$$

   Then choose a row and column from A. To apply the circular shift on A. Suppose a^{th} row of A as a row vector h is taken and b^{th} column of A is column verctor k.

5. Modified row vector h and the column vector k as

$$\begin{aligned} h^{'} &= \lceil h \times 10^{14} \rceil \mod i \\ k^{'} &= \lceil k \times 10^{14} \rceil \mod j \end{aligned} \tag{3.12}$$

$h^{'}$ is used for the circular permutation row wise and k is for column wise. Permuted blocks images P1, P2, P3 and P4 are obtained.

$$P1 = \begin{bmatrix} 141 & 138 & 116 \\ 118 & 116 & 154 \\ 116 & 99 & 122 \end{bmatrix} P2 = \begin{bmatrix} 99 & 136 & 150 \\ 180 & 141 & 110 \\ 110 & 146 & 159 \end{bmatrix} \tag{3.13}$$

$$P3 = \begin{bmatrix} 104 & 117 & 88 \\ 110 & 88 & 84 \\ 67 & 96 & 116 \end{bmatrix} P4 = \begin{bmatrix} 174 & 138 & 102 \\ 132 & 121 & 167 \\ 150 & 102 & 159 \end{bmatrix} \tag{3.14}$$

6. Combining all blocks to get new permuted block $P^{'}$.

$$P^{'} = \begin{bmatrix} 141 & 138 & 116 & 99 & 136 & 150 \\ 118 & 116 & 154 & 180 & 141 & 110 \\ 116 & 99 & 122 & 110 & 146 & 159 \\ 104 & 117 & 88 & 174 & 138 & 102 \\ 110 & 88 & 84 & 132 & 121 & 167 \\ 67 & 96 & 116 & 150 & 102 & 159 \end{bmatrix} \tag{3.15}$$

7. The image blocks are shuffled in this phase. use formula, a_1= $h^{'}$ mod 4 then apply horizontal circularshift with respect to a_1. A permuted image P is formed.

$$P = \begin{bmatrix} 104 & 117 & 88 & 174 & 138 & 102 \\ 110 & 88 & 84 & 132 & 121 & 167 \\ 67 & 96 & 116 & 150 & 102 & 159 \\ 99 & 136 & 150 & 141 & 138 & 116 \\ 180 & 141 & 110 & 118 & 116 & 154 \\ 110 & 146 & 159 & 116 & 99 & 122 \end{bmatrix} \tag{3.16}$$

8. Iterate Brownian motion, reshape it into matrix of order 6 ×6.

9. Apply absolute and modulus 3 operation on it and get U_1, U_2 and U_3.

$$U_1 = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 2 & 2 & 1 & 2 & 0 \\ 1 & 2 & 0 & 0 & 0 & 1 \\ 1 & 0 & 2 & 0 & 1 & 1 \\ 2 & 1 & 1 & 2 & 0 & 0 \\ 2 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \quad U_2 = \begin{bmatrix} 2 & 0 & 0 & 1 & 0 & 1 \\ 2 & 2 & 1 & 0 & 0 & 2 \\ 0 & 0 & 2 & 2 & 1 & 2 \\ 1 & 0 & 1 & 1 & 2 & 0 \\ 0 & 1 & 2 & 2 & 2 & 2 \\ 1 & 2 & 1 & 0 & 2 & 1 \end{bmatrix} \quad U_3 = \begin{bmatrix} 0 & 1 & 1 & 2 & 1 & 2 \\ 1 & 2 & 0 & 0 & 0 & 2 \\ 2 & 1 & 0 & 2 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 2 & 2 & 0 & 2 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 2 \end{bmatrix} \tag{3.17}$$

10. Multiply it with permuted image P separately and stored as V_1, V_2 and V_3.

$$V_1 = \begin{bmatrix} 846 & 548 & 824 & 497 & 510 & 364 \\ 902 & 465 & 671 & 440 & 475 & 383 \\ 855 & 526 & 661 & 367 & 501 & 425 \\ 898 & 710 & 791 & 511 & 529 & 407 \\ 948 & 618 & 814 & 553 & 554 & 382 \\ 827 & 709 & 733 & 454 & 530 & 397 \end{bmatrix} \quad V_2 = \begin{bmatrix} 718 & 576 & 845 & 730 & 916 & 892 \\ 695 & 631 & 797 & 652 & 924 & 863 \\ 635 & 612 & 841 & 653 & 938 & 854 \\ 727 & 642 & 969 & 816 & 940 & 1063 \\ 914 & 706 & 865 & 750 & 886 & 1068 \\ 750 & 635 & 900 & 742 & 833 & 1040 \end{bmatrix} \tag{3.18}$$

$$V_3 = \begin{bmatrix} 845 & 804 & 278 & 834 & 242 & 908 \\ 797 & 779 & 242 & 762 & 231 & 946 \\ 841 & 738 & 217 & 720 & 169 & 910 \\ 969 & 913 & 240 & 915 & 237 & 993 \\ 865 & 958 & 298 & 930 & 296 & 1178 \\ 900 & 881 & 226 & 852 & 209 & 1031 \end{bmatrix} \tag{3.19}$$

11. Iterate CCS and take bitwise XOR with these values and get encrypted layers of image J.

$$V1 = \begin{bmatrix} 836 & 547 & 829 & 498 & 510 & 365 \\ 911 & 470 & 666 & 442 & 475 & 382 \\ 862 & 521 & 657 & 365 & 501 & 424 \\ 906 & 704 & 787 & 509 & 529 & 405 \\ 956 & 620 & 813 & 552 & 554 & 380 \\ 819 & 704 & 734 & 455 & 530 & 399 \end{bmatrix} \quad V2 = \begin{bmatrix} 718 & 579 & 840 & 733 & 925 & 887 \\ 695 & 628 & 792 & 644 & 917 & 852 \\ 634 & 615 & 847 & 645 & 928 & 861 \\ 726 & 646 & 975 & 824 & 934 & 1067 \\ 912 & 710 & 871 & 743 & 892 & 1056 \\ 748 & 638 & 899 & 751 & 842 & 1052 \end{bmatrix} \tag{3.20}$$

$$V1 = \begin{bmatrix} 836 & 547 & 829 & 498 & 510 & 365 \\ 911 & 470 & 666 & 442 & 475 & 382 \\ 862 & 521 & 657 & 365 & 501 & 424 \\ 906 & 704 & 787 & 509 & 529 & 405 \\ 956 & 620 & 813 & 552 & 554 & 380 \\ 819 & 704 & 734 & 455 & 530 & 399 \end{bmatrix} V2 = \begin{bmatrix} 718 & 579 & 840 & 733 & 925 & 887 \\ 695 & 628 & 792 & 644 & 917 & 852 \\ 634 & 615 & 847 & 645 & 928 & 861 \\ 726 & 646 & 975 & 824 & 934 & 1067 \\ 912 & 710 & 871 & 743 & 892 & 1056 \\ 748 & 638 & 899 & 751 & 842 & 1052 \end{bmatrix} \tag{3.21}$$

$$V3 = \begin{bmatrix} 872 & 768 & 309 & 864 & 208 & 941 \\ 824 & 815 & 209 & 728 & 197 & 915 \\ 876 & 710 & 250 & 754 & 139 & 943 \\ 1004 & 949 & 211 & 945 & 204 & 960 \\ 837 & 922 & 265 & 896 & 265 & 1211 \\ 928 & 850 & 193 & 886 & 240 & 1062 \end{bmatrix} \tag{3.22}$$

3.4.2 Implementation of Decryption Algorithm

Implementation of decryption algorithm is applied on encrypted layers $V1$, $V2$ and $V3$.

1. Firstly, a 3D CCS is itrated and take bitwise XOR with encrypted layers and get D_1, D_2 and D_3.

$$D_1 = \begin{bmatrix} 846 & 548 & 824 & 497 & 510 & 364 \\ 902 & 465 & 671 & 440 & 475 & 383 \\ 855 & 526 & 661 & 367 & 501 & 425 \\ 898 & 710 & 791 & 511 & 529 & 407 \\ 948 & 618 & 814 & 553 & 554 & 382 \\ 827 & 709 & 733 & 454 & 530 & 397 \end{bmatrix} D_2 = \begin{bmatrix} 718 & 576 & 845 & 730 & 916 & 892 \\ 695 & 631 & 797 & 652 & 924 & 863 \\ 635 & 612 & 841 & 653 & 938 & 854 \\ 727 & 642 & 969 & 816 & 940 & 1063 \\ 914 & 706 & 865 & 750 & 886 & 1068 \\ 750 & 635 & 900 & 742 & 833 & 1040 \end{bmatrix} \tag{3.23}$$

$$D_3 = \begin{bmatrix} 845 & 804 & 278 & 834 & 242 & 908 \\ 797 & 779 & 242 & 762 & 231 & 946 \\ 841 & 738 & 217 & 720 & 169 & 910 \\ 969 & 913 & 240 & 915 & 237 & 993 \\ 865 & 958 & 298 & 930 & 296 & 1178 \\ 900 & 881 & 226 & 852 & 209 & 1031 \end{bmatrix} \tag{3.24}$$

2. Iterate the brownian motion, absolute and modulus function is applied to get U_1, U_2, U_3.

$$U_1 = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 2 & 2 & 1 & 2 & 0 \\ 1 & 2 & 0 & 0 & 0 & 1 \\ 1 & 0 & 2 & 0 & 1 & 1 \\ 2 & 1 & 1 & 2 & 0 & 0 \\ 2 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} U_2 = \begin{bmatrix} 2 & 0 & 0 & 1 & 0 & 1 \\ 2 & 2 & 1 & 0 & 0 & 2 \\ 0 & 0 & 2 & 2 & 1 & 2 \\ 1 & 0 & 1 & 1 & 2 & 0 \\ 0 & 1 & 2 & 2 & 2 & 2 \\ 1 & 2 & 1 & 0 & 2 & 1 \end{bmatrix} U_3 = \begin{bmatrix} 0 & 1 & 1 & 2 & 1 & 2 \\ 1 & 2 & 0 & 0 & 0 & 2 \\ 2 & 1 & 0 & 2 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 2 & 2 & 0 & 2 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 2 \end{bmatrix} \tag{3.25}$$

3. Taking the inverse of U_1, U_2, U_3 and is multiplied with D_1, D_2 and D_3 and results are stored in G.

$$G = \begin{bmatrix} 104 & 117 & 88 & 174 & 138 & 102 \\ 110 & 88 & 84 & 132 & 121 & 167 \\ 67 & 96 & 116 & 150 & 102 & 159 \\ 99 & 136 & 150 & 141 & 138 & 116 \\ 180 & 141 & 110 & 118 & 116 & 154 \\ 110 & 146 & 159 & 116 & 99 & 122 \end{bmatrix} \tag{3.26}$$

4. Divide the image G into four blocks g_1, g_2, g_3, g_4 and each block have same size of 3×3.

$$g_1 = \begin{bmatrix} 104 & 117 & 88 \\ 110 & 88 & 84 \\ 67 & 96 & 116 \end{bmatrix} g_2 = \begin{bmatrix} 174 & 138 & 102 \\ 132 & 121 & 167 \\ 150 & 102 & 159 \end{bmatrix} \tag{3.27}$$

$$g_3 = \begin{bmatrix} 99 & 136 & 150 \\ 180 & 141 & 110 \\ 110 & 146 & 159 \end{bmatrix} g_4 = \begin{bmatrix} 141 & 138 & 116 \\ 118 & 116 & 154 \\ 116 & 99 & 122 \end{bmatrix} \tag{3.28}$$

5. Iterate the 2D HCM using initial keys and reshape it into size of 3×3 and use it as row and column back circular shift process.

6. Decrypted four blocks $M1$, $M2$, $M3$ and $M4$ is obtained.

$$M1 = \begin{bmatrix} 138 & 102 & 174 \\ 132 & 121 & 167 \\ 159 & 150 & 102 \end{bmatrix} M2 = \begin{bmatrix} 117 & 88 & 104 \\ 110 & 88 & 84 \\ 116 & 67 & 96 \end{bmatrix} \tag{3.29}$$

$$M3 = \begin{bmatrix} 136 & 150 & 99 \\ 180 & 141 & 110 \\ 159 & 110 & 146 \end{bmatrix} M4 = \begin{bmatrix} 138 & 116 & 141 \\ 118 & 116 & 154 \\ 122 & 116 & 99 \end{bmatrix} \tag{3.30}$$

7. After shuffling and combining these blocks plainimage M is obtained.

$$M = \begin{bmatrix} 138 & 116 & 141 & 136 & 150 & 99 \\ 118 & 116 & 154 & 180 & 141 & 110 \\ 122 & 116 & 99 & 159 & 110 & 146 \\ 117 & 88 & 104 & 138 & 102 & 174 \\ 110 & 88 & 84 & 132 & 121 & 167 \\ 116 & 67 & 96 & 159 & 150 & 102 \end{bmatrix} \tag{3.31}$$

Chapter 4

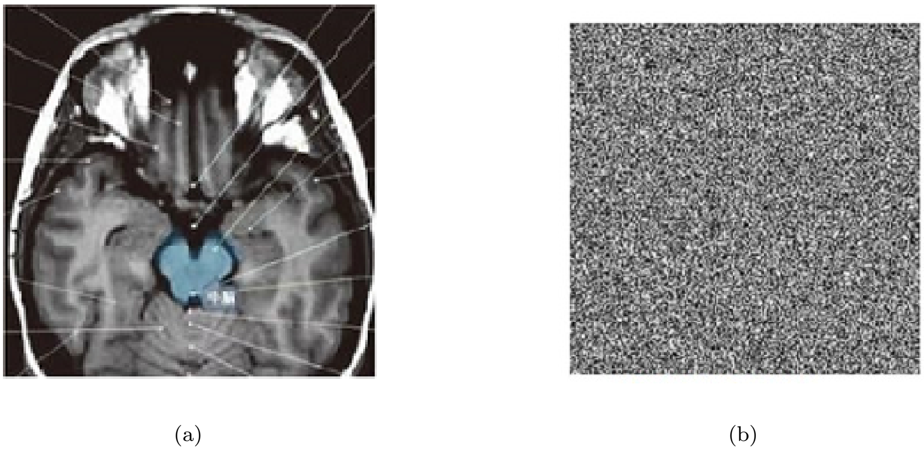
Security Analysis

The efficiency and security of scheme presented in Chapter 3 is checked by a variety of tests that are commonly utilized to analyse the statistical measurements and confidentiality of cryptosystems. This efficiency is done by histogram analysis, correlation analysis, differential anaylsis and entropy analysis.

4.1 Histogram Analysis

A histogram may used to visualise the statistical data that appears many times in an image. This analysis must show uniform behaviour and with no abrupt peaks which indicates that encryption is more secure and efficient.

This program is applied on different grey medical images like brain MRI and Chest X-ray. brain MRI original image and encrypted image are shown in Figure 4.1

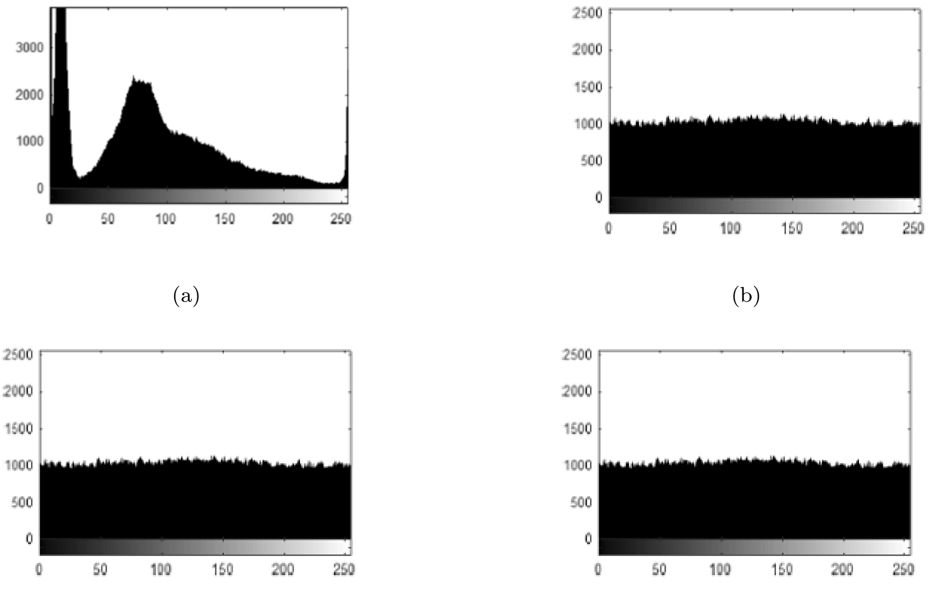


(a)

(b)

FIGURE 4.1: MRI original image and encrypted image

Histogram of brain MRI orignal image is shown in Figure 4.2 (a) and histogram of three encrypted images are shown in Figure 4.2 (b, c, d).



(a)

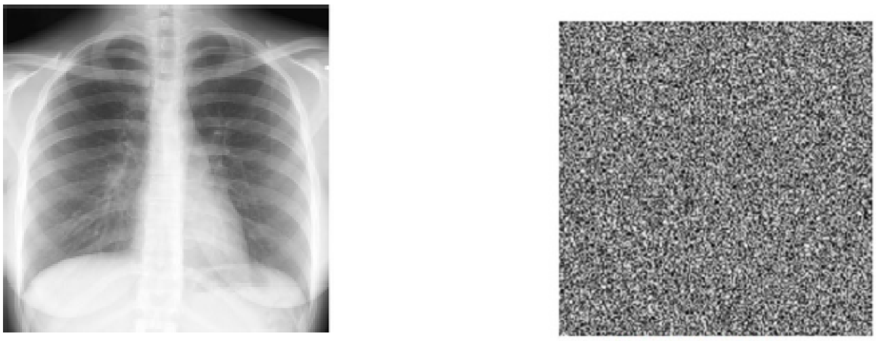
(b)

(c)

(d)

FIGURE 4.2: Histogram (a) shows original brain MRI image. Figure (b, c, d) shows the histogram of three encrypted image

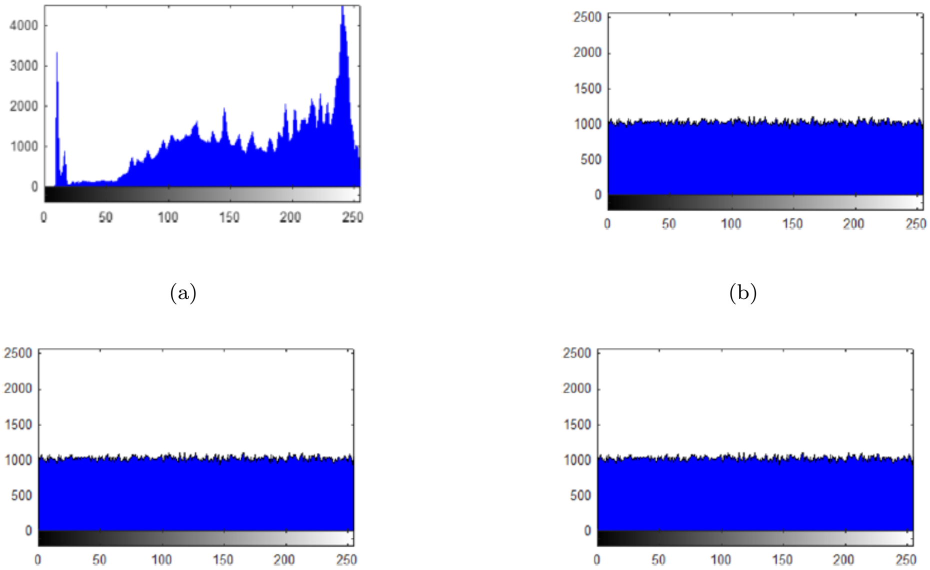
Chest X-ray original image and encrypted image are shown in Figure 4.3. Histogram of chest X-ray orignal image is shown in Figure 4.4 (a) and histogram of three encrypted images are shown in Figure 4.4 (b, c, d). Figure 4.2 (a) and 4.4 (a) does not show uniform behaviour but in Figure 4.2 (b, c, d) and 4.4 (b, c, d) encrypted images show uniformly. As a result, the findings of these tests have passed the security test of the proposed cryptosystem.



(a)

(b)

FIGURE 4.3: Chest X-ray original image and encrypted image



(a)

(b)

(c)

(d)

FIGURE 4.4: Histogram (a) shows original chest X-ray image. Histogram (b, c, d) shows encrypted image along H, I and J respectively

4.2 Pearson's Coefficient Correlation

Correlation between adjacent pixels is used for demonstrating encrypted data's diffusion and confusion features. The correlation is measured by using pearson's coefficient correlation. Encryption technique which is applied on any plain-image should achieve weak correlation between adjacent pixel of encrypted image. The correlation of plain-image and encrypted-image (through vertically, horizontally, and diagonally directions) is determined from following formulas when we compare them as follows:

$$\begin{aligned}
U(t) &= \frac{1}{m}\sum_{h=1}^{m} t_h \\
V(t) &= \frac{1}{m}\sum_{h=1}^{m} (t_h - U(t))^2 \\
W(s,t) &= \frac{1}{m}\sum_{h=1}^{m} (s_h - U(s))(t_h - U(t)) \\
\delta_{st} &= \frac{W(s,t)}{\sqrt{V(s)V(t)}}
\end{aligned} \tag{4.1}$$

where s and t show the value of grey scale, $U(t)$ is expected mean value and their correlation coeffient is δ_{st}.

Sr. #	image	Plainimage Dimension			Cipherimage Dimension		
		Hzt Dim	Dia Dim	Ver Dim	Hzt Dim	Dia Dim	Ver Dim
1.	chest-H direction	0.9987	0.9974	0.9986	0.0024	-0.0008	0.0008
2.	chest-I direction	0.9987	0.9974	0.9986	-0.0011	0.0020	-0.0003
3.	chest-J direction	0.9987	0.9974	0.9986	-0.0034	0.0015	0.0004
4.	MR-H direction	0.9851	0.9782	0.9882	0.0022	-0.0015	0.0066
5.	MR-I direction	0.9851	0.9782	0.9882	0.0011	0.0007	0.0057
6.	MR-J direction	0.9851	0.9782	0.9882	0.0021	-0.0023	0.0051

Here, Hzt Dim= Horizonal Dimension, Dia Dim=Diagonal Dimension, Ver Dim=Vertical Dimension

Table 4.1: PCC results for each dimension

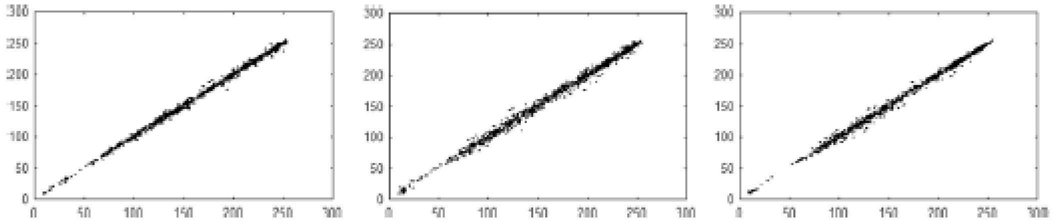


Figure 4.5: Pixel correlation of chest x-ray along all three directions

shows dimension wise different values. The range of correlation coefficient is between -1 to 1, where 1 illustrate the exact similarity between two images or pixels. For the scenario of highest random pixel, it is necessary to get a value close to 0. For various healthcare imaging, the pixel resemblance or discrepancy between plaintext and ciphertext is evaluated. The visual results given in Figure 4.5 reflect all three directions of image which shows pixel is combine in diagnoal form. These results discribe the highest similarity of pixels. The pixels diffuses in all directions when pixel have no similarity between them as shown in Figures 4.6, 4.7 and 4.8. It is clear from the Table 4.1 that plainimage values of chest and

MR are aproximately 0.9981, 0.9702, 0.9837 very close to 1 which shows its strong correlation. While in case of cipherimage of chest and MR are $(0.0016, 0.0018)$. These encrypted values are lie in between 0 and -1 which prove our system.

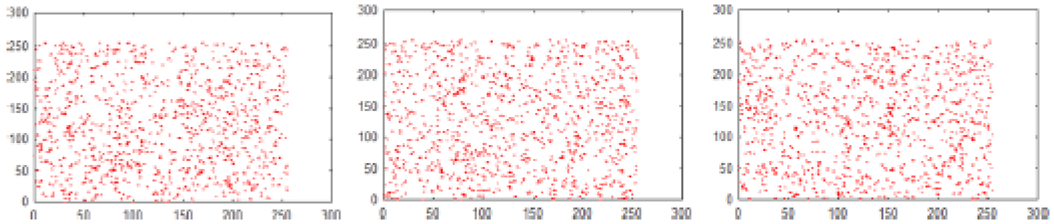


FIGURE 4.6: Pixel correlation of chest x-ray along X-Horizontal, X-Diagonal, X-Vertical

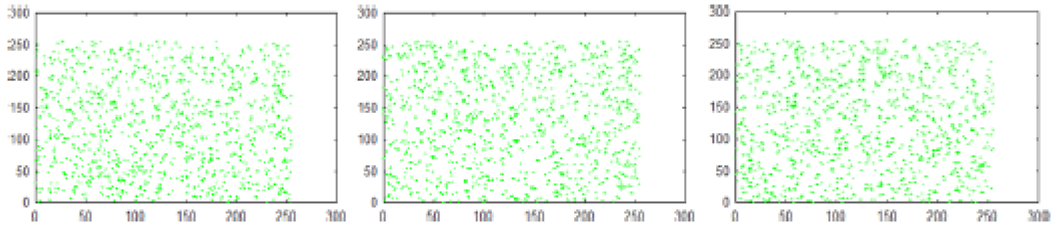


FIGURE 4.7: Pixel correlation of chest x-ray along Y-Horizontal, Y-Diagonal, Y-Vertical

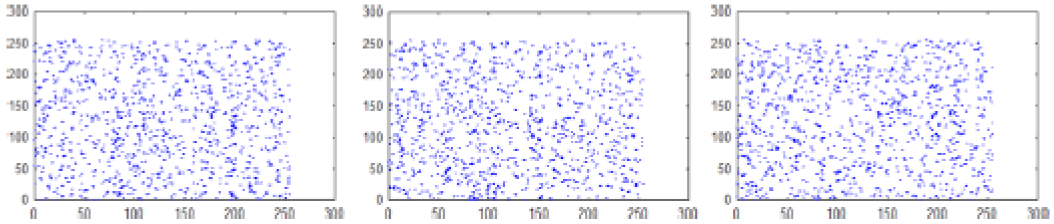


FIGURE 4.8: Pixel correlation of chest x-ray along Z-Horizontal, Z-Diagonal, Z-Vertical

4.3 Homogeneity, Energy and Contrast Analysis

- **Homogeneity**

  Homogeneity analysis can be used to quantify the closeness of gray level co-occurrence matrices elements . It shows statistical combinations of pixel luminosity. The encryption algorithm is cheap if the homogeneity value are low. Its values can be found by this formula.

$$H = \sum_{u,v=1}^{N} \frac{f(u,v)}{1+|x-y|}, \tag{4.2}$$

where f(u,v) is GLCM.

- **Contrast**

  Contrast is the difference in luminance or colour that allows viewers to distinguish between different things in a photograph. This analysis can be used to calculate the difference in luminosity between neighbouring pixels over the whole image. The contrast values shoud be higher for additional protection, as they reflect the number of unpredictability in the encrypted image.

$$C = \sum_{u,v=1}^{N} |x-y|^2 g(u,v), \tag{4.3}$$

  where $g(u,v)$is gray level co-occurrence matrice.

- **Energy**

  Energy may also determine from grey level co-occurrence matrices. Here we find the squared elements. The mathematical form of this analysis is given below:

$$E = q(u,v)^2, \tag{4.4}$$

where $q(u,v)$ is number of Gray Level Co-occurrence Matrice.

Results of homogeneity for images of chest x-ray and brain MRI are shown in Table 4.2. The found value of homogeneity are approximately near to 0.3904 along H, I and J direction. So low values obtained which show the efficiency of our proposed scheme.

Results of energy of images of chest x-ray and brain MRI are shown in Table 4.2. The found values of energy are approximately near to 0.0155. So results show the authentication of our system.

Results of contrast of images of chest x-ray and brain MRI are shown in Table 4.2.

The found value of contrast values are approximately near to 10.4976. So results show our system has access of good resistance to attacks.

Sr. #	image	direction	homogenity	energy	contrast
1.	Chest x-ray	H-direction	0.3891	0.0155	10.5304
2.	Chest x-ray	I-direction	0.3893	0.0155	10.4843
3.	Chest x-ray	J-direction	0.3898	0.0155	10.4781
4.	Brain MRI	H-direction	0.3934	0.0156	10.2802
5.	Brain MRI	I-direction	0.3935	0.0156	10.2777
6.	Brain MRI	J-direction	0.3933	0.0156	10.2947

Table 4.2: Average homogenity, energy and contrast values

4.4 Differential Attack Analysis

Encryption secheme has also ability to secure differential attacks. For the security of these attack there are two test named number of pixels changed rate (NPCR) and unify average changed intensities (UACI).

4.4.1 Number of Pixel Change Rate

NPCR test is used to determine the number of pixel change rate in two encrypted images, when there is a little change of just one pixel among their plain-text images. For calculation of this test mathematical formula is given below:

$$NPCR = \frac{\sum_{n,m} V(n,m)}{H \times K} \times 100\%, \tag{4.5}$$

where $V(n,m)$ shows pixels of encrypted image.

If two encrypted photographs have similar results, then $V(n,m) = 0$, but if they do not have, then $V(n,m) = 1$. Although the NPRC has a maximum value of

100 % but a strong cryptosystem should have an NPRC value of at least 99.5%. Our results are in between 99.58 to 99.62 as shown in Table 4.3.

4.4.2 Unified Average Change in Intensity

UACI test is used to determine the average change in intensity of two encrypted photos, while there is a one-pixel change among respective plain photos. For caluclation of this test methematical formula is given below:

$$UACI = \frac{1}{H \times K}[\sum_{p,q} \frac{|D_1(p,q) - D_2(p,q)|}{255}] \times 100\%, \tag{4.6}$$

where $D_1(p,q)$ and $D_2(p,q)$ represents the cipherimages whose plainimages are different by one pixel.

Table 4.3 shows the caculations of UACI. These results show that our system are highly secure.

Sr. #	image	directions	NPCR	UACI
1.	Chest x-ray	H	99.61	33.66
2.	Chest x-ray	I	99.62	34.61
3.	Chest x-ray	J	99.62	34.53
4.	Brain MRI	H	99.61	34.35
5.	Brain MRI	I	99.62	34.26
6.	Brain MRI	J	99.61	34.33

Table 4.3: NPCR and UACI values of different images

4.5 Entropy Analysis

In 1948 the concept of Entropy is given first time by Claude E. Shannon. Entropy is a fundamental tool to determine the randomness and unpredictable behaviour. As per Shannon, it defines the unpredictability across every communications network. Information entropy is matematically defined as:

$$K(n) = \sum_{q=0}^{2^M-1} p(n_q) \log_2 \frac{1}{p(n_q)}, \tag{4.7}$$

where $p(n_q)$ shows probability of n_q and M represent number of bits representing n_q. In any random number 2^Q, the entropy will be Q. Now any colorless picture have 2^8 gray steps, thus here eight is required entropy. Table 4.4 and 4.5 shows the calculations of chest x-ray and brain MRI images . The calculation of entropy shows that the suggested system has high entropy rate.

Sr. #	name	H-direction	I-direction	J-direction
1.	Real value	7.0888	7.0888	7.0888
2.	Absolute value	8.000	8.000	8.000
3.	Encrypted	7.9995	7.9994	7.9994

Table 4.4: Three dimensional entropy analysis of Chest image

Sr. #	name	H-direction	I-direction	J-direction
1.	Real value	7.0633	7.0633	7.0633
2.	Absolute value	8.0000	8.0000	8.000
3.	Encrypted	7.9985	7.9985	7.9985

Table 4.5: Three dimensional entropy analysis of brain MRI image

Chapter 5

Conclusion

In this chapter, the concluding views on the approach discussed in Chapter 3 [3] are presented.

1. In the present study, firstly a complete review of the work of masood et al. [3] on “A Lightweight Chaos Based Medical Image Encryption Scheme using Random Shuffling and XOR Operations” is described. For this purpose a secure and multi stages algorithm (for medical images using substitution and permutation methods) was introduced. This multi stage algorithm produces random numbers from chaotic maps and due to this randomness correlation between pixels of image has reduced.

2. The scheme combines the chaotic map with Brownian Motion (BM) and Chen’s chaotic system (CCS) and achieves the required security in hospital and other healthcare units. The confusion is achieved with the help of two dimensional (2D) Henon chaotic map (HCM) whereas diffusion is obtained by using BM and CCS. Furthermore, the implementation of the encryption Algorithm 3.3 is successfully done on MATLAB and the performed security analysis has provided the significant results.

3. At the receiver end, the cipherimage is decrypted by using decryption Algorithm 3.4 to get the plainimage back. In decryption algorithm, the receiver will use three operation, i.e XOR operation and modulation using secret keys to recover plainimage from the cipherimage.

4. Key is a very sensitive element in the encryption scheme, the image is encrypted using secret keys l_0, m_0, $l_0^{'}$, $m_0^{'}$ while in the decryption, if the same key is used only then the original image is obtained. As this scheme is symmetric so the secret keys are mutually shared through a secure channel. If a very small change of 10^{-14} in any of the key l_0, m_0, $l_0^{'}$, $m_0^{'}$ is done, then the real image cannot be obtained.

5. The information obtained through randomness test, the consistency and variance through hisogram examination and the pixel similarity using a coefficient of correlation. The results show that the proposed system outperform existing image encryption systems in terms of higher security. In addition, the proposed system requires less computational resources and at the same time, offer fast processing making it suitable for application in real-time encryption.

As a future direction, the proposed image encryption scheme by Masood et al. [3] can be modified in order to encrypt other media formats including audio and video.

Bibliography

[1] D. Sellars, “An introduction to steganography,” 2007.

[2] K. Kavitha, B. P. Shan, *et al.*, “An introduction to the digital watermarking,” *International Journal of Advanced Engineering Research and Science*, vol. 3, no. 6, p. 236763, 2016.

[3] F. Masood, M. Driss, W. Boulila, J. Ahmad, S. U. Rehman, S. U. Jan, A. Qayyum, and W. J. Buchanan, “A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations,” *Wireless Personal Communications*, pp. 1–28, 2021.

[4] D. N. Trivedi, N. D. Shah, A. M. Kothari, and R. M. Thanki, “Dicom® medical image standard,” in *Dental Image Processing for Human Identification*, pp. 41–49, Springer, 2019.

[5] A. H. Seh, M. Zarour, M. Alenezi, A. K. Sarkar, A. Agrawal, R. Kumar, and R. Ahmad Khan, “Healthcare data breaches: Insights and Implications,” in *Healthcare*, vol. 8, p. 133, Multidisciplinary Digital Publishing Institute, 2020.

[6] A. K. Singh *et al.*, “A survey of image encryption for healthcare applications,” *Evolutionary Intelligence*, pp. 1–18, 2022.

[7] P. F. Edemekong, P. Annamaraju, and M. J. Haydel, “Health insurance portability and accountability act,” 2018.

[8] P. Mahajan and A. Sachdeva, “A study of encryption algorithms AES, DES and RSA for security,” *Global Journal of Computer Science and Technology*, 2013.

[9] 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.

[10] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *International Journal of Bifurcation and chaos*, vol. 8, no. 06, pp. 1259–1284, 1998.

[11] T. Gao and Z. Chen, "A new image encryption algorithm based on hyper-chaos," *Physics letters A*, vol. 372, no. 4, pp. 394–400, 2008.

[12] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image and vision computing*, vol. 24, no. 9, pp. 926–934, 2006.

[13] L. Chierchia and J. N. Mather, "Kolmogorov-Arnold-Moser theory," *Scholarpedia*, vol. 5, no. 9, p. 2123, 2010.

[14] M. Sukharev-Chuyan, "The Lorenz system simulation," *Rivier Academic Journal*, vol. 9, no. 2, pp. 1–6, 2013.

[15] L. Billings and E. Bollt, "Probability density functions of some skew tent maps," *Chaos, Solitons & Fractals*, vol. 12, no. 2, pp. 365–376, 2001.

[16] M. Sciamanna and K. A. Shore, "Physics and applications of laser diode chaos," *Nature photonics*, vol. 9, no. 3, pp. 151–162, 2015.

[17] J.-g. Du, T. Huang, and Z. Sheng, "Analysis of decision-making in economic chaos control," *Nonlinear Analysis: Real World Applications*, vol. 10, no. 4, pp. 2493–2501, 2009.

[18] S. Ackerman and J. Knox, *Meteorology.* Jones & Bartlett Publishers, 2011.

[19] S. Phatak and S. S. Rao, "Logistic map: A possible random-number generator," *Physical review E*, vol. 51, no. 4, p. 3670, 1995.

[20] N. Raghava and A. Kumar, "Image encryption using Henon chaotic map with byte sequence," *International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR)*, vol. 3, no. 5, pp. 11–18, 2013.

[21] M. Yassen, "Chaos control of Chen chaotic dynamical system," *Chaos, Solitons & Fractals*, vol. 15, no. 2, pp. 271–283, 2003.

[22] A. G. Radwan and S. K. Abd-El-Hafiz, "Image encryption using generalized tent map," in *2013 IEEE 20th International Conference on Electronics, Circuits, and Systems (ICECS)*, pp. 653–656, IEEE, 2013.

[23] C. Liu, L. Liu, and T. Liu, "A novel three-dimensional autonomous chaos system," *Chaos, Solitons & Fractals*, vol. 39, no. 4, pp. 1950–1958, 2009.

[24] M. Sobottka and L. P. de Oliveira, "Periodicity and predictability in chaotic systems," *The American Mathematical Monthly*, vol. 113, no. 5, pp. 415–424, 2006.

[25] L. Min, L. Ting, and H. Yu-jie, "Arnold transform based image scrambling method," in *3rd International Conference on Multimedia Technology (ICMT-13)*, pp. 1302–1309, Atlantis Press, 2013.

[26] I. Karatzas and S. Shreve, *Brownian motion and stochastic calculus*, vol. 113. Springer Science & Business Media, 2012.

[27] 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.

[28] C. Zhu, S. Xu, Y. Hu, and K. Sun, "Breaking a novel image encryption scheme based on Brownian motion and pwlcm chaotic system," *Nonlinear Dynamics*, vol. 79, no. 2, pp. 1511–1518, 2015.

[29] J. L. Massey, "An introduction to contemporary cryptology," *Proceedings of the IEEE*, vol. 76, no. 5, pp. 533–549, 1988.

[30] G. Jindal, S. Baranwal, and M. Memoria, "Cryptography using multi-dimensional objects," in *International Conference on Advances in Engineering Science Management & Technology (ICAESMT)-2019, Uttaranchal University, Dehradun, India*, 2019.

[31] R. Sarkar, S. Banerjee, P. Sadhukhan, M. Majhi, A. Das, and R. Bhattacharyya, "An overview of cryptosystem,"

[32] A. ChandraSekhar, D. C. Kumari, and S. A. Kumar, "Symmetric key cryptosystem for multiple encryptions," *International Journal of Mathematics Trends and Technology (IJMTT)*, vol. 29, 2016.

[33] J. O. Grabbe, "The DES algorithm illustrated," 2010.

[34] G. Singh, "A study of encryption algorithms (RSA, DES, 3DES and AES) for information security," *International Journal of Computer Applications*, vol. 67, no. 19, 2013.

[35] M. Hellman, "An overview of public key cryptography," *IEEE Communications Society Magazine*, vol. 16, no. 6, pp. 24–32, 1978.

[36] V. S. Rajput, J. Keller, and P. Mor, "Secure cryptography with ngdh protocol along with RSA & AES algorithm," 2022.

[37] W. U. Khan, T. Ullah, H. K. Jadoon, and N. U. Arfeen, "Lightweight pretty good privacy email encryption,"

[38] D. S. Laiphrakpam and M. S. Khumanthem, "Medical image encryption based on improved elgamal encryption technique," *Optik*, vol. 147, pp. 88–102, 2017.

[39] S. Agrawal and D. Boneh, "Homomorphic macs: Mac-based integrity for network coding," in *International conference on applied cryptography and network security*, pp. 292–305, Springer, 2009.

[40] T. Syben, "Introduction to block cipher," *University of Bonn, Germany [cited 18 Feb. 2014], year=2011.*

[41] R. Verdult, "Introduction to cryptanalysis: Attacking stream ciphers," *Institute for Computing and Information Sciences Radboud University Nijmegen, The Netherlands, year = 2001.*

[42] C. Christensen, "Review of cryptography and network security: Principles and practice," *Cryptologia*, vol. 35, no. 1, pp. 97–99, 2010.

[43] F. Grieu, "A chosen messages attack on the iso/iec 9796-1 signature scheme," in *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 70–80, Springer, 2000.

[44] P. Goyal, S. Batra, and A. Singh, "A literature review of security attack in mobile Ad-hoc networks," *International Journal of Computer Applications*, vol. 9, no. 12, pp. 11–15, 2010.

[45] M. Babenko, N. Chervyakov, A. Tchernykh, N. Kucherov, M. Deryabin, G. Radchenko, P. O. Navaux, and V. Svyatkin, "Security analysis of homomorphic encryption scheme for cloud computing: Known-plaintext attack," in *2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, pp. 270–274, IEEE, 2018.

[46] W. K. Pratt, *Introduction to digital image processing.* CRC press, 2013.

[47] S. Sowmiya, I. M. Tresa, and A. P. Chakkaravarthy, "Pixel based image encryption using magic square," in *2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET)*, pp. 1–4, IEEE, 2017.

[48] N. Ritter, M. Ruth, B. B. Grissom, G. Galang, J. Haller, G. Stephenson, S. Covington, T. Nagy, J. Moyers, J. Stickley, *et al.*, "Geotiff format specification geotiff revision 1.0," *SPOT Image Corp*, vol. 1, pp. 154–172, 2000.

[49] J. Schönhut, "Formats," in *Document Imaging*, pp. 97–118, Springer, 1997.

[50] D. Barina and O. Klima, "Region of interest in jpeg,"

[51] G. E. James, "Chaos theory: The essentials for military applications," tech. rep., Naval war coll newport ri advanced research program, 1995.

[52] D. A. Hsieh, "Chaos and nonlinear dynamics: Application to financial markets," *The journal of finance*, vol. 46, no. 5, pp. 1839–1877, 1991.

[53] G. Williams, *Chaos theory tamed.* CRC Press, 1997.

[54] É. Ghys, "The butterfly effect," in *The Proceedings of the 12th International Congress on Mathematical Education*, pp. 19–39, Springer, Cham, 2015.

[55] Z. Qiao, *Nonlinear dynamics, applications to chaos-based encryption.* PhD thesis, École centrale de Nantes, 2021.

[56] A. Veres and M. Boda, "The chaotic nature of tcp congestion control," in *Proceedings IEEE INFOCOM 2000. Conference on Computer Communications. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies (Cat. No. 00CH37064)*, vol. 3, pp. 1715–1723, IEEE, 2000.

[57] S. Lian, "A block cipher based on chaotic neural networks," *Neurocomputing*, vol. 72, no. 4-6, pp. 1296–1301, 2009.

[58] 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, p. e0225031, 2019.

[59] R. Stoop and P. Meier, "Evaluation of lyapunov exponents and scaling functions from time series," *JOSA B*, vol. 5, no. 5, pp. 1037–1045, 1988.

[60] T. S. Ali and R. Ali, "A novel medical image signcryption scheme using TLTS and Henon chaotic map," *IEEE Access*, vol. 8, pp. 71974–71992, 2020.

[61] U. M. Roslan, Z. Salleh, and A. Kılıçman, "Solving Zhou chaotic system using fourth-order Runge-Kutta method," *World Applied Sciences Journal*, vol. 21, no. 6, pp. 939–944, 2013.

[62] G. Chen and T. Ueta, "Yet another chaotic attractor," *International Journal of Bifurcation and chaos*, vol. 9, no. 07, pp. 1465–1466, 1999.