CAPITAL UNIVERSITY OF SCIENCE AND
TECHNOLOGY, ISLAMABAD

A Chaotic Color Image Encryption Algorithm Based on Information Entropy

by

Khuzaima Nasir

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

in the

Faculty of Computing
Department of Mathematics

2021

Dedicated to

My Parents

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

CERTIFICATE OF APPROVAL

A Chaotic Color Image Encryption Algorithm Based on Information Entropy

by

Khuzaima Nasir

(MMT193033)

THESIS EXAMINING COMMITTEE

S. No.	Examiner	Name	Organization
(a)	External Examiner	Dr. Nasir Siddiqui	UET, Taxila
(b)	Internal Examiner	Dr. Mohammad Masroor Ahmed	CUST, Islambad
(c)	Supervisor	Dr. Rashid Ali	CUST, Islamabad

Dr. Rashid Ali
Thesis Supervisor
December, 2021

Dr. Muhammad Sagheer
Head
Dept. of Mathematics
December, 2021

Dr. M. Abdul Qadir
Dean
Faculty of Computing
December, 2021

Author's Declaration

I, **Khuzaima Nasir** hereby state that my MPhil thesis titled "**A Chaotic Color Image Encryption Algorithm Based on Information Entropy**" 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 M.Phil Degree.

Khuzaima Nasir

Registration No: MMT193033

Plagiarism Undertaking

I solemnly declare that research work presented in this thesis titled "**A Chaotic Color Image Encryption Algorithm Based on Information Entropy**" 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 M.Phil Degree, the University reserves the right to withdraw/revoke my M.Phil 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.

Khuzaima Nasir
Registration No: MMT193033

Acknowledgement

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

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

I am 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 Ali sajad**, **Muhammad Zeeshan** and **Shazia Ramzan** also helped me a lot and guided me whenever I needed it.

Khuzaima Nasir

Abstract

In this thesis, first the encryption of the chaotic image, based on information entropy by Ye et al. is reviewed. The encryption scheme is implemented using MATLAB, then the scheme is extended for the color images. This method contains permutation, modulation and diffusion operation. Information entropy is employed to influence the generation of the keystream. The initial keys used in the permutation and diffusion stages interact with each other. In the scheme a compound chaotic map namely, the two-dimensional logistic adjusted sine map, is used. The map is generated with the help of well known chaotic logistic map and sine map. As a result, the algorithm acts as an indivisible entity to enhance security. Experimental results and security analysis demonstrate the good performance of the algorithm as a secure and effective communication method for color images.

Contents

List of Figures

List of Tables

Abbreviations

AES	Advanced Encryption Standard
CRT	Cathode Ray Tube
DES	Data Encryption Standard
JPEG	Joint Photographic Experts Group
LE	Lyapunove Exponent
MRI	Magnetic Resonance Imaging
NPCR	Number of Pixel Changing Rate
PCC	Pearson Correlation Coefficient
PNG	Portable Network Graphic
PWLCM	Piece Wise Linear Chaotic map
PMD	Permutation Modulation Diffusion
RSA	Rivest – Shamir – Adleman
RC4	Rivest Cipher 4
SPN	Substitution Permutation Network
TIFF	Tagged Image File Format
UACI	Unified Averaged Changed Intensity
2D - LASM	Two Dimensional Logistic Adjusted Sine Map
3DES	Triple Data Encryption Standard

Symbols

A	Gray scale image
B	Color (RGB) Image
B_r	Red Channel of Color Image
B_g	Green Channel of Color Image
B_b	Blue Channel of Color Image
C	Ciphertext
C	Cipherimage
C_r	Red Channel of Cipherimage
C_g	Green Channel of Cipherimage
C_b	Blue Channel of Cipherimage
D	Decryption Algorithm
E	Encryption Algorithm
$I(\alpha)$	Information Entropy of α
K	Key
m	Number of Rows
n	Number of Columns
P	Plaintext
$p(\alpha)$	Probability of α
$\lceil \cdot \rceil$	Ceiling function of $\cdot$
log	Logarithm

Greek Letters

λ	Lyapunove Exponent

ς	Control Parameter of Logistic Map
σ	Control Parameter of Chaotic Sine Map
μ	Control Parameter of 2D-LASM
δ_{yz}	Pearson Correlation Coefficient

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. Then the think tanks of such states sit together to evolve a mechanism to secure the relevant secret message sending from them to their loyal ones. In the modern age the technology used for cryptography provides the solution for securing secret information/message. The method of securing data during its communication, so that only the person to whom the information is intended can read, change and process it. In cryptography the original message is known as **plaintext** (P) and **ciphertext** (C) is the codded message. **Encryption algorithm** (E) is the algorithm that is used to convert the plaintext into ciphertext using the key. **Decryption algorithm** (D) is the algorithm that is used to convert the ciphertext into plaintext using the secret key. On the basis of the key, cryptography is divided into symmetric key cryptography (secret key cryptography) and asymmetric key cryptography (public key cryptography). **Symmetric key cryptography** is a cryptography technique in which encryption/decryption is done by a single confidential key. **Asymmetric key cryptography** is cryptographic technique in which encryption/decryption is done by two different keys one is public key and other is secret key. The simplest cryptographic scheme is **caesar cipher** (shift cipher) [1]. In the shift cipher each letter in the plaintext is replaced by a letter located at a fixed number of positions down the alphabet. There are many other cryptographic technique such as Hill cipher [2], AES [3], RSA [4] etc. Nowadays most of cryptographic scheme rely on

dynamic structure (chaos theory) due to its cryptographic supporting properties further detail is given in the next section.

1.1 Image Encryption

An image is a piece of art that depicts visual perception, such as a photograph or other two-dimensional representation. It is defined as two variable function $f(x, y)$ where every position (x, y) in the projection plane is the light intensity at this point. There are two type of images Analog image and Digital image. The **Analog image** is mathematically represented as a continuous range of value representing position and intensity. For example the produced image on the screen of CRT monitor is analog. The **Digital image** is composed of the picture element known as Pixel. Pixels are the smallest representation of an image, which represent the brightness at a point. It plays an important role in the daily life such as satellite television, magnetic resonance imaging as well as in the research such as astronomy and geographical information system.

Image encryption is the process of encoding an image with the help of some encryption algorithm. CT scans and MRI images are used to diagnose abnormal symptoms. When patients seek a second opinion, they frequently face the challenge of maintaining their privacy while also ensuring the secure transmission of their CT or MRI images. However, with the advancement of technology and the development of image encryption algorithms, transmitting and receiving images has become much easier. Moreover, an open platform such as the internet may not always be safe for transmission. Military and medical images are sensitive and should be kept out of the hands of unauthorized users. As a result, a secure image sharing method that ensures safe image transmission is required. Cryptography is playing an important role to achieve a secure image sharing method that ensures safe image transmission. There are many methods for image encryption have been developed as a result of its growing popularity and necessity. As image is totally different from the text due to their characteristic such as strong correlation analysis, bulky data capacity, etc. So the well known methods such as advanced

encryption standard (AES), international data encryption algorithm (IDEA), are always not efficient [5].

1.2 Literature review

The field of chaotic dynamics research advanced rapidly during the 1960s and 1970s. Around 1960, Arnold, Kolmogorov and Moser proposed the famous KAM theorem [6]. KAM theorem based on the study of motion stability in the Hamiltonian system, which laid the basis for chaos theory. In 1963, Lorenz[7], proposed a three-dimensional (3D) autonomous system to describe weather change. This is the well-known Lorenz system, which was the first chaos model to be mathematically described. He discovered that the evolution of weather was closely intertwined to the initial conditions. In other words, a small change in the initial condition will result in a significant difference in the output, which is a characteristic of chaos: high sensitivity to the initial condition. He also described this behavior as **Butterfly effect**. In 1971, Ruelle and Takens [8] used chaos to explain the nature of turbulence for the first time. They discovered a particularly complex new attractor in the dynamic system and coined it as **strange attractor**. They also used it in a dissipative system to show that the motion associated with this strange attractor is chaotic. Li and Yorke [9] introduced **chaos** in their paper. After that the term chaos has been officially used in the scientific community. Since 1990s the study of chaotic dynamics has rapidly developed. Numerous researches have been carried to investigate the theoretical properties of chaotic systems [10–12]. Today, chaos theory is important not only in meteorology, turbulence, and biology, but also in many other fields such as mathematics, physics [13], economics [14, 15], etc.

Chaos theory has caught the interest of the cryptography community due to its deterministic nature, randomness, sensitive to initial condition and unpredictability [16]. Since 1990, many studies on digital chaotic cryptography have been proposed, such as chaotic block ciphers [17–21], chaotic cryptography hash functions

[22–24] , and chaotic pseudorandom number generators [25–27]. In general, when tested against known cryptanalysis techniques, chaos theory provides a base for secure algorithm. Cryptographers have used dynamic chaotic systems to create new cryptographic primitives by utilizing chaotic maps such as logistic maps [28], Henon maps [29], and Tent maps [30]. There are some method of image encryption such as chaos system [31], Arnold transform [32], fractional fourier transform [33], elliptic curve AES system [34], wavelet transform [35] etc.

A chaos based image encryption is used to protect the image content [36–38]. However, due to the nonlinearity, nonperiodicity, nonconvergence, ergodicity, and sensitivity to the initial conditions in chaotic maps (or systems) [39]. The design/applications of chaos have piqued the interest of many researchers [40, 41].

In 1998, Fridrich [42] proposed a chaotic image encryption scheme based on permutation and diffusion, in which permutation algorithm is applied on the plainimage to shuffle the pixel location. Hence the permuted image become unreadable. However, only by applying permutation on the plainimage would not change the statistical properties of the plainimage. It is easy to break the permuted image by using inverse permutation algorithm. In Fridrich's structure, diffusion is further extended to modify gray levels by using to a pseudorandom sequence. The main goal is to achieve the avalanche effect, *i.e.*, one bit change in the plainimage results in a significant difference in the cipherimage. Afterward, many image encryption scheme based on chaos [43, 44] adopted diffusion-permutation framework. For example, an image encryption based on permutation-diffusion using XOR operator and a crossover was proposed in [45]. The confusion and diffusion is placed in the one step for the fast implementation of the image encryption algorithm [46].

Chaos based image encryption scheme is insecure under some attacks. For example the scheme proposed by Wang et al [47] the scheme is then cryptanalyzed by [48] as Monte Carlo method is used to simulate brownian motion to scramble the plainimage pixels. Then diffusion operation is applied to permute the image by using PWLCM (Piece Wise Linear Chaotic Map). Chosen plaintext attack is applied on encryption algorithm to get a diffusion sequence and permutation

vector.

Therefore, the algorithm becomes insecure for encryption.

On the basis of cryptanalysis, there are some factor that shows the lack of the security in the encryption algorithm which are as follows:

- The keystream used in the encryption is created independent of the plain-image.
- Permutation-based image encryption.
- Diffusion only encryption.
- There is no change in the pixel distribution prior to the diffusion operation.

To address the above mentioned shortcomings and to improve the security of the encryption algorithm, a method for image encryption [49] is proposed. In both steps of encryption, that is, the permutation and diffusion, key-streams are generated based with the help of the plainimage. For the pixel distribution a modulation operation is introduced between permutation and diffusion. As a result, the scheme using permutation, modulation, and diffusion (PMD) for image encryption provides a secure way for image communication.

1.3 Thesis Contribution

In this dessertation, an encryption scheme presented by Ye et al in [49] is reviewed. Information entropy and the initial keys are used to generate an updated keys. Updated keys are further used to iterate chaotic map. In this scheme, a compound chaotic map two- dimensional logistic adjusted sine map(2D-LASM) [44] is used, which is generated with the combination of logistic map [50] and sine map to improve the chaotic properties. A gray scale image encryption and decryption of the scheme [49] is discussed. Firstly, circular permutation is applied on the gray scale image. Then, apply the modulation operation on the permuted image. At

the end, diffusion is applied on it. 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 gray scale image is achieved. The scheme is successfully implemented on the MATLAB to encrypt and decrypt the grayscale image, the security analysis of the scheme such as key sensitivity and statistical analysis is also determined. After successful implementation of the reviewed scheme [49] for the grayscale image on MATLAB, it is then extended for color image, by utilizing information entropy of its red (R), green (G) and blue (B) channels.

In the color image encryption, the encryption scheme first converts the color image into three channels (red, green, blue). Then operate the encryption algorithm on each channel to get the cipherimages of channels. After getting the cipherimage of each channel combine them to get the color cipherimage. As mentioned above that the scheme is symmetric so the decryption is done in the reverse order *i.e.*, inverse diffusion, modulation and circular permutation. The security analysis of the extended scheme provides good result and is discussed in Section 4.3.

1.4 Thesis Layout

In This dessertation, a review of Chaotic image encryption scheme [49] for gray scale image and further encryption scheme is then extended for color (RGB) image. The main contribution of the thesis presented in different chapters are summarized below:

- **Chapter 2** shows the basic introduction to the cryptology in which fundamental concepts of the cryptography, some properties of cryptography are presented. Then, detail on cryptosystem and cryptanalysis are discussed. After that few mathematical structure which are used in the encryption scheme are addressed. Then the brief introduction on chaos theory and chaotic maps that are used to generate the 2D-LASM is given.

- **Chapter 3** the review of an article "A chaotic image encryption algorithm based on information entropy" by Ye et al. [49] is presented. For that purpose, the chaotic map 2D-LASM, information entropy and the encryption/decryption is discussed in detail. At the end, security analysis of the scheme is discussed.

- **Chapter 4** a review of the scheme [49] is discussed in Chapter 3 is then extended to "A chaotic color image encryption scheme based on information entropy". Furthermore, security analysis of the extended scheme is discussed.

- **Chapter 5** The conclusion of the above work is given in this chapter also some future work is given.

Chapter 2

Preliminaries

Cryptography is becoming extremely important in the digital world for providing services such as encryption, digital signature and key establishment etc. In this chapter, the introduction is given first to the cryptography in Section 2.1, which includes some fundamental concept of cryptography, properties of cryptography, cryptosystem. Then the Cryptanalysis and some common cryptographic attacks is described in Section 2.2. In Section 2.3 some terminologies related to image encryption are discussed. The detailed description of chaos theory is in Section 2.4. The Section 2.5 is about the introduction of chaotic maps such as logistic map and sine map. Finally, the chaos and cryptography is discussed in Section 2.6

The term 'cryptology' is a combination of the Greek words 'kryptos' (hidden) and 'logos' (words). Cryptology is an all-inclusive term that includes cryptography, cryptanalysis, and the interaction between them [51]. As depicted in Figure 2.1.

2.1 Cryptography

'Cryptography' provides the methods of secure communication in which the information used to the person to whom the information is intended can read, change and process it. The prefix 'crypt' means hidden, and the suffix 'graphy' means

writing so cryptography means 'covered writing'. In cryptography the term 'plaintext' refers to a secret message that the sender wishes to transmit. Plaintext cannot be sent in its original form instead, it is converted into a form that cannot be understood and then sent to its intended recipient. The codded message that cannot be understand by the intended recipient is known as 'Ciphertext'. The method that convert plaintext to ciphertext is 'Encryption' whereas 'Decryption' is the process of converting ciphertext back to plaintext. 'Encrption Algorithm' is the algorithm that is used to convert plaintext into ciphertext using secret key. The algorithm used to extract the plaintext from the ciphertext with the help of secret key is known as the 'Decryption Algorithm'. The conversion of plaintext to ciphertext and vice versa is accomplished with the assistance of a highly sensitive information known as 'Key'. This key must be kept secret throughout this process because the security of the entire communication depends on it.

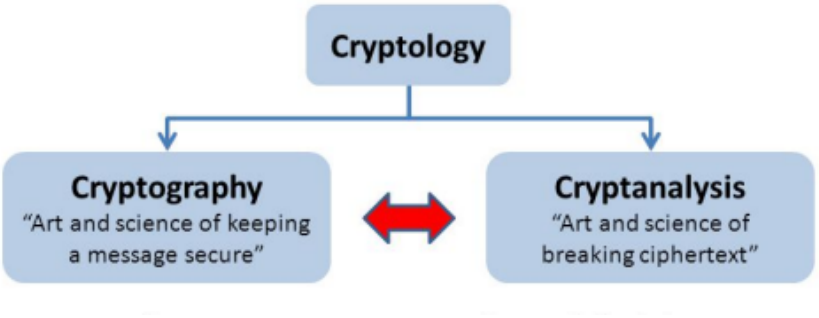


FIGURE 2.1: Types of Cryptology

2.1.1 Cryptosystem

In cryptography, a cryptosystem is a structure or scheme consisting of a set of algorithms that converts plaintext to chipertext to securely encode or decode messages. The term cryptosystem is an abbreviation for cryptographic system and refers to a computer system that employs cryptography. A method of protecting information and communication by using code so that only intended person can process the information. A cryptosystem includes algorithms for key generation, encryption, and decryption to help keep data secure.

- **Components of Cryptosystem**

  There are five basic component of cryptosystem which are listed below:

  (a) Plaintext (P)

  (b) Ciphertext (C)

  (c) Encryption Algorithm (E)

  (d) Decryption Algorithm (D)

  (e) Key (K)

- **Types of Cryptosystem**

  The secret key for encryption and decryption may be the same or different. This depends on the type of cryptosystem. Cryptosystems are typically divided into two categories:

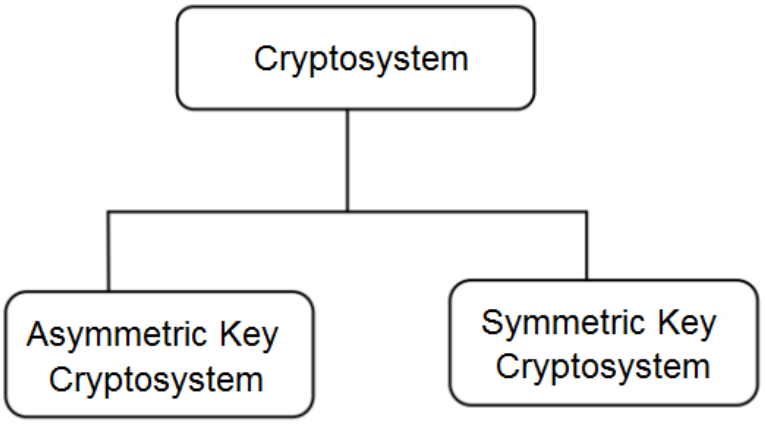


FIGURE 2.2: Types of Cryptosystem

1. Symmetric Key Cryptosystem (Secret Key Cryptosystem)
2. Asymmetric Key Cryptosystem (Public Key Cryptosystem)

1. **Symmetric Key Cryptosystem**

   The Symmetric key cryptosystem is also known as secret Key cryptosystem. Symmetric key cryptography is a type of encryption/decryption that uses a single confidential key to cipher and decipher message. It is used to convert the plain message into a ciphered message that uses a confidential key. The

key can be a number or a word that is included with the plain message. Two parties use identical keys for encryption/decryption in the secret key cryptosystem. This key may also be used to obtain the decryption results for an encrypted message. Until 1976, this was the only method of secure communication.

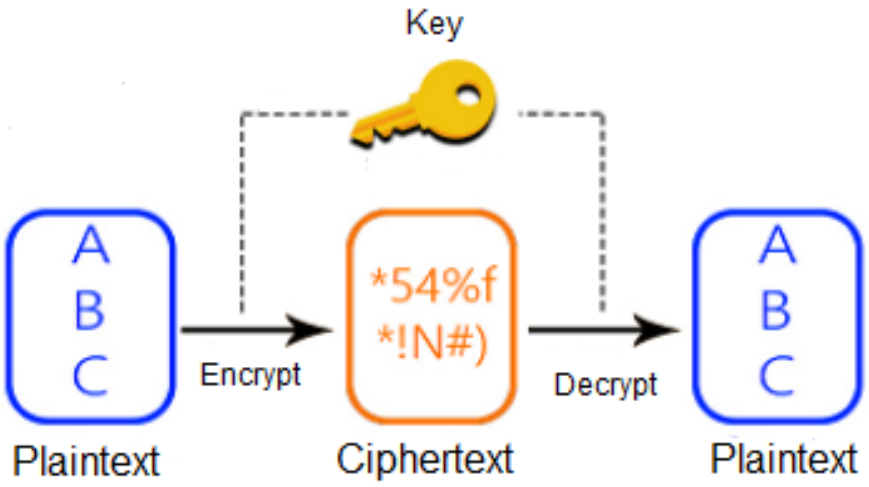


FIGURE 2.3: Symmetric Key Cryptosystem

For communication, consider two parties: Ayesha and Badar. Ayesha wishes to communicate with Badar over an insecure channel, such as the Internet. Ayesha employs a secret key, which she must share with Badar, that will be used in encryption algorithm. She now sends the encrypted text to Badar over the internet and shares that key with him trough a secure channel. When Badar receives both the text and the key, he can easily decrypt the text using the decryption algorithm. To send the key to the designated receiver, a secure channel is required. Otherwise security cannot be achieved. The two main issues with symmetric key cryptosystem are key management and the use of the same key by the sender and receiver. AES [3] , RC4 [52] , DES [53] and 3DES [54] are examples of symmetric key-based cryptographic schemes. There are two main drawback of Symmetric Key cryptosystem which are as follows:

i) **Key Sharing**

When there are 'n' people communicating with each other, key distribution becomes a problem. If any person reveals the key, the entire communication will be at risk.

ii) **Authentication**

Authentication is another major issue in symmetric key cryptosystems. If Ayesha and Badar communicate with each other and the man in the middle (known as Eve) intercepts or guesses the key and initiates communication, the cryptosystem cannot determine whether or not he/she is an authentic user.

2. **Asymmetric Key Cryptography**

Diffie-Helman [55] proposed asymmetric key cryptosystem in 1976 to solve problems that appear in symmetric key cryptosystem. The invention of asymmetric key cryptosystem is the most significant achievement in the history of cryptography. The theory they proposed is based on a one-way trapdoor function (A trapdoor function is one that is simple to compute in one direction but difficult to compute in the opposite way (identifying its inverse) without particular information. In cryptography, trapdoor functions are commonly used.) that allows two parties to exchange keys. Asymmetric key cryptosystem enables the communicant to generate an encryption key that is accessible to all, while decryption keys are kept secret. From the beginning to the present, almost all cryptosystems had been relied on permutation and substitution. In addition to substitution and permutation techniques, the asymmetric key cryptosystem also used mathematical functions to operate.

Generally, Asymmetric encryption employs two keys: 'Key 1' for encryption and 'Key 2' for decryption. The encryption key is accessible to public, but the decryption key must be kept private. There is no need to send the key to the designated receiver over a secure channel. It is critical to understand that anyone who has the access to the confidential key can decrypt the text, that is why two related keys are used for boosting the security. The public

key is made widely available so that anyone who wishes to send a text message can do so. However, only the owner knows the decryption key and thus has access to the original message. That's how asymmetric key cryptosystem addresses the issues raised by symmetric key cryptosystem.

The use of a secure channel to share the decryption key is no longer required. To improve the security, the owner of the private key can now ensure that they have full authority to decipher the text. ElGamal [56], RSA [4], etc are the examples of asymmetric key cryptosystem.

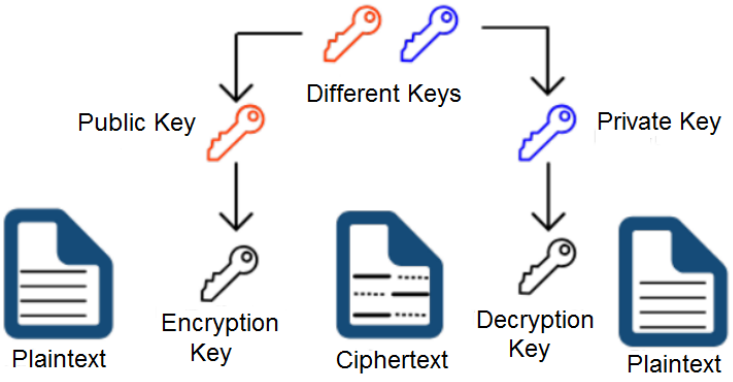


FIGURE 2.4: Asymmetric Key Cryptosystem

2.1.2 Security Services of Cryptography

The primary goal of using cryptography is to provide the four fundamental information security services listed below. Let us now look at the various goals that cryptography might be able to achieve.

1. **Confidentiality**

   Data confidentiality and privacy are implied by confidentiality. The original information about the data is known only to the sender and receiver. There are no one who can understand the transmitted information except intended person. Confidentiality refers to the situation in which someone knows the secret information but is unable to obtain the original data.

2. **Integrity**

   During information transmission, integrity ensures that the message is not

altered or modified. For example, if Ayesha sends encrypted data to Badar, integrity ensures that the data is not altered or changed during transmission or storage, and it leads Badar to believe that the data is in its original form.

3. **Authentication**

   A cryptographic scheme also includes authentication. It allows the sender's or recipient's identity to be verified. It ensures that the data is taken from a reliable source. It correctly identifies the source of the message and the transmitter or receiver. As a conclusion, it ensures that the transmitter and acceptor verify each other. Consider the case, where Ayesha and Badar use a proper algorithm to communicate securely. In order to avoid being tricked, they must be able to verify each other's identities using a cryptographic scheme. The authentication property assists participants in ensuring that they are communicating with one another rather than the attacker.

4. **Non-Repudiation**

   Non-repudiation means that the source of the information cannot refuse by sending the information later. If Badar sends the information, there is no way for Badar to later deny it. This helps the receiver gain the trust of the sender in any cryptographic protocol.

2.2 Cryptanalysis

Cryptanalysis [2] is a method for analysing the security of encrypted data without having access to the confidential information required. It is a method of obtaining plaintext from ciphertext without knowing the key. The analysed data is used to investigate the system's hidden points. Someone who attempts to perform this task is known as a cryptanalyst. Cryptanalyst uses an algorithm to decrypt ciphertext without knowing the plaintext sources or encryption keys. A cryptanalyst also works to improve the existing techniques by identifying flaws in a security protocol. This can be accomplished by locating the key and improving the methods if they are lacking in the four properties of confidentiality, integrity, authentication,

and non-repudiation. If a system lacks any of the four properties, the communication's security is compromised, and the ciphertext is easily decrypted.
Crypatanalysis is carried out by two types of attacks active and passive. A cryptanalyst must defeat some cryptographic mechanism in order to conduct cryptanalysis.

1. **Passive Attack**

   In this attack [57], a cryptanalyst attempts to break the system independently based on observed data while he is unable to interact with any of the communicators.

2. **Active Attack**

   The cryptanalyst modifies the communication in this attack [58]. He attempts to uncloak the key by creating, forging, altering, replacing, blocking, or rerouting communication.

There are multiple cryptographic attacks, some of which are discussed here.

1. **Ciphertext only Attack**

   An attack in which the attacker uses a collection of known ciphertexts to try to decipher the original text or key. The main point to remember about this attack is that the cryptanalyst has no knowledge of the original message, so he uses ciphertext or an algorithm to obtain the plaintext.

2. **Plaintext Attacks**

   A cryptanalyst knows the ciphertext with the corresponding known partial plaintext in this type of attack. Using this knowledge, he attempts to develop an efficient algorithm for decrypting any ciphertext as well as the key of its corresponding plaintext.

3. **Chosen Plaintext Attacks**

   Chosen plaintext attack means that the cryptanalyst uses the same algorithm on ciphertext that matches arbitrarily with the selected plaintext. He obtains the ciphertext for any arbitrarily chosen plaintext by employing the proper

algorithm. Using these plaintexts and ciphertexts, he attempts to recover the key.

4. **Chosen Ciphertext Attacks**
   This is equivalent to selected pliantext attacks. The attacker gathers information using ciphertext in this attack. He obtains the plaintext of the chosen ciphertext and then attempts to deduce the secret key from these results.

5. **Brute Force Attack**
   In this type of attack, the attacker has no knowledge of the plaintext from the ciphertext. He tries every possible guess to extract the key from the ciphertext. This attack can be made more difficult by increasing the key space.

2.3 Terminologies Related to Image Encryption

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

2.3.1 Digital Image

Image is a two-dimensional light intensity function $f(x, y)$, where x and y are spatial coordinate. The value of f at any point (x, y) is the brightness (or gray level) of the image at that point.
A digital image is a visual representation of an object that has been digitally encoded. It is the numerical representation of a two-dimensional image, also known as a raster image or a bit-mapped image. Pixels in a digital image are arranged in a 2-dimensional grid in a rectangular pattern that produces a matrix of M columns and N rows.

2.3.2 Pixel

A pixel is the fundamental unit of an image. This means that the image is a collection of different pixels. The colors in any pixel are the functions of red, green, and blue portions.

2.3.3 Types of Image Format

Image file formats are classified into several types. A few examples are provided below.

1. Tagged Image File Format.
2. Joint Photographic Experts Group.
3. Portable Network Graphics.

2.3.3.1 Tagged Image File Format (TIFF)

TIFF is a versatile format with file extensions of .tif or .tiff. The structures that type can be tagged with this format are typically designed to be extendible. This format is not useful in web browsers, but it is widely accepted as a photographic file in printing. The original file remains unchanged in this format regardless of how many times it is copied, compressed, or re-saved (lossless compression). This format is typically used for high-quality prints, archival copies, and professional publications, among other things.

2.3.3.2 Joint Photographic Experts Group (JPEG)

ISO and ITU members make up the JPEG. The file extension used for this format is .jpg or .jpeg. This format applies 'lossy compression' to the original image, resulting in significant degradation but generally undetectable loss. This format is commonly used for online photos, E-mailing, web images, memory cards, and PowerPoint presentations, among other things.

2.3.3.3 Portable Network Graphics (PNG)

PNG file extension for this format is .png. This format is most commonly used for interactive files/documents, such as web pages, but it is not well suited for

printing. This format is also loss-less, which means that one can edit but not lose the quality of the original file. This format is fully color-rich, which means it can display more color variations. This is one of the most commonly used image formats on the internet.

2.3.4 Image Resolution

The number of pixels in an image is referred to as its resolution. The width and height of the image, as well as the total number of pixels in the image, are sometimes used to identify resolution. Assume that an image with resolution $m \times n$ contains m columns and n rows. So, the order $m \times n$ shows the total number of pixels in an image. For example, a 2046 pixel wide and 1530 pixel high image (2046 $\times$ 1530) contains 3,130,380 pixels (or 3.1 Megapixels). It is also known as a 2046 $\times$ 1530 or 3.1 Megapixel image. Now, as another example a 2048 pixels wide and 800 pixel high image (2048 $\times$ 800) contains $1,638,400$ pixels (or 1.6 Megapixels). By comparing both images on the basis of resolution. The image having the resolution 3.1 Megapixel have better result in quality then the image having resolution 1.6 Megapixel. Therefore, image with high resolution will have better image quality. As shown in Figure 2.5, there are three images of size 512 $\times$ 512, 512 $\times$ 1080 and 1080 $\times$ 1200. It is clearly seen from figure that image having size 1080 $\times$ 1200 have visually better performance than other.

FIGURE 2.5: Different Image Resolution

2.3.5 Image Encryption and Decryption

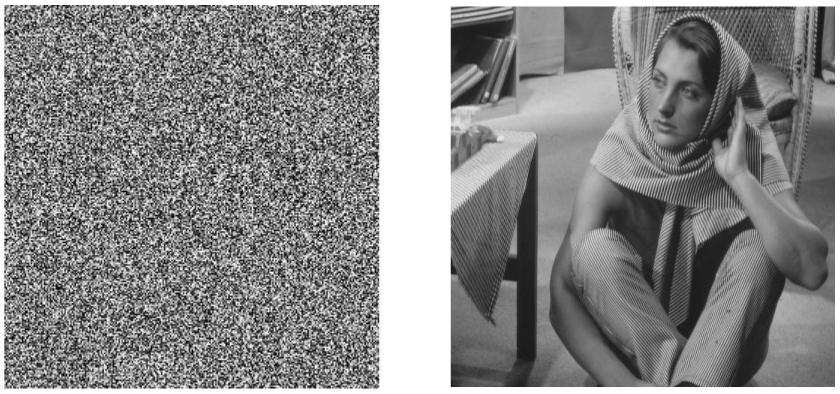
Image encryption describes the process of converting an original image into a coded image. It secures the image during transmission over a public network. There is always a need to protect the information related to the secret image in order to maintain its security, and no one can easily identify them other than the authentic receiver.

(a) (b)

FIGURE 2.6: Image Encryption: a) Original Barbera Image, b) Ciphered Barbera Image

As shown in Figure 2.6, an encrypted image is obtained by implementing a specific image encryption algorithm. Here, the Permutation Modulation and Diffusion (PMD) based Image encryption algorithm (presented in Section 3.2) is applied to the image Barbera for encryption. After that, the encrypted image is sent to the authorized person through a unsecure channel. Decryption is the reversible

encryption procedure in which one can convert an encrypted image back to its original form. An authorized person can only obtain the original image in this process by using the secret keys and decryption algorithm. When the receiver receives the encrypted image, he decrypts it to obtain the original image. Because the key is only known to the sender, decryption can only be performed by an authorized person who has access to the secret key. A receiver apply the Inverse PMD to get the plainimage. At receivers end, the original image is then obtained by the using the image decryption algorithm (presented in Section 3.2).



(a) (b)

FIGURE 2.7: Image Decryption: a) Cipherimage of Barbera, b) Decrypted Image of Barbera

2.4 Chaos Theory

The term chaos refers to the science of unexpected events. It involves dynamic systems with nonlinear and unpredictable behavior. Chaos theory provides a method for dealing with unpredictable behavior such as turbulence, weather, the stock market, brain states, and so on. Fractal mathematics is frequently used in chaos theory. A fractal pattern is one that never ends and is self-similar across different scales. Fractals include trees, rivers, coastlines, mountains, clouds, hurricanes, and so on. Many of the systems around us are involved in complex chaotic behavior in some cases. From chaos theory one can get new insights, strength, and ideas in many natural phenomenon. In order to explain the fractal nature of dynamic system. The balloon pilot's example is the best example to explains the entire scenario. When he arrives at his destination while keeping in mind the complex, chaotic change of atmosphere. Chaos theory provides us a platform to find a better approach towards things that have chaotic and fractal nature.
Chaos theory is also influencing the development of subjects such as physics [59], economics [14, 15], engineering, and biology, among others.

2.4.1 Butterfly Effect

The phenomenon of the butterfly effect helps to explain the chaotic behavior. The butterfly effect depicts that a large change that occurs as a result of a very small

effect or change. The butterfly effect teaches us that a small change in the input can result in a large change in the output. In mathematics, chaos theory serves an important purpose. To demonstrate the chaotic behavior, consider a linear equation to explain the concept in mathematics. It will help to determine whether or not there is chaos by comparing the initial values and the correspondence resulted values.

Example 2.4.1. Consider a linear equation

$$v_{m+1} = v_m - 1 \quad \text{with} \quad v_0 = 0.3542 \tag{2.1}$$

In the above equation, the variable involved is v. By performing iterations, the obtained values of v_1, v_2, v_3, ..., v_{10} are as follows:

$$v_1 = v_0 - 1 = 0.3542 - 1 = -0.6458$$

$$v_2 = v_1 - 1 = -0.6458 - 1 = -1.6458$$

$$v_3 = v_2 - 1 = -1.6458 - 1 = -2.6458$$

$$\vdots$$

$$v_{10} = v_9 - 1 = -8.6458 - 1 = -9.6458.$$

Now the behavior of linear Equation (2.1) is examined by considering $v_0 = 0.3543$.

$$v_1 = v_0 - 1 = 0.3543 - 1 = -0.6457$$

$$v_2 = v_1 - 1 = -0.6457 - 1 = -1.6457$$

$$v_3 = v_2 - 1 = -1.6457 - 1 = -2.6457$$

$$\vdots$$

$$v_{10} = v_9 - 1 = -8.6457 - 1 = -9.6457.$$

Observing the both resulting values obtained from Equation(2.1), it is concluded that after 10 iterations, the both resulting values become the same, despite the fact that the initial values assumed were different. It indicates that there is a normal and predictable change in the final results and thus no chaos exists in this example.

Now, consider the another linear equation and then iterate it by using the same initial values assumed in Equation (2.1).

$$v_{m+1} = 4v_m - 1 \quad \text{with} \quad v_0 = 0.3542 \tag{2.2}$$

Here are the results of the first 10 iterations:

$$v_1 = v_0 - 1 = 4(0.3542) - 1 = 0.4168$$

$$v_2 = v_1 - 1 = 4(0.4168) - 1 = 0.6672$$

$$v_3 = v_2 - 1 = 4(0.6672) - 1 = 1.6688$$

$$\vdots$$

$$v_{10} = v_9 - 1 = 4(5470.4048) - 1 = 21880.6192.$$

Now check the behavior of linear Equation (2.2) by considering $v_0 = 0.3543$.

$$v_1 = v_0 - 1 = 4(0.3543) - 1 = 0.4172$$

$$v_2 = v_1 - 1 = 4(0.4172) - 1 = 0.6688$$

$$v_3 = v_2 - 1 = 4(0.6688) - 1 = 1.6752$$

$$\vdots$$

$$v_{10} = v_9 - 1 = 4(5496.6192) - 1 = 21985.4768.$$

The resulting values for Equation (2.2) shows that the difference in final results is 104.8576. With a small change of 0.00001 in initial condition. This variation in the outcome is unexpected and unpredictable. As a result, there exist a chaotic behavior in this example.

2.4.2 Properties of Chaotic System

Chaos has been witnessed in many natural structures that cover a significant amount of technical and industrial areas. Such occurrences indicate definite possessions that are difficult and unpredictable to identify. The phenomenon of chaos can be found in almost all nonlinear deterministic systems. Chaos appears to exist when there is a continuous and disorganized progression in long-term mathematical function. There are a number of properties that summaries the characteristics observed in chaotic system.

1. **Self-similarity:** It indicates the similar appearance at dissimilar scales of observation in an evolving system, with time or space.

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 evolve chaotically and non-periodically.

3. **Sensitivity to Initial Conditions:** Each point in a chaotic system is arbitrarily closely approximated by other locations with significantly differing future paths or trajectories, which is known as sensitivity to initial conditions. As a result, even a minor alteration or disruption of the current trajectory can result in drastically different future behaviour.

4. **Long-term Prediction:** Small changes in initial conditions, such as those caused by measurement errors or rounding errors in numerical computation, can lead to significantly different outcomes for such dynamical systems, making long-term prediction difficult in general.This can happen despite the fact that these systems are deterministic, which means that their future behaviour follows a unique evolution and is entirely specified by their initial conditions, with no random elements. In other words, the deterministic nature of these systems prevents them from being predictable.

2.5 Chaotic Map

A map that demonstrates chaotic behavior is said to be a chaotic map. A discrete-time or continuous-time parameter can be used to parameterize a map. Discrete maps are usually the iterated functions. Chaotic maps are frequently occurs in the study of dynamical systems.

Control Parameter

A control parameter is an essential part of any chaotic map. It actually control the behavior of map. Many chaotic maps provide the chaotic behavior on a specific region of control parameter. This region can be seen from Bifurcation diagram or Lyapunov exponent.

2.5.1 Lyapunove Exponent

The term 'Lyapunove Exponent' (LE) [60] has been widely used in the study of dynamical systems. The degree of divergence between two close trajectories of a dynamical system is described by LE. A positive LE indicates that, regardless of how close the two trajectories are, their divergence increases with each iteration, eventually causing them to be completely different. As a result, the LE of a chaotic dynamical system is positive. In a multidimensional dynamical system, there may be more than one LE. If it has more than one positive LE, its close trajectories exponentially diverge in several dimensions. This phenomenon is known as hyperchaotic behavior. A dynamical system with hyperchaotic behaviour performs extremely well in terms of chaos and its outputs are difficult to predict.
Lyapunove exponent can be defined as:

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n-1} \ln|h^{'}(x_i)| \tag{2.3}$$

The Lyapunove exponent has dynamics cases, as shown below:

1. When Lyapunove exponent is less than zero, the orbit is directed to a fixed or stable point.

2. When the Lyapunove exponent is zero, the system is neutrally stable. such system are conservative and in a steady state mode. They exhibit lyapunove stability.

3. When Lyapunove exponent is greater than zero then the system is chaotic and unstable, and the near by points will diverge irrespective of how close they are.

2.5.2 Bifurcation Diagram

When the control parameter is altered, a bifurcation happens, which is a period-doubling, or a change from an M-point attractor to a 2M-point attractor. A Bifurcation Diagram is a graphic representation of the sequence of period-doubling that occurs as control parameter (ς) increases. The bifurcation diagram of logistic map is illustrated in Figure 2.8, with ς on the horizontal axis. Before plotting sequential values of z over a few hundred iterations, the system is allowed to settle down for each value of ς. It is clear from the Figure 2.8, when $\varsigma \leq 0.25$ every point are plotted at zero. So for $\varsigma \leq 0.25$ there is only one point attractor. Now when $\varsigma \in (0.25, 0.75)$, there is still one point attractors but the attracted value of z increases as ς increases. Bifurcation occurs at $\varsigma = 0.75$, 0.8625, 0.855 (approximately) etc. Until just beyond 0.89, where the system become chaotic. However the system is not chaotic for all value of $\varsigma \in [0.89,\ 1]$, even there are some point in which it show three point attractors.

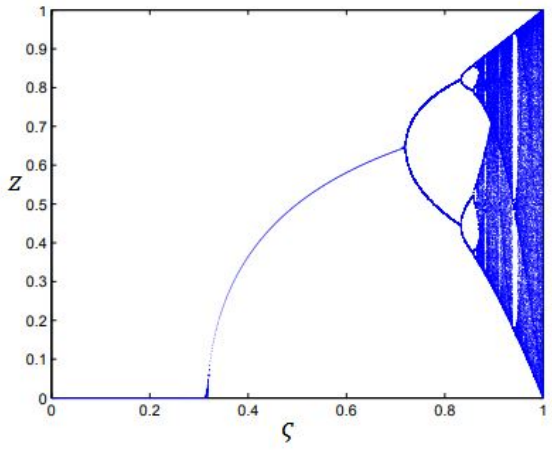


FIGURE 2.8: Bifurcation diagram

2.5.3 Logistic Map

Logistic map [50] is a one dimensional chaotic map, that has a simple mathematical structure but complex chaotic behavior. The mathematical definition of logistic map is:

$$z_{i+1} = 4\varsigma z_i(1 - z_i) \tag{2.4}$$

where $\varsigma \in [0, 1]$. The Lyapunove exponent of logistic map under different pa-

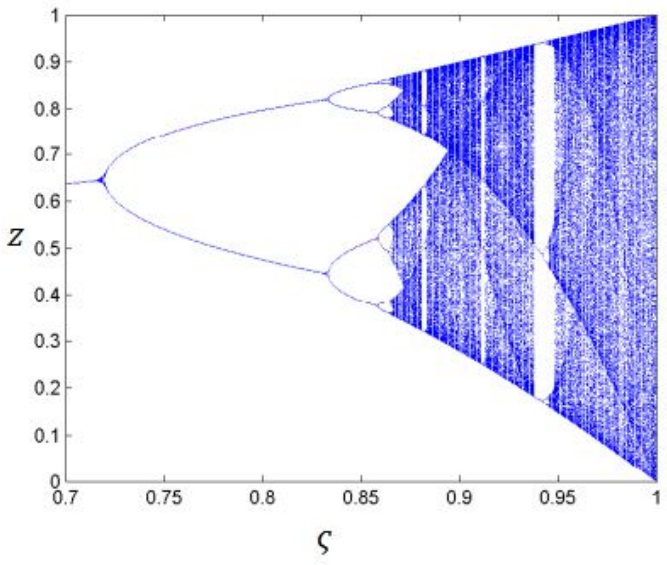


FIGURE 2.9: Bifurcation diagram of logistic map

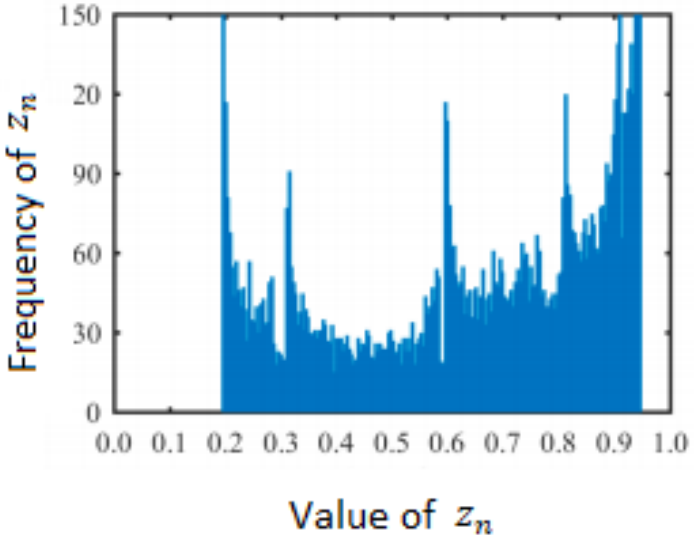


FIGURE 2.10: Distribution of state value

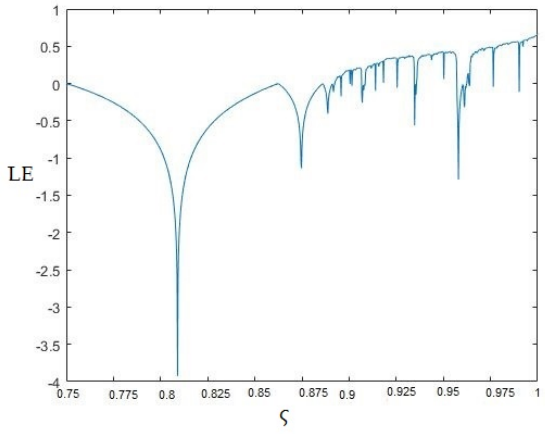


FIGURE 2.11: Lyapunove exponent of logistic map

rameters is also determine the region of parameters corresponding to its chaotic phenomena. The chaotic behavior of logistic map exhibits for $\varsigma \in [0.89, 1]$. Figure 2.11 shows the Lyapunove exponent of the logistic map. Figure 2.10 shows the bifurcation diagram of logistic map.

Drawbacks

1. The chaotic region of the system is limited i.e., $\varsigma \in [0.89, 1]$. Even within this range, there are some parameters which ensure that it does not exhibit chaotic behavior.

2. There is a non-uniform distribution of state values between [0, 1].
   These drawbacks reduce the logistic map's applicability.

2.5.4 Chaotic Sine Map

The input of the Sine function is the set of real no ($\mathbb{R}$) and the output lies in the interval [-1, 1]. The chaotic sine map is derived from the sine function by transforming its input into [0, 1]. Mathematical definition of the 1D chaotic sine map is:

$$y_{i+1} = \sigma \sin(\pi y_i); \qquad y_0 \in [0, 1], \quad i \in \mathbb{Z}^+ \tag{2.5}$$

Where, $\sigma \in [0, 1]$ is the control parameter.

The bifurcation diagram of sine map 2.12 shows chaotic behaviour when $\sigma \in [0.87, 1]$. The mathematical form of logistic map and sine map are totally different but their chaotic behaviour are quite similar, which is clear from their bifurcation diagrams as shown in Figure 2.9 and Figure 2.12. From the bifurcation diagram of sine map clearly seen that the sine map becomes chaotic when σ approaches to 1. The LE of a chaotic sine map is positive for σ in [0.87, 1]. Figure 2.12 shows the Lyapunove exponent of the chaotic sine map.

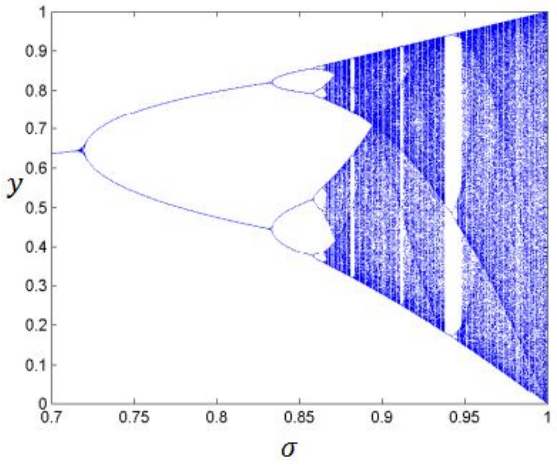


FIGURE 2.12: Bifurcation diagram of sine map

Drawbacks

1. The chaotic region of the system is limited i.e., $\sigma \in [0.87, 1]$. Even within this region, there are some parameters which ensure that it does not exhibit chaotic behavior.

2. There is a non-uniform distribution of state values between [0, 1].
   These drawbacks reduce the chaotic sine map's applicability.

2.6 Chaos and Cryptography

The chaos phenomenon, which exhibits pseudo-random behavior, is most commonly seen in nonlinear structures and is extremely sensitive to the system's initial

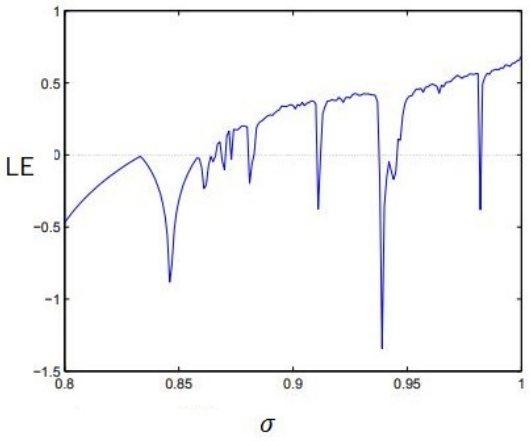


FIGURE 2.13: Lyapunove exponent of sine map

conditions. Understanding system output for an analyst who is aware of the initial conditions governing the characteristics is an important feature of these systems. On the other hand, if the system's initial inputs are uncertain, the system tends to be highly random. Unless the owner data is aware of the pseudo-random behavior. This feature can be used to substitute and diffuse plain-text. In order to achieve resistance and protection against unauthorized entities. Encryption schemes based on chaos are capable of encrypting a wide range of data types, as text [61], image [49] , video [62] etc.

2.6.1 Chaos Based Cryptosystem

It is impossible to avoid an unauthorized person who eavesdrops on a communication network, such as the ones we use for satellite, mobile phones, and the internet. If we want to use a communication network while maintaining confidentiality, we must use a cryptographic technique. The security of content such as video and image has become increasingly important in many applications such as medical imaging, industrial imaging, video conferencing, military imaging systems, and private multimedia messages.

Chaos theory, a branch of mathematics that was developed in 1970, has played an important role in protecting confidential images and videos.

Chaotic systems are deterministic, non-linear and extremely sensitive to control parameters and initial conditions. They also behave in a pseudo-random manner. Mathews [63] presented a chaotic encryption algorithm in 1989. This is useful for encrypting text-based data. Fridrich's research included the important chaos-based system [64].In his scheme, the confusion is created by permuting all pixels as a whole with one of three types of (2 D) chaotic maps, namely the Standard map [65], the Cat map [66], and the Baker map [67]. The diffusion system modifies successive pixel values in such a way that the change generates a cumulative effect on the previous pixel values.

Most chaos-based encryption/decryption schemes rely on the substitution permutation network (SPN) [68] chaos theory is well-known in modern cryptographic research due to its unpredictable behaviour and cryptographic-like properties. As a result, many researchers are now using it to develop secure cryptographic protocols. such as image secret sharing based on a chaotic map [69] and a chaotic-based watermarking scheme [70]. The inclusion of chaotic maps in these cryptographic algorithms increased their security of secret data.

2.6.2 Confusion and Diffusion in Chaos

To improve the cryptographic security of a system, it must incorporate confusion and diffusion effects, as described in Shannon[71]. The purpose of confusion is to complicate the statistical relationship between secret key and the cipherimage. While the diffusion makes the statistical relationship to generate a significant difference in cipherimage in comparison to the plainimage. In other words, the property of confusion states that there should be no link between the key and the cipher. According to the property of diffusion, any change in a single bit of a plainimage affects many cipher bytes/bits. In most chaos-based image cryptosystems, image confusion can be achieved by using chaotic maps with permutations and/or substitutions. In substitution and permutation networks, the confusion and diffusion is provided by Substitution boxes and permutation boxes respectively.

Chapter 3

A Chaotic Image Encryption Scheme Based on Information Entropy

In this chapter, a recent method for image encryption proposed by Ye et al [49] is explained. First, a compound chaotic map (two-dimensional logistic adjusted sine map) is discussed which is used in the scheme. The method uses information entropy and in both steps of encryption i.e., the permutation and diffusion, key-streams are generated based with the help of the plainimage. Modulation is inserted among permutation and diffusion for pixel distribution. For a secure way of communication, the proposed PMD(permutation, modulation and diffusion) based encryption of image is used.

3.1 2D-Logistic Adjusted Sine Map

Logistic map (2.4) and sine map (2.5) are already explained in Section 2.5. To improve the chaotic properties of logistic and sine map a new chaotic map is generated. Two-dimensional logistic adjusted sine map (2D-LASM) is introduced

in [44]. The mathematical form of the 2D-LASM is given below, for $i = 0, 1, \cdots$

$$\begin{cases} x_{i+1} = \sin(\pi\mu(y_i + 3)x_i(1 - x_i)) \\ y_{i+1} = \sin(\pi\mu(x_{i+1} + 3)y_i(1 - y_i)), \end{cases} \tag{3.1}$$

where parameter $\mu \in [0, 1]$. The logistic map (2.4) and sine map (2.5) are used to generate the 2D-LASM. The logistic equation $x_i(1 - x_i)$ is first scaled by a factor of μ, before being fed into the Sine map input. The phase plane is then extended from one dimension to two dimensions. Two inputs are interactively influenced in 2D-LASM, and the output pairs (x_{i+1}, y_{i+1}) are distributed into the 2D phase plain. It has a more complicated structure than Sine and Logistic maps, and its outputs are more difficult to predict. Where the chaotic orbits (An orbit that can alter in a largely unpredictable manner, or one in which even minor changes in the orbiting body's position cause significant changes in the orbit) of 2D-LASM using $\mu = 0.8116$, $x_0 = 0.1307$, $y_0 = 0.4126$ shown in Figure 3.1 and 3.2.

To predict the chaotic behavior of the map (3.1), the graph of LE of 2D-

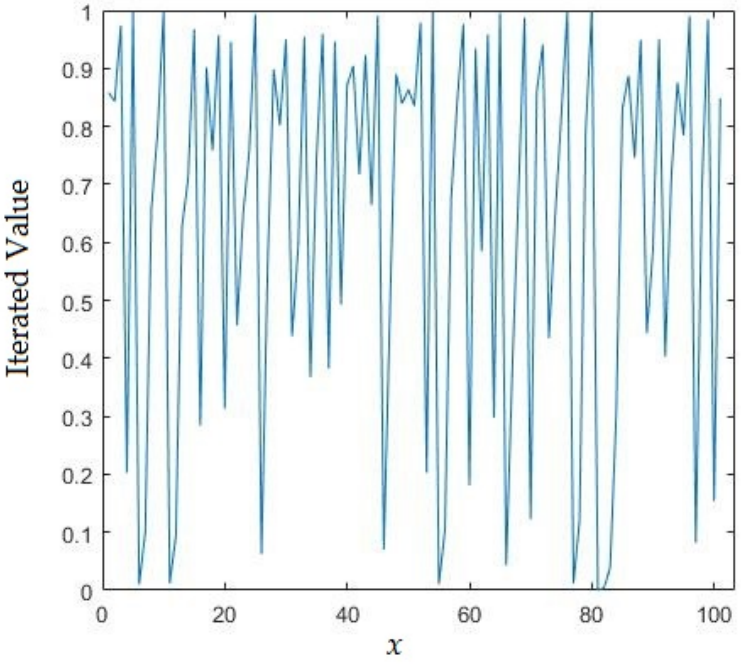


FIGURE 3.1: Chaotic orbits of x-values

LASM is given in [44] as shown in Figure 3.3. A 2-dimensional chaotic map

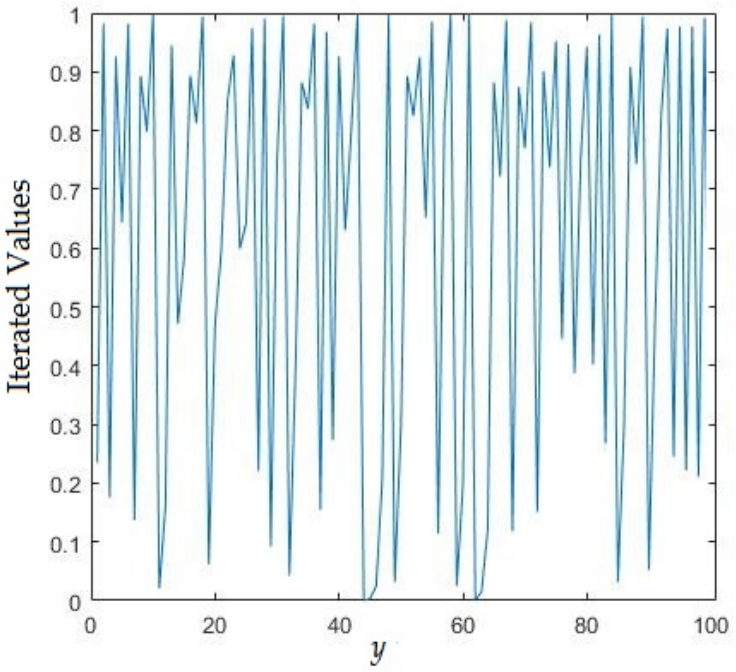


FIGURE 3.2: Chaotic orbits of y-values

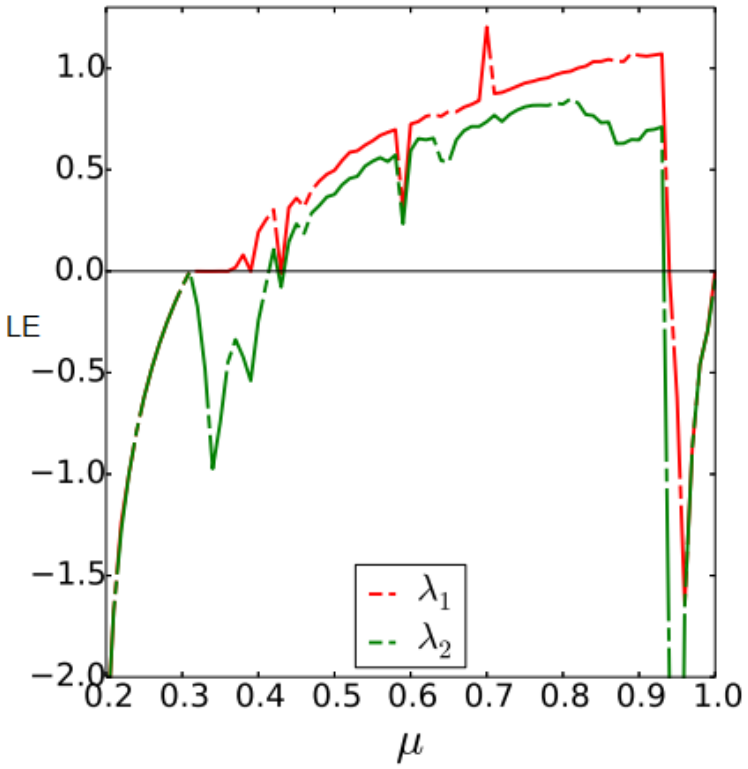


FIGURE 3.3: Lyapunove exponent of 2D-LASM

has two LEs. For 2D-LASM Figure 3.3 shows that how there LE (λ_1 and λ_2) change with the control parameter (μ). Now observe the following: Logistic map

(2.4) has chaotic when its parameter $\varsigma \in [0.89,1]$; Sine map (2.5) has chaotic behavior when its parameter $\sigma \in [0.87,1]$; 2D-LASM has chaotic behavior when $\mu \in [0.37, 0.38] \cup [0.4, 0.42] \cup [0.44, 0.93] \cup \{1\}$. Therefore, 2D-LASM has much wider chaotic range then Logistic map and sine map and have large key space.

TABLE 3.1: Chaotic range of chaotic maps

Sr.no	**Chaotic Map**	**Chaotic Range**
1	Logistic map	[0.89, 1]
2	Chaotic sine map	[0.87, 1]
3	2D - LASM	$[0.37, 0.38] \cup [0.4, 0.42] \cup [0.44, 0.93] \cup \{1\}$

3.2 Chaotic Image Encryption Based on Information Entropy

Before the description of the image encryption scheme of Ye et al [49], start with the explanation of the information entropy. A gray scale image of size $m \times n$ is used. A circular Permutation is applied on the image. Then, a modulation operation for the permuted image is implemented. At the end, the diffusion operation is used to get the cipher image. To get the plainimage back, the inverse diffusion, modulation and circular permutation is applied on cipher image. By doing all these steps a plain image can be achieved.

3.2.1 Information Entropy

In Information theory, the entropy of a pseudo-random variable is the average level of information essential in the variable's possible outcome. In 1948, Claude Shannon developed the concept of information entropy in [72]. In communication

theory, the information entropy $I(\alpha)$ is the statistical measure of uncertainty. The calculation for information entropy $I(\alpha)$ of Information source α is defined as:

$$I(\alpha) = \sum_{n=0}^{2^Q-1} p(\alpha_n) \log_2 \frac{1}{p(\alpha_n)} \tag{3.2}$$

When the information source is image then Q shows the no of bits in pixel value, an image of size 256×256 containing 8 bit pixel value has $Q = 8$. $p(\alpha_n)$ is the probability of the information source α_n. For a random source α in the 256 gray level it is easy to obtain I(α) is 8 when $Q = 8$ and $p(\alpha_n) = \frac{1}{256}$. Then,

$$I(\alpha) = \sum_{n=0}^{255} p(\alpha_n) \log_2 \frac{1}{p(\alpha_n)} = 8$$

i.e., the theoretical value of information entropy is 8.
The value of information entropy of the gray scale image (Lena) is "7.56828525761". The value of the information entropy is very sensitive, even when the value of single/double pixel is change so the value of information entropy is also changed. Table 3.2 and 3.3 show the values of the information entropy of the image Lena, with single/double pixel change in some random position. Due to high sensitivity of Information entropy, it is used in our algorithm to influence the generation and selection of the keystream. The information entropy is calculated by using Equation (3.2).

TABLE 3.2: Value of information entropy with single pixel change.

Position	$(2, 2)$	$(255, 255)$	$(100, 80)$
Values	7.568282002138077	7.568280588530810	7.568274951615647

TABLE 3.3: Value of information entropy with double pixel change.

Position	$(3, 114)$&$(26, 210)$	$(77, 55)$&$(39, 177)$	$(222, 111)$&$(15, 12)$
Values	7.568278778781513	7.568277178633389	7.568272881325982

3.2.2 Preliminary Setting

There are some parameters that are playing a vital role in the encryption/decryption scheme are as follows:

- The scheme uses Chaotic map (2D-LASM) for encryption purpose in the algorithm is discussed in Section 3.1.
- For sub-key generation the information Entropy discussed in Section 3.2.
- Common shared secret keys x_0, y_0, $x_0^{'}$ and $y_0^{'}$ are values chosen from [0,1]. These secret keys are used to generate the updated keys ($\overline{\mathrm{x}}_0$, $\overline{\mathrm{y}}_0$, $\overline{x}_0^{'}$ and $\overline{y}_0^{'}$).

Algorithm 3.2.1. (Encryption Algorithm)
Suppose the gray scale image A of size $m \times n$, and the keys x_0, y_0, $x_0^{'}$ and $y_0^{'}$. The entire permutation modulation and diffusion(PMD) encryption process is described as follow:

Input: Plainimage (A), chaotic map (3.1), information entropy (3.2), initial keys (x_0, y_0, $x_0^{'}$, $y_0^{'}$).
Output: Cipherimage (C).

1. Using Equation (3.2) calculate the information entropy of the plainimage A and get $s = I(A)$. Then, find the updated keys using secret keys $x_0, y_0, x_0^{'}, y_0^{'}$ as

$$\begin{cases} \overline{x}_0 = x_0 + \dfrac{s+1}{s + x_0 + y_0 + 1} & \mod 1, \\ \overline{y}_0 = y_0 + \dfrac{s+2}{s + x_0^{'} + y_0^{'} + 2} & \mod 1, \end{cases} \tag{3.3}$$

Positive number 1 and 2 are simply added in the above equation for avoiding pure color image attack. Now iterate the chaotic map (3.1) using updated keys $\overline{\mathrm{x}}_0$ and $\overline{\mathrm{y}}_0$ to generate the random matrix B of same size as the size

of the plainimage. To avoid transient effect previously 20,000 iterated value were discarded.

2. Use keys x_0, y_0, $x_0^{'}$, $y_0^{'}$ to find middle parameter u and v as

$$\begin{cases} u = \lceil (x_0 + y_0 + 1) \times 10^7 \rceil \mod m + 1, \\ v = \lceil (x_0^{'} + y_0^{'} + 1) \times 10^7 \rceil \mod n + 1, \end{cases} \tag{3.4}$$

where $\lceil \cdot \rceil$ is the ceiling function *i.e.*, $\lceil \cdot \rceil$ gives the nearest integer value. Then select a row and a column from B. To implement the circular permutation on A. Assume u^{th} row of B as a vector a are selected, while the v^{th} column of B is b.

3. To save the time consumption by using the sort function, an alternate function is used to transform the row vector a of order m and the column vector b of order n as:

$$\begin{cases} a^{'} = \lceil a \times 10^{14} \rceil \mod m, \\ b^{'} = \lceil b \times 10^{14} \rceil \mod n, \end{cases} \tag{3.5}$$

In the plainimage (A), $a^{'}$ is used for the circular permutation encryption column-wise and $b^{'}$ is for row direction. After applying the permutation to the plainimage A in the row and column direction, a permuted image P is obtained. The value of the Information entropy remains invariant after applying the permutation, *i.e.*, $I(A) = I(P)$. The keystreams are different with respect to different plainimages.

4. A modulation operation is designed for the permuted image P. For the modulation operation, first a matrix Q is designed with the same size as the permuted image P.

$$Q(j,k) = (mn + j + k) \mod 256,$$
$$\text{where, } j = 1, 2, 3, ..., m; \ k = 1, 2, 3, ..., n. \tag{3.6}$$

Then, apply the modulation operation on the permuted image P as

$$R = P + Q \mod 256. \tag{3.7}$$

Now, a new image R is obtained after applying modulation operation to the permuted image P.

5. For the eradication of the avalanche effect, diffusion is applied to image R. Using prior keys $(x_0,\ y_0,\ x_0^{'},\ y_0^{'})$ to generate the update keys $\overline{x}_0^{'}$ and $\overline{y}_0^{'}$ as:

$$\begin{cases} \overline{x}_0^{'} = x_0^{'} + \dfrac{1}{x_0 + y_0 + 1} \mod 1, \\ \overline{x}_0^{'} = y_0^{'} + \dfrac{2}{x_0 + y_0 + 2} \mod 1, \end{cases} \tag{3.8}$$

To obtain a random matrix K with the same size as the plain image, iterate the chaotic map(3.1) using initial keys $\overline{x}_0^{'}$ and $\overline{y}_0^{'}$. The matrix K is then processed using the following equation:

$$K = \lceil K \times 10^{14} \rceil \mod 256 \tag{3.9}$$

Where, $\lceil \cdot \rceil$ is the ceiling function.

6. A middle parameter is required for the image R to affect keystream usage and frustrate the chosen-plaintext and known-plaintext attacks. Here, a middle parameter d is designed according to the information entropy. The diffusion process is employed in the column direction, which is given by

$$\begin{cases} d = \lceil I(R(:, i+1:n)) \times 10^{14} \rceil \mod n+1, \\ C_i = R_i + d \times C_{i-1} + d \times K_i + K_d \mod 256, \\ \qquad\qquad\qquad\qquad\qquad\qquad i = 1, 2, 3, ..., n. \end{cases} \tag{3.10}$$

where $C_0 = 0$ is a column vector, K_i and R_i is the column vectors of matrices K and R. K_d is the column vector of matrix K at the d position. As a consequence, cipherimage C is achieved. It is clear that the information entropy influences the encryption process in permutation as well as in the diffusion stages.

Figure 3.4 depicts a block diagram of the proposed image encryption algo-

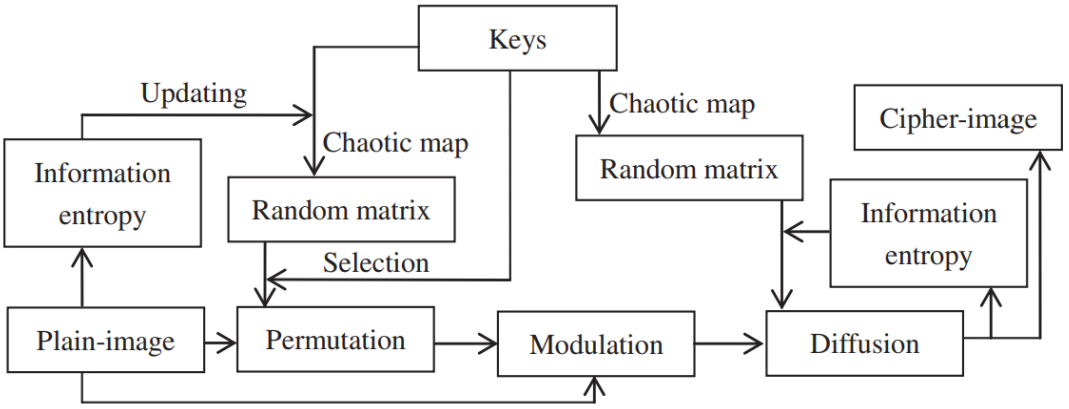


FIGURE 3.4: Block Diagram of Encryption

rithm [49] using information entropy.

As the proposed image cryptosystem is symmetric in nature therefore the decryption process can also be carried out by using similar steps in the opposite direction. After receiving the encrypted image, the receiver will use three modules, i.e inverse diffusion, modulation, and Permutation using the secret keys x_0, y_0, $x_0^{'}$, $y_0^{'}$ to recover the plainimage A from cipherimage C.

Algorithm 3.2.2. (Decryption Algorithm)

The procedure of recovering the plainimage from the cipherimage is given as follow:

Input: Cipherimage (C), chaotic map (3.1), information entropy (3.2), initial keys (x_0, y_0, $x_0^{'}$, $y_0^{'}$).

Output: Plainimage (A)

1. Using the secret keys x_0, y_0, $x_0^{'}$, $y_0^{'}$ to get the update keys $\overline{x_0}^{'}$ and $\overline{y_0}^{'}$ with the help Equation(3.10). Produce K according to the updated keys.

2. Suppose $d = 1$ to 256 and iterate the value of R_i and after using $R_i's$ values, we have to obtain the value of d_1. Until and unless it is equal to the value of d.

$$\begin{cases} R_i = C_i - d \times C_{i-1} - d \times K_i + K_d \mod 256, \\ \qquad\qquad\qquad\qquad\qquad\qquad i = n, ..., 2, 1. \\ d_1 = \lceil I(R(:, i+1:n)) \times 10^{14} \rceil \mod n+1, \end{cases} \tag{3.11}$$

where $C_0 = 0$ is a column vector. As a result, matrix R is obtained.

3. Use Equation(3.6), to generate matrix Q of the size $m \times n$. Also use matrix Q to get the permuted image P as:

$$P = R - Q \mod 256. \tag{3.12}$$

4. As the value of information entropy is same for the plain image and permuted image i.e., $I(A) = I(P)$. To compute the updated keys ($\overline{x}_0$ and $\overline{y}_0$) from Equation (3.3) by using secret keys x_0, y_0, $x_0^{'}$, $y_0^{'}$ and $s = I(P)$. Then using updated keys compute random matrix B from chaotic map (3.1).

5. To calculate middle parameter u and v use Equation (3.4).

6. Select u^{th} row of B as a vector a, while the v^{th} column of B is b. Then, compute $a^{'}$ and $b^{'}$ by using Equation (3.5).

7. Apply the inverse circular permutation on the permuted image P, to obtain the plainimage A.

3.3 Results and Discussion

The experiments carried out to demonstrate the proposed method's performance and validity. The used image (Lena, Barberaera, Baboon) are taken from USC SIPI open image repository gray scale. The implementation of the image encryption scheme is performed on the PC with MATLAB R2017a having operating system Window 8.1 pro 64-bit, Core i5-4300M with 2.60 GHz CPU and 8 GB

RAM. Initial keys are randomly selected as $x_0 = 0.0056$, $y_0 = 0.3678$, $x_0^{'} = 0.6229$ and $y_0^{'} = 0.7676$. Figure 3.5 shows the result of encryption and decryption using proposed algorithm.

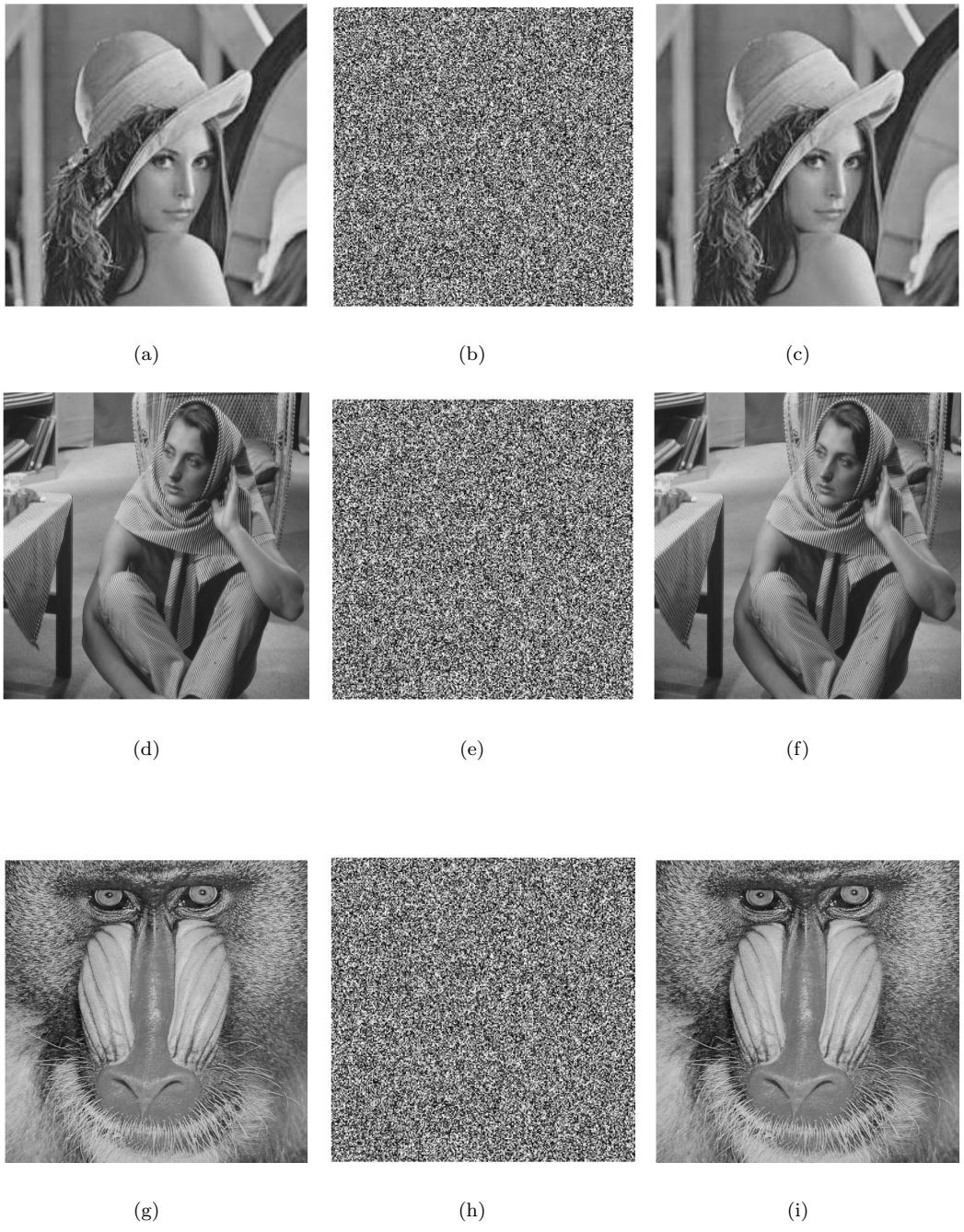


FIGURE 3.5: Experimental results (a, d, g) Plain-Image of Lena, Barbera and Baboon. (b, e, h) cipher-image of Lena, Barbera and Baboon. (c, f, i) decrypted image of Lena, Barbera and Baboon.

3.3.1 Performance Analysis

There are some security analyses which are examined in this subsection including key space, sensitivity, and statistics, with comparisons.

1. **Key Space Analysis:**

   The minimum key space recommended for high security and resistance to brute-force attacks is 10^{30} [73]. The proposed algorithm employs the keys x_0, y_0, $x_0^{'}$, and $y_0^{'}$. If the precision is set to 10^{-14}, the number of possible key combinations is 10^{56}. As a consequence, the brute force attack is impossible to carry out successfully.

2. **Key sensitivity:**

   A good image encryption algorithm should be key sensitive, preventing illegal tentative attacks. Figure 3.6(a) shows the plainimage of the Boat of size 512×512 as an example. While Figure 3.6 (b) shows the cipherimage of boat. However, The decryption is then performed on x_0, y_0, $x_0^{'}$, and $y_0^{'}$. If a minor change of 10^{-14} is made in keys the results are incorrect as shown in Figures 3.6 (c - f). This demonstrate that the algorithm has high sensitivity to key.

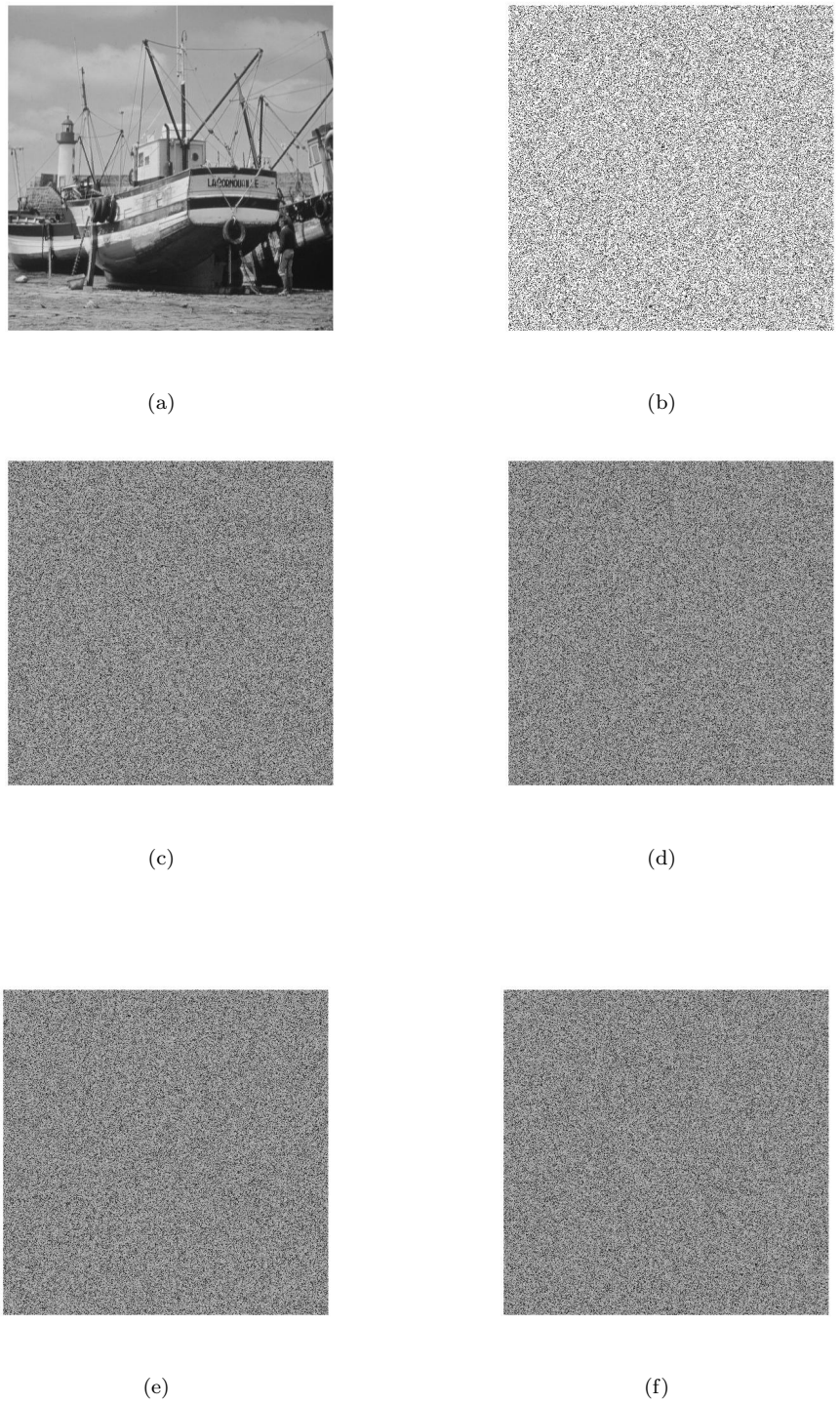
3. **Plaintext sensitivity:**

   To test an algorithm, unified averaged changed intensity (UACI) and number of pixel changing rate (NPCR) [74] measurements are used to check the avalanche effect and plaintext sensitivity.

$$\text{UACI} = \frac{1}{m \times n}\left[\sum_{g,h}\frac{|D_1(g,h) - D_2(g,h)|}{255}\right] \times 100\% \tag{3.13}$$

$$\text{NPCR} = \frac{\sum_{g,h} H(g,h)}{m \times n} \times 100\% \tag{3.14}$$

   where D_1 and D_2 are two different cipherimages with a one pixel change in the same plainimage.



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

FIGURE 3.6: Key sensitivity test for Boat: (a) plainimage of boat, (b) cipher-image of boat, (c-f) incorrect decryption of (b) using $x_0 + 10^{-14}$, $y_0 + 10^{-14}$, $x_0^{'} + 10^{-14}$, $y_0^{'} + 10^{-14}$

Here,

$$\begin{cases} H(g,h) = 0, & if \quad D_1(g,h) = D_2(g,h) \\ H(g,h) = 1, & if \quad D_1(g,h) \neq D_2(g,h) \end{cases}$$

The ideal UACI value is around 33.4635 percent, while the ideal NPCR value is around 99.6094 percent [75]. Table 3.4 shows the results of testing various images by changing the value of the pixel at random position. As a result, a minor change in the plain-image results in a completely different cipherimage. In other words, our method meets the requirement of high plaintext sensitivity. The value of UACI is calculated by using (3.13) and the value of NPCR is calculated by using Equation 3.14.

TABLE 3.4: UACI and NPCR values of 256×256 Image

Images	**Lena**	**House**	**Tree**
UACI	33.36271	33.4758	33.4177
NPCR	99.609375	99.5956	99.5956

3.3.2 Statistical Analysis

The relationship between plainimage and cipherimage can be determined by analyzing data statistically. In this manner, plainimage is totally different after encryption. For a image there are few analysis to figure out if the ciphered image releases any data about the first one or not.

1. **Histogram**

   The gray distribution can be visualized using a histogram. To meet the requirements of a good encryption method, the histogram of the cipherimage should be uniform or nearly uniform, and it should differ from the plain-image after encryption. Figures 3.7(a, c, e) show the histograms for the

plainimages Lena, Barbera, and Boat, while Figures 3.7(b, d, f) show the cipherimages. It can be concluded that the proposed algorithm is effective at thwarting the histogram attack.

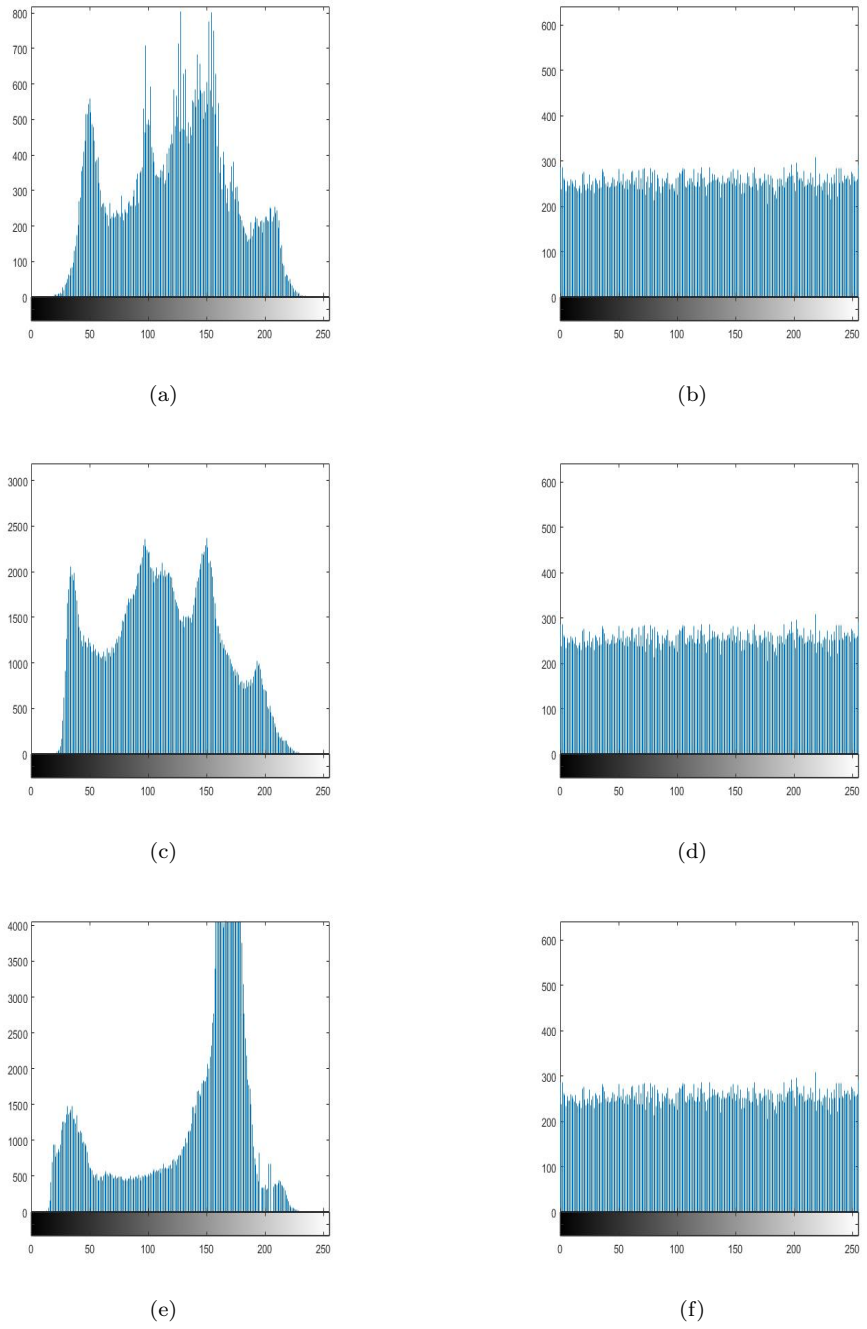


FIGURE 3.7: Histogram (a, c, e) plainimage of Lena, Barbera and Boat. Histogram (b, d, f) cipherimage of Lena, Barbera and Boat.

2. **Correlation Coefficient**

In a natural plainimage, the Pearson correlation Coefficient (PCC) [76] of two

adjacent pixels is normally high. A low correlation among neighboring pixels in the corresponding cipherimage should be achieved for a good encryption algorithm used on a plainimage. When comparing the similarity of two adjacent pixels in plainimage and cipherimage, the PCC of all two-adjacent pairs of pixels (in vertical, horizontal, and diagonal directions) in plainimage and cipherimage are calculated using the following formula

$$S(z) = \frac{1}{M}\sum_{g=1}^{M} z_g$$

$$T(z) = \frac{1}{M}\sum_{g=1}^{M}(z_g - S(z))^2$$

$$W(y,z) = \frac{1}{M}\sum_{g=1}^{M}(y_g - S(y))(z_g - S(z))$$

$$\delta_{yz} = \frac{W(y,z)}{\sqrt{T(y)}\sqrt{T(z)}}$$

The gray scale values of two adjacent pixels are y and z, and their correlation coefficient is δ_{yz}. Table 3.5 displays the test results. It is clear from the data that the PCC in the cipherimage using our method are close to zero.

TABLE 3.5: Pearson correlation coefficient analysis.

Direction	**Plainimage**	**Cipherimage**
Horizontal	0.9783154	0.006185
Diagonal	0.933060	0.003079
Vertical	0.954656	- 0.002944

3. **Information Entropy**

The important characteristic of randomness is information entropy. Equation (3.2) is used to compute information entropy, which is then used to test the various images. Table 3.6 shows the results of the information entropy. Because the proposed algorithm's information entropy values are close to the theoretical value of 8, it can resist information entropy attacks well, and it

can generate an analogous random message for the cipher-image after using the method.

TABLE 3.6: Information Entropy analyses.

Images	**Lena**	**Barbera**	**Boat**	**Baboon**
Plainimage	7.5682	7.4664	7.1237	7.3583
Cipherimage	7.9974	7.9992	7.9992	7.9769

Chapter 4

A Chaos Based Color Image Encryption Algorithm using Information Entropy

In the previous chapter, a permutation, modulation and diffusion (PMD) based grayscale image encryption scheme by using information entropy is discussed. In this Chapter, an extended version of PMD is presented that uses a color image encryption by using information entropy. The introduction is given first to the color image encryption using information entropy in Section 4.1, which includes preliminary setting, encryption process and decryption process. Then the results and discussion of the extended version of the algorithm is described in Section 4.2. Finally, Section 4.3 is about the performance analysis of the extended version of the algorithm.

4.1 Color Image Encryption Algorithm Using Information Entropy

The scheme proposed by Ye et al. [49] is extended for the color image B of size $m \times n$, where m is the number of rows and n is the number of columns of RGB

image. Firstly, the color image is converted into three channel (Red, Green, Blue) and label it as ($B_r,\ B_g,\ B_b$). Then, a red channel image B_r is used to apply the Circular permutation. A modulation operation is applied for the permuted image. At the end the diffusion operation is used to get the cipherimage of red channel C_r. Similarly repeat all these steps for the blue B_b and green B_g channel to get the cipherimage components ($C_b,\ C_g$) of these channels. After getting cipherimage components of all channel combine it to get the cipherimage of the color image C. To get the color image back inverse circular permutation, inverse modulation and inverse diffusion is applied on each component of cipherimage in reverse order. By doing all these steps a plain color image components ($B_r,\ B_g,\ B_b$) can be achieved. At the end combine channels (red, green, blue) to get the original color image B.

4.1.1 Preliminary Setting

There are some parameters that are playing a vital role in the encryption/decryption scheme are as follows:

- The scheme uses Chaotic map (2D-LASM) for encryption purpose in the extended algorithm is discussed in Section 3.1.
- For sub-key generation the information Entropy discussed in Section 3.2.
- Common shared keys $x_0,\ y_0,\ x_0^{'}$ and $y_0^{'}$ are values chosen from [0,1]. These secret keys are used to generate the update keys ($\overline{x}_0$, $\overline{y}_0$, $\overline{x}_0^{'}$ and $\overline{y}_0^{'}$).

Algorithm 4.1.1. (Encryption Algorithm)
For the encryption purpose a color-image of Barbera *i.e.*, B is used, whose all the channels are of size $m \times n$ where m is the number of rows and n is the number of columns. The entire encryption process is described below:

1. Convert the color (RGB) image B in its digital form B_z (containing three, two dimensional matrices B_r, B_g, B_b for the Red, Green and Blue channel respectively), where the entries of B *i.e.*, $b_i \in [0,\ 255]$. The order of each

component of B is $m \times n$, where m is the number of rows and n is the number of columns of B_r, B_g, B_b respectively.

2. Use Algorithm 3.2.1 to compute various cipher components C_z ($z \in r,\ g,\ b$) for red, green and blue channels respectively.

3. After getting the cipherimage C_z of all components, combine them to get the color (RGB) cipherimage C.

The cipherimage generated through the above algorithm is sent by insecure channel. Then its decryption can be perform by using the following decryption process. As the proposed image cryptosystem is symmetric in nature therefore the decryption can also be carried-out by using the similar steps in the opposite direction. After receiving the color (RGB) cipherimage, receiver first convert the cipherimage into three channels (C_r, C_g, C_b). Then, receiver employs three modules, *i.e.*, inverse permutation, modulation, and diffusion by using secret keys x_0, y_0, $x_0^{'}$, and $y_0^{'}$ on each channel individual . The procedure of recovering the plain color image form the cipher color image is given as follows:

Algorithm 4.1.2. (Decryption Algorithm)
Input: Cipher color image, chaotic map (3.1), information entropy (3.2), initial keys (x_0, y_0, $x_0^{'}$, $y_0^{'}$).
Output: Color (RGB) image

1. Convert the color (RGB) cipherimage C in its digital form C_z (containing three, two dimensional matrices C_r, C_g, C_b for the red, green and blue channel respectively), where the entries of C_z *i.e.*, $c_i \in [0,\ 255]$. The order of each component of C_z is $m \times n$, where m is the number of rows and n is the number of columns of C_r, C_g, C_b respectively.

2. Use Algorithm 3.2.2 to compute the plainimage components B_z for red, green and blue channels respectively.

3. After getting plainimage's component B_z *i.e.*, (B_r, B_g, B_b), combine them to get a color (RGB) image B.

4.2 Results and Discussion

The experiments are carried out to demonstrate the proposed method's performance and validity. The used image (Lena, Pepper, Baboon) are taken from USC SIPI open image repository for color (RGB) images. The implementation of the image encryption scheme is performed on the PC with MATLAB R2017a having operating system Window 8.1 pro 64-bit, Core i5-4300M with 2.60 GHz CPU and 8 GB RAM. Initial keys are randomly selected as $x_0 = 0.0056$, $y_0 = 0.3678$, $x_0^{'} = 0.6229$ and $y_0^{'} = 0.7676$. Figure 4.1 shows the result of encryption and decryption using proposed algorithm [49].

4.3 Performance Analysis

In this section some security analysis for the performance evaluation are examined such as key space, sensitivity, and statistical analysis with comparisons.

1. **Key Space Analysis:**

   The minimum key space recommended for high security and resistance to brute-force attacks is 10^{30} [73]. The algorithm uses the keys x_0, y_0, $x_0^{'}$, and $y_0^{'}$. If the precision is set to 10^{-14}, the number of possible key combinations is 10^{42}. As a result, carrying out a successful brute-force attack is impossible.

2. **Key Sensitivity:**

   A good image encryption algorithm should be sensitive for used keys, preventing illegal tentative attacks. Figure 4.2(a) shows the plain color image of Baboon (512×512). While Figure 4.2(b) shows the cipherimage of Baboon. However, The decryption performed on the cipherimage using x_0, y_0, $x_0^{'}$, and $y_0^{'}$. For an significant of 10^{-14} in keys the results of algorithm as shown in Figures 4.2(c-d) is totally change. This demonstrates that the algorithm has high sensitivity to keys.

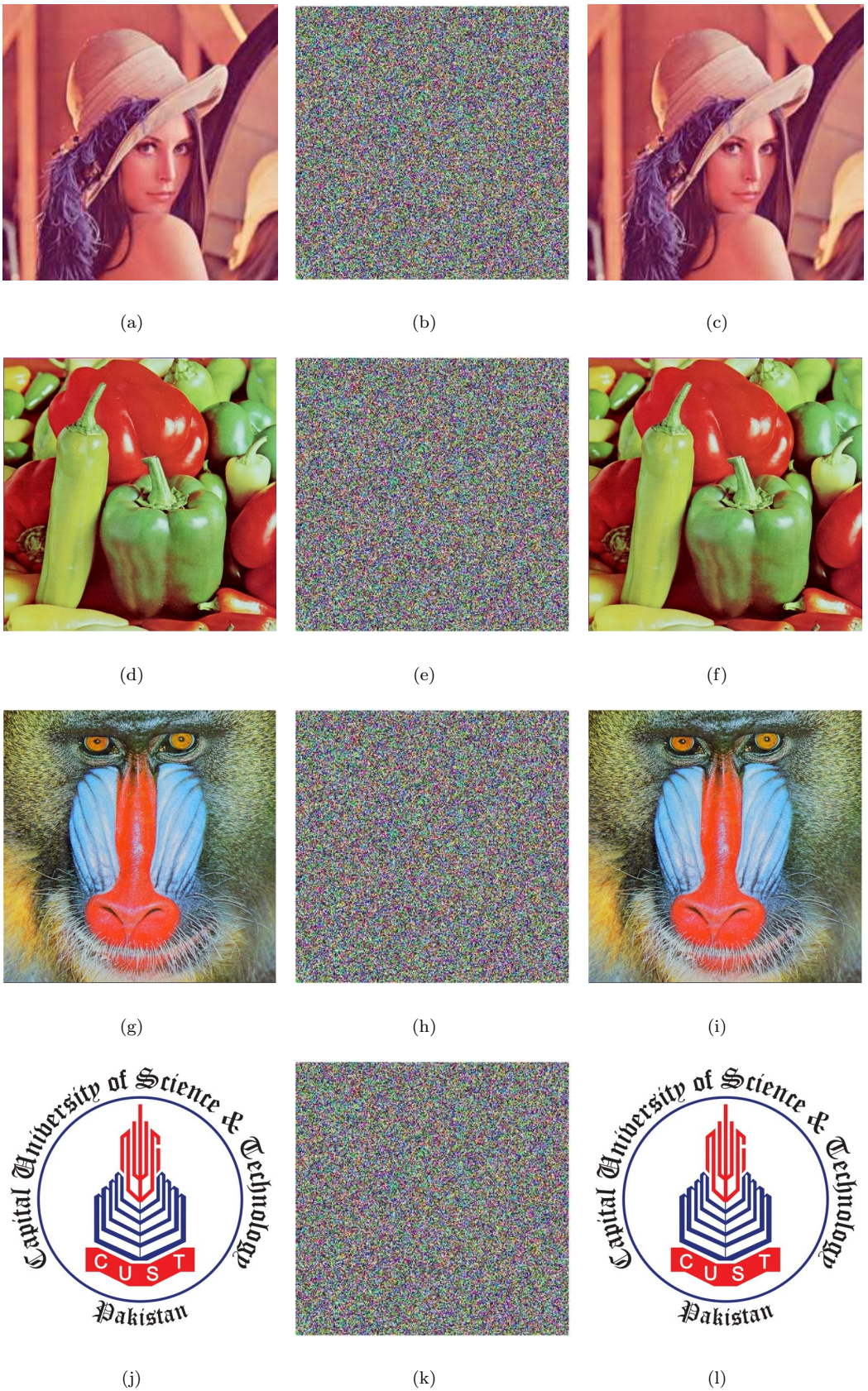


FIGURE 4.1: Experimental results: (a, d, g, j) color Image of Lena, Pepper, and Baboon, (b, e, h, k) cipherimage of Lena, Pepper, Baboon, and CUST Logo. (c, f, i, l) decrypted image of Lena, Pepper, Baboon, and CUST Logo.

3. **Plaintext sensitivity:**

Unified averaged changed intensity (UACI) and number of pixel changing rate (NPCR) [74] measurements are used to check the plaintext sensitivity and the avalanche effect.

$$\text{UACI} = \frac{1}{m \times n}\left[\sum_{j,k}\frac{|D_1(j,k) - D_2(j,k)|}{255}\right] \times 100\% \tag{4.1}$$

$$\text{NPCR} = \frac{\sum_{j,k} H(j,k)}{m \times n} \times 100\% \tag{4.2}$$

where $D1$ and $D2$ are two different cipherimages with a one pixel change in the same plain color image.

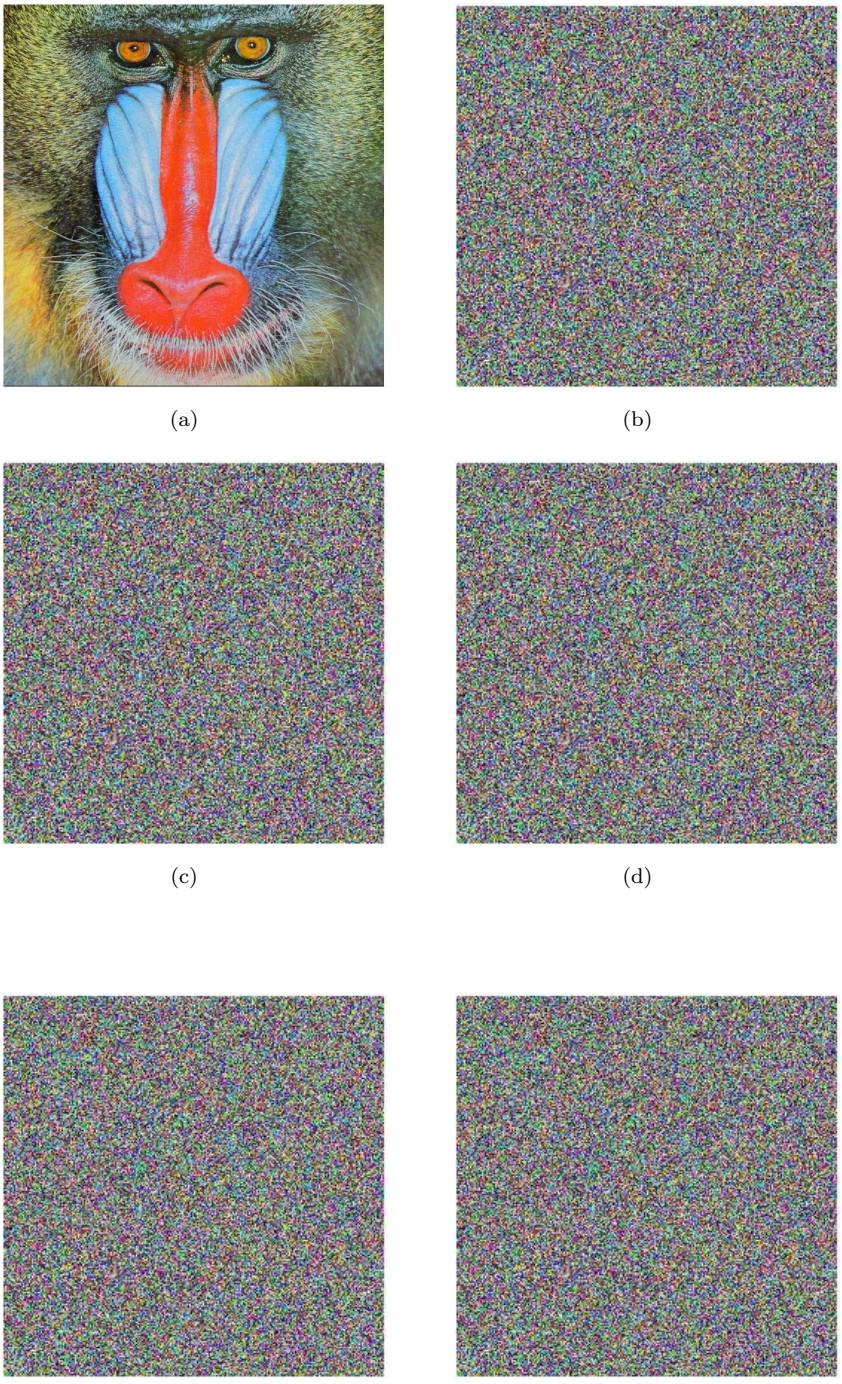
Here,

$$\begin{cases} H(j,k) = 0, & if \quad D_1(j,k) = D_2(j,k) \\ H(j,k) = 1, & if \quad D_1(j,k) \neq D_2(j,k) \end{cases}$$

The ideal value of UACI and NPCR are around 33.4635 percent and 99.6094 percent [75] respectively. Table 4.1 shows the comparison of NPCR Of all components of color (RGB) image Lena. Table **??** Shows the comparison of UACI of all components of Color (RGB) image Lena. The value of UACI is calculated by using Equation 4.1 and the value of NPCR is calculated by using Equation 4.2.

TABLE 4.1: NPCR Comparison of Image Lena

Methods	**NPCR (R)**	**NPCR (G)**	**NPCR (B)**
Wang et al. [77]	99.6475	99.6063	99.6536
Cho et al. [78]	99.6585	99.6570	99.6570
Ours	99.5987	99.5804	99.5697



(a) (b)

(c) (d)

(e) (f)

FIGURE 4.2: Key sensitivity test for color image of Baboon: (a) plain-image, (b) cipherimage, (c, d, e, f) incorrect decryption using $x_0 + 10^{-14}$, y_0, $x_0^{'}$, and $y_0^{'}$

TABLE 4.2: UACI Comparison of Image Lena

Methods	**UACI (R)**	**UACI (G)**	**UACI (B)**
Wang et al. [77]	33.4274	33.4215	33.4796
Cho et al. [78]	33.5101	33.5173	33.4767
Ours	33.3705	33.5036	33.2883

4.3.1 Statistical Analysis

The relationship between plainimage and cipherimage can be determined by analyzing data statistically. In this manner, plainimage is totally different after encryption. For a image there are few analysis to figure out if the ciphered image releases any data about the first one or not.

1. **Histogram**

   The gray distribution can be visualized using a histogram. To meet the requirements of a good encryption method, the histogram of the cipherimage should be uniform or nearly uniform, also differ from the plain color image of different channels. Figures 4.3 (a, c, e) shows the histograms for channels (red, green, blue) of plainimages Lena. While Figures 4.3 (b, d, f) shows the histogram of the cipherimage for channels (red, green, blue) of image Lena. It can be concluded that the proposed algorithm is effective at thwarting the histogram attack.

2. **Correlation Coefficient**

   In a plain color image, the Pearson correlation coefficient (PCC) [76] of two adjacent pixels is normally high. A low correlation among neighboring pixels in the corresponding cipher-image should be achieved for a good encryption algorithm. When comparing the similarity of two adjacent pixels in color

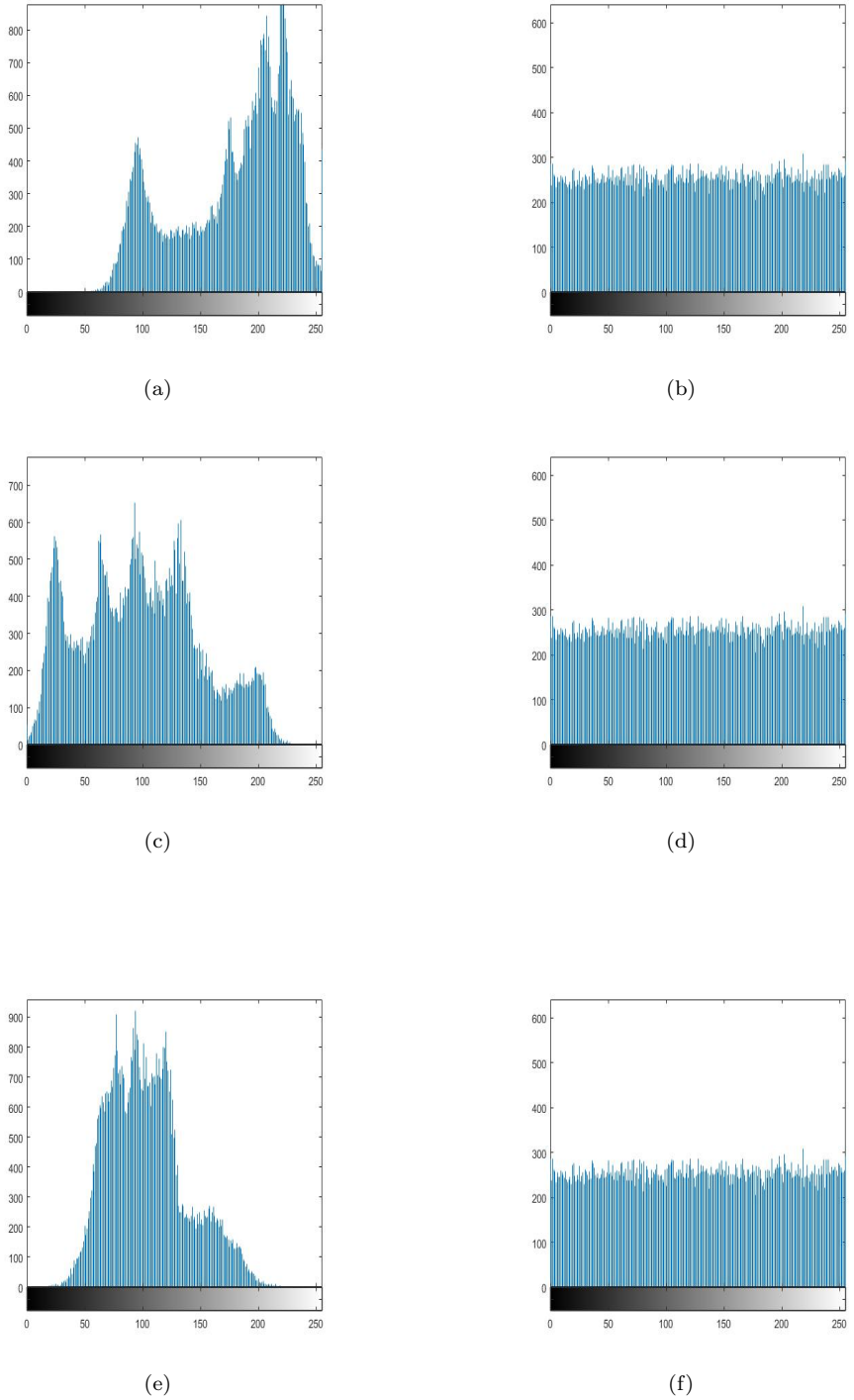


FIGURE 4.3: Histogram (a, c, e) shows Red, Green and Blue Channel of plain-image Lena. Histogram (b, d, f) shows Red, Green and Blue Channel of cipher-image Lena.

image and cipherimage, the PCC of all two-adjacent pairs of pixels (in horizontal, diagonal, and vertical directions) in color image and cipherimage are calculated using the following formula:

$$S(z) = \frac{1}{M}\sum_{g=1}^{M} z_g$$

$$T(z) = \frac{1}{M}\sum_{g=1}^{M}(z_g - S(z))^2$$

$$W(y,z) = \frac{1}{M}\sum_{g=1}^{M}(y_g - S(y))(z_g - S(z))$$

$$\delta_{yz} = \frac{W(y,z)}{\sqrt{T(y)}\sqrt{T(z)}}$$

The color values of two adjacent pixels are y and z and their PCC is δ_{yz}. Table 4.3 displays the test results. From these results it is clear that the PCC in the cipherimage using the extended scheme are close to zero.

TABLE 4.3: Analysis of correlation Coefficient.

Directions	**Plainimage**	**Cipherimage**
Horizontal	0.9582	0.0023
Vertical	0.9798	- 0.0020
Diagonal	0.9371	-0.0029

3. **Information Entropy**

The most important characteristic of randomness is information entropy. Equation (3.7) is used to compute information entropy, which is then used to test the various images. Table 4.4 shows the results of the information entropy of all components (RGB) of plainimage and cipherimage of Lena. Theoretical value of information entropy is 8 and the proposed algorithm's information entropy values are close to 8, therefore the proposed algorithm can resist information entropy attacks well and it can generate an analogous random message for the cipherimage after using the method. Table 4.5

compares some methods [79] that use the color image of Lena of size 512 × 512. This comparison demonstrates our method's good performance.

TABLE 4.4: Information Entropy analyses.

Images	**Red**	**Green**	**Blue**
Plainimage	7.2938	7.5729	7.0489
Cipherimage	7.9971	7.9974	7.9972

TABLE 4.5: Information Entropy analyses.

Methods	[**Faraoun**, [80]]	[**Wu et al.,** [81]]	[**Liu et al.,** [74]]	**Ours**
Red	7.9899	7.9899	7.9914	7.9971
Green	7.9997	7.9894	7.9915	7.9974
Blue	7.9979	7.9896	7.9915	7.9972

Chapter 5

Conclusion

In this chapter, the concluding remarks regarding the scheme [49] reviewed in Chapter 3 and extended work presented in Chapter 4.

1. In the present study, first a detailed review of the work of Ye et al [49] on "A chaotic Image Encryption Algorithm Based on Information Entropy" is Presented. For this purpose the well known chaotic maps (logistic map and sine map) are combined to form compound chaotic map (2D-LASM) and a new structure of PMD was introduced. The information entropy is used to make permutation's keystream on the basis of plainimage, the information entropy of the plainimage is same as the information entropy of the permuted image. The modulation operation is used between diffusion and permutation functions, which avoids the drawback of unchangeable gray distribution prior to diffusion. During the diffusion stage, designed the information entropy of the pre-encrypted image to influence the random sequence selection. As a result, the known-plaintext and chosen-plaintext have a more difficult time accessing the proposed algorithm. Furthermore, the implementation of the encryption Algorithm 3.2.1 is successfully implemented on MATLAB and security analysis provides significant result.

2. At the receiver end, the cipherimage is decrypted by using decryption Algorithm 3.2.2 to get the plainimage back. In decryption algorithm, the receiver

will use three modules, *i.e.*, inverse diffusion, modulation and permutation using secret keys and updated keys. As the updated keys is generated with the help of information entropy of permuted image, to recover plainimage from cipherimage.

3. As the scheme is symmetric so the secret keys are mutually shared through a secure channel. In the scheme, information entropy of the plainimage and the secret keys are used to generate the updated keys, which is then used to make permutation's keystream. As information entropy is very sensitive to the information such that the value of the information entropy is different for different images. So the keystream is different for the different images.

4. Key is very sensitive element in the encryption scheme, the image is encrypted using secret keys (x_0, y_0, $x_0^{'}$ and $y_0^{'}$). While in the decryption, if the same key is used only then the original image is obtained. If a very insignificant change of 10^{-14} in any of the key x_0, y_0, $x_0^{'}$ and $y_0^{'}$ is done, then the real image cannot be obtained.

5. The Scheme [49] is then extended for the color image. For Color (RGB) image, first convert the color image into three channels (Red, Green and Blue) then apply the encryption Algorithm 3.2.1 on all channels individually. After getting the cipherimage of each channel combine them to get the cipher color image. At the receiver's end, first the cipher color image is converted into three channels then apply the decryption Algorithm 3.2.2 on all channels individually to get the plainimage of each channel. After getting plainimage of each channel combine them to get the color (RGB) image. The implementation of the extended scheme is carried out on MATLAB and security analysis provides significant result.

As a future work, the image encryption scheme proposed by Ye et al [49] can be extended by using the chaotic map that provides hyper chaotic behaviour then 2D-LASM. The scheme discussed in this thesis can also be extended to video and speech encryption.

Bibliography

[1] O. Abraham and G. O. Shefiu, "An improved caesar cipher (icc) algorithm," *International Journal Of Engineering Science & Advanced Technology (IJESAT)*, vol. 2, pp. 1198–1202, 2012.

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

[3] J.-S. Coron, "What is cryptography?," *IEEE security & privacy*, vol. 4, no. 1, pp. 70–73, 2006.

[4] M. Shand and J. Vuillemin, "Fast implementations of rsa cryptography," in *Proceedings of IEEE 11th Symposium on Computer Arithmetic*, pp. 252–259, IEEE, 1993.

[5] X. Chai, Z. Gan, Y. Lu, Y. Chen, and D. Han, "A novel image encryption algorithm based on the chaotic system and dna computing," *International Journal of Modern Physics C*, vol. 28, no. 05, p. 1750069, 2017.

[6] D. Salamon, "The kolmogorov-arnold-moser theorem," *Math. Phys. Electron. J*, vol. 10, no. 3, pp. 1–37, 2004.

[7] E. N. Lorenz, "Deterministic nonperiodic flow," *Journal of atmospheric sciences*, vol. 20, no. 2, pp. 130–141, 1963.

[8] D. Ruelle and F. Takens, "On the nature of turbulence," *Les rencontres physiciens-mathématiciens de Strasbourg-RCP25*, vol. 12, pp. 1–44, 1971.

[9] T.-Y. Li and J. A. Yorke, "Period three implies chaos," in *The theory of chaotic attractors*, pp. 77–84, Springer, 2004.

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

[11] I. Sushko, V. Avrutin, and L. Gardini, "Bifurcation structure in the skew tent map and its application as a border collision normal form," *Journal of Difference Equations and Applications*, vol. 22, no. 8, pp. 1040–1087, 2016.

[12] K. Feltekh, D. Fournier-Prunaret, and S. Belghith, "Analytical expressions for power spectral density issued from one-dimensional continuous piecewise linear maps with three slopes," *Signal processing*, vol. 94, pp. 149–157, 2014.

[13] J. Travis, "Why eric mazur brings chaos-not chaos theory-to physics," *Science*, vol. 266, no. 5186, pp. 890–892, 1994.

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

[15] N. Basalto, R. Bellotti, F. De Carlo, P. Facchi, and S. Pascazio, "Clustering stock market companies via chaotic map synchronization," *Physica A: Statistical Mechanics and its Applications*, vol. 345, no. 1-2, pp. 196–206, 2005.

[16] M. Maqableh, A. B. Samsudin, and M. A. Alia, "New hash function based on chaos theory (cha-1)," *International Journal of Computer Science and Network Security*, vol. 8, no. 2, pp. 20–27, 2008.

[17] Z. Kotulski and J. Szczepański, "Discrete chaotic cryptography," *Annalen der Physik*, vol. 509, no. 5, pp. 381–394, 1997.

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

[19] D. Yang, X. Liao, Y. Wang, H. Yang, and P. Wei, "A novel chaotic block cryptosystem based on iterating map with output-feedback," *Chaos, Solitons & Fractals*, vol. 41, no. 1, pp. 505–510, 2009.

[20] A. Akhshani, S. Behnia, A. Akhavan, H. A. Hassan, and Z. Hassan, "A novel scheme for image encryption based on 2d piecewise chaotic maps," *Optics Communications*, vol. 283, no. 17, pp. 3259–3266, 2010.

[21] T. Habutsu, Y. Nishio, I. Sasase, and S. Mori, "A secret key cryptosystem by iterating a chaotic map," in *Workshop on the Theory and Application of of Cryptographic Techniques*, pp. 127–140, Springer, 1991.

[22] K.-w. Wong, "A fast chaotic cryptographic scheme with dynamic look-up table," *Physics Letters A*, vol. 298, no. 4, pp. 238–242, 2002.

[23] K.-W. Wong, "A combined chaotic cryptographic and hashing scheme," *Physics letters A*, vol. 307, no. 5-6, pp. 292–298, 2003.

[24] B. Yang, Z. Li, S. Zheng, and Y. Yang, "Hash function construction based on coupled map lattice for communication security," in *2009 Global Mobile Congress*, pp. 1–7, IEEE, 2009.

[25] E. Alvarez, A. Fernández, P. Garcıa, J. Jiménez, and A. Marcano, "New approach to chaotic encryption," *Physics Letters A*, vol. 263, no. 4-6, pp. 373–375, 1999.

[26] R. Anderson, "Letter to the editor: Chaos and random numbers," *Cryptologia*, vol. 16, no. 3, p. 226, 1992.

[27] A. Kanso and N. Smaoui, "Logistic chaotic maps for binary numbers generations," *Chaos, Solitons & Fractals*, vol. 40, no. 5, pp. 2557–2568, 2009.

[28] 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.

[29] B. R. B. I. Mendua, "A new approach of colour image encryption based on henon like chaotic map," *Journal of Information Engineering and Applications*, vol. 3, no. 6, 2013.

[30] 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.

[31] J.-I. Guo *et al.*, "A new chaotic key-based design for image encryption and decryption," in *2000 IEEE International Symposium on Circuits and Systems (ISCAS)*, vol. 4, pp. 49–52, IEEE, 2000.

[32] M. R. Abuturab, "Color information security system using arnold transform and double structured phase encoding in gyrator transform domain," *Optics & Laser Technology*, vol. 45, pp. 525–532, 2013.

[33] A. Singh and P. Banerji, "Fractional integrals of fractional fourier transform for integrable boehmians," *Proceedings of the National Academy of Sciences, India Section A: Physical Sciences*, vol. 88, no. 1, pp. 49–53, 2018.

[34] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of computation*, vol. 48, no. 177, pp. 203–209, 1987.

[35] Y. Luo, M. Du, and J. Liu, "A symmetrical image encryption scheme in wavelet and time domain," *Communications in Nonlinear Science and Numerical Simulation*, vol. 20, no. 2, pp. 447–460, 2015.

[36] N. K. Pareek, V. Patidar, and K. K. Sud, "Diffusion–substitution based gray image encryption scheme," *Digital signal processing*, vol. 23, no. 3, pp. 894–901, 2013.

[37] M. Zhang and X. Tong, "Joint image encryption and compression scheme based on a new hyperchaotic system and curvelet transform," *Journal of Electronic Imaging*, vol. 26, no. 4, p. 043008, 2017.

[38] G. Ye and X. Huang, "Spatial image encryption algorithm based on chaotic map and pixel frequency," *Science China Information Sciences*, vol. 61, no. 5, pp. 1–3, 2018.

[39] Y. Abanda and A. Tiedeu, "Image encryption by chaos mixing," *IET Image Processing*, vol. 10, no. 10, pp. 742–750, 2016.

[40] K. Cho and T. Miyano, "Chaotic cryptography using augmented lorenz equations aided by quantum key distribution," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 62, no. 2, pp. 478–487, 2014.

[41] Y. Zhou, Z. Hua, C.-M. Pun, and C. P. Chen, "Cascade chaotic system with applications," *IEEE transactions on cybernetics*, vol. 45, no. 9, pp. 2001–2012, 2014.

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

[43] Y. Wang, K.-W. Wong, X. Liao, and G. Chen, "A new chaos-based fast image encryption algorithm," *Applied soft computing*, vol. 11, no. 1, pp. 514–522, 2011.

[44] Z. Hua and Y. Zhou, "Image encryption using 2d logistic-adjusted-sine map," *Information Sciences*, vol. 339, pp. 237–253, 2016.

[45] R. Guesmi, M. A. B. Farah, A. Kachouri, and M. Samet, "Hash key-based image encryption using crossover operator and chaos," *Multimedia tools and applications*, vol. 75, no. 8, pp. 4753–4769, 2016.

[46] W. Liu, K. Sun, and C. Zhu, "A fast image encryption algorithm based on chaotic map," *Optics and Lasers in Engineering*, vol. 84, pp. 26–36, 2016.

[47] 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.

[48] X. Zhang, X. Wang, and Y. Cheng, "Image encryption based on a genetic algorithm and a chaotic system," *IEICE Transactions on Communications*, vol. 98, no. 5, pp. 824–833, 2015.

[49] G. Ye, C. Pan, X. Huang, Z. Zhao, and J. He, "A chaotic image encryption algorithm based on information entropy," *International Journal of Bifurcation and Chaos*, vol. 28, no. 01, p. 1850010, 2018.

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

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

[52] A. Mousa and A. Hamad, "Evaluation of the rc4 algorithm for data encryption.," *Int. J. Comput. Sci. Appl.*, vol. 3, no. 2, pp. 44–56, 2006.

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

[54] D. Coppersmith, "The data encryption standard (des) and its strength against attacks," *IBM journal of research and development*, vol. 38, no. 3, pp. 243–250, 1994.

[55] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[56] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE transactions on information theory*, vol. 31, no. 4, pp. 469–472, 1985.

[57] A. Serjantov and P. Sewell, "Passive attack analysis for connection-based anonymity systems," in *European Symposium on Research in Computer Security*, pp. 116–131, Springer, 2003.

[58] 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.

[59] E. Schöll and E. Scholl, *Nonlinear spatio-temporal dynamics and chaos in semiconductors*. No. 10, Cambridge University Press, 2001.

[60] 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.

[61] M. Irsan and S. Antoro, "Text encryption algorithm based on chaotic map," in *Journal of Physics: Conference Series*, vol. 1341, p. 062023, IOP Publishing, 2019.

[62] S. Yang and S. Sun, "A video encryption method based on chaotic maps in dct domain," *Progress in natural science*, vol. 18, no. 10, pp. 1299–1304, 2008.

[63] R. Matthews, "On the derivation of a "chaotic" encryption algorithm," *Cryptologia*, vol. 13, no. 1, pp. 29–42, 1989.

[64] Z. Su, G. Zhang, and J. Jiang, "Multimedia security: a survey of chaos-based encryption technology," *Mutimedia: A Multidisiplinary Approach to Complex Issues, Ed. I. Karydis, InTech*, pp. 99–124, 2012.

[65] K.-W. Wong, B. S.-H. Kwok, and W.-S. Law, "A fast image encryption scheme based on chaotic standard map," *Physics Letters A*, vol. 372, no. 15, pp. 2645–2652, 2008.

[66] R. K. Sinha, N. San, B. Asha, and S. Sahu, "Chaotic image encryption scheme based on modified arnold cat map and henon map," in *2018 International Conference on Current Trends towards Converging Technologies (ICCTCT)*, pp. 1–5, IEEE, 2018.

[67] C. Fu, W.-J. Li, Z.-y. Meng, T. Wang, and P.-x. Li, "A symmetric image encryption scheme using chaotic baker map and lorenz system," in *2013 Ninth International Conference on Computational Intelligence and Security*, pp. 724–728, IEEE, 2013.

[68] G. Piret and J.-J. Quisquater, "A differential fault attack technique against spn structures, with application to the aes and khazad," in *International workshop on cryptographic hardware and embedded systems*, pp. 77–88, Springer, 2003.

[69] L. Dolendro Singh and K. Manglem Singh, "Visually meaningful multi-image encryption scheme.," *Arabian Journal for Science & Engineering (Springer Science & Business Media BV)*, vol. 43, no. 12, 2018.

[70] L. Chen, J. Chen, G. Zhao, and S. Wang, "Cryptanalysis and improvement of a chaos-based watermarking scheme," *IEEE Access*, vol. 7, pp. 97549–97565, 2019.

[71] Y.-q. Xu, M. Sun, and J.-h. Shen, "Shannon wavelet chaotic neural networks," in *Asia-Pacific Conference on Simulated Evolution and Learning*, pp. 244–251, Springer, 2006.

[72] J. Núñez, P. Cincotta, and F. Wachlin, "Information entropy," in *Chaos in Gravitational N-Body Systems*, pp. 43–53, Springer, 1996.

[73] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International journal of bifurcation and chaos*, vol. 16, no. 08, pp. 2129–2151, 2006.

[74] H. Liu, A. Kadir, and X. Sun, "Chaos-based fast colour image encryption scheme with true random number keys from environmental noise," *IET Image Processing*, vol. 11, no. 5, pp. 324–332, 2017.

[75] M. Ghebleh, A. Kanso, and H. Noura, "An image encryption scheme based on irregularly decimated chaotic maps," *Signal Processing: Image Communication*, vol. 29, no. 5, pp. 618–627, 2014.

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

[77] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Processing*, vol. 92, no. 4, pp. 1101–1108, 2012.

[78] U. S. Choi, S. J. Cho, J. G. Kim, S. W. Kang, H. D. Kim, and S. T. Kim, "Color image encryption based on pc-mlca and 3-d chaotic cat map," in *2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS)*, pp. 272–277, IEEE, 2019.

[79] X.-L. Chai, Z.-H. Gan, Y. Lu, M.-H. Zhang, and Y.-R. Chen, "A novel color image encryption algorithm based on genetic recombination and the four-dimensional memristive hyperchaotic system," *Chinese Physics B*, vol. 25, no. 10, p. 100503, 2016.

[80] K. M. Faraoun, "Fast encryption of rgb color digital images using a tweakable cellular automaton based schema," *Optics & Laser Technology*, vol. 64, pp. 145–155, 2014.

[81] X. Wu, C. Bai, and H. Kan, "A new color image cryptosystem via hyperchaos synchronization," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 6, pp. 1884–1897, 2014.