CAPITAL UNIVERSITY OF SCIENCE AND TECHNOLOGY, ISLAMABAD

Chaos Based Image Encryption and Authentication Schemes for Multimedia Applications

by

Tahir Sajjad Ali

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

in the

Faculty of Computing

Department of Mathematics

2023

Chaos Based Image Encryption and Authentication Schemes for Multimedia Applications

By

Tahir Sajjad Ali

(DMT151011)

Dr. Fatih Ozakaynak, Associate Professor
Firat University, Elazig, Turkiye
(Foreign Evaluator 1)

Dr. Faheem Ahmed, Associate Professor
Thompson Rivers University, Canada
(Foreign Evaluator 2)

Dr. Rashid Ali
(Supervisor Name)

Dr. Muhammad Sagheer
(Head, Department of Mathematics)

Dr. Muhammad Abdul Qadir
(Dean, Faculty of Computing)

DEPARTMENT OF MATHEMATICS
CAPITAL UNIVERSITY OF SCIENCE AND TECHNOLOGY
ISLAMABAD
2023

DEDICATION

The thesis is dedicated to the people who have supported me throughout my education. Thanks for making me see this adventure through to the end.

CAPITAL UNIVERSITY OF SCIENCE & TECHNOLOGY
ISLAMABAD

Expressway, Kahuta Road, Zone-V, Islamabad
Phone:+92-51-111-555-666 Fax: +92-51-4486705
Email: info@cust.edu.pk Website: https://www.cust.edu.pk

CERTIFICATE OF APPROVAL

This is to certify that the research work presented in the thesis, entitled "**Chaos Based Image Encryption and Authentication Schemes for Multimedia Applications**" was conducted under the supervision of **Dr. Rashid Ali**. No part of this thesis has been submitted anywhere else for any other degree. This thesis is submitted to the **Department of Mathematics, Capital University of Science and Technology** in partial fulfillment of the requirements for the degree of Doctor in Philosophy in the field of **Mathematics**. The open defence of the thesis was conducted on **December 07, 2022**.

Student Name : Tahir Sajjad Ali (DMT-151011) Tahir

The Examining Committee unanimously agrees to award PhD degree in the mentioned field.

Examination Committee :

(a) External Examiner 1: Dr. Tariq Shah
Professor
QAU, Islamabad
Tariq Shah

(b) External Examiner 2: Dr. Shabieh Farwa
Associate Professor
CUI, Wah Cantt Campus

(c) Internal Examiner : Dr. Abdul Rehman Kashif
Associate Professor
CUST, Islamabad
ARKashif

Supervisor Name : Dr. Rashid Ali
Associate Professor
CUST, Islamabad

Name of HoD : Dr. Muhammad Sagheer
Professor
CUST, Islamabad

Name of Dean : Dr. Muhammad Abdul Qadir
Professor
CUST, Islamabad

AUTHOR'S DECLARATION

I, **Tahir Sajjad Ali (Registration No. DMT151011)**, hereby state that my PhD thesis entitled, '**Chaos Based Image Encryption and Authentication Schemes for Multimedia Applications**' 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/ world.

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

Tahir

(Tahir Sajjad Ali)

Registration No : DMT151011

Dated: 07- December, 2022

PLAGIARISM UNDERTAKING

I solemnly declare that research work presented in the thesis titled "**Chaos Based Image Encryption and Authentication Schemes for Multimedia Applications**" 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 PhD Degree, the University reserves the right to withdraw/ revoke my PhD 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 thesis.

Tahir

(Tahir Sajjad Ali)

Registration No : DMT-151011

Dated: 07 - December, 2022

List of Publications

It is certified that following publication(s) have been made out of the research work that has been carried out for this thesis:-

1. **T. S. Ali**, R. Ali, “A new chaos based color image encryption algorithm using permutation substitution and Boolean operation,” *Multimedia Tools and Applications*, vol. 79, pp. 19853-19873, 2020.
2. **T. S. Ali**, R. Ali, “A novel medical image signcryption scheme using TLTS and Henon chaotic map,” *IEEE Access*, vol. 8, pp. 71974-71992, 2020.
3. **T. S. Ali**, R. Ali, “A novel color image encryption scheme based on a new dynamic compound chaotic map and S-box,” *Multimedia Tools and Applications*, vol. 81, pp. 20585-20609, 2022.

Tahir Sajjad Ali
(Registration No. DMT151011)

Acknowledgements

All praises are for Allah Almighty, the Most Gracious and the Most Merciful, who gave me the strength to complete this task effectively. I would like to express my true gratefulness and heartfelt thanks to my supervisor Dr. Rashid Ali, for his innovative direction, intellectual support, invigorating discussion and inspiring words. I am appreciative for his astounding friendliness and wonderful attitude.

I would like to extend my gratitude to my teachers Dr. Shafqat Hussain, Dr. Muhammad Afzal, Dr. Abdur Rehman Kashif and specially Dr. Muhammad Sagheer for encouragement, invaluable advice, critical comments and constructive contribution.

I am obligated to my Parents for their trust in me that built my confidence to perform this work. Great thanks from my heart for their prayers, my success is really the fruit of their devoted prayers and encouragement, their support in a number of ways must also be acknowledged here.

I must express my very deep appreciation to my family members for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without them.

Finally, to me, there is nothing better than having good friends so with great pride I am very thankful to my Friends who helped me to bring this research project to fruition.

Thank you.

Tahir Sajjad Ali

Abstract

In modern technological era image encryption has become an attractive and interesting field for researchers. The work has been taken for improving the security of image data from unauthorized sources. Chaos theory, due to its randomness and unpredictable behaviors, is considered favorite for the purpose of image encryption. This study presents various image encryption schemes based on simple as well as compound chaotic maps. These techniques use S-box for confusion and Boolean function XOR for diffusion purpose.

Another aspect of this study is the use of chaotic map to deal with the images in telemedicine. In telemedicine, images based on patient diagnostic tests and reports are usually required to broadcast securely so that recipient can receive them without any error. For the secure communication of sensitive medical data, there is a need of authenticated and unforgeable cryptosystem. A novel medical image signcryption algorithm is presented that provides confidentiality, integrity, authentication, non repudiation, forward secrecy for sensitive data transmission.

Contents

List of Figures

List of Tables

Abbreviations

AES	Advanced Encryption Standard
DES	Data Encryption Standard
DICOM	Digital Imaging and Communications in Medicine
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie Hellman Problem
ECDLP	Elliptic Curve Discrete Logarithm Problem
ISO	International Standard Organization
MSE	Mean Square Error
NPCR	Number of Pixel Change Rate
PSNR	Peak Signal to Noise Ratio
PWLCM	Piece-wise Linear Chaotic Map
RGB	Red Green Blue
RSA	Rivest Shamir Adleman
S-box	Substitution Box
SET	S-box Evaluation Tool
TLTS	Tent Logistic Tent System
UACI	Unified Averaded Changing Intensity
XOR	Exclusive OR

Symbols

C_r	Pearson correlation coefficient
$E(\mathbb{F}_P)$	Points of elliptic curve with coordinates in $\mathbb{F}_P$
$\oplus$	Exclusive OR
F	Field
$\lfloor x_n \rfloor$	Floor function of x returns the largest integer no larger than x.
$\mathrm{gcd}(a,\, b)$	Greatest common divisor of a and b
G	Group
GF	Galois field
$\min(r_k)$	Minimum value of the sequence r_k
$\max(r_k)$	Maximum value of the sequence r_k
$\mathcal{O}$	Big-$\mathcal{O}$ notation
$\mathrm{P}(g)$	Probability of g
$\mathbb{R}$	Set of real number
R	Ring
$\mathbb{Z}$	Set of integers
$\mathbb{Z}_n$	Set of integers under modulo n
$\mathbb{Z}_p$	Set of integers under modulo p (a prime number p)

Chapter 1

Introduction

Due to rapid development in the field of information technology, the secure commercial and private communication has become an essential requirement. 21st century is the century of innovation and technology. In its early years, a rapid progress is seen in every aspect of life. Social media and communication sector revolutionized in previous two decades. They have completely changed the way people communicate and socialize on the internet. Social networking does, unfortunately, have certain drawbacks. Some of these are cyberbullying [1] online harassment [2] and privacy theft. Giving personal information on social media sites might expose users to crimes such as stalking, identity theft, and other forms of harassment.

The current era of digital technology, such as the internet, the internet of things (IoT), and big data, has virtually transformed all nations' culture. With the advancement of technology and its widespread usage to preserve, store, and transfer a large amount of sensitive and important information in all sectors of life, maintaining information confidentiality has become a serious concern. Due to the rapid increase in computing power, the stakes for digital security are now higher than ever. The fast and efficient technology enables people to secure their valuable information. Adversaries are always there to thwart secret information during the communication. To combat the data breaching, a strong defense is essential.

Cryptography has been crucial in the secure transmission of sensitive information between two or more persons. Cryptography's basic goal is to share information among participants in such a way that adversarial threats are minimized.

The next section gives a brief introduction and literature review of cryptogyaphy, encryption and signcryption techniques to protect the multi-media information. Section 1.2 presents the contribution of the thesis and, finally layout of the thesis is provided in Section 1.3.

1.1 Literature Review

The literature review covers various aspects of multimedia content security. In the first section cryptography its introduction and types with historical background is presented. In Section 1.1.2 image encryption and related work from the literature is discussed. Section 1.1.3 describes the origination and progressive work for the security of image based data. Medical images, their importance and encryption techniques from the literature are stated in Section 1.1.4, while the Section 1.1.5 covers the introduction and related research for medical image signcryption techniques.

1.1.1 Cryptography

Cryptography is the study of methods and strategies for changing a secret message so that only an authorised recipient with a secret key can decrypt it. If a third party (enemy or hacker) intercepts the message during transmission, he should not be able to extract the original information.

The term 'cryptosystem', a short for 'cryptographic system' is a computer system that is used to protect data during the communications. The important ingredients of cryptosystem are: the message which has to be encrypted is known as plaintext, encryption algorithm transforms data into another form, called a ciphertext, that is very difficult to understand by unauthorized people.

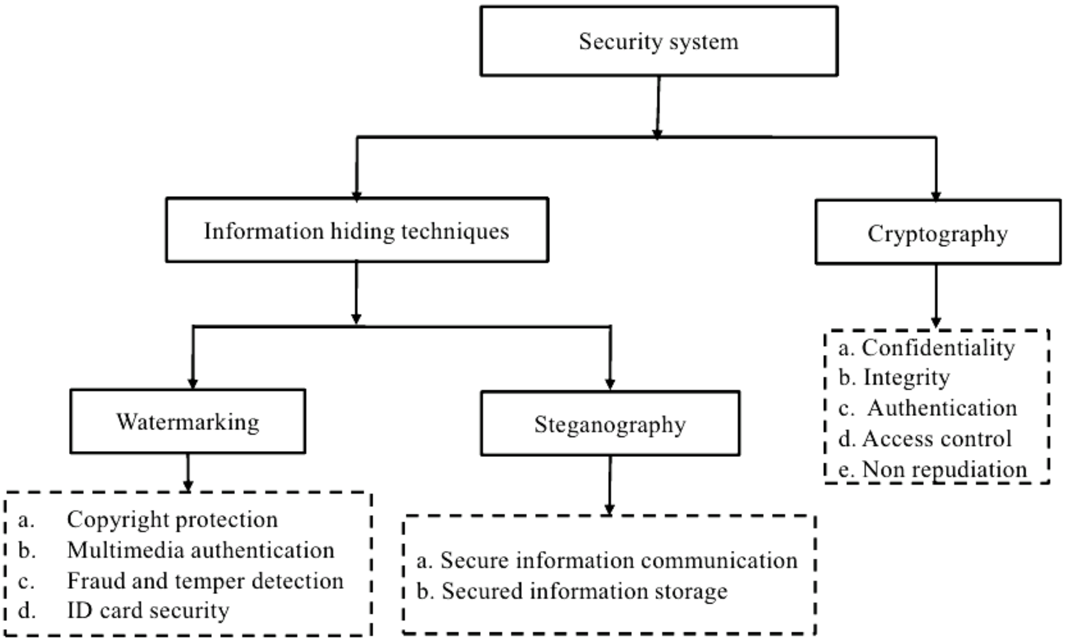


Figure 1.1: Information security systems

The above mentioned Figure 1.1 is taken from [3] that depicts the information security system and different techniques adopted for this purpose. According to the above figure a security system can provide data protection between communicating parties using two different ways, that are information hiding techniques and cryptographic modes. The information hiding techniques involves the methods of water marking and steganography. In water marking techniques, a water mark sign is dispatched on the secret information that fully or partially hides the original information. The main purpose of using this technique for information security is that it gives copyright protection. It is famous for providing multimedia authentication. It provides protection against fraud and temper detection and makes secure the identity of the sender, while in steganography the original message is changed into another coded form using a defined coding pattern. The steganographic techniques provide the way for secure information communication and also provide secure information storage. Cryptography is a secret key based secure communication technique that provides many security features like confidentiality, authentication, non repudiation, integrity etc.

In cryptography a secret key is a part of information that is used to provide the output of any cryptographic algorithm or cipher. Without the use of a secret key, a cryptographic algorithm would not generate any useful information. During the encryption process a particular transformation takes secret key and turns plaintext into ciphertext, or vice versa during decryption. In decryption process an encrypted message (ciphertext) is transformed into its original shape.

The two main branches of cryptography are called, symmetric (secret) key cryptography and asymmetric (public) key cryptography. In symmetric (secret) key cryptography, the key which is used to encrypt and decrypt data is shared between two (or more) parties. The security of symmetric key cryptography relies on keeping the key secret by each communicating party. DES (Data Encryption Standard) [4], introduced in 1977, is the most well-known cryptographic method in the literature. It was a block cipher that had been widely used until, it was discovered to be insecure and superseded by AES (Advanced Encryption Standard) [5]. AES is also a block cipher that runs through three different rounds. The S-box is the main component that provides non-linearity and confusion in the resulting ciphertext.

S-box can be used in a variety of ways in image encryption [6, 7], low profile mobile applications [8], multimedia encryption [9], watermarking [10], and steganography [11]. Nowadays researchers use different optimization approaches [12–15] to optimize the performance of S-box.

On the other hand in asymmetric (public) key cryptography, a pair of keys for each party is being used. In this set, one key is kept "public" and the other is kept "secret". The secret key is maintained as a secret and only known by the communication parties, the public key is known to both parties. Asymmetric key cryptography uses, for instance: Diffie Hellman key exchange protocol [16], RSA [17], Elliptic curve cryptography (ECC) [18] etc.

1.1.2 Image Encryption

Another aspect of cryptography is its huge use for the security in multimedia communication over the internet. Security of confidential image based data has become an essential requirement for communication purpose and images stored in different databases [19]. Image encryption is the process of transforming a plain-image into a cipherimage, whereas image decryption is its opposite process. Image encryption schemes are mainly used to maintain image security by converting plain images into another images, that are difficult to recognize. For maintaining image confidentiality between two users, it is required that nobody else could meet the content of image without having proper key for decryption. Image and video encryption have vast application in many fields like internet communication [20], medical imaging [21], multimedia systems [22], telemedicine [23] etc.

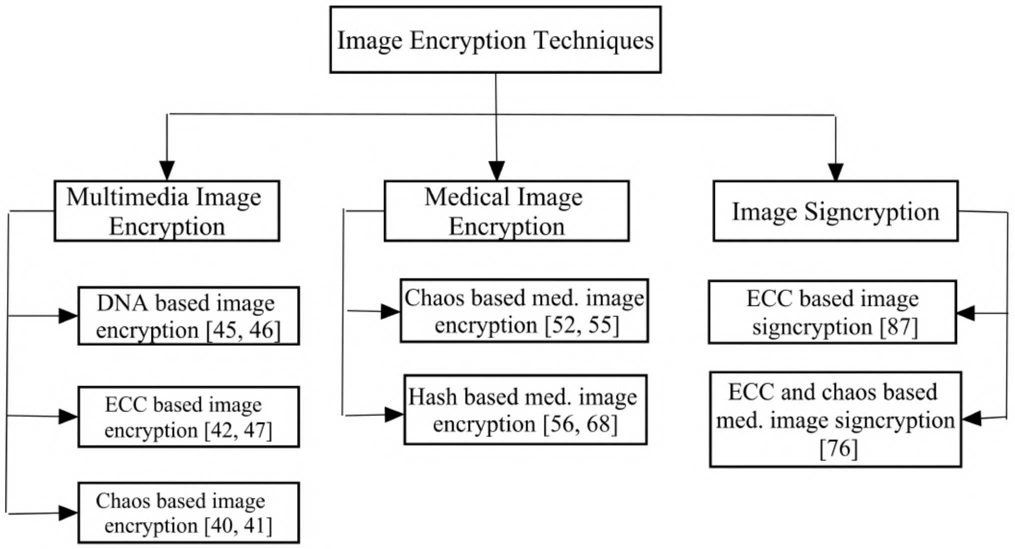


Image Encryption Techniques
Multimedia Image Encryption
Medical Image Encryption
Image Signcryption
DNA based image encryption [45, 46]
ECC based image encryption [42, 47]
Chaos based image encryption [40, 41]
Chaos based med. image encryption [52, 55]
Hash based med. image encryption [56, 68]
ECC based image signcryption [87]
ECC and chaos based med. image signcryption [76]

Figure 1.2: Classification of image encryption schemes

In Figure 1.2 a classification of image encryption techniques is shown. According to the scope of this study, image encryption techniques are divided into three ma in categories that are multimedia image encryption techniques, medical image encryption techniques and image signcryption techniques. Different structures are used for the encryption purposes of multimedia images for example using DNA, Zhang and Wang [45] devised a multi-image encryption technique. The use of DNA was suggested as a method of image encryption by Yousif *et al.* [46]. Elliptic curve cryptography is also used for the encryption purpose of multmedia images. Luo *et al.* [42] proposed image encryption method based on elliptic curve Elgamal cryptosystem. A unique image encryption method based on the elliptic curve over finite rings was developed by Hayat *et al.* [47]. Use of chaotic maps for the encryption of multi-media information has become a recent trend. A chaotic sequence-based image encryption method related to plaintext was proposed by Ma *et al.* [40]. Another technique is proposed by Li *et al.* [41] that uses Arnold chaotic map for multi media image encryption.

Security of medical information is another aspect of image encryption mechanism as shown in Figure 1.2. Many encryption techniques are proposed for this purpose. Chen and Hu [55] used multiple chaotic maps to protect medical images. Reyad *et al.* [56] used hash enhanced elliptic curve based medical image encryprtion scheme. Wong [68] also used hash function to generate cryptography based trust center for securing medical images. Image signcryption is another way used for secure image transmission. Saini and Vaisla in [87] presented an elliptic curve based image signcryption technique. Recently Ali and Ali [76] developed a method for securely transmitting medical images that uses chaos theory-based signcryption.

In 1989, Matthews [24] initiated the concept that, under certain conditions, easy non-linear iterative functions have tendency of producing chaotic sequences of random numbers. He created a chaotic function and suggested that it would be useful for cryptography. He developed and applied a key stream based on a well-known logistic chaotic chaotic map [25] also used it for encryption of secret information. Habutsu [26] introduced the use of chaos for cryptography in 1991. His proposed symmetric key encryption scheme involves one dimensional chaotic map and its iteration known as tent map [27].

Later on 1998 Fridrich [28] developed a method for encrypting images that makes use of chaotic maps. The main aspects of his proposed encryption scheme were large block size, variable key length and efficient encryption. The cipherimage was generated by using two dimensional chaotic maps. He had used these chaotic maps to produce complex, key dependent permutations. Then in 2004 Chen *et al.* [29] and Mao [30] used 3D chaotic cat map and baker map for generating permutations in image encryption scheme. Guan *et al.* [31] in 2005 employed 2D cat map and Chen's map for permutation in pixel position and also for pixel value masking. In 2009 Patidar *et al.* [32] suggested substitution-diffusion type image encryption scheme that employs chaotic logistic and standard maps as part of its encryption scheme. The proposed scheme was robust having confusion and diffusion properties. He also put forth a modified version [33] of his technique that was more resistant to known and chosen attacks using plaintext. In 2011 Francois et al. [34] used coupling of chaotic functions and XOR operator in image encryption scheme. The main features of his scheme were the ability of producing large key space, possessing confusion and diffusion properties and encrypt images with any entropy structure. Zhang *et al.* [35] developed a spatial-temporal chaos of mixed linear-nonlinear coupled map lattices-based encryption technique in 2014. In proposed scheme he used the technique of bit level pixel-permutation that enables the permutation of pixels' lower and higher-bit planes in an image. In [36], an encryption approach made use of a parametric switching chaotic system and its accompanying transforms.

The growing popularity of digital images has increased the problems concerning with the security, storage and transportation of secret images. A variety of cryptographic schemes such as image steganography [37], copy detection [38] and image encryption [6, 7, 39–48] for the protection of secret images during communication are proposed.

1.1.3 Medical Image Encryption

With the advancement in tele-medicine field the security of medical images is becoming more important. The use of modern computer based technology has revolutionized the health-care system. Recent advancements in public health-care system provides an easy way to access patient's health record, treatment history, and medicine used records through cloud storage for effective health delivery. The malicious activities on cyber infrastructure are increasing day by day, therefore the security requirements of health-care sector are also rising. Medical images are dominant part of health infrastructure. In e-health system DICOM (digital images communication in medicine) [49] is considered as standard (ISO 12052 [50]) for medical imaging. It provides the details about the bio-medical structure of organ, being examined. Many advanced tools are invented for the diagnostic purpose of pre-medical analysis and examination using DICOM system. These tools are based on imaging technology using signal processing to get the vision of internal body systems. Nowadays surgical operations are guided by sensors and artificial intelligence [51]. These real time information systems collaborate in real time surgical operations.

As medical data is mostly occurred in image format, therefore a rigorous security approach is required to secure it. In e-health care system, there are serious threats to data containing secret information of a patient's health reports. During the management and transmission of health-care data to third parties like private/public or hybrid clouds, there may occur many problems about the safety and security of this data. Therefore an efficient and robust approach is required to provide secure transmission of sensitive medical data along-with its authentication over public networks.

Many conventional approaches like DES, AES, RSA etc, are not suitable to protect sensitive records in DICOM system [52] due to large storage requirements and long computational time. In 2012 Mohamed et al. [53] suggested an image encryption system based on chaos and compared the simulation results with AES against NPCR (number of pixel change rate), UACI (unified average changing intensity) [54], correlation among the pixels in cipher image, histogram analysis and encryption time. On the basis of the above security tests it was concluded that for digital multimedia data, the traditionally used cryptographic schemes are less suitable. Recently in 2017 Chen and Hu [55] used multiple chaotic mappings for adaptive medical image encryption. A hash-based method of medical image encryption was presented by Rayed *et al.* [56]. Rajendran *et al* [57] in 2021 proposed a secure medical image transmission model based on chaos theory for the use in IoT-Powered healthcare systems.

1.1.4 Signcryption

Encryption and authentication are two essential primitives of cryptography. These are vastly used for maintaining privacy of communication. Authenticated encryption (AE) [58] simultaneously offers encryption along with data authenticity and confidentiality of secret data. For this purpose authenticated encryption combines symmetric encryption scheme and message authentication code (MAC) [59]. Other methods used for protection and authentication are; sign-then-encrypt, encrypt-then-sign, sign and encrypt and authenticated encryption with associated data (AEAD). But these cryptographic protocols take extra computational efforts. In 1997 Zheng [60] combined these primitives in a single operation and named it "signcryption". It takes less computational cost and effort. Signcryption provides confidentiality, integrity, authentication of information and non-repudiation. Therefore, the signcryption technique is used in many applications like electronic transaction protocols [61], key management [62], routing protocols [63] etc. It also plays an important role in cloud computing [64] and internet of things [65].

In contrast to signing then encrypting, Deng and Bao's [66] suggested signcryption approach reduces computational cost to 16% and communicational cost to 85%. But their proposed scheme is less efficient than that of Zheng [60]. Mahmood and Dony [67] have proposed an enhanced segmentation based medical image encryption scheme. Region of interest (ROI) and region of background (ROB) are the two categories into which medical images are classified in this method.. It uses AES and Gold code (GC) algorithm to reduce computational time and also to provide hybrid design of encryption. Wong [68] proposed the idea of a digital trust center in 1996. It provides confidentiality and authenticity of digital images in hospitals.

In order to encrypt data, Eldayem *et al.* [69] in 2013 presented an encryption method. They used watermarking technique and MD5 hash function for integrity of images. Their proposed scheme provides patient authentication, image integrity and patient information confidentiality. Bhopi *et al.* [70] in 2016 proposed a method for the security of medical images. In this proposed work, medical image encryption (MIE) is taken in two stages. In the first stage rotation is performed row-wise, column-wise and diagonally using binary keys. In the second phase four chaotic logistic maps are used to generate pseudo random sequences. Pixel value permutation is performed with these generated sequences.

Singh and Singh [71] used elliptic curve cryptography for encryption, decryption and digital signature of cipher image to give the authenticity and integrity. Shukla *et al.* [72] proposed an image encryption scheme that uses Elgamel elliptic curve encryption with smaller key size. It reduces storing and transmission requirements. The scheme also provides confidentiality, authentication and integrity.

Cao *et al.* [73] proposed a method of medical image encryption using edge maps. The proposed method consists of bit plane decomposition, chaotic sequence generation and scrambling technique.

Many other methods based on chaos theory such as proposed by Dhall *et al.* [74] offers a probabilistic symmetric encryption method that takes a customized block size and appropriate for image encryption. It is computationally efficient because it uses a Random Bits Insertion phase. Additionally, this stage aids in boosting entropy and uniforming the intensity distribution within the cipher. The size of the created ciphertext is two times that of plaintext. The results demonstrate that the technique provides good resistance to statistical and cryptographic attacks.

In 2018 Ye *et al.* [75] introduce a novel and effective pixel-level picture encryption technique. The proposed method improves the relationship between position shifting for pixels and value shifting for greyness in comparison to the conventional permutation-diffusion architecture.

Before performing the diffusion operation, a rewriting function is performed to the permuted image as a workaround for permutation's inability to alter the frequency of pixels. Additionally, the plainimage is a requirement for the keystream's architecture. Consequently, the suggested technique can interfere with the chosen plainimage and known plainimage attacks.

A one time key based technique was proposed by Liu and Wang [77]. In order to enhance dynamical deterioration and obtain excellent security, they Used the piecewise linear chaotic map to produce a pseudo-random key-stream sequence. The MD5 of the mouse positions, which are actual random number generators, produced the initial conditions. They used the technique to encrypt the color image and achieved the desired level of security. The resulting cipherimage is resistant to noise and renders known attack impractical.

Liu and Wang [78] suggested a method for image encryption that makes advantage of high-dimensional chaotic maps and bit level permutation. The key space of this scheme is sufficiently large to fend off typical attacks.

DNA sequence operations were used by Wang *et al.* [79] for image encryption scheme. They suggestion the creation and the use of the new initial conditions for the CML, which can cause the encryption outcome to be highly dependent on each pixel of the original image. Then, the DNA matrix's rows and columns are switched around. Once more, the perverted DNA matrix is confused. Finally, by utilizing DNA decoding rule, a cipher image is acquired. Experimental findings demonstrate the scheme's ability to fend against different attacks.

An image encryption method based on the dynamic random growth methodology was suggested by Wang *et al.* [80] in 2015. The image block, in this technique is used to calculate an intermediate parameter in the diffusion process. The intermediate parameter is used as the initial parameter of chaotic map. As a result, the created key streams depends on plainimages.

Wang *et al.* use perceptron model [81] for the encryption of multi-media images. There are some non chaos based methods for image encryption that use compressive sensing [82], non adjacent coupled mapped lattices [35, 83], parallel computing system [84], based on the principle of the matrix semi-tensor product, synchronously updating Boolean networks [85] and JPEG compression algorithm [86]. All these methods do not provide information about the key distribution or the authentication, non repudiation, integrity, unforgeability, forward secracy etc. In 2014 [87] proposed an image signcryption scheme based on ECC that fulfills the above discussed security parameters. Another signcryption scheme based on chaotic maps and ECC [76] for medical images is proposed in Chapter 6 for the security of sensitive medical images.

1.2 Contribution of Thesis

With the recent developments in the field of wireless network communication technology, digital image transfer over the internet has become widely used source of communication in many public and private services like medical imaging, satellite communication, military intelligence sharing, confidential multimedia messaging etc. Meanwhile many activities took place to forge, get illegal access or intercept the secret communication.

Therefore a high level, reliable and robust security mechanism is necessary to prevent the unauthorised usage of digital images. Image encryption is a method deployed to provide a secure way of image transmission. It provides security in communication over open networks. The main contribution of the thesis is presented below:

- Based on 1-dimensional chaotic maps, an image encryption scheme is presented in Chapter 4. A detailed security analysis is also performed that tells the proposed scheme presented good results for correlation and entropy analysis, while a comparable performance is observed against NPCR (number of pixel change rate), UACI (unified average changing intensity), noise and data loss attacks. The investigated work is published as "A new chaos based color image encryption algorithm using permutation substitution and Boolean operation" in a well reputed international journal [7].
- A compound chaotic map is used to build an image encryption technique. The compound chaotic map provides a large chaotic range than the tent

and logistic maps. It does not have periodic windows and have uniformly distributed output in [0, 1]. Use of this chaotic map in encryption scheme increase the internal complexity and security of the proposed scheme. The analysis results shows that hence generated scheme provides huge key space and good complexity to resist the cryptographic attacks. While the other analysis indicators shows the satisfactory results. This study [88] is published in a reputed international journal.

- A new medical image signcryption scheme is proposed that uses two chaotic maps. These maps have large Lyapunov exponents that ensures their chaotic behavior, also provide uniformly distributed output. The proposed medical image signcryption scheme provides key generation, digital signature and authentication mechanism. These additional security features makes the communication of sensitive medical image more safe and secure. Due to these properties it seems to be the first image sincryption scheme that deals with sensitive medical images. The work and its finding are published as "A novel medical image signcryption scheme using TLTS and Henon chaotic map" in IEEE ACCESS [76] and available in 'open access' for further study and analysis.

1.3 Organization of Thesis

The rest of the work presented in this thesis is organized as follows:

- **Chapter 2** presents the review of some fundamental concepts of mathematics. It includes the introduction of elliptic curves, brief review of the properties of elliptic curves and operations on elliptic curves. The introduction of chaos theory, its properties and some commonly used chaotic maps are also the parts of this chapter.

- **Chapter 3** covers certain essential features and background of cryptography. The introduction of cryptography, its types, objectives, digital signature and public key based cryptographic schemes and different possible cryptographic attacks are presented in this chapter. It also provides the information about a digital image, its different features, encryption mechanism and analysis techniques.

- **Chapter 4** includes a proposed chaos based image encryption scheme. The scheme contains the image encryption/decryption algorithm, results and discussion with the help of examples and figures, security analysis of the scheme and its comparison with other such schemes.

- **Chapter 5** shows a chaos based image encryption scheme. It contains S-box and its construction technique, proposed image encryption and image decryption algorithm results and discussions with the help of examples and figures. The security analysis is provided with the help of key space analysis, distribution of pixels in original and cipher images, correlation analysis, information entropy mean squared error, peak signal to noise ratio, complexity analysis and the speed analysis of proposed encryption scheme.

- **Chapter 6** introduces proposed signcryption scheme for medical images. It consists of global parameter setting, the key generation process, image signcryption/unsigncryption algorithm. The correctness of the proposed algorithm and complete security analysis of the image encryption, signcryption attributes their comparison and possible attack model are also discussed.

- **Chapter 7** provides the conclusion of thesis and some suggestions for the future work are accommodated.

Chapter 2

Mathematical Background

Modern cryptography uses the fundamental concepts of mathematics involving algebra, number theory, chaos theory etc. Therefore it is necessary to review some basic concepts of these scientific disciplines before the study of cryptography. Section 2.1 is focused on the introduction of elliptic curve its types, also a brief review of the properties of elliptic curves and operations on elliptic curve are presented here. Then the introduction of chaos theory, types of chaotic maps, their advantages and disadvantages, properties of some commonly used chaotic maps and their selection criteria are given in Section 2.2.

2.1 Elliptic Curve

It is a smooth algebraic curve that is defined by a certain type of cubic equation in two variables. The concept of elliptic curves is taken from algebraic geometry, that is a sub-field of mathematics and focuses on the study of algebraic varieties. An algebraic variety is actually the locus that is defined by a polynomial equation. the collection of solutions of polynomial equations with real or complex numbers. Algebraic curve is produced by dimension one's algebraic variety. An algebraic curve is a bivariate polynomial equation whose solution defines a set of points of the Euclidean plane. Elliptic curves are not actually ellipses. They are so named because they are defined in cubic equations similar to that used for the measure of ellipse circumference. The operations used in elliptic curve based schemes include point doubling and adding, are computationally more efficient than RSA exponentiation. Elliptic curve theory is used in many computational problems involving the group law and also in cryptographic applications. The main benefit of using ECC is that, with significantly smaller key sizes, ECC can give the same cryptographic strength as an RSA-based system [89] as shown in Table 2.1.

Table 2.1: Comparison of the key size of ECC with RSA

RSA key size (bits)	**ECC key size (bits)**	**Key size ratio**	**Cost ratio**
1024	160	1:7	1:3
2048	224	1:10	1:6
3072	256	1:12	1:10
7680	384	1:20	1:32
15360	521	1:30	1:64

2.1.1 Elliptic Curve over $\mathbb{R}$

It is defined as the set of all points (x, y) satisfying the following equation,

$$y^2 = x^3 + ax + b \tag{2.1}$$

where the parameters $a, b \in \mathbb{R}$ follow the relation

$$4a^3 + 27b^2 \neq 0.$$

In the above Equation (2.1) constants a, b and variables x, y are real numbers. The set of points that satisfies the Equation (2.1) are denoted by $E_{\mathbb{R}}(a, b)$. Cryptography typically employs elliptic curves because they provide a large number of finite abelian groups with rich algebraic structures. For the geometrical interpretation of elliptic curve over real number $\mathbb{R}$, an elliptic curve is considered as shown below:

$$E_{\mathbb{R}}(1, 6) : y^2 = x^3 + x + 6 \tag{2.2}$$

In the above shown elliptic curve $a = 1,\ b = 6$ and variable $x, y \in \mathbb{R}$. The set of points satisfying Equation (2.2) are depicted through a graph in Figure 2.1.

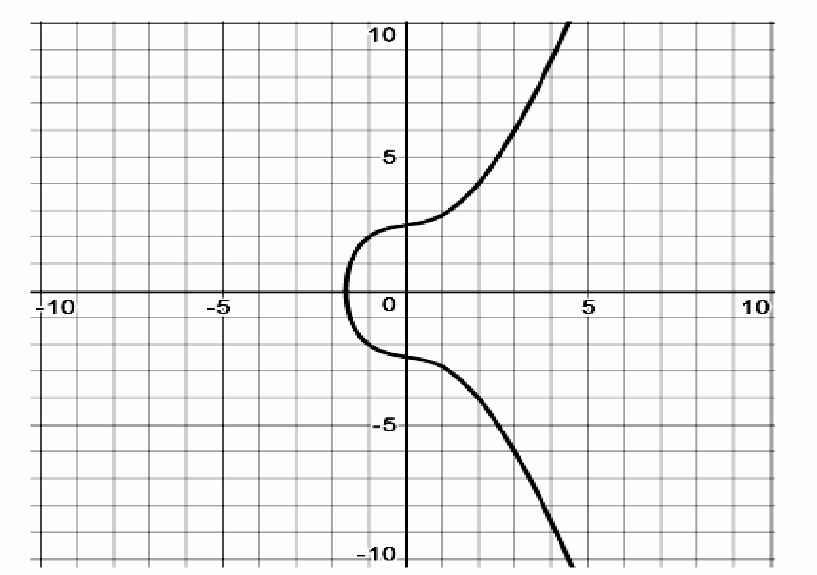


FIGURE 2.1: Elliptic curve

In the next discussion the algebraic description of points of elliptic curves along with its geometrical interpretation will be given.

Definition 2.1.1.

Let $P = (x_1,\ y_1)$ and $Q = (x_2,\ y_2)$ be two distinct elliptic curve points, that satisfy the elliptic curve 2.1, then their addition is defined as:

$$\begin{gathered} R(x_3,\ y_3) = P(x_1,\ y_1) + Q(x_2,\ y_2) \\ x_3 = m^2 - x_1 - x_2 \\ y_3 = m(x_1 - x_3) - y_1 \\ m = \frac{y_2 - y_1}{x_2 - x_1} \end{gathered} \tag{2.3}$$

The resulting point of addition $R = (x_3,\ y_3)$ (the negative of S) can be obtained by performing the calculations as shown in Equation (2.3).

For two points $P(2,4)$ and $Q(-1,2)$ of elliptic curve (2.2), their sum R *i.e,*

$$R = P + Q$$

is represented in Figure 2.4. In this figure, for the addition of two points P and Q, a tangent line through these points is drawn that intersects the curve at another point S. To find the required point R, that is the sum of P and Q, first find additive inverse of S *i.e.,*$-S$. The point R that is the sum of P and Q, is actually $-S$.

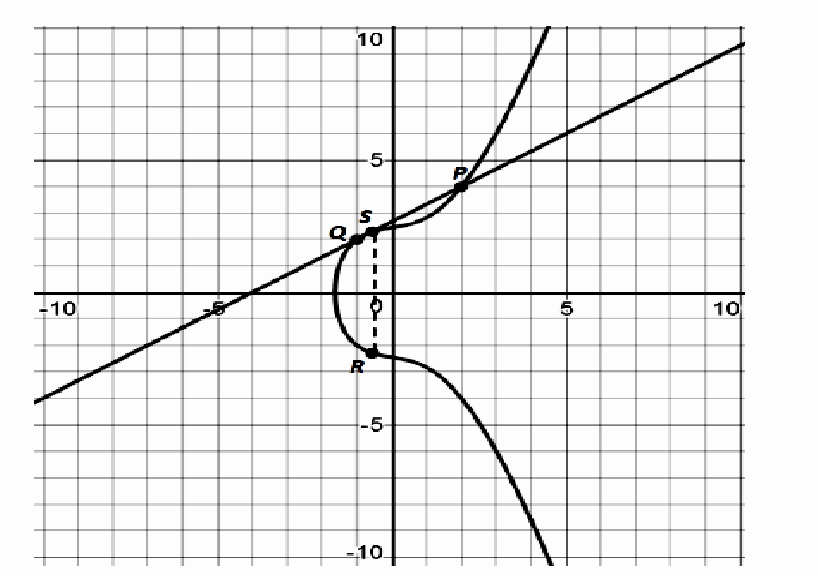


FIGURE 2.2: Elliptic curve point addition

Definition 2.1.2.

For a point $Q(x_1, y_1)$, where $x_1 \neq 0$, lying on the Elliptic curve 2.2, then its addition with itself is called **Elliptic curve point doubling** and it is defined as:

$$\begin{gathered} P'(x_2,\ y_2) = Q(x_1,\ y_1) + Q(x_1,\ y_1) \\ x_2 = m^2 - 2x_1 \\ y_2 = m(x_1 - x_2) - y_1 \\ m = \frac{3(x_1)^2 + a}{2y_1} \end{gathered} \tag{2.4}$$

The resulting point of such addition is another point $P'(x_2,\ y_2)$, where $P' = 2Q$. The coordinates of this point P' are obtained by taking the calculations shown in Equation (2.4).

For a point $Q = (-1, 2)$ and its sum with itself can be displayed by drawing a tangent line through Q intersecting the elliptic curve at another point P. Then the additive inverse of P *i.e,* P' will give the resulting point obtained from the point doubling of Q. The geometrical interpretation of point doubling for Q is shown in 2.5.

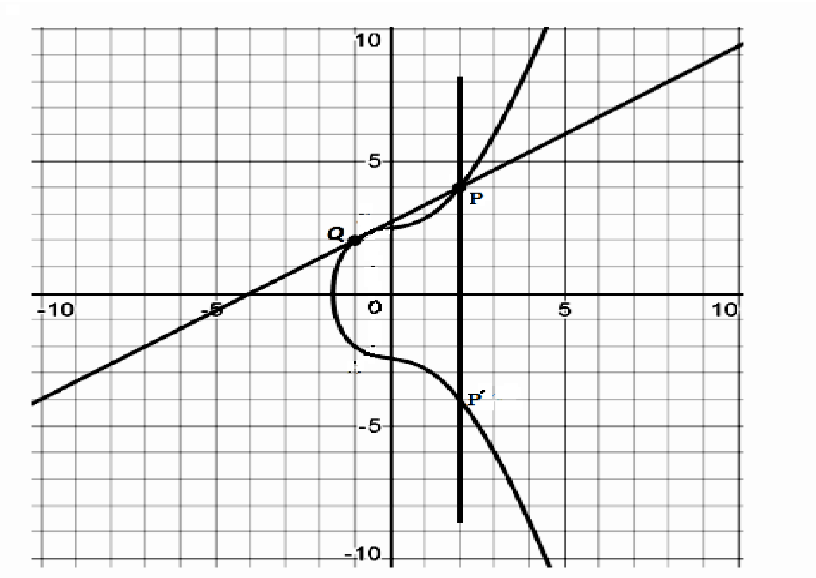


Figure 2.3: Elliptic curve point doubling

2.1.2 Elliptic Curve over a Finite Field

In cryptography, it is a general interest to define a group on elliptic curve over a finite field denoted by $E_F(a,b)$. The concept of the use of elliptic curve in cryptography was presented independently by Koblitz [90] and Miller [91] in 1985. Over a finite field, an elliptic curve is defined by a two-variable cubic equation using some coefficients. The equation for elliptic curve over GF(p) is:

$$E_p(a,b) = \{(x,y) : (y^2 = x^3 + ax + b) \bmod p\} \cup \{\mathcal{O}\}, \tag{2.5}$$

where the point (x,y) lies on the elliptic curve E and $\mathcal{O}$ is a point at infinity. The determinant $4a^3 + 27b^2 \neq 0$ where a, $b \in \mathbb{F}_p$ ensures that this curve is not singular and has distinct roots. It basically ensures that there are no vertices or self-intersections in the curve. The advantage for working in $\mathbb{F}_p$ over $\mathbb{R}$ is that the modulo p must be used in each operation, while the graph does not form a curve; instead, it shows scattered points.

Example 2.1.3.

An elliptic curve over GF(p) is considered as an example where the prime number $p = 23$ is used in Equation (2.6) as mod and by using the constants $a = 1$ and $b = 1$ as well, the elliptic curve generated in this way is:

$$y^2 = x^3 + x + 1 \pmod{23} \tag{2.6}$$

Now the set of residues $\mathbb{Z}_{23} = \{0, 1, 2, \cdots, 22\}$ is used to calculate the quadratic residue (*i.e.,* an integer which is congruent to a perfect square modulo 23) $\mathbb{Q}_{23}$ as in the table given below.

TABLE 2.2: Quadratic residue $\mathbb{Q}_{23}$ of Elliptic curve (2.6)

x^2 **mod 23**	$(p-x)^2$ **mod 23**	**value**
$(1)^2$	$(22)^2$	1
$(2)^2$	$(21)^2$	4
$(3)^2$	$(20)^2$	9
$(4)^2$	$(19)^2$	16
$(5)^2$	$(18)^2$	2
$(6)^2$	$(17)^2$	13
$(7)^2$	$(16)^2$	3
$(8)^2$	$(15)^2$	18
$(9)^2$	$(14)^2$	12
$(10)^2$	$(13)^2$	8
$(11)^2$	$(12)^2$	6

Hence $\mathbb{Q}_{23} = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$ are $\dfrac{p-1}{2} = 11$ quadratic residues. A necessary condition for Equation (2.6) is also verified to know about its behavior as elliptic curve: *i.e.,*

$$\begin{aligned}
&4a^3 + 27b^2 \neq 0 \pmod{23} \\
&= 4 \times (1)^3 + 27 \times (1)^2 \pmod{23} \\
&= 4 + 27 \pmod{23} \\
&= 31 \pmod{23} \\
&= 8\ (\neq 0) \pmod{23}
\end{aligned}$$

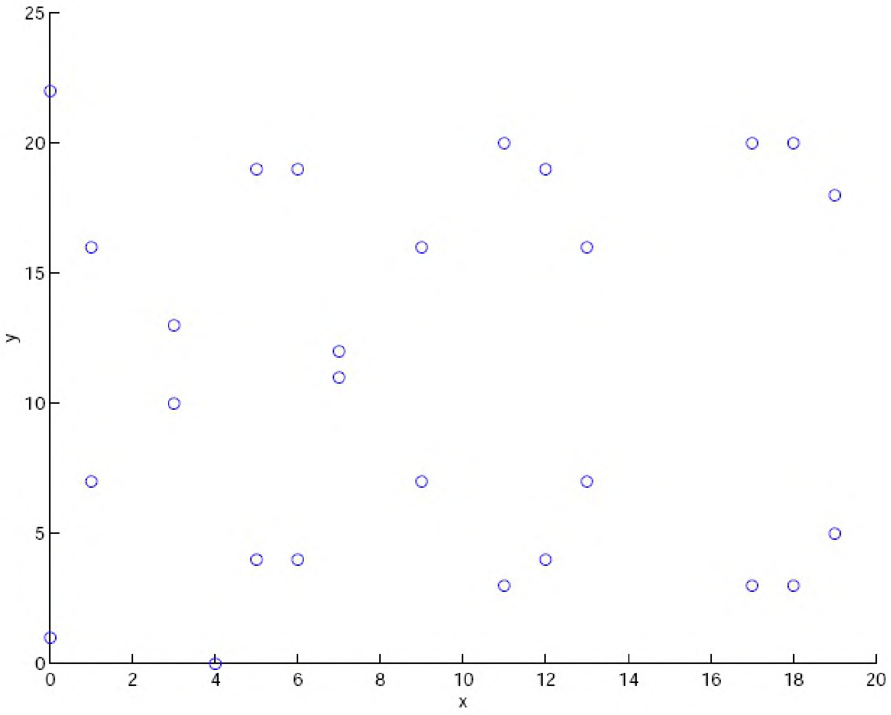


FIGURE 2.4: Scatter diagram of elliptic curve

In the next step, for elliptic curve $y^2 = x^3 + x + 1 \pmod{23}$, where $0 \le x < p$, it is determined that y^2 lies in $\mathbb{Q}_{23}$ or not.

TABLE 2.3: Points of elliptic curve

x	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
y^2	1	3	11	8	0	16	16	6	15	3	22	9
$y^2 \in \mathbb{Q}_{23}$?	√	√	×	√	×	√	√	√	×	√	×	√
y_1	1	7		10	0	4	4	11		7		3
y_2	22	16		13	0	19	19	12		16		20
x	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	
y^2	16	3	22	10	19	9	9	2	17	14	22	
$y^2 \in \mathbb{Q}_{23}$?	√	√	×	×	×	√	√	√	×	×	×	
y_1	4	7				3	3	5				
y_2	19	16				20	20	18				

The elliptic curve $E_{23}(1,1)$ has these points,

$$E_{23}(1,1) = \left\{ \begin{array}{ccccccc} (0,1), & (0,22), & (1,7), & (1,16), & (3,10), & (3,13), & (4,0), \\ (5,4), & (5,19), & (6,4), & (6,19), & (7,11), & (7,12), & (9,7), \\ (9,16), & (11,3), & (11,20), & (12,4), & (12,19), & (13,7), & (13,16), \\ (17,3), & (17,20), & (18,3), & (18,20), & (19,25), & (19,18) & \end{array} \right\}$$

The points of elliptic curve $E_{23}(1,1)$ form a scatter diagram. Figure 2.4 depicts the diagram of above discussed elliptic curve:

2.1.3 Basic ECC Operations

The use of elliptic curves in cryptography, requires certain operations over finite field (Galois Field) with focus on prime field (e.g. $\mathbb{F}_p$), as it gives a fast and precise well defined arithmetic. This section focuses on the elliptic curve operations over a finite field. Let $P = (p_x, p_y)$, represents a point on an elliptic curve, where p_x and p_y must satisfy Equation (2.5) and the coordinates of P must be integers in $\mathbb{F}_p$. One must initially be familiar with elliptic curve point calculations in order to do any significant cryptographic operation. The three commonly utilized point operations that are taken into account by ECC are as follows:

- **Point addition**: Considering the two points of an elliptic curve, $P = (p_x, p_y)$ and $Q = (q_x, q_y)$, then there exists a point $R = (r_x, r_y)$ such that $R = P + Q$ where P is distinct from Q. The coordinates of R can be calculated using the following formulas:

$$s = \frac{p_y - q_y}{p_x - q_x} \pmod{p}$$

$$r_x = s^2 - p_x - q_x \pmod{p}$$

$$r_y = s(p_x - r_x) - p_y \pmod{p}$$

  For each point P on the elliptic curve, there is a point $\mathcal{O}$ at infinity for which $P + (-P) = \mathcal{O}$ and $P + \mathcal{O} = P$ holds.

- **Point doubling**: For any point P on elliptic curve, there exists another point R such that $R = 2P$. By employing the following formulas the coordinates of R can be calculated:

$$s = \frac{3p_x + a}{2p_y} \mod p$$

$$r_x = s^2 - 2p_x - q_x \mod p$$

$$r_y = s(p_x - r_x) - p_y \mod p$$

- **Point multiplication**: One can get the result of a multiplication between one point and a natural number k by only using point addition. The point R can be found such that $R = kP$ by applying k point additions. The simple double and add approach can also be used for such multiplication, which takes only $\mathcal{O}(\log k)$ steps. The inverse of that point multiplication, is known as discrete logarithm. Since the problem is computationally infeasible therefore it is considered as the foundation of ECC cryptosystems. More detail of is given in the next section.

Definition 2.1.4.

"Let g be a primitive root for $\mathbb{F}_p$ and let h be a nonzero element of $\mathbb{F}_p$. The **Discrete Logarithm Problem** (DLP) is the problem of finding an exponent x such that

$$g^x \equiv h \pmod{p}.$$

The number x is called the discrete logarithm of h to the base g and is denoted by $\log_g(h)$." [127]

2.1.4 Elliptic Curve Discrete Logarithm Problem

Elliptic curves provide hard problems like elliptic curve discrete logarithm problem (ECDLP) etc. to use for cryptographic purposes. The (ECDLP) is defined as: for given two values b and S^* of an elliptic curve E, where

$$S = bS^*, \quad (b < p).$$

It is easy to find the value of S, but it is it is computationally infeasible to find the integer b knowing only S and S^*.

2.2 Chaos Theory

Chaos is an interesting phenomenon found in nature (fluid flow, climate and weather, population growth in ecology, time evolution in the magnetic field of celestial bodies) as well as in the laboratories (chemical reactions, electric circuits, magneto mechanical devices, lasers). There are numerous applications of chaotic behaviors in information and communication technologies [92], biology and medicine [93], electrical and communication engineering [94] etc. Chaos theory is the study of seemingly random or unexpected behaviors of the systems that are being governed under the deterministic laws of nature. It is an important mathematical property of many dynamic systems. These are studied as mathematical objects and often used to describe physical phenomenon, biological or economic systems.

2.2.1 Dynamic System

The dynamic system is actually a deterministic mathematical model that uses time as continuous or discrete variable. For the description of generic properties of a dynamic system, it is preferred to take a low dimensional system. For a chaotic map time is taken as an integer value *i.e.* $n \in \mathbb{Z}^+$ and F is the state function that gives back the next state as shown below:

$$x_{n+1} = F(x_n). \tag{2.7}$$

The vector $x_n \in \mathbb{R}^n$ shows the state of system and forms $x(t) = (x_1, x_2, \ldots, x_k)$ are known as state variables, while x_0 or $x(0)$ is the initial condition of the the system is when $t = 0$. The space formed by x is usually known as phase space or state space and considered as Euclidean space. The function F also consists the parameters of map $\mathbf{P} = (p_1,\ p_2, \ldots, p_k)$. A trajectory or an orbit is the set of all those point that start with the initial condition.

Definition 2.2.1.

Butterfly effect actually indicates the sensitivity of a dynamic system towards its initial conditions. It implies that any point in a chaotic system can closely approximated by other points that have substantially different trajectories or future paths. Thus an arbitrarily small change or disruption in the current trajectory can result a dramatically different behaviors in the future state. The name of this phenomenon was suggested by Edward Lorenz in 1972, in his well known article entitled "Predictability: Does the Flap of a Butterfly's Wings in Brazil set off a Tornado in Texas?" [95].

Definition 2.2.2.

A **bifurcation diagram** is a graphic representation of the succession of period-doubling that occurs when control parameter grows. It compares the value of a control parameter to the locations, where the output of dynamic system has concentrated after a few iterations. It also tells about the chaotic region of dynamic system. The chaotic region starts where the bifurcation diagram shows the infinite period of attractors.

Definition 2.2.3.

The concept of **Lyapunov exponen**t for a chaotic map was first presented by Alexander Mikhailovich Lyapunov. He examined the equilibrium and motion of mechanical systems, as well as the stability of rotating liquids. Lyapunov was also interested in probability theory and potential theory. The mathematical description of the Lyapunov exponent of a point sequence x_n is:

$$\lambda = \lim_{n \to \infty} \frac{1}{n} \sum_{l=1}^{n-1} ln|f'(x_l)|. \tag{2.8}$$

The values of $f'(x_l)$ refer to as how fast the neighboring solutions x_n and $\tilde{x}_n$ ($\tilde{x}_n = x_n + \delta x_n$) move away from each other (or move towards each other). The Lyapunov exponent is an assessment tool that uses logarithm for the evaluation of mean expansion rate per iteration of the difference between two infinitesimally close trajectories. The first general analysis for the stability problem for the non-periodic motions was presented by Russian mathematician Lyapunov in 1892 [96]. In the theory of nonlinear processes, the characteristic exponents proposed by Lyapunov have played a central role. The case $\lambda > 0$ is of particular interest. A dynamical system with a positive Lyapunov exponent is said to be chaotic [97].

2.2.2 Some Important Chaotic Maps

Chaotic map are extensively studied as they are the simplest mechanism to generate a complex and chaotic behavior. Chaos theory due to its randomness and unpredictable behavior is considered favorite for many engineering problems, digital communications, cryptographic designs, network behavior modeling etc.

There are mainly two types of chaotic maps.

- Discrete time systems
- Continuous time systems

In discrete chaotic systems change of state occurs only at regularly distributed instants. A difference equation or a map can be used to represent a discrete-time nonlinear dynamical system as follows:

$$x_{n+1} = f(x_n, n; p), \quad n = 0, 1, 2, \cdots$$

where n is shows the time index; $n = 0$ represents the initial time and x_0 is the initial condition of the state x. This system's current state, x_n, is the result of iterating over its prior state, x_{n-1}, according to function f. The earlier state, x_{n-1}, uses the same mode as x_{n-2}, and similarly, the current state of this system can be determined by its initial condition. Examples of discrete time chaotic systems are logistic map [98], pwlcm [99] etc. Computers can easily handle discrete maps, and powerful available microcontrollers can process them. As a result, based on the preceding factors, their employment in commonly used applications is becoming viable nowadays.

A continuous-time nonlinear dynamical system is described by a differential equation:

$$\dot{x} = f(x, t; p), \quad t \in [t_0, \infty)$$

where $x = x(t)$ shows the state of system that belongs to a bounded region $\Omega_x \subset \mathbb{R}^r$, r is the dimension of x, the initial time is t_0 and the initial condition $x_0 = x(t_0) \in \Omega_x$,

p is the vector of system parameters, and f is a nonlinear or piece-wise linear function. For a continuous time the required condition for its chaotic behavior is that, it must have at least three degree. Some examples of continuous time chaotic systems are Chua system [100], Chen system [101] etc. Continuous chaotic system (Chen map, Chua circuit etc.) are more complex than discrete chaotic maps and due to their complex structure they provide slow operational speed [102].

Many physical problems can be expressed and solved using fractional calculations. Current studies reveal that fractional order differential equations are a useful tool for defining complicated dynamics and can be used to better simulate a variety of physical and engineering systems [103, 104]. Even though the system order is less than three, chaotic behaviour happens in fractional-order (FO) nonlinear systems. Examples of fractional order chaotic systems are fractional order Chua chaotic system [105], fractional order Chen chaotic system [106] etc.

Fractional order chaotic systems [107] contain high complexity, therefore the design and hardware realization of these systems are hard and demands extensive memory.

In this thesis the discrete chaotic systems are considered in the subsequent chapters. These chaotic maps have also been frequently used in many cryptographic schemes [76, 108–111]. Some other type of chaotic systems as continuous time, fractional order, time delay etc will be considered as future work. The discrete chaotic maps that are frequently used in many cryptographic schemes are discussed below.

2.2.2.1 Logistic Map

A chaotic system shows deterministic, non-linear behavior in nature. Logistic map [98] is a type of chaotic system. In this system, states change with iterations in a deterministic way. Logistic map is one dimensional, discrete time and non-linear map with quadratic non-linearity. The state equation of Logistic map with initial state y_0 is given by

$$y_{n+1} = f(y_n) = \mu y_n(1 - y_n), \tag{2.9}$$

where $y_0 \in (0, 1)$ shows the state of the system at any time n and $\mu \in (0, 4)$, μ is the control parameter also known as bifurcation parameter.

Term y_{n+1} expresses the next state and n shows the discrete time. The behavior of Logistic map highly depends on the value of control parameter μ. For the values of μ between 3.567 and 4 the logistic map gives chaos with infinite period.

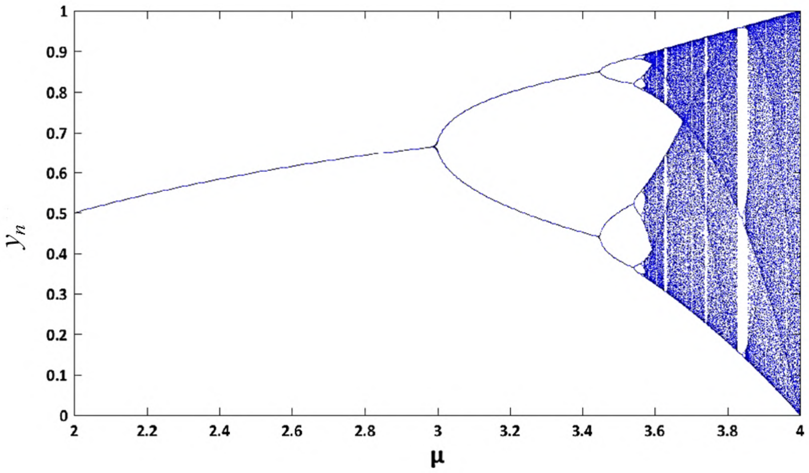


FIGURE 2.5: Bifurcation diagram of logistic map

In this range there are uncountable initial points y_0 that give non-periodic trajectories, no matter how much long time series created by $f(y_n)$, generated pattern never repeats itself. Sequences generated in this way are highly sensitive to initial condition y_0. Hence it can be characterized as deterministic system having long term non-periodic behavior.

Lyapunov exponent [112] is used to measure sensitive dependence on initial condition. Negative value of Lyapunov exponent expresses that the orbit converges with time, while positive value of Lyapunov exponent shows that distance between nearby orbit increases with time. For $\mu = 3.57$ to 4 the value of Lyapunov exponent is mostly positive, which shows that in this interval logistic map exhibit chaotic behavior.

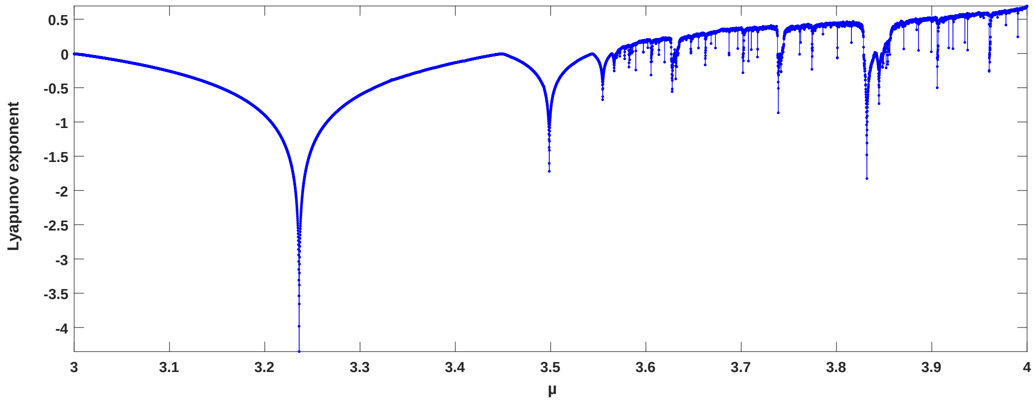


Figure 2.6: Lyapunov exponent of logistic map

Due to these properties, sequences generated by logistic map are considered highly useful for image encryption purposes in cryptography. There are various shortcoming of logistic map [113] such as periodic window in its chaotic region, non uniform distribution and limited chaotic range.

2.2.2.2 Piecewise Linear Chaotic Map

Piecewise linear chaotic map (PWLCM) is a multi segmental map.

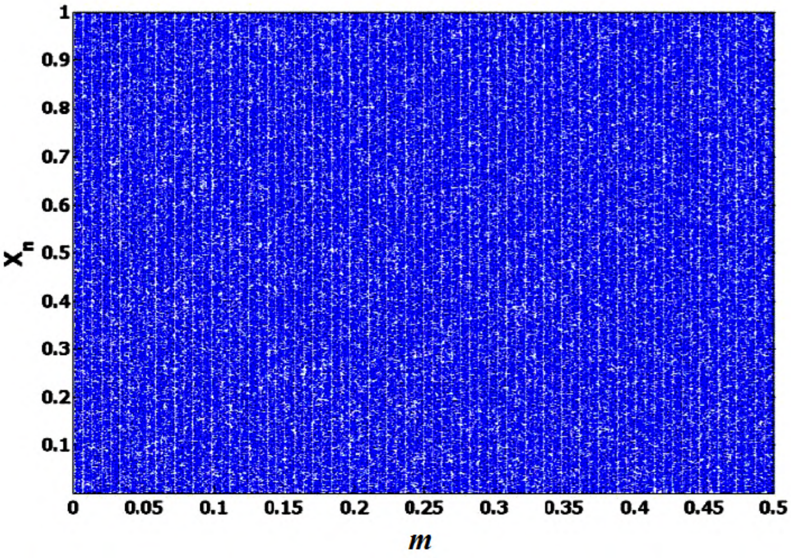


Figure 2.7: Bifurcation diagram of piecewise linear chaotic map

Li and Chen *et al.* [99] described that PWLCM has fantastic dynamic properties like large positive Lyapunov exponent, uniform invariant density function and random like behavior. These properties look highly useful and applicable for cryptographic purposes.

These properties are particularly valuable and useful for cryptographic purposes. A piecewise linear chaotic map is given by:

$$x_{n+1} = f(x_n, m) = \begin{cases} \dfrac{x_n}{m} & \text{if} \quad 0 \le x_n < m \\ \dfrac{x_n - m}{0.5 - m} & \text{if} \quad m \le x_n < 0.5 \\ \dfrac{1 - m - x_n}{0.5 - m} & \text{if} \quad 0.5 \le x_n < 1 - m \\ \dfrac{1 - x_n}{m} & \text{if} \quad 1 - m \le x_n \ < 1 \end{cases} \tag{2.10}$$

Here $x_0 \in [0, 1)$ is the initial state/initial condition and $m \in (0, 0.5)$ is the control parameter of chaotic map 2.10.

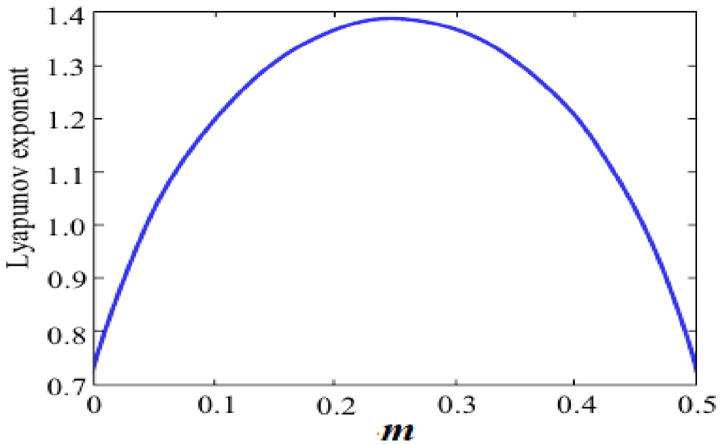


FIGURE 2.8: Lyapunov exponent of piecewise linear chaotic map

The output of PWLCM has uniformly continuous distribution, confusion and ergodicity. From the Figure 2.7 it is evident that there are no blank windows or periodic windows in the graph. As a result, PWLCM will produce a pseudo random chaotic sequence with good statistical properties [114]. It can also be used to generate good chaotic sequences for making strong S-boxes. Here x_o is the initial state/initial condition of chaotic map, when we use it for cryptographic purposes, it will be considered as secret key. The output of PWLCM has ergodicity, confusion and uniformly continuous distribution. It is used to generate good chaotic sequence for making strong S-box.

2.2.2.3 Tent Map

Tent map [115] is the simplest chaotic iterative map.

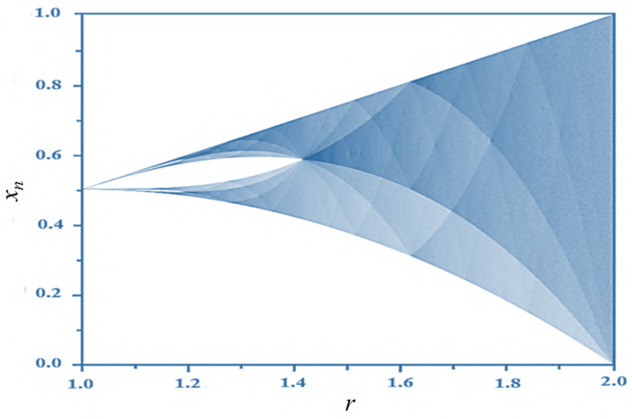


FIGURE 2.9: Bifurcation diagram of tent map

It is one dimensional map and also known as triangle map defined as,

$$x_{n+1} = \begin{cases} rx_n & \text{if} \quad 0 \le x_n \le 0.5 \\ r(1-x_n) & \text{if} \quad 0.5 < x_n < 1 \end{cases} \tag{2.11}$$

Here $x_0 \in (0,1)$ is the state variable and $r \in (0,2)$ is the control parameter. Note that the tent map just doubles x in the left half of the range as shown in the Figure 2.9, while x is subtracted from 1 in the right half, and the result is then doubled.

Although the chaotic map 2.11 is simple having linear equations but for certain parameter values, it shows highly complex and even chaotic behavior. Short chaotic range and lack of uniform distribution across output state values are some of the disadvantages of the tent map.

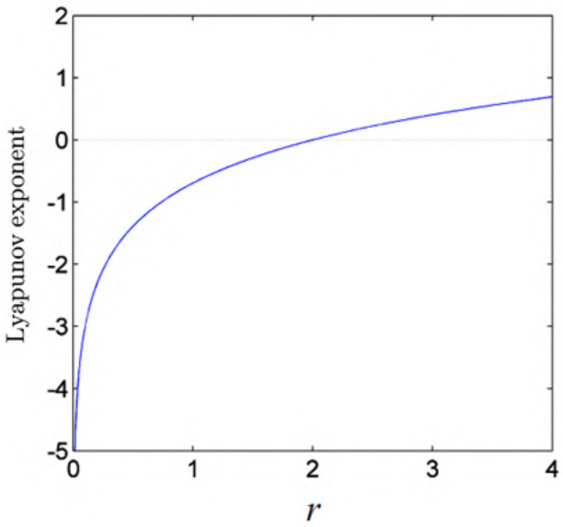


FIGURE 2.10: Lyapunov exponent of tent map

2.2.2.4 Henon Map

Henon map [116] is two dimensional invertible discrete time non-linear quadratic chaotic map in R^2. It was proposed by French mathematician Michel Henon in 1976.

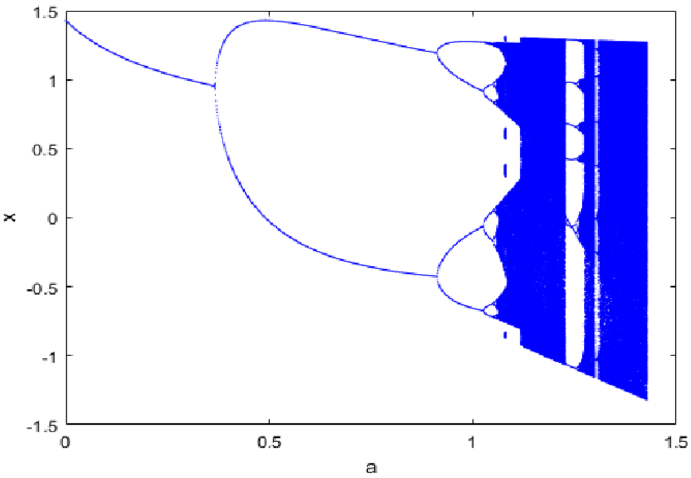


FIGURE 2.11: Bifurcation diagram of Henon chaotic map

The two dimensional invertible Henon map is defined as,

$$
\begin{aligned}
x_{n+1} =& 1 - ax^2(n) + y(n), \\
y_{n+1} =& b\ x(n),
\end{aligned}
\tag{2.12}
$$

where x_0 and y_0 are the state variables and a and b are the control parameters of chaotic map (6). For $a \in (0.54, 2)$, and $b \in (0, 1)$, it shows chaotic behavior.

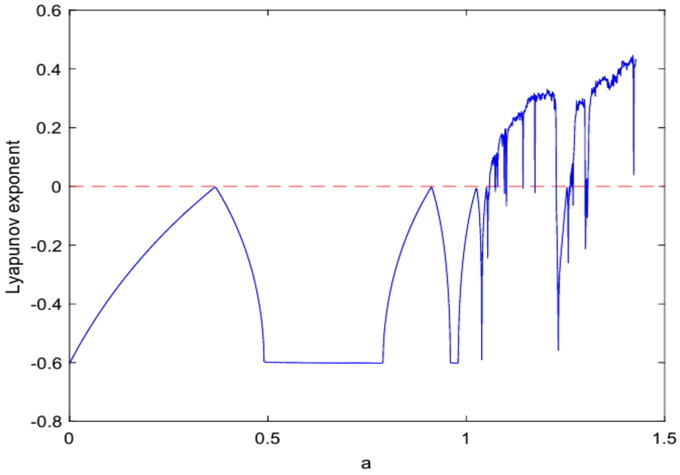


FIGURE 2.12: Lyapunov exponent of Henon chaotic map

The bifurcation diagram of chaotic maps illustrated in Figure 2.11, if $b = 0.3$ is fixed and a varies between 0 and 1.5. In Figure 2.12, the calculated Lyapunov exponents have been shown against the parameter a, which is corresponding to its behaviour (chaotic or periodic) and coherent with the bifurcation diagram presented in Figure 2.11. Henon map has a simple implementation and it easily accords itself to the numerical explorations. But it has also some shortcomings. such as it shows chaotic behavior in the range of $a \in [1.06, 1.4]$ only and having periodic windows in chaotic region [117].

2.2.2.5 The Tent Logistic System

Lu et al. [118] proposed a novel compound chaotic system by combining the tent and logistic map to address issues with the logistic and tent maps. Tent logistic system is the new system that was subsequently created. The mathematical form of this system can be presented as:

$$x_{n+1} = \begin{cases} \frac{4(9-\mu)}{9}(x_n)(1-x_n) + \frac{2\mu}{9}(x_n), & x_n < 0.5 \\ \frac{4(9-\mu)}{9}(x_n)(1-x_n) + \frac{2\mu}{9}(1-x_n), & x_n \geq 0.5 \end{cases} \tag{2.13}$$

where $\mu \in [0,9]$ is the system parameter of the chaotic map 2.13. For $\mu = 0$ the above equation behaves like logistic map, while for $\mu = 9$ the above described equation degenerates to form the tent chaotic map. Due to this, both the logistic and tent chaotic maps can be considered as the special cases of this system.

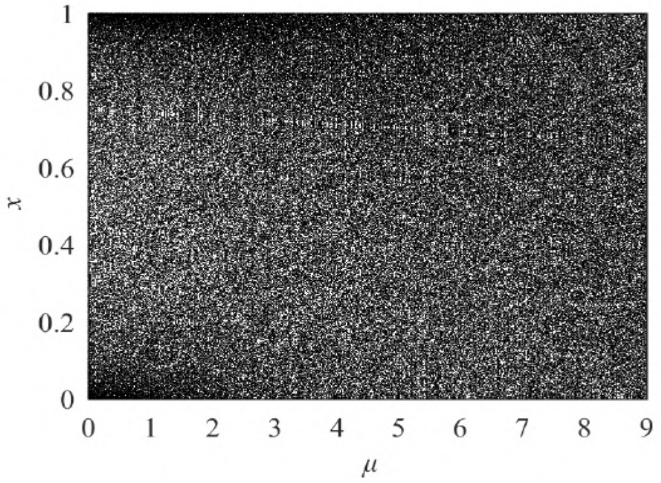


FIGURE 2.13: Bifurcation diagram of tent logistic chaotic map

Figure 2.13 and 2.14 show the bifurcation and state distribution diagram of said chaotic system. From this figure it is evident that the whole range $\mu \in [0,9]$ has chaotic behavior, also this chaotic region is much greater than the logistic and tent map. The output of this system is uniformly distributed within $[0,1]$.

This chaotic system is more suitable for the use in cryptographic application as it provides a large chaotic range. Also if the control parameter is used as the secret key for the generation of random chaotic sequences, then this key space for the generation of such sequence would be much large to resist brute force attacks. Also the output random sequence is uniformly distributed to give a good uniformly distributed random sequence.

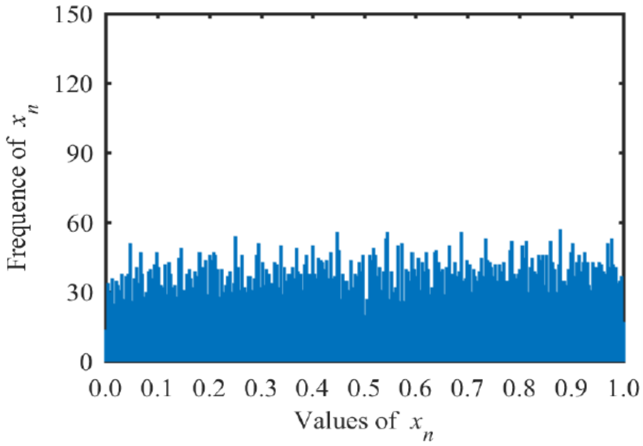


FIGURE 2.14: State distribution of tent logistic chaotic map

2.2.2.6 Tent Logistic Tent Map

From the combination of tent and logistic chaotic maps, recently in [119] a new chaotic system namely the tent logistic tent map is introduced.

The proposed system has more complex and chaotic characteristics than individual chaotic maps. This chaotic system is defined as,

$$x_{n+1} = \begin{cases} \left(\dfrac{r^2}{2}x_n\left(1-\dfrac{r}{2}x_n\right)+\dfrac{r}{2}x_n\right)r^{14} \bmod 1, & \text{if } 0 < x_n < 0.5 \\ \left(\dfrac{r^2}{2}(1-x_n)\left(1-\dfrac{r}{2}(1-x_n)\right)+\dfrac{r}{2}(1-x_n)\right)r^{14} \bmod 1, & \text{if } 0.5 \le x_n < 1 \end{cases} \tag{2.14}$$

where $r \in (0,4)$ is the control parameter and $x_0 \in (0,1)$ is the state variable. Here r^{14} is selected experimentally to generate a balance between optimal chaotic behavior and speed of system.

In this system '+' and '×' are floating point addition and multiplication respectively. The exponentiation r^σ is a multiplier that is employed for better distribution of state variables.

Tent and logistic chaotic maps have limited chaotic ranges. Therefore, when their control parameters are used as secret keys they provide limited key space. Also it is known that they have periodic windows hence these are inclined towards parameter estimation attacks

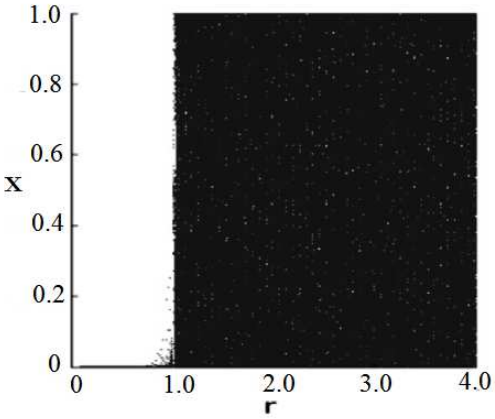


Figure 2.15: Bifurcation diagram of tent logistic tent map

To overcome the weaknesses of tent and logistic maps, they are combined to generate a new stronger chaotic system [119].

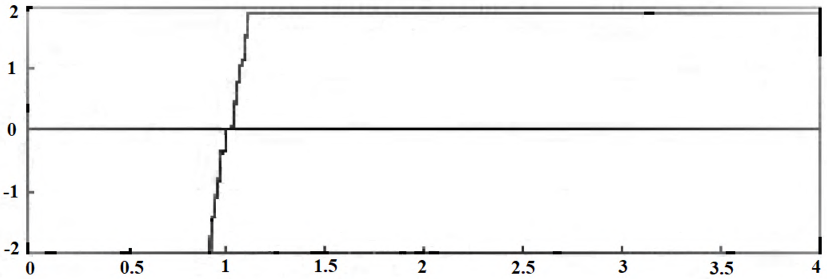


Figure 2.16: Lyapunov exponenent of tent logistic tent map

In this system logistic chaotic map plays main role while tent map plays the role of seed map. Hence generated chaotic system is called tent logistic tent system (TLTS). The proposed chaotic system shows chaotic behavior without window of periodicity in $r \in (1.05, 4)$ as presented in Figure 2.16. The Lypunouv exponent of this new system is also greater than tent and logistic maps. Hence it shows better results when used for cryptographic purposes.

Table 2.4: Comparison of different chaotic maps in terms of their advantages, disadvantages, strength, weaknesses, dimensions and complexity order.

Chaotic maps	**Compl-exity order**	**Dim.**	**Advantages (Strengths)**	**Disadvantages (Weaknesses)**
Logistic Map	n^2	one	⋆ Easy implementation ⋆ Initial conditions can implicitly use as secret keys	⋆ Periodic windows in chaotic region
Piecewise linear chaotic map	n	one	⋆ High speed implementation	⋆ Error amplification and precision truncation
Tent map	n	one	⋆ Simple in structure ⋆ Easy implementation	⋆ Small chaotic range ⋆ No uniform distribution of the output state
Henon map	n^2	two	⋆ More chaotic parameters can serve as more security keys	⋆ Multiple chaotic parameters increases difficulty of hardware implementation
Tent Logistic map	n^2	one	⋆ Good mixing property ⋆ Large key space	⋆ Time consumption is greater than Logistic and Tent map
Tent Logistic Tent map	n^2	one	⋆ Uniform random distribution ⋆ Lyapunov exp. is greater than Tent and Log. map	⋆ Due to complex internal structure utilize more time in implementation

The above shown Table 2.4 represents advantages and disadvantages of some chaotic maps used in this study. For this purpose some simple chaotic maps like logistic, tent, piecewise linear and Henon chaotic map as well as derived structures from these simple maps like tent logistic and tent logistic tent map are discussed. From the above table it is evident that the derived structures have complex internal structures therefore time consuming but yield better chaotic performance.

2.2.3 Application of Chaotic Maps and Selection Criteria

The sequences generated from chaotic maps are vastly used in the encryption process of cryptographic schemes. To create cryptograms with sound statistical features, the encryption process's sequences must be checked and validated chaotically. Their aperiodic and chaotic behavior produces good statistical properties in cryptograms [120].

The initial conditions and control parameters are considered as the secret keys of cryptographic schemes. Therefore they must be selected adequately to avoid non chaotic regimes [121]. For instance, when the control parameter is between 3.57 and 4, the logistic map results a chaos. Nevertheless, the dynamics can take on a periodic behavior at some points. In some circumstances, it is possible to adjust the control parameter to ensure chaotic behavior. For instance, if the logistic map's control parameter begins at 3.9 and double precision (64 bits) floating-point format is used, we can modify it to 14 digits, but it always results in chaotic sequences (strong keys).

While using a chaotic map, a stong numerical evaluation must be presented [122] such as Lyapunov exponent [112]. The positive value of Lyapunov exponent ensures its chaotic behavior. Bifurcation diagram is another useful way to see the chaotic behavior of certain chaotic map in any specific region. According to [121] a good chaotic map should satisfy these conditions:

- **C1**: The generated random numbers from the chaotic map should have reasonably good statistical properties.
- **C2**: Knowing random number sub-sequences will not help anyone to calculate predecessors or successors in practice.
- **C3**: One must not be able to practically compute "old" random numbers or even a previous internal state with the internal state after having knowledge of it.

- **C4**: Even knowing the chaotic system's internal state won't actually let anyone to calculate the next random number.

In a pure deterministic random number generator (DRNG), the initial internal state (x_1) is computed from the seed (x_0) value via a seeding technique. The output, which was generated using the output function, is the random integer (n_1). The next state, (x_2), is calculated using the state transition function. Linear feedback shift registers (LFSRs), hash function-based techniques, block cipher-based techniques, number-theoretic techniques, and elliptic curve-based methods are a few examples of DRNGs.

The output sequence of LFSRs has good statistical features. As a result, they typically satisfy criterion C1, but an LFSR's output sequence is the outcome of a linear function. An attacker can simply calculate all random numbers if he/she knows 't' output bits. As a result, when such basic structures are helpful for effective implementations, they contain significant security shortcomings.

The output function or state transition function must be sufficiently complex in order to satisfy C2, and it must be nearly unfeasible to guess the seed or any internal state. Requirement of C4 (increased forward security) is preferable for some specific applications. An attacker has the ability to access or alter a DRNG's internal state undetected by the person using the DRNG to generate the subsequent random numbers.

After the internal state has been compromised, a hybrid DRNG may satisfy C4 for the random numbers that are created by following the initial update with random data. Whenever necessary and upon an application's requirement, additional input is added to the hybrid random number generator (HRNG) design process after each phase. Any condition C1-C3 that the corresponding pure DRNG satisfies will also be satisfied by the hybrid DRNG.

By using relatively simple mathematical models, chaos theory has been developed to simulate complicated behavior. In nonlinear dynamic systems, chaos is a deterministic, random-seeming process. Long sequence storage is unnecessary because chaotic sequences have been shown to be quick and simple to construct and store.

The choice of chaos based number generator can also be justified theoretically by their spread-spectrum characteristic [123], complex temporal behavior [124], unpredictability [125], non-periodic behavior and ergodic properties.

Chapter 3

Cryptographic Background

The chaotic dynamic theory along with some low dimensional chaotic maps that have a vast application in cryptography are introduced earlier. This chapter covers the certain essential features of cryptography with their implementations. A discussion about the algebraic structures used in cryptography *i.e.*, group, rings, Galois field is presented in Section 3.1. The concepts of number theory and modular arithmetic are discussed in Section 3.2. After that The introduction of cryptography, its types, objectives, digital signature and public key based cryptographic schemes are presented in Section 3.3. The detail about different possible cryptographic attacks is in Section 3.4. The information about image, its different features and encryption mechanism is addressed in Section 3.5, while Section 3.6 provides the different analysis techniques about the encryption algorithm evaluation. Then Section 3.7 shows the existing problems in image encryption schemes and their solutions.

3.1 Algebraic Structures for Cryptography

Algebraic constructions are actively employed in many cryptographic protocols. In algebraic cryptography the encoding and decoding process uses group homomorphism. Therefore, in this section some basic algebraic terms are introduced that will frequently be used in the coming chapters.

Definition 3.1.1.

A **group** G is essentially a collection of elements together with a binary operation '$\star$' to combine any two elements in such a way that it forms another element satisfying certain properties/axioms (closure, associative, identity, inverses). If group $(G, \star)$ meets the following criteria, then, it is a commutative group or an abelian group.

$$x_1 \star x_2 = x_2 \star x_1, \;\; \forall \;\; x_1, x_2 \in G$$

Example 3.1.2.

The example of abelian group under ordinary addition are 'the set of integers $\mathbb{Z}$' and 'the set of rational numbers $\mathbb{Q}$'.

Definition 3.1.3.

A **ring** $(R, +, \cdot)$ is a set with two binary operation '+' (addition) and '$\cdot$' (multiplication), defined on R that follows the following axioms:

1. The set R, under addition '+', is an abelian group.
2. Multiplication in R is associative.
3. For all $a, b, c \in R$, the **left distributive law**

   $$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

   and the **right distributive law**

   $$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$$

   hold.

In a **commutative ring** the operation of multiplication '$\cdot$' is commutative.

For a ring R with unity $1 \neq 0$, an element r in R is called a **unit** of R if it really seems to have a multiplicative inverse in R. In a **division ring** every non zero element of R has a multiplicative inverse. A commutative division ring is a **field**.

Definition 3.1.4.

A field of finite order (containing finite numbers of elements) is known as finite or Galois field. The order of a finite field is power of some prime number or a prime number. For a Galois field, GF(p^n), the number of elements are p^n, where p is prime number and n is a positive integer. There exists only one finite field $GF(p^n)$ (or also written as $\mathbb{F}_{p^n}$) for each prime power p^n.

GF(p) is a special type of Galois field and known as a order p prime field. It is also referred to as the field of residue classes modulo p, where the elements of GF(p) are $0, 1, \cdots, p-1$. Here $a = b$ in GF(p) has the similar meanings as $a \equiv b \pmod p$.

Example 3.1.5.

1. The examples of ring are, set of integers $(\mathbb{Z}, +, \cdot)$ and the set of matrices of order $n \times n$ having entries from any ring also form a ring.

2. The set of real numbers $(\mathbb{R})$, the set of rational numbers $(\mathbb{Q})$ and the set of integers $(\mathbb{Z}_p)$ under modulo p (for a prime p) are examples of field.

3.2 Number Theory

This section will go through some basic definitions and terminologies of number theory. In public-key cryptography, modular arithmetic has a major importance. some fundamental concepts which are the basic necessity to describe and prove the fundamental results concepts for example divisibility, largest common divisor etc are discussed in this section. In addition, the division algorithm and the Euclidian algorithm are thoroughly explored.

Definition 3.2.1.

The **division** of two integers can be defined as: let two integers a and $d \in \mathbb{Z}$, where $d \neq 0$, then there exist some unique integers k and r, such that

$$a = kd + r, \quad \text{where } 0 \leq r < d.$$

Here k is the quotient that is obtained when a is divided by d with remainder r.

3.2.1 Modular Arithmetic

A straightforward method for doing math operations with a finite set of integers is modular arithmetic. The modulo operation in detail can be defined as,

Consider the set $\mathbb{Z}$ of integers, with a, r, $m \in \mathbb{Z}$ and $m > 0$. Then

$$a \equiv r \mod m, \tag{3.1}$$

if the integer m divides another integer $a - r$, where r is called the remainder and m is the modulus. The definition can be described in a simple way as considering the common rule of dividing by the modulus and taking the residual into account.

One can use the above definition to get the value of r from Equation (3.1). The chosen value of the remainder r is such that

$$0 \leq r \leq m - 1$$

By repeating the above defined division process, one can find the value of gcd (greatest common divisor) of two integers. The well known method for finding (gcd) is known as Euclidean Algorithm.

Algorithm 3.2.2. (The Euclidean Algorithm)
Input: Two positive integers s and t.
Output: gcd(s, t).

```
1. $S \longleftarrow s, T \longleftarrow t$
2. If $T = 0$ return $S = \gcd(s,\ t)$
3. $R = S \mod T$
4. $S \longleftarrow T$
5. $T \longleftarrow R$
6. Go to Step 2
```

Definition 3.2.3.

For the given two integers s and t, the **modular multiplicative inverse** of s modulo t is an integer u such that

$$s\,u \equiv 1 \mod t.$$

The value of modular inverse u should be in$\{1, 2, \cdots, t-1\}$. The inverse of s modulo t exists when s and t are relatively prime *i.e.*, gcd(s, t)=1. The extended form of Euclidean Algorithm (3.2.2) is used to find $s^{-1} = u \mod t$ as follows:

Algorithm 3.2.4. (The Extended Euclidean Algorithm)

Input: Two positive integers s and t such that $t > s$.
Output: Multiplicative inverse of $s \mod t$.

```
1. $(X_1, X_2, X_3) \leftarrow (1, 0, s); (Y_1, Y_2, Y_3) \leftarrow (0, 1, t)$
2. If $X_3 = 0$ return $Y_3 = \gcd(s, t)$; no inverse
3. If $X_3 = 1$ return $x_3 = \gcd(s, t)$; $x_2 = s^{-1} \mod t$
4. $Q = \left\lfloor \frac{X_3}{Y_3} \right\rfloor$; (quotient $Q$ is obtained when $X_3$ is divided by $Y_3$)
5. $(Z_1, Z_2, Z_3) \leftarrow (X_1 - QY_1, X_2 - QY_2, X_3 - QY_3)$
6. $(X_1, X_2, X_3) \leftarrow (Y_1, Y_2, Y_3)$
7. $(Y_1, Y_2, Y_3) \leftarrow (Z_1, Z_2, Z_3)$
8. Goto Step 2.
```

Definition 3.2.5.

There is a certain type of functions, referred to **one way function**, whose computation is simple but the working in the reverse order is quite difficult. For instance the value of $f(x)$ for a given x value is all that a one-way function provides, whereas obtaining x from $f(x)$ is quiet difficult. These are the essential components of many modern cryptographic protocols such as digital signatures, message authentication schemes, pseudo number generators etc.

Definition 3.2.6.

One-way functions with a “back door” are referred to as **trapdoor one-way functions**. These are simple to compute the function values for given data, just as it is for conventional one-way functions, though it is extremely difficult to compute their inverse functions. However If someone has extra secret information, then, the inverse function can be easily computed. The prime factors of large numbers, for example, are almost unfeasible to find. But knowing one of the factors, makes calculating the others a breeze.

Definition 3.2.7.

In cryptographic primitives, researchers use one way trapdoor functions as **hard problems** [126] to make their schemes safe and secure. Some of the famous hard problems for cryptographic purposes are discrete log problem, integer factorization problem etc.

Definition 3.2.8.

“Let g be a primitive root for $\mathbb{F}_p$ and let h be a nonzero element of $\mathbb{F}_p$. The **Discrete Logarithm Problem** (DLP) is the problem of finding an exponent x such that

$$g^x \equiv h \pmod{p}.$$

The number x is called the discrete logarithm of h to the base g and is denoted by $\log_g(h)$.” [127]

Definition 3.2.9.

“The **integer factorization problem** is the following: given a positive integer n, find its prime factorization; that is,

$$n = p_1^{e_1}\, p_2^{e_2}\, p_3^{e_3} \cdots p_k^{e_k},$$

where p_i’s are pairwise distinct primes and each $e_i \geq 1$.” [128]

3.2.2 Hash function

It accepts an arbitrary long input (document D) and gives back a small bit string H. The result of hash function [48] is referred to as an image, hash, digest or hash value. The term 'hash' is frequently used to refer, both the hash value and the hash function, which is the result of applying this function to a specific message. Cryptography highly depends on the hash functions. A hash function is the absolute opposite of a pseudo random generator, that extends a short, fixed-length string into an arbitrarily large one. To be a useful cryptographic tool, the hash function needs to have the following characteristics.

- **Preimage resistance**: This property suggests that reversing a hash function should be computationally infeasible.

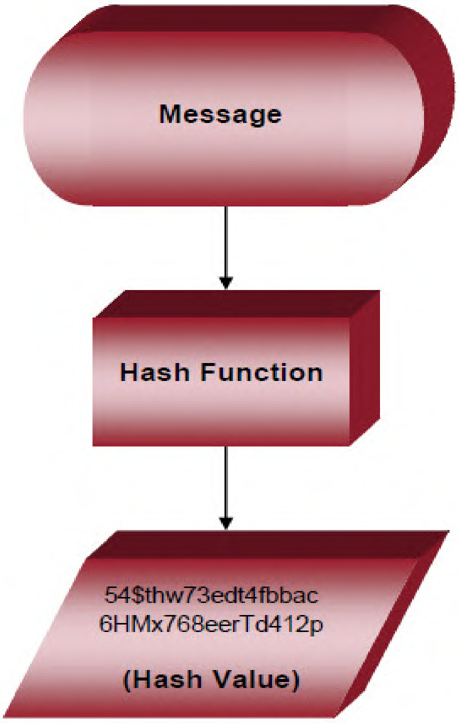


FIGURE 3.1: Hash function

- **Second preimage resistance**: It should be difficult to get another input that has the same hash value as a given input.

- **Collision resistance**: Finding two inputs should be a tough challenge of different lengths that produce the same hash, it should be difficult to discover any two different inputs u and v for a hash function 'h' such that $h(u) = h(v)$.

- **Avalanche effect**: The original message's single bit alteration must result in an entirely different hash, (diffusion).

- **Random function**: Each hash function output must have an equal chance of happening since the hash algorithm must evenly cover the whole hash space. As a result, any value in the hash space could be a hash function output.

3.3 Cryptography

Two Greek words, cryptos and graphein are the sources of the term "cryptography". According to Greek language, cryptos means hidden and graphein means writing. Cryptography provides the secure communication techniques used for the secret writing to secure the knowledge present in a secret document.

These techniques allow only the intended sender and recipient to view the contents of sent message. The most fundamental and basic problem of cryptography is to provide secret communication over insecure medium. The communication setting comprises of two parties communicating over an insecure channel that has the possibility to tap by an adversary, called the wire-tapper.

These communicating parties want to exchange the secret information with each other, but they also wish to keep the wire-tapper as ignorant as it may possible for the content of this information.

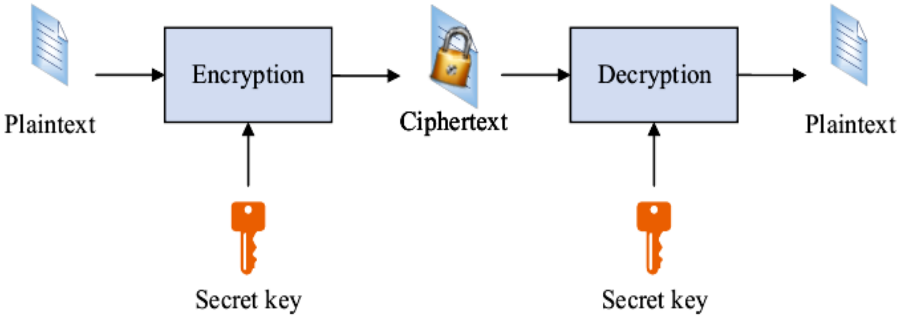


Figure 3.2: Cryptography: encryption and decryption procedure

In other words, cryptography provides such protocols that allow these parties to interact secretly with each other. Traditionally, a cryptographic scheme has a pair of algorithms. Amongst this pair, one algorithm is called **encryption**, used by the sender, whereas the other algorithm, called **decryption**, is used by the recipient.

From one of the communicating parties, the message is encrypted using the encryption technique before being sent over the insecure channel. The resulting hidden script, called the **ciphertext**. After getting the ciphertext, the other party (*i.e.*, the receiver) uses the decryption algorithm on it and recovers the original message (known as the **plaintext**).

3.3.1 Cryptosystem

A cryptosystem is a combination of various cryptographic algorithms required for the implementation of some specific security service. Usually it contains consists of three different algorithms: a decryption algorithm, a key generation algorithm and an encryption algorithm. A cryptosystem is a five-tuple (P, C, K, E, D), consisting of the following components:

1. P is a finite set of plaintexts that can be used.

2. K the keyspace, is a finite collection of keys.

3. C is the possible collection of ciphertexts.

4. There is an encryption technique, $e_k \in E$ and a corresponding decryption technique $d_k \in D$. For each plaintext element P, $e_k : P \to C$ and $d_k : C \to P$ such that $d_k(e_k(x)) = x$, for every plaintext element $x \in P$.

3.3.2 Types of Cryptosystem

A cryptosystem (also known as cipher system) is used for the implementation of cryptographic methods and techniques. On the basis of secret key a cryptosystem can be characterized into two fundamental types.

1. **Symmetric Key Cryptosystem**

   When two communication parties, such as Alice and Bob, are conversing with each other, it ensures the confidentiality. The contents of the messages of communicating parties intercepted by the adversary should not reveal significant information. For this purpose, prior to establishing a secure communication channel, Alice and Bob agree on a key, and make their shared key k secret. Alice encodes m by using the encryption algorithm E and the key k before sending it to Bob. After the encryption she obtains the cipher as:

   $$c = E_k(m),$$

   and then delivers Bob with this cipher c. Then similar key and decryption algorithm D is used to decrypt the cipher c. The plaintext is recovered by following the relation:

   $$m = D_k(c).$$

   The fundamental issue with a symmetrical method is the only secure and effective way for Bob and Alice to communicate, decide on a common secret key, k. To tackle with this challenging issue of key exchange, a technique of public-key cryptography is required. It is required that, there exists the ciphertext c as the only place where m can be found. Alternatively, a bijective encryption map for a fixed key k, should exists. Some examples of symmetric cryptographic systems are DES [153], AES [154] etc

2. **Asymmetric Key Cryptosystem**

   It was first suggested by Diffie and Hellman [16] in 1976. They have designed a public-key agreement protocol, which is widely used in modern cryptography. The communicating parties have no need to divulge a secret key in an asymmetric key based cryptosystem. There is a set of keys for each party, including a private key s_k, which is exclusively known to him and a public key p_k that is accessible to everyone.

   If Alice wants to encrypt a message m for Bob and Bob has a key pair $(p_k,\ s_k)$, then Alice uses the encryption function E along with Bob's public key p_k to compute the ciphertext as;

$$c = E(p_k, m).$$

   As stated earlier, the encryption is defined with a fixed key p_k by E_{p_k}, *i.e.*,

$$E(p_k, m) = E_{p_k}(m).$$

   Obviously, the security of the encryption method can only be ensured if extracting m from $c = E_{p_k}(m)$ is practically infeasible. The encryption function must satisfy the property that, it is simple to utilise secret key s_k to generate the pre-image m from the ciphertext as, $c = E_{p_k}(m)$.

   Due to his possession of the secret key s_k, Bob is the only one who can decrypt the communication. Even if Alice, who had previously encrypted the message, loses m, it will be impossible for her to retrieve m from $E_{p_k}(m)$.

The fundamental benefit of asymmetric cryptography is the increased data security. It is a best method for secure encryption, because users are never compelled to divulge or exchange their private keys, which reduces the possibilities for cybercriminal discovering a user's private key during transmission.

Asymmetric cryptography is used by many protocols, like the secure sockets layer (SSL), transport layer security (TLS) protocols etc. This encryption process is also employed in software applications, like browsers, that need to create a secure connection over an unsecured network, such as the internet, or validating a digital signature.

3.3.3 Public Key Based Elliptic Curve Cryptosystem

ECC (Elliptic curve cryptography) is a sort of public-key encryption that is based on the algebraic structure of elliptic curves over finite fields. Elliptic curves are useful for a variety of cryptographic tasks, including key agreement, pseudo-random number generators, digital signatures etc. Here, in this section "public key based, elliptic curve Diffie Hellman key exchange method (ECDH)" [129] is discussed.

In the (ECDH) scheme, for the given order n and base point G of elliptic curve, the sender and receiver compute $U = c_1G, \quad U^* = c_2G$ respectively by using their private keys c_1 and c_2 (for $c_1, c_2 < n$), and send to each other. Now for the sender it is easy to compute

$$V = c_1U^* = c_1c_2G,$$

and similarly for the receiver to get

$$V = c_2U = c_2c_1G.$$

But it is computationally infeasible to get the point $V = c_1c_2G$ by having the knowledge of G, U and U^*. For further details on ECC see [130].

Definition 3.3.1.

One of the most crucial public key primitives: the **digital signature**, which can provide authentication, non-repudiation and authorization properties. It is similar to a written signature in the sense that the bearer can claim ownership of a document as a result of the signature.

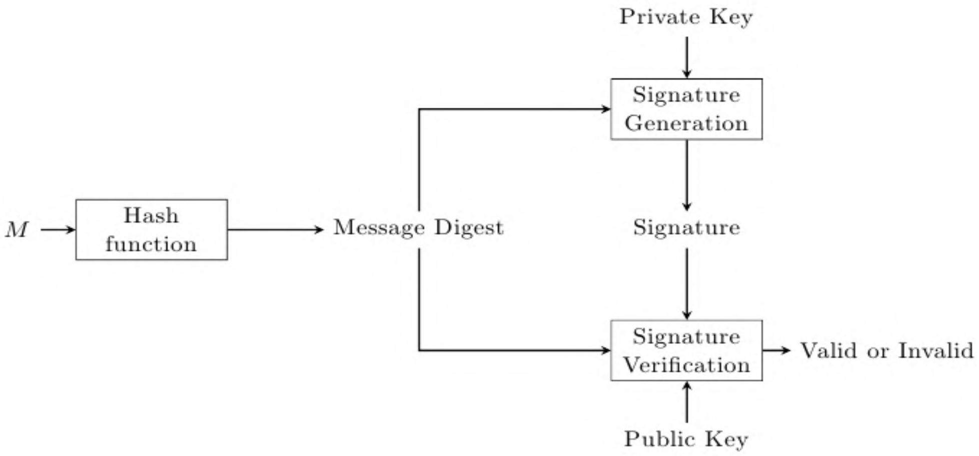


FIGURE 3.3: Digital signatures using Hash function

In today's digital world, signed papers are typically text messages or binary files. A key pair(two types of keys, private and public) is necessary for the signer to create a signature. The Signature generation and signature verification are the two algorithms that make up a signature scheme.

In the signature generation procedure, the private key is used. This key must be kept confidential, otherwise, anyone with access to it can forge a valid signature. Signature algorithm is then applied on the message digest generated by hash function. The signature verification procedure compares the signed message digest to the newly calculated message digest.

Digital signature schemes are vastly used in cryptograhy to enhance the security of encryption algorithm such as signature then encryption scheme, signcryption etc. Further applications of digital signature will be discussed In the next section.

Definition 3.3.2.

Encryption and authentication are two essential primitives of cryptography. These are vastly used for maintaining privacy of communication. Authenticated encryption simultaneously offers encryption along with data authenticity and confidentiality of secret data. For this purpose authenticated encryption combines symmetric encryption scheme and message authentication. Commonly used methods for the protection and authentication are; sign-then-encrypt, encrypt-then-sign etc. These cryptographic protocols' fundamental flaw is that they demand additional computing work.

In 1997, Zheng [60] combined these primitives in a single operation and named it '**signcryption**'. It takes less computational cost and effort. Signcryption provides confidentiality, authentication of information and non-repudiation integrity. Therefore it is used in many applications like electronic transaction protocols, key management, routing protocols etc. It also plays an important role in internet of things and cloud computing. Further details about signcryption is given in the next section.

3.3.4 Elliptic Curve Based Signcryption Scheme

Zheng *et al.* [131] presented a signcryption scheme based on elliptic curve based. The scheme's noteworthy signcryption attribute is that it satisfies both public key, encryption, and digital signature requirements at a cost that is significantly less than that of the signature-then-encryption approach. The signcryption scheme uses two versions named as short elliptic curve based digital signature standard (SEDS1) and (SEDS2) respectively. The global parameters for the signcryption scheme are as follows:

- E ——— elliptic curve over $GF(p^m)$ where $p \geq 150$ and $m = 1$,
- q ——— large prime with size approximately equal to $|p^m|$.
- G ——— taken randomly from the points of E, the order of G is q,
- hash ——— one-way hash function of 128 bits output.

- (E, D) — the encryption and decryption algorithms of a private key cryptosystem.

The signcryption scheme is used by two participants say Alice and Bob for communication over the insecure channel. For this purpose the keys used by Alice are:

- x_a — the private key, chosen uniformly at random from $[1, 2, ..., q-1]$,
- P_a — the public key ($P_a = x_a G$, a point on E),

where the keys used by Bob are:

- y_b — the private key, taken uniformly at random from $[1, 2, ..., q-1]$,
- P_b — the public key ($P_b = y_b G$, a point on E).

The implementation of the signcryption is shown in the following table.

Table 3.1: Summary of the signcryption scheme

Signcryption of message **by the sender (Alice)**	**Unsigncryption of** (c, r, s) **by recipient (Bob)**
1. Select $y \in [1, 2, ..., q-1]$ and compute $(k', k'') = \text{hash}(y\, P_b)$.	1. Receive (c, r, s) and compute $x = s y_b \bmod q$.
2. Encrypt the message as: $c = E_{k'}(m)$ cipher image c as: $c = \mathrm{E}_{H(K)}(I)$.	2. $(k', k'') = \text{hash}(xP_a + xrG)$., if SEDS1 is used.
3. $r = H_{k''}(m, \text{bind info})$	3. $(k', k'') = \text{hash}(xG + xrP_a)$, if SEDS2 is used.
4. $s = (y/(r + x_a)) \bmod q$ if SEDS1 is used.	4. $m = D_{k'}(c)$.
5. $s = (y/(1 + x_a.r)) \bmod q$ if SEDS2 is used.	5. Accept the m only if $H_{k''}(m, \text{bind info}) = r$.

Two signcryption schemes are built as shown in Table 3.1. The points of elliptic curve yP_a, $xP_a + xrG$ and $xG + xrP_a$ are treated as binary string when used for hashing. The public keys or public key certificates of Alice and Bob can be stored in the bind info component of the r during the computation.

3.3.5 Objectives of Cryptography

The fundamental goals of cryptography is to detect and prevent malicious, disruptive activities and cheating. Some of the important cryptographic security attributes are described here as:

1. **Confidentiality**

   Confidentiality means to secure the message containing plain image from unauthorized sources. For this purpose, the contents of information are kept hidden from everyone except those who have permission to see it. Secrecy has the same meanings as confidentiality and privacy.

2. **Data Integrity**

   It deals with data alteration that is not authorised, during its communication over unsecure media. In order to ensure data integrity, one must have the ability to ascertain any rigging in the data from unauthorized parties. Data rigging includes such things as manipulation, insertion, deletion, and substitution.

3. **Authentication**

   This service addresses the identification of both communicating parties the sender and the the receiver and also the secret information itself. The two communicating parties, that are entering into a communication should identify each other. Information transmitted over an insecure channel should be authenticated as to origin, time sent, date of origin, data content, etc. As a result of these considerations, this aspect of cryptography is usually divided into two main categories: entity authentication and data origin authentication. Authentication based on the data origin utterly provides data integrity (for if a message is altered, the source has changed).

4. **Non-Repudiation**

   This service prevents an entity from declining for earlier commitments or actions taken by him. It also guarantees that the sender cannot deny from something he had sent. For example, a dealing party may authorize the purchase of property from the other party but after some time refuse and deny such authorization was conceded. In case of denial, the recipient may send the dispute to a trusted third party (judge) to verify it. In judge verification process, the judge can decide about the authenticity of the sender.

5. **Unforgeability**

   It ensures that, if a fake (unauthorized) user place himself between two communicating parties and tries to forge the communication by his generated fake key, then the inbuilt structure of particular cryptographic scheme makes it practically infeasible. And the fake user cannot get any meaningful information from his generated fake keys.

6. **Forward Secracy**

   It means that attacker cannot recover sender's previous message even if he gets access to the sender's private key. For this a random number k is used for key generation. Which is known only to the sender. Attacker does not know about k, hence cannot find the decryption key k for decryption of the cipher to get plaintext.

3.4 Cryptanalysis

Cryptanalysis addresses the attacks mounted on the cryptographic schemes. Successful attacks may have the ability to extract the plaintext (or some portion of the plaintext) from its encrypted form, substitute sections, or forge its digital signatures. Cryptography and cryptanalysis are frequently grouped together by the more general term cryptology. Kerkhoff [132] was the first to propose an underlying assumption in cryptanalysis in the ending of nineteenth century. It is usually known as Kerkhoff's Principle.

It asserts that the adversary has complete knowledge of the cryptosystem, including algorithms and how they can be implemented. In accordance to the Kerkhoff principle, the cryptosystem's security is exclusively relied on the secret keys used in it.

3.4.1 Cryptographic Attacks

Attacks against the secrecy of an encryption scheme attempt to get plaintexts from ciphertexts, or even more radically, to retrieve the secret key. In this section, some basic cryptographic attacks are discussed.

3.4.1.1 Brute Force Attacks

To obtain the 'key' to decrypt an encrypted message, brute-force method tests every conceivable character combination. In brute-force assaults, it may take less time with smaller key spaces, signature-then-encryption will take an immeasurable length of time with larger key spaces. As a result, it is impossible to undertake brute-force attacks on encryption methods with large keyspaces.

For example an image in digital form is taken as 'I' and a key matrix of same size 'K' is XORed to get a cipher image 'C', as:

$$\mathrm{K} \bigoplus \mathrm{I} = \mathrm{C}$$

Example 3.4.1.

The above discussed process is applied on a small image of size 4×4 as shown below:

$$\begin{array}{ccccc} \text{Key} & & \text{Digital image} & & \text{Cipherimage} \\ \begin{bmatrix} 01 & 03 & 07 & 08 \\ 04 & 05 & 09 & 02 \\ 07 & 06 & 03 & 06 \\ 00 & 02 & 04 & 05 \end{bmatrix} & \bigoplus & \begin{bmatrix} 11 & 30 & 45 & 7 \\ 23 & 8 & 6 & 200 \\ 6 & 13 & 29 & 11 \\ 19 & 23 & 07 & 18 \end{bmatrix} & = & \begin{bmatrix} 10 & 29 & 42 & 15 \\ 19 & 13 & 15 & 202 \\ 01 & 11 & 30 & 13 \\ 19 & 21 & 03 & 23 \end{bmatrix} \end{array} \tag{3.2}$$

Here in Equation (3.2) the key matrix has entries $k_i \in \{0,\ 1,\ 2, \cdots,\ 9\}$. An attacker, who wants to use brute force attack, will have to try $10! = 3628,800$ possible combinations of key matrix to get any meaningful image. If the key space is sufficient, an attacker would have trouble obtaining any useful information during the document's valid period.

3.4.1.2 Ciphertext-only Attack

In this type of attack the adversary has the ability to obtain ciphertexts. This type of cryptographic attack has the possibility to mount on any encryption situation. Even if the adversary do not have the ability to perform the more sophisticated attacks. It should be remembered that she has the ability to read encrypted messages. An encryption mechanism is regarded entirely unsafe, if it cannot withstand a ciphertext-only attack.

For example an image in digital form is taken as 'I' and an S-box is used for the value substitution of that image to convert it into a cipher image 'C', as:

$$\mathrm{S} \longrightarrow \mathrm{I} = \mathrm{C}$$

Example 3.4.2.

The above discussed process is applied on a small image of size 4 × 4 as shown below:

$$\overset{\text{S-box}}{\begin{bmatrix} 14 & 3 & 11 & 2 \\ 9 & 0 & 6 & 15 \\ 8 & 4 & 13 & 7 \\ 12 & 05 & 10 & 1 \end{bmatrix}} \longrightarrow \overset{\text{Digital image}}{\begin{bmatrix} 01 & 03 & 07 & 08 \\ 04 & 05 & 09 & 03 \\ 07 & 03 & 06 & 04 \\ 00 & 04 & 02 & 03 \end{bmatrix}} = \overset{\text{Cipherimage}}{\begin{bmatrix} 3 & 2 & 15 & 8 \\ 9 & 0 & 4 & 2 \\ 15 & 2 & 6 & 9 \\ 14 & 9 & 11 & 2 \end{bmatrix}} \tag{3.3}$$

In the above discussed encryption example (Equation (3.3)), an attacker using ciphertext only attack got access to the cipherimages. Now he analyzes the encryption procedure and relationship of different cipherimages. Then the attacker tries different statistical properties of data like frequency analysis, histogram analysis etc to get the access with decryption key or some part of it.

For the security of such an attack it is sufficient to use Shanon's [133] idea of confusion and diffusion by incorporating both permutation and substitution operations in the encryption scheme. This will make the resulting cipherimage a random sequence with a uniform frequency distribution.

3.4.1.3 Chosen Plaintext Attack

In this type of attack, Eve is capable of obtaining ciphertexts from the plaintexts of her choice. She then tries to decrypt a ciphertext whose plaintext is not known to her. While this may seems unusual, even then, in some cases it is feasible. For instance, an adversary sends her chosen victim some intriguing material about whom she is confident that the receiver would encrypt and send out. In this type of attack, Eve can get as many plaintext-ciphertext pairs as she likes and then conduct her analysis without any further interaction. This means the adversary just has to use the encrypting device once.

Example 3.4.3.
For example an image in digital form is taken as 'I' and an S-box is used for the value substitution of that image to convert it into a cipher image 'C', as:

$$\mathrm{S} \longrightarrow \mathrm{I} = \mathrm{C}$$

The above discussed process is applied on a small image of size 4 × 4 as shown below: For example a digital image is encrypted as follows:

$$\overset{\text{S-box}}{\begin{bmatrix} 14 & 3 & 11 & 2 \\ 9 & 0 & 6 & 15 \\ 8 & 4 & 13 & 7 \\ 12 & 05 & 10 & 1 \end{bmatrix}} \longrightarrow \overset{\text{Digital image}}{\begin{bmatrix} 01 & 03 & 07 & 08 \\ 04 & 05 & 09 & 02 \\ 07 & 06 & 03 & 06 \\ 00 & 02 & 04 & 05 \end{bmatrix}} = \overset{\text{Cipherimage}}{\begin{bmatrix} 3 & 2 & 15 & 8 \\ 9 & 0 & 4 & 11 \\ 15 & 6 & 2 & 6 \\ 14 & 11 & 9 & 0 \end{bmatrix}} \tag{3.4}$$

Now let Eve inputs a special type of digital image I_S in encryption machine then she can get the secret S-box, that was used to encrypt the image.

$$\overset{\text{S-box}}{\begin{bmatrix} 14 & 3 & 11 & 2 \\ 9 & 0 & 6 & 15 \\ 8 & 4 & 13 & 7 \\ 12 & 05 & 10 & 1 \end{bmatrix}} \longrightarrow \overset{\text{I}_S}{\begin{bmatrix} 0 & 1 & 2 & 3 \\ 4 & 5 & 6 & 7 \\ 8 & 9 & 10 & 11 \\ 12 & 13 & 14 & 15 \end{bmatrix}} = \overset{\text{Cipherimage}}{\begin{bmatrix} 14 & 3 & 11 & 2 \\ 9 & 0 & 6 & 15 \\ 8 & 4 & 13 & 7 \\ 12 & 05 & 10 & 1 \end{bmatrix}} \tag{3.5}$$

The cipherimage obtained from the encryption of special image in Equation (3.5) is actually the secret S-box. Eve then calculates its inverse S-box and uses it to decrypt another cipherimage whose plainimage was unknown yet.

For the protection of such an attack it is necessary to use Shanon's [133] idea of confusion and diffusion by incorporating both permutation and substitution operations in the encryption scheme. This will make the resulting cipher image a random sequence with a uniform frequency distribution. Hence by using these measures, one can make these types of attacks infeasible.

3.4.1.4 Chosen Ciphertext Attack

The attacker selects a piece of the decrypted ciphertext in the chosen ciphertext attack. He then compares the plaintext with the decrypted ciphertext to determine the key. The attacker has limited time access to decryption machine. He can enter a cipher text to obtain its corresponding plaintext. This is a difficult sort of attack, and it was used against earlier versions of RSA. For example an image in digital form is taken as 'I' and a key matrix of same size 'K' is XORed to get a cipher image 'C', as:

$$\text{K} \bigoplus \text{I} = \text{C}$$

Example 3.4.4.

The above discussed process is applied on a small image of size 4 × 4 as shown below:

$$\overset{\text{Key}}{\begin{bmatrix} 01 & 03 & 07 & 08 \\ 04 & 05 & 09 & 02 \\ 07 & 06 & 03 & 06 \\ 00 & 02 & 04 & 05 \end{bmatrix}} \bigoplus \overset{\text{Digital image}}{\begin{bmatrix} 11 & 30 & 45 & 7 \\ 23 & 8 & 6 & 200 \\ 6 & 13 & 29 & 11 \\ 19 & 23 & 07 & 18 \end{bmatrix}} = \overset{\text{Cipherimage}}{\begin{bmatrix} 10 & 29 & 42 & 15 \\ 19 & 13 & 15 & 202 \\ 01 & 11 & 30 & 13 \\ 19 & 21 & 03 & 23 \end{bmatrix}} \tag{3.6}$$

Equation (3.6) shows the encryption process of a sample digital image. Now let an attacker inputs cipherimage in the decryption machine to get the plainimage as:

$$\overset{\text{Key}}{\begin{bmatrix} 01 & 03 & 07 & 08 \\ 04 & 05 & 09 & 02 \\ 07 & 06 & 03 & 06 \\ 00 & 02 & 04 & 05 \end{bmatrix}} \bigoplus \overset{\text{Cipherimage}}{\begin{bmatrix} 10 & 29 & 42 & 15 \\ 19 & 13 & 15 & 202 \\ 01 & 11 & 30 & 13 \\ 19 & 21 & 03 & 23 \end{bmatrix}} = \overset{\text{Plainimage}}{\begin{bmatrix} 11 & 30 & 45 & 7 \\ 23 & 8 & 6 & 200 \\ 6 & 13 & 29 & 11 \\ 19 & 23 & 07 & 18 \end{bmatrix}} \tag{3.7}$$

The attacker now has a cipherimage and its corresponding plainimage. As the encryption algorithm and decryption algorithm are kept public and only the key is a secret thing. Hence by carefully observing the decryption process the attacker analyze underlying operation and relationship of plainimage and cipherimage. He then perform the following operation:

$$\overset{\text{Cipherimage}}{\begin{bmatrix} 10 & 29 & 42 & 15 \\ 19 & 13 & 15 & 202 \\ 01 & 11 & 30 & 13 \\ 19 & 21 & 03 & 23 \end{bmatrix}} \bigoplus \overset{\text{Plainimage}}{\begin{bmatrix} 11 & 30 & 45 & 7 \\ 23 & 8 & 6 & 200 \\ 6 & 13 & 29 & 11 \\ 19 & 23 & 07 & 18 \end{bmatrix}} = \overset{\text{Key}}{\begin{bmatrix} 01 & 03 & 07 & 08 \\ 04 & 05 & 09 & 02 \\ 07 & 06 & 03 & 06 \\ 00 & 02 & 04 & 05 \end{bmatrix}} \tag{3.8}$$

By performing the XOR operation of the cipherimage and corresponding plainimage the attacker gets the secret key as shown in the Equation (3.8).

For the security of such an attack it is required to use Shanon's [133] idea of confusion and diffusion by incorporating both permutation and substitution operations in the encryption scheme. This will make the resulting cipher image a random sequence with a uniform frequency distribution. Hence it will effectively resist against these types of attacks.

3.5 Image Encryption

Image encryption is used to make image communication secure over the internet such that no unauthorized person can decode it. Structure of images is quite different from ordinary text data therefore conventional cryptographic encryption schemes become ineffective for image encryption. Image encryption techniques scramble images in such a way that they become unidentifiable. There are many methods for this purpose to fulfill this requirement for instance stegnography, packing, advanced watermarking, meaningful image encryption, image hiding etc. Image encryption methodologies are used to change data using different algorithms to make images ambiguous for anybody except those having the knowledge of secret key. The advancement in image encryption techniques is going forward towards the hope of absolute inconceivable outcome. Nowadays new improved, strong and advanced encryption schemes are being developed. In this section the structure of image, its use in computer application types and the structure of an image encryption cryptographic scheme will be discussed.

3.5.1 Image Layout

The output of light stimulus created by a two-dimensional support is an image. This phenomenon occurs when the image is created through an intermediate stage, such as a photograph, or by projecting our three-dimensional world onto our retina directly.

A mathematical model for the description of an image is defined on two dimensional surface and taking values from a color space, to express a picture.

An image is represented by the map $f : U \to C$ where $U \subset R^2$ is a subset of the plane and rectangle of plane where C is a vector space. The function f is the image function, U is the support of the image, and the set of values of f are the image color gamut. For one-dimensional color space C, the image is refer to as monochrome or **grayscale image**.

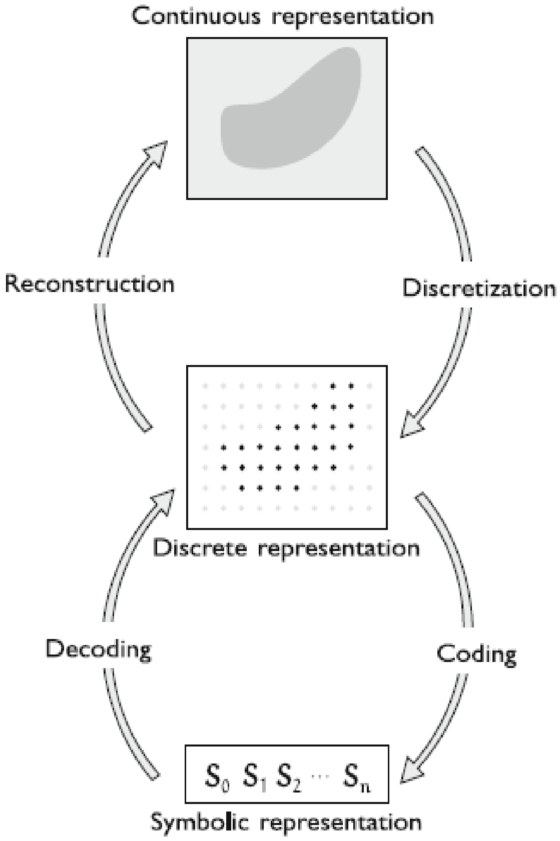


FIGURE 3.4: Quantization of image and its use in digital applications.

To use the image in a computer, image model is chosen with an image function f that takes the values from a discrete subset of the color space C. The conversion from continuous representation to discrete representation is called **quantization**.

3.5.2 Digital Image

The visual representation of an object processed digitally is known as a digital picture. The numerical representation of a two-dimensional image is also known as a raster image or a bit-mapped image. Picture elements, (also known as **pixels**), are the digital values that make up raster images. Pixels are the shortest individual elements of an image, storing numerical values that represent the brightness of a given color at every given instant in time. The digital image has a specific number of pixels in each row and column.

3.5.3 Image Color

The intensity or color at a certain pixel location in an image is defined by one or more color channels. In the most basic form, each pixel position includes only a single numerical value that represents the signal level at that particular spot in the image. A color map is used to convert this set of numbers into an actual (displayed) image. A color map adds a specific shade of color to each numerical level in the image to provide a visual representation of the data. The grayscale is the most popular color map, which allocates all shades of grey from black (zero) to white (maximum) based on the signal strength.

In addition to greyscale images, where each pixel has a single numerical value, there are color images that have the most frequent use in the modern applications. True color images are those in which the entire color spectrum is represented as a triplet vector, with the (R, G, B) components at each pixel point. A color image can be thought of as consisting of three, 2-D planes, with the color represented as a linear combination of the basis colors or values.

3.5.4 Resolution and Quantization

The spatial resolution and color quantization of a picture are determined by the size of the 2-D pixel grid and the data size recorded for each individual image pixel. The resolution of an image determines its representational power (or size). The resolution of an image source (such as a camera) can be expressed in three ways.

- **Spatial resolution**: The number of image's column (C) and row (R) specify that how many pixels are employed to cover the visual space recorded by the image. Digital resolution of an image is also a famous term used for it. C × R is a well-known formula to find the resolution (for example 640×480, 800×600, 1024×768, etc.)

- **Bit resolution**: The number of colors that a pixel can display is simply referred to as its bit resolution. It tells the number of bits required for the storage at a specific quantization level, *e.g.* binary is 2 bits, grey-scale is 8 bits, and color (most often) is 24 bits, is known as bit resolution. The dynamic range of a image refers to the range of possible values that a pixel can take.

3.5.5 Chaos-Based Image Cryptosystems

Lorenz in 1963 [134] investigated a non linear dynamic system that later on known as chaos. In this system he observed that a little change in beginning condition yields contrastive results. Chaotic sequences are random, non-periodic and highly sensitive to system parameters.

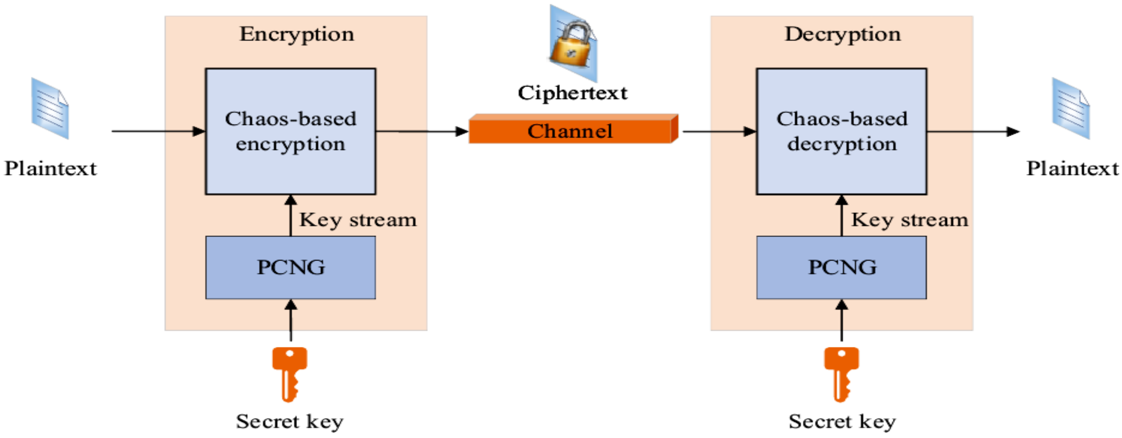


FIGURE 3.5: Chaos based image cryptosystem

An image encryption scheme requires two essential properties that are confusion and diffusion. These properties are extensively found in chaotic systems as ergodicity and sensitivity to initial condition therefore chaotic maps are highly useful in image encryption cryptosystems.

3.5.5.1 Structure of Chaos Based Image Cryptosystem

Chaotic image encryption schemes mainly consist two mutually independent stages. These stages are substitution and diffusion.

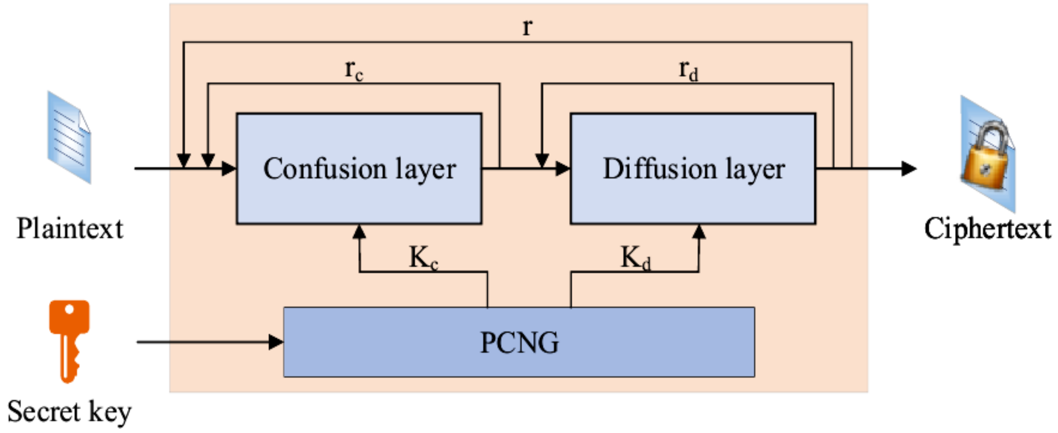


FIGURE 3.6: Structure of chaos based image encryption scheme

- **Confusion**

  In a natural image, adjacent pixels are highly correlated to each other. In order to break the relationship of adjacent pixels, it is required to move them on different positions. For this purpose permutation is performed to all pixels. The relocation should be performed in such a way that it can be reversed to decrypt the process. This relocation should also be irregular and unpredictable. In this stage the values of pixels are not changed. To eliminate correlation among neighboring pixels, r_c permutation rounds are used, where $r_c \geq 1$. After this step every pixel is changed by some other pixel in the same image. Hence confusion effect is generated in image.

- **Diffusion**

  Substitution phase does not change the histogram results. This phenomenon gives rise to a risk of statistical attack. Therefore an additional step is required for the improvement of security against such types of attacks. In diffusion stage, pixel values are changed. Chaotic maps due to their randomness and unpredictable behavior are useful for this stage. After this stage pixel values become random and histogram shows uniformity in data.

3.6 Integral Analysis of Image Encryption Scheme

Several security analysis tests for chaos-based image cryptosystems are presented in this section. The security analysis described here is based on a review of the literature. These basic tests such as key size, sensitivity of the secret key and plain picture, information entropy, histograms, and correlation were included by the majority of authors. Further detail of these security aspects is given below:

3.6.1 Key Space

The key is a bit string that specifies how the algorithm will map the plain image P to the image E, which is encrypted. It is considered very important from a security perspective, because the opponent knows everything about the cryptosystem except the key. The brute-force attack or exhaustive search attack in which every potential key is employed until the cryptosystem is cracked, is the most obvious attack on the cryptosystem. The adversaries, now, have the access to supercomputers. With the current technology, the key space is designed to be large enough to withstand such an attack. For example, today's fastest supercomputer (Summit) can perform 200 PFLOPS (10^{15} floating-point operations per second), or 200,000 trillion calculations per second. According to Alvarez and Li [135], the key space must be larger than 100 bits. With the aforesaid supercomputer and 1000 FLOPS, it would take 1.99×10^{23}.

$$\text{Years} = \frac{\text{Key combinatons} \times 1000}{\text{FLOPS}} \times 31536000, \tag{3.9}$$

years to break this cryptosystem. All key spaces in the encryption design must have chaotic behaviour (*i.e.*, strong keys), and weak keys must be avoided. The bifurcation diagram, or calculating the Lyapunov exponent to validate chaos, are the methods for determining the strength of key spaces. Key space is considered an important feature in any cryptosystem. The adequate key space for chaotic image encryption scheme necessarily greater than 2^{100} to prevent brute force attacks.

3.6.2 Key Sensitivity

An essential requirement for an ideal image encryption scheme is that, it should be conscious about secret key. In case of the change of one bit in its secret key should crop an entirely different encryption results. For the sensitivity analysis with respect to secret key, a highly sensitive key is demanded. The high sensitivity in an encryption scheme can be ensured by using a pseudorandom chaotic sequence in encryption process. Chaos theory has the property of high sensitivity for its initial state. By using properly a pseudorandom sequence generated from a chaotic map in encryption process will yield to generate a key sensitivity effect in the encrypted image.

3.6.3 Distribution of Pixels in Cipher Image

An image's histogram is a visual analysis of statistical data and the image's tone. It graphically depicts the frequency of image pixel intensity values. In the histogram horizontal axis depicts intensity variations, while the vertical axis shows the frequency of a specific intensity.

To avoid the leakage of statistical information related to the plain image and to withstand statistical attacks, the graphic histogram of the encrypted image must display identical frequencies for each pixel intensity value (uniform distribution). From the histogram one can observe the dispersion of pixels in an image as the number of pixels and their frequencies are plotted in an histogram. For all 256 intensity values, an ideal uniform histogram of an encrypted image must have the same pixel frequency.

3.6.4 Correlation Analysis of Two Adjacent Pixels

The Pearson correlation coefficient (PCC) [136] is a statistical measure used to aid visual correlation analysis. In statistics, PCC uses a numeric index that ranges from $[-1, 1]$ to determine the grade of a linear relationship between two quantitative variables. There is a perfect inverse relationship when it is -1, and a perfect direct relationship when it is one. Also neither of the variables examined, exhibits a linear connection when PCC is zero (null correlation). As PCC is highly associated, therefore plain images do not depict PCC near to zero. Encrypted images, on the other hand, must have a PCC close to zero in order to withstand statistical attacks. The property of having high confusion and diffusion can be checked by a test of correlation among neighboring pixels in the plain-image and similarly in the associated cipherimage. For the calculation of correlation coefficients among the neighboring pixels in horizontal, vertical and diagonal directions, the following Pearson correlation coefficient [136] has been used,

$$C_r = \frac{(n\sum_{t=1}^{n} x_t y_t - \sum_{t=1}^{n} x_t \sum_{t=1}^{n} y_t)}{\sqrt{(n\sum_{t=1}^{n}(x_t)^2 - (\sum_{t=1}^{n} x_t)^2)((n\sum_{t=1}^{n}(y_t)^2 - (\sum_{t=1}^{n} y_t)^2)}}. \tag{3.10}$$

Here x_t and y_t are values of neighboring pixels in the image and n is the total number of pixels taken for calculation of correlation.

3.6.5 Information Entropy

This feature of analysis measures the randomness in a cipher image. It also tells us the average amount of information carried by cipher image. Let G be a ciphered image then entropy value of image G can be calculated by the formula,

$$H(G) = \sum_{i=o}^{2^N-1} P(g_i)\mathrm{log}_2(\frac{1}{P(g_i)}). \tag{3.11}$$

Here $P(g_i)$ shows the probability of appearing of symbol g_i in cipher image G. For exact random source having 256 different symbols, the ideal value of entropy $H(G)$ is 8.

3.6.6 Differential Analysis

An essential property for good performance image encryption scheme is that, images encrypted with that scheme should be totally different from plain images. To check the difference in an encrypted image and encrypted by making a change of one pixel in plain-image, “number of pixel change rate” (NPCR). Also “unified average changing intensity” (UACI) used on two encrypted images. The values of NPCR and UACI can be calculated by;

$$\begin{aligned} \text{NPCR} &= \frac{\sum_{i,j} K(i,j)}{w \times h} \times 100 \\ \text{UACI} &= \frac{1}{w \times h}\left[\sum_{i,j} \frac{|X(i,j) - X'(i,j)|}{255}\right] \times 100. \end{aligned} \tag{3.12}$$

Here w and h show the width and height of the encrypted image respectively. X and X' are cipher images generated by plain image and one pixel difference in plane image respectively. If $X = X'$ then $K_{i,j} = 0$ otherwise 1.

The results of this test show the capability of any image encryption scheme to resist against differential attacks.

3.6.7 Encryption Quality

Quality measurement techniques such as mean-squared error (MSE) and peak signal-to-noise ratio (PSNR) are used to objectively validate image encryption. The MSE is a parameter that is used to calculate the difference between two images.

$$\text{MSE} = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{i=0}^{N-1} (\mathrm{I}_P(i,j) - \mathrm{I}_D(i,j))^2. \tag{3.13}$$

where $M \times N$ represents image size, I_P is the plain image, and I_D denotes decrypted image. The least value of MSE shows the minimum error by using any encryption scheme. Hence the least MSE value, interprets the better encryption quality. The MSE analysis is also applicable for a color RGB plain image and an decrypted RGB color image with pixel values between 0 and 255.

$$\text{PSNR} = 10.\log \frac{255^2}{\text{MSE}} \,(db), \tag{3.14}$$

The PSNR is the ratio of a signal’s maximum achievable power to the power of distorting noise that influences the quality of its representation. It is a quantitative measure used for the distinction between the original plain image I_P and its decryption result I_D. The greater value of PNSR indicates the higher fidelity of decrypted image towards its original plain image.

3.6.8 Analysis of Algorithms

Algorithm analysis is considered as an important feature in the complexity analysis of algorithm. A good problem solving algorithm possesses many qualities like correctness, simplicity etc. If an algorithm does not provide satisfactory results for simplicity and generality then it is required to redesign it to get these desired properties. This analysis is also used for the performance comparison purpose of different algorithm generated for the solution of same problem. For this purpose the following two analysis are frequently used:

3.6.8.1 Algorithm Correctness

It must be shown that a newly designed algorithm always produce the intended result in all legal cases of the problem. For this purpose usually these methods are used.

- **Counter examples**

  True-value configurations that interpret the formula or statement is false are known as counterexamples. It is usually enough to present a counterexample to prove that something is incorrect. A counterexample is supplied when a system fails to satisfy the given properties, however counterexamples are sometimes difficult to interpret manually. There are few and imperfect automated ways for doing so. A manual effort is usually required for this purpose.

  The absence of a counterexample for a given algorithm does not imply that the algorithm is right.

- **Induction**

  In the analysis of algorithms, mathematical induction plays a prominent role.

It is a direct method used to prove a formula or statement. It is based on the rule of mathematical induction. The technique has two steps:

1. **The initial case**: It is to prove that the statement or formula is true for 0 or 1.
2. **Inductive step**: In this step, it is required to prove that if a statement or formula is true for n where $n \in \mathbb{N}$ (the set of natural numbers), then it is also true for $n + 1$.

Once a theorem, formula is proved by mathematical induction, then it can be used to build an algorithm. Mathematical induction is particularly used to show the correctness of recursive algorithms.

- **Loop Invariant**

  A loop invariant is a condition that must be true immediately before and after each iteration of the loop. It is a condition that is true for each loop iteration. The loop invariant supports the design of iterative algorithm, When treated as an assertion that specifies important relationships among the variables that must be true at the start of each iteration and when the loop closes. If it holds then the computation is on the right track. But if it's false, the algorithm will not work.

- **Lots of examples**

  The construction of examples by applying the implementation of an algorithm on different structures is another method to prove the correctness. In this method an algorithm is tested by implementing through various examples, and if it gives the correct desired results each time then it is considered valid for the practical use.

3.6.8.2 Algorithm Complexity

The encryption algorithm is actually a step wise procedure written in a programming language, whose internal structure should be complex. With big-O notation '$\mathcal{O}$', the complexity is asymptotically approximated as a function that depends on the input size n. The overall complexity of an encryption algorithm is the sum of individual complexities of the series of sentences in that algorithm. To evaluate the complexity some practical rules are considered.

- The simple input/output and 'if' sentences has the complexity $\mathcal{O}(1)$.
- The 'for' cycle for n iterations that is independent of the input n has the complexity $\mathcal{O}(n)$.
- A double cycle nested 'for' has complexity order $\mathcal{O}(n^2)$ for n iterations for each cycle.
- For n iterations, the iterative cycles with divisive-multiplicative sentences are of order $\mathcal{O}(\log n)$.
- In the cycle of $\mathcal{O}(\text{log}n)$ consisting of n iterations has the complexity $\mathcal{O}(n\text{log}n)$.

Chaos-based image encryption algorithms mainly depends on the substitution-permutation network, which may be approximated with complexity order $\mathcal{O}(mn)$, where m and n are the input image's pixel sizes.

3.7 Existing Problems and Solutions

Despite the fact that several chaos-based picture cryptosystems have been suggested, some of them do not offer the high security that they claim and have been shown to be vulnerable to particular attacks.

Farajallah et al. [137] investigated the security of a chaos-based image cryptosystem [138] that employed the logistic map to perform dependent diffusion and demonstrated that the diffusion effect can be removed because the argument is visible in the ciphered image. As a result, key space was reduced, and a permuted version of the ciphered image could be retrieved, allowing brute-force and selected plaintext attacks.

Zhou *et al.* [140] proposed a symmetric image encryption thai is based on skew tent chaotic map and line map. In this scheme R, G, B components of a color image are simultaneously encrypted at bit level. Chen *et al.* [139] analyzed the security of [140] and found that it depends only on the permutation key that reduces the keyspace and $(H \times W + 1)$ chosen plain images can be used to obtain the similar permutation key of one round encryption process. Here $(H \times W)$ is the size of the image used for this purpose.

The encryption process containing two rounds, authors proposed two way differential comparison method. Under chosen-ciphertext conditions, authors suggested a codebook attack, design the codebook with $(H \times W)$ differential binary images, and completely break the multi-round cryptosystem using the XOR operation of $\mathcal{O}(H \times W)$ images.

Wang *et al.* [144] anayzed an image encryption technique that is proposed by using a combination of one dimensional chaotic maps. In this scheme the main encryption mechanism was developed by using confusion, diffusion and linear transformation. The chaotic sequences used for confusion and diffusion are generated by sine-sine system. The analysis of this schemes disclosed some algebraic weakness also found that the linear transformation used there can be converted as a part of permutation. For this purpose an equivalent encryption mechanism is designed and chosen plaintext attack is successfully mounted on it. To improve the process, authors omitted the linear transformation process. The complexity of hence improved scheme is $\mathcal{O}(MN\log(MN))$.

The cryptanalysis approach presented in [148] has shown that [149, 150] contain design flaws in confusion and diffusion, as well as a lack of complexity in the avalanche effect, allowing an attacker to leak the key stream and defeat the system using the chosen-plaintext attack. As the encryption technique proposed in [151] can be downgraded to a diffusion-only algorithm and a permutation-only algorithm, in [152] can be used as differential attack to break the scheme in [151].

By observing more closely these vulnerable cryptosystems, one can note the following major flaws.

- Unsecure and insufficiently complex confusion and diffusion have the potential to leak key stream information, including the secret key [141–147] and cryptologists can remove the effect of confusion or diffusion, resulting in a simple to break diffusion-only or confusion-only scheme [144, 145, 148–152].

- Without cryptographic characteristics, a key stream can reveal the secret key [141–147].

- Multiple rounds are required due to insufficient confusion and diffusion, resulting in low efficiency, preventing these schemes from being used in real-time applications [137, 138, 140].

The foregoing three issues necessitate effective solutions. Therefore, a good image encryption technique should be equipped with a secure and complicated confusion and diffusion structure, as well as a cryptographic key stream that is capable of safeguarding the secret key. Also it is essential to use a PCNG that can creates pseudo-chaotic key streams with good unpredictability and chaotic features. Another phenomenon that came into our knowledge is the transient effect lies in the starting numbers of pseudo chaotic random sequence. To remove this effect some starting numbers of the sequence are terminated. Hence the remaining sequence shows good randomness. The fact is kept in mind, while working with chaos in the subsequent chapters.

Chapter 4

A Chaos Based Color Image Encryption Scheme

With the rapid growth in computer network technology, it becomes a trend to transmit a lot of sensitive information over a public network. Therefore information security has become very important in modern sciences. The rapid increase in image transmission grabs the attention of scientists towards making efficient and secure image encryption algorithms. The information carried by an image is quite different from plaintext. Images have bulk data, high redundancy and strong correlation between neighboring pixels. Therefore image encryption is far different from ordinary text encryption [76]. Traditionally occurring encryption techniques DES [153], AES [154], RSA [17] etc. are not beneficial for the purpose of encryption of images.

Chaotic maps [155] have some very useful properties like sensitivity to initial conditions, non-periodicity and random like behavior. Chaotic maps have been highly appreciated for the generation of confusion and diffusion in image cryptography. As a result, it has endorsed a huge application in image coding, decoding, encryption, image hiding etc.

Image encryption algorithms have vast applications to benefit in many real life fields such as electronic medical record; this record is used to manage, transmit and even sometimes need to reproduce previous health history of the patients securely. The use of chaotic maps in image encryption algorithms can enhance the security of such encryption schemes.

In 2020, [156] proposed an image encryption technique that uses bit wise permutation of pixels and S-box for diffusion purpose. Recently [157] introduced a grey and color medical image encryption technique. In this scheme authors first split image into blocks then perform zig zag permutation, rotation and random permutation then XOR is used for diffusion purpose. In this research chaos based permutation technique is used then S-box is used for diffusion further diffusion is added in by using XOR with chaos based sequence and recursion. Incorporating chaotic maps in permutation and diffusion contributed significantly to the strength of resulting cipher. The use of such combination makes the scheme more robust in comparison with [156], [157] and many others.

The chapter is organized as: in Section 4.1 the image encryption scheme is described. Section 4.2 contains the image decryption algorithm. Results and discussion with the help of examples and figures are in section 4.3. The security analysis of the scheme and comparison with other schemes is discussed in Section 4.4. Finally the work is concluded in Section 4.5.

4.1 The Proposed Image Encryption Scheme

In this section, a new color image encryption algorithm is described. It contains three cryptogrphic phases and uses two chaotic systems to control the structure of the scheme for obtaining high encryption performance.

4.1.1 Global Parameters

The main advantage of the use of the chaos based cryptosystem is that, it facilitates the key management approach. This method needs only the protection and the secure transmission of secret keys *i.e.*, the initial keys and parameters of chaotic maps. These secret keys have the small volume, therefore necessitating not only a small memory to sustain it, but also more confidence during its transfer. During data transmission over an insecure channel, unauthorized access to short length keys is significantly less likely than it is to large length keys.

For the proposed image encryption three keys k_1, k_2, k_3 are respectively used in permutation, substitution and diffusion phases. The secret keys k_1 and k_2 use the parameters y, $y' \in (0, 0.5)$ and initial values x_0, $x'_0 \in (0, 1)$ for the chaotic map (2.10) in Algorithm (4.1.1) and (4.1.2) of permutation and substitution respectively. While the secret key k_3 has the parameter μ and initial value w_0 of chaotic map 2.9 in Algorithm (4.1.3) of diffusion phase.

The proposed cryptosystem is symmetric in nature that uses same keys for the encryption and decryption. Therefore Alice (the sender) and Bob (the receiver) first agree to share secret keys securely and then communicate each other by using the following encryption/decryption algorithms respectively.

4.1.2 Layout of the Proposed Cryptosystem

In the proposed image encryption scheme, initially the permutation is performed by a permutation table generated by the chaotic map (2.10).

Then for substitution, a strong S-box generated by chaotic map (2.10) is used. Finally, in diffusion phase an XOR function is used with another chaotic map (2.9) to reinforce the statistical performance of the proposed scheme.

The flow diagram shown in Figure 4.1 describes the step-wise working procedure of encryption scheme. In this flow diagram three keys k_1, k_2, k_3 and the plainimage I are given as input, while the noise like scrambled cipherimage P is received as an output. A random chaotic sequence together with the sorted sequence are obtained by iterating piece-wise linear chaotic map (PWLCM) using k_1.

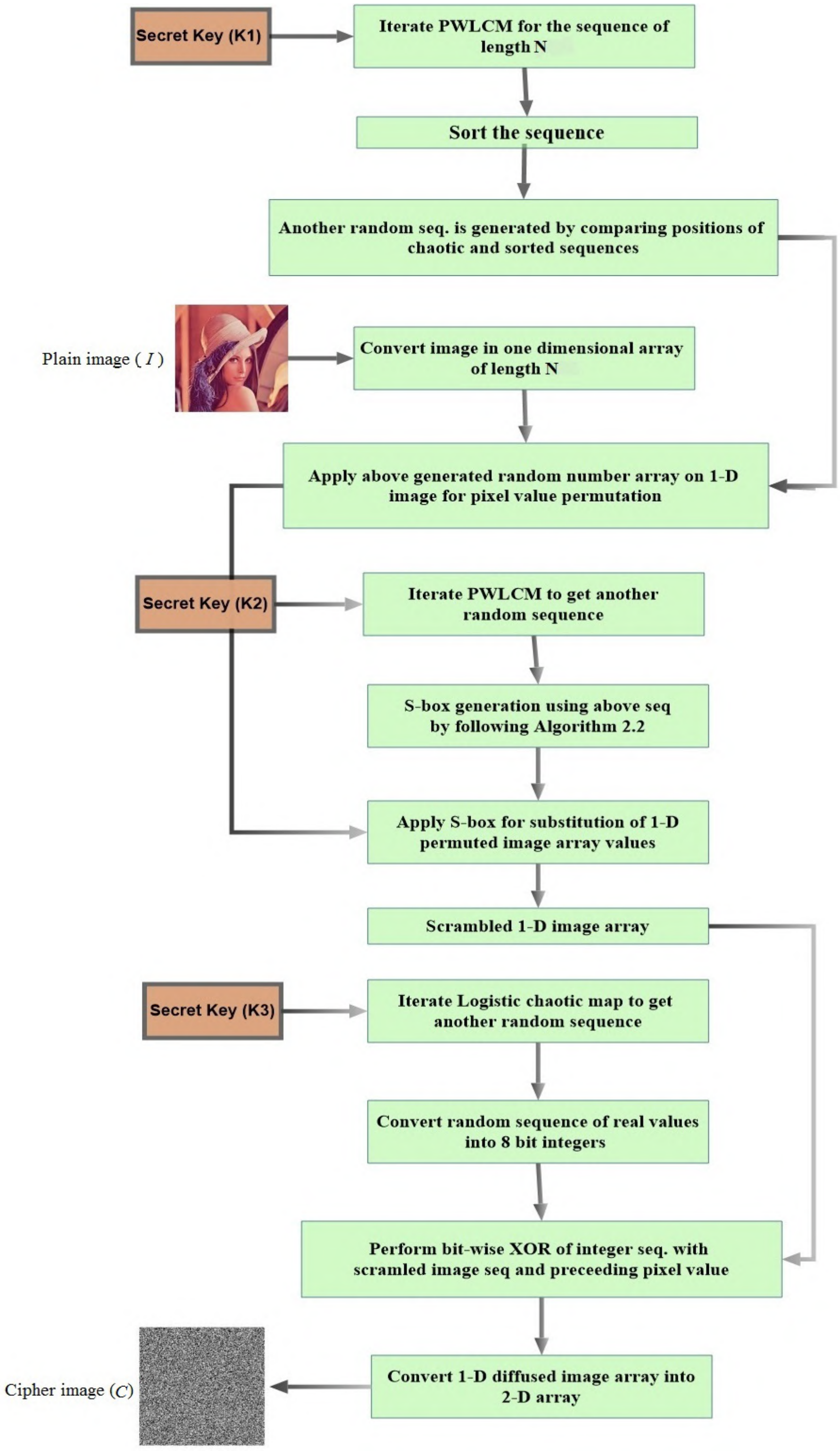

Secret Key (K1)
Iterate PWLCM for the sequence of length N
Sort the sequence
Another random seq. is generated by comparing positions of chaotic and sorted sequences
Plain image (I)
Convert image in one dimensional array of length N
Apply above generated random number array on 1-D image for pixel value permutation
Secret Key (K2)
Iterate PWLCM to get another random sequence
S-box generation using above seq by following Algorithm 2.2
Apply S-box for substitution of 1-D permuted image array values
Scrambled 1-D image array
Secret Key (K3)
Iterate Logistic chaotic map to get another random sequence
Convert random sequence of real values into 8 bit integers
Perform bit-wise XOR of integer seq. with scramled image seq and preceeding pixel value
Convert 1-D diffused image array into 2-D array
Cipher image (C)

FIGURE 4.1: Flowchart of image encryption algorithm

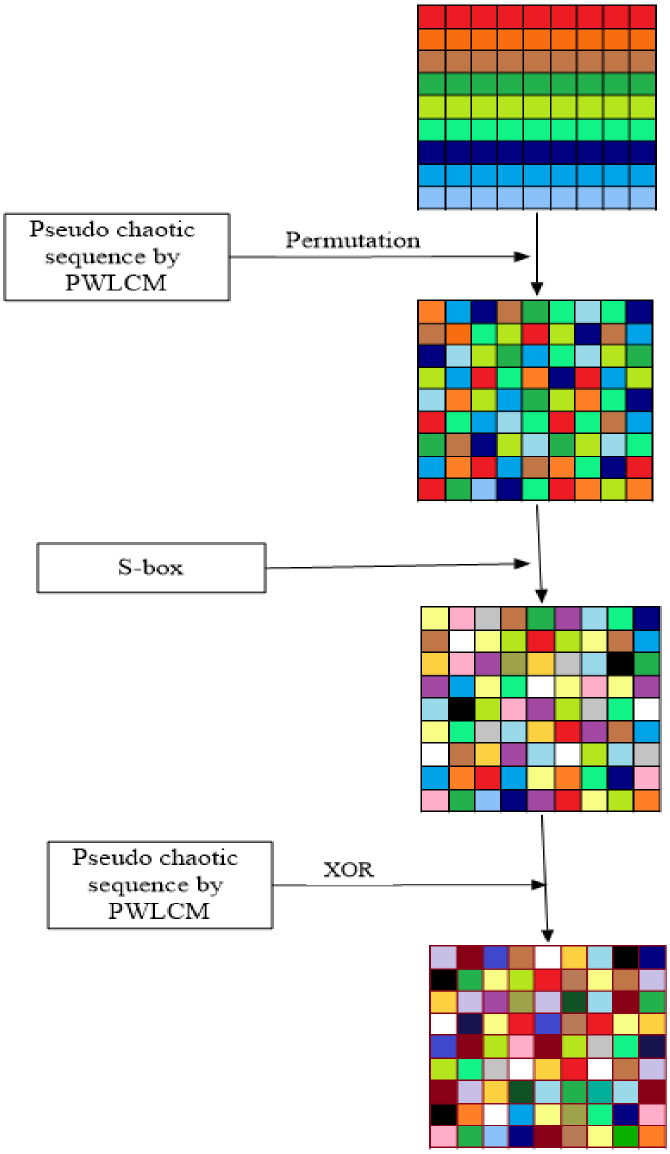

Pseudo chaotic sequence by PWLCM
Permutation
S-box
Pseudo chaotic sequence by PWLCM
XOR

FIGURE 4.2: Pixel change effect in various stages of encryption

The permutation sequence is formed by comparing position of numbers in the chaotic sequence and sorted sequence. Plainimage is converted into 1-dimensional array and permuted using the permutation sequence. Then another chaotic sequence is generated by iterating PWLCM using k_2 and the S-box is constructed by using this chaotic sequence. The S-box is applied on the permuted 1-dimensional image sequence. Finally a chaotic sequence of real numbers is constructed by logistic map using k_3 and converted into integers sequence. This sequence is XORed with the substituted 1-dimensional image array sequence. The cipher image is received by converting this 1-dimensional array into image form. A sample 9 × 9 color image and effects of various encryption stages are depicted in Figure 4.2. The structure of proposed image encryption scheme is shown in Figure 4.3, while the summarized form of the procedure is depicted as block diagram and shown in Figure 4.1.

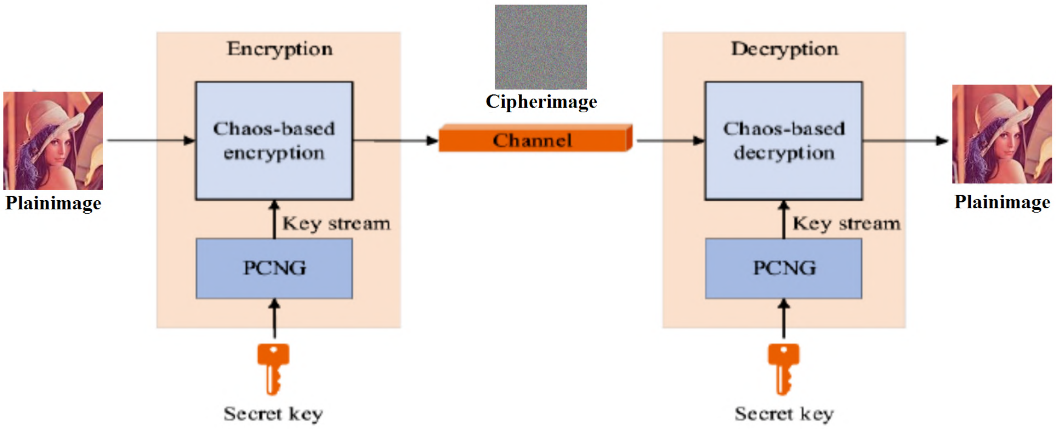


FIGURE 4.3: General architecture of the proposed image encryption scheme

The above shown Figure 4.3 represents the general architecture of the proposed image encryption scheme. Here the scheme inputs the plainimage, uses chaos based image encryption technique involving the key stream generated by psudo chaotic number generators (chaotic maps) and converts it into cipherimage. Then image decryption algorithm inputs cipherimage and works vice versa to reveal the plainimage. Figure 4.4 describes the internal structure of the proposed image encryption scheme.

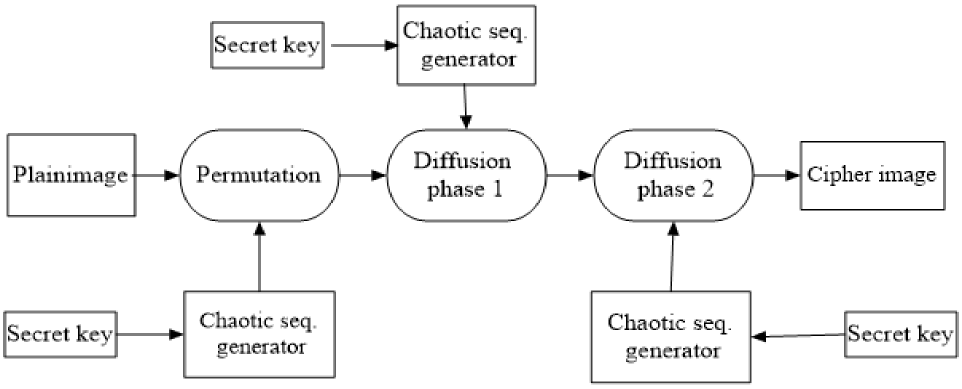


FIGURE 4.4: Structure of image encryption algorithm

4.1.3 Permutation Phase

In this phase, the pixel positions of the color image I are altered by using a suitable permutation. The permutation array is generated by using the piecewise linear chaotic map (PWLCM).

Algorithm 4.1.1. (Algorithm for Permutation of image pixels)
Input: Color image I, secret key $k_1 = \{x_0,\ y\}$, chaotic map (2.10).
Output: Scrambled image vector P.

1. Convert the color (RGB) image I in its digital form M (containing three, two dimensional matrices M_R, M_G and M_B for the Red, Green and Blue color channel respectively) of size N, where the entries of M *i.e.*, $m_i \in [0,\ 255]$ and $a \times b$ is the order of each component of M, while a, b are the numbers of rows and columns of M_R, M_G and M_B respectively.

2. Reshape the matrix M as one dimensional array,
$$M = \{m_{R_1}, m_{R_2}, \ldots, m_{R_{ab}}, m_{G_1}, m_{G_2}, \ldots, m_{G_{ab}}, m_{B_1}, m_{B_2}, \ldots, m_{B_{ab}}\},$$
hence the new formed array is denoted as $Z = \{z_1, z_2, \ldots, z_N\}$.

3. Obtain the sequence $A = \{a_1, a_2, ..., a_N\}$ by iterating the chaotic map (2.10) and discarding first 10000 numbers to avoid transient effect, using the key k_1.

4. Sort sequence A in ascending order to form $B = \{b_1, b_2, \ldots, b_N\}$ as:
$$B = \text{Sort}(A)$$

5. Using the relationship of the sequences A and B, $b_i = a_{t_i}$, for $i = 1, 2, \ldots, N$, compute permutation vector $T = \{t_1, t_2, \ldots, t_N\}$.
$$[B,\ T] = \text{Sort}(A)$$

6. Use T to permute the position of elements of vector Z.

$$P = Z(T)$$

7. After applying permutation on Z it becomes $P = \{p_1, p_2, ..., p_N\}$.

4.1.4 Substitution Phase

In this step permuted pixel vector P undergoes the substitution by using a substitution box as look up table. This technique is used to hide statistical properties of data and reduces correlation between neighboring data.

Substitution box, in short, S-box is used as the main non-linear component of algorithm. The purpose of using such S-box is to generate non-linearity in an encryption process and also to generate confusion and diffusion (Section 3.5.5.1) in cipher image. The use of S-box enhances the protection of scheme against linear and differential cryptanalysis.
Here the given algorithm comprising the generation of S-box with the help of chaotic map (2.10) and then its use as look up table for image encryption purpose. It is slightly modified algorithm presented in [158]. The secret key k_2 as described in the Section 4.1.1, is used for this algorithm. The proposed algorithm is stated below:

Algorithm 4.1.2. (Algorithm for the substitution of image pixel values using S-box)
Input: Secret key k_2, chaotic map (2.10), permuted image vector $P = \{p_1, p_2, ..., p_N\}$.
Output: Pre-encrypted image S'.
Using the given chaotic map (2.10), an S-box is constructed and used for pixel value substitution by executing the following steps.

1. Make 256 sub-interval regions of the interval $[0.1, 0.9]$ of fixed length $\triangle h$. That is,

$$\triangle h = (0.9 - 0.1)/256 = 0.003125$$

Label each sub-interval region as $R_0, R_1, ..., R_{255}$.

$$R_{i+1} = (0.1 + i. \triangle h,\ 0.1 + (i+1) \triangle h); \quad \text{for } i = 0, 1, 2, \cdots, 255$$

2. Use the parameters x'_0 and y' of the secret key k_2 for chaotic map (2.10) to generate a sequence x_n (by reoving initial initial 10000 values to avoid transient effect)of only those values that lies in [0.1, 0.9].

$$x_{n+1} = f(x'_n, y') = \begin{cases} \dfrac{x'_n}{y'} & \text{if} \quad 0 \le x'_n < y' \\ \dfrac{x'_n - y'}{0.5 - y'} & \text{if} \quad y' \le x'_n < 0.5 \\ \dfrac{1 - y' - x'_n}{0.5 - y'} & \text{if} \quad 0.5 \le x'_n < 1 - y' \\ \dfrac{1 - x'_n}{y'} & \text{if} \quad 1 - y' \le x'_n \ < 1 \end{cases}$$

3. Initialize an empty array S.

init[ ] array S = new int[8];

4. Whenever a value x_n of generated chaotic sequence belongs to some particular sub-interval R_i $(i = 0, 1, ..., 255)$, store that sub-interval region's index i in S.

```
for   $x_n \in \mathrm{R}_i$
      $S \leftarrow \mathrm{int}[i];$
```

Discard those values which does not fall in any sub-interval region or giving repeated sub-interval region's index-value.

$$S = \mathrm{unique}(S,\ \text{‘stable’});$$

5. For each pixel p_i in the permuted image $P = \{p_1, p_2, \ldots, p_N\}$ replace p_i by $S(p_i)$ where $i \in \{1, 2, \ldots, 256\}$. The resulting array is then denoted by $S' = \{s_1, s_2, \ldots, s_N\}$.

$$S' = S(p_i)$$

The output of this algorithm is the pre-encrypted image S'. Note that in Step 2 the use of a slightly different value of x'_0 or y' will result in an entirely different S-box. Thus, the above algorithm can be used to generate infinitely many S-boxes. One such S-box is constructed by setting parameter $x'_0 = 0.7666$ and with fixed value of $y' = 0.15$ in (2.10). The resulting array after Step 5 is given in Table 4.1 as 16×16 matrix.

By using SET (S-box Evaluation Tool) [159], the properties of this S-box are examined. It is noted that S-box is balanced. Other characteristics of thus generated S-box are as follows:

Table 4.1: S-box

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

Table 4.2: Comparison of properties of S-box

S-box	**Non-linearity**				**SAC**		**BIC**	**BIC-**
	Min	**Avg.**	**Max**	**Min**	**Avg.**	**Max**	**nonlinearity**	**SAC**
APA S-box [160]	112	112	112	0.4140	0.4987	0.6015	112	0.499
AES S-box [161]	112	112	112	0.3671	0.5058	0.5975	112	0.504
Gray S-box [162]	112	112	112	0.3906	0.5058	0.5781	112	0.502
Skipjack S-box [163]	104	105.7	108	0.3750	0.4980	0.6093	104.1	0.499
Residue Prime [164]	94	99.5	104	0.4062	0.5012	0.5937	101.7	0.502
Xyi S-box [165]	104	105	106	0.4218	0.5048	0.5937	103.7	0.503
Prop. S-box	100	103	106	0.4062	0.5029	0.6562	103.9	0.506

4.1.5 Diffusion Phase

To scramble the internal structure of pixels, we use chaotic logistic map and a Boolean operation XOR. For this purpose first a random sequence is generated by using chaotic logistic map. This sequence is used to generates randomness in pre-encrypted image S'.

Algorithm 4.1.3. (Algorithm for the diffusion of pre-encrypted image)

Input: Pre-encrypted image S', secret key $k_3 = \{w_0, \mu\}$, chaotic map (2.9).

Output: Final encrypted image C.

1. Input the secret key $k_3 = (w_0, \mu)$ in logistic map (2.9) and iterate it $N+10000$ times, discard initial 10000 values to remove transient effect for obtaining a sequence R of N real numbers $R = \{r_1, r_2, ..., r_N\}$.

2. The real number sequence r_k where $k = 1, 2, ..., N$ is changed into integer sequence using the relation,

$$Q_k = \text{int}(254 \times (r_k - \min(r_k))/d) + 1, \tag{4.1}$$

   where $d = \max(r_k) - \min(r_k)$.

3. Encrypt each element of array S' by mixing with the corresponding element of Q, using bitwise XOR *i.e.*,

```
for $i$ = 1, $i$ ++, $i$ = $N$ do
    if $i$ = 1, then
        $c(i) \leftarrow s(i) \oplus q(i)$
    else
        $c(i) \leftarrow c(i-1) \oplus q(i) \oplus s(i)$;
    end
end
```

4. By converting resulting matrix into image form, a cipher image C is obtained.

$$C = \text{reshape}(C, 256, 256, 3).$$

Example 4.1.4.

The above explained encryption process can be illustrated by a simple example. Let us take a two dimensional matrix block I of order $a \times b$ as the original image, where a, $b = 4$

$$I = \begin{bmatrix} 10 & 13 & 6 & 14 \\ 15 & 7 & 9 & 2 \\ 8 & 1 & 4 & 11 \\ 3 & 12 & 5 & 16 \end{bmatrix}$$

it is converted into one dimensional array Z as:

$$Z = \{10, 15, 8, 3, 13, 7, 1, 12, 6, 9, 4, 5, 14, 2, 11, 16\}$$

Let the control parameter of chaotic map (2.10) be $x_0 = 0.766$, $y = 0.3432$ as k_1, $x'_0 = 0.7666$, $y' = 0.15$ as k_2 and that of chaotic map (2.9) be $w_0 = 0.7666$, $\mu = 0.3432$ as k_3. Iterate the chaotic map (2.10) with the given parameters the following sequence and its sorted sequence are obtained by using Algorithm (4.1.1)

$$A = \{0.7660, 0.2340, 0.6818, 0.3182, 0.9217, 0.0729, 0.2129, 0.6189, 0.3811, 0.2418, \\ 0.7045, 0.2955, 0.8611, 0.1389, 0.4046, 0.3915\}$$

Then the chaotic sequence A is sorted in ascending order to get another sequence B as follows:

$$B = \{0.0729, 0.1389, 0.2124, 0.2340, 0.2418, 0.2955, 0.3182, 0.3811, 0.3915, 0.4046, \\ 0.6189, 0.6818, 0.7045, 0.7660, 0.8611, 0.9271\}$$

Using the relationship of the sequences A and B, $b_i = a_{t_i}$, hence computed permutation sequence T is:

$$T = \{6, 14, 7, 2, 10, 12, 4, 9, 16, 15, 8, 3, 11, 1, 13, 5\}$$

Sequence T is then applied on Z to get permuted image array P. That is:

$$P = \{7, 2, 1, 15, 9, 5, 3, 6, 16, 11, 12, 8, 4, 10, 14, 13\}$$

The S-box given in Table 4.1 is applied on the array P to get S' as;

$$S' = \{253, 61, 48, 213, 92, 76, 97, 139, 49, 120, 113, 196, 202, 186, 251, 245\}$$

After this for diffusion purpose chaotic map (2.9) is used to generate a random sequence R.

$$\begin{aligned} R = \{&0.7666, 0.7157, 0.8139, 0.6058, 0.9552, 0.1713, 0.5677, 0.9816, 0.0721, 0.2675,\\ &0.7838, 0.6778, 0.8735, 0.4420, 0.9865, 0.0531\} \end{aligned}$$

The integer sequence Q from R is obtained by using the Step (2) of Algorithm (4.1.3):

$$Q = \{195, 181, 208, 151, 246, 33, 141, 254, 6, 59, 200, 171, 224, 107, 255, 1\}$$

Finally, by using Q, the cipher image C is obtained by following Step (3, 4) of Algorithm (4.1.3).

$$C = \begin{bmatrix} 62 & 190 & 125 & 194 \\ 182 & 211 & 62 & 19 \\ 86 & 63 & 135 & 23 \\ 20 & 74 & 232 & 227 \end{bmatrix}$$

4.2 Decryption Algorithm

The ciphered image C can be converted back to its original color image by using the decryption algorithm. Decryption process has a similar combination of three stages as used in encryption scheme. The effects made by the XOR operation on the pre-encrypted image are first removed during decryption. For this purpose a random sequence R of real number is generated using k_3. The sequence is converted into integers Q and bitwise XOR is performed with the cipher image array including the preceding value.

In order to reverse the effects generated by substitution using S-box, an inverse S-box of an S-box (generated by Algorithm (4.1.2)) is constructed. The use of inverse S-box on the pre-encrypted image demolish all the effects generated by the use of S-box. In this way the permuted image array is retrieved.

Finally a random sequence together with sorted sequence and the inverse permutation sequence is determined using Algorithm (4.1.1). The permutation effects are reversed by applying inverse permutation sequence. After converting the resulting array into image form, the original plain image is obtained.

Algorithm 4.2.1. (Image Decryption Algorithm)
Input: Color cipher image C, Secret keys k_1, k_2, k_3, Algorithm (4.1.1, 4.1.2, 4.1.3), Chaotic map (2.9), Chaotic map (2.10).
Output: Original image I.

1. Convert the color (RGB) cipher image in digital form C (containing three, two dimensional matrices C_R, C_G and C_B for the Red, Green and Blue color channel respectively) of size $N = a \times b \times 3$, where the entries of C *i.e.*, $c_i \in [0,\ 255]$ and $a \times b$ is the order of each component of C, while a, b are the numbers of rows and columns of C_R, C_G and C_B respectively.

2. Reshape the matrix C as one dimensional array,

$$C = \{c_{R_1}, c_{R_2}, \ldots, c_{R_{ab}}, c_{G_1}, c_{G_2}, \ldots, c_{G_{ab}}, c_{B_1}, c_{B_2}, \ldots, c_{B_{ab}}\}.$$

3. As in step 1 and 2 of Algorithm (4.1.3), the receiver by using common secret key k_3 generate the sequence $R = \{r_1,\ r_2 \ldots, r_N\}$ of size N.

4. Each element c_i of C (in step 2) is pre-decrypted as:

```
for $i = 1, i ++, i = N$ do
    if $i = 1$, then
        $s(i) \leftarrow c(i) \oplus r(i)$
    else
        $s(i) \leftarrow c(i-1) \oplus r(i) \oplus c(i)$;
    end
end
```

5. Again using common secret key k_2, generate S-box S as in step 5 of Algorithm 4.1.2.

6. Find the inverse S-box S^{-1} of S.

7. Using S^{-1} as lookup table each element of pre-decrypted image S' is replaced by corresponding element in S^{-1} that is $p_i = S^{-1}(s_i)$, $i = 1, 2, \ldots, N$. The resulting array is stored in $P = \{p_1, p_2, \ldots, p_N\}$.

8. Now using common secret key k_1, iterate the chaotic map (2.10) for k_1 to get the sequence $A = \{a_1, a_2, \ldots, a_N\}$.

9. Sort sequence A in ascending order to form $B = \{b_1, b_2, \ldots, b_N\}$.

$$B = \mathrm{sort}(A)$$

10. The permutation array is computed as in step 5 of Algorithm (4.1.1), then the inverse permutation vector T^{-1} is calculated.

$$[B,\ T] = \mathrm{sort}(A)$$

$$[D,\ T^{-1}] = \mathrm{sort}(T).$$

11. Use T^{-1} to permute the position of elements of image array P of step (7) to get pre-permuted array $Z = \{z_1, z_2, \ldots, z_N\}$.

$$Z = P(T^{-1})$$

12. Store Z_i in a matrix to form image I.

Example 4.2.2.

The above stated decryption algorithm wipes out all the effects of encryption on the original image. For the illustration of working procedure a cipher image block C is taken and the decryption Algorithm (4.2.1) is applied on it as follows;

$$C = \begin{bmatrix} 62 & 190 & 125 & 194 \\ 182 & 211 & 62 & 19 \\ 86 & 63 & 135 & 23 \\ 20 & 74 & 232 & 227 \end{bmatrix}$$

The one dimensional array of C is:

$$C = \{62, 182, 86, 20, 190, 211, 63, 74, 125, 62, 135, 232, 194, 19, 23, 227\}$$

Let the control parameter of chaotic map (2.10) be $x_0 = 0.766$, $y = 0.3432$ as k_1, $x'_0 = 0.7666$, $y' = 0.15$ as k_2 and that of chaotic map (2.9) be $w_0 = 0.7666$, $\mu = 0.3432$ as k_3. The chaotic map (2.9) is iterated with the given parameters in k_3 for a real sequence that is converted into an integer sequence R using Algorithm (4.2.1) as:

$$R = \{195, 181, 208, 151, 246, 33, 141, 254, 6, 59, 200, 171, 224, 107, 255, 1\}$$

Bitwise XOR of R, C and its preceding elements are performed as described in Step 4 of the Algorithm (4.2.1) to get S' as:

$$S' = \{253, 61, 48, 213, 92, 76, 97, 139, 49, 120, 113, 196, 202, 186, 251, 245\}$$

By using k_2 in chaotic map (2.10) and following Algorithm (4.1.2), an S-box is constructed and then its inverse S-box is formed. To get the permuted array P an inverse S-box is applied on S', that is:

$$P = \{7, 2, 1, 15, 9, 5, 3, 6, 16, 11, 12, 8, 4, 10, 14, 13\}$$

Finally, chaotic map (2.10) is iterated with the given parameters in k_1 to make a random sequence, it is sorted and the inverse permutation sequence is determined using Algorithm (4.1.1), that is,

$$T^{-1} = \{14, 4, 12, 7, 16, 1, 3, 11, 8, 5, 13, 6, 15, 2, 10, 9\}$$

This inverse permutation sequence T^{-1} is applied on P to get Z, as:

$$Z = \{10, 15, 8, 3, 13, 7, 1, 12, 6, 9, 4, 5, 14, 2, 11, 16\}$$

By converting it into a matrix form the original image I can be obtained as:

$$I = \begin{bmatrix} 10 & 13 & 6 & 14 \\ 15 & 7 & 9 & 2 \\ 8 & 1 & 4 & 11 \\ 3 & 12 & 5 & 16 \end{bmatrix}$$

4.3 Results and Discussions

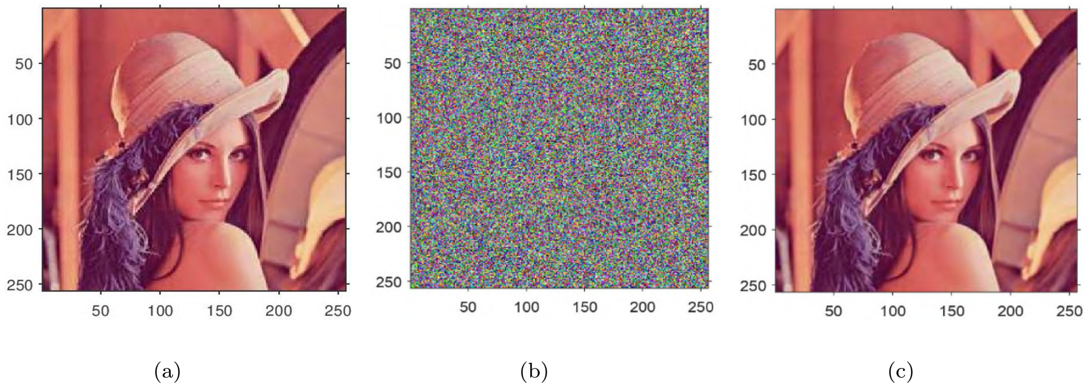
For the demonstration of the proposed scheme, Algorithm (4.1.1, 4.1.2, 4.1.3) and Algorithm (4.2.1) are implemented on Matlab R2016b and applied on two images as shown in the figures below. The MATLAB implementation code of image encryption scheme is available at https://github.com/tahirsajjad?tab=repositories. In the first example, as shown in the Figure 4.5(a), the standard color image of Lena (256 × 256) is selected for the demonstration of proposed image encryption scheme and also used for the comparison of the results with many other existing schemes. After applying the proposed image encryption scheme, the resulting cipher image is shown in Figure 4.5(b). Finally Figure 4.5(c) shows the result of decryption algorithm by getting back the original image from the cipher image.

It is evident that the decryption results are same as the original image having no distortion, noise or data loss effects. To see the further security aspects of encryption results, the cipher image is split into red, green and blue channels. The distribution of pixels around the image can be observed by using the histogram. Figure 4.8 shows the uniform distribution of cipher image component's pixels.

This shows that the cipher image does not provide any information about the distribution of pixel in the plain image. It is also important to see the correlation in the neighboring pixels of cipher image.

From Figure 4.9 (b, d, f) it is evident that the neighboring pixels in RGB components of plain image are highly correlated. Figure 4.9 (a, b, c) shows that the RGB components of the cipher image's pixels have almost no correlation with each other.

It means that the neighboring pixel's information of the original image is properly concealed in the RGB components of the cipher image.



(a)

(b)

(c)

Figure 4.5: Image encryption algorithm performance for Lena image: (a) original image, (b) encrypted image, (c) decrypted image.

Similarly, the proposed encryption and decryption algorithm are applied on the second color image of Baboon (256×256) depicted as Figure 4.6(a). The resulting cipher image is shown in Figure 4.6(b) and Figure 4.6(c) is the decrypted image.

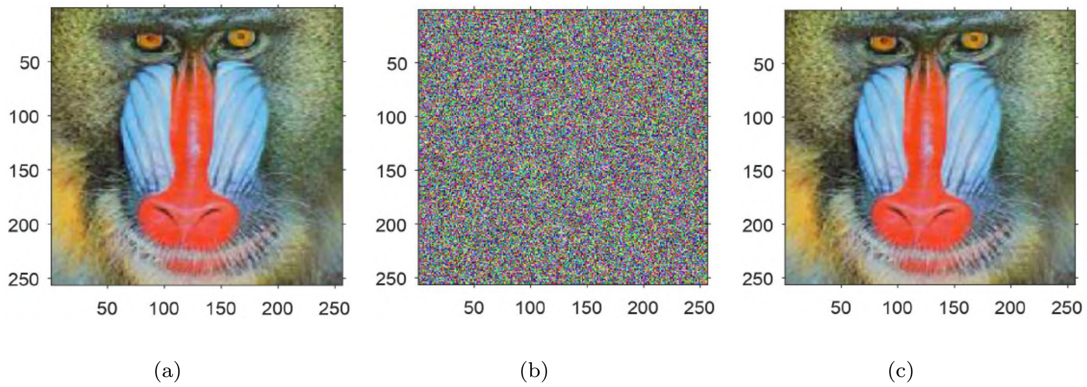


Figure 4.6: Image encryption algorithm performance for Baboon image: (a) original image, (b) encrypted image, (c) decrypted image.

4.4 Security Analysis

This section is devoted to address the security properties of the proposed scheme.

4.4.1 Key Space

Key space is considered as an important feature in any cryptosystem. It should be large enough to have the ability to resist against brute force attacks. In the proposed encryption algorithm, secret key is a tuple of $k = (\ k_1, k_2, k_3\ )$ comprising of 3 secret keys, each for the different phase of encryption scheme. These secret keys contain parameters of associated chaotic maps that is x_0, y, x'_0, y', w_0, μ. If the precision of these parameters is taken as 10^{-15}, the key space size will be $(10^{15})^3 \times (10^{15})^3 = 10^{90} \approx 2^{299}$. Alvarez *et al* [135] identified that the adequate key space for image encryption scheme should be larger than 2^{100} to oppose brute force attacks. Here the key space of the proposed algorithm is compared with other image encryption techniques that use chaotic maps, for example [44] uses PWLCM and XOR operation for encryption process, similarly [45] uses PWLCM's generated chaotic sequence for cyclic shift and then uses XOR operation for diffusion etc. The key space of the proposed scheme is large enough to resist against brute force attack.

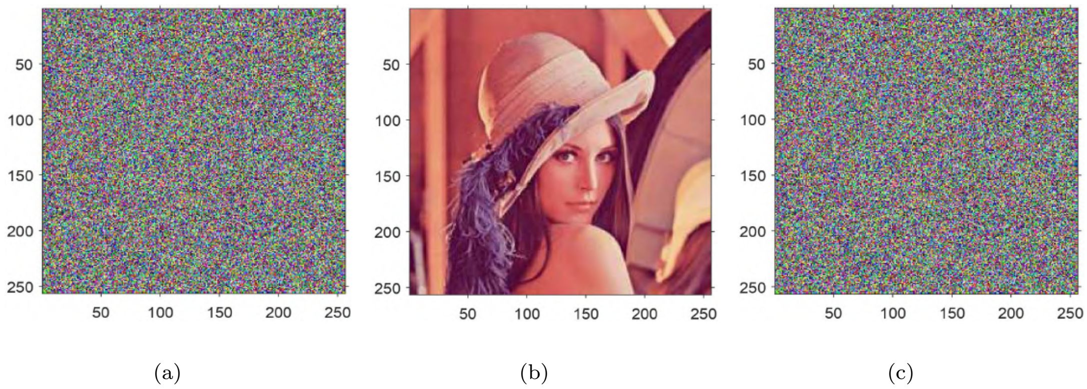
Table 4.3: Key space size comparison

Image encryption schemes	**Key Space**
Zhang et al. [45]	2^{186}
Wang et al. [44]	2^{149}
Guesmi et al. [166]	2^{256}
Zhu et al. [167]	2^{339}
Proposed scheme	2^{299}

Table 4.3 shows the key space comparison of the proposed image encryption scheme with other existing image encryption schemes. For the recovery of the original image the adversary needs to correctly guess all these six components of shared secret key.

4.4.2 Key Sensitivity

An image encryption scheme should be highly conscious for its secret key and a change of single-bit in its secret key should crop an entirely different encrypted result. In the sensitivity analysis for secret key, a highly sensitive key is demanded.



(a)

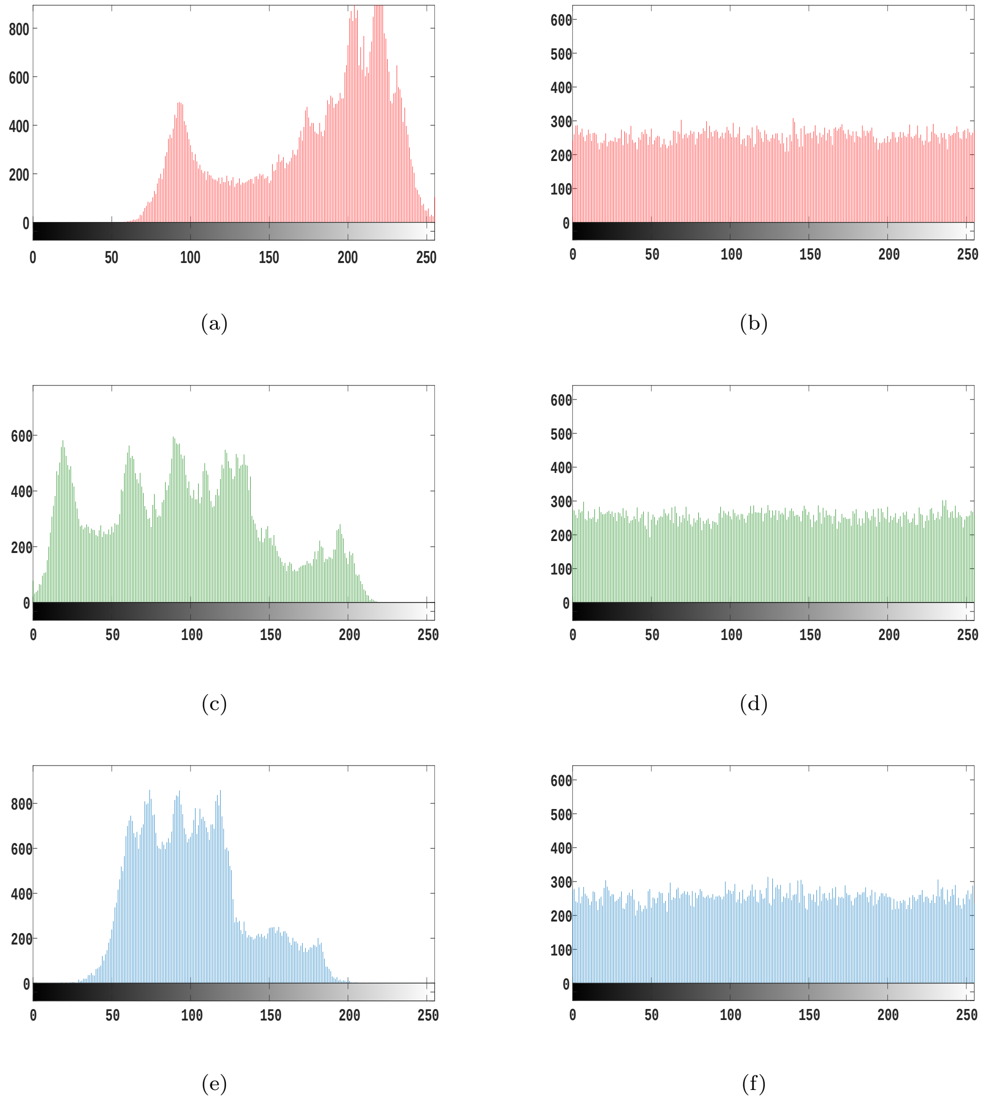
(b)

(c)

Figure 4.7: Key sensitivity performance with: (a) encrypted image, (b) decrypted image, (c) decrypted by slightly changed key.

Cipher image should not be decrypted accurately even if there is a very small change in encryption key.

Note that in the proposed scheme, the output of decrypted Algorithm (4.2.1) completely changed even if there is a very minor change in any of the component of used Key $k = (k_1,\ k_2,\ k_3)$. For example, by making a change in one parameter x_0 of k_1 that is, on adding 0.0000000000000001, the new value of x_0 will become 0.7660000000000001. Using this the decryption algorithm will not produce the original image. Here the encrypted image is shown in Figure 4.7(a), decrypted image in Figure 4.7(b) and the decryption result obtained by using slightly different key is shown in Figure 4.7(c).



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

FIGURE 4.8: Experimental results for the histogram of red, green, blue component of: (a, c, e) plain image, (b, d, f) cipher image.

Similar effects can be seen for a slight change in any parameter of used chaotic maps. From the decrypted image with the changed key, it is observed that, no clue or gesture about the original image is found. Hence it is evident that the proposed scheme is highly sensitive to secret keys.

4.4.3 Distribution of Pixels in Cipher Image

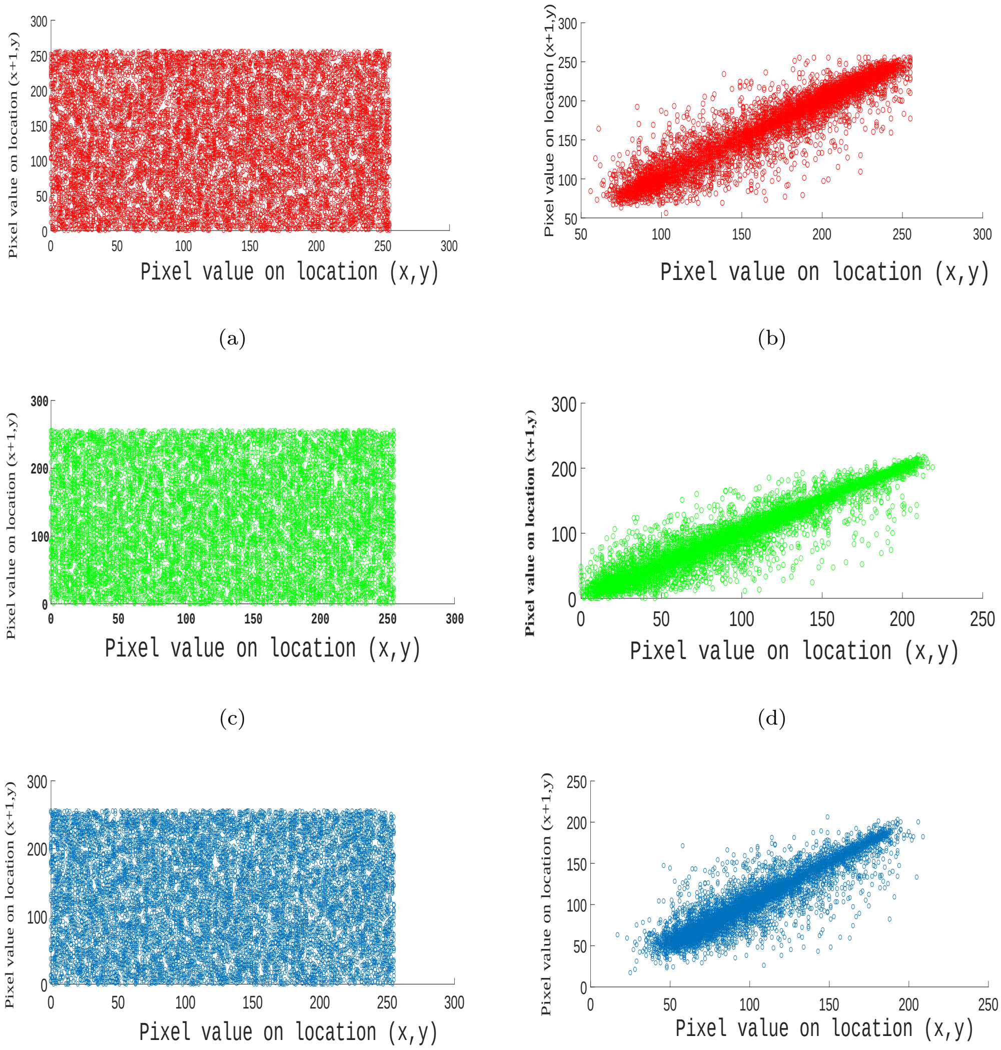
Image histogram displays the dispersion of pixels in an image. This can be observed when the number of pixels are plotted in histogram. In the above examples RGB component-wise histograms of the plain image of Lena and its cipher image are shown in Figure 4.8 (a, c, e) and Figure 4.8 (b, d, f). From these figures It is clear that, there does not exist any clue to mount a statistical attack on the encrypted image.

4.4.4 Correlation Analysis

The property of having high confusion and diffusion can be checked by a test of correlation among neighboring pixels in the plainimage and their corresponding cipher image. The correlation is analyzed in the adjacent pixels of the plain image as shown in Figure 4.9 (b, d, f) and cipherimage of Lena through Figure 4.9 (a, c, e). For the calculation of correlation coefficients among the neighboring pixels in horizontal, vertical and diagonal directions. Equation (3.10) has been used for this purpose.

Table 4.4: Correlation coefficient of two neighboring pixels in plain and cipher image

	Red		**Green**		**Blue**	
Direction	**Orig.**	**Ciph.**	**Orig.**	**Ciph.**	**Orig.**	**Ciph.**
Horizontal	0.9794	-0.0024	0.9806	-0.0009	0.9604	-0.0032
Vertical	0.9574	0.0052	0.9593	-0.0004	0.9237	-0.0017
Diagonal	0.9363	-0.0003	0.9400	-0.0012	0.8898	0.0027



(a)

(b)

(c)

(d)

(e)

(f)

FIGURE 4.9: Row-wise correlation in: (a, c, e) cipher image red green, blue color components, (b, d, f) plain image's red, green, blue color component.

The values in resulting Table 4.4 obtained from the Equation (3.10) are closer to zero for the cipher image. Hence neighboring pixels in encrypted image are almost uncorrelated.

4.4.5 Information Entropy

This feature of analysis measures the randomness in a cipher image. It also tells about the average amount of information carried by cipher image. Let g be a cipher image then entropy value of image can be calculated by the Formula (3.11).

Table 4.5: Statistical analysis of the proposed scheme for different types of plain and encrypted images

Images		**Correlation in the Dir. of plainimage**			**Correlation in the Dir. of cipherimage**			**Entropy**	
		Row	**Diag.**	**Column**	**Row**	**Diag.**	**Column**	**Orig.**	**Cipher**
For gray 256×256 **size images**									
1. Moon		0.9390	0.9037	0.9020	-0.0009	0.0046	0.0009	6.7093	7.9971
2. Aerial		0.8602	0.8213	0.9050	0.0107	0.0022	0.0021	7.3118	7.9969
3. Airplane		0.9366	0.8927	0.9571	-0.0038	0.0057	0.0022	6.4523	7.9970
4. Clock		0.9741	0.9389	0.9565	-0.0002	0.0010	-0.0087	6.7057	7.9968
5. Chemical plant		0.8984	0.8529	0.9466	-0.0014	-0.0023	-0.0065	7.3424	7.9972
6. Resolution chart		0.8667	0.7562	0.8722	-0.0089	0.0009	0.0027	1.5483	7.9969
For gray 512×512 **size images**									
7. Couple		0.8926	0.8557	0.9371	-0.0007	-0.0047	0.0005	7.2010	7.9993
8. Stream		0.9275	0.8975	0.9404	-0.0002	0.0009	-0.0022	5.7056	7.9994
9. Aerial		0.8602	0.8031	0.9008	-0.0025	0.0016	-0.0014	6.9940	7.9992
10. Truck		0.9205	0.9074	0.9620	0.0001	0.0034	-0.0006	6.0274	7.9994
11. Airplane		0.9459	0.8962	0.9463	0.0001	0.0001	0.0028	4.0045	7.9993
12. Tank		0.9321	0.9017	0.9456	-0.0001	-0.0034	-0.0010	5.4957	7.9992
For color $256 \times 256 \times 3$ **size images**									
13. Female	Red	0.9294	0.9129	0.9779	0.0004	0.0042	0.0033	5.7150	7.9969
	Green	0.9106	0.8941	0.9748	0.0027	0.0050	0.0030	5.3738	7.9967
	Blue	0.9130	0.8958	0.9726	0.0024	-0.0057	-0.0051	5.7116	7.9969
14. House	Red	0.9353	0.9126	0.9671	-0.0011	-0.0005	-0.0016	6.4311	7.9969
	Green	0.9474	0.9320	0.9805	-0.0025	-0.0019	0.0001	6.5389	7.9970
	Blue	0.9749	0.9625	0.9820	0.0051	-0.0019	0.0008	6.2320	7.9970
15. Tree	Red	0.9361	0.9159	0.9590	-0.0052	0.0114	0.0022	7.2104	7.9968
	Green	0.9457	0.9318	0.9687	-0.0045	0.0042	-0.0020	7.4136	7.9974
	Blue	0.9406	0.9265	0.9612	-0.0011	0.0069	0.0095	6.9207	7.9974
16. Jelly bean	Red	0.9763	0.9537	0.9745	-0.0010	-0.0001	-0.0014	5.2626	7.9974
	Green	0.9801	0.9603	0.9757	-0.0013	-0.0020	-0.0031	5.6947	7.9972
	Blue	0.9880	0.9799	0.9890	-0.0001	0.0003	-0.0041	6.5464	7.9974
17. Couple	Red	0.9562	0.9176	0.9493	-0.0047	-0.0055	-0.0052	6.2499	7.9974
	Green	0.9534	0.9002	0.9308	0.0073	0.0085	0.0048	5.9641	7.9973
	Blue	0.9442	0.8890	0.9178	-0.0046	0.0012	0.0033	5.9309	7.9970
For color $512 \times 512 \times 3$ **size images**									
18. Splash	Red	0.9951	0.9894	0.9936	-0.0022	0.0044	0.0013	6.9481	7.9992
	Green	0.9871	0.9711	0.9812	-0.0012	0.0001	-0.0042	6.8845	7.9994
	Blue	0.9789	0.9649	0.9826	0.0005	0.0023	-0.0008	6.1265	7.9993
19. Mandrill	Red	0.8660	0.8543	0.9231	0.0036	0.0007	-0.0021	7.7067	7.9993
	Green	0.7650	0.7348	0.8655	-0.0004	0.0011	-0.0015	7.4744	7.9993
	Blue	0.8809	0.8399	0.9073	-0.0015	-0.0028	-0.0014	7.7522	7.9994
20. Airplane	Red	0.9568	0.9343	0.9726	0.0036	0.0007	-0.0021	6.7178	7.9993
	Green	0.9678	0.9326	0.9578	-0.0004	0.0011	-0.0015	6.7990	7.9994
	Blue	0.9353	0.9146	0.9640	-0.0015	-0.0028	-0.0014	6.2138	7.9994
21. Sailboat	Red	0.9541	0.9420	0.9558	0.0036	0.0007	-0.0021	7.3124	7.9994
	Green	0.9663	0.9530	0.9715	-0.0004	0.0011	-0.0015	7.6429	7.9993
	Blue	0.9694	0.9530	0.9710	-0.0015	-0.0028	-0.0014	7.2136	7.9993

For exact random source having 256 different symbols, the ideal value of entropy $H(g)$ is 8. If the value of entropy is less than 8 in cipher image then it means that there is a possibility of predictability of plain image, which is dangerous for security of image encryption algorithm.

In the example of proposed scheme, the entropy of cipher image C (as shown in Figure 4.5 (b)) with 2^N as 255, using Matlab R2016b, turns out to be 7.9984. A comparison of information entropy values of different image encryption schemes is given in Table 4.6.

The result shows that entropy value of the encryption result is very near to the ideal entropy value 8. It ensures that amount of information lost in proposed image encryption scheme is almost zero.

Table 4.6: Entropy values comparison

Image encryption Schemes	**Entropy values**
Zhang et al. [45]	7.9992
Wang et al. [44]	7.9975
Thiyagarajan et al. [43]	7.9943
Wu et al. [168]	7.9912
Proposed scheme	7.9984

4.4.6 Differential Analysis

An essential property of a good performance image encryption algorithm is that, images encrypted with that algorithm should be totally different from plain images.

To check the difference in an encrypted image and making one pixel change in original image then encrypted image, the number of pixel change rate (NPCR) and unified average changing intensity (UACI) are used. The values of NPCR and UACI can be calculated by using Equation (3.12).

To resist against the differential attacks, NPCR and UACI values should large and approach to their ideal values. It can be seen from the experimental results obtained from Equation eqrefdiffer , that the proposed scheme gets high performance for NPCR and UACI. Therefore it will give well resistance against "known plain text attacks" and "chosen plain text attacks".

Table 4.7: NPCR and UACI values comparison

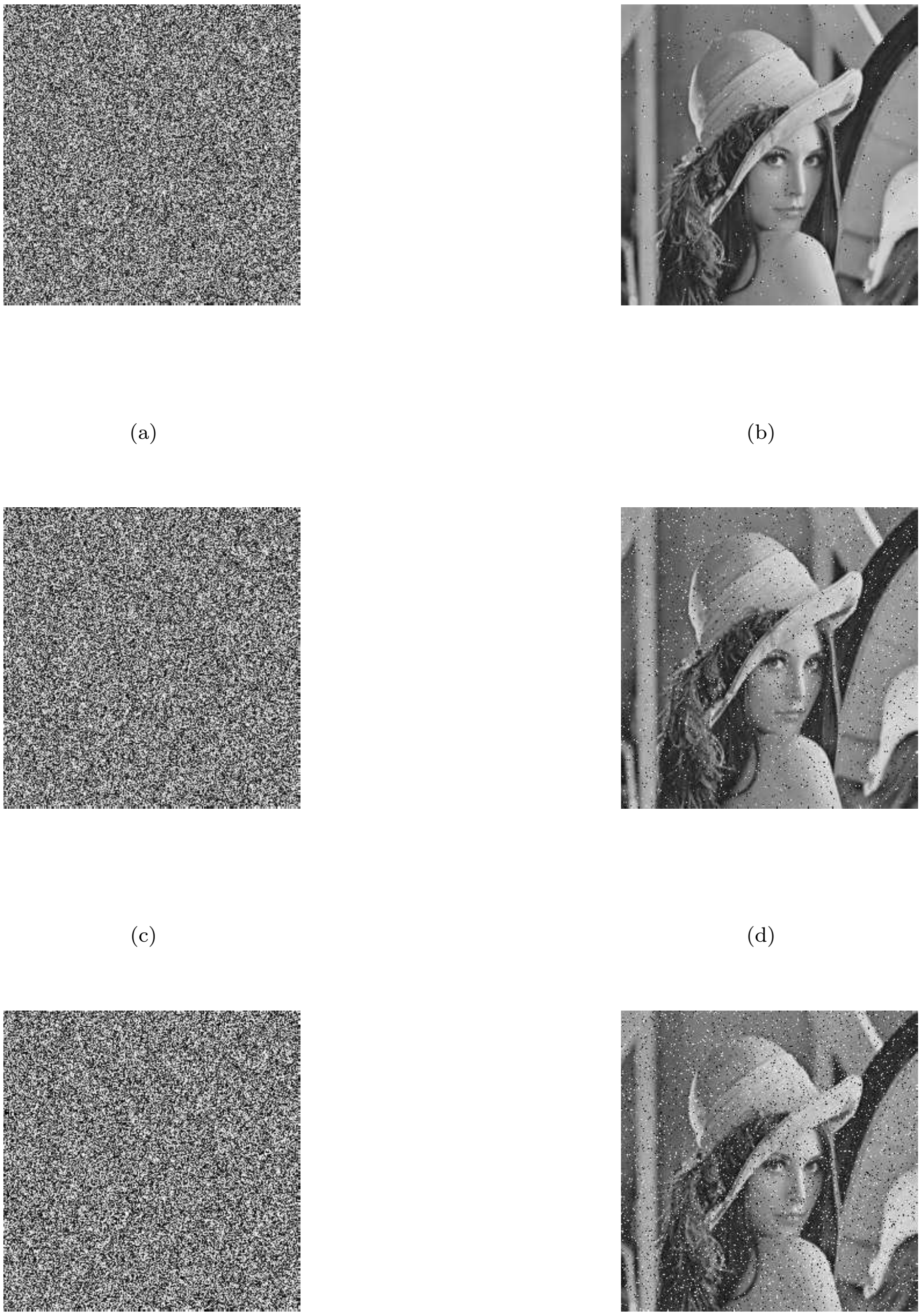
Image encryption Schemes	**NPCR**	**UACI**
Luo et al. [42]	99.6113	33.4682
Luo et al. [169]	99.5815	33.6665
Wang et al. [44]	99.5956	33.5512
Zhang et al. [45]	99.61	33.35
Proposed scheme	99.6094	33.4635

4.4.7 Noise and Data Loss Attacks

A perfect encryption scheme ought to diminish the noise effects caused by differences in pixels in the dectypted image. For checking the capability of proposed scheme in opposing noise and data loss attacks, a Lena image of size 256×256 is taken as test case.

In the encryption result of test image, we add 1%, 5% and 10% salt and pepper noise as shown in the Figure 4.10 (a, c, e). The decryption results of noised cipher images are also shown in Figure 4.10 (b, d, f). From the figure, it is clear that when the cipherimage endure salt and pepper noise or data loss attacks, the decrypted image obtained by using our encryption scheme maintain vast majority of original image information having only a small portion of uniformly distributed noise.

The peak signal to noise ratio (PSNR) provides a quantitative measure for the distinction between the original plain image I_P and its decryption result I_D.



(a) (b)

(c) (d)

(e) (f)

FIGURE 4.10: Experimental results for the performance evaluation of data loss attacks: (a, c, e) cipher images with 1%, 5% and 10% salt and pepper noise, (b, d, f) decryption results of corresponding images using our scheme.

The cumulative squared error between the decrypted image and the original image can be measured by using mean square error (MSE).For an image of size MN the PSNR and MSE values can be calculated using Equations (3.13) and (3.14).

The least value of MSE shows the minimum error by using the encryption scheme. While the PSNR is usually employed to calculate the ability of rehabilitation.

Table 4.8: Performance of MSE and PSNR about salt and pepper noise

Salt & pepper noise	**1%**	**5%**	**10%**
MSE	108.7962	497.3975	1030.7
PSNR	27.7987	21.1978	18.0335

The greater value of PNSR indicates the higher fidelity of decrypted image towards its original plain image. If I$_D$ and the I$_P$ are similar then the calculated value of PSNR approaches to infinity.

The value above 30 db shows that I$_D$ and I$_P$ are not sensible for PSNR. For the values above 35 db, it is difficult to differentiate between the original image and decrypted image. For checking the cipher image's robustness against noise attacks, 1%, 5% and 10% noise is added in the cipher image, as shown in Figure 4.10 (a, c, e). The calculated values of PSNR for these modified cipher images are shown in Table 4.8.

By observing the test results it can be seen that the encryption technique gives good performance for anti data loss and noise attacks.

4.4.8 Analysis of speed

For any algorithm, security considerations are important but a good encryption algorithm should also robust and efficient. The computational cost of the algorithm depends on the major operations like permutation process, S box generation and diffusion process. For an image of size $M \times N$, the time complexity for the number of floating point operations is $\mathcal{O}(5MN\log(MN))$ and for the other operations like Bitwise XOR etc is $\mathcal{O}(7MN)$. The running speed of encryption algorithm also depends upon the internal structure of algorithm. The internal structure of proposed scheme is designed in such a way that it is efficient by computation. In permutation phase only single round is adopted, that gives efficiency in computation. In second phase S-box is used as lookup table then XOR is used for generation of randomness. All these stages are computationally efficient. By using the 'tic' and 'toc' commands of MATLAB for the execution time of algorithm. It is found that the encryption algorithm approximately takes 0.25 sec while decryption algorithm takes 0.27 sec for 256×256 (grayscale) Lena image. For a color image of size 256×256 the average encryption and decryption times are 0.64 and 0.67 seconds, similarly for a grayscale image of 512×512 the encryption and decryption times are 0.82 and 0.85 seconds. A 512×512 sized color image consume 2.42 and 2.47 seconds for encryption and decryption.

4.4.9 Modifications Required for implementation on Other Types of Images

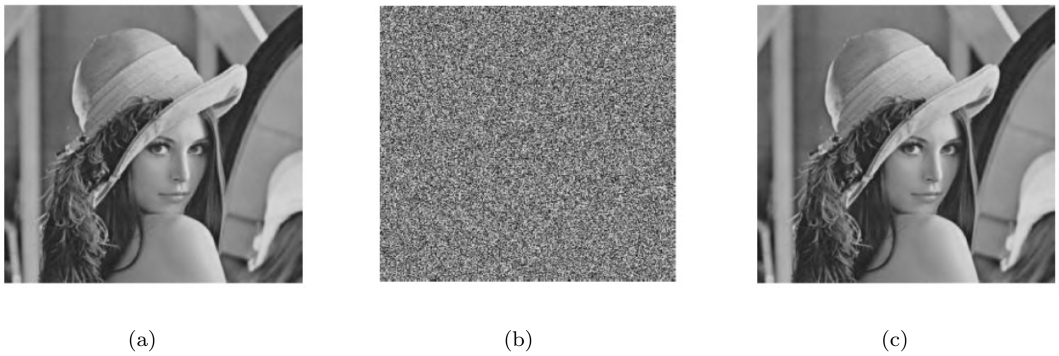
Different types of images, such as grayscale, RGB, or color (multi-channel) images, can be encrypted using the suggested image encryption scheme. Here the proposed encryption scheme is described for color images, but it can be implemented on gray scales images after some modification. For a gray scale of size $(m{\times}n)$, in Algorithm (4.1.1) the chaotic sequence of size $(m \times n)$ will be used for permutation and in the same way in Algorithm (4.1.3), for diffusion purpose the sequence of length $(m \times n)$ will be used. The rest part of the Algorithm works similarly as used for a color image.

For the encryption of a multi-channel image of size $(m \times n \times t)$, in Algorithm (4.1.1) chaotic map (2.10) is iterated to produce a pseudo random sequence of length $(m \times n \times t)$ that will be used for the permutation purpose. Then in the diffusion phase another pseudo random sequence of length $(m \times n \times t)$ will be generated and used through XOR operation.

The proposed scheme is not valid for binay images in its current form. The implementation at different types of images is further expressed in the next section.

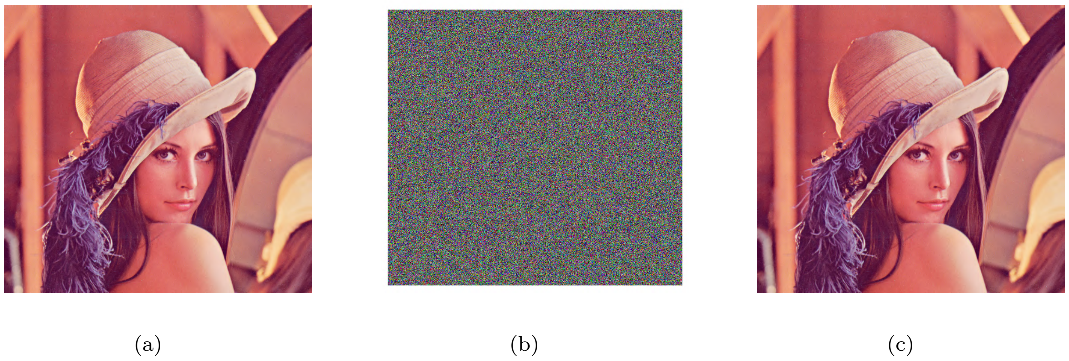
4.4.10 Performance for Different Type Images

The proposed image encryption scheme can be used for the encryption of different types of images like gray-scale, RGB or color (multi channel) images etc.



(a) (b) (c)

FIGURE 4.11: Encryption and decryption results of gray scale 256 × 256 size Lena: (a) plain image, (b) encrypted image, (c) decrypted image.



(a) (b) (c)

FIGURE 4.12: Encryption and decryption results of RGB (color) 512 × 512 size Lena: (a) plain image, (b) encrypted image, (c) decrypted image.

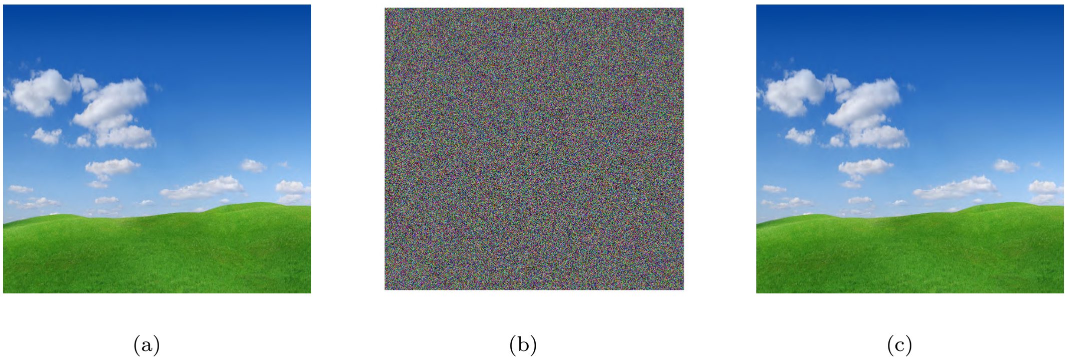


FIGURE 4.13: Encryption and decryption results of RGB (color) 768 × 768 size: (a) plain image, (b) encrypted image, (c) decrypted image.

Different size images can be encrypted by using the proposed image encryption scheme, for example 256 × 256, 512 × 512, 768 × 768 etc. Some results regarding the encryption and decryption of different type and sizes are illustrated in the above figures. For the performance evaluation, a Lena gray image of size 256 × 256 is taken as shown in the Figure 4.11 (a), encrypt it by using proposed image encryption scheme. The encryption results are shown in Figure 4.11 (b), then applied the decryption scheme to get the original image as shown in Figure 4.11 (c). The proposed encryption scheme is also implemented on RGB or color (multi-channel) images of 256 × 256 size and encryption/decryption results are depicted in Figure 4.5 and Figure 4.6. Here it is implemented on different size images, for this purpose another Lena RGB 512 × 512 size image is chosen as shown in Figure 4.12 (a). The encryption and decryption are performed under the proposed encryption scheme and results are displayed in Figure 4.12 (b, c). Another multi-channel 768 × 768 size image is taken. It is encrypted and decrypted by using the proposed scheme and results are depicted in Figure 4.13. From these results, it can be seen that the proposed scheme is implementable for various image types of different sizes.

Comparison

Overall comparison of proposed image encryption scheme with some other image encryption schemes is given below in Table 4.9:

Table 4.9: Properties comparison of cipher generated by taking Lena as test image

Algorithms	**NPCR**	**UACI**	**Correlation**	**Keyspace**	**Entropy**
Proposed scheme	99.6094	33.4635	0.0020	10^{90}	7.9984
Dhall et al. [74]	99.5808	33.5008	−0.0005	10^{76}	7.9987
Luo et al. [42]	99.6113	33.4682	0.0018	10^{169}	7.9993
Zhang et al. [45]	99.61	33.45	0.0038	10^{56}	7.9993
S. Sun. [170]	99.61	33.46	0.0044	10^{90}	7.9967
Wang et al. [44]	99.5956	33.5512	0.0038	10^{56}	7.9975

4.5 Conclusion

In this chapter a color image encryption scheme is presented. This scheme firstly used a chaotic map to generate permutation vector. Plain image pixels are permuted using this vector. Then an S-box is generated using chaotic map and used for substitution purpose. The properties of confusion and diffusion can be observed after the use of S-box. Finally a random sequence is generated by using chaotic map and bitwise XOR is performed to each pixel value with the generated sequence. By mixing of pixels in this way, has shown a significant change in relationship of nearby pixels horizontally, vertically and diagonally. The proposed algorithm has also offered resistance to different types of cryptographic attacks as known plain text attack, brute force attack etc. Security analysis is done by using statistical analysis, differential analysis, key space analysis, key sensitivity analysis, entropy analysis and speed analysis. The calculated value of proposed scheme for key space is 2^{299}, average correlation in cipher image is 0.0020, while NPCR, UACI and entropy values are 99.609, 33.46, 7.9984 respectively. From the security analysis, it seems that the perfect original image cannot be recovered by applying the known cryptographic attacks. Hence it is secure and implementable on real time image encryption transmission applications.

Chapter 5

A Color Image Encryption Scheme Based on Compound Chaotic Map

Image encryption has emerged as a promising and fascinating subject for researchers in the modern technology era. Using chaotic maps, this chapter gives a diffusion-based picture encryption technique. A chaotic map (2.10) is first used to create an S-box, and then it is utilised to modify the pixel values to create element of non-linearity.

With the aid of the S-box for image data, non-linearity and diffusion are generated, and the pre-encrypted image is given more randomness with the help of the Boolean operation XOR. Then a compound chaotic system (2.13) is used as pseudo random number generator to produce three chaotic sequences that are used to encrypt each component of color image individually. The encryption process based on compound chaotic system mainly used Boolean function XOR to mix the chaotic random sequence, substituted pixel value and preceding pixel value.

Image components are also mixed with each other to distribute the generated randomness uniformly. The use of compound chaotic system in this encryption technique provides good performance for the encryption of color images. It is a different approach that successfully addresses security concerns with the use of chaotic maps in combination with S-box and Boolean operator XOR.

In 2020 [156] proposed an image encryption technique that uses bit wise permutation of pixels and S-box for diffusion purpose. Recently [157] introduced a grey and color medical image encryption technique. In this scheme authors first split image into blocks then perform zig zag permutation, rotation and random permutation then XOR is used for diffusion purpose. In [7] chaos based permutation technique is used then S-box is used for diffusion further diffusion is added in by using XOR with chaos based sequence and recursion. The current research research replaces permutation with inversible self mixing operation. Then S-box is applied and XOR operation is performed for further diffusion effects. Also a compound chaotic map is used that has better chaotic properties and gives large key space then above discussed used schemes.

In this chapter, Section 5.1 is concerned with the S-box and its generation technique. Remaining part of the chapter is arranged as: In Section 5.2 a proposed image encryption and image decryption algorithm is discussed. Section 5.3 has results and discussions with the help of examples and figures. Section 5.4 consists of security analysis taken with the help of key space analysis, distribution of pixels in original and cipher images, correlation analysis, information entropy mean squared error, peak signal to noise ratio, complexity analysis and the speed analysis of proposed algorithm. Section 5.5 gives the comparison with other such schemes. Section 5.6 is the conclusion of above discussed work.

Key management

The proposed cryptosystem is hybrid in nature, it uses a symmetric and asymmetric scheme for the security of images. For this purpose initial secret key is developed by using the plain image. SHA 256 is implemented on the image that gives 256 bits output.

$$H(I) = b_{255}\, b_{254} \dots\, b_0 \tag{5.1}$$

This hash value will be used in the generation of secret keys. The output H_i is split into 8 bit blocks h_i as follows:

$$H_i = h_1 | h_2 | h_3 | \dots | h_{32}. \tag{5.2}$$

The initial states of used chaotic maps are derived from the above blocks as:

$$x_0' = 0.\ (h_{50} \times 2^{51} + h_{49} \times 2^{50} + \dots + h_1 \times 2^0). \tag{5.3}$$

$$x_0 = 0.\ (h_{100} \times 2^{51} + h_{99} \times 2^{50} + \dots + h_{51} \times 2^0). \tag{5.4}$$

$$y_0 = 0.\ (h_{150} \times 2^{51} + h_{149} \times 2^{50} + \dots + h_{101} \times 2^0). \tag{5.5}$$

$$z_0 = 0.\ (h_{200} \times 2^{51} + h_{199} \times 2^{50} + \dots + h_{151} \times 2^0). \tag{5.6}$$

While the control parameters m, μ_1, μ_2, μ_3 are formed as:

$$\begin{gathered} m' = 0.(b_{19} \times 2^{19} + \dots b_1 \times 2^1 + b_0 \times 2^0) \\ m = \begin{cases} m' & m' < 0.5 \\ \\ 1 - m' & m' \geq 0.5 \end{cases} \end{gathered} \tag{5.7}$$

$$\mu_1 = (b_{23} \times 2^3 + \dots + b_{20} \times 2^0).\ (b_{43} \times 2^{19} + \dots + b_{24} \times 2^0) \bmod 9 \tag{5.8}$$

$$\mu_2 = (b_{47} \times 2^3 + \dots + b_{44} \times 2^0).\ (b_{67} \times 2^{19} + \dots + b_{48} \times 2^0) \bmod 9 \tag{5.9}$$

$$\mu_3 = (b_{71} \times 2^3 + \dots + b_{68} \times 2^0).\ (b_{91} \times 2^{19} + \dots + b_{72} \times 2^0) \bmod 9 \tag{5.10}$$

The secret random numbers T_0, M_0 and N_0 used in encryption are generted as:

$$T_0 = (b_{108} \times 2^{19} + \dots b_{90} \times 2^1 + b_{89} \times 2^0) \bmod 256 \tag{5.11}$$

$$M_0 = (b_{128} \times 2^{19} + \dots b_{110} \times 2^1 + b_{109} \times 2^0) \bmod 256 \tag{5.12}$$

$$N_0 = (b_{148} \times 2^{19} + \dots b_{130} \times 2^1 + b_{129} \times 2^0) \bmod 256 \tag{5.13}$$

The SHA 256 value of plainimage is encrypted by RSA encryption algorithm.

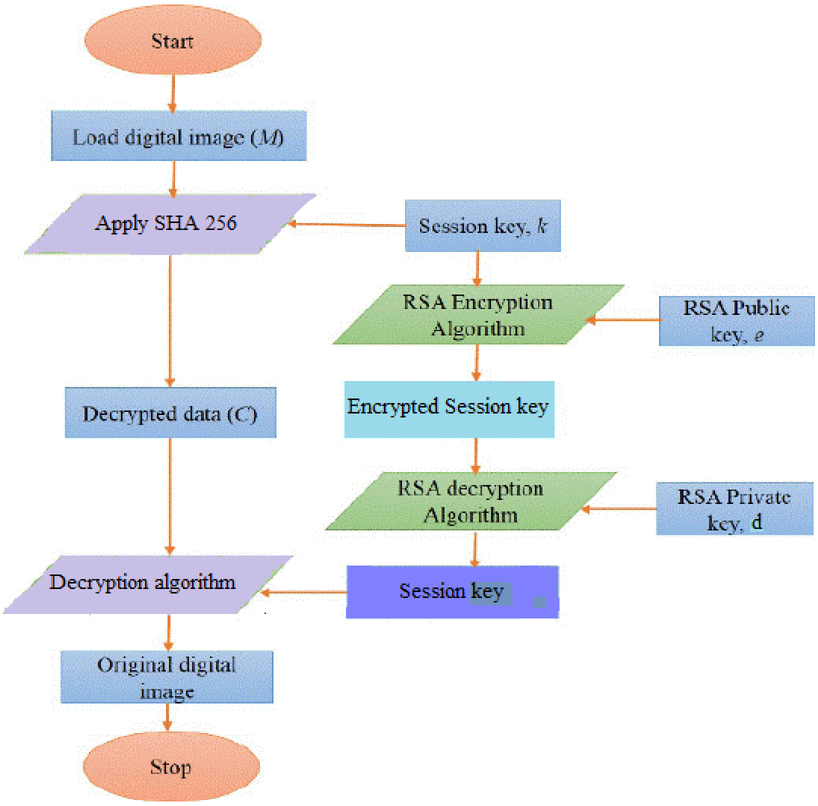


FIGURE 5.1: Flow diagram of the proposed cryptosystem

The asymmetric encryption technique is adopted for the secure transmission of key. The receiver's public key is used to encrypt the hash value in Equation (5.1). The receiver only uses his private key for the decryption of the master key.

$$K_f = H_m^e \mod (r).$$

Here H_m is the master key, K_f is its related encrypted key and (e, r) is the public key of receiver. For the decryption receiver uses his private key (d, r) in the following relation to get the master key as:

$$H_m = K_f^d \mod (r).$$

After receiving H the receiver uses Equations 5.2-5.13 to form the subkeys and then use them in decryption algorithm to get the secret image.

5.1 S-boxes in Cryptography

Substitution boxes, in short, S-boxes are considered as the main component in many conventional algorithms of cryptography like DES [153], AES [154] etc. The design of S-box is based on Shannon's theory of confusion and diffusion [133]. S-boxes can also be used efficiently as look-up table for substitution in encryption and decryption processes [171]. The objective of such substitution boxes is to establish the element of non-linearity in the encrypted data and also to induce confusion and diffusion [133] in cipher. Use of S-box gives high resistance for linear and differential cryptanalysis. Cryptographically strong S-boxes play vital role in the design of a secure cryptosystem. They increase security level against known attacks. Many researchers have proposed different methods [158], [172] to generate strong S-boxes. Chaotic maps, due to its properties as ergodicity, sensitive to initial condition, randomness and ability to generate again with a key are potential platform for the generation of a strong S-box. In this section an algorithm for generating S-box using chaotic map (2.10) is presented. The following shows the proposed algorithm:

Algorithm 5.1.1. (Algorithm for S-box generation using chaotic map (2.10))
Input: Chaotic map (2.10), x'_0, m.
Output: S-box.

1. Divide the interval $[0.1, 0.9]$ into 256 sub-intervals each of fixed length $\triangle h$, *i.e.*, $\triangle h = (0.9 - 0.1)/256 = 0.003125$.

2. Classify each sub-interval as $L_0,\ L_1, ..., L_{255}$.

3. Take an initial condition x'_0 for (2.10) and a value $m \in (0, 0.5)$ to create a sequence x'_n of the values lying in [0.1, 0.9].

4. Start a void array S.

5. Whenever an output value x'_n lies in a particular interval $L_i\,(i = 0, 1, ..., 255)$, give that sub-interval index i to S. Leave those values which do not belong to any sub-interval or giving repeated sub-interval index value.

6. Stop iterating chaotic map (2.10) when it traverses all the sub-intervals L_0 to L_{255}.

7. Return the elements of array as S in the range of 0 to 255, containing 256 distinct integers.

Note that in Step 3, a slightly different value of x'_0 will provide a totally different S-box. Thus, it is possible to create many S-boxes using the above stated Algorithm (5.1.1).

One such S-box is generated by setting parameter $x'_0 = 0.76$ and with fixed value of $m = 0.15$ in (2.10). Table 5.1 displays the resulting S-box.

TABLE 5.1: S-box

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

The properties of this S-box are tested using SET (S-box Evaluation Tool) [159]. It is observed that S-box is fairly balanced and holds reasonably strong cryptographic characteristics.

Table 5.2: Comparison of properties of S-box

S-box	**Non-linearity**			SAC			**BIC**	**BIC-**
	Min	**Avg.**	Max	**Min**	**Avg.**	**Max**	**nonlineaity**	**SAC**
APA S-box [160]	112	112	112	4140	0.4987	0.6015	112	0.499
AES S-box [161]	112	112	112	0.3671	0.5058	0.5975	112	0.504
Gray S-box [162]	112	112	112	0.3906	0.5058	0.5781	112	0.502
Skipjack S-box [163]	104	105.7	108	0.3750	0.4980	0.6093	104.1	0.499
Residue Prime [164]	94	99.5	104	0.4062	0.5012	0.5937	101.7	0.502
Xyi S-box [165]	104	105	106	0.4218	0.5048	0.5937	103.7	0.503
Prop. S-box	98	102	106	0.4063	0.4993	0.5938	103.07	0.502

5.2 Proposed Algorithm

In this section, a new image encryption algorithm for encrypting a digital image of size I is presented. In the proposed algorithm an S-box generated by PWLCM is used as lookup table for pixel substitution. Then three random sequences are generated and bitwise XOR is performed with substituted pixel values of each image component. The algorithm is based mainly on two external secret keys k_1, k_2 containing the parameters of both PWLCM (2.10) and chaotic tent logistic map (2.13), that is $k_1 = (m,\ x_0')$, where $m \in (0, 0.5)$, $x_0' \in [0, 1)$ and $k_2 = (\mu_1,\ \mu_2,\ \mu_3,\ x_0,\ y_0,\ z_0)$, where $\mu_1,\ \mu_2,\ \mu_3 \in (0,\ 4)$ and $x_0,\ y_0,\ z_0 \in (0,\ 1)$. The parameters of both PWLCM (2.10) and tent logistic map (2.13) are kept secret.

Algorithm 5.2.1. (Image encryption algorithm)

Input: Image I, Secret keys $(k_1,\ k_2)$, Algorithm (5.1.1), chaotic map (2.10), chaotic map (2.13).

Output: Encrypted image C.

1. Read the given secret image I.

2. Convert the color (RGB) image I into its primary color components *i.e.,* Red, Green and Blue components.

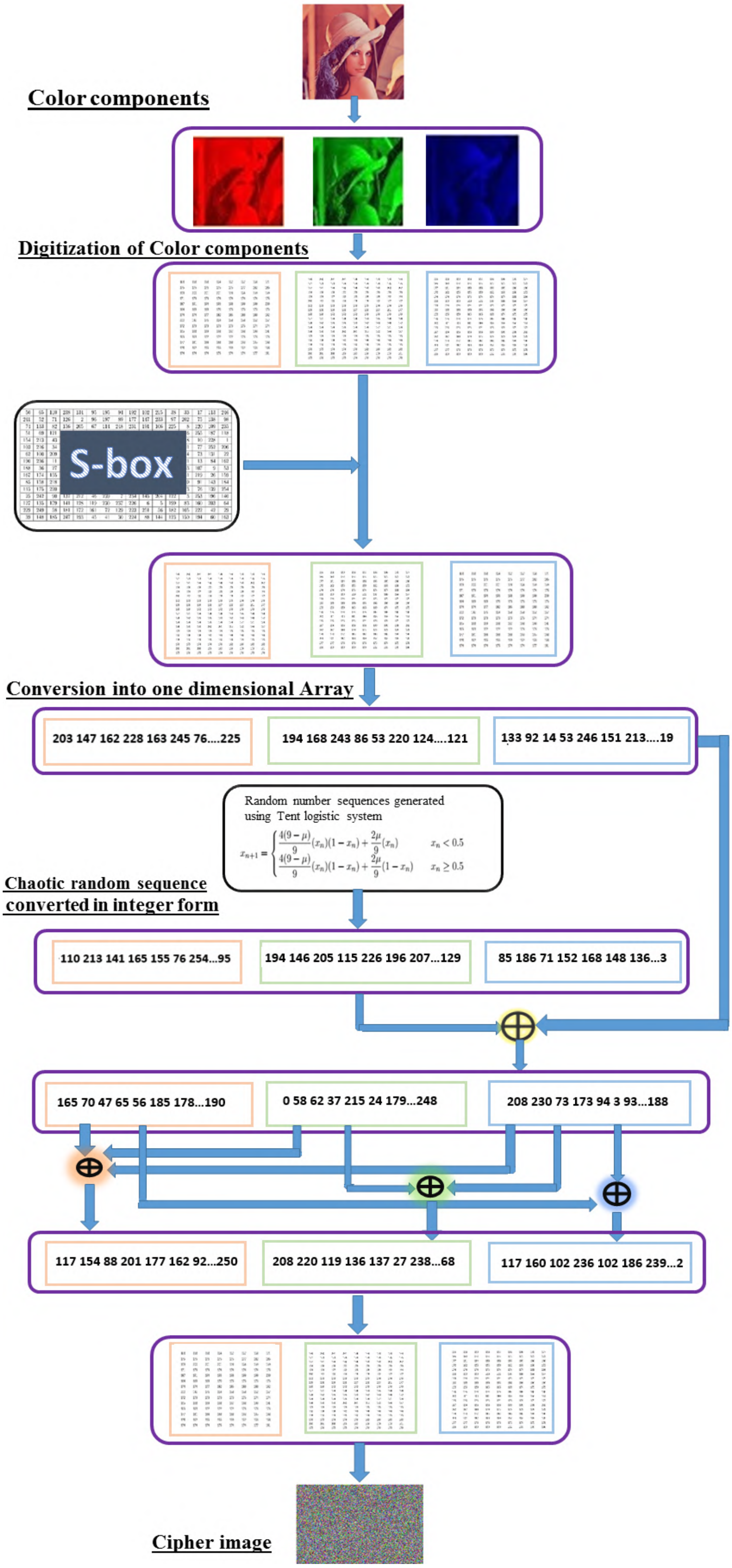


Figure 5.2: Flow diagram of the proposed image encryption scheme

3. Input m and x'_0 from secret key k_1 in Algorithm (5.1.1) to generate an S-box, S.

4. Use S as lookup table, for the color components of I obtained in Step 1. That is, replace each entry $m \in I$ by $\mathrm{S}(m)$, $p_i \leftarrow \mathrm{S}(m_i)$ to get $\mathrm{P} = \{p_1,\ p_2, ..., p_N\}$.

5. Change the substituted color components into 1 dimensional array of numbers.

6. Iterate the tent logistic map for initial state $x_0,\ y_0,\ z_0$ and control parameter $\mu_1,\ \mu_2,\ \mu_3$ for L times.

7. Discard first n_0 values to eliminate the harmful effects of transient process, hence the remaining values are L^* *i.e.*, $L^* = L - n_0$.

8. Convert the obtained sequence to 8-bit integer values using the relation

$$\begin{aligned} x_i &= \mathrm{mod}(\mathrm{floor}(x_i \times 10^{14}), 256), \quad i = 1, 2, ..., L^*,\\ y_i &= \mathrm{mod}(\mathrm{floor}(y_i \times 10^{14}), 256), \quad i = 1, 2, ..., L^*,\\ z_i &= \mathrm{mod}(\mathrm{floor}(z_i \times 10^{14}), 256), \quad i = 1, 2, ..., L^*, \end{aligned}$$

   where mod gives back the remainder after dividing by 256, while the floor(x) gives the largest integer less than or equal to x. Hence the output sequences lie in the range of [0, 255].

9. Pre encrypt each color component separability by using the above generated chaotic sequence as follows:
   The scrambling process of the pre encrypted image's red component:

```
for $i$ = 1, $i$ ++, $i$ = $L^*$ do
    if $i$ = 1, then
        $R'(i) \leftarrow R(i) \oplus X(i) \oplus T_o$
    else
        $R'(i) \leftarrow R'(i-1) \oplus R(i) \oplus X(i)$;
    end
end
```

The green component of pre encrypted image is scrambled as follows:

```
for $i = L^*$, $i$ −−, $i = 1$ do
    if $i = L^*$, then
        $G'(i) \leftarrow G(i) \oplus Y(i) \oplus M_o$
    else
        $G'(i) \leftarrow G'(i+1) \oplus G(i) \oplus Y(i)$;
    end
end
```

The scrambling process of the pre encrypted image's blue component:

```
for $i = 1$, $i$ ++, $i = L^*$ do
    if $i = 1$, then
        $B'(i) \leftarrow B(i) \oplus Z(i) \oplus N_o$
    else
        $B'(i) \leftarrow B'(i-1) \oplus B(i) \oplus Z(i)$;
    end
end
```

10. Mix pre encrypted color components to combine the diffusion effects as follows:

$$R''(i) = R'(i) \oplus G'(i) \oplus B'(i)$$

$$G''(i) = G'(i) \oplus B'(i)$$

$$B''(i) = R'(i) \oplus B'(i)$$

11. Convert R'', G'' and B'' into image form and concatenate these color components, to get ciphered image C.

The ciphered image C can be converted back to its original image by using the following decryption algorithm.

Algorithm 5.2.2. (Image decryption algorithm)

Input: Cipher image C, Secret key $(k_1,\ k_2)$, Algorithm (5.1.1), chaotic map (2.10), chaotic map (2.13).

Output: Original image I.

1. Read the cipher image C.

2. Convert the cipher image into its primary color components *i. e.,* R'', G'', B''.

3. Transform these color components into their digital form and then reshape into one dimensional array form.

4. Re-mix color components as follows to get the pre decrypted image components R', G', B'

$$\begin{aligned} R'(i) &= R''(i) \oplus G''(i) \\ G'(i) &= R''(i) \oplus B''(i) \\ B'(i) &= R''(i) \oplus G''(i) \oplus B''(i) \end{aligned}$$

5. Iterate the tent logistic map for initial states $x_0, y_0,\ z_0$ and control parameters $\mu_1,\ \mu_2,\ \mu_3$ for L times to get three chaotic random sequences.

6. Discard first n_0 values to eliminate the harmful effects of transient process, hence the remaining values are L^* *i.e.*, $L^* = L - n_0$.

7. Convert the obtained sequences to 8-bit integer values using these relations:

$$\begin{aligned} x_i &= \text{mod}(\text{floor}(x_i \times 10^{14}), 256), \quad i = 1, 2, ..., L^*, \\ y_i &= \text{mod}(\text{floor}(y_i \times 10^{14}), 256), \quad i = 1, 2, ..., L^*, \\ z_i &= \text{mod}(\text{floor}(z_i \times 10^{14}), 256), \quad i = 1, 2, ..., L^*, \end{aligned}$$

where mod gives back the remainder after dividing by 256, while the floor(x) gives the largest integer less than or equal to x. Hence the output sequences lie in the range of [0, 255].

8. Perform the initial decryption using chaotic random sequences of Step 7 as follows:
   The unscrambling process of red component of cipher image:

```
for $i$=1, $i$ ++, $i = L^*$ do
    if $i$ = 1, then
        $R'(i) \leftarrow R(i) \oplus X(i) \oplus T_o$
    else
        $R'(i) \leftarrow R'(i-1) \oplus R(i) \oplus X(i)$;
    end
end
```

   The green component of the cipher image is unscrambled as follows:

```
for $i = L^*$, $i$ −−, $i = 1$ do
    if $i = L^*$, then
        $G'(i) \leftarrow G(i) \oplus Y(i) \oplus M_o$
    else
        $G'(i) \leftarrow G'(i+1) \oplus G(i) \oplus Y(i)$;
    end
end
```

   The following shows the unscrambling procedure off the blue component of cipher image:

```
for $i$ = 1, $i$ ++, $i = L^*$ do
    if $i$ = 1, then
        $B'(i) \leftarrow B(i) \oplus Z(i) \oplus N_o$
    else
        $B'(i) \leftarrow B'(i-1) \oplus B(i) \oplus Z(i)$;
    end
end
```

9. Convert the obtained one dimensional sequences into two dimensional array.

10. Input k_1 for m and x'_0 in Algorithm (5.1.1) to generate an S-box and then generate its inverse S-box, S^{-1}.

11. By using inverse S-Box, (S^{-1}) as lookup table for substitute values, obtained after Step 5. That is, $m_i \leftarrow \mathrm{S}^{-1}(p_i)$ to get $\mathrm{I} = \{m_1,\ m_2, ..., m_N\}$.

12. By converting resulting matrix I into image form, original image I is obtained.

The validation of the proposed image encryption scheme is demonstrated by correctly recovering the original image from the encrypted image. The decryption algorithm correctly reverses all the effects performed during encryption and only the intended receiver can successfully recover the original image.

5.3 Results and Discussions

For the demonstration of proposed scheme, Algorithm (5.2.1) and (5.2.2) are applied on two different image files. The MATLAB implementation code is available at https://github.com/tahirsajjad?tab=repositories. The proposed approach is designed for the security of color images but it is also applicable for gray and other images. For this purpose, the length of generated chaotic sequences should be adjusted with image resolution. For gray images the process of invertible self-mixing operation is omitted.

A main problem in chaos based encryption schemes is digital deterioration [122]. When a chaos is simulated on computer then its expected chaotic behavior is negatively effected. Digital chaos implementation results finite numbers either with fixed point arithmetic, floating point arithmetic or some other arithmetic with reasonable word size.

To minimize this problem, while implementing on MATLAB, long format is used that has 64-bit word size for fixed point algorithm [173]. Another format long E provides 64-bit word size for floating. The use of format long E in the proposed approach reduces affects of numerical deterioration problem.

For image encryption we have selected the standard Lena 256 × 256 image. The original Lena image shown in the Figure 5.3 is encrypted by using the proposed Algorithm (5.2.1).

The resulting encrypted image is visible in Figure 5.3 (b). The figure shows that the proposed encryption mechanism completely scramble the original image without leaving any clue to reveal the original information. The decryption is then performed by using the proposed image decryption Algorithm (5.2.1) and displayed in Figure 5.3(c). The decryption result indicates that the proposed scheme effectively works and perfectly recover the original image.

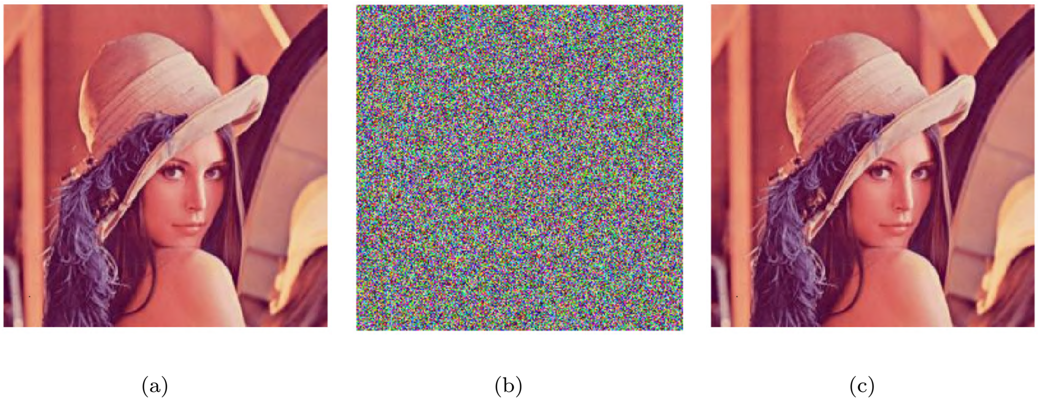

(a) (b) (c)

FIGURE 5.3: Experimental results for the Lena image (a) Original image (b) Encrypted image (c) Decryption

In the next example a Pepper 256 × 256 image is taken. The original image is shown in Figure 5.4 (a), the encryption result is displayed in Figure 5.4 (b). The encryption result signifies that the proposed technique generates a noise like structure that does not disclose any useful information about the original image.

The decryption result using Algorithm (5.2.2) is presented in Figure 5.4 (c). From the decryption result it is evident that the proposed scheme is able to give a flawless recovery.

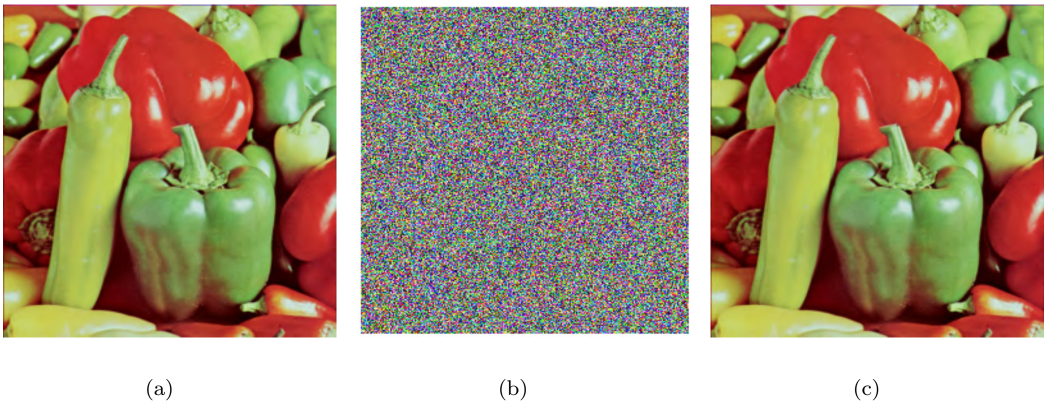


FIGURE 5.4: Experimental results for the Pepper image (a) Original image (b) Encrypted image (c) Decryption

5.4 Security Analysis

This section is devoted to address the security properties of the proposed scheme.

5.4.1 Key Space

Key space in a cryptosystem is considered an essential feature. It should be sufficiently large to withstand against brute force attack. For the designed algorithm, secret key is actually a combination of two secret subkeys k_1, k_2 used in encryption algorithm. These keys have the parameters of used chaotic maps, *i.e.*, $k_1 = (x'_0, m)$ for chaotic map (2.10) and $k_2 = (x_0, \mu_1, y_0, \mu_2, z_0, \mu_3)$ for tent logistic map (2.13). In consonance with IEEE floating point precision [174] the precision of each key should be greater than 10^{-15}. The precision level for chaotic map's parameters is used as 10^{-15}. Hence the keyspace size will be $(10^{15})^8 = 10^{120} \approx 2^{398}$.

This keyspace is large enough to prevent brute force attack. The resulting keyspace is bigger than minimum requirement of key size 2^{100} [135]. A comparison of key space using the proposed technique with some other state of the art schemes is also shown in Table 5.3.

Table 5.3: Key space size comparison

Image encryption schemes	**Key Space**
Cuaric *et al.* [175]	2^{128}
Wang *et al.* [44]	2^{149}
Rehman *et al.* [176]	2^{209}
Guesmi *et al.* [166]	2^{256}
Ali *et al.* [7]	2^{299}
Idress *et al.* [156]	8×2^{252}
Kamal *et al.* [157]	2^{116}
Proposed scheme	2^{398}

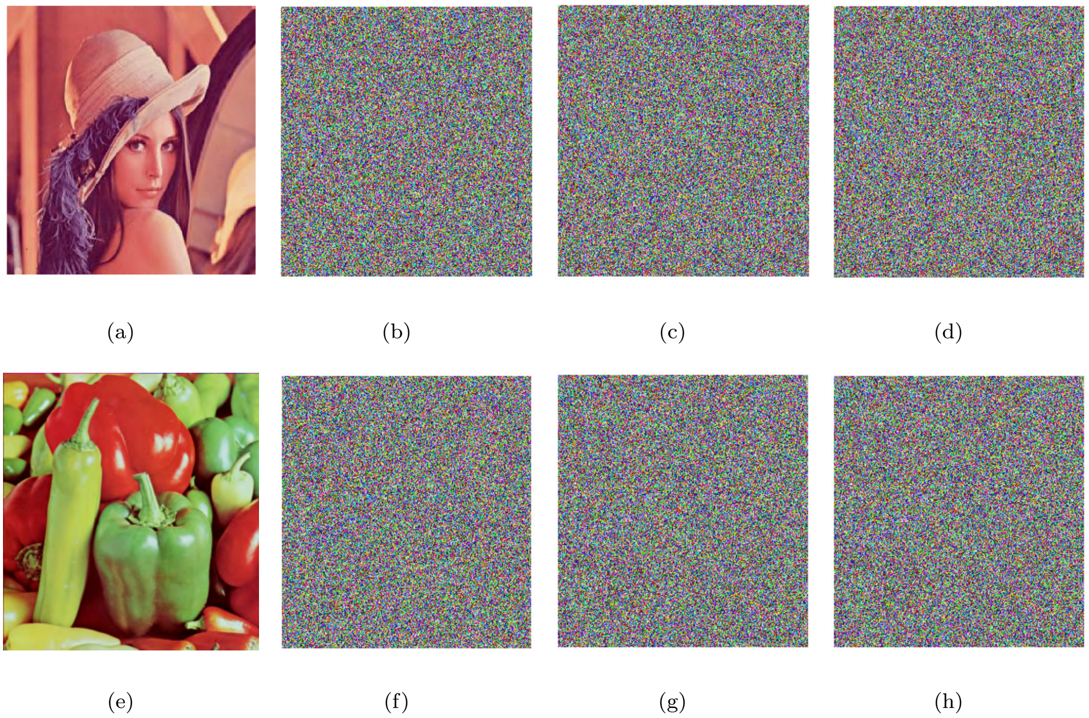
5.4.2 Key Sensitivity

Another concern for any encryption scheme is about its highly sensitive behavior towards the secret keys. For a good encryption system, a single-bit modification in key gives totally changed encrypted result. In this research PWLCM and tent logistic maps are used. For a very insignificant change in key or control parameter, the resulting generated random sequence will completely changed. Which in response gives entirely different encryption/decryption results.

In Figure 5.5 two different trial images Lena and Peppers are employed for key sensitivity analysis. First these images are encrypted by using key components $x_0 = 0.76$ and $m = 0.15$ for PWLCM and $x_0 = 0.479$, $\mu_1 = 4.5$, $y_0 = 0.596$, $\mu_2 = 6.2$, $z_0 = 0.964$, $\mu_3 = 7.9$ for tent logistic map.

Figure 5.5 (c, g) shows the result of using slightly different key than original key, that is x_0 is changed from 0.479 to 0.47900000000000000009. Figure 5.5 (d, h) depicts the difference between the encryption results and modified key based encryption results.

From these results it is evident that the encryption results are significantly changed by taking a minor modification in any of the key component.

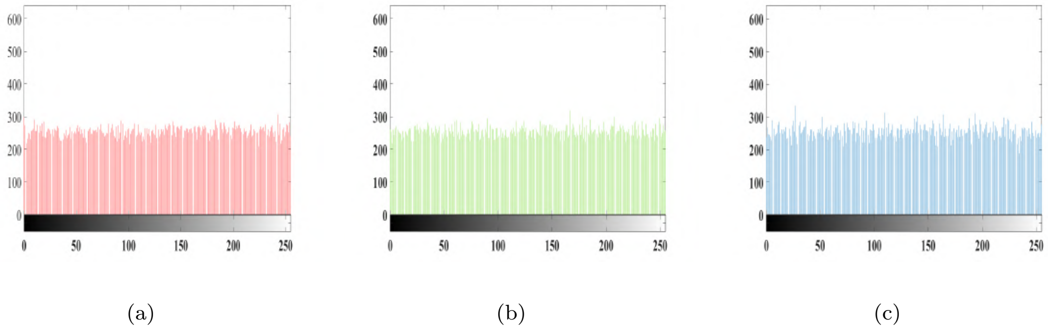

(a) (b) (c) (d)

(e) (f) (g) (h)

FIGURE 5.5: Experimental results of proposed encryption method for the minor modification in the secret key: (a, e) original images of Lena and Peppers (b, f) encrypted images (c, g) encrypted images using slightly modified key (d, h) absolute intensity difference images

5.4.3 Distribution of Pixels in Cipher Image

Image histogram tells about the dissemination of pixels in an image. From the above discussed experiment 1, Lena image, Figure 5.3 (a) is taken as original image, with size (256×256).



(a) (b) (c)

FIGURE 5.6: Histogram of encrypted image (a) red component (b) green component (c) blue component

Histograms of its corresponding ciphered image components are shown in Figure 5.6 (a, b, c). From the histogram it is clear that, there does not exist any information to mount a statistical attack on the cipherimage.

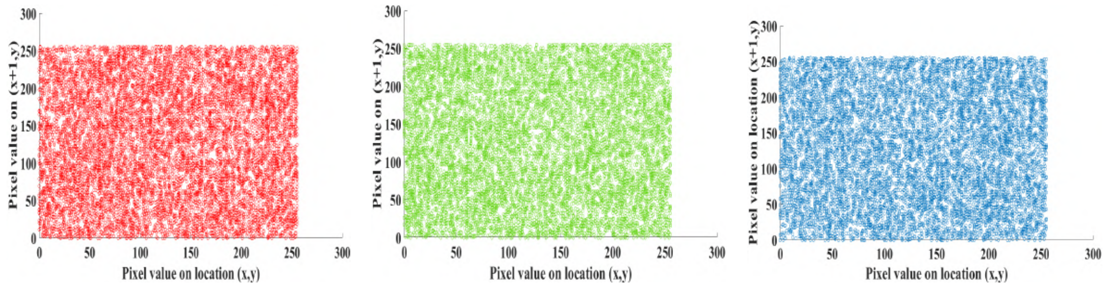
5.4.4 Correlation Analysis

The quantitative analysis for the evaluation of having high confusion and diffusion among neighboring pixels in plainimage and the corresponding cipherimage is evaluated by a test of correlation. The correlation in the adjacent pixels in Lena cipherimage is examined here. Figure 5.7 shows row-wise correlation in components of encrypted Lena image. For its calculation in vertical, horizontal and diagonal in cipherimage, Equation (3.10) has been used.

TABLE 5.4: Correlation Coefficient of two neighboring pixels in the original and cipherimage

Direction	**proposed scheme**	**Wang *et al.* [80]**	**Wang *et al.* [44]**	**Zhang *et al.* [177]**
Horizontal	0.0019	0.0019	0.0037	0.0036
Vertical	0.0035	0.0038	0.0029	0.0023
Diagonal	0.0008	0.0019	0.0047	0.0039

The values in resulting Table 5.4 tells that correlation coefficient of cipher image approaches to zero. Hence neighboring pixels in cipher image are almost uncorrelated.



(a) (b) (c)

FIGURE 5.7: Correlation (row-wise) in the encrypted Lena image (a) red component (b) green component (c) blue component

5.4.5 Information Entropy

This feature of analysis is used to test the randomness in the encrypted image. It also indicates an average amount of information contained in ciphered image.

Table 5.5: Statistical analysis of different encrypted images

Images		**Correlation in the Dir. of plainimage**			**Correlation in the Dir. of cipherimage**			**Entropy**	
		Row	**Diagonal**	**Column**	**Row**	**Diagonal**	**Column**	**Orig.**	**Ciph.**
Moon		0.9390	0.9037	0.9020	0.0003	-0.0001	-0.0057	6.7093	7.9888
Aerial		0.8602	0.8213	0.9050	-0.0023	0.0051	-0.0001	7.3118	7.9894
Airplane		0.9366	0.8927	0.9571	-0.0036	-0.0046	-0.0072	6.4523	7.9893
Clock		0.9741	0.9389	0.9565	-0.0034	0.0038	-0.0023	6.7057	7.9894
Chemical plant		0.8984	0.8529	0.9466	0.0038	0.0003	-0.0004	7.3424	7.9891
Resolution chart		0.8667	0.7562	0.8722	-0.0011	0.0040	-0.0012	1.5483	7.9897
Female	Red	0.9294	0.9129	0.9779	0.0033	0.0032	-0.0009	5.7150	7.9890
	Green	0.9106	0.8941	0.9748	0.0010	0.0037	-0.0066	5.3738	7.9902
	Blue	0.9130	0.8958	0.9726	-0.0035	-0.0100	0.0095	5.7116	7.9451
House	Red	0.9353	0.9126	0.9671	-0.0037	-0.0008	-0.0033	6.4311	7.9900
	Green	0.9474	0.9320	0.9805	-0.0020	-0.0004	0.0007	6.5389	7.9898
	Blue	0.9749	0.9625	0.9820	0.0056	0.0044	0.0044	6.2320	7.9881
Tree	Red	0.9361	0.9159	0.9590	0.0053	0.0062	-0.0009	7.2104	7.9891
	Green	0.9457	0.9318	0.9687	-0.0018	0.0026	0.0006	7.4136	7.9902
	Blue	0.9406	0.9265	0.9612	0.0135	0.0036	0.0013	6.9207	7.9868
Jelly bean	Red	0.9763	0.9537	0.9745	-0.0077	0.0008	0.0028	5.2626	7.9897
	Green	0.9801	0.9603	0.9757	0.0017	-0.0030	-0.0020	5.6947	7.9892
	Blue	0.9880	0.9799	0.9890	-0.0072	-0.0078	-0.0048	6.5464	7.9517
Couple	Red	0.9562	0.9176	0.9493	-0.0038	-0.0007	-0.0066	6.2499	7.9886
	Green	0.9534	0.9002	0.9308	-0.0070	-0.0059	-0.0059	5.9641	7.9896
	Blue	0.9442	0.8890	0.9178	0.0421	0.0062	0.0101	5.9309	7.9533

For the cipher image C the entropy value can be computed with the Formula (3.11). In exact random source emitting 256 symbols, entropy's optimal value is eight. If value of entropy less than 8 in cipherimage then it means that there is a possibility of predictability of plainimage, which is dangerous for security of image encryption algorithm.

Table 5.6: Entropy values comparison

Encryption Schemes	Entropy values
Fu *et al.* [178]	7.988
Wu *et al.* [179]	7.997
Choi *et al.* [180]	7.819
Wu *et al.* [168]	7.991
Proposed scheme	7.995

In the proposed algorithm entropy for cipher image C, is checked. The calculated value of entropy of ciphered image C with comparison to other images is shown in Table 5.6.

The outcome demonstrates that the cipherimage's entropy is close to the optimum entropy value. Therefore the suggested encryption technique has minimum risk of information leaking. Hence it is secure enough.

5.4.6 Sensitivity Analysis of the Proposed Algorithm

NPCR and UACI are used to measure the effects of varying a pixel of the plain-image on the cipherimage. These indicators are calculated by the Formula (3.12).

In this scheme, for Lena 256×256 image the calculated values are 99.62 and 33.46 respectively. The proposed scheme shows high performance for these indicators. Therefore it will provide well resistance against "known plaintext attacks" and "chosen plaintext attacks".

5.4.7 Noise and Data Loss Attacks

A good encryption system also has the property to minimize the noise effects generated due to the pixel discrepancies in the decrypted image. For the capacity evaluation of the proposed method against the resistance of noise and data loss attacks, the color Lena image is used as test case of size 256 × 256. The encrypted test image is noised by adding 1%, 5% and 10% salt and pepper noise as shown in the Figure 5.8.

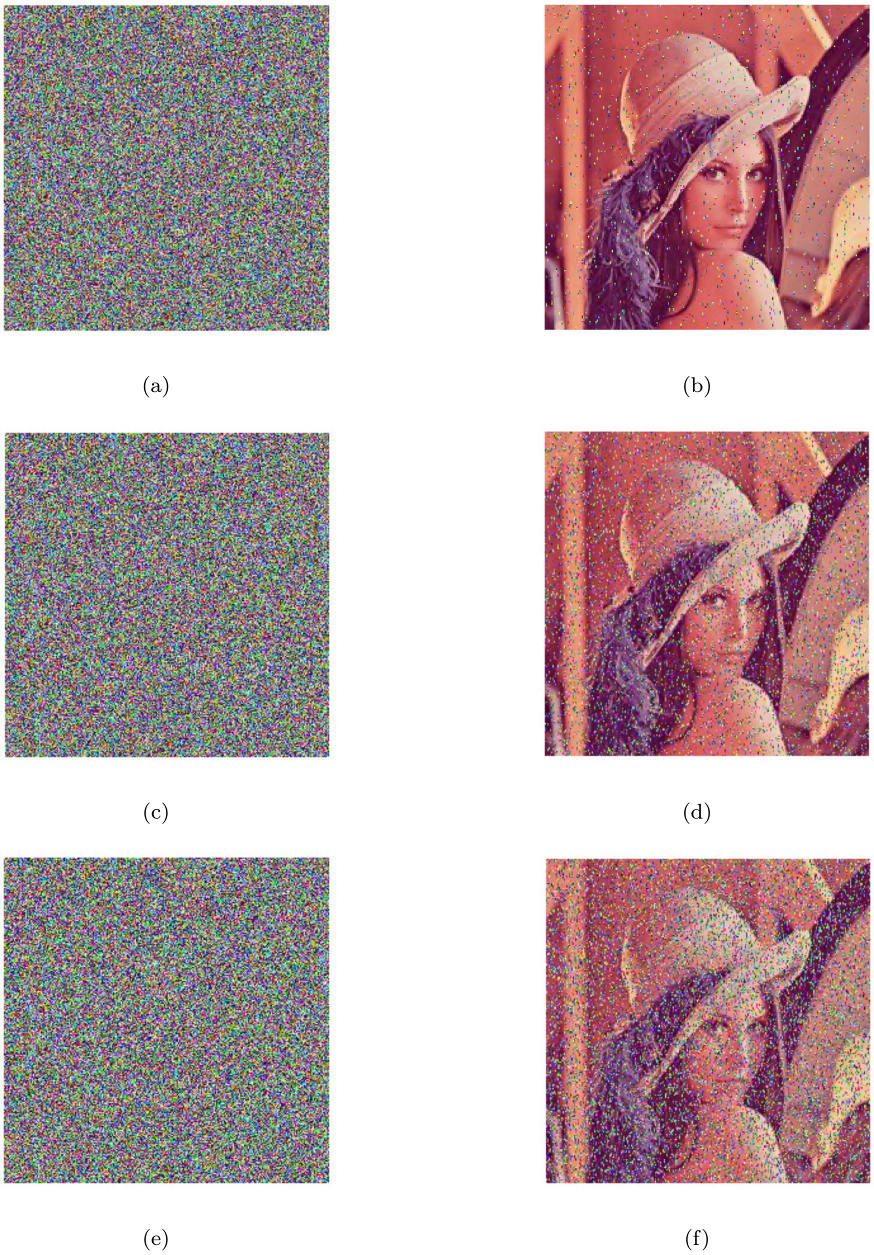


FIGURE 5.8: Experimental results for the performance evaluation of data loss attacks: (a, c, e) cipher images with 1%, 5% and 10% salt and pepper noise, (b, d, f) decryption results of corresponding images using our scheme.

It is obvious from the figure that when the encrypted image encounter the salt and pepper noise, the decryption results retains a significant majority of original information and also contains a small portion of evenly distributed noise. The quantitative analysis for the difference between the plain image I_P and the decrypted image I_D is carried out by using peak signal to noise ratio (PSNR). While the mean square error (MSE) is used to measure the cumulative squared error between the original image and the decrypted image.

For the calculation of PSNR and MSE of MN sized image, Equations (3.13) and (3.14) are used. The smaller MSE value calculated from Equation (3.13) indicates the minimal error in the decryption results. Whereas the higher PNSR value obtained from Equation (3.14) reveals the higher decrypted image fidelity against its original plain image.

TABLE 5.7: Performance of MSE and PSNR about salt and pepper noise

Salt & pepper noise	**1%**	**5%**	**10%**
MSE	392.49	1845.3	3357.43
PSNR	22.2370	15.5095	12.9098

The calculated values of PSNR for these modified cipher images by $1\%, 5\%$ and 10% salt and pepper noise are shown in Table 5.7. The findings show that the encryption strategy provides reasonable efficiency for data loss and noise attacks.

5.4.8 Complexity Analysis

There is a strong relationship between the complexity in the chaotic system and the robustness of the cryptosystem based on that chaotic system. In this encryption scheme, two chaotic maps are used, the piecewise linear chaotic map (2.10) and tent logistic map (2.13). The chaotic map (2.10) is used to generate a random sequence of length MN, where as chaotic map (2.13) gives 3 random sequences, floor function is used to convert these values into integer form. The XOR function is used to generate randomness in the image and also to accumulate the generated randomness in different components of image. Thus the calculated complexity value for used chaotic maps and applied operations, is $10(MN)+3MN\log_2(MN)$. The high complexity of the proposed scheme ensures good quality encryption results.

5.4.9 Encryption/Decryption Time

For any algorithm, security considerations are important but a good encryption algorithm should also robust and efficient. The running speed of encryption algorithm is an important aspect. Using the proposed algorithm, the encryption/decryption time of Lena image is measured. The time analysis is done on CORE i3-3110M, 2.40GHz CPU with 4GB RAM notebook running on Windows 8, 64 bit operating system using Matlab R2013a (8.1.0.604). The average time taken for encryption/decryption of proposed algorithm for Lena image of size 256 × 256 is 0.277 second.

5.5 Comparison

A deep and detailed overall comparison of the proposed scheme with other image encryption schemes is given below.

Table 5.8: Properties comparison of cipher generated by taking Lena as test image

Algorithms	**NPCR**	**UACI**	**Correlation**	**Keyspace**	**Entropy**
Proposed scheme	99.62	33.46	0.002066	10^{120}	7.995
Ali et al. [7]	99.6094	33.4635	0.0020	10^{90}	7.998
Kanwal et al. [39]	99.61	33.46	0.002977	10^{84}	7.999
Chai et al. [181]	99.63	–	0.0037	10^{51}	7.998
Wu et al. [168]	100	33.47	0.00603	10^{112}	7.991
Wang et al. [44]	99.5956	33.5512	0.0038	10^{56}	7.997

The comparison presented in Table 5.8 shows that the proposed scheme has better results for correlation analysis and key space while the performance against entropy analysis, NPCR and UACI is also comparable with many other state of the art encryption techniques.

5.6 Conclusion

An alternative method of image encryption is presented in this chapter. This algorithm firstly takes PWLCM to produce an S-box. The role of this S-box in the encryption is for the substitution of image pixel values. This substitution can be observed after S-box substitution. The tent logistic system is used as PRNG for the generation of random chaotic sequence. Then a mixing technique employed for the mixing of this generated sequence with substituted image pixels values and their preceding values. Finally XOR is used to generate uniformly random pixel values distributed components for stable noise like effects in the cipherimage.

This technique has provided resistance to different types of cryptographic attacks. The security analysis of proposed scheme is performed by using statistical and differential analysis. On the basis of this analysis, it is found that the proposed scheme is safe and operable in applications for transmission of images in real time.

Chapter 6

A Novel Medical Image Signcryption Scheme

Images based on patient-diagnostic tests and their reports are securely broadcast in telemedicine, so that recipients can get them without any error. For this, an authenticated and unforgeable cryptosystem is required for the secure communication of sensitive medical data. This chapter proposes a new signcryption technique for medical images that uses a tent logistic tent system (TLTS) (2.14) and a Henon chaotic map (2.12) to meet the security needs of sensitive medical data during transmission.

A hybrid cryptography technique is used for the development of a the medical image signcryption scheme. To generate secret encryption key, public key cryptography (PKC) using elliptic curves is employed. The proposed technique utilizes chaotic maps for the encryption of these images and elliptic curve cryptography for their signcryption. It provides a combined mechanism for the chaotic image encryption technique, key exchange and digital signature.

For pixel scrambling, the image encryption step includes permutation and diffusion. The cryptographic properties like authentication, non-repudiation, confidentiality, forward secrecy, integrity and unforgability are provided through the suggested image signcryption mechanism. The application of a symmetric image encryption technique based on chaos yields good results for statistical and differential analysis. The suggested signcryption technique is strong and offers good security for sensitive medical images, according to the findings of above mentioned analyses.

In this chapter, the introduction of proposed signcryption scheme, its global parameter setting and the key generation process, detailed image signcryption algorithm, decryption algorithm and correctness of the proposed algorithm is given in Section 6.1. Results and discussion with the help of examples and figures, are discussed in the Section 6.2. The complete security analysis of image encryption, signcryption attributes their comparison and possible attack model are discussed in Section 6.3. Finally the work is concluded in Section 6.4.

6.1 The Proposed Signcryption Scheme

In this scheme, the patient/user uses the public key of health-care center to generate common secret encryption key 'K'. Then the patient (sender) encrypts the desired medical image/report by using secret key 'K' in the proposed chaos-based medical image encryption scheme,

The patient/user signs the cipher image 'C' and send it along with the digital signature 's' and authentication parameter 'G'' to the health care center. Figure 6.1 shows the proposed signcryption model, while Figure 6.2 and Figure 6.3 are the block diagrams of the proposed signcryption and unsigncryption schemes.

At the receiver's end, the signature 's', the center's private key 's_b', the public key of sender P_a and authentication parameter 'G'' are used to generate common secret key K. Following that, the image is recovered by symmetric decryption using that key, also verified by using G' and accepted, if it is authenticated.

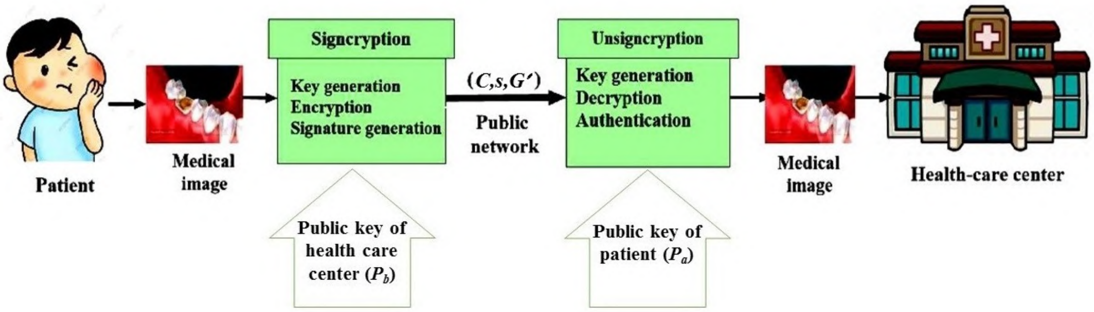


FIGURE 6.1: Proposed signcryption model

6.1.1 Global Parameters

In this phase following parameters are selected and published:

p: A large prime number, where $p > 2^{256}$.

$E(a,b)$: The used elliptic curve over finite field $\mathbb{F}_p$,

$$y^2 = x^3 + ax + b \bmod p.$$

Here a and b are two integers that are smaller than p and satisfy

$$4a^3 + 27b^2 \neq 0 \qquad \bmod p.$$

G: The base point of elliptic curve $E(a,b)$ with order n.

O: The point of $E(a,b)$ at infinity.

n: The order of G, *i.e.*, $n\,G = \mathcal{O}$.

H: A one-way hash function.

6.1.2 Key Generation

Patient selects a random integer $s_a < n$ as private key and generates public key $P_a = s_aG$. Similarly health-care center chooses a random integer $s_b < n$ as private key and gets the public key $P_b = s_bG$. These public keys will be used at both the sender and the receiver ends to generate a common secret key K.

6.1.3 Signcryption Phase

For sending a medical image to health-care center, the patient uses symmetric chaos-based image encryption scheme to generate cipher image. To signcrypt the medical image, following steps will be performed:

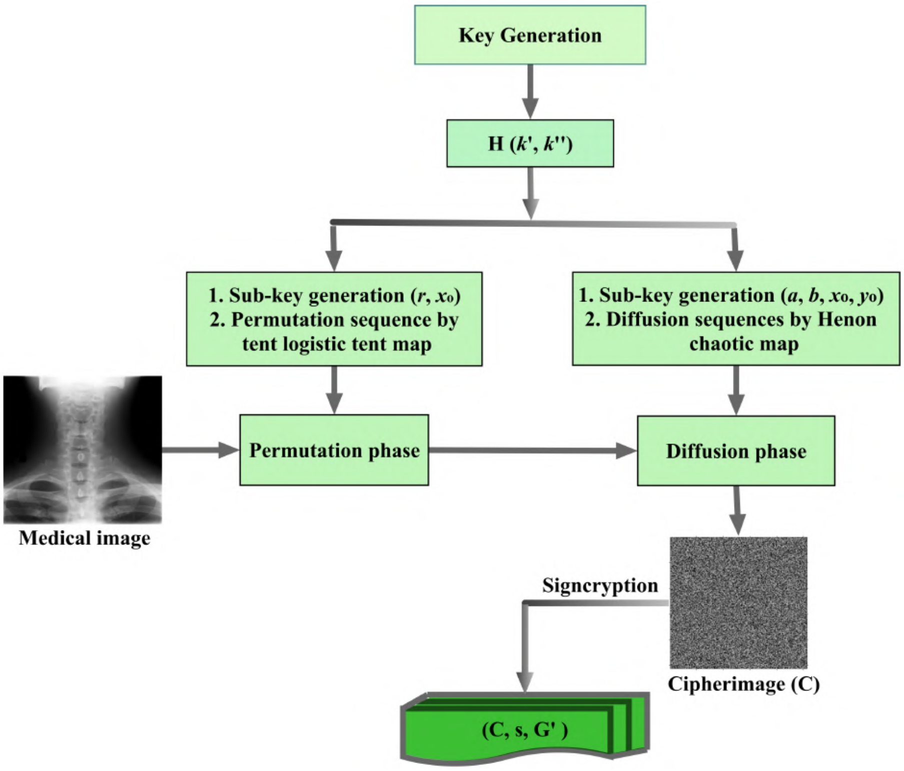

Key Generation
H (k', k'')
1. Sub-key generation (r, x₀)
2. Permutation sequence by tent logistic tent map
1. Sub-key generation (a, b, x₀, y₀)
2. Diffusion sequences by Henon chaotic map
Medical image
Permutation phase
Diffusion phase
Signcryption
Cipherimage (C)
(C, s, G')

FIGURE 6.2: Block diagram of the proposed medical image signcryption scheme

6.1.4 The Proposed Image Signcryption Algorithm

In this section an image signcryption algorithm is presented. It takes the medical image/report I of patient, public key of receiver P_b and returns the encrypted image C, digital signature s and authentication parameter G' that will be sent through the public network to the health care center. The detailed working process of the algorithm is given below:

Algorithm 6.1.1. (Image Signcryption Algorithm)

Input: Image I, Hash function (SHA-256), public key of receiver P_b , chaotic map (2.12) and chaotic map (2.14).

Output: Encrypted image C, signature s, authentication key G'.

1. Select a random integer $k \in \mathbb{F}_p$, multiply it with health-care authority's public key P_b to generate the secret key as,

$$K = kP_b = (k', k'').$$

2. Apply the hash function H (using SHA-256) on the components of secret key $K = (k', k'')$, as:

$$H(k') = b'_{255},\ b'_{254},\ \dots, b'_1,\ b'_0,$$
$$H(k'') = b''_{255},\ b''_{254},\ \dots, b''_1,\ b''_0,$$

where $b'_i,\ b''_i \in [0,1]$ for $i \in 0, 1, \dots, 255$ are used to get the parameters of the chaotic maps (2.12) and (2.14) as stated below:

(a) Compute the parameters $r \in (0,4)$ and $x_0 \in (0,1)$ of the chaotic map (2.14) from the two halves of 256-bits of $H(k')$ as follows:

$$r = (b'_{255} \times 2^1 + b'_{254} \times 2^0).\ (b'_{253} \times 2^{125} + \dots\ +\ b'_{128} \times 2^0),$$

similarly compute $x_0 \in (0,1)$ as:

$$x_0 = 0.\ (b'_{127} \times 2^{128} + b'_{126} \times 2^{127} + \dots + b'_0 \times 2^0).$$

(b) Generate the initial values, control parameters of Henon chaotic map (2.12) and the subkeys $M_0,\ N_0$ (for encryption of the first pixel and the last pixel of pre-encrypted image D respectively). Use the output of $H(k'')$ to get the values of $a \in (0.54, 2),\ b,\ x'_0,\ y_0 \in (0,1)$ and $M_0,\ N_0 \in [0, 255]$ as follows:

$$a' = (b''_{239} \times 2^1 +\ b''_{238} \times 2^0).\ (b''_{237} \times 2^{45} + \dots + b''_{192} \times 2^0),$$

$$a = \begin{cases} 2 - a' & \text{if} \quad 0 \le a' < 0.54 \\ a' & \text{if} \quad 0.54 \le a' < 2 \end{cases}$$

$$b = 0.(b''_{191} \times 2^{47} + b''_{126} \times 2^{46} + \cdots + b''_{144} \times 2^{0}),$$

$$x'_0 = 0.(b''_{143} \times 2^{47} + b''_{142} \times 2^{46} + \cdots + b''_{96} \times 2^{0}),$$

$$y_0 = 0.(b''_{95} \times 2^{47} + b''_{94} \times 2^{46} + \cdots + b''_{48} \times 2^{0}),$$

$$M_0 = b''_{47} \times 2^{7} + b''_{46} \times 2^{6} + ... + b''_{40} \times 2^{0},$$

$$N_0 = b''_{39} \times 2^{7} + b''_{38} \times 2^{6} + ... + b''_{31} \times 2^{0}.$$

Encryption Process

3. Convert the image I in digital form as the matrix D' of order $M \times N$, where M and N are the dimensions of the image.

4. Rewrite the matrix D' as one dimensional array,

$$Z = \{z_1, z_2, \ldots, z_{MN}\}.$$

5. Iterate the chaotic map (2.14) using the parameters from Step 2 (a) to obtain the sequence:

$$A = \{a_i\}_{i=1}^{MN},$$

and sort sequence A in ascending order to form,

$$B = \{b_i\}_{i=1}^{MN}.$$

6. Using the relationship of the sequences A and B,

$$b_i = a_{t_i}, \text{ for } i = 1,\ 2, \ldots, MN,$$

compute permutation vector,

$$T = \{t_1, t_2, \ldots, t_{MN}\}.$$

7. Use T to permute the position of elements of the array Z. After applying permutation on Z it becomes,

$$D = \{g_1, g_2, ..., g_{MN}\},$$

convert D into two dimensional array of order $M \times N$.

8. Use parameters generated from $H(k'')$ in Step 2(b) for Henon chaotic map (2.12) to generate two random sequences,

$$X = \{x_k\}_{k=1}^{MN} \text{ and } Y = \{y_k\}_{k=1}^{MN}$$

9. Convert the real number sequences x_k and y_k where $k = 1, 2, ..., MN$ into integer sequences using these relations:

$$x_k = \text{int}(254 \times (x_k - \min(x_k))/d) + 1,$$

where $d = \max(x_k) - \min(x_k)$.

$$y_k = \text{int}(254 \times (y_k - \min(y_k))/d) + 1,$$

where $d = \max(y_k) - \min(y_k)$.

10. Express $\{x_k\}$ and $\{y_k\}$ as two dimensional arrays of order MN.

11. Mix these two dimensional arrays with permuted image D (obtained from Step 7). This process will be done in two steps to get encrypted image C:

    - For the generation of diffusion effects in 'D', start from the first value and XOR it with its corresponding value of X and M_o, then other values of first column will be altered by using XOR with the corresponding X values and preceding values. After this the same process will be used with next columns to get C' as:

```
for $r$ = 1 : $M$ do
    for $c$ = 1 : $N$ do
        if $r$ = 1, $c$ = 1 then
            $C'(r, c) \leftarrow D(r, c) \oplus X(r, c) \oplus M_o$
        else
            if $r \geq 2$ and $c = 1$ then
                $C'(r, c) \leftarrow X(r, c) \oplus C'(r-1, 1) \oplus D(r,c)$;
            else
                $C'(r, c) \leftarrow X(r, c) \oplus C'(r, c-1) \oplus D(r, c)$;
            end
        end
    end
end
```

- For the generation of further diffusion effects in 'C'', start from the last value and XOR it with its corresponding value of Y and N_o, then other values of row will be altered by using XOR with the corresponding Y values and preceding values. After this the same process will be used for all other rows while going backward to get C as:

```
for $c$ = $N$, $N$−−,$c$ = 1 do
    for $r$ = $M$, $M$−−, $r$ = 1 do
        if $r$ = $M$, $c$ = $N$ then
            $C(r, c) \leftarrow C'(r, c) \oplus Y(r, c) \oplus N_o$
        else
            if $r = M$ and $c < N$ then
                $C(r, c) \leftarrow C'(r, c) \oplus C(r, c+1) \oplus Y(r, c)$;
            else
                $C(r, c) \leftarrow C'(r, c) \oplus C(r+1, c) \oplus Y(r, c)$;
            end
        end
    end
end
```

Signature Generation :

12. Compute h by applying hash function H on I, C and K. That is:

$$h = H(I, C, K).$$

13. Also find digital signature s as:

$$s = \frac{k}{h + s_a} \quad \text{mod } p.$$

14. Calculate authentication parameter G' as:

$$G' = hG.$$

15. Send (C, s, G') to the health-care authority.

6.1.5 Image Unsigncryption Phase

The health-care authority receives cipher image C, digital signature s and verification parameter G'. Then it uses the following steps to get plain image I with its authentication.

Algorithm 6.1.2. (Image Unsigncryption Algorithm)

Input: Encrypted image C, Hash function (SHA-256), signature s, authentication parameter G', public key of sender P_a, chaotic map (2.12), chaotic map (2.14).

Output: Original image I.

1. Solve

$$s_b\, s\, G' + s_b\, s\, P_a = K,$$

to generate the secret key K.

2. Use hash function H to get sub-keys as described in Step (2) of above signcryption algorithm.

Decryption Method:

3. Generate $\{x_k\}$ and $\{y_k\}$, two dimensional arrays of order $M \times N$ by following the Step (8) and Step (9) of above used signcryption algorithm.
4. To eliminate diffusion effects, apply Step (10) of the above mentioned scheme, by replacing G with C to obtain permuted array G.
5. Perform Step (5, 6) of the signcryption phase to get permutation vector T, also calculate inverse permutation vector i.e., T^{-1}.
6. Apply T^{-1} on D to get original medical image I.
7. Take the hash value of plain image I, cipher image C and secret key K to find h as:
$$h = H(I,\ C,\ K).$$
8. Calculate another authentication parameter A' as:
$$A' = h\,G.$$

Authentication:

9. The received image is accepted, if the calculated value of A' and received G' are same, that is, accept the image if *i.e.*,
$$A' = G'.$$

The above described unsigncryption algorithm first generates the key then by using it decrypt the cipher image to get the original plain image and finally authenticate it for its originality. The image decryption process correctly reverses all the effects performed during encryption and only the health care center can successfully recover the original image by using the generated key K.

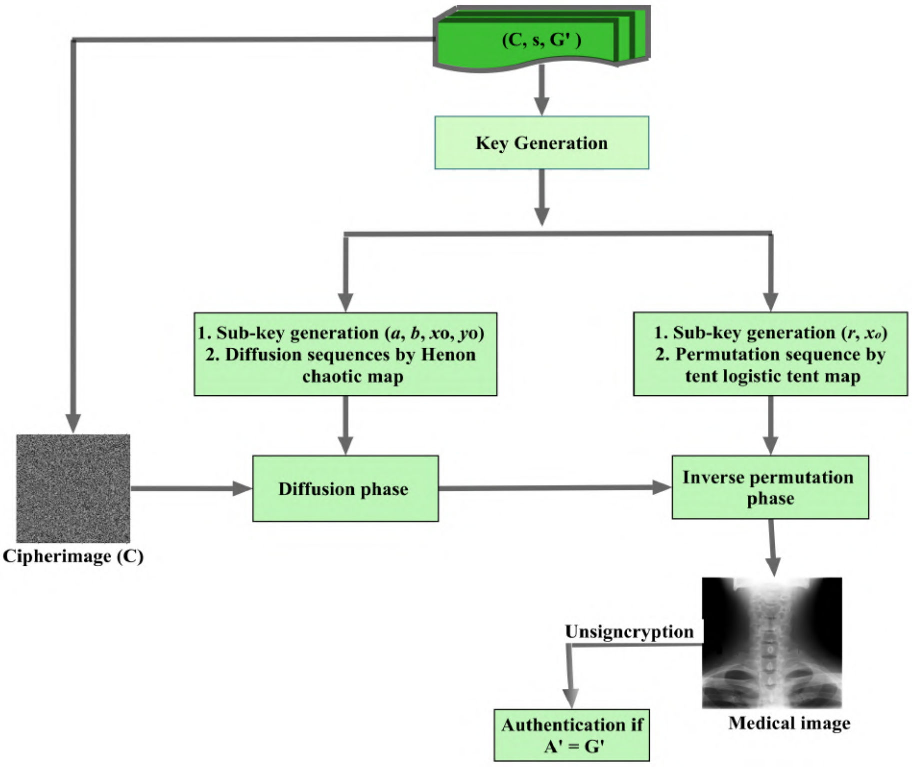

(C, s, G')
Key Generation
1. Sub-key generation (a, b, xo, yo)
2. Diffusion sequences by Henon chaotic map
1. Sub-key generation (r, xo)
2. Permutation sequence by tent logistic tent map
Cipherimage (C)
Diffusion phase
Inverse permutation phase
Unsigncryption
Medical image
Authentication if A' = G'

FIGURE 6.3: Block diagram of the proposed medical image unsigncryption scheme

6.1.6 Correctness

The health-care center receives $(C,\ s,\ G')$ from patient. It calculates key by using its private key s_b, patient's public key P_a, received digital signature s and authentication parameter G'.

$$s_b\ s\ \ G' + s_b\ \ s\ P_a = s_b \frac{k}{h + s_a}\ \ h\ G + s_b \frac{k}{h + s_a} s_a\ G \quad \mod p$$

$$= \frac{s_b\ k\ h\ G}{h + s_a} + \frac{s_b\ k\ G\ s_a}{h + s_a} \quad \mod p$$

$$= \frac{(s_b\ k\ G)(h + s_a)}{h + s_a} \quad \mod p$$

$$= (s_b\ k\ G) \qquad \mod p$$

$$= k\ P_b = K$$

6.1.7 Summary of Proposed Scheme

A brief summary of the whole process is given in Table 6.1. It shows the working of signcryption algorithm that uses public key of receiver to generate secret key that is used for encryption then a digital signature along with authentication parameter is generated and sent to the health care center where the unsigncryption algorithm used them to recover the key and use it to decrypt the cipher image and finally authenticate the information.

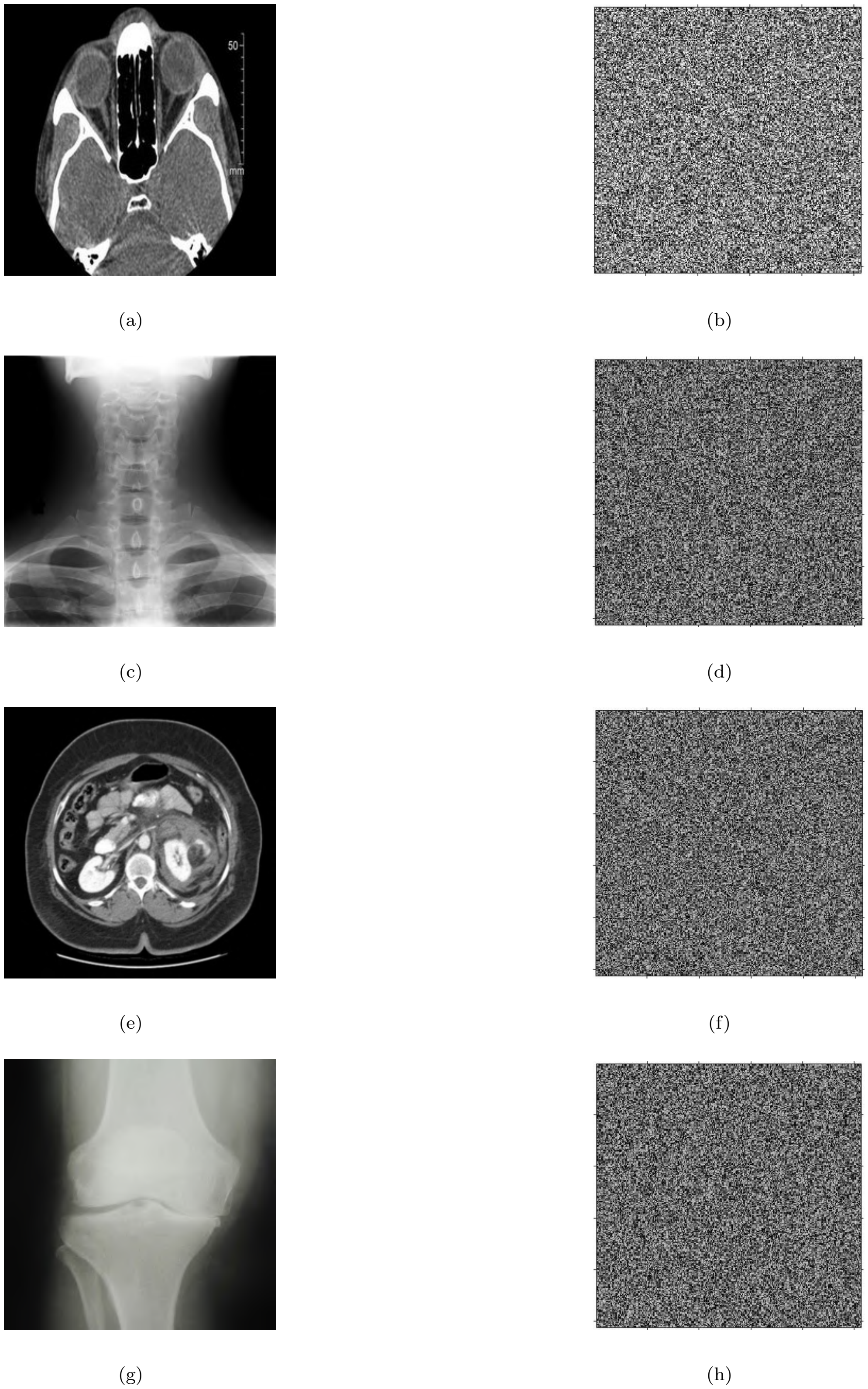
Table 6.1: Summary of proposed image signcryption scheme

Signcryption	**Unsigncryption**
1. Select a random integer $k \in \mathbb{F}_p$ and compute $K = kP_b = (k', k'')$.	1. Receive (C, s, G') from the sender.
2. Encrypt the medical image I to obtain the cipher image C as: $C = \mathrm{E}_{H(K)}(I)$.	2. Use s, G' to compute the shared key K, $K = s_b s G' + s_b s P_a$.
3. Use the hash function H to generate the signature $s = \frac{k}{h + s_a} \bmod p$, where $h = H(I, C, K)$.	3. Decrypt the cipher image C to get the medical image I as: $I = \mathrm{D}_{H(K)}(C)$.
4. From the above values of h compute also $G' = hG$.	4. Use the hash function H to compute, $h = H(I, C, K)$ and calculate $A' = hG$.
5. Send (C, s, G') to authority.	5. Accept the medical image if $A' = G'$.

6.2 Results and Discussions

For the performance evaluation, it is applied on four different medical images (*i.e.*, CT Paranasal, Cervical X-Ray, CT Abdomem, Knee X-Ray). These test images are taken from open-access medical image repositories/Ayland.org [182] image database. All the related experiments and simulations are taken on a laptop CORE i7-3520M, 2.90GHz CPU with 8GB RAM running on Windows 8, 64 bit operating system using environment of MATLAB R2013a (8.1.0.604). The MATLAB implementation code is available at https://github.com/tahirsajjad?tab=repositories.

The encryption results of these four images are shown in Figure 6.4. The proposed method can be used for different types/sizes of medical images. Further analysis for the evaluation are given in the next section.



(a) (b)

(c) (d)

(e) (f)

(g) (h)

Figure 6.4: (a, b) CT Paranasal and its cipher image, (c, d) Pair of Cervical X-Ray image with the corresponding cipher image, (e, f) CT Abdomem image with the corresponding cipher image, (g, h) Knee X-Ray image with its corresponding cipher image

6.3 Analysis of the Proposed Scheme

In this section, firstly, the security features of chaos-based encryption are addressed, then signcryption attributes and possible attacks on the proposed scheme are discussed.

6.3.1 Security Features of Chaos-based Encryption

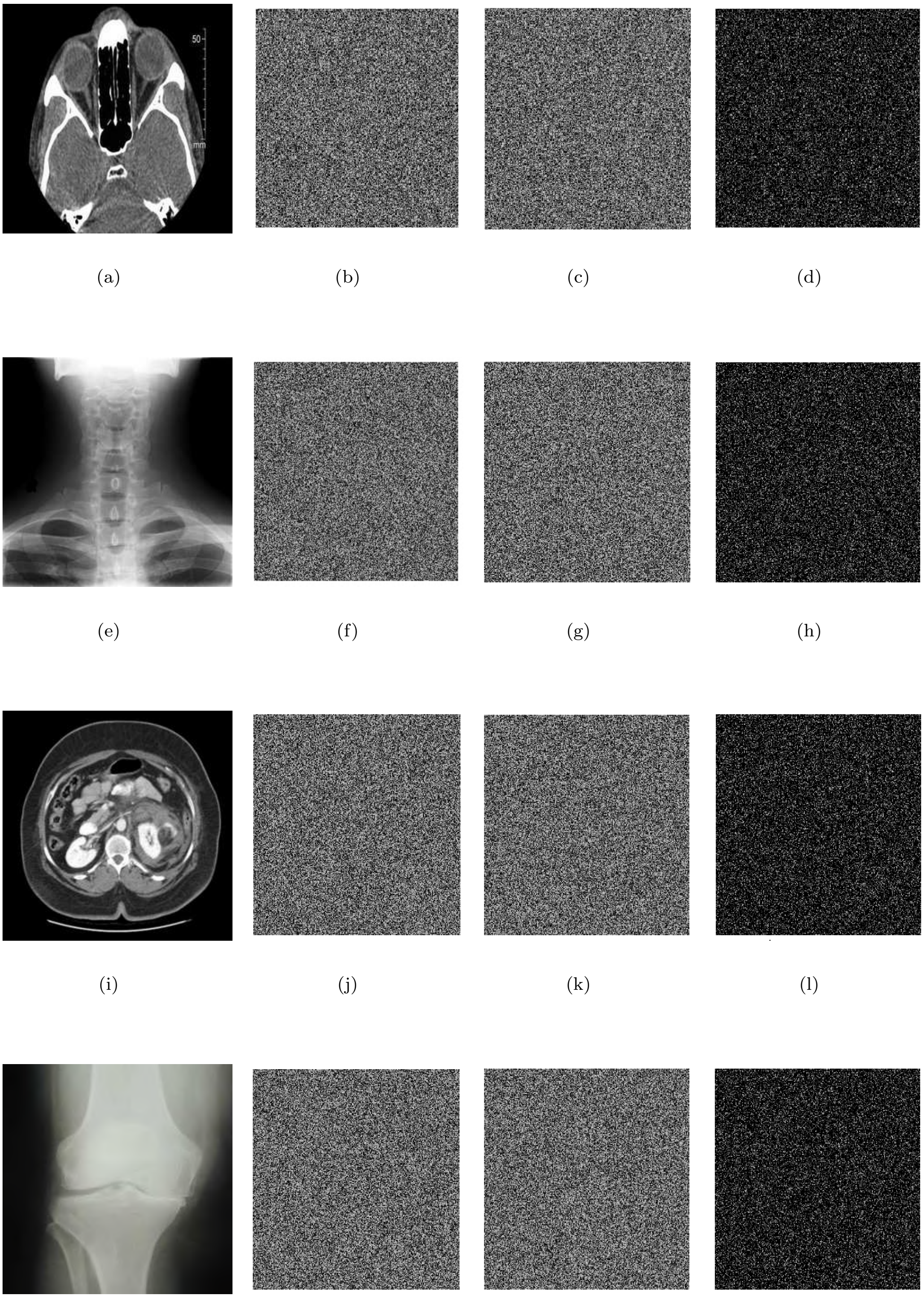
In the proposed scheme a novel chaos-based encryption mechanism is adopted for secure transmission of medical image. Figure 6.4 shows the encryption results of various medical images. Performance evaluation tests like key space, key sensitivity, ability of resisting against differential attacks, histogram analysis, correlation analysis and information entropy are also employed in this section.

6.3.1.1 Key Space Analysis

Analysis of key space is a crucial feature in any cryptosystem. It produces the ability to resist against brute force attacks. In this encryption model, two chaotic maps are used. For tent-logistic-tent map (2.14) control parameter r and initial state x_0 are used. Another chaotic map used in proposed encryption scheme is Henon map (2.12).

It uses a and b as control parameters and two state variables x'_0 and y_0. M_0 is the key used for encryption of first pixel. According to IEEE floating format precision [174] each key component should be greater than 10^{-15}. If the precision of these parameters is taken as 10^{-15}, the key space size will be $(10^{15})^6 = 10^{90} \approx 2^{299}$. Alvarez *et al.* [135] identified that the adequate key space for image encryption scheme should be larger than 2^{100} to oppose brute force attacks.

The key space of this scheme is sufficiently large to fend off brute force attack. In order to decrypt the medical image correctly, the adversary has to guess all these six components.



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

(e) (f) (g) (h)

(i) (j) (k) (l)

(m) (n) (o) (p)

FIGURE 6.5: Experimental encryption results with a small change in secret key component, (a, e, i, m) original images, (b, f, j, n) cipher images I_c, (c, g, k, o) encrypted images by slightly changed key I'_c, (d, h, l, p) absolute intensity difference images $|\mathrm{I}_c - \mathrm{I}'_c|$.

6.3.1.2 Key Sensitivity Analysis

For secret keys, an encryption system should be sensitive. In this scheme, tent logistic tent map (2.14) has key components $a = 1.4$, $b = 0.3$, $x'_0 = 0.7666$ and $y_0 = 0.3$, while Henon map (2.12) takes $r = 3.78$ and $x_0 = 0.5748$.

For testing the key sensitivity, four medical images are used in Figure 6.5 of size 256 × 256 as a test case, and modify only one key component *i.e.* x'_0 from 0.7666 to 0.7666000000000001. Figure 6.5 shows the experimental results of key sensitivity for encryption process using slightly changed key. From here it is evident that the outcomes of the encryption are completely different. Similar results can be seen by making a small change in any other component of used secret key. Hence the obtained results show that this scheme is sensitive for secret keys.

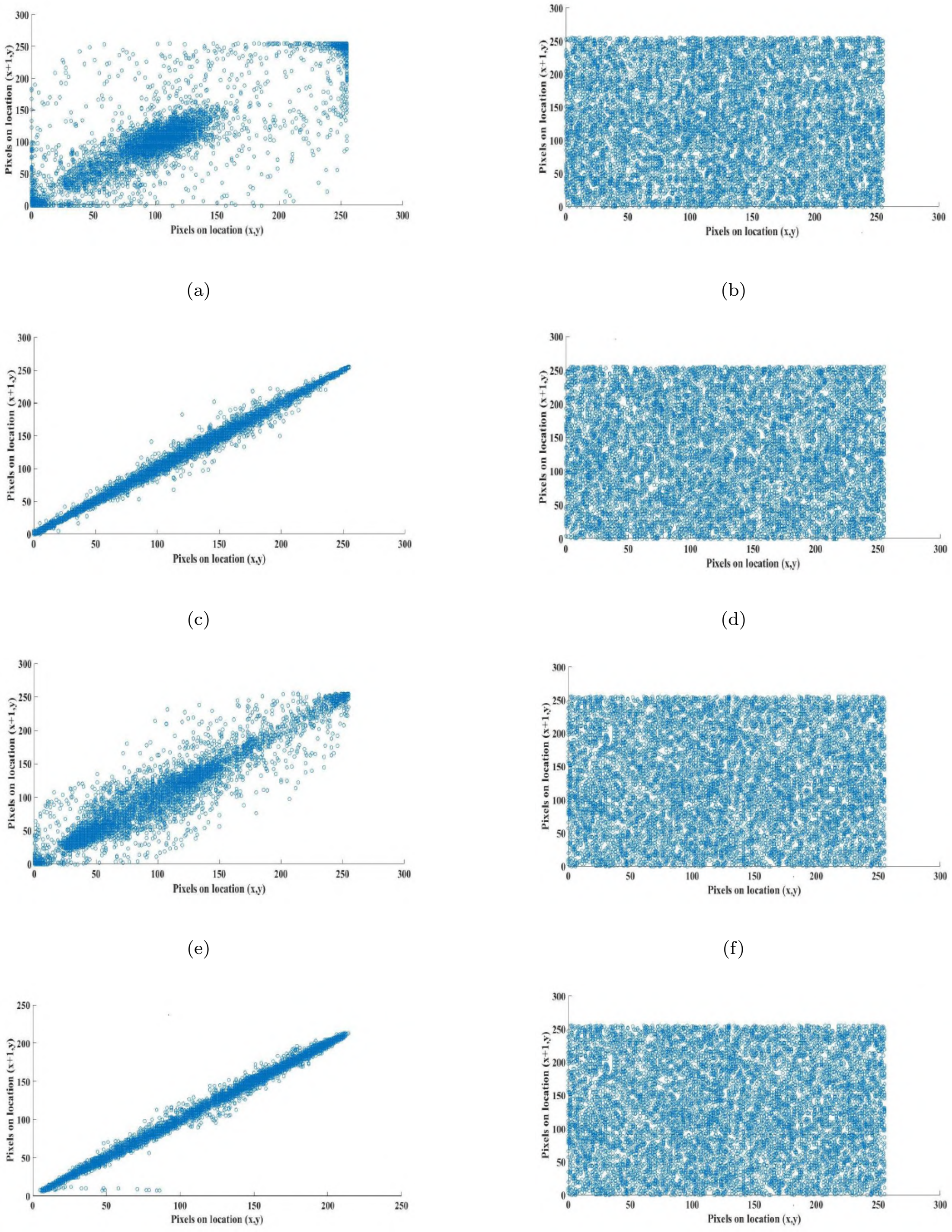
6.3.1.3 Correlation Analysis

A test of correlation between adjacent pixels in the plainimage and their matching encrypted image is used to determine whether there is confusion or diffusion. For the calculation of correlation coefficients in horizontal, vertical and diagonal directions, Equation (3.10) has been used.

The correlation in the adjacent pixels of the plainimage and cipherimage is also analyzed in Figure 6.6. From the results of Table 6.2 and Figure 6.6, it is seen that cipher image has very low correlation among neighboring pixels.

Table 6.2: Correlation coefficient of two neighboring pixels in Plain and Cipherimage

Figure 6.4	**CT Paranasal**		**Cervical X-Ray**		**CT Abdomen**		**Knee X-Ray**	
Direction	**Orig.**	**Ciph.**	**Orig.**	**Ciph.**	**Orig.**	**Ciph.**	**Orig.**	**Ciph.**
Horizontal	0.9776	0.0359	0.9960	0.0299	0.9580	0.0126	0.9994	0.0920
Vertical	0.9432	0.0025	0.9979	0.0043	0.9710	0.0030	0.9989	0.0045
Diagonal	0.9310	0.0037	0.9942	-0.0043	0.9311	0.0011	0.9986	0.0027



(a)

(b)

(c)

(d)

(e)

(f)

(g)

(h)

FIGURE 6.6: Correlation among neighboring pixels in (a, b) CT Paranasal with its corresponding cipherimage, (c, d) Cervical X-Ray with its corresponding cipherimage (e, f) CT Abdomen with its corresponding cipherimage (g, h) Knee X-Ray with its corresponding cipherimage.

6.3.1.4 Histogram Analysis

It tells about the dispersion of pixels. The uniform dispersion can be observed by analyzing the shape of histogram, generated by plotting the pixels of image. Figure 6.7 depicts the histograms of the original images and their corresponding encrypted images. From histogram analysis it is clear that, there does not exist any clue to mount a statistical attack on the encrypted image.

However the histogram visual effects are not sufficient to validate the randomness of pixel value in cipher image. Therefore the histogram is also evaluated quantitatively by using chi-square (χ^2) test. Chi-square (6.1) can be defined as:

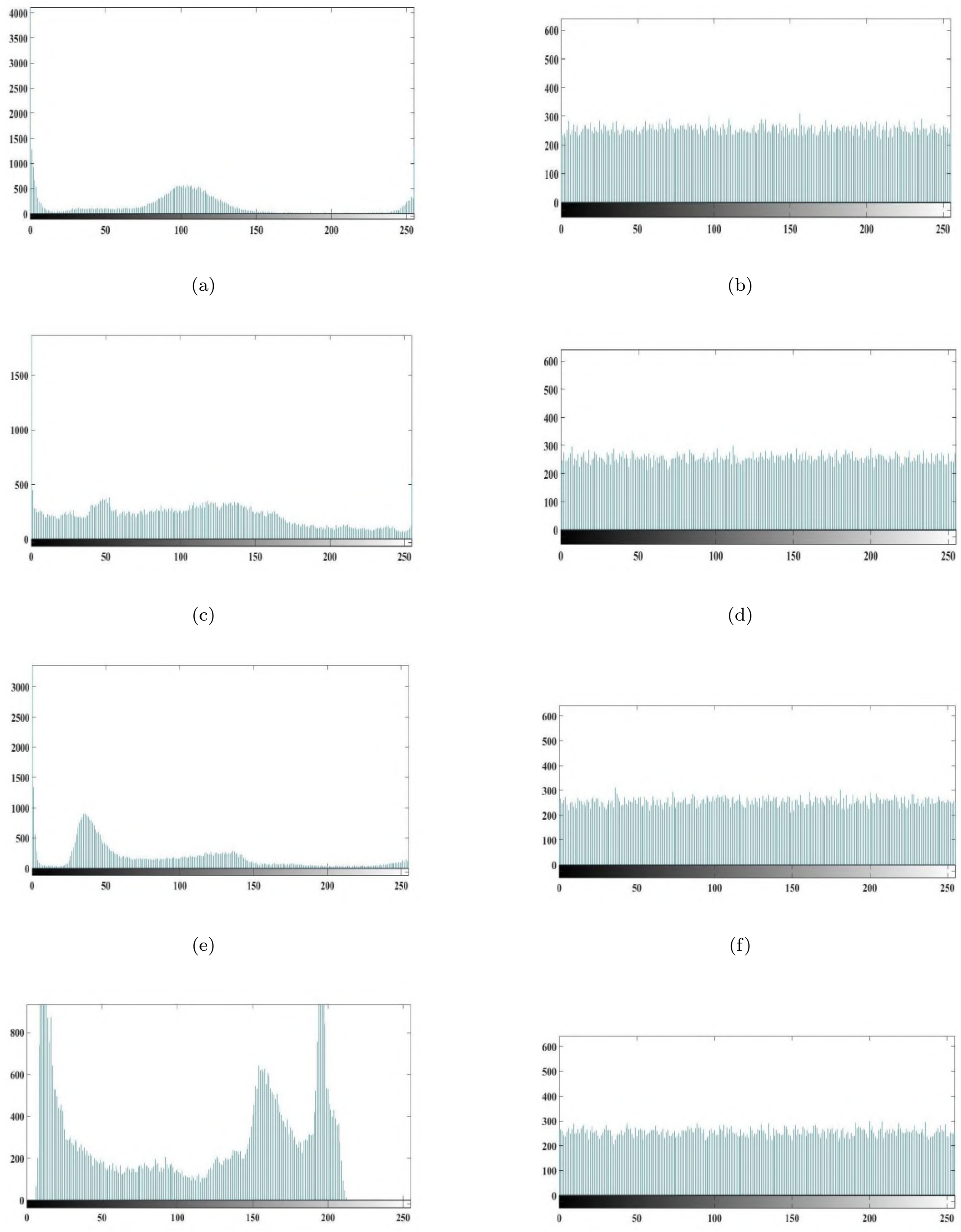
$$\chi^2_{\text{exp}} = \sum_{i=1}^{S} \frac{(o_i - e_i)^2}{e_i}, \tag{6.1}$$

$$e_i = \frac{\mathrm{M} \times \mathrm{N}}{S} \tag{6.2}$$

where S indicates grayscale ($S = 256$ in this case), o_i represents the frequency of occurrence of each level observed on the histogram of cipherimage, e_i is the expected frequency of occurance, based on uniform distribution of occurrence and M × N is the total length of image sequence in Equation (6.2).

Table 6.3: Results of chi-square test for cipherimage

			Chi-square test scores		
Figure 6.7	**Image type**	**Image size**	**Theoretical value**	**Proposed scheme**	**Results**
CT Paranasal	Gray	256 × 256	293	257	Pass
Cervical X-Ray	Gray	256 × 256	293	268	Pass
CT Abdomen	Gray	256 × 256	293	214	Pass
Knee X-Ray	Gray	256 × 256	293	244	Pass



(a) (b)

(c) (d)

(e) (f)

(g) (h)

FIGURE 6.7: Histogram of (a, b) CT Paranasal image with its corresponding cipherimage, (c, d) Cervical X-Ray image with its corresponding cipherimage, (e, f) CT Abdomen image with its corresponding cipherimage, (g, h) Knee X-Ray image with its corresponding cipherimage

It is expected that The experimental chi-square value is less than its theoretical value (293 with significance level 0.05). Table 6.3 indicates the output of chi-square test and pass rate. The chi-square test is passed by all the test images. It is therefore clear that the redundancy of plainimage is fully concealed, which demonstrates the inability of stability of statistical attacks.

6.3.1.5 Entropy Analysis

This feature of analysis measures the randomness in a cipherimage. It also tells us the average amount of information carried by cipher image. Let g be a cipher image then entropy value of g can be calculated by the Formula (3.11).

Table 6.4: Entropy values comparison

Image #	Figure 6.4	Image size	Entropy values	
			Orig. image	Encrypted image
1	CT Paranasal	256×256	5.2795	7.9975
2	Cervical X-Ray	256×256	7.1655	7.9973
3	CT Abdomen	256×256	5.8963	7.9970
4	Knee X-Ray	256×256	7.3071	7.9969

For exact random source having 256 different symbols, $E(g)$ has an optimum value of 8 for entropy. If the calculated value of entropy is significantly less than the ideal value of entropy in cipherimage then it means that there is a possibility of predictability of plainimage. In this scheme entropy values for cipherimage g, is checked. The calculated values of entropy for the plainimages and their corresponding cipherimages are shown in Table 6.4.

In the example of proposed scheme, the entropy value of cipherimages with 2^N as 255, turn out to be ≈ 8. Hence it is assumed that proposed scheme is robust having minimum information dissipation.

6.3.1.6 Local Shannon Entropy

It is used to measure the randomness of a cipherimage. Higher entropy values generally indicate a stronger encryption result.

Table 6.5: Comparison with theoretical mean and standard deviation of LSE scores

Sr. #	**Figure 6.4**	**Type**	**Block** size(T_B)	**LSE of cipher**	**Random Grayscale values** $\mu_{\overline{H_{(k,T_B)}}(R)}$	$\sigma_{\overline{H_{(k,T_B)}}(R)}$
1	CT Paranasal	Gray	16×16	7.1756	7.174966353	$0.052437999/\sqrt{k}$
		Gray	32×32	7.8121	7.808756571	$0.017246343/\sqrt{k}$
		Gray	64×64	7.9542	7.954588734	$0.004024888/\sqrt{k}$
2	Cervical X-Ray	Gray	16×16	7.1741	7.174966353	$0.052437999/\sqrt{k}$
		Gray	32×32	7.8081	7.808756571	$0.017246343/\sqrt{k}$
		Gray	64×64	7.9543	7.954588734	$0.004024888/\sqrt{k}$
3	CT Abdomen	Gray	16×16	7.1698	7.174966353	$0.052437999/\sqrt{k}$
		Gray	32×32	7.8090	7.808756571	$0.017246343/\sqrt{k}$
		Gray	64×64	7.9546	7.954588734	$0.004024888/\sqrt{k}$
4	Knee X-Ray	Gray	16×16	7.1828	7.174966353	$0.052437999/\sqrt{k}$
		Gray	32×32	7.8084	7.808756571	$0.017246343/\sqrt{k}$
		Gray	64×64	7.9559	7.954588734	$0.004024888/\sqrt{k}$

The values obtained from the GSE (global Shannon entropy) test sometimes does not represent the true randomness [183] in an image.

Local Shannon entropy is capable of capturing the randomness in local image block that could not be accurately reflected in GSE score. Also GSE is also considered incompatible for images of different sizes, thus inappropriate for universal measure.

Local Shannon entropy tests the randomness of an image with the same parameters irrespective to the size of test image and offer relatively fair random comparison between multiple images. The local Shannon entropy can be measured by following these steps: (1) Take S_k, non overlapping image blocks containing T_B pixels each.

(2) Find the entropy value H(S_k) of each image block S_k. (3) Find the average of all the calculated entropy values H(S_k).

Table 6.6: Local Shannon entropy values of 8-bit gray medical images with k = 30 and T_B = 1936 and their comparison with significance level 0.05 and 0.01

Figure 6.4	**LSE of cipher image**	**Theoretical LSE critical values**			
		Significance level = 0.05		**Significance level = 0.01**	
		h^{l*}_{left}	h^{l*}_{right}	h^{l*}_{left}	h^{l*}_{right}
CT Paranasal	7.901874247	7.901901305	7.90303732	7.901722822	7.903215812
Cervical X-Ray	7.902626309	7.901901305	7.90303732	7.901722822	7.903215812
CT Abdomen	7.902892198	7.901901305	7.90303732	7.901722822	7.903215812
Knee X-Ray	7.901989084	7.901901305	7.90303732	7.901722822	7.903215812

In this test the parameters (k, T_B, α) are used, where k is number of blocks taken, T_B shows number of pixel in each block and α is the significance level. By taking different block size the local Shannon entropy values of test images are checked and compared the results with standard random local Shannon entropy values with the mean and variance in Table 6.5.

The cipherimage passes the test if result falls in the interval otherwise it fails, Also by using the standard parameters *i.e.*, (k, T_B) = (30, 1936) the local Shannon entropy for various medical images is calculated and found in range as shown in Table 6.6. Cipherimages obtained from proposed encryption scheme goes in the critical interval. It shows that the proposed image encryption scheme produces cipher images that results high randomness for non overlapping blocks.

6.3.1.7 Differential Analysis

An essential property of a good performance image encryption algorithm is that, images encrypted with that algorithm should be totally different from plain images.

Table 6.7: NPCR values of 8-bit 256 × 256 gray medical images and their comparison with theoretical values of significance level 0.05, 0.01 and 0.001

			Theoretical NPCR critical values		
Sr. #	**Images**	**NPCR**	**Significance level**		
		values	**0.05**	**0.1**	**0.01**
1	CT Paranasal	99.6014%	99.5693%	99.5527%	99.5341%
2	Cervical X-Ray	99.5755%	99.5693%	99.5527%	99.5341%
3	CT Abdomen	99.5976%	99.5693%	99.5527%	99.5341%
4	Knee X-Ray	99.6189%	99.5693%	99.5527%	99.5341%

Table 6.8: UACI values of 8-bit 256 × 256 gray medical images and their comparison with theoretical values of significance level 0.05 and 0.01

			Theoretical UACI critical values			
Sr.	**Images**	**UACI**	**Signif. level 0.05**		**Signif. level 0.01**	
#		**values**	$u^{*-}_{0.05}$	$u^{*+}_{0.05}$	$u^{*-}_{0.01}$	$u^{*+}_{0.01}$
1	CT Paranasal	33.4385%	33.2824%	33.6447%	33.2255%	33.7016%
2	Cervical X-Ray	33.3571%	33.2824%	33.6447%	33.2255%	33.7016%
3	CT Abdomen	33.4123%	33.2824%	33.6447%	33.2255%	33.7016%
4	Knee X-Ray	33.5643%	33.2824%	33.6447%	33.2255%	33.7016%

The values of NPCR and UACI for differential analysis can be calculated by using Equation (3.12).

It can be seen from the experimental results shown in Table 6.7 and Table 6.8, that the proposed scheme gets high performance for NPCR and UACI. Therefore it will give well resistance against “known plain text attacks” and “chosen plain text attacks”.

6.3.1.8 Noise and Data Loss Attacks

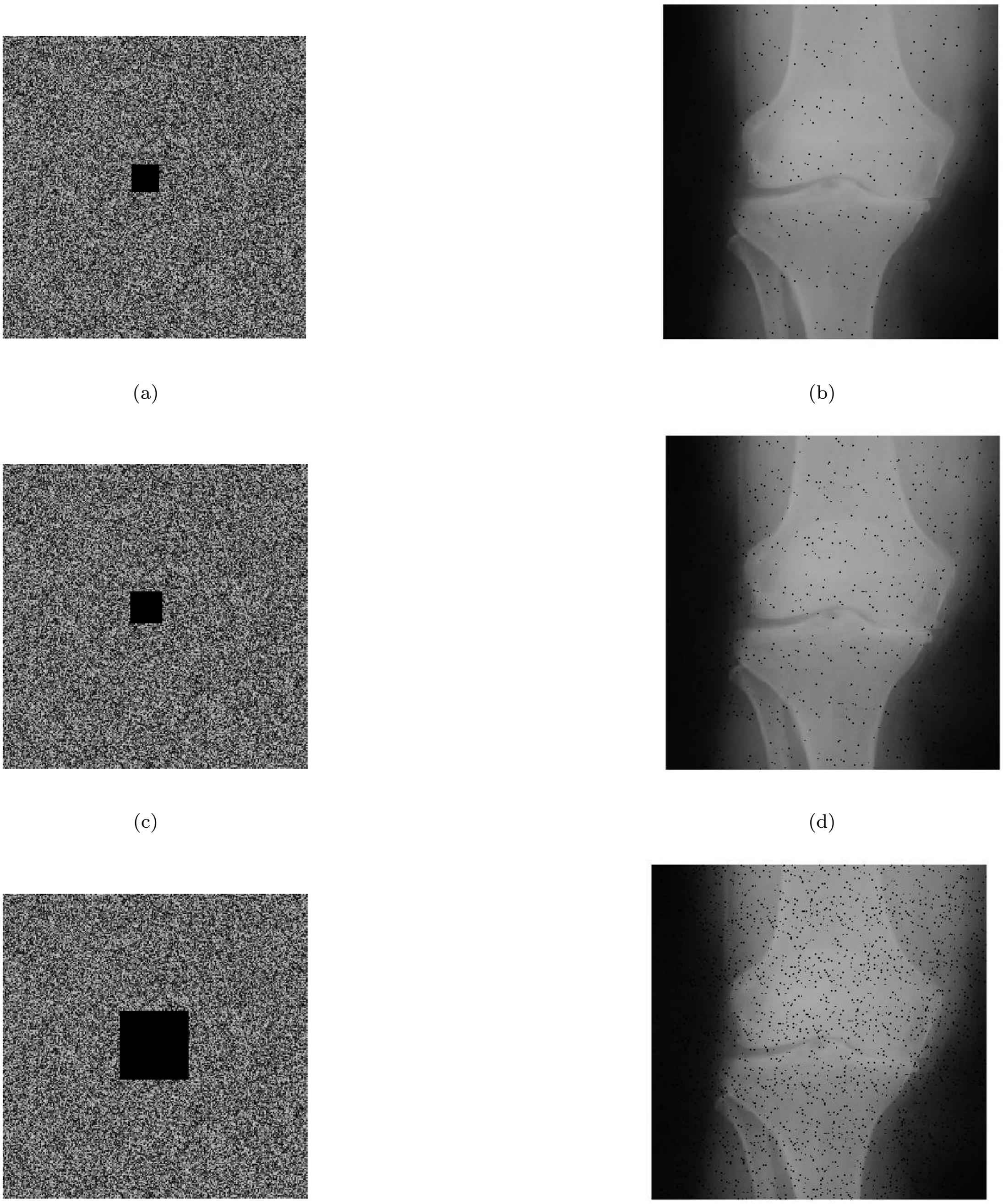
The perfect encryption scheme ought to diminish the noise effects caused by differences in pixels in the decrypted image. For checking the capability of the proposed scheme in opposing noise and data loss attacks, a medical image from Figure 6.4 (g) of size 256×256 is taken as test case.

In the encryption result of test image, 1%, 2% and 5% pixels are replaced with the dark part as shown in the Figure 6.8 (a, c, e). The decryption results of noised cipher images are also shown in Figure 6.8 (d, e, f).

From the Figure 6.8 it is clear that when the cipher image endure data loss attacks, the decrypted image obtained by using the encryption process maintain vast majority of original image information containing only a small portion of uniformly distributed noise.

The peak signal to noise ratio (PSNR) provides a quantitative measure for the distinction between the original plain image I_P and its decryption result I_D. The cumulative squared error between the decrypted image and the original image can be measured by using mean square error (MSE).

For an image of size MN the PSNR and MSE values can be calculated using Equations (3.13) and (3.14). The least value of MSE (3.13) shows the minimum error by using the proposed encryption scheme, while the PSNR (3.14) measure is usually employed to calculate the ability of rehabilitation. The greater value of PNSR indicates the higher fidelity of decrypted image towards its original plain image. If I_D and I_P are similar then the calculated value of PSNR approaches to infinity. The value above 30 db shows that I_D and I_P are not sensible for PSNR. For the values above 35 db, it is difficult to differentiate between the original image and decrypted image.



(a) (b)

(c) (d)

(e) (f)

Figure 6.8: Experimental results for the performance evaluation of data loss attacks: (a, c, e) cipher images with 1%, 2% and 5% data loss, (b, d, f) decryption results of corresponding images using our scheme

For checking the cipher image's robustness against noise attacks, 1%, 2% and 5% noise is added in cipher image of Figure 6.4 (g), as shown in Figure 6.8 (a, c, e). The calculated values of PSNR for these modified cipher images are 25.34, 22.78 and 19.36 respectively. By observing the test results it can be seen that the encryption technique gives good performance for anti data loss and noise attacks.

6.3.1.9 Computational Complexity

It is determined by analyzing the encryption scheme and sequence generation method. The complexity of various image encryption schemes is analyzed by using the identical approach as adopted in [184] and then compared their complexities with the proposed encryption scheme. The overall complexity of the proposed encryption scheme is $O(3MN\log_2(MN)+12MN)$, with the image size taken as $M \times N$.

TABLE 6.9: Comparison of computational complexity with different encryption schemes

Sr. no.	Schemes	Computational complexity	
		Scrambling	Diffusion
1	Ref [185]	$2MN+2MN\log_2(MN)$	$2MN$
2	Ref [184]	$4MN+2\log_2(MN)$	$2MN$
3	Ref [40]	$10MN+2\log_2(MN)$	$2MN$
4	Ours	$8MN+3MN\log_2(MN)$	$4MN$

The scrambling process of proposed encryption scheme consists of $3MN\log_2(MN)+8MN$ times floating point operations, while $10MN$ floating point operations are used in diffusion process. For time complexity computation one time floating point operation indicates one bit level operation.

By comparing the complexity of the proposed scheme in Table 6.9, with the schemes presented in [185], [184], [40], it can be seen that computational complexity of the proposed image encryption schemes exceeds by [185], [184]. It shows that the internal structure of proposed scheme is complex, hence resists against various attacks.

6.3.2 Signcryption Attributes

The security components of proposed signcryption scheme are:

6.3.2.1 Confidentiality

Confidentiality means to secure the message containing plain image from unauthorized sources. The proposed scheme is secure from unauthorized access as if some unauthorized party/user wants to find secret key component k' or k''. It is almost infeasible because for this he/she has to solve ECDLP.

6.3.2.2 Authentication

Authentication is the method by which receiver can authenticate the user by following the verification method. The authentication process works by using the comparison of hash values. If the comparison returns true results, then it means that the user and his sent medical image is authenticated.

In the proposed scheme the patient calculates hash value of image I, cipher image C and key K, then multiply with base point of elliptic curve G to get authentication parameter G'. Patient sends this G' to health-care center. The health care center decrypt C with K to get image I. It also calculates hash value of I, C and K, and multiply it with G to get A'. The patient along with his sent image I will be authenticated if G'= A'.

6.3.2.3 Integrity

In this process data is maintained in its actual form, that could not be changed by adversary during its communication. In the proposed scheme

$$h = H(I, C, K) \text{ and } s = \frac{k}{h + P_a} \mod p$$

are used in signcryption stage. If a fake user changes some contents of cipher image, then new cipher image will become C', so he sends (C', s, G').

The related image I' is also changed, but one way hash function makes it infeasible. Also the change will be detected at the time of verification, hence changed cipher image will be rejected. In this way the integrity of original image will be confirmed.

6.3.2.4 Unforgeability

In the proposed signcryption scheme, a fake user can try to forge the signcryption scheme as following:

1. The fake user chooses k_1 and multiply it with health-care authority's public key P_b to get secret key K_f.

2. He/she takes the forged image I' and encrypt it with the hashed key as $C' = E_{H(K_f)}(I')$.

3. Then he/she computes h' and s' as:

$$h' = H(I', C', K_f), \quad s' = \frac{k_1}{h' + s'_a} \mod p$$

4. Also computes authentication parameter

$$G'_1 = h'G$$

   and sends (C', G'_1, s') to health-care authority.

The health-care center receives (C', s', G'_1) from fake user. It tries to find key by using its private key s_b, patient's public key P_a, received digital signature s' and authentication parameter G'_1.

$$\begin{aligned}
s_b\ s'\ G'_1 + s_b\ s'\ P_a & \\
&= s_b\ \frac{k_1}{h' + s'_a}\ h'\ G + s_b \frac{k_1}{h' + s'_a}\ s_a\ G \mod p \\
&= \frac{s_b\ k_1\ h'\ G}{h' + s'_a} + \frac{s_b\ k_1\ G\ s_a}{h' + s'_a} \mod p \\
&= \frac{(s_b\ k_1\ G)(h' + s_a)}{h' + s'_a} \mod p \\
&\neq (s_b\ k\ G) \text{ or } k\ P_b = K_f
\end{aligned}$$

Hence the forged key is not rightly generated and image I cannot be decrypted rightly.

6.3.2.5 Non-repudiation

Non-repudiation means that the sender cannot deny from something he had sent earlier. In case of denial of sending the message by the sender, the recipient may send (C, s, G') requiring the judge to verify it. In judge verification process, the judge can decide that signature is generated by the sender if the equation

$$K = (k', k'') = s_b\ s\ G' + s_b\ s\ P_a,$$

holds. In the proposed signcryption scheme, digital signature

$$s = \frac{k}{h + s_a}$$

contains private key s_a of the sender. Digital signature cannot be generated without sender's compliance. Therefore sender cannot deny from sending at any stage.

6.3.2.6 Forward Secrecy

It means that attacker cannot recover sender's previous message even if he gets access to the sender's private key s_a and (C, s, G'). Because a random number k

is used for key generation. Which is known only to the sender. For the generation of secret key anyone has to solve the following equation:

$$K = k\ P_b$$

Here P_b is the public key of receiver and k is the random number chosen by the sender. Attacker does not know about k, hence cannot find key K and decrypt C to get plainimage I.

The proposed scheme shows good result against authentication, confidentiality, integrity, unforgeability and forward secrecy. The comparison of signcryption attributes of proposed scheme with other signcryption schemes is shown in Table 6.12.

6.3.2.7 Analysis of Computational Cost

In the proposed signcryption scheme, the computational cost for sender and receiver is calculated. Table 6.10 gives a comparison for operations used by the sender and receiver, while Table 6.11 shows average computational time of mainly used operations.

Sender uses only 2 elliptic curve point multiplications, while receiver takes 3 elliptic curve point multiplications hence it is more efficient than the schemes presented in [66], [186], [187] .

The elliptic curve point multiplication requires 83 ms, while modular exponentiation needs 220 ms as average computational time on infineon's SLE66CUX640P [188]. The computational time is calculated in Table 6.11 and compared with other signcryption schemes. The proposed scheme provides some added functions like forward secrecy and non repudiation without using another protocols with less computational cost.

TABLE 6.10: Comparison of computational cost of proposed signcryption scheme

Signc. schemes	**Entity**	***ECPM***	***ECPA***	***EXP***	***DIV***	***MUL***	***ADD***	***H***
Proposed scheme	sender	3	-	-	1	2	1	2
	receiver	4	-	-	-	-	1	1
Zheng [60]	sender	-	-	1	1	-	1	2
	receiver	-	-	2	-	2	-	2
Zheng and Lmai [131]	sender	1	-	-	1	1	1	2
	receiver	2	1	-	-	2	-	2
Deng and Bao [66]	sender	-	-	2	1	-	1	3
	receiver	-	-	3	-	1	-	3
Gamage *et al.* [186]	sender	-	-	2	1	-	1	2
	receiver	-	-	3	-	1	-	2
Jung *et al.* [187]	sender	-	-	2	1	-	1	2
	receiver	-	-	3	-	1	-	2

The number of operations used for: ECPM (elliptic curve point multiplication), ECPA (elliptic curve point addition), EXP (modular exponentiation), DIV (modular division), MUL (modular multiplication), ADD (modular addition), H (one-way hash functions).

TABLE 6.11: Comparison of average computation time of main operations used

Signcrypt. schemes	**Sender**	**Recipient**
	Average computation time(ms)	**Average computation time(ms)**
Proposed scheme	$3 \times 83 = 249$	$4 \times 83 = 332$
Deng and Bao [66]	$2 \times 220 = 440$	$3 \times 220 = 660$
Gamage *et al.* [186]	$2 \times 220 = 440$	$3 \times 220 = 660$
Jung *et al.* [187]	$2 \times 220 = 440$	$3 \times 220 = 660$
Zheng [60]	$1 \times 220 = 220$	$2 \times 220 = 440$
Zheng and Lmai [131]	$1 \times 83 = 83$	$2 \times 83 = 166$

6.3.3 Man in the Middle Attack

For an unauthorized user say "Mallory" that insert himself in communication between patient and health-care authority. He intercepts (C, s, G') sent by patient. Then produces his own secret key and uses it for the generation of cipher image (C'), signature (s') and authentication parameter (G''). He alters patient's sent parameters (C, s, G') by his generated tuple (C', s', G'') and sends it to the health-care center. The center works for the the generation of secret key K^* to decrypt received C'. This key does not provide any help to reveal the secret image. Also the signature generated by the attacker will not be verified by signcryption algorithm. Hence it can be seen that, man in the middle attack is not applicable for the proposed scheme.

Table 6.12: Comparison of security properties of proposed signcryption scheme

Signc. schemes	**Conf.**	**Unforgability**	**Integrity**	**Non-repudiation**	**F. Secrecy**
Proposed scheme	**Yes**	**Yes**	**Yes**	**Directly**	**Yes**
Zheng [60]	Yes	Yes	Yes	Another protocol	No
Zheng and Lmai [131]	Yes	Yes	Yes	Another protocol	No
Deng and Bao [66]	Yes	Yes	Yes	Directly	No
Jung *et al.* [187]	Yes	Yes	Yes	Another protocol	Yes
Gamage *et al.* [186]	Yes	Yes	Yes	Directly	No

6.4 Comparison of Proposed Schemes

A color image encryption approach by implementing permutation, substitution and XOR is presented in Chapter 4. Then, another image encryption scheme by taking a new dynamic compound chaotic is given in Chapter 5, while for medical data, an image signcryption scheme using TLTS and Henon chaotic map is given in Chapter 6. A structural comparison of these approaches is given below in Table 6.10.

Table 6.13: A structural comparison of different image encryption schemes

Chapters	**Permutation**	**S-box**	**XOR**	**Invertible Self Mixing**	**Recursion**
Chapter 4	Yes	Yes	Yes	No	Yes
Chapter 5	No	Yes	Yes	Yes	Yes
Chapter 6	Yes	No	Yes	No	Yes

6.5 Conclusion

In this chapter, a novel medical image signcryption scheme is proposed. It uses hybrid cryptographic technique for the signcryption of image based data. Firstly patient/sender uses his private key and health-care center's public key to make symmetric encryption key and then he/she uses its hash value for chaos based medical symmetric image encryption. The health-care center also uses the same key for decryption. Hash value of cipher image is signed and exchanged for authentication of communication.

The proposed scheme provides authentication, confidentiality, unforgability, integrity, and non-repudiation, While chaos-based symmetric encryption is checked against key space analysis, key sensitivity, correlation analysis, NPCR and UACI, local and global Shannon entropy analysis, histogram analysis, noise and data loss attacks and its complexity.

On the basis of results obtained from all these analysis, it is believed that the proposed signcryption scheme is robust, provides good security for sensitive medical images.

Chapter 7

Conclusion and Future Work

The security aspects of multi-media information are discussed in this thesis. Particularly, Chapter 1 presents the introduction of this thesis, Chapter 2 and 3 provides background of mathematical and cryptographic concepts, the chaos based image encryption schemes and a signcryption scheme for medical images are proposed in Chapter 4, 5 and 6.

7.1 Conclusion

The internet, the internet of things (IoT) etc, are the examples of technologies that have virtually changed every nations' culture. In the modern age, digital image have gained a lot of importance in every aspect of life. These images are generated and used in the diverse areas as weather forecasting, commerce research, government and diplomatic missions, personal affairs, tele-medicine, military, space sciences etc. These images are frequently saved and transmitted through a public network. Their storage and transmission has serious consequences if they are very sensitive and hacked by attackers or enemies. Therefore, protecting these images has become an urgent and serious task. As a result, researchers are constantly exploring new approaches to find a perfect answer to this problem. The use of chaos theory is thought to be a suitable platform in this regard. By keeping in mind all these things, some methods for the security of secret images are proposed in this thesis. The following shows some more concluding remarks of this thesis.

- A new chaos based encryption scheme for color image is proposed. Simple one dimensional chaotic maps *i.e.*, PWLCM and logistic map are employed in it. S-box is used for confusion purpose while XOR operation is used for diffusion purpose. It is a lightweight encryption scheme that has an easy implementation. The security analysis shows that it has fairly good results against the correlation, information entropy, key space, NPCR and UACI, and noise and data loss attacks.

- The analysis of some well known one dimensional chaotic maps (*e. g.*, tent map, logistic map etc) shows that they have certain drawbacks like short chaotic range, open periodic windows in chaotic region etc. To handle with these problems a new color tent logistic chaotic system based image encryption scheme is designed. This system is generated by combining the tent and logistic map in such a way that it provide a huge key space with no periodic window in its chaotic region. The diffusion stage of encryption also contains a novel mixing technique that makes the internal structure of encryption more complex. Due to the uses of tent logistic map the proposed scheme provides a high key sensitivity and big key space, while other analysis indicators also provide comparative results with other proposed algorithms

- A medical image signcryption scheme is proposed in this study, that provides additional security attributes for the sensitive medical data. It not only gives encryption but also provides a complete mechanism of key generation, digital signatures and authentication process of the sent image in a single algorithm. In the chaos based encryption phase, the use of tent logistic tent system results in hyper chaotic behavior in the encrypted image. Due to these salient features it seems to be the first scheme in literature providing key management, confidentiality, authentication, unforgeability, forward secrecy, integrity and non repudiation of medical images.

7.2 Suggestion for Future Work

The current research proposed in this thesis and its contribution in literature along with future directions is given as followings.

The method proposed in Chapter 4 uses simple one dimensional chaotic maps, chaotic permutation technique, S-box as look up table and bitwise XOR operation for encryption of color images. In 2020, Wang and Liu [189] introduced a new image encryption scheme that takes large parameter interval for one dimensional sine chaotic system. In this technique, by using dynamic parameter Arnold map, the image is first scrambled. Then dynamic formulas are suggested through one dimensional chaotic sine map. Suman *et al.* [190] presented an approach for secure color image encryption that uses chaotic Duffin map for the pseudo random numbers to perform permutation and diffusion of image pixels.

A medical image encryption scheme is developed by Rajendran *et al.* [191] that uses novel cross cosine map for dynamic bit level diffusion. Chaotic series is generated by proposed two dimensional cross cosine map and then utilized in confusion and diffusion architecture. Recently in 2022, Vidhya and Brindha [111] presented an image encryption approach that is based on bit level substitution and block level permutation.

These encryption approaches and many others [110, 192–194] use the approach presented in Chapter 4 in their research. As the method proposed in Chapter 4 uses simple one dimensional chaotic maps, chaotic permutation technique, S-box as look up table and bitwise XOR, that makes it lightweight in comparison to the above discussed approaches. A comparison of cryptographic properties of this approach with other existing schemes is given in Table 4.9.

The approach [88] given in Chapter 5 is recently published. Guler[195] uses this research in graphical coded algorithm in secure communication applications based on memristor-based chaotic circuit. A comparison of cryptographic properties of this approach with other existing schemes is given in Table 5.8.

In Chapter 6, a novel signcryption scheme based on chaos for medical images is proposed that provides security features like authentication, forward secrecy, unforgeability, integrity, non repudiation etc. Ghosh et al. [196] analyzed several chaotic systems used for image encryption purposes and also described their advantages and disadvantages.

Authors claimed that chaotic, low-dimensional maps based imaging security approaches have less ability to handle the attacks also provides less security. They also presented solution of this problem by multiple broad chaotic charts. Henon chaotic map is used by Masood *et al.* [109] for a medical image encryption scheme that uses, Brownian motion, and Chen's chaotic system with elevated security. A mechanism developed by Harshitha *et al.* [108] for secure medical image encryption. This uses linear feedback shift register and logistic map for the protection of medical images.

For IoT-powered healthcare systems Rajendran *et al.* [57] proposed medical image transmission model based on chaotic maps used. Combined chaotic maps are used by Kari *et al.* [197] presented a novel multi-image cryptosystem that also uses weighted plainimages. The degree of correlation between their neighboring pixels is utilized to give a certain weight to the plainimages.

These medical image encryption approaches and many others [198–200] use the approach presented in Chapter 6 in their research. In comparison to above medical image encryption techniques, the image signcryption technique presented in Chapter 6 has many additional security features like authentication, forward secrecy, unforgeability, integrity, non repudiation etc that other medical encryption schemes lacks. Due to the presence of these security features it is more secure and robust then other ones.

As a future work the following ideas are suggested to improve the performance and the effectability of the recent work.

- The proposed image encryption schemes presented in Chapter 4, 5 can be extended to signcryption schemes for providing extra confidential security features and authenticated communication, simultaneously.

- Most of the existing proposal of image cryptosystem only give the encryption mechanism while lacking the key exchange protocol. A key exchange protocol can be developed and accommodated with these encryption scheme.

- Optimization techniques can be applied on the existing encryption algorithms to optimize their performance.

- The use of chaotic neural network and artificial intelligence in the proposed encryption schemes may enhance their security level.

- Image encryption schemes proposed in this study can be extended to video and speech encryption schemes.

- As a future work, the security aspects of proposed encryption techniques presented in this thesis will be compared with current researches in this field.

Bibliography

[1] M. Diomidous, K. Chardalias, A. Magita, P. Koutonias, P. Panagiotopoulou, and J. Mantas, “Social and psychological effects of the internet use,” *Acta informatica medica*, vol. 24, no. 1, pp. 66, 2016.

[2] H. Dreßing, J. Bailer, A. Anders, H. Wagner, and C. Gallas, “Cyberstalking in a large sample of social network users: Prevalence, characteristics, and impact upon victims,” *Cyberpsychology, Behavior, and Social Networking*, vol. 17, no. 2, pp. 61–67, 2014.

[3] U. Zia, M. McCartney, B. Scotney, J. Martinez, M. AbuTair, J. Memon, and A. Sajjad, “Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains,” *International Journal of Information Security*, pp. 1–19, 2022.

[4] M. Hellman, “An extension of the shannon theory approach to cryptography,” *IEEE Transactions on Information Theory*, vol. 23, no. 3, pp. 289–294, 1977.

[5] J. Daemen and V. Rijmen, “The Rijndael block cipher, AES proposal,” *In First Candidate Conference*, pp. 343–348, 1999.

[6] M. Farah, A. Farah, and T. Farah, “An image encryption scheme based on a new hybrid chaotic map and optimized substitution box,” *Nonlinear Dynamics*, vol. 99, no. 4, pp. 3041–3064, 2020.

[7] T. S. Ali and R. Ali, “A new chaos based color image encryption algorithm using permutation substitution and boolean operation,” *Multimedia Tools*

and Applications; Springer: Berlin/Heidelberg, Germany, vol. 79, no. 27, pp. 19853–19873, 2020.

[8] A. H. ElSafty, M. F. Tolba, L. A. Said, A. H. Madian, and A. G. Radwan, "Hardware realization of a secure and enhanced s-box based speech encryption engine," *Analog Integrated Circuits and Signal Processing*, vol. 106, no. 2, pp. 385–397, 2021.

[9] M. A. Khan, A. Ali, V. Jeoti, and S. Manzoor, "A chaos-based substitution box (s-box) design with improved differential approximation probability (dp)," *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, vol. 42, no. 2, pp. 219–238, 2018.

[10] S. S. Jamal, M. U. Khan, and T. Shah, "A watermarking technique with chaotic fractional s-box transformation," *Wireless Personal Communications*, vol. 90, no. 4, pp. 2033–2049, 2016.

[11] A. A. Abd EL-Latif, B. Abd-El-Atty, and S. E. Venegas-Andraca, "A novel image steganography technique based on quantum substitution boxes," *Optics & Laser Technology*, vol. 116, pp. 92–102, 2019.

[12] M. M. Dimitrov, "A framework for fine-grained nonlinearity optimization of boolean and vectorial boolean functions," *IEEE Access*, vol. 9, pp. 124910–124920, 2021.

[13] S. Ibrahim and A. M. Abbas, "A novel optimization method for constructing cryptographically strong dynamic s-boxes," *IEEE Access*, vol. 8, pp. 225 004–225 017, 2020.

[14] R. Soto, B. Crawford, F. González, and R. Olivares, "Human behaviour based optimization supported with self-organizing maps for solving the s-box design problem," *IEEE Access*, vol. 9, pp. 84605–84618, 2021.

[15] M. Ahmad, I. A. Khaja, A. Baz, H. Alhakami, and W. Alhakami, "Particle swarm optimization based highly nonlinear substitution-boxes generation for security applications," *IEEE Access*, vol. 8, pp. 116 132–116 147, 2020.

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

[17] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[18] J. Lopez and R. Dahab, "An overview of elliptic curve cryptography," 2000.

[19] F. Faridi, H. Sarwar, M. Ahtisham, K. Jamal *et al.*, "Cloud computing approaches in health care," *Materials Today: Proceedings*, 2021.

[20] C. Xie and B. Li, "Introduction: Understanding chinese social media," *Internet Pragmatics*, vol. 4, no. 2, pp. 177–189, 2021.

[21] B. J. Erickson, "Imaging systems in radiology," in *Biomedical Informatics.* Springer, pp. 733–753, 2021.

[22] K. M. Barth and N. R. Ciobanu, "Integration of multimedia technologies in the teaching-learning-assessment process," *Proceedings of INTCESS*, vol. 2021, no. 8th, 2021.

[23] A. Costantino, F. Bortoluzzi, M. Giuffrè, R. Vassallo, L. M. Montalbano, F. Monica, D. Canova, D. Checchin, P. Fedeli, R. Marmo *et al.*, "Correct use of telemedicine in gastroenterology, hepatology, and endoscopy during and after the covid-19 pandemic: Recommendations from the italian association of hospital gastroenterologists and endoscopists (aigo)," *Digestive and Liver Disease*, vol. 53, no. 10, pp. 1221–1227, 2021.

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

[25] R. M. May, "Simple mathematical models with very complicated dynamics," *Nature*, vol. 261, no. 5560, pp. 459–467, 1976.

[26] 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.* Springer, pp. 127–140, 1991.

[27] S. Oishi and H. Inoue, "Pseudo-random number generators and chaos," *IEICE Transactions (1976-1990)*, vol. 65, no. 9, pp. 534–541, 1982.

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

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

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

[31] Z. H. Guan, F. Huang, and W. Guan, "Chaos-based image encryption algorithm," *Physics Letters A*, vol. 346, no. 1-3, pp. 153–157, 2005.

[32] V. Patidar, N. Pareek, and K. Sud, "A new substitution–diffusion based image cipher using chaotic standard and logistic maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 14, no. 7, pp. 3056–3075, 2009.

[33] V. Patidar, N. Pareek, G. Purohit, and K. Sud, "Modified substitution–diffusion image cipher using chaotic standard and logistic maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 10, pp. 2755–2765, 2010.

[34] M. François, T. Grosges, D. Barchiesi, and R. Erra, "A new image encryption scheme based on a chaotic function," *Signal Processing: Image Communication*, vol. 27, no. 3, pp. 249–259, 2012.

[35] Y. Q. Zhang and X.-Y. Wang, "A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice," *Information Sciences*, vol. 273, pp. 329–351, 2014.

[36] Y. Zhou, L. Bao, and C. P. Chen, “Image encryption using a new parametric switching chaotic system,” *Signal processing*, vol. 93, no. 11, pp. 3039–3052, 2013.

[37] Z. Zhou, Q. J. Wu, C. N. Yang, X. Sun, and Z. Pan, “Coverless image steganography using histograms of oriented gradients-based hashing algorithm,” *Journal of Internet Technology*, vol. 18, no. 5, pp. 1177–1184, 2017.

[38] Z. Zhou, Y. Wang, Q. J. Wu, C.-N. Yang, and X. Sun, “Effective and efficient global context verification for image copy detection,” *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 1, pp. 48–63, 2016.

[39] S. Kanwal, S. Inam, O. Cheikhrouhou, K. Mahnoor, A. Zaguia, and H. Hamam, “Analytic study of a novel color image encryption method based on the chaos system and color codes,” *Complexity*, vol. 2021, 2021.

[40] S. Ma, Y. Zhang, Z. Yang, J. Hu, and X. Lei, “A new plaintext-related image encryption scheme based on chaotic sequence,” *IEEE Access*, vol. 7, pp. 30 344–30 360, 2019.

[41] C. Li, G. Luo, K. Qin, and C. Li, “An image encryption scheme based on chaotic tent map,” *Nonlinear Dynamics*, vol. 87, no. 1, pp. 127–133, 2017.

[42] Y. Luo, X. Ouyang, J. Liu, and L. Cao, “An image encryption method based on elliptic curve elgamal encryption and chaotic systems,” *IEEE Access*, vol. 7, pp. 38 507–38 522, 2019.

[43] J. Thiyagarajan, B. Murugan, and N. G. A. Gounden, “A chaotic image encryption scheme with complex diffusion matrix for plain image sensitivity,” *Serbian Journal of Electrical Engineering*, vol. 16, no. 2, pp. 247–265, 2019.

[44] X. Wang, X. Zhu, X. Wu, and Y. Zhang, “Image encryption algorithm based on multiple mixed hash functions and cyclic shift,” *Optics and Lasers in Engineering*, vol. 107, pp. 370–379, 2018.

[45] X. Zhang and X. Wang, "Multiple-image encryption algorithm based on dna encoding and chaotic system," *Multimedia Tools and Applications*, vol. 78, no. 6, pp. 7841–7869, 2019.

[46] S. F. Yousif, A. J. Abboud, and R. S. Alhumaima, "A new image encryption based on bit replacing, chaos and dna coding techniques," *Multimedia Tools and Applications*, pp. 1–41, 2022.

[47] U. Hayat, I. Ullah, N. A. Azam, and S. Azhar, "A novel image encryption scheme based on elliptic curves over finite rings," *Entropy*, vol. 24, no. 5, pp. 571, 2022.

[48] X. Wang, S. Wang, N. Wei, and Y. Zhang, "A novel chaotic image encryption scheme based on hash function and cyclic shift," *IETE Technical Review*, vol. 36, no. 1, pp. 39–48, 2019.

[49] I. Indrajit, "Digital imaging and communications in medicine: A basic review," *Indian Journal of Radiology and Imaging*, vol. 17, no. 1, 2007.

[50] N. E. M. Association *et al.*, "Digital imaging and communications in medicine (DICOM)," *http.//medical. nema. org/*, 2003.

[51] A. A. Gumbs, I. Frigerio, G. Spolverato, R. Croner, A. Illanes, E. Chouillard, and E. Elyan, "Artificial intelligence surgery: how do we get to autonomous actions in surgery?" *Sensors*, vol. 21, no. 16, pp. 5526, 2021.

[52] M. Boussif, N. Aloui, and A. Cherif, "Securing dicom images by a new encryption algorithm using arnold transform and vigenère cipher," *IET Image Processing*, vol. 14, no. 6, pp. 1209–1216, 2020.

[53] M. Mohamed, F. Zaki, and A. El-Mohandes, "Novel fast encryption algorithms for multimedia transmission over mobile wimax networks," *International Journal of Computer Science Issues (IJCSI)*, vol. 9, no. 6, pp. 60, 2012.

[54] Y. Wu, J. P. Noonan, S. Agaian *et al.*, "Npcr and uaci randomness tests for image encryption," *Cyber journals: multidisciplinary journals in science*

and technology, Journal of Selected Areas in Telecommunications (JSAT), vol. 1, no. 2, pp. 31–38, 2011.

[55] X. Chen and C. J. Hu, “Adaptive medical image encryption algorithm based on multiple chaotic mapping,” *Saudi journal of biological sciences*, vol. 24, no. 8, pp. 1821–1827, 2017.

[56] O. Reyad, K. Hamed, and M. E. Karar, “Hash-enhanced elliptic curve bit-string generator for medical image encryption,” *Journal of Intelligent & Fuzzy Systems*, vol. 39, no. 5, pp. 7795–7806, 2020.

[57] S. Rajendran and M. Doraipandian, “Chaos based secure medical image transmission model for iot-powered healthcare systems,” in *IOP Conference Series: Materials Science and Engineering*, vol. 1022, no. 1. IOP Publishing, pp. 012106, 2021.

[58] W. Oszywa and R. Gliwa, “Combining message encryption and authentication,” *Annales Universitatis Mariae Curie-Sklodowska, sectio AI–Informatica*, vol. 11, no. 2, pp. 61–79, 2011.

[59] M. Bellare, J. Kilian, and P. Rogaway, “The security of the cipher block chaining message authentication code,” *Journal of Computer and System Sciences*, vol. 61, no. 3, pp. 362–399, 2000.

[60] Y. Zheng, “Digital signcryption or how to achieve cost (signature & encryption) cost (signature)+ cost (encryption),” in *Annual international cryptology conference.* Springer, pp. 165–179, 1997.

[61] M. Kumar and P. Gupta, “An efficient and authentication signcryption scheme based on elliptic curves,” *MATEMATIKA: Malaysian Journal of Industrial and Applied Mathematics*, pp. 1–11, 2019.

[62] E. A. Hagras, D. El-Saied, and H. H. Aly, “Energy efficient key management scheme based on elliptic curve signcryption for wireless sensor networks,” in *2011 28th National Radio Science Conference (NRSC).* IEEE, pp. 1–9, 2011.

[63] A. Elkhalil, R. Elhabob, N. Eltayieb *et al.*, "An efficient signcryption of heterogeneous systems for internet of vehicles," *Journal of Systems Architecture*, vol. 113, pp. 101885, 2021.

[64] Y. Zhou, Y. Xu, Z. Qiao, B. Yang, and M. Zhang, "Continuous leakage-resilient certificate-based signcryption scheme and application in cloud computing," *Theoretical Computer Science*, vol. 860, pp. 1–22, 2021.

[65] I. Ullah, N. U. Amin, M. A. Khan, H. Khattak, and S. Kumari, "An efficient and provable secure certificate-based combined signature, encryption and signcryption scheme for internet of things (iot) in mobile health (m-health) system," *Journal of Medical Systems*, vol. 45, no. 1, pp. 1–14, 2021.

[66] F. Bao and R. H. Deng, "A signcryption scheme with signature directly verifiable by public key," in *International Workshop on Public Key Cryptography.* Springer, pp. 55–59, 1998.

[67] A. B. Mahmood and R. D. Dony, "Segmentation based encryption method for medical images," in *2011 International Conference for Internet Technology and Secured Transactions.* IEEE, pp. 596–601, 2011.

[68] S. T. Wong, "A cryptologic based trust center for medical images," *Journal of the American Medical Informatics Association*, vol. 3, no. 6, pp. 410–421, 1996.

[69] M. M. Abd-Eldayem, "A proposed security technique based on watermarking and encryption for digital imaging and communications in medicine," *Egyptian Informatics Journal*, vol. 14, no. 1, pp. 1–13, 2013.

[70] S. K. Bhopi, N. M. Dongre, and R. R. Gulwani, "Binary key based permutation for medical image encryption," in *2016 International Conference on Inventive Computation Technologies (ICICT)*, vol. 3. IEEE, pp. 1–6, 2016.

[71] L. D. Singh and K. M. Singh, "Image encryption using elliptic curve cryptography," *Procedia Computer Science*, vol. 54, pp. 472–481, 2015.

[72] A. Shukla, J. Shah, and N. Prabhu, "Image encryption using elliptic curve cryptography," *International Journal of Students' Research in Technology & Management*, vol. 1, no. 2, pp. 115–117, 2015.

[73] W. Cao, Y. Zhou, C. P. Chen, and L. Xia, "Medical image encryption using edge maps," *Signal Processing*, vol. 132, pp. 96–109, 2017.

[74] S. Dhall, S. K. Pal, and K. Sharma, "A chaos-based probabilistic block cipher for image encryption," *Journal of King Saud University-Computer and Information Sciences*, 2018.

[75] G. Ye, C. Pan, X. Huang, and Q. Mei, "An efficient pixel-level chaotic image encryption algorithm," *Nonlinear Dynamics*, vol. 94, no. 1, pp. 745–756, 2018.

[76] T. S. Ali and R. Ali, "A novel medical image signcryption scheme using tlts and henon chaotic map," *IEEE Access*, vol. 8, pp. 71 974–71 992, 2020.

[77] H. Liu and X. Wang, "Color image encryption based on one-time keys and robust chaotic maps," *Computers & Mathematics with Applications*, vol. 59, no. 10, pp. 3320–3327, 2010.

[78] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Optics Communications*, vol. 284, no. 16-17, pp. 3895–3903, 2011.

[79] X. Y. Wang, Y.-Q. Zhang, and X.-M. Bao, "A novel chaotic image encryption scheme using dna sequence operations," *Optics and Lasers in Engineering*, vol. 73, pp. 53–61, 2015.

[80] X. Wang, L. Liu, and Y. Zhang, "A novel chaotic block image encryption algorithm based on dynamic random growth technique," *Optics and Lasers in Engineering*, vol. 66, pp. 10–18, 2015.

[81] X. Y. Wang, L. Yang, R. Liu, and A. Kadir, "A chaotic image encryption algorithm based on perceptron model," *Nonlinear Dynamics*, vol. 62, no. 3, pp. 615–621, 2010.

[82] C. Pan, G. Ye, X. Huang, and J. Zhou, “Novel meaningful image encryption based on block compressive sensing,” *Security and Communication Networks*, vol. 2019, 2019.

[83] Y. Q. Zhang and X. Y. Wang, “A new image encryption algorithm based on non-adjacent coupled map lattices,” *Applied Soft Computing*, vol. 26, pp. 10–20, 2015.

[84] X. Wang, L. Feng, and H. Zhao, “Fast image encryption algorithm based on parallel computing system,” *Information Sciences*, vol. 486, pp. 340–358, 2019.

[85] X. Wang and S. Gao, “Image encryption algorithm for synchronously updating boolean networks based on matrix semi-tensor product theory,” *Information Sciences*, vol. 507, pp. 16–36, 2020.

[86] M. K. Abdmouleh, A. Khalfallah, and M. S. Bouhlel, “A novel selective encryption scheme for medical images transmission based-on jpeg compression algorithm,” *Procedia computer science*, vol. 112, pp. 369–376, 2017.

[87] R. Saini and K. S. Vaisla, “Image signcryption using ecc,” in *2014 International Conference on Computational Intelligence and Communication Networks*. IEEE, pp. 829–834, 2014.

[88] T. S. Ali and R. Ali, “A novel color image encryption scheme based on a new dynamic compound chaotic map and s-box,” *Multimedia Tools and Applications*, vol. 81, pp. 20585–20609, 2022.

[89] T. D. P. Bai, K. M. Raj, and S. A. Rabara, “Elliptic curve cryptography based security framework for internet of things (iot) enabled smart card,” in *2017 World Congress on Computing and Communication Technologies (WCCCT)*. IEEE, pp. 43–46, 2017.

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

[91] V. S. Miller, "Use of elliptic curves in cryptography," in *Conference on the theory and application of cryptographic techniques.* Springer, pp. 417–426, 1985.

[92] G. S. Dhillon and J. Ward, "Chaos theory as a framework for studying information systems," in *Advanced Topics in Information Resources Management, Volume 2.* IGI Global, pp. 320–337, 2003.

[93] J. E. Skinner, M. Molnar, T. Vybiral, and M. Mitra, "Application of chaos theory to biology and medicine," *Integrative Physiological and Behavioral Science*, vol. 27, no. 1, pp. 39–53, 1992.

[94] Z. C. Wang, H. R. Hou, and Y. Gan, "Research on modeling of the low-voltage power line communication channel based on chaos theory," *Electrical Measurement & Instrumentation*, vol. 44, no. 500, pp. 20–24, 2007.

[95] E. Lorenz, "Predictability: Does the flap of a butterfly wings in Brazil set of a tornado in Texas," *Proceedings American Association for the Advancement of Science in Washington*, 1979.

[96] A. M. Lyapunov, "The general problem of the stability of motion," *International journal of control*, vol. 55, no. 3, pp. 531–534, 1992.

[97] W. Greiner, *Classical mechanics: systems of particles and Hamiltonian dynamics.* Springer Science & Business Media, 2009.

[98] M. Markus and B. Hess, "Lyapunov exponents of the logistic map with periodic forcing," *Computers & graphics*, vol. 13, no. 4, pp. 553–558, 1989.

[99] S. Li, G. Chen, and X. Mou, "On the dynamical degradation of digital piecewise linear chaotic maps," *International journal of Bifurcation and Chaos*, vol. 15, no. 10, pp. 3119–3151, 2005.

[100] L. O. Chua, "Chuas circuit: An overview ten years later," *Journal of Circuits, Systems, and Computers*, vol. 4, no. 02, pp. 117–159, 1994.

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

[102] X. Wang, S. Zhou, H. Zhang, and Y. Zhang, "New 4d discrete hyperchaotic map and its application in image encryption," *Information Sciences*, vol, 585, pp. 465–485, 2022.

[103] J. C. Sprott, *Elegant chaos: algebraically simple chaotic flows.* World Scientific, 2010.

[104] E. Zambrano-Serrano, J. Muñoz-Pacheco, and E. Campos-Cantón, "Chaos generation in fractional-order switched systems and its digital implementation," *AEU-International Journal of Electronics and Communications*, vol. 79, pp. 43–52, 2017.

[105] F. Ozkaynak, "A novel random number generator based on fractional order chaotic Chua system," *Elektronika ir Elektrotechnika*, vol. 26, no. 1, pp. 52–57, 2020.

[106] F. Özkaynak, V. Çelik, and A. B. Özer, "A new S-box construction method based on the fractional-order chaotic Chen system," *Signal, Image and Video Processing*, vol. 11, no. 4, pp. 659–664, 2017.

[107] A. El-Maksoud, J. Ahmed, A. El-Kader, A. Ayman, B. G. Hassan, N. G. Rihan, M. F. Tolba, L. A. Said, A. G. Radwan, and M. F. Abu-Elyazeed, "Fpga implementation of integer/fractional chaotic systems," in *Multimedia Security Using Chaotic Maps: Principles and Methodologies.* Springer, pp. 199–229, 2020.

[108] M. Harshitha, C. Rupa, K. P. Sai, A. Pravallika, and V. K. Sowmya, "Secure medical data using symmetric cipher based chaotic logistic mapping," in *2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS)*, vol. 1. IEEE, pp. 476–481, 2021.

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

[110] B. Parameshachari, H. Panduranga *et al.*, “Medical image encryption using scan technique and chaotic tent map system,” in *Recent Advances in Artificial Intelligence and Data Engineering.* Springer, pp. 181–193, 2022.

[111] R. Vidhya and M. Brindha, “A novel approach for chaotic image encryption based on block level permutation and bit-wise substitution,” *Multimedia Tools and Applications*, vol. 81, no. 3, pp. 3735–3772, 2022.

[112] M. Markus and B. Hess, “Lyapunov exponents of the logistic map with periodic forcing,” in *Chaos and Fractals.* Elsevier, pp. 73–78, 1998.

[113] J. Oravec, L. Ovseník, J. Turán, and T. Huszaník, “Mitigating drawbacks of logistic map for image encryption algorithms,” *Computing and Informatics*, vol. 39, no. 6, pp. 1250–1281, 2020.

[114] A. Thane and R. Chaudhari, “Hardware design and implementation of pseudorandom number generator using piecewise linear chaotic map,” in *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI).* IEEE, pp. 456–459, 2018.

[115] M. Crampin and B. Heal, “On the chaotic behaviour of the tent map,” *Teaching Mathematics and its Applications: An International Journal of the IMA*, vol. 13, no. 2, pp. 83–89, 1994.

[116] M. Hénon, “A two-dimensional mapping with a strange attractor,” in *The Theory of Chaotic Attractors.* Springer, pp. 94–102, 1976.

[117] S. Sheela, K. Suresh, and D. Tandur, “Image encryption based on modified henon map using hybrid chaotic shift transform,” *Multimedia tools and applications*, vol. 77, no. 19, pp. 25 223–25 251, 2018.

[118] Q. Lu, C. Zhu, and G. Wang, “A novel s-box design algorithm based on a new compound chaotic system,” *Entropy*, vol. 21, no. 10, pp. 1004, 2019.

[119] M. Alawida, J. S. Teh, A. Samsudin *et al.*, “An image encryption scheme based on hybridizing digital chaos and finite state machine,” *Signal Processing*, vol. 164, pp. 249–266, 2019.

[120] R. B. Naik and U. Singh, "A review on applications of chaotic maps in pseudo-random number generators and encryption," *Annals of Data Science*, pp. 1–26, 2022.

[121] F. Özkaynak, "A novel method to improve the performance of chaos based evolutionary algorithms," *Optik*, vol. 126, no. 24, pp. 5434–5438, 2015.

[122] Z. M. Z. Muhammad and F. Özkaynak, "An image encryption algorithm based on chaotic selection of robust cryptographic primitives," *IEEE Access*, vol. 8, pp. 56 581–56 589, 2020.

[123] N. Xuan Quyen, V. Van Yem, and T. Manh Hoang, "A chaos-based secure direct-sequence/spread-spectrum communication system," in *Abstract and applied analysis*, Hindawi, vol. 2013 2013.

[124] M. K. Das and L. M. Saha, "Chaotic dynamics and complexity in real and physical systems," in *Advances in Dynamical Systems Theory, Models, Algorithms and Applications.* IntechOpen, 2021.

[125] M. Doebeli and I. Ispolatov, "Chaos and unpredictability in evolution," *Evolution*, vol. 68, no. 5, pp. 1365–1373, 2014.

[126] N. P. Smart, "Cryptography based on really hard problems," in *Cryptography Made Simple.* Springer, pp. 349–367, 2016.

[127] J. Hoffstein, J. Pipher, J. H. Silverman, and J. H. Silverman, *An introduction to mathematical cryptography.* Springer, vol. 1, 2008.

[128] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, "Applied cryptography," *CRC, Boca Raton*, 1996.

[129] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to elliptic curve cryptography.* Springer Science & Business Media, 2006.

[130] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren, *Handbook of elliptic and hyperelliptic curve cryptography.* CRC press, 2005.

[131] Y. Zheng and H. Imai, “How to construct efficient signcryption schemes on elliptic curves,” *Information processing letters*, vol. 68, no. 5, pp. 227–233, 1998.

[132] A. Kerckhoffs, “A. kerckhoffs, la cryptographie militaire, journal des sciences militaires ix, 38 (1883),” *Journal des sciences militaires*, vol. 9, pp. 38, 1883.

[133] C. E. Shannon, “Communication theory of secrecy systems,” *The Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

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

[135] G. Alvarez and S. Li, “requirements for chaos-based cryptosystems,” *International journal of bifurcation and chaos*, vol. 16, no. 08, pp. 2129–2151, 2006.

[136] K. Pearson, “Notes on regression and inheritance in the case of two parents proceedings of the royal society of london, 58, 240-242,” 1895.

[137] M. Farajallah, S. E. Assad, and O. Deforges, “Cryptanalyzing an image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion,” *Multimedia Tools and Applications*, vol. 77, no. 21, pp. 28 225–28 248, 2018.

[138] W. Zhang, K. Wong, H. Yu, and Z. Zhu, “An image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion,” *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 8, pp. 2066–2080, 2013.

[139] L. Chen, B. Ma, X. Zhao, and S. Wang, “Differential cryptanalysis of a novel image encryption algorithm based on chaos and line map,” *Nonlinear Dynamics*, vol. 87, no. 3, pp. 1797–1807, 2017.

[140] G. Zhou, D. Zhang, Y. Liu, Y. Yuan, and Q. Liu, “A novel image encryption algorithm based on chaos and line map,” *Neurocomputing*, vol. 169, pp. 150–157, 2015.

[141] X. Wu, B. Zhu, Y. Hu, and Y. Ran, "A novel color image encryption scheme using rectangular transform-enhanced chaotic tent maps," *IEEE Access*, vol. 5, pp. 6429–6436, 2017.

[142] C. Zhu and K. Sun, "Cryptanalyzing and improving a novel color image encryption algorithm using rt-enhanced chaotic tent maps," *IEEE Access*, vol. 6, pp. 18 759–18 770, 2018.

[143] Z. M. Z. Muhammad and F. Özkaynak, "Security problems of chaotic image encryption algorithms based on cryptanalysis driven design technique," *IEEE Access*, vol. 7, pp. 99 945–99 953, 2019.

[144] H. Wang, D. Xiao, X. Chen, and H. Huang, "Cryptanalysis and enhancements of image encryption using combination of the 1d chaotic map," *Signal processing*, vol. 144, pp. 444–452, 2018.

[145] R. Huang, X. Liao, A. Dong, and S. Sun, "Cryptanalysis and security enhancement for a chaos-based color image encryption algorithm," *Multimedia Tools and Applications*, vol. 79, no. 37, pp. 27 483–27 509, 2020.

[146] Y. Ma, C. Li, and B. Ou, "Cryptanalysis of an image block encryption algorithm based on chaotic maps," *Journal of Information Security and Applications*, vol. 54, pp. 102566, 2020.

[147] L. Liu, S. Hao, J. Lin, Z. Wang, X. Hu, and S. Miao, "Image block encryption algorithm based on chaotic maps," *IET Signal Processing*, vol. 12, no. 1, pp. 22–30, 2018.

[148] J. M. K. Mastan and R. Pandian, "Cryptanalysis of two similar chaos-based image encryption schemes," *Cryptologia*, vol. 45, no. 6, pp. 541–552, 2021.

[149] A. Beloucif, O. Noui, and L. Noui, "Design of a tweakable image encryption algorithm using chaos-based schema," *International Journal of Information and Computer Security*, vol. 8, no. 3, pp. 205–220, 2016.

[150] Y. Liu, Z. Qin, and J. Wu, “Cryptanalysis and enhancement of an image encryption scheme based on bit-plane extraction and multiple chaotic maps,” *IEEE Access*, vol. 7, pp. 74 070–74 080, 2019.

[151] R. Boriga, A. C. Dăscălescu, and I. Priescu, “A new hyperchaotic map and its application in an image encryption scheme,” *Signal Processing: Image Communication*, vol. 29, no. 8, pp. 887–901, 2014.

[152] W. Wen, Y. Zhang, M. Su, R. Zhang, J.-x. Chen, and M. Li, “Differential attack on a hyper-chaos-based image cryptosystem with a classic bi-modular architecture,” *Nonlinear Dynamics*, vol. 87, no. 1, pp. 383–390, 2017.

[153] R. Davis, “The data encryption standard in perspective,” *IEEE Communications Society Magazine*, vol. 16, no. 6, pp. 5–9, 1978.

[154] C. Sanchez-Avila and R. Sanchez-Reillol, “The Rijndael block cipher (AES proposal) : a comparison with DES,” *Proceedings IEEE 35th Annual 2001 International Carnahan Conference on Security Technology* (Cat. No.01CH37186), pp. 229-234, 2003.

[155] R. Matthews, “On the derivation of a chaotic encryption algorithm,” *Cryptologia*, vol. 8, no. 1, pp. 29–41, 1984.

[156] B. Idrees, S. Zafar, T. Rashid, and W. Gao, “Image encryption algorithm using S-box and dynamic hénon bit level permutation,” *Multimedia Tools and Applications*, vol. 79, no. 9, pp. 6135–6162, 2020.

[157] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish, and M. M. Fouda, “A new image encryption algorithm for grey and color medical images,” *IEEE Access*, vol. 9, pp. 37 855–37 865, 2021.

[158] M. Asim and V. Jeoti, “Efficient and simple method for designing chaotic s-boxes,” *ETRI journal*, vol. 30, no. 1, pp. 170–172, 2008.

[159] S. Picek, L. Batina, D. Jakobović, B. Ege, and M. Golub, “S-box, set, match: a toolbox for s-box analysis,” in *IFIP International Workshop on Information Security Theory and Practice.* Springer, pp. 140–149, 2014.

[160] L. Cui and Y. Cao, "A new s-box structure named affine-power-affine," *International Journal of Innovative Computing, Information and Control*, vol. 3, no. 3, pp. 751–759, 2007.

[161] J. Daemen and V. Rijmen, *The design of Rijndael.* Springer, vol. 2, 2002.

[162] M. T. Tran, D. K. Bui, and A. D. Duong, "Gray s-box for advanced encryption standard," in *2008 international conference on computational intelligence and security*, vol. 1. IEEE, pp. 253–258, 2008.

[163] J. Kim and R. C. W. Phan, "A cryptanalytic view of the nsas skipjack block cipher design," in *International Conference on Information Security and Assurance.* Springer, pp. 368–381, 2009.

[164] E. S. Abuelyman and A.-A. S. Alsehibani, "An optimized implementation of the s-box using residue of prime numbers," *International Journal of Computer Science and Network Security*, vol. 8, no. 4, pp. 304–309, 2008.

[165] X. Yi, S. X. Cheng, X. H. You, and K. Y. Lam, "A method for obtaining cryptographically strong 8/spl times/8 s-boxes," in *GLOBECOM 97. IEEE global telecommunications conference. conference record*, vol. 2. IEEE, pp. 689–693, 1997.

[166] R. Guesmi, M. A. B. Farah, A. Kachouri, and M. Samet, "A novel chaos-based image encryption using dna sequence operation and secure hash algorithm sha-2," *Nonlinear Dynamics*, vol. 83, no. 3, pp. 1123–1136, 2016.

[167] S. Zhu, C. Zhu, and W. Wang, "A new image encryption algorithm based on chaos and secure hash sha-256," *Entropy*, vol. 20, no. 9, pp. 716, 2018.

[168] J. Wu, X. Liao, and B. Yang, "Color image encryption based on chaotic systems and elliptic curve elgamal scheme," *Signal Processing*, vol. 141, pp. 109–124, 2017.

[169] Y. Luo, S. Tang, X. Qin, L. Cao, F. Jiang, and J. Liu, "A double-image encryption scheme based on amplitude-phase encoding and discrete complex random transformation," *IEEE Access*, vol. 6, pp. 77 740–77 753, 2018.

[170] S. Sun, "A novel hyperchaotic image encryption scheme based on dna encoding, pixel-level scrambling and bit-level scrambling," *IEEE Photonics Journal*, vol. 10, no. 2, pp. 1–14, 2018.

[171] I. Hussain, T. Shah, M. A. Gondal, and H. Mahmood, "Analysis of s-box in image encryption using root mean square error method," *Zeitschrift für Naturforschung A*, vol. 67, no. 6-7, pp. 327–332, 2012.

[172] M. Khan, T. Shah, and S. I. Batool, "Construction of s-box based on chaotic boolean functions and its application in image encryption," *Neural Computing and Applications*, vol. 27, no. 3, pp. 677–685, 2016.

[173] M. A. Murillo-Escobar, M. O. Meranza-Castillón, R. M. López-Gutiérrez, and C. Cruz-Hernández, "Suggested integral analysis for chaos-based image cryptosystems," *Entropy*, vol. 21, no. 8, pp. 815, 2019.

[174] N. Whitehead and A. Fit-Florea, "Precision & performance: Floating point and ieee 754 compliance for nvidia gpus," *rn (A+ B)*, vol. 21, no. 1, pp. 18 749–19 424, 2011.

[175] D. I. Curiac and C. Volosencu, "Chaotic trajectory design for monitoring an arbitrary number of specified locations using points of interest," *Mathematical Problems in Engineering*, vol. 2012, 2012.

[176] A. Rehman, X. Liao, A. Kulsoom, and S. A. Abbas, "Selective encryption for gray images based on chaos and dna complementary rules," *Multimedia Tools and Applications*, vol. 74, no. 13, pp. 4655–4677, 2015.

[177] Q. Zhang, L. Guo, and X. Wei, "Image encryption using dna addition combining with chaotic maps," *Mathematical and Computer Modelling*, vol. 52, no. 11-12, pp. 2028–2035, 2010.

[178] C. Fu, B. Lin, Y. Miao, X. Liu, and J. Chen, "A novel chaos-based bit-level permutation scheme for digital image encryption," *Optics Communications*, vol. 284, no. 23, pp. 5415–5423, 2011.

[179] Y. Wu, Y. Zhou, J. P. Noonan, and S. Agaian, "Design of image cipher using latin squares," *Information Sciences*, vol. 264, pp. 317–339, 2014.

[180] J. Choi, S. Seok, H. Seo, and H. Kim, "A fast arx model-based image encryption scheme," *Multimedia Tools and Applications*, vol. 75, no. 22, pp. 14 685–14 706, 2016.

[181] X. Chai, J. Bi, Z. Gan, X. Liu, Y. Zhang, and Y. Chen, "Color image compression and encryption scheme based on compressive sensing and double random encryption strategy," *Signal Processing*, vol. 176, pp. 107684, 2020.

[182] X. Wang, Y. Peng, L. Lu, Z. Lu, M. Bagheri, and R. M. Summers, "Chestx-ray8: Hospital-scale chest x-ray database and benchmarks on weakly-supervised classification and localization of common thorax diseases," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp. 2097–2106, 2017.

[183] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J. P. Noonan, and P. Natarajan, "Local shannon entropy measure with statistical tests for image randomness," *Information Sciences*, vol. 222, pp. 323–342, 2013.

[184] Z. Hua, S. Yi, and Y. Zhou, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Processing*, vol. 144, pp. 134–144, 2018.

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

[186] C. Gamage, J. Leiwo, and Y. Zheng, "Encrypted message authentication by firewalls," in *International Workshop on Public Key Cryptography.* Springer, pp. 69–81, 1999.

[187] H. Y. Jung, D. H. Lee, J. I. Lim, and K. S. Chang, "Signcryption schemes with forward secrecy," *Proceeding of Information Security Application-WISA*, vol. 1, pp. 403–475, 2001.

[188] L. Batina, S. B. Örs, B. Preneel, and J. Vandewalle, "Hardware architectures for public key cryptography," *Integration*, vol. 34, no. 1-2, pp. 1–64, 2003.

[189] X. Wang and P. Liu, "A new image encryption scheme based on a novel one-dimensional chaotic system," *IEEE Access*, vol. 8, pp. 174 463–174 479, 2020.

[190] R. R. Suman, B. Mondal, S. K. Singh, and T. Mandal, "A secure color image encryption scheme based on chaos," in *Machine Vision and Augmented IntelligenceTheory and Applications.* Springer, pp. 365–375, 2021.

[191] S. Rajendran, K. Krithivasan, and M. Doraipandian, "A novel cross cosine map based medical image cryptosystem using dynamic bit-level diffusion," *Multimedia Tools and Applications*, vol. 80, no. 16, pp. 24 221–24 243, 2021.

[192] C. Li, L. Wang, D. Yan, and H. Shi, "Research on a new type of chaotic image encryption algorithm combining dna operation and s-box," in *2021 International Conference on Neuromorphic Computing (ICNC).* IEEE, pp. 359–367, 2021.

[193] E. H. Rachmawanto, R. Zulfiningrum *et al.*, "Medical image cryptosystem using dynamic josephus sequence and chaotic-hash scrambling," *Journal of King Saud University-Computer and Information Sciences*, 2022.

[194] H. Shi, D. Yan, L. Wang, and S. Duan, "A novel memristor-based chaotic image encryption algorithm with hash process and s-box," *The European Physical Journal Special Topics*, pp. 1–16, 2021.

[195] H. Guler, "Real-time fuzzy-pid synchronization of memristor-based chaotic circuit using graphical coded algorithm in secure communication applications," *Physica Scripta*, vol. 97, no. 5, pp. 055212, 2022.

[196] G. Ghosh, S. Verma, N. Jhanjhi, M. Talib *et al.*, "Secure surveillance system using chaotic image encryption technique," in *IOP conference series: materials science and engineering*, vol. 993, no. 1. IOP Publishing, pp. 012062, 2020.

[197] A. Pourjabbar Kari, A. Habibizad Navin, A. M. Bidgoli, and M. Mirnia, "A novel multi-image cryptosystem based on weighted plain images and using combined chaotic maps," *Multimedia Systems*, vol. 27, no. 5, pp. 907–925, 2021.

[198] B. Ahuja and R. Doriya, "Patients medical data security via bi chaos bi order fourier transform," in *Data Science.* Springer, pp. 25–39, 2021.

[199] A. Mashat, S. Bhatia, A. Kumar, P. Dadheech, and A. Alabdali, "Medical image transmission using novel crypto-compression scheme," *Intelligent Automation and Soft Computing*, vol. 32, no. 2, pp. 841–857, 2022.

[200] I. Q. Abduljaleel and A. H. Khaleel, "Hide medical images in a speech signal using DNA coding and fuzzy c-means," in *2020 2nd Annual International Conference on Information and Sciences (AiCIS).* IEEE, pp. 119–126, 2020.