A
Major Project Report
On

Enhanced Multi Chaotic Systems Based Pixel Shuffling for Encryption

Submitted in partial fulfilment of the requirements

for the award of the degree of

Master of Technology
In
Information Systems

Submitted By:

MUNAZZA NIZAM

Roll No. 07/IS/2010

Under the Guidance of

Prof. O. P. Verma

(HOD, IT Department)

Department of Information Technology

DELHI TECHNOLOGICAL UNIVERSITY

Bawana Road, Delhi-110042

2010-2012

CERTIFICATE

This is to certify that **Ms. Munazza Nizam (07/IS/2010)** has carried out the major project titled **"Enhanced Multi-Chaotic Systems Based Pixel Shuffling for Encryption"** as a partial requirement for the award of Master of Technology degree in Information Systems by Delhi Technological University.

The major project is a bonafide piece of work carried out and completed under my supervision and guidance during the academic session 2010-2012. The matter contained in this report has not been submitted elsewhere for the award of any other degree.

Prof. O. P. Verma

(Project Guide)

Head of Department

Department of Information Technology

Delhi Technological University

Bawana Road, Delhi-110042

ACKNOWLEDGEMENT

It's true and proved that behind every success, there is certainly an unseen power of Almighty Allah, He is the grand operator of all projects.

First of all, I thank my parents who have always motivated me and given their blessings for all my endeavors.

I take this opportunity to express my profound sense of gratitude and respect to all those who helped me throughout the duration of this project. I would like to express my sincere gratitude to Prof. O.P. Verma, HOD, IT Dept., Delhi Technological University, for his invaluable guidance and cooperation extended during the pursuit of my project work. I would also like to thank Mr. Musheer Ahmad, Assistant Professor, Computer Engineering Dept., Jamia Millia Islamia University to provide me guidance and helping me throughout this project work.

I humbly extend my most grateful appreciation to my sisters and friends for their support, in particular Faraz Alam, Prerana Yadav and Reena Negi who have done everything possible to help me complete my project. They have been my source of inspiration and without their love and support I would not have been able to reach this place.

Munazza Nizam

Roll No. 07/IS/2010

M.Tech (Information Systems)

Department of Information Technology

Delhi Technological University

Bawana Road, Delhi-110042

Abstract

The problem of secure transmission of digital media is addressed and dealt using the chaotic systems. The system of chaotic maps are considered a very interesting complex nonlinear phenomenon in the last four decades. Encryption of data is the most prevalent technique used for the transmission of highly sensitive information. This is achieved by using the chaotic maps for shuffling the image bits in order to increase randomness and confusion among the pixels of image. We have performed color image encryption using the chaotic maps by exploiting its intrinsic features. A set of four chaotic maps namely Hénon map(discrete time), Lorenz (butterfly attractor), Chua (double scroll attractor) and Rössler (spiral attractor) are used and the chaotic sequences generated by them acts as the key to the cryptosystem. We have proposed a new shuffling pattern of plaintext image bits using the information contained in the image and design a scheme for the resistance to two differntial attacks, chosen-ciphertext attack(CCA) and known-plaintext attack(KPA). The method first preprocesses the plaintext color image to convert it into binarized form, and then evaluate the number of binary 1s in the image. Now, the encryption scheme makes use of this information to generate the chaotic sequences. A completely different set of sequences is generated for different plaintext images. The indices of the chaotic sequences are used for the encryption of RGB image by shuffling the bits of the three components columnwise and then rowise in a pair of two bits. The dependence of chaotic sequences on the original image makes the scheme resistant to the attacks. Thus, by analyzing any plain/cipher image pairs one cannot deduce the key of the cryptosystem.In order to perform the statistical measure, Number of Pixel Change Rate (NPCR), UACI (Unified Average Changed Intensity) , histogram analysis, information entropy and correlation coefficient are used as parameters to evaluate the performance of the proposed method. It is also shown that the ciphered image is very sensitive to a slight change in the bit values of original image. Eventually, empirical images and results are used to prove the higher security and performance of the proposed approach over the existing algorithm.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF SYMBOLS

$x = x\ coordinate\ of\ 3D\ map$

$y = y\ coordinate\ of\ 3D\ map$

$z = z\ coordinate\ of\ 3D\ map$

$x_0 = Initial\ value\ of\ x\ coordinate$

$y_0 = Initial\ value\ of\ y\ coordinate$

$z_0 = Initial\ value\ of\ z\ coordinate$

$\dot{x} = \ Diffrential\ of\ x\ with\ respect\ to\ time$

$\dot{y} = \ Diffrential\ of\ y\ with\ respect\ to\ time$

$\dot{z} = \ Diffrential\ of\ z\ with\ respect\ to\ time$

$\sigma = Prandtl\ number$

$\gamma = Rayleigh\ number$

$x_n = nth\ value\ of\ x\ coordinate$

$y_n = nth\ value\ of\ y\ coordinate$

$m = Number\ of\ rows\ in\ the\ image$

$n = Number\ of\ columns\ in\ the\ image$

$N = Total\ number\ of\ pixels\ in\ the\ image$

$\omega = Total\ number\ of\ 1s\ in\ the\ color\ image$

$\varphi = Total\ iterations\ of\ the\ chaotic\ map$

$X_1 to\ X_4 = Chaotic\ sequences\ in\ x\ direction$

$Y_1 to\ Y_4 = Chaotic\ sequences\ in\ y\ direction$

$Z_1 to\ Z_4 = Chaotic\ sequences\ in\ z\ direction$

$Fx_1\ to\ Fx_4 = Sorted\ indexing\ sequence\ of\ x\ coordinates$

$Fy_1\ to\ Fy_4 = Sorted\ indexing\ sequence\ of\ y\ coordinates$

$Fz_1\ to\ Fz_4 = Sorted\ indexing\ sequence\ of\ z\ coordinates$

$\mu = Pixel\ number$

$\Psi ergb_{\mu i} = Column\ shuffled\ RGB\ level\ matrix$

$S = Source\ image$

$H(S) = Entropy\ of\ source\ image$

$p(s_i) = Probability\ of\ symbol\ s_i$

$T = Largest\ supported\ pixel\ value$

$N = Number\ of\ Pixel\ Change\ Rate$

$U = Unified\ Averaged\ Change\ Intensity$

$C, C_1, C_2 = Ciphered\ images$

$P, P_1, P_2 = Plaintext\ images$

$\rho = Correlation\ Coefficient$

Chapter 1

Image Encryption

1.1 Introduction

In cryptography, **encryption** is the process of transforming any information into forms that are unreadable to anyone except those possessing the right to access that information. In other words we can say that encryption is the manipulation of data, based on a password (also known as a key), for security purposes. The raw information in its understandable form is called as **plaintext** that is converted into its ciphertext by applying certain algorithms and key using the steps of encryption. The result of the process is encrypted information in cryptography is referred to as **ciphertext**. The process, the algorithms and the techniques, including hardware and software used in the encryption should be difficult to attack by an attacker. The reverse process of making the encrypted information in readable and understandable forms is known as **decryption**.

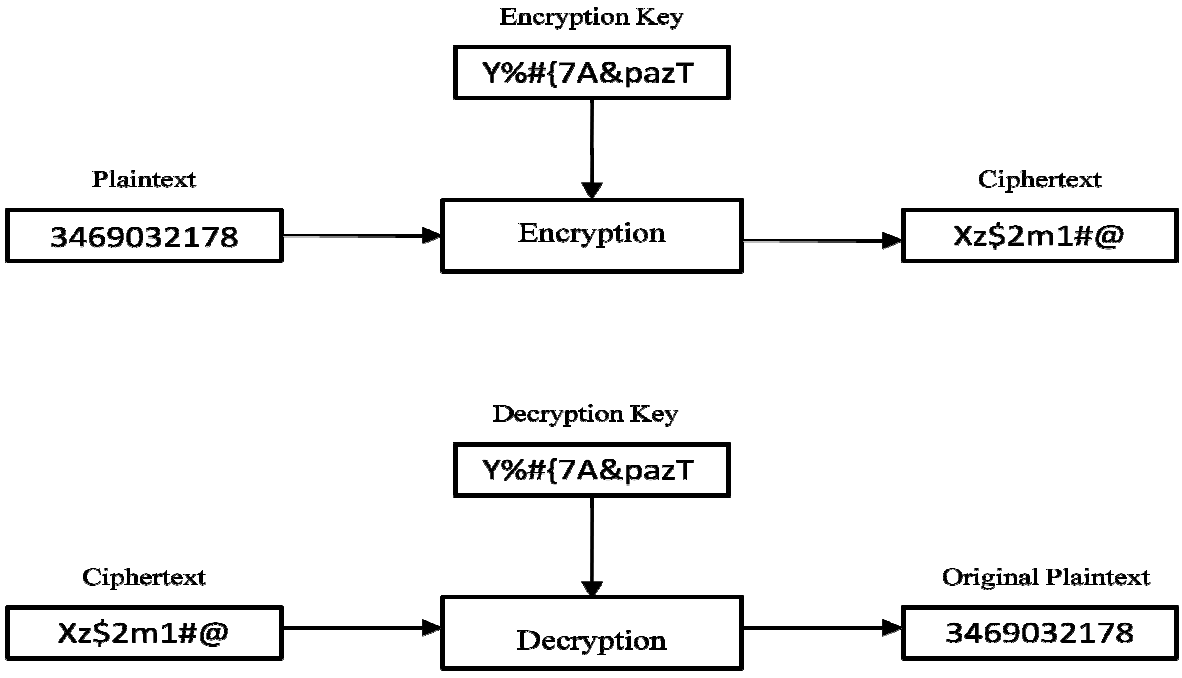


Fig.1.1: General Flowchart of Encryption-Decryption Process

Data to be protected can be static such as stored in files, disks, databases or can be transferred via networks (e.g. the Internet, e-commerce), mobile telephones, wireless microphones, wireless intercom systems, bluetooth devices.

Encryption is one of the widely used techniques to safeguard the secrecy of important content. Encrypting data while transmission is helpful as it is difficult to secure access to networks. Encryption technique can be applied to any data and information that are sensitive and cannot be revealed to others without authorization.

With the rapid advancement in internet and multimedia technology, great number of researchers and scientists have made various attempts to solve the issue of data security and integrity by incorporating the data with several encrypton and decryption algorithms. The prevalence of multimedia technology has promoted digital images to play a more significant role than the traditional texts, which demand serious protection of users' privacy for all applications. It is the utmost requirement of important data to be protected from fabrication and illegal access. Encryption is the transformation of any information like text, audio, video, images, etc into forms that protects it against illegal copying. The encrypted information is called the cipher text or image. The process, the algorithms and the techniques, including hardware and software used in the encryption should be difficult to decode. The core idea behind encryption is to convert the valuable or private information that can only be understood after decryption by the correct key. A good encryption/decryption technique does not distort the valuable and important content and is resistant to various attacks.

1.2 Cryptography and Cryptanalysis

Cryptography is the art and science of protecting information from undesirable individuals by converting it into a form non-recognizable by its attackers while stored and transmitted. Data cryptography mainly is the scrambling of the content of data, such as text, image, audio, video and so forth to make the data unreadable, invisible or unintelligible during transmission or storage called Encryption. The main goal of cryptography is keeping data secure form unauthorized attackers. The reverse of data encryption is data Decryption, which recuperate the original data.

Cryptanalysis is the study of methods for obtaining the meaning of encrypted information, without access to the secret information that is normally required to do so. Typically, this involves knowing how the system works and finding a secret key.

1.3 Types of Cryptographic Attacks

There are different types of cryptographic attacks depending upon the type of information utilized for the secret key determination. Three attacks are based on plaintext and three are based on ciphertext. They form the very foundation of the Known Plaintext Attacks and Ciphertext Only Attacks.

1.3.1 Known Plaintext and Ciphertext-Only Attack:

Known Plaintext is an attack when a cryptanalyst has access to plaintext-ciphertext pair and he discovers the relation between them.

In Ciphertext Only attack the cryptanalyst has access to ciphertext only. Through frequency analysis the key of the encryption is deduced.

1.3.2 Chosen Plaintext and Chosen Ciphertext Attacks

In Chosen Plaintext attack, the cryptanalyst can encrypt a plaintext of his choice and analyze its corresponding ciphertext for key determination.

A chosen ciphertext attack is an attack where a cryptanalyst chooses a ciphertext and attempts to find a matching plaintext.

1.3.3 Adaptive Chosen Plaintext and Adaptive Chosen Ciphertext Attacks

In case of Adaptive Chosen Plaintext Attacks and Adaptive Chosen Ciphertext Attacks the plaintext or ciphertext is chosen adaptively based on prior results.

1.3.4 Side Channel Attacks

In cryptography Side Channel Attack refers to breaking the cryptosystem using the hardware and physical implementation of the cryptosystem rather using the plaintext-ciphertext of the encryption process. It requires the technical knowledge of the internal operation involved in the cryptosystem. These are mostly based on statistical analysis of the cryptosystem.

1.3.5 Brute Force Attacks

A Brute Force Attack is to try all the possible combination of keys to break the cryptosystem. It involves making an exhaustive search for the key. This type of attack is feasible only when the key space is small and the attacker can try all the possible combination in less time. An encryption system with larger key space is robust against these types of attacks.

1.4 Cryptographic Services

Every encryption system must provide security services that assure the secrecy of information. The different security services that an efficient cryptosystem must provide are:

1.4.1 Authentication: When there is a communication, then the sender and the receiver must verify the identity of each other before starting the transfer of information. Therefore there must be some way in which the sender and receiver can prove their identity to make sure that they are communicating with the right person and not with any imposter. This process is called user authentication.

1.4.2 Secrecy or Confidentiality: The cryptosystem must be efficient enough to maintain the secrecy of the system. It should allow only the authenticated people to access and interpret the message.

1.4.3 Integrity: Integrity implies that the content of the information should not be tampered and altered during the transmission between the sender and the receiver.

1.4.4 Non-Repudiation: This function implies that neither the sender nor the receiver can falsely deny that they have sent a certain message.

1.4.5 Service Reliability and Availability: The cryptosystem must provide assured services by being available all the time, since systems usually get attacked by intruders, which may affect their availability and type of service to their users

1.5 Related work

One of the growing data protection technique is encryption. Traditional image encryption techniques used for encryption are International Data Encryption Standard (IDEA),

Advanced Encryption Standard (AES) and Data Encryption Standard (DES). These are block cipher techniques that encrypt the data in blocks of fixed size and are very complicated. They involve large rounds of encryption and key generation along with time consuming computations. The vast amount of data generated by multimedia applications does not allow a software DES implementation to process them fast enough and a hardware DES implementation (a set-top box) adds extra costs both to broadcasters and to receivers. AES is comparatively faster symmetric block algorithm . These encryption algorithms were mainly designed to encrypt texts, and images are different from text. Although we can use the traditional cryptosystems to encrypt images directly but it has its own disadvantages. One is that the image size is almost always much greater than that of text [1, 2]. Therefore, the traditional cryptosystems need much time to directly encrypt the image data. The other problem is that the decrypted text must be equal to the original text. However, this requirement is not necessary for image data. Due to the characteristic of human perception, a decrypted image containing small distortion is usually acceptable. In order to transmit secret images to other people, a variety of encryption schemes have been proposed [3-8]. These schemes have structural complexity with a number of encryption-decryption rounds, the secret key singleness and the encryption speed is very slow that it becomes difficult to encrypt images that have a lot of data. So using the conventional encryption solely is not enough.

To overcome this challenge, variety of image encrytion techniques have been proposed in the literature. Among them, chaos based encryption techniques has gained special attention due to its intrinsic features like stochasticity, dynamic behaviour and sensitivity to initial conditions. Chaos based image encryption algorithm was first proposed in 1989 [9] by R. Matthews. The highly sensitive response of chaotic system to the initial value conditions and variation in parameters makes the chaotic trajectory so unpredictable that a great number of researches implement chaotic sequences to perform encryption of images that are transmitted heavily over the communication network.

In 2005, L.Zhang *et al.* [10] proposed a scheme to resist differential attack by first analysing the performance of discrete exponential chaotic map and then permuting the pixels of the

image. A video encryption method based on chaotic maps in discrete cosine transform(DCT) domain is presented in [11].

Two coupling chaotic maps were employed to scramble the DCT coefficient of the original frame and to encrypt the DCT coefficient of the scrambled frame respectively.

One dimensional chaotic cryptosystem have the drawbacks of small key space and weak security.Chong Fu *et al.* [12] proposed a 3D encryption system based on Lorenz maps over existing one dimensional chaos based encryption techniques. A new encryption scheme was recommended in [13] which also employed 3D chaotic systems for confusion and diffusion in the cipher image. It has the advantage of bigger key space and smaller iteration times. In [14], an approach was designed to resist chosen-plain-text cryptanalysis and to protect secrecy of digital image.

Many encryption algorithm has been proposed that uses chaotic maps for encryption as their basic tool [15-20] as chaos based methods gives strong encryption strength. In [21], a scheme for encrypting color images was proposed to increase confusion and diffusion among pixels. It was based on chaotic-maps and genetic operations as tools. The sequences were controlled by parameters and given initial values which were considered the key for the encryption technique.

In [22], a cryptosystem is proposed that exploits the ergodic property of the simple low-dimensional and chaotic logistic equation. However there were certain drawbacks that were removed in [23] by a chaos-based cryptosystem with adjustable sensitivity on initial conditions. A non linear chaotic algorithm (NCA) was proposed [24] to get over the drawbacks of one-dimensional linear logistic maps that provided small key spaces and weak security levels [25, 26]. The algorithm employed non linear functions such as tangent function and power function with improved larger key space and high-level security.

In [27], Qiang Wang *et al* performed research on digital image encryption based on Discrete Wavelet Transform (DWT). A digital watermark algorithm based on DWT and chaos theory was developed. This technique promoted the resistance on JPEG compression, noise attack, filter and so on.

Yong-Hong Zhanghas designed and developed an image encryption [28] using extended chaotic sequences. In this study the extended chaotic processes are generated by using the n - rank rational Bezier curve. High key space and good security level was achieved.

1.6 Applications

- Image encryption has applications in internet communication, multimedia systems, and military communication medical and military imaging systems**.**
- Investigation Bureau, Defense services, E-Mail services transmit their data in the form of text, audio, video, images, etc in encrypted form.
- Sensitive information like credit cards, banking transactions and social security numbers need to be protected.

Chapter 2

The Chaotic Maps

2.1 History of Chaos

Chaos can be defined as any state of disorder, disarray, or randomness; however it has a much detailed meaning and significance when dealt scientifically.

The first person to discover a chaotic deterministic system that laid the foundation of modern chaos theory was Henri Poincaré in late 1800s. Although, Poincaré first noticed the possibility of chaos system, Lorenz was the first one to discover the chaotic motion in 1963. He developed equations to predict the weather conditions through rolls in the atmosphere. Lorenz found that his equations continued to oscillate in an irregular pattern, and that if he changed his initial conditions, the results would be completely different. However, there was some order when these equations were plotted in three dimensions. This happened in the early 1960s whereas the mathematical understanding of chaos came into full swing by 1970s.

The term 'chaos' was first coined by James Yorke and T.Y. in 1975 in their paper, "Period Three Implies Chaos". Yorke was also the first person to attempt to mathematical define chaos; he did this in the 1970s. Some other contributors to the rise of popularity in chaos include Ruelle and Takens, May, and Feigenbaum.

There are a number of examples involving chaotic behavior as in economics, fluid dynamics, optics, chemistry, changing weather, and even in the swirling patterns of cream being stirred into a cup of coffee. One of the most unique examples pertains to a butterfly flapping its wings that led to the most popular phenomenon known as the butterfly effect. Chaos can be used to manipulate and create something that is very important in this era of fast multimedia technology. One such example is that of encryption. Chaos theory has played a major role in presenting a completely different aspect for encryption techniques as they gives randomness with stochasticity.

2.2 Types of Chaotic Maps

Chaotic maps often generate fractals. There are various examples of chaotic maps based on their time domain, space domain and number of space dimensions. Some of them are listed in Table 2.1.

Table 2.1: List of Chaotic Maps

Map Name	Time Domain	Space Domain	Number of Space Dimensions
Arnold's cat map	Discrete	Real	2
Baker's map	Discrete	Real	2
Circle map	Discrete	Real	1
Complex Quadratic map	Discrete	Complex	1
Guass map	Discrete	Real	1
Hénon map	Discrete	Real	2
Logistic map	Discrete	Real	1
Lorenz attractor	Continuous	Real	3
Rössler map	Continuous	Real	3
Van der Pol Oscillator	Continuous	Real	1

2.2.1 Lorenz Map (Butterfly Attractor)

As previously mentioned, in 1960s Edward Lorenz was working on the equations that could predict the weather conditions. He discovered the three dimensional real and continuous equation dependent on some initial values and parameters. The maps generated from Lorenz equation were very sensitive as the patters would change dramatically when the initial

conditions $x_0, y_0 \; and \; z_0$ were varied. These gave a new direction to chaotic maps as a great degree of randomness was generated with very sensitive initial conditions.

The set of Lorenz differential Equations are:

$$\dot{x} = -\sigma x + \sigma y \tag{2.1}$$

$$\dot{y} = -xz + \gamma y - y \tag{2.2}$$

$$\dot{z} = xy - bz, \tag{2.3}$$

Here σ, γ, and b are parameters, where σ is the Prandtl number and γ is the Rayleigh number.

A strange attractor is an attractor that exhibits sensitive dependence on initial conditions. An attractor is what the behavior of a system settles down to or is attracted to. Although the chaotic dynamical system does not ever set into a certain pattern or converge to a certain point it does develop a pattern once it is plotted in three dimensions. The shape that forms corresponds to unpredictable motions, and therefore there is not a set cycle or pattern. The Lorenz equations provide the most common example of a strange attractor, the Lorenz attractor.

All attractors have an underlying shape; the Lorenz attractor's shape is referred to as a butterfly, and it can be seen in Fig. 2.1.

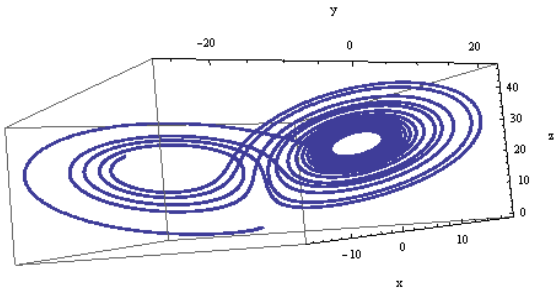


Fig. 2.1: Lorenz Attractor with $\sigma = 10, b = \frac{8}{3} and \; \gamma = 28$

2.2.2 Hénon Map

The first simple equation in which the fractal structure is easily observed was given through Hénon map. It was based on the idea of return maps. These are the set of very simple non linear difference equations. The **Hénon map** is a discrete-time dynamical system. The map was introduced by Michel Hénon as a simplified model of the Poincaré section of the Lorenz model. It is one of the most common and significant example to study the chaotic behavior of dynamical systems. The Hénon map takes a point (x_n, y_n) in the plane and maps it to a new point.

The equations for Hénon map can be given as:

$$x_{n+1} = y_n + 1 - ax_n^2 \tag{2.4}$$

$$y_{n+1} = bx_n \tag{2.5}$$

where the parameters a and b were chosen as a = 1.4 and b = 0.3 by Hénon (1976). The Hénon attractor is shown in Fig. 2.2 and is computationally cheap, requiring no more than the simplest algebraic operations.

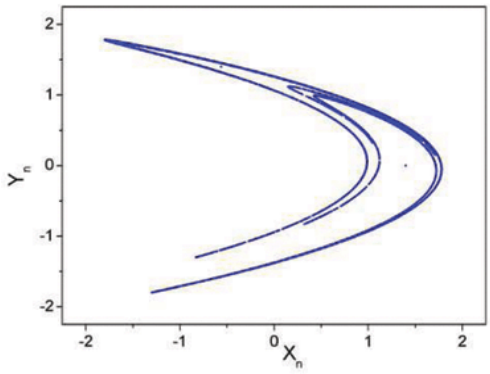


Fig. 2.2: Chaotic attractor for Hénon Map with parameters values $a = 1.4$ *and* $b = 0.3$

2.2.3 Rössler Map (Spiral Attractor)

Rössler systems were introduced in the 1970s as prototype equations for continuous time chaos. Rössler was motivated by the reinjection principle and the three dimensional geometrical flows. **Rössler system** is a system of three non-linear ordinary differential equations defining a continuous-time three dimensional equations. These differential equations exhibit chaotic behavior with the fractal properties of the attractor. The three dimensional attractor is shown in Fig. 2.3.

The equations are described as:

$$\dot{x} = -(y + z) \tag{2.6}$$

$$\dot{y} = x + ay \tag{2.7}$$

$$\dot{z} = b + z(x - c), \tag{2.8}$$

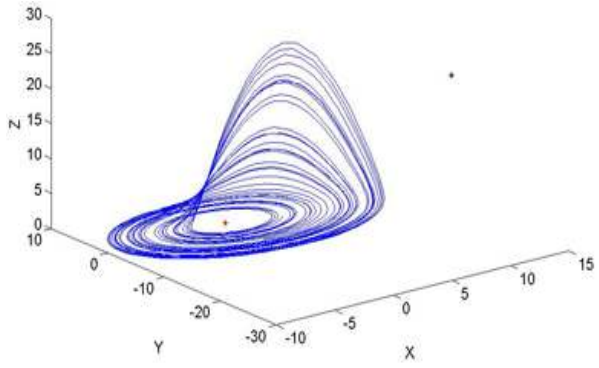


Fig. 2.3: Rössler attractor with $a = 0.2, b = 0.2$, and $c = 5.7$.

This system shows chaotic characteristics as there is a quadratic term in the equation, its phase space has three dimensions and it generates a chaotic attractor with a single lobe. It is less chaotic in nature when compared to the Lorenz attractor since Lorenz attractor has two lobes.

2.2.4 Chua Map (Double Scroll Attractor)

The Chua's attractor is also known as double scroll attractor. The double scroll attractor is often described by a system of three nonlinear ordinary differential equations. The state equations below describe a Chua oscillator that generates even or odd number of scrolls depending upon the values of the parameters:

$$\dot{x} = \propto \big(y - x - h(x)\big) \tag{2.9}$$

$$\dot{y} = x - y + z \tag{2.10}$$

$$\dot{z} = -\beta y - \gamma z \tag{2.11}$$

$$h(x) = m_{2q-1}x + 0.5\sum_{i-1}^{2q-1}(m_{i-1} - m_i)(|x + c_i| |x - c_i|), \tag{2.12}$$

where q is a natural number and m and c are two vectors:

$m = [m_0, m_1, \ldots\ldots, m_{2q-1}]$ and $c = [c_0, c_1, \ldots\ldots, c_{2q-1}]$.

According to Sukyens *et al.*(1997) and Yalcin *et al.*(2000), n-scroll attractors are generated when:

$\propto = 9,\ \beta = 14.286, \gamma = 0.0385.$

Different parameter values in the h function produce different number of scrolls.

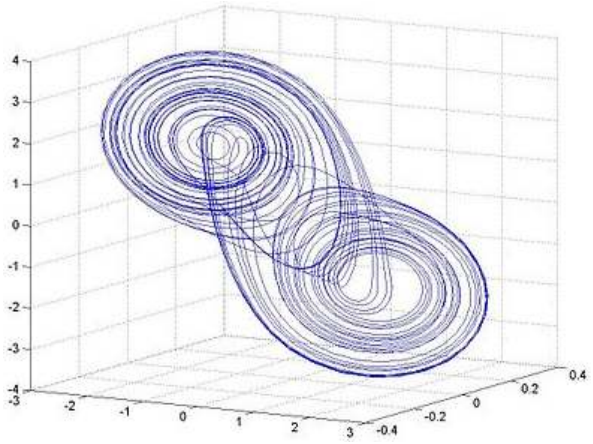


Fig. 2.4: Chua's Double Scroll attractor

2.3 Role of Chaotic Maps in Encryption

With the advent of captivating developments in digital image processing and digital media communications, a great demand for a secure real-time transmission of data over networks has been created. A variety of encryption techniques has been evolving ever since to meet this challenge [29, 30]. The images have some intrinsic properties such as high correlation among pixels and large amount of information that does not allow the traditional encryption algorithms such as DES, IDEA and RSA to meet the criteria for encryption of practical image. Among the proposed scheme for encryption, the chaos based algorithms have shown some exceptionally good properties in many concerned aspects regarding security, complexity, speed, computing power and computational overhead, etc. the most important property is the sensitivity of chaotic systems to initial conditions and control parameters. There are many other features of chaos systems that make them more efficient for encryption. Such as the traditional encryption algorithms show sensitivity to keys of cryptosystem, whereas chaotic maps are sensitive to initial conditions and parameters; there are different rounds to introduce diffusion and confusion among pixels in classical encryption system while chaotic maps perform iterations to spread the initial region over the entire phase spaces. One of the most striking differences between the two is that, in case of traditional system, the encryption operations are defined on finite sets, while in chaos based system, mathematical sense is defined on real numbers. Chaos-based cryptosystem can be one-dimensional, two dimensional or three-dimensional. One-dimensional chaotic maps are generally used for the generation of the encryption key [31, 32]. Shuffling of image pixels are done according to this key. The image is represented as a 2D matrix; therefore some encryption algorithms use two-dimensional maps. Three dimensional chaotic maps are generally used for color images with three components to be encrypted.

2.4 Salient features of Chaotic Maps

The chaotic maps exhibit features that make them significant in various fields. Some of them are listed below:

- Period 3 region.

- Chaotic systems show self-similarity or fractal behaviour.
- Sensitive Dependence on Initial Conditions (SDOIC) – points that start off close together can be widely separated at a later time (also referred to as "mixing").
- A small difference in the value of parameters or initial conditions can make a huge difference in the outcome of the system at generation ("butterfly effect").
- No formula can tell us what *x* will be at some specified generation *n* even if we know the initial conditions (where *x* is value of coordinate at some *nth* iteration)
- The system is unpredictable.

Although one-dimensional chaotic system enjoys the advantages of high-level efficiency and simplicity, such as Logistic map, it has the weakness of small key space and weak security. Chaotic systems have many important properties as listed above, such as the sensitive dependence on initial conditions and system parameters, pseudorandom property, no periodicity and topological transitivity, etc. The properties make the cryptosystem efficient by meeting the requirements such as diffusion and mixing in the sense of cryptography. Therefore, chaotic cryptosystems have more useful and practical applications.

2.5 Examples of Chaos:

- Laser instabilities.
- Fluid turbulence.
- Progression to heart attack.
- Population biology.
- Weather.

Chapter 3

Proposed Approach

3.1 Motivation

Although chaotic system provides some ideal cryptographical properties as confusion, diffusion, balance and avalanche, it cannot be considered completely robust against differential attacks. The cryptosystem proposed in [33] applied cipher-block chaining (CBC) encryption and was penetrable to chosen ciphertext attack (CCA) and chosen plaintext attack (CPA) since the keystream generated for every plaintext image was identical. This was cryptanalyzed by Rhouma [34] and in order to make the cryptosystem robust against CCA and CPA, the keystream was updated in a way to depend directly on the plaintext that is to be encrypted.

In 2009 C. K. Huang and H. H. Nien [35] proposed Pixel Chaotic Shuffle (PCS) encryption system that was purely based on pixel shuffling using the chaotic sequences generated by multi-chaotic maps. These sequences act as the key for the cryptosystem to perform vertical and horizontal shuffling of the plaintext image bits. However, Rhouma *et al.*[36] broke the encryption scheme successfully by cracking the sorting sequences that are the keys of the cryptosystem. This was due to the reason that the chaotic sequence used for shuffling of the plaintext image bits neither depend on the plaintext image nor on ciphertext image and the key was same for all plaintext image. By analyzing the plain-ciphered image pair one can deduce the key sequences making the scheme prone to chosen plain-text attack and known-plaintext attack. Thus in order to make PCS cryptosystem robust to aforesaid attacks, we propose a cryptosystem to achieve a more secure encryption technique.

3.2 Key Aspects of Proposed Encryption Algorithm

Our approach focuses on two important security aspects, namely **confusion** and **diffusion.** Confusion refers to making the relationship between the ciphertext and key as complex as possible. Diffusion is the property that dissipates the redundancy in the statistics of the plaintext to the statistics of the ciphertext. The values in the plaintext should be diffused

in the ciphertext so that the relation between the two becomes complicated. This is done to prevent differential attacks.

The proposed approach makes sure that these two key properties of cryptography are achieved. An encryption technique with good diffusion property is proposed, in which if pixel intensity of one of the image pixel is altered, then the ciphertext changes completely. For making the relationship between key and ciphertext complex, the keystream is made dependent on the plaintext. The keystream is the chaotic sequences that are used for encryption of the color image. The keystream generated for encryption process is very sensitive to the initial conditions and parameters that it is very hard to find the key even if one has a large number of plain-cipher image pairs. Each cipher image depends on the plain image for the keystream. Therefore, changing one pixel of the plain image changes the cipher image completely.

We propose a scheme to make the keystream dependent on the plaintext image that is to change the generated chaotic-sequence with the changing plaintext image. An improved shuffling pattern of the bits of plain image using the information contained in the image is designed for the resistance to chosen-ciphertext attack (CCA) and known-plaintext attack (KPA). The method generates different chaotic sequences for different plain images. The indices of the chaotic sequences are used for the encryption of RGB image by shuffling the bits of the three components columnwise and then row-wise in a pair of two bits. The dependency of the chaotic sequences on the original image makes the scheme resistant to the attacks.

3.3 Description of the PCS encryption algorithm [35]

The PCS encryption scheme uses four 3D chaotic maps for pixel shuffling. These chaotic maps are iterated to generate 12 random sequences. The indices of the sequences are used to map the plaintext image bits. The encryption is executed in two steps. In the first step the bits of plaintext image are shuffled among themselves using column wise shuffling and in the second stage the bits are rearranged within pixels of the image using row wise shuffling. Each color component is shuffled separately using the chaotic sequences.

3.3.1 Weaknesses in the PCS Scheme

The cryptanalysis performed in [36] on the cryptosystem [35] shows that the scheme is prone to two different attacks namely chosen ciphertext attack and known-plaintext attack. This weakness arises from the fact that same shuffling indices is used to shuffle the plaintext images without taking into account the plaintext image for sequence generation. Thus the mapping of the pixel bits were same for all plaintext images. A slight change in the pixel values of original image produces negligible change in the respective encrypted image, thus making the encrypted image easy to comprehend by analyzing pairs of (plain/ciphered) images .

Another drawback of PCS encryption originates as the RGB components of the image are encrypted separately using the x, y and z chaotic sequences of the maps thereby decreasing the randomness of bits in encrypted image. The CCA and KPA are unresistant since the attacks are employed on the 8-bit pixels of each of the color component of the image using the four chaotic sequence generated by the chaotic maps. Decoding of the pixel values of the RGB components separately needs lower computation and lesser time consumption.

3.4 Proposed Enhanced Multi Chaotic Systems Based Pixel Shuffling Scheme

In this section we propose a modified version of the cryptosystem presented in [35] with similar basic description and values of the parameters. The modification is performed to deal with the drawbacks mentioned in Section 3.1. The chaotic maps are generated in a way so that it extracts information from the plain image and utilizes it to generate mapping sequences. Thus an entirely different mapping sequence is used for shuffling each plain image. Further the bits of the RGB components are permuted to increase the randomness and confusion among pixels. Finally column wise and row wise shuffling is performed to render the image totally unrecognizable and unpredictable.

3.4.1 The Chaotic Maps used in the Algorithm

The proposed pixel shuffling method for color image encryption is based on multiple three dimensional chaotic systems like the Hénon, the Lorenz, the Chua and the Rössler systems

having great encryption performance. The chaotic maps show chaotic behavior only for a set of values of the parameters that are obtained experimentally. This makes the chaotic systems very sensitive to initial conditions of parameters.

The 3D chaotic maps with coordinates x, y and z used in the proposed cryptosystem and the values of the parameters used in the algorithm are as follows [35]:

(1) Hénon map (discrete time):

$$x(k+1) = a - y^2(k) - bz(k) \tag{3.1}$$

$$y(k+1) = x(k) \tag{3.2}$$

$$z(k+1) = y(k), \tag{3.3}$$

where $a = 1.76$ and $b = 0.1$.

(2) Lorenz (butterfly attractor):

$$\dot{x} = -\sigma x + \sigma y \tag{3.4}$$

$$\dot{y} = -xz + \gamma y - y \tag{3.5}$$

$$\dot{z} = xy - bz \tag{3.6}$$

where $\sigma = 16, \gamma = 40$ and $b = 4$.

(3) Chua (double scroll attractor):

$$\dot{x} = \propto \big(y - x - h(x)\big) \tag{3.7}$$

$$\dot{y} = x - y + z \tag{3.8}$$

$$\dot{z} = -\beta y - \gamma z \tag{3.9}$$

$$h(x) = m_1 x + 0.5(m_0 - m_1)(|x+1| |x-1|), \tag{3.10}$$

where $\propto = 10,\ \beta = 14.78, \gamma = 0.0385, m_0 = -1.27,$ and $m_1 = -0.68$.

(4) Rössler (spiral attractor):

$$\dot{x} = -(y + z) \tag{3.11}$$

$$\dot{y} = x + ay \tag{3.12}$$

$$\dot{z} = b + z(x - c), \tag{3.13}$$

where $a = 0.2, b = 0.2$, and $c = 5.7$.

3.4.2 Initial value conditions of the Chaotic Maps

3.4.2.1 Hénon Map

(a) Initial value of $x_0 = 1.0$

(b) Initial value of $y_0 = 1.5$

(c) Initial value of $z_0 = -1.2$

3.4.2.2 Lorenz Map

(a) Initial value of $x_0 = 0.1$

(b) Initial value of $y_0 = 0.6$

(c) Initial value of $z_0 = 10$

3.4.2.3 Chua Map

(a) Initial value of $x_0 = 10$

(b) Initial value of $y_0 = 12$

(c) Initial value of $z_0 = 23$

3.4.2.4 Rössler Map

(a) Initial value of $x_0 = 0.12$

(b) Initial value of $y_0 = 0.42$

(c) Initial value of $z_0 = 5.0$

3.4.3 Plaintext preparation

The plaintext is a color image of size $m \times n$ where m and n are number of rows and columns in the image respectively. Each pixel is represented as a byte. The plaintext is first vectorized

using row scan method to obtain an array of size $N \times 1$, where $N = mn$. The array of pixel is further split into its binary equivalents represented in 8-bit format. For example a pixel with intensity value of *125* is represented in 8-bt binary format by *01111101* . Similarly the pixel intensity of the color image is converted into its binary equivalent forming an array of size $N \times 8$ for each of the color components.

3.4.4 Chaotic map generation

Let the size of image be $m \times n$ where m and n are number of rows and columns in the image. To make the keystream dependent on the plaintext image total number of *1s* in binarized color image is calculated.

Let ω be total number of 1s in the image. It plays the key role in generating different chaotic sequences for different plaintext images. The chaotic maps are evaluated iteratively and their iteration is controlled by

$$\varphi = \omega + mn \tag{3.14}$$

where φ is the total iterations of the chaotic maps. Two images differing from each other by just one pixel will also have entirely differen sorting sequences. The chaotic sequence used for shuffling of plaintext image bits are $x(k), y(k)$ and $z(k)$ where k varies from $(\omega + 1)$ to φ.

3.4.5 Permutation of the plaintext image bits

The data in the plaintext image have strong correlation among adjacent pixels, therefore the pixels of image are permuted among themselves in order to decrease the correlation and increase the confusion as shown in Fig. 3.1. This increases the dependency of color components on each other and increases the computation while decoding the information by any unauthorised individual. The 8-bit RGB pixel that was shuffled individually [35] by 4 chaotic sequences $X_1 to\, X_4$, $Y_1 to\, Y_4$ and $Z_1 to\, Z_4$ respectively are replaced by 24-bit shuffling of RGB pixel using 12 chaotic sequences.

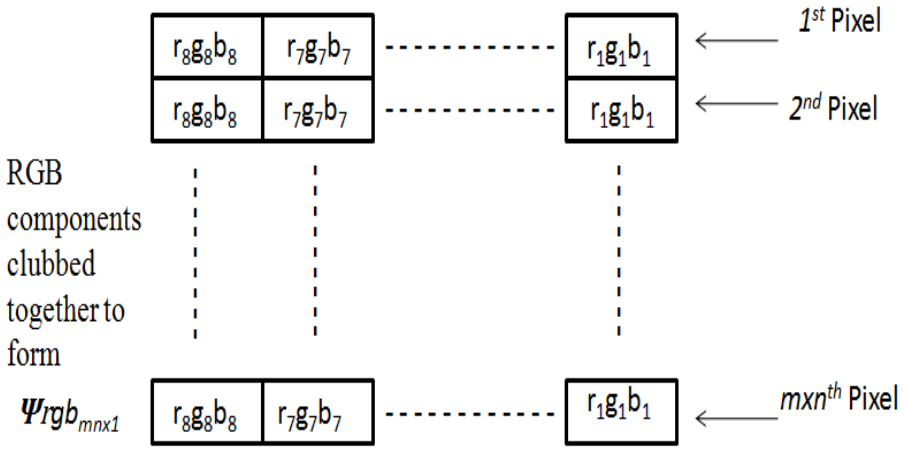


Fig. 3.1: Permutation of the RGB color components

3.4.6 Algorithm for the Enhanced Multi Chaotic Image Encryption

Step 1: The chaotic sequences X_1 *to* X_4 , Y_1 *to* Y_4 and Z_1 *to* Z_4 are generated as discussed in *Section 3.4.4*.

Step 2: Prepare the chaotic sequences $X_{1_{(\mu,1)}}$ *to* $X_{4_{(\mu,1)}}$, $Y_{1_{(\mu,1)}}$*to* $Y_{4_{(\mu,1)}}$ and $Z_{1_{(\mu,1)}}$ *to* $Z_{4_{(\mu,1)}}$ generated from chaotic variable sets, and make the indexing sequences Fx_1 *to* Fx_4 , Fy_1 *to* Fy_4 and Fz_1 *to* Fz_4 ; that are:

$Fx_1 = sort(X_{1_{(\mu,1)}})$

$Fx_2 = sort(X_{2_{(\mu,1)}})$

$Fx_3 = sort(X_{3_{(\mu,1)}})$

$Fx_4 = sort(X_{4_{(\mu,1)}})$

for $\mu = 1,2,3, \dots, m \times n$, where $sort(\cdot)$ is the sequencing index function and $m \times n$ is the dimension of the original plaintext image. Similarly we will calculate the sequences Fy_1 *to* Fy_4 and Fz_1 *to* Fz_4 respectively as in [35, section 2.2]

Step 3: Combine the original binarized R-level, G-level and B-level matrix to form $\Psi rgb_{mn\times1}$ as shown in Fig. 3.1. Each row consists of 24 bits of the RGB image.

Step 4: Apply the shuffle function sq(·) on pixels of Ψrgb for column indexing and shuffling as shown in Fig. 3.2. $sq(\cdot)$ shuffles and indexes bits of each pixel by the indexing sequences. Thus, we have the encrypted column shuffled RGB-level matrix as:

$$\Psi ergb = \left[\Psi ergb_{\mu 1}, \Psi ergb_{\mu 2}, \ldots \Psi ergb_{\mu 24}\right];$$

$where,$

$$\Psi ergb_{\mu i} = \begin{cases} sq\left(\Psi rgb_{\mu i}, Fx_1\right), i = 1{,}2 \\ sq\left(\Psi rgb_{\mu i}, Fx_2\right), i = 3{,}4 \\ sq\left(\Psi rgb_{\mu i}, Fx_3\right), i = 5{,}6 \\ sq\left(\Psi rgb_{\mu i}, Fx_4\right), i = 7{,}8 \\ sq\left(\Psi rgb_{\mu i}, Fy_1\right), i = 9{,}10 \\ sq\left(\Psi rgb_{\mu i}, Fy_2\right), i = 11{,}12 \\ sq\left(\Psi rgb_{\mu i}, Fy_3\right), i = 13{,}14 \\ sq\left(\Psi rgb_{\mu i}, Fy_4\right), i = 15{,}16 \\ sq\left(\Psi rgb_{\mu i}, Fz_1\right), i = 17{,}18 \\ sq\left(\Psi rgb_{\mu i}, Fz_2\right), i = 19{,}20 \\ sq\left(\Psi rgb_{\mu i}, Fz_3\right), i = 21{,}22 \\ sq\left(\Psi rgb_{\mu i}, Fz_4\right), i = 23{,}24 \end{cases}$$

and the $\Psi rgb_{\mu i}$ is the ith bit of the cth pixel of the original binary RGB-level matrix.

Step 5*:* Now, perform row wise shuffling of bits within each RGB block in pairs of 2-bits by $Fx_1\ to\ Fx_4$, $Fy_1\ to\ Fy_4$ and $Fz_1\ to\ Fz_4$.

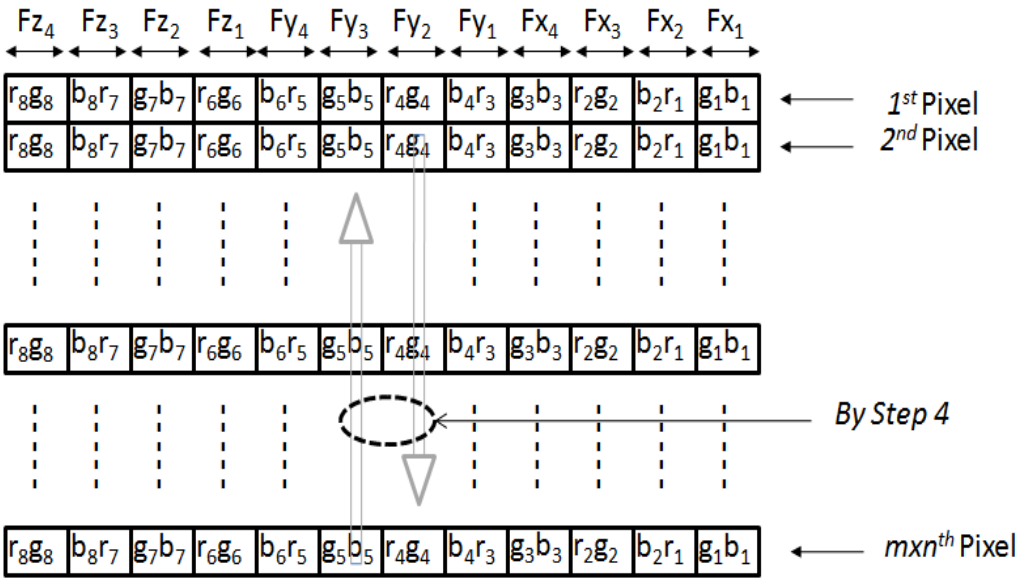


Fig. 3.2: Column wise shuffling of the plaintext image bits

The general flowchart of the proposed cryptosystem is shown in Fig. 3.3

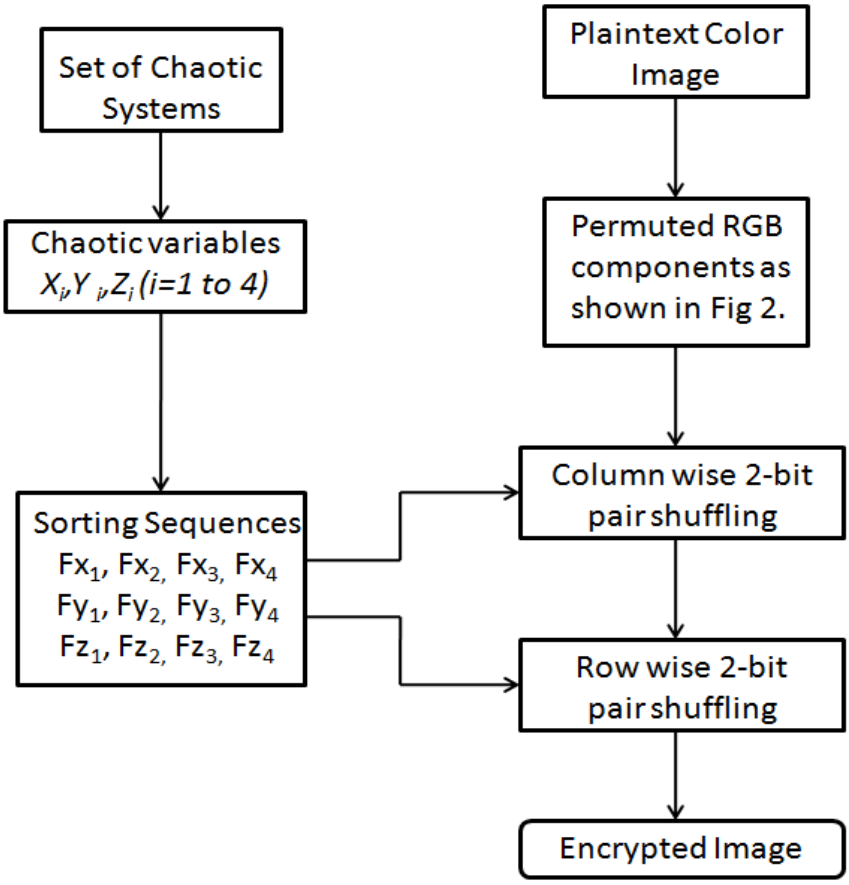


Fig. 3.3: Flowchart of the Enhanced Multi-Chaotic Image Encryption

3.5 Decryption

The plain image can be recovered successfully by applying the encryption process in a reverse order. The key for the decryption is the set of parameters of the chaotic systems used and the initial values of the variables in the maps.

Chapter 4

Performance Evaluation Methodology

4.1 Performance Analysis Parameters

In order to verify and test the security strength of the Modified Multi Chaotic Systems Based Pixel Shuffle Scheme, different types of statistical analysis has been performed on the proposed algorithm. The analysis parameters used for the evaluation of proposed scheme over existing PCS scheme are:

- Histogram Analysis
- Information Entropy Analysis
- NPCR and UACI Analysis
- Correlation Coefficient Analysis

4.1.1 Histogram Analysis

In image processing histogram is the graphical representation of the pixel intensity distribution of the image. It is a plot of total number of pixels against its tonal value. The histogram of an image gives the distribution pattern of its intensities for the entire image. The horizontal axis of the graph represents the intensity variations, while the vertical axis represents the number of pixels in that particular intensity. For an eight bit image, the intensity value of zero represents a complete black pixel and intensity value of 255 represents a white pixel. Thus, the histogram for a very dark image, the histogram will be concentrated on the left side and center of the graph. Conversely, the histogram for a very bright image with few dark areas and/or shadows will have most of its data points on the right side and center of the graph.

In case of image encryption, algorithms with uniform distribution of pixel intensities are considered efficient. A flat histogram represents that of a noised image that makes the encryption resistant to histogram analysis attack.

4.1.2 Information Entropy Analysis

Entropy of an image is a basic criterion used to depict the randomness of data and the distribution of the gray value. A greater value of information entropy shows a more uniform distribution of the gray value of the image. The entropy H of a symbol source S image can be computed by [37].

$$H(S) = \sum_{i=0}^{255} p(s_i)\, log\left(\frac{1}{p(s_i)}\right) \tag{4.1}$$

Where $p(s_i)$ represents the probability of symbol s_i and the entropy is expressed in bits. If the source S emits 2^8 symbols with equal probability, i.e. $S = \{s_0, s_1, \ldots\ldots s_{255}\}$ then the result of entropy is $H(S) = 8$, which corresponds to a true random source and represents the ideal value of entropy for message source S. If the entropy value tends to 8, then the predictability of the method decreases that strengthens the image security.

4.1.3 NPCR and UACI Analysis

The two most common and efficient parameters to evaluate the strength of the image encryption algorithms with respect to differential attacks are the Number of Pixel Change Rate (NPCR) and the Unified Averaged Changed Intensity (UACI). The higher the score of these parameters, the better is the encryption technique. These values determine the sensitivity of the encryption algorithm to small change in plaintext image.

Definition of NPCR and UACI:

(a) NPCR and *UACI between Ciphertext images before and after one pixel change:*

Let the plaintext image be P_1 and the corresponding ciphertext image be C_1. Now after altering a single pixel value in P_1 we get the changed plaintext image as P_2 and its ciphered image C_2.

The NPCR and UACI value for the two ciphertext images C_1 and C_2 can be mathematically represented by equations (7) and (8), respectively, where T denotes the largest supported pixel value compatible with the ciphertext image format, $|\cdot|$ denotes the absolute value function and other symbols have their usual meaning [38].

$$\text{NCPR: } N(C_1, C_2) = \sum_{ij} \frac{D(i,j)}{m \times n} \times 100\% \tag{4.2}$$

$$\text{UACI: } U(C_1, C_2) = \frac{1}{m \times n} \sum_{ij} \frac{|C_1(i,j) - C_2(i,j)|}{T} \times 100\% \tag{4.3}$$

where,

$$D(i,j) = \begin{cases} 0, if\ C_1(i,j) = C_2(i,j) \\ 1, if\ C_1(i,j) \neq C_2(i,j) \end{cases} \tag{4.4}$$

(b) NPCR and UACI between Original Image and Encrypted Image:

Let the plaintext image be denote as P and the respective ciphered image obtained after applying proposed encryption algorithm is C. The formulae to calculate NPCR and UACI for the two images are represented by following equations:

$$\text{NCPR: } N(P, C) = \sum_{ij} \frac{D(i,j)}{m \times n} \times 100\% \tag{4.5}$$

$$\text{UACI: } U(P, C) = \frac{1}{m \times n} \sum_{ij} \frac{|P(i,j) - C(i,j)|}{T} \times 100\% \tag{4.6}$$

where,

$$D(i,j) = \begin{cases} 0, if\ P(i,j) = C(i,j) \\ 1, if\ P(i,j) \neq C(i,j) \end{cases} \tag{4.7}$$

4.1.4 Correlation Coefficient Analysis

Correlation coefficient is widely used in statistical analysis, pattern recognition and image processing [39-42]. It defines the relationship between neighboring pixels in an image. To withstand statistical attack, the correlation between adjacent pixels of cipher image should be as low as possible.

Then the correlation coefficient of each pair is calculated by [37].

$$\rho = \frac{N \sum_{i=1}^{N} (x_i \times y_i) - \sum_{i=1}^{N} x_i \times \sum_{i=1}^{N} y_i}{\sqrt{\left(N \sum_{i=1}^{N} x_i^2 - \left(\sum_{i=1}^{N} x_i\right)^2\right) \times \left(N \sum_{i=1}^{N} y_i^2 - \left(\sum_{i=1}^{N} y_i\right)^2\right)}} \tag{4.8}$$

where x and y are gray values of two adjacent pixels in an image and N is the total number of pairs of horizontally,vertically or diagonally adjacent pixels.

Chapter 5
Experiments and Results

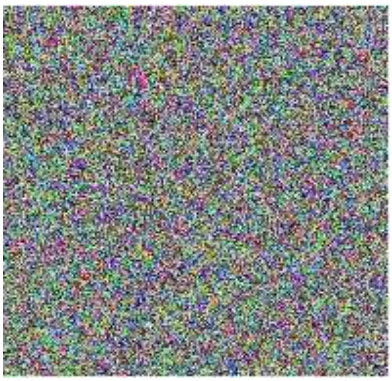
The proposed Modified Multi-Chaotic Systems Based Pixel Shuffle Scheme for color images has been implemented in Matlab. No preprocessing is required prior the application of the algorithm. The performance of the algorithm depends on the randomness of the pixel in the encrypted image. The proposed algorithm and the PCS scheme has been evaluated for color images of Lena, Peppers and Baboon of size 256×256 , to prove the security and robustness of the proposed cryptosystem over PCS scheme. In order to perform the statistical measure, Number of Pixel Change Rate (NPCR) , Unified Average Changed Intensity (UACI), Information Entropy and Correlation Coefficient are used as parameters to evaluate the performance of the proposed method.

5.1 Results for test image Lena

5.1.1. Encryption and Decryption test

The encrypted image can be decrypted by following the steps of encryption in reverse order. The key to decryption is the chaotic maps with initial value conditions. Any change in the key will not decrypt the ciphered image.

(a)



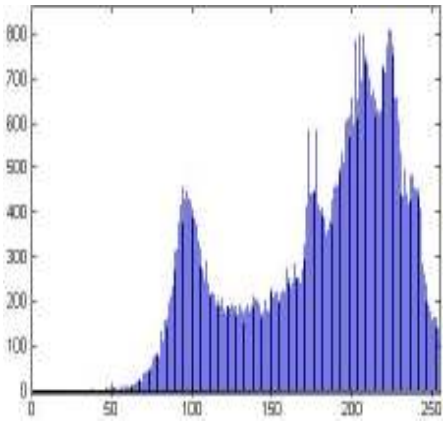
(b)

(c)

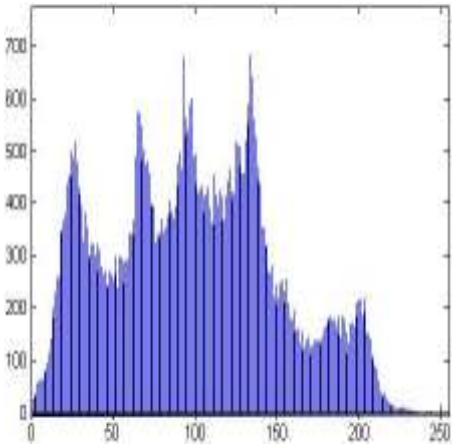
Fig. 5.1.1: (a) Original Lena Image (b) Encrypted Image using Proposed Scheme (c) Decrypted Image

5.1.2 Histogram Analysis

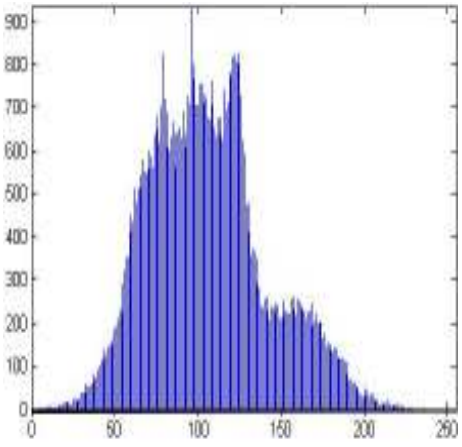
(a)



(b)

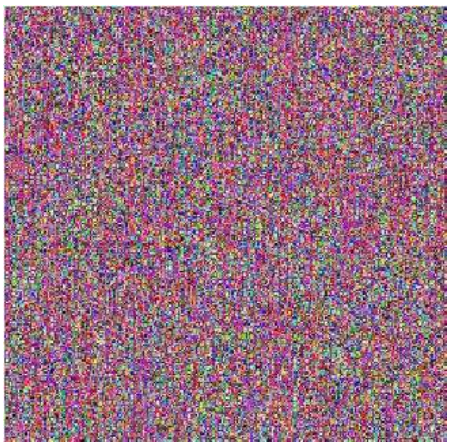


(c)

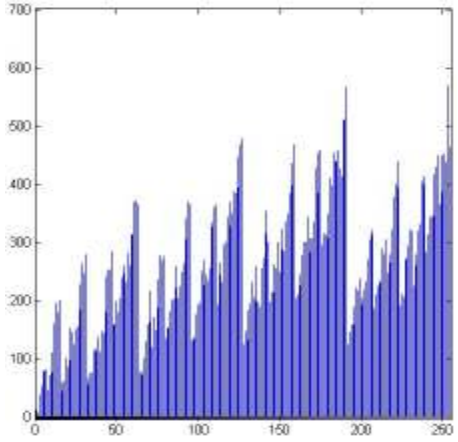


(d)

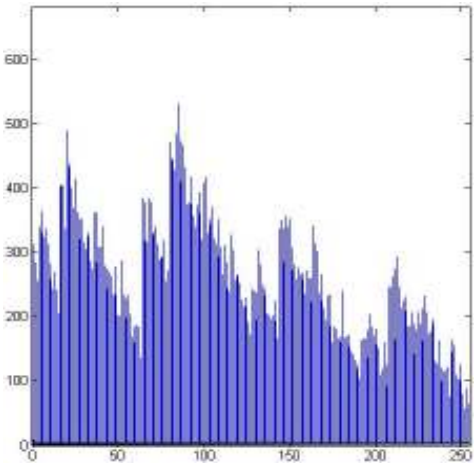
Fig. 5.1.2: Lena and its RGB-Level Spectrums: (a) Original Image (b) R-Level Spectrum (c) G-Level Spectrum (d) B-Level Spectrum



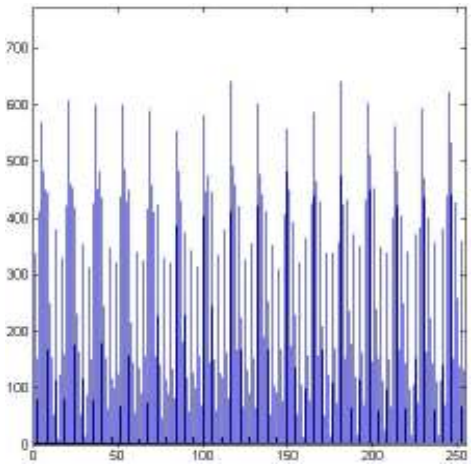
(a)



(b)



(c)



(d)

Fig. 5.1.3: Encrypted Lena using PCS technique and its RGB-Level Spectrums: (a) Encrypted Image (b) R-Level Spectrum (c) G-Level Spectrum (d) B-Level Spectrum

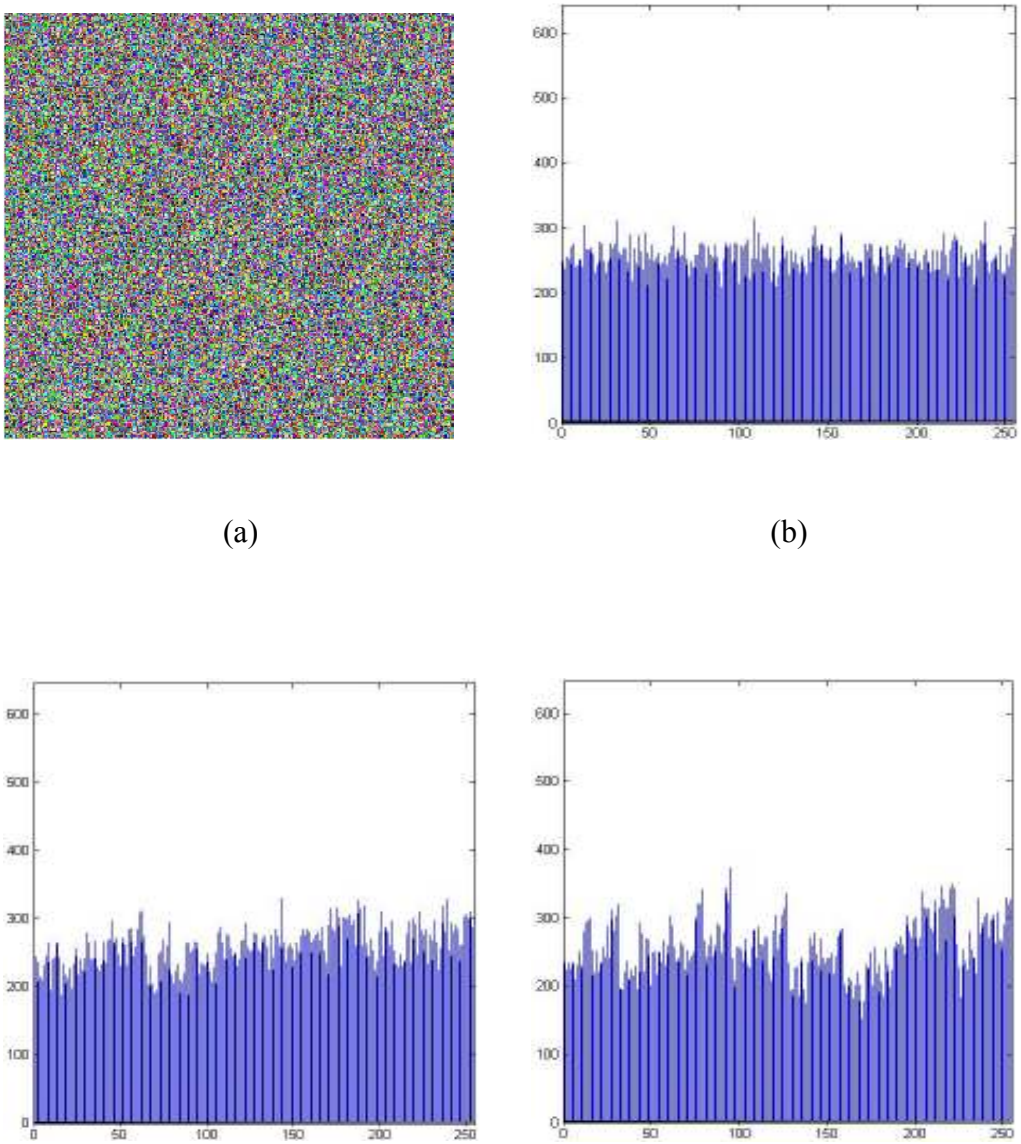


Fig. 5.1.4: Encrypted Lena using proposed technique and its RGB-Level Spectrums: (a) Encrypted Image (b) R- Level Spectrum (c) G-Level Spectrum (d) B-Level Spectrum

The histogram obtained from the PCS technique shown in Fig. 5.1.3 has more number of peaks as compared to the proposed scheme. The image with flat histogram level is analogous to a noised image and the ciphered image is indistinguishable when compared with the original image. The histograms shown in Fig. 5.1.4 resembles that of a noisy image and does not reveal any information regarding the pixel values of the image. We can observe that we obtain a fairly uniform and significantly different histogram using the proposed encryption scheme when compared with PCS cryptosystem.The histogram does not provide any clue to employ any statistical attack on the proposed image encryption procedure.

5.1.3 Entropy Analysis

Table 5.1.1 shows that the entropy value for proposed system is closer to ideal value 8 than those computed from PCS encryption. Therefore, the leakage of information through entropy is lesser in proposed encryption system when compared with PCS technique.

Table 5.1.1: Information Entropy for Original and Ciphered Images

Test Image	Original Image	Proposed	PCS
Lena	7.7847	7.9838	7.6722

5.1.4 NPCR and UACI Evaluation

(a) NPCR and *UACI between Ciphertext images before and after one pixel change:*
For example, the test image *Lena* say P_1 is encrypted and ciphered image is C_1 is obtained. To calculate NPCR/UACI a pixel from the plaintext image P_1 is randomly chosen $(P_1(i,j), i = 40, j = 56)$ whose R color component is set to *0* while the value of the other two component remains the same. Let this new image be named P_2 and its corresponding ciphered image be C_2. NPCR and UACI values for C_1 and C_2 are calculated for the proposed scheme and the original scheme and listed in Table 5.1.2. Similarly, green and blue components are set to zero turn wise for the same pixel position $(P_1(i,j))$ and values of NPCR and UACI are evaluated.The results in Table 5.1.2 shows that a small change in the plain image is reflected by a large difference in ciphered image.

Table 5.1.2: NPCR and UACI between C_1 and C_2

Changed Pixel position $P_1(i,j)$ here,(i=40,j=56)		Proposed Encryption Scheme		PCS Encryption Scheme	
		NPCR%	UACI%	NPCR%	UACI%
$P_1(i,j,1) = 0$	R	99.51	33.44	0.0156	0.0
	G	99.54	33.85	0.0	0.0
	B	99.57	33.89	0.0	0.0
$P_1(i,j,2) = 0$	R	99.51	33.44	0.0	0.0
	G	99.54	33.85	0.0	0.0
	B	99.57	33.89	0.0	0.0
$P_1(i,j,3) = 0$	R	99.52	33.10	0.0	0.0
	G	99.44	33.14	0.0	0.0
	B	99.38	33.47	0.0	0.0

We can analyse from Table 5.1.2 that our scheme is significantly more sensitive towards initial conditions than PCS. The drastic variation in the values of NPCR and UACI arises from the fact that we employ dynamic chaotic maps that varies with varying plaintext image. On the other hand, a constant chaotic sequence for every plaintext image is being used in PCS and it shuffles the pixels to entirely same indices for all plaintext images. The two ciphered images in case of PCS encryption differs from each other at utmost four pixel values corresponding to the mapping done by the 4 chaotic sequences for the changed pixel value. The proposed technique changes the chaotic map completely and the two ciphered images differ entirely from each other,thus giving a higher score of NPCR and UACI.

(b) NPCR and UACI between Original Image and Encrypted Image:

These values are calculated for the test image *Lena* and tabulated in Table 5.1.3. The NPCR and UACI scores determine the randomness between the plaintext image and its ciphertext image. We get a better UACI value for our system and NPCR score is also significantly good.

Table 5.1.3: NPCR and UACI between $\boldsymbol{P}$ and $\boldsymbol{C}$ for *Lena*

	NPCR %			UACI%		
	R	G	B	R	G	B
Proposed	99.62	99.60	99.57	33.15	30.67	28.27
PCS	99.48	99.55	99.67	24.55	27.51	27.58

5.1.5 Correlation Coefficients Analysis

The values of the correlation coefficients for the proposed algorithm and the PCS scheme are given in Table 5.1.4. According to the results, our proposed algorithm has a lesser value of

correlation coefficient when compared to PSC scheme, thus our algorithm outperforms the PCS encryption technique.

Table 5.1.4: Correlation Coefficients for test image *Lena*

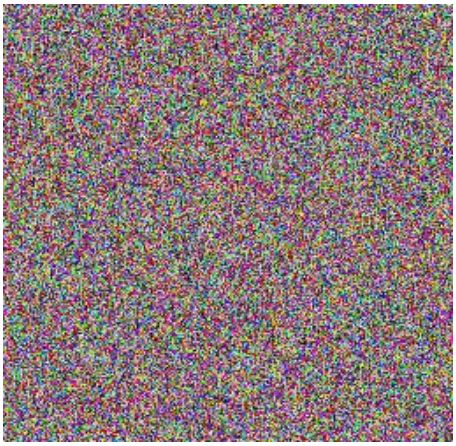
	Original Image	Proposed	PCS
Horizontal	0.90795	0.07457	0.08622
Vertical	0.95298	0.120745	0.19197
Diagonal	0.85709	0.08087	0.08429

5.1 Results for test image Peppers

5.2.1 Encryption and Decryption test

The proposed algorithm is used to obtain ciphered image of the color image *Peppers*. The decrypted image is produced using the correct key and correct initial value conditions of the chaotic-maps.

(a)



(b)

(c)

Fig. 5.2.1: (a) Original Peppers Image (b) Encrypted Image using Proposed Scheme (c) Decrypted Image

5.2.2 Histogram Analysis

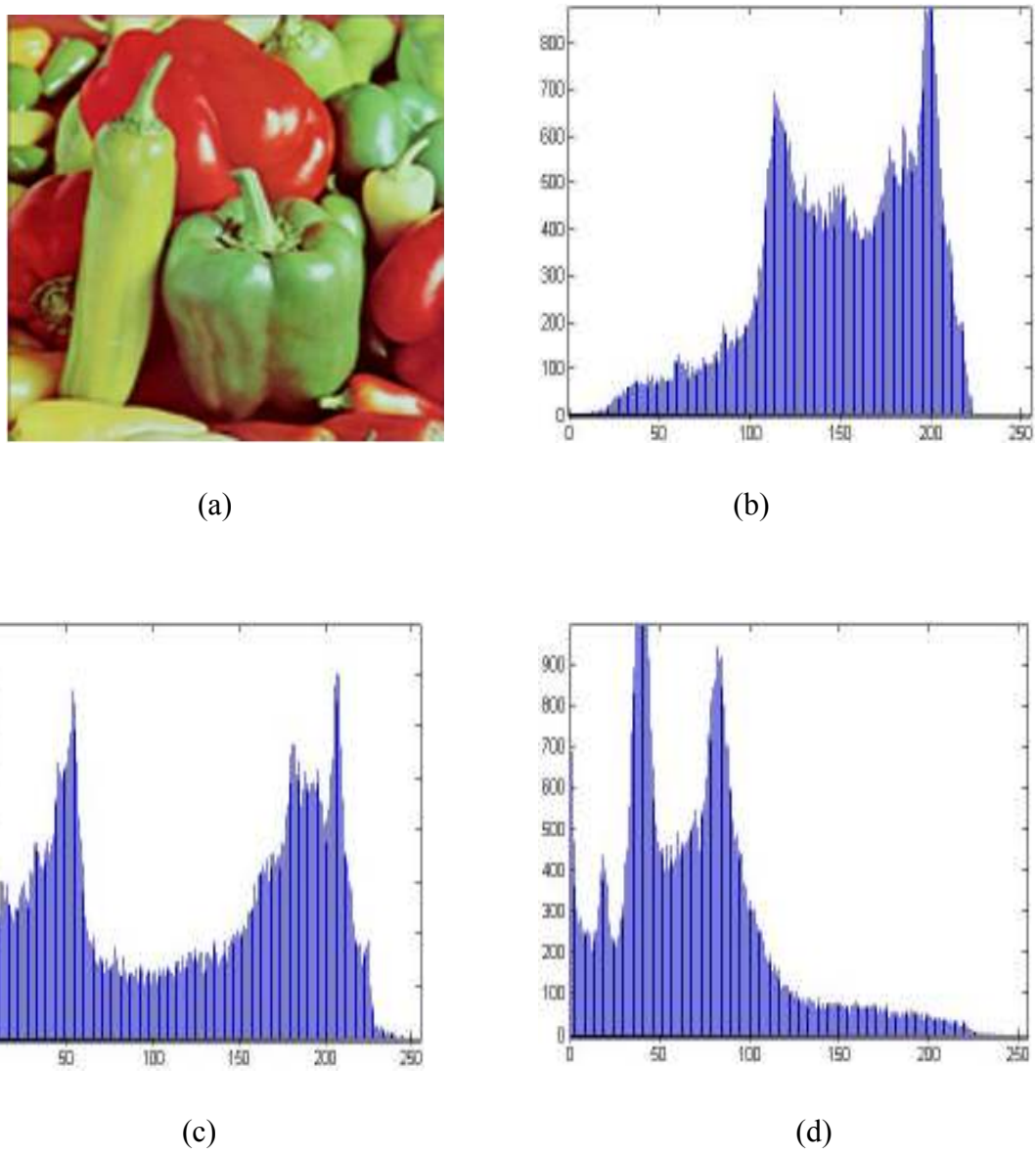
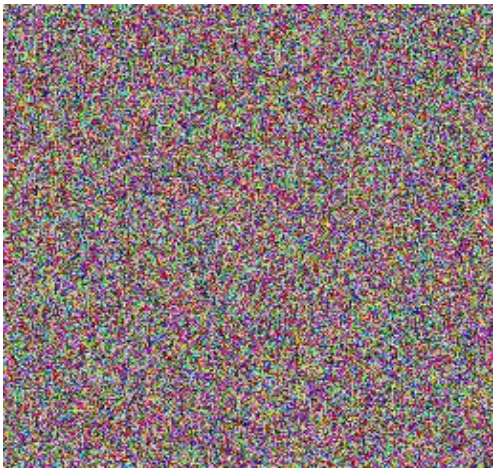
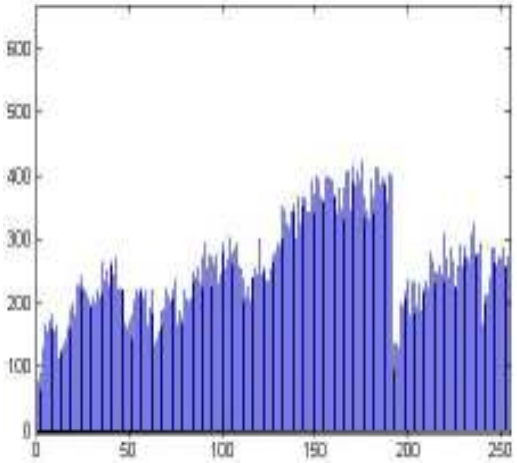


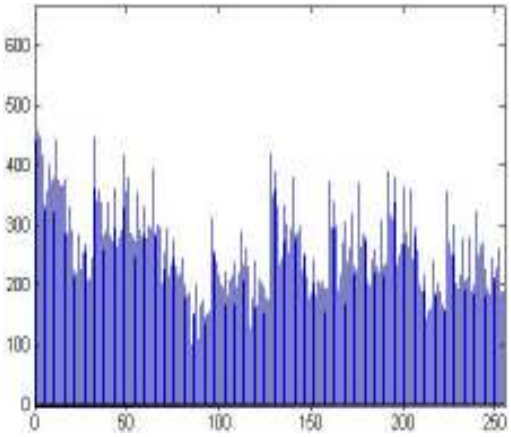
Fig. 5.2.2: Peppers and its RGB-Level Spectrums: (a) Original Image (b) R-Level Spectrum (c) G-Level Spectrum (d) B-Level Spectrum



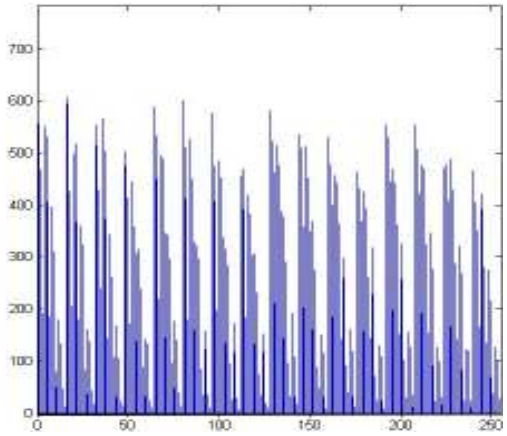
(a)



(b)



(c)



(d)

Fig. 5.2.3: Encrypted Peppers using PCS technique and its RGB-Level Spectrums: (a) Encrypted Image (b) R-Level Spectrum (c) G-Level Spectrum (d) B-Level Spectrum

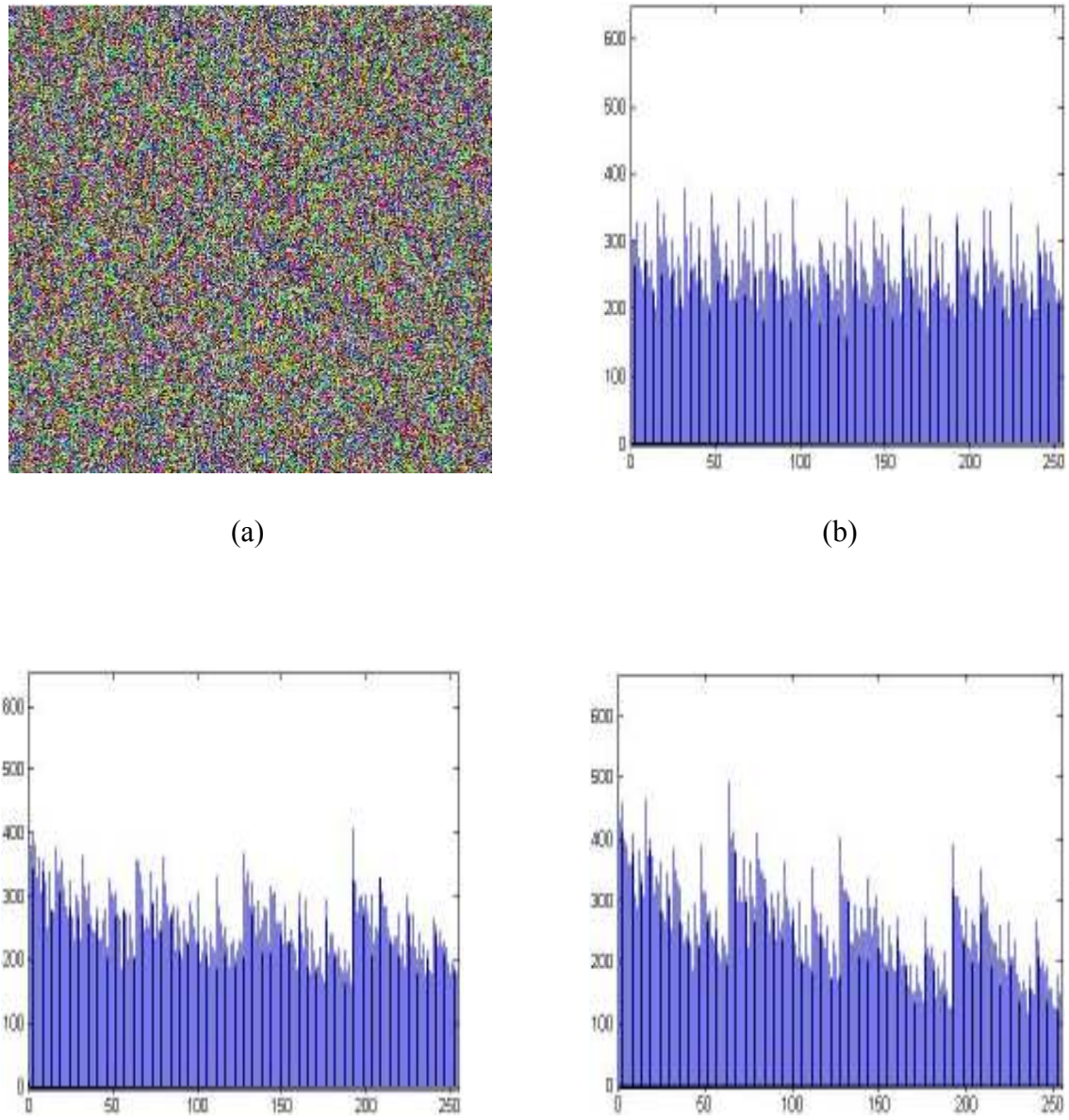


Fig. 5.2.4: Encrypted Peppers using Proposed technique and its RGB-Level Spectrums: (a) Encrypted Image (b) R-Level Spectrum (c) G-Level Spectrum (d) B-Level Spectrum

Fig. 5.2.2 show the RGB level spectrum of the original image, Fig. 5.2.3 and Fig. 5.2.4 shows the histograms of the ciphered images obtained from PCS cryptosystem and the proposed Multi-Chaotic Systems Based Pixel Shuffle respectively. The histogram of the

proposed algorithm does not have peaks as compared to that obtained from PCS method. Hence attacks by histogram analysis are difficult in proposed method.

5.2.3 Entropy Analysis

Entropy is the measure of degree of randomness of the pixels. In case of 8-bit images this value tends to *8* for ideal images.

Table 5.2.1: Information Entropy for Original and Ciphered Images

Test Image	Original Image	Proposed	PCS
Peppers	7.7242	7.9628	7.5510

5.2.4 NPCR and UACI Evaluation

(a) NPCR and *UACI between Ciphertext images before and after one pixel change:*

The score of NPCR and UACI of the proposed scheme is close to ideal value of 99.50% whereas the PCS scheme has poor results of NPCR and UACI. The evaluated values are shown in Table 5.2.2.

Table 5.2.2: NPCR and UACI between C_1 and C_2

Changed Pixel position $P_1(i,j)$ here,(i=40,j=56)		Proposed Encryption Scheme		PCS Encryption Scheme	
		NPCR%	UACI%	NPCR%	UACI%
$P_1(i,j,1) = 0$	R	99.50	33.49	0.01	0.0
	G	99.56	30.89	0.0	0.0
	B	99.53	33.56	0.0	0.0
$P_1(i,j,2) = 0$	R	99.52	32.74	0.0	0.0
	G	99.64	32.89	0.0	0.0
	B	99.48	32.49	0.014	0.0
$P_1(i,j,3) = 0$	R	99.55	32.51	0.0	0.0
	G	99.51	33.64	0.0	0.0
	B	99.38	33.37	0.0	0.0

(b) NPCR and UACI between Original Image and Encrypted Image:

These values are calculated for the test image *Peppers* and tabulated in Table 5.2.3. The NPCR and UACI scores evaluated from proposed algorithm are better than those obtained from PCS scheme.

Table 5.2.3: NPCR and UACI between $\boldsymbol{P}$ and $\boldsymbol{C}$ for *Peppers*

	NPCR %			UACI%		
	R	G	B	R	G	B
Proposed	99.60	99.62	99.64	29.25	30.62	31.29
PCS	99.40	99.67	99.26	23.35	31.22	31.26

5.2.5 Correlation Coefficients Analysis

The correlation coefficient analysis shows the relation among the adjacent pixels. The overall value of correlation coefficient is comparatively better than the PCS cryptosystem.

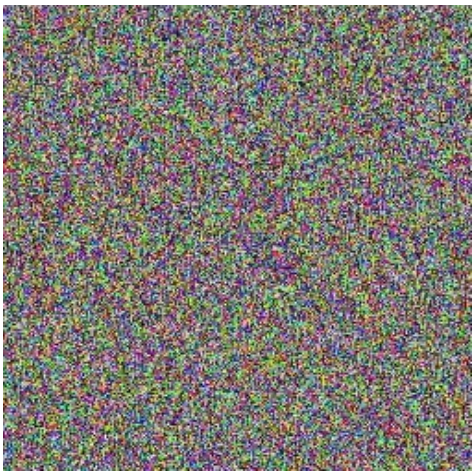
Table 5.2.4: Correlation Coefficients for test image *Peppers*

	Original Image	Proposed	PCS
Horizontal	0.9373	0.12	0.16
Vertical	0.9183	0.08	0.14
Diagonal	0.8683	0.07	0.09

5.3 Results for test image Baboon

5.3.1 Encryption and Decryption test

(a)



(b)

(c)

Fig. 5.3.1: (a) Original Baboon Image (b) Encrypted Image using Proposed Scheme (c) Decrypted Image

5.3.2 Histogram Analysis

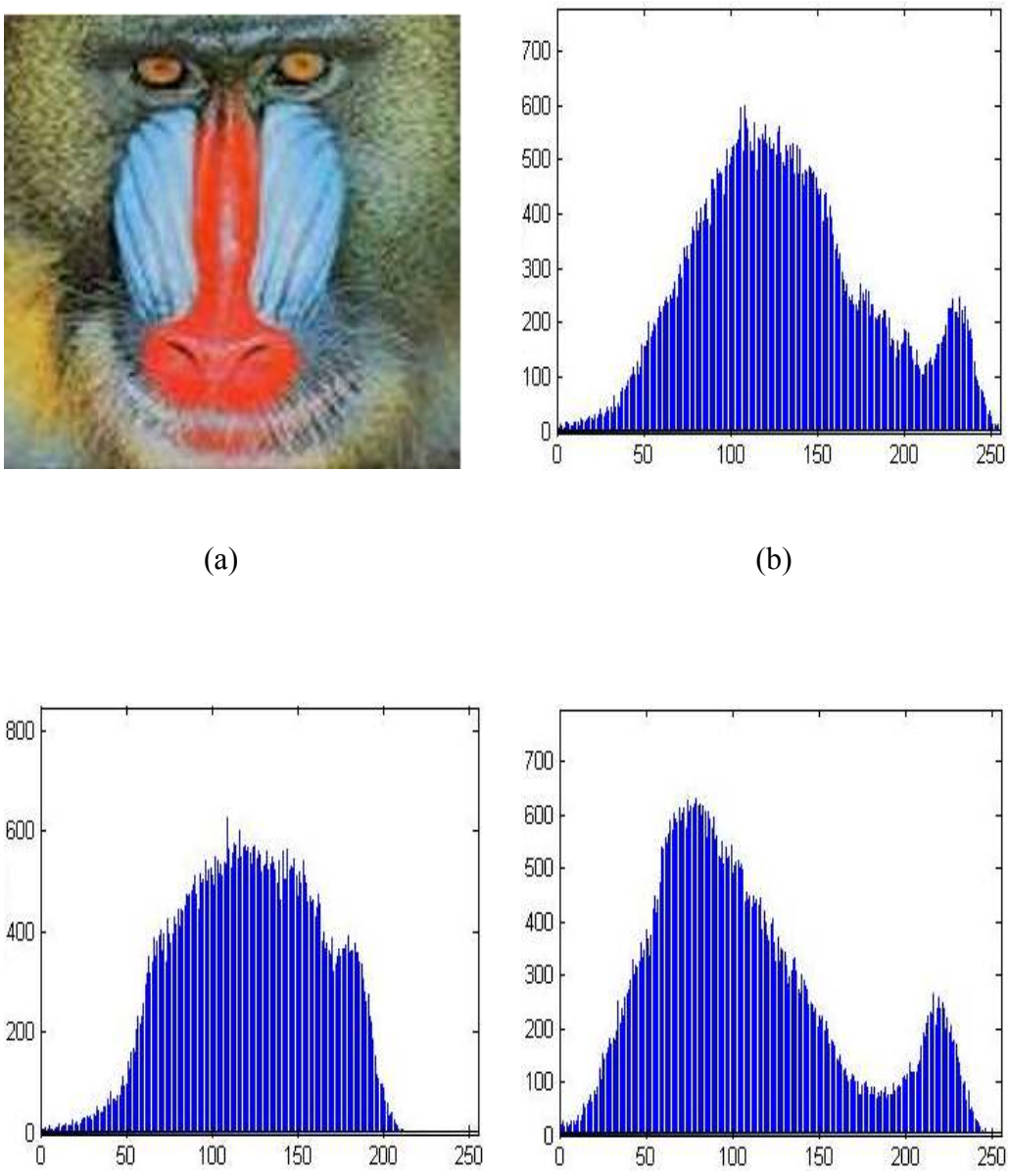
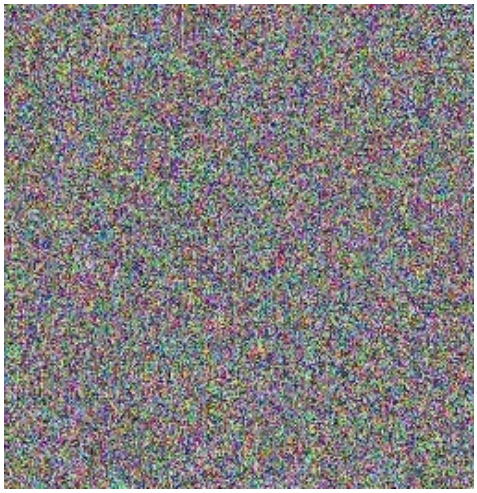
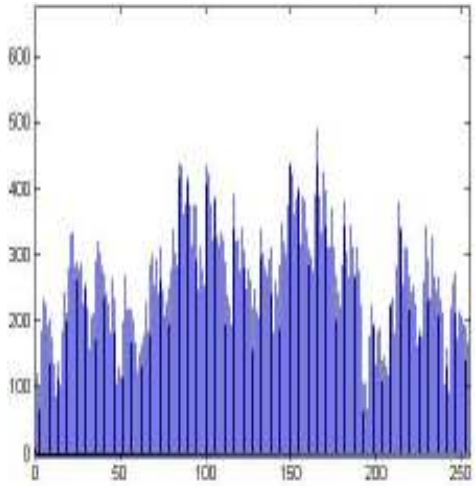


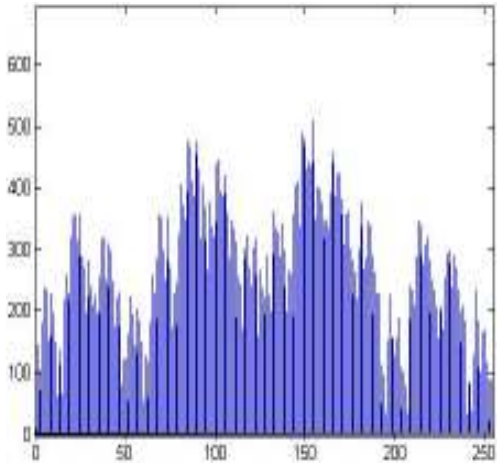
Fig. 5.3.2: Peppers and its RGB-Level Spectrums: (a) Original Image (b) R-Level Spectrum (c) G-Level Spectrum (d) B-Level Spectrum



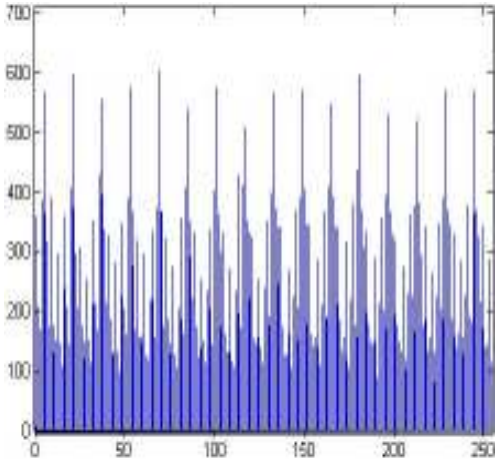
(a)



(b)

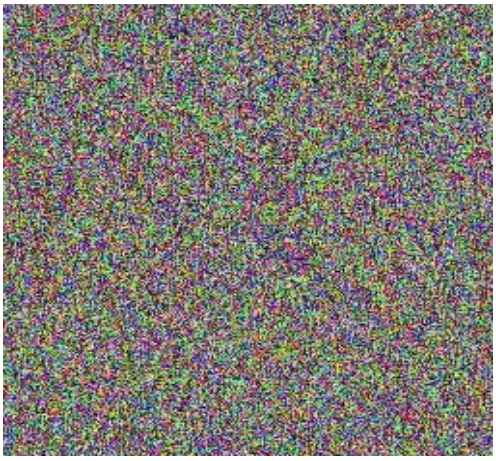


(c)

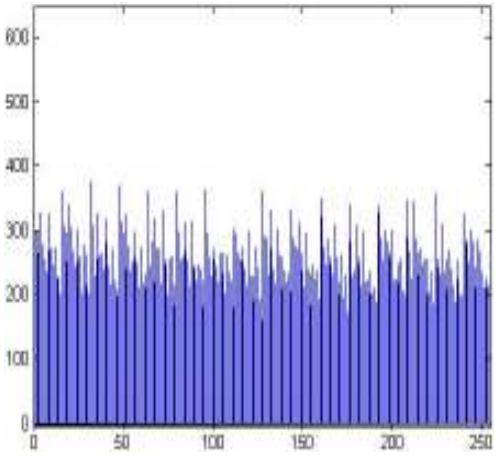


(d)

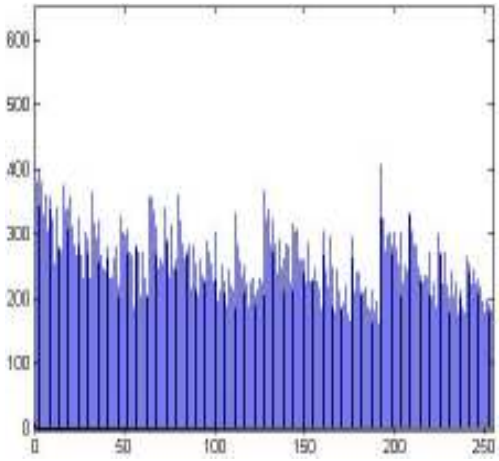
Fig. 5.3.3: Encrypted Baboon using PCS technique and its RGB-Level Spectrums: (a) Encrypted Image (b) R-Level Spectrum (c) G-Level Spectrum (d) B-Level Spectrum



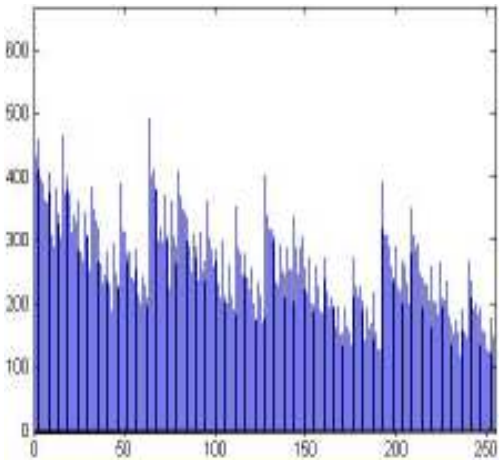
(a)



(b)



(c)



(d)

Fig. 5.3.4: Encrypted Baboon using proposed technique and its RGB-Level Spectrums: (a) Encrypted Image (b) R-Level Spectrum (c) G-Level Spectrum (d) B-Level Spectrum

The histogram of the ciphered image obtained from proposed method is uniform in contrast to the histogram of the original image. This shows that the intensity of pixels is distributed uniformly in the ciphered image. The RGB levels in Fig. 5.3.3 is not much uniform.

5.3.3 Entropy Analysis

The information entropy of the test image *Baboon* comes out to be very close to ideal value of 8. The PCS encryption scheme has a lower value of entropy as compared to the proposed encryption method. Thus, the proposed method gives a better entropy value.

Table 5.3.1: Information Entropy for Original and Ciphered Images

Test Image	Original Image	Proposed	PCS
Baboon	7.6310	7.9798	7.5272

5.3.4 NPCR and UACI Analysis

(a) NPCR and UACI between Ciphertext images before and after one pixel change:

These values determine the degree of randomness in the encrypted images if the corresponding plaintext images differ minutely by single pixel value. The values obtained shows that a small change in plain image is reflected by a significant change in encrypted image.

Table 5.3.2: NPCR and UACI between C_1 and C_2

Changed Pixel position $P_1(i,j)$ here,(i=40,j=56)		Proposed Encryption Scheme		PCS Encryption Scheme	
		NPCR%	UACI%	NPCR%	UACI%
$P_1(i,j,1) = 0$	R	99.55	27.78	0.0	0.0
	G	99.26	27.66	0.0	0.0
	B	99.33	24.94	0.0	0.0
$P_1(i,j,2) = 0$	R	99.42	28.07	0.0	0.0
	G	99.60	30.93	0.012	0.0
	B	99.54	25.23	0.0	0.0
$P_1(i,j,3) = 0$	R	99.57	28.57	0.0	0.0
	G	99.53	30.45	0.0	0.0
	B	99.63	25.36	0.0	0.0

(c) NPCR and UACI values between Original Image and Encrypted Image:

The NPCR and UACI values provide qualitative analysis of the encryption scheme. The evaluated scores from proposed and PCS method are tabulated below. The NPCR scores are not far different from each other and close to 100%. The values of UACI show better results for the proposed encryption algorithm.

Table 5.3.3: NPCR and UACI between P and C for *Baboon*

	NPCR %			UACI%		
	R	G	B	R	G	B
Proposed	99.62	99.60	99.57	33.15	30.67	28.27
PCS	99.82	99.55	99.45	24.41	22.51	28.08

5.3.4 Correlation Coefficient Analysis

The correlation coefficient for the proposed encryption method gives a better value as shown in Table 5.3.4. It is the measure of the relation between the pixel and its adjacent neighboring pixels. The lower the value of correlation coefficient is, the better is the encryption algorithm considered.

Table 5.3.4: Correlation Coefficients for test image

	Original Image	Proposed	PCS
Horizontal	0.8845	0.1199	0.122
Vertical	0.8796	0.0810	0.137
Diagonal	0.8334	0.0642	0.08

Chapter 6

Conclusion and Future Work

In this paper a new way of image encryption have been proposed that is robust against CPA and CCA. The drawback of PCS technique is overcome by dynamically updating the chaotic map with changing plaintext image which ensures that there is no chance that CPA and CCA can break the improved cryptosystem. This is achieved by giving weightage to the total number of binary 1s in the plaintext image that is used in determining the key of the encryption scheme. To make the cipher image more robust against any attack, the color image is permuted before performing the actual column wise and row wise shuffling. The experimental values of NPCR and UACI show that proposed encryption scheme is resistant to differential attacks, thus cryptanalysis of plain-cipher image pair will not reveal the keystream. It is also shown that the ciphered image is very sensitive to a slight change in the bit values of original image. If one pixel of the plaintext image is changed, then the cipher image obtained changes completely in an unpredictable or pseudorandom manner. We have performed several tests to ensure the security of the proposed system namely, statistical analysis which includes Histogram analysis, Correlation analysis, NPCR and UACI analysis and Information Entropy analysis. The experimental values govern that proposed algorithm yields a very good performance over the PCS algorithm. Hence, this paper presents a cryptosystem that is highly secure against attacks and is useful for secure image encryption and transmission applications.

Currently the chaos-based encryption scheme is designed for color images. The chaos-based image encryption scheme gives a good value of NPCR and UACI for C_1 and C_2, when their corresponding plaintext image P_1 and P_2 differ by one pixel. In other words we can say that the proposed algorithm gives a good score when the plaintext images differ in the count of binary 1s for P_1 and P_2 . Even a difference of one bit can generate an entirely different chaotic map and hence the ciphered images, but if the total number of 1s remain constant in the plaintext images P_1 and P_2 then same mapping is done for both the images. Thus, the corresponding ciphertext images will have same mapping indices and consequently the NPCR and UACI score will be quite less than the ideal values.

To overcome such situations we can incorporate some techniques to include the effect of changed pixel value as well as its respective coordinates to enhance the security and privacy needed in various applications.

References:

[1] Chen, G.; Mao, Y.; Chui, C.; "A symmetric image encryption scheme based on 3D chaotic cat maps", Chaos, Solitons & Fractals, 2004, Vol. 21, Issue 3, pp. 749–61.

[2] Chiaraluce, F.; Ciccarelli, L.; "A new chaotic algorithm for video encryption", IEEE Transactions on Consumer Electronics, 2002, Vol. 48, Issue 4, pp. 838–44.

[3] Sinha, A.; Singh, K.; "A technique for image encryption using digital signature", Optics Communications, ARTICLE IN PRESS, 2003, pp. 1-6.

[4] Maniccam, S.S.; Bourbakis, N. G.; "Lossless image compression and encryption using SCAN", Pattern Recognition 34, 2001, pp. 1229-1245.

[5] Chang, C.C.; Hwang, M. S.; Chen, T.S.; "A new encryption algorithm for image cryptosystems", The Journal of Systems and Software 58, 2001, pp. 83-91

[6] Guo, J.I.; Yen, J. C.; "A new mirror-like image encryption algorithm and its VLSI architecture", Pattern Recognition and Image Analysis, 2007, pp. 236-247.

[7] Giesl, J.; Behal, L.; Vlcek, K.; "Improving Chaos Image Encryption Speed", International Journal of Future Generation Communication and Networking Vol. 2, No. 3, 2009, pp. 23-36.

[8] Zhang, S.; Karim, M. A.; "Color image encryption using double random phase encoding", microwave and optical technology letters, Vol. 21, No. 5, June 5 1999, pp. 318-322.

[9] Matthews, R.; "On the derivation of a chaotic encryption algorithm", Cryptologia, Vol. 13, No. 1, 1989, pp. 29-41.

[10] Zhang, L.; Liao, X.; Wang, X.; "An image encryption approach based on chaotic maps", Chaos Solitons Fractals 2005; Vol. 24, Issue 3, pp. 759-765.

[11] Yang, S.; Sun, S.; “A video encryption method based on chaotic maps in DCT domain”, Progress in Natural Science; Vol. 18, 2008, pp. 1299–1304.

[12] Fu, C.; Zhang, Z.; Cao, Y.; “An improved image encryption algorithm based on chaotic maps,” in Proc. of the 3rd Int. Conf. on Natural Computation, (ICNC 2007): Haikou, Vol. 3, pp. 189-193.

[13]Sakthidasan, K. @ Sankaran; Santhosh Krishna, B.V.; “A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images”, International Journal of Information and Education Technology, June 2011, Vol. 1, No. 2, pp. 137-141.

[14] Li, W.; Yu, N.; “A Robust chaos based Image encryption scheme” ICME 2009. IEEE International Conference on Multimedia and Expo: New York, 2009, pp. 1034-1037.

[15] Zhai, Y.; Lin, S.; Zhang, Q.; “Improving Image Encryption Using Multi-chaotic Map”, Workshop on Power Electronics and Intelligent Transportation System (PEITS): Guangzhou, 2008, pp. 143-148.

[16] Xin, G.; Fen-lin, L.; Bin, L.; Wei, W.; Juan, C.; “An Image Encryption Algorithm Based on Spatiotemporal Chaos in DCT Domain”, The 2nd International Conference on Information Management and Engineering (ICIME): Chengdu, 2010, pp. 267-270.

[17] Nien, H. H.; Huang, C. K.; Changchien, S.K.; Shieh, H.W.; Chen, C.T.; Tuan, Y.Y.; “Digital color image encoding and decoding using a novel chaotic random generator,” Chaos, Solitons and Fractals,2007, Vol. 32, Issue 3, pp. 1070-1080.

[18] Wang, K.; Pei, W.; Zou, L.; Song, A.; He, Z.; “On the security of 3D Cat map based symmetric image encryption scheme,” Phys. Lett. A, 2005, Vol. 343, Issue 6, pp. 432-439.

[19] Guan, Z.H.; Huang, F.; Guan, W.; “Chaos-based image encryption algorithm”, Phys. Lett. A, 2005, Vol. 346, Issue 1-3, pp. 153-157.

[20] Gao, T.G.; Chen, Z.Q.; “A new image encryption algorithm based on hyper-chaos”, Phys. Lett. A, 2008, Vol. 372, Issue 4, pp. 394-400.

[21] El-Sayed, M.; El-Alfy; Khaled, A.; Al-Utaibi; “An Encryption Scheme for Color Images Based on Chaotic Maps and Genetic Operators”, The Seventh International Conference on Networking and Services, 2011, Venice/Mestre, Italy, pp. 92-97.

[22] Baptista, M.S.; “Cryptography with chaos”, Phys Lett A, 1998, Vol. 240, Issue 1-2, pp. 50–54.

[23] Luiz, P.L. de Oliveira, Sobottka, M.; “Cryptography with chaotic mixing” Chaos, Solitons and Fractals, 2008, Vol. 35, Issue 3, pp. 466–471.

[24] Gao, H.; Zhang, Y.; Liang, S.; Li, D.; “A new chaotic algorithm for image encryption”, Chaos, Solitons and Fractals, 2006, Vol. 29, Issue 2, pp. 393–399.

[25] Kocarev, L.; “Chaos-based cryptography: a brief overview”, Circuits and Systems Magazine, IEEE, 2001, Vol. 1, issue 3, pp. 6–21.

[26] Ponomarenko, V.I.; Prokhorov, M.D.; “Extracting information masked by the chaotic signal of a time-delay system”, Phys Rev E, 2002, Vol. 66, Issue 2, pp. 15-21.

[27] Wang, Q.; Ding, Q.; Zhang, Z.; Ding, L.; “Digital Image Encryption Research Based on DWT and Chaos” IEEE Transactions, 2008, pp. 494-498.

[28] Zhang, Y.H.; “Image encryption using extended chaotic sequences”, IEEE Transactions International Conference on Intelligent Computation Technology and Automation, 2011, pp. 143-146.

[29] Shen, J., Jin, X., and Zhou, C.; “A Color Image Encryption Algorithm Based on Magic Cube Transformation and Modular Arithmetic Operation”, PCM, Part II, LNCS, 2005, 3768, pp. 270-280.

[30] Li. C.; Li, S.; Zhang, D.; Chen, G.; “Cryptanalysis of a Chaotic Neural Network Based Multimedia Encryption Scheme”, in Proceedings of Advances in Multimedia Information Processing, PCM 2004, Part III, LNCS, Vol. 3333, pp. 418-425.

[31] Keshari, S., Modani, S.G.; “Image Encryption Algorithm based on Chaotic Map Lattice

and Arnold cat map for Secure Transmission", International Journal of Computer Science and Technology, 2011, Vol. 1, Issue 2, pp. 132-135.

[32] Fu, C.; Zhang, Z.; Cao, Y.; "An Improved Image Encryption Algorithm Based on Chaotic Maps", ICCS, 2007, Vol. 4487, pp. 575-582.

[33] Lian, S.; "Efficient image or video encryption based on spatiotemporal chaos system", Chaos Solitons Fractals, 2009, Vol. 40, Issue 5, pp. 2509-2519.

[34] Rhouma, R.; Belghith, S.; "Cryptanalysis of a spatiotemporal chaotic image/video cryptosystem", Phys. Lett. A, 2008, Vol. 372, Issue 36, pp. 5790-5794.

[35] Huang, C.K.; Nien, H. H.; "Multi chaotic systems based pixel shuffle for image encryption," Optics Communications, 2009, Vol. 282, Issue 11, pp. 2123–2127.

[36] Solak, E.; Rhouma, R.; Belghith, S.; "Cryptanalysis of a multi-chaotic systems based image cryptosystem", Optics Communications, 2010, Vol. 283, Issue 2, pp.232–236.

[37] Ahmad, M.; Farooq, O.; "A Multi-Level Blocks Scrambling Based Chaotic Image Cipher", Communications in Computer and Information Science, 2010, Vol. 94, Part 1, pp. 171-182.

[38] Wu, Y.; Noonan, J.P.; Agaian, S.; "NPCR and UACI Randomness Tests for Image Encryption", Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), April Edition, 2011, pp. 31-38.

[39] Rodgers, J.L.; J.L.; Nicewander, W.A.; "Thirteen Ways to look at the Correlation Coefficient", American Statistic, 1992, Vol. 42, pp. 59-66.

[40] Jenkin, M.; Jepson, A.D.; Tsotsos, J.L.; "Techniques for Disparity Measurement", CVGIP: Image Understanding, 1991, Vol. 53, pp. 14-30.

[41] Hall, E.H.; "Computer Image Processing and Recognition", Academic: New York, 1979, pp. 480-485.

[42] Lee, J.; "Cautionary Note on the Use of the Correlation-Coefficient", British Journal of Industrial Medicine, 1992, Vol. 79, pp. 526-527.